



## **VPN Client User Guide for Linux and Solaris**

Release 4.6  
August, 2004

### **Corporate 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: 408 526-4100

Text Part Number: OL-5491-01



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

*Cisco VPN Client User Guide for Linux and Solaris*  
Copyright © 2004, Cisco Systems, Inc.  
All rights reserved.

<b>About This Guide</b>	<b>v</b>
Audience	v
Contents	v
Related Documentation	vi
Terminology	vi
Document Conventions	vi
Data Formats	vii
Obtaining Documentation	vii
Cisco.com	vii
Documentation CD-ROM	vii
Ordering Documentation	vii
Documentation Feedback	viii
Obtaining Technical Assistance	viii
Cisco.com	viii
Technical Assistance Center	ix
Cisco TAC Website	ix
Cisco TAC Escalation Center	ix
Obtaining Additional Publications and Information	x
<b>Understanding the VPN Client</b>	<b>1-1</b>
VPN Client Overview	1-1
VPN Client Features	1-2
Main Features	1-2
Program Features	1-3
IPSec Features	1-5
IPSec Attributes	1-5
Authentication Features	1-6
<b>Installing the VPN Client</b>	<b>2-1</b>
Uninstalling an Old Client	2-1
Uninstalling a VPN Client for Solaris	2-1
Uninstalling a VPN Client for Linux	2-1
Gathering Information You Need	2-2
Verifying System Requirements	2-2
Linux System Requirements	2-2
Firewall Issues	2-2

- Troubleshooting Tip 2-3
  - Bundling a Root Certificate with the Installation Package—Linux 2-3
  - Bundling a Root Certificate with the Installation Package—Solaris 2-3
  - Solaris System Requirements 2-4
    - Changing a Kernel Version 2-4
  - Unpacking the VPN Client Files 2-4
  - Installing the Software 2-5
    - Installing the VPN Client for Linux 2-5
      - Kernel Source Requirements 2-6
      - VPN Client for Linux Install Script Notes 2-6
    - Installing the VPN Client for Solaris 2-7
      - VPN Client for Solaris Install Script Notes 2-8
- User Profiles 3-1**
  - Sample Profile Description 3-1
  - Modifying the Sample Profile 3-2
  - Creating a User Profile 3-2
- Using the Command-Line Interface 4-1**
  - Displaying a List of Commands 4-1
  - Establishing a Connection 4-1
    - Authentication Prompts 4-2
    - Rekeying Issues 4-3
    - DNS Server Settings 4-3
  - Disconnecting the VPN Client 4-3
  - Displaying VPN Client Statistics 4-4
    - Examples 4-4
      - No Options 4-4
      - Reset Option 4-5
      - Traffic Option 4-5
      - Tunnel Option 4-5
      - Route Option 4-5
  - Event Logging 4-6
    - Enabling Logging 4-6
    - Viewing Log Files 4-6
    - Client Auto Update Messages 4-7



## About This Guide

---

This guide describes how to install, use, and manage the Cisco VPN Client for the following operating systems:

- Linux for Intel—Red Hat Version 6.2 or later, or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.
- Solaris UltraSPARC 5
- SunBlade

## Audience

This guide is for remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. You should be familiar with UNIX platforms and know how to use UNIX applications. Network administrators should be familiar with UNIX system configuration and management and know how to install, configure, and manage internetworking systems.

## Contents

This guide contains the following chapters:

- [Chapter 1, “Understanding the VPN Client.”](#) This chapter provides a brief introduction to the VPN Client software.
- [Chapter 2, “Installing the VPN Client.”](#) This chapter describes how to install the VPN Client software on your workstation.
- [Chapter 3, “User Profiles.”](#) This chapter describes how to set up user profiles for connection entries.
- [Chapter 4, “Using the Command-Line Interface.”](#) This chapter describes the command-line interface and lists the commands and their descriptions.
- Index

## Related Documentation

The following is a list of user guides and other documentation related to the VPN Client for Linux and Solaris and the VPN devices that provide the connection to the private network.

- *Release Notes for the Cisco VPN Client, Version 4.6*
- *Cisco VPN Client Administrator Guide, Release 4.6*
- *Cisco VPN 3000 Series Concentrator Getting Started Guide, Release 4.1*
- *Cisco VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.1*
- *Cisco VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.1*

## Terminology

In this user guide:

- The term *Cisco VPN device* refers to the following Cisco products:
  - Cisco IOS devices that support Easy VPN server functionality
  - VPN 3000 Series Concentrators
  - Cisco PIX Firewall Series
- The term *PC* refers generically to any personal computer.

## Document Conventions

This guide uses the following typographic conventions:

- **Boldface** font—Describes user actions and commands.
- *Italic* font—Describes arguments that you supply the values for.
- `Screen` font—Describes terminal sessions and information displayed by the system.
- **Boldface screen** font—Describes information that you must enter.



### Note

---

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

---



### Caution

---

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

---

## Data Formats

When you configure the VPN Client, enter data in these formats unless the instructions indicate otherwise.

- IP Address—Use standard 4-byte dotted decimal notation (for example, 192.168.12.34). You can omit leading zeros in a byte position.
- Host names—Use legitimate network host or end-system name notation (for example, VPN01). Spaces are not allowed. A host name must uniquely identify a specific system on a network. A host name can be up to 255 characters in length.
- User names and Passwords—Text strings for user names and passwords use alphanumeric characters in both upper- and lower case. Most text strings are case sensitive. For example, simon and Simon would represent two different user names. The maximum length of user names and passwords is generally 32 characters, unless specified otherwise.

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpc/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## 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.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:  
[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)



# Understanding the VPN Client

---

The Cisco VPN Client is a software application that runs on computers using any of the following operating systems:

- Linux for Intel—Red Hat Version 6.2 or later, or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.
- Solaris UltraSPARC 5
- SunBlade

The following platforms are not supported

- SunRay
- SunFire Series
- Netra Series
- Tadpole

Solaris and Linux VPN Clients support only single interface FastEthernet network adapters. These VPN Clients do not support multiport adapters such as dual and quad FastEthernet.



**Note**

---

The VPN Client for Solaris can receive no greater than 20 subinterfaces (IP addresses assigned to the same machine).

---

The VPN Client on a remote PC, communicating with a Cisco VPN device on an enterprise network or with a service provider, creates a secure connection over the Internet. This connection allows you to access a private network as if you were an on-site user, creating a virtual private network (VPN).

The following VPN devices can terminate VPN connections from VPN Clients:

- Cisco IOS devices that support Easy VPN server functionality
- VPN 3000 Series Concentrators
- Cisco PIX Firewall Series

## VPN Client Overview

The VPN Client works with a Cisco VPN device to create a secure connection, called a tunnel, between your computer and a private network. It uses Internet Key Exchange (IKE) and IP Security (IPSec) tunneling protocols to establish and manage the secure connection.

The steps used to establish a VPN connection can include:

- Negotiating tunnel parameters (addresses, algorithms, lifetime)
- Establishing VPN tunnels according to the parameters
- Authenticating users (from usernames, group names and passwords, and X.509 digital certificates)
- Establishing user access rights (hours of access, connection time, allowed destinations, allowed protocols)
- Managing security keys for encryption and decryption
- Authenticating, encrypting, and decrypting data through the tunnel

For example, to use a remote PC to read e-mail at your organization, the connection process might be similar to the following:

1. Connect to the Internet.
2. Start the VPN Client.
3. Establish a secure connection through the Internet to your organization's private network.
4. When you open your e-mail

The Cisco VPN device

- Uses IPSec to encrypt the e-mail message
- Transmits the message through the tunnel to your VPN Client

The VPN Client

- Decrypts the message so you can read it on your remote PC
  - Uses IPSec to process and return the message to the private network through the Cisco VPN device
- 



## VPN Client Features

The tables in the following sections describe the VPN Client features.

### Main Features

Table 1-1 lists the VPN Client main features.

**Table 1-1 Main Features**

Features	Description
Operating Systems	<ul style="list-style-type: none"> <li>Linux (Intel)</li> <li>Solaris (UltraSPARC-32 and 64 bit)</li> <li>SunBlade</li> </ul>
Connection types	<ul style="list-style-type: none"> <li>Linux supports—async serial PPP, Internet-attached Ethernet, and ISDN.</li> <li>Solaris supports—async serial PPP and Internet-attached Ethernet.</li> </ul> <p> <b>Note</b> The VPN Client no longer supports the ipdptp dialup interface used on older versions of the Solaris platform.</p> <ul style="list-style-type: none"> <li>– Solaris 6 and 7 users must use VPN Client Versions 3.7 or earlier to continue using the ipdptp dialup interface.</li> <li>– Solaris 8 users must apply the patch from SUN that allows them to use the new pppd 4.0 driver.</li> </ul> <p> <b>Note</b> The VPN Client supports only one PPP and one Ethernet adapter.</p>
Protocol	IP
Tunnel protocol	IPSec
User Authentication	<ul style="list-style-type: none"> <li>RADIUS</li> <li>RSA SecurID</li> <li>VPN server internal user list</li> <li>PKI digital certificates</li> <li>NT Domain (Windows NT)</li> </ul>

## Program Features

The VPN Client supports the program features listed in [Table 1-2](#).

**Table 1-2 Program Features**

Program Feature	Description
Servers Supported	<ul style="list-style-type: none"> <li>Cisco IOS devices that support Easy VPN server functionality</li> <li>VPN 3000 Series Concentrators</li> <li>Cisco PIX Firewall Series</li> </ul>
Local LAN access	The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN device (if the central site grants permission).

Table 1-2 Program Features (continued)

Program Feature	Description
Automatic VPN Client configuration option	The ability to import a configuration file.
Event logging	The VPN Client log collects events for viewing and analysis.
NAT Transparency (NAT-T)	Enables the VPN Client and the VPN device to automatically detect when to use IPSec over UDP to work properly in port address translation (PAT) environments.
Update of centrally controlled backup server list	The VPN Client learns the backup VPN server list when the connection is established. This feature is configured on the VPN device and pushed to the VPN Client. The backup servers for each connection entry are listed on the Backup Servers tab.
Set MTU size	The VPN Client automatically sets a size that is optimal for your environment. However, you can also set the MTU size manually. For information on adjusting the MTU size, see the <i>Cisco VPN Client Administrator Guide</i> .
Support for Dynamic DNS (DDNS host name population)	The VPN Client sends its host name to the VPN device when the connection is established. If this occurs, the VPN device can send the host name in a DHCP request. This causes the DNS server to update its database to include the new host name and VPN Client address.
Notifications	Software update notifications from the VPN server upon connection.
Delete with reason	<p>The VPN Client provides you with a reason code or reason text when a disconnect occurs. The VPN Client supports the delete with reason function for client-initiated disconnects, concentrator-initiated disconnects, and IPSec deletes.</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• If you are using a command-line client, the message appears on your terminal and is logged in the IPSec log.</li> <li>• 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.</li> </ul> <p><b>Note</b> The VPN device must be running software version 4.0 or later to support this functionality.</p>
Single-SA	The ability to support a single security association (SA) per VPN connection. Rather than creating a host-to-network SA pair for each split-tunneling network, this feature provides a host-to-ALL approach, creating one tunnel for all appropriate network traffic apart from whether split-tunneling is in use.
Auto initiation	The ability to automatically initiate secure wireless VPN connections seamlessly. For information on this feature, see <i>VPN Client Administrator Guide</i> .

## IPSec Features

The VPN Client supports the IPSec features listed in [Table 1-3](#).

**Table 1-3** IPSec Features

IPSec Feature	Description
Tunnel Protocol	IPSec
Transparent tunneling	<ul style="list-style-type: none"> <li>IPSec over UDP for NAT and PAT</li> <li>IPSec over TCP for NAT and PAT</li> </ul>
Key Management protocol	Internet Key Exchange (IKE)
IKE Keepalives	A tool for monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer. This lets the VPN Client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
Split tunneling	The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel. The VPN device supplies a list of networks to the VPN Client for tunneled traffic. You enable split tunneling on the VPN Client and configure the network list on the VPN device.
Support for Split DNS	The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network. For example, a query for a packet destined for corporate.com would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for myfavoritesearch.com would be handled by the ISP's DNS. This feature is configured on the VPN server (VPN concentrator) and enabled on the VPN Client by default. To use Split DNS, you must also have split tunneling configured.


## IPSec Attributes

The VPN Client supports the IPSec attributes listed in [Table 1-4](#).

**Table 1-4** IPSec Attributes

IPSec Attribute	Description
Main Mode and Aggressive Mode	Ways to negotiate phase 1 of establishing ISAKMP Security Associations (SAs)
Authentication algorithms	<ul style="list-style-type: none"> <li>HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function</li> <li>HMAC with SHA-1 (Secure Hash Algorithm) hash function</li> </ul>

**Table 1-4** IPsec Attributes (continued)

IPsec Attribute	Description
Authentication Modes	<ul style="list-style-type: none"> <li>• Preshared Keys</li> <li>• Mutual group authentication</li> <li>• X.509 Digital Certificates</li> </ul>
Diffie-Hellman Groups	<ul style="list-style-type: none"> <li>• Group 1 = 768-bit prime modulus</li> <li>• Group 2 = 1024-bit prime modulus</li> <li>• Group 5 = 1536-bit prime modulus</li> </ul> <p> <b>Note</b> See the <i>Cisco VPN Client Administrator Guide</i> for more information about DH Group 5.</p>
Encryption algorithms	<ul style="list-style-type: none"> <li>• 56-bit DES (Data Encryption Standard)</li> <li>• 168-bit Triple-DES</li> <li>• AES 128-bit and 256-bit</li> </ul>
Extended Authentication (XAUTH)	The capability of authenticating a user within IKE. This authentication is in addition to the normal IKE phase 1 authentication, where the IPsec devices authenticate each other. The extended authentication exchange within IKE does not replace the existing IKE authentication.
Mode Configuration	Also known as ISAKMP Configuration Method
Tunnel Encapsulation Modes	<ul style="list-style-type: none"> <li>• IPsec over UDP (NAT/PAT)</li> <li>• IPsec over TCP (NAT/PAT)</li> </ul>
IP compression (IPCOMP) using LZS	Data compression algorithm

## Authentication Features

The VPN Client supports the authentication features listed in [Table 1-5](#).

**Table 1-5** Authentication Features

Authentication Feature	Description
User authentication through VPN central-site device	<ul style="list-style-type: none"> <li>• Internal through the VPN device's database</li> <li>• RADIUS</li> <li>• NT Domain (Windows NT)</li> <li>• RSA (formerly SDI) SecurID or SoftID</li> </ul>
Certificate Management	Allows you to manage the certificates in the certificate stores.
Certificate Authorities (CAs)	CAs that support PKI SCEP enrollment.



**Table 1-5 Authentication Features**

<b>Authentication Feature</b>	<b>Description</b>
Ability to authenticate using smart cards	Physical SecurID cards or keychain fobs for passcode generation.
Peer Certificate Distinguished Name Verification	Prevents a VPN Client from connecting to an invalid 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 VPN Client connection also fails.





## Installing the VPN Client

---

This chapter describes how to install the VPN Client software on your workstation.

You should be familiar with software installation on UNIX computers to perform this procedure.

The VPN Client consists of:

- A driver, which is a loadable module.
- A set of commands accessible through your shell, which is used to access the applications.

The commands and some parts of the driver are distributed in binary form only.

## Uninstalling an Old Client

This section describes how to uninstall the VPN Client.

- You *must* uninstall an old VPN Client for Solaris before you install a new VPN Client.
- You are *not required* to uninstall an old VPN Client for Linux before you install a new VPN Client.
- You must uninstall any VPN 5000 Client before you install a VPN Client. Refer to the Cisco VPN 5000 Client documentation for more information.

## Uninstalling a VPN Client for Solaris

If a VPN Client for Solaris was previously installed, you must remove the old VPN Client before you install a new one.

To uninstall a package, use the **pkgrm** command. For example:

```
pkgrm vpnclient
```

## Uninstalling a VPN Client for Linux

To uninstall the VPN Client for Linux:

---

**Step 1** Run the following command:

```
sudo /usr/local/bin/vpn_uninstall
```

**Step 2** You are prompted to remove all profiles and certificates.

- If you answer yes, all binaries, startup scripts, certificates, profiles, and any directories that were created during the installation process are removed.
  - If you answer no, all binaries and startup scripts are removed, but certificates, profiles, and the vpnclient.ini file remain.
- 

## Gathering Information You Need

To configure and use the VPN Client, you might be required to have the following information.

This information is normally obtained from the system administrator of the private network you want to access. The system administrator might preconfigure much of this data.

- Hostname or IP address of the secure gateway you are connecting to
- Your IPsec Group Name (for preshared keys)
- Your IPsec Group Password (for preshared keys)
- The name of the certificate, if authenticating with a digital certificate
- Your username and password, if authenticating through:
  - The secure gateway's internal server
  - A RADIUS server
  - An NT Domain server
- Your username and PIN, if authenticating through a token vendor
- The hostnames or IP addresses of the backup servers, if you should configure backup server connections

## Verifying System Requirements

This section describes system requirements for the VPN Client for each operating system.

### Linux System Requirements

The VPN Client for Linux supports Red Hat Version 6.2 Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.

**Note**

The VPN Client for Linux does not support kernel Version 2.5 prior to VPN Client Release 4.0.1.A and does not support SMP (multiprocessor) kernels in any release of the VPN Client.

---

### Firewall Issues

If you are running a Linux firewall (for example, ipchains or iptables), be sure that the following types of traffic are allowed to pass through:

- UDP port 500

- UDP port 10000 (or any other port number being used for IPSec/UDP)
- IP protocol 50 (ESP)
- TCP port configured for IPSec/TCP
- NAT-T (Standards-Based NAT Transparency) port 4500

## Troubleshooting Tip

The following two lines might be added by default with your Linux installation in the `/etc/sysconfig/ipchains` directory. For Red Hat, this might be written to the `/etc/sysconfig/ipchains` directory. These two commands might prevent UDP traffic from passing through.

```
-A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT
-A input -p udp -s 0/0 -d 0/0 2049 -j REJECT
```

If you have problems with UDP traffic, try one of the following solutions:

- First delete the above two reject lines, then enter the following two commands:

```
/etc/init.d/ipchains stop
/etc/init.d/ipchains start
```



**Note** The ipchains might be replaced by iptables or it might be located in a different directory on your Linux distribution.

- Add the following rule to the default ipchains firewall configuration, or add it above any UDP reject line.

```
-A input -p udp -s 0/0 -d 0/0 500 -j ACCEPT
```

This rule allows UDP port 500, which is required for the VPN Client connection.

## Bundling a Root Certificate with the Installation Package—Linux

To use mutual authentication, the VPN Client system must have a root certificate installed. You can bundle a root certificate with the installation package so that the root certificate is installed automatically during installation. The following commands place a root certificate with the installation package. The root certificate is contained in a file. The name of the file must be rootcert with no extension.

```
zcat vpnclient-linux-<version>-K9.tar.gz | tar xf -
rm -f vpnclient-linux-<version>-K9.tar.gz
cp -f <path_to_root_cert>/<root_cert_filename> vpnclient/rootcert
tar czf vpnclient-linux-<version>-K9.tar.gz vpnclient
```

## Bundling a Root Certificate with the Installation Package—Solaris

To use mutual authentication, the VPN Client computer must have a root certificate installed. You can bundle a root certificate with the installation package so that the root certificate is installed automatically. The following commands place a root certificate with the installation package. The root certificate is contained in a file. The name of the file must be rootcert with no extension.

```
zcat vpnclient-solaris-<version>-K9.tar.Z | tar xf -
rm -f vpnclient-solaris-<version>-K9.tar.Z
cp -f <path_to_root_cert>/<root_cert_filename> vpnclient/rootcert
tar cf - vpnclient | compress -c > vpnclient-solaris-<version>-K9.tar.Z
```

## Solaris System Requirements

The VPN Client for Solaris runs on any UltraSPARC computer running a 32-bit or 64-bit Solaris kernel OS Version 2.6 or later.

## Changing a Kernel Version

You can install the VPN Client running the 32-bit or 64-bit version of the kernel (referred to as 32-bit mode and 64-bit mode). If you experience problems installing or running the VPN Client in one mode, try the other one.

To see which mode the system is running in, enter this command:

```
isainfo -kv
```

If the cipsec module is loaded correctly, the dmesg log displays a message similar to the following:

```
Oct 29 11:09:54 sol-2062 cipsec: [ID 952494 kern.notice] Cisco Unity IPsec Module Load OK
```



### Note

If the dmesg log does not show the cipsec log message, you should switch to the other mode.

To switch to 32-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):  
`ok boot kernel/unix`
- Permanently—Enter the following command as root, then restart your computer:  
`eeeprom boot-file=/platform/sun4u/kernel/unix`

To switch to 64-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):  
`ok boot kernel/sparcv9/unix`
- Permanently—Enter the following command as root, then restart your computer:  
`eeeprom boot-file=/platform/sun4u/kernel/sparcv9/unix`

## Unpacking the VPN Client Files

The VPN Client is shipped as a compressed tar file.

To unpack the files

- 
- Step 1** Download the packed files, either from your internal network or the Cisco website, to a directory of your choice.
  - Step 2** Copy the VPN Client file to a selected directory.

**Step 3** Unpack the file using the **zcat** and **tar** commands.

For example, the command for Linux is:

```
zcat vpnclient-linux-3.7.xxx-K9.tar.gz | tar xvf -
```

The command for Solaris is:

```
zcat vpnclient-solaris-3.7.xxx-K9.tar.Z | tar xvf -
```

This command creates the `vpnclient` directory in the current directory.

---

## Installing the Software

The following sections describe the installation procedure for the VPN Client for each operating system.

### Installing the VPN Client for Linux

Before you install a new version of the VPN Client, or before you reinstall your current version, you must use the **stop** command to disable VPN service.

If you are upgrading from the VPN 5000 Client to the VPN Client, use the following **stop** command:

```
/etc/rc.d/init.d/vpn stop
```

If you are upgrading from the VPN 3000 Client to the VPN Client, use the following **stop** command:

```
/etc/rc.d/init.d/vpnclient_init stop
```

To install the VPN Client for Linux

---

**Step 1** Obtain superuser privileges to run the install script.

**Step 2** Enter the following commands:

```
cd vpnclient
./vpn_install
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/lib/modules/<kernel version>/build/]
- Automatically start the VPN service at boot time [yes]
- Directory containing linux kernel source code [/usr/src/linux]
- Is the above correct [y]

**Step 3** Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.

**Step 4** If the installer cannot auto detect these settings, you might receive the following prompts:

- Directory containing init scripts:
  - The directory where scripts that are run at boot time are kept. Typically this is `/etc/init.d` or `/etc/rc.d/init.d`

- Directory containing run level directories (rcX.d):
  - The directory that contains init's run level directories. Typically this is /etc or /etc/rc.d

**Step 5** Enable the VPN service by using one of the following methods:

- Restart your computer.
- Enable the service without restarting. Enter the following command:

```
/etc/rc.d/init.d/vpnclient_init start
```

## Kernel Source Requirements

To install the VPN Client, you must have the kernel source that was used to build the kernel that is running on the system. If the system is using a kernel that came as part of the Linux distribution, or a custom built kernel, the kernel code can be obtained in different ways:

- For users running kernels that came with their distribution—You must install the corresponding kernel-source rpm. The `vpn_install` script should be able to automatically find the kernel source.
- For users running a custom-built kernel—You must use the same copy of the kernel source that was used to build the kernel you are running. Unpacking the source code for the version of the kernel you are using is insufficient. There are several files generated when the kernel is compiled that the VPN Client uses. These files must exactly match with the kernel you are running. Otherwise, the VPN Client installation might fail.



### Note

If you install a patch on the workstation kernel, you must reinstall the VPN Client using these guidelines.

## VPN Client for Linux Install Script Notes

During the installation process:

1. The module is compiled, linked, and copied to either the directory `/lib/modules/preferred/CiscoVPN`, if it exists, or to `/lib/modules/system/CiscoVPN`, where *system* is the kernel version.
2. The application binaries are copied to the specified destination directory.
3. The startup file `/etc/rc.d/init.d/vpnclient_init` is created to enable and disable the VPN service.
4. The links `/etc/rc3.d/s85vpnclient` and `/etc/rc5.d/s85vpnclient` are added to run level 3 and level 5 if startup at boot time is requested.

These links allow the tunnel server to start at boot time and run in levels 3 and 5.



## Installing the VPN Client for Solaris

Before you install a new version of the VPN Client, or before you reinstall your current version, you must uninstall the old VPN Client. See the “[Uninstalling an Old Client](#)” section on page 2-1 for more information.

**Note**

---

If you are installing the VPN Client for Solaris, Release 3.7 or later on a Version 2.6 Solaris platform, you receive the following message during the VPN Client installation: “Patch 105181 version 29 (or higher) to Solaris 2.6 is required for the client to function properly. Installing without this patch will cause the kernel to crash as soon as the client kernel module is loaded. This patch is available from Sun as part of the "Recommended Solaris Patch Cluster". If you proceed with installation, the kernel module will not be enabled. After you have installed the patch, you may enable the kernel module by uncommenting all lines in /etc/iu.ap that contain ‘cipsec’.”

---

To install the VPN Client for Solaris

---

**Step 1** Obtain superuser privileges to run the install script.

**Step 2** Enter the following command:

```
pkgadd -d . vpnclient
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/usr/local/bin]
- Is the above correct [y]
- If the installer finds a conflict with the VPN Client files and another application, you receive this message:  
The following files are already installed on the system and are being used by another package:<installer lists files> Do you want to install these conflicting files [y,n,?,q]
- The following files are being installed with setuid and/or setgid permissions:<installer lists files>Do you want to install these as setuid/setgid files [y,n,?,q]
- This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <vpnclient> [y,n,?]

**Step 3** Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user’s path.

**Step 4** Restart your computer.

---

## VPN Client for Solaris Install Script Notes

During the installation process:

1. The following line is added to the `/etc/iu.ap` file to enable the autopush facility at startup:

```
<dev_name> -1 0 cipsec
```

where `dev_name` is the name of the interface without the trailing numbers (for example `ipdtp`, `le`, or `hme`). A line is added for every supported network device detected.

2. The VPN module is copied to the `/kernel/strmod` directory, which is in the system's module search path.

The **pkginfo** command provides information about the installed packages. For more information on other package-related commands, enter:

```
man pkgadd
```



## User 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). User profiles reside in the default directory `/etc/CiscoSystemsVPNClient/Profiles/`, or in the directory specified during the VPN Client installation.

User profile parameters include the remote server address, IPSec group name and password, use of a log file, use of backup servers, and automatic connect upon startup. Each connection entry has its own user profile.



### Note

---

User profiles for the VPN Client are interchangeable between platforms. Keywords that are specific to the Windows platform are ignored by other platforms.

---

This chapter describes how to create a VPN Client user profile.

To set global profiles for all users, refer to the *Cisco VPN Client Administrator Guide*.

## Sample Profile Description

There are two ways to create a user profile:

- Use a text editor to modify the sample profile that comes with the VPN Client installer and rename it.
- Create a unique user profile using a text editor.

There is only one user profile per connection.

The VPN Client software is shipped with a sample user profile. The file is named `sample.pcf`.

The following is an example of a sample user profile that might be shipped with your installer.

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=gawf
SaveUserPassword=0
EnableBackup=0
```

```

BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0

```

## Modifying the Sample Profile

To modify the sample profile

- 
- Step 1** Using a text editor, open the sample user profile.
  - Step 2** Modify the keywords you want to change.  
See your administrator for IP addresses, user name, and any security information.
  - Step 3** Save your new profile with a unique name in the `/etc/CiscoSystemsVPNClient/Profiles/` directory.  
When you use the `vpnclient connect` command to establish a connection, use your new profile name.
- 

## Creating a User Profile

You can create your own user profile from scratch by using any text editing program.

At a minimum, you need the following keywords listed in your profile:

- [main]
- Host
- AuthType
- GroupName
- Username

Save your new profile in the `/etc/CiscoSystemsVPNClient/Profiles/` directory. See your administrator for IP addresses, user names, and any security information.

[Table 3-1](#) describes keywords that can be in a user profile. User profile keywords are not case sensitive unless indicated in the description.


**Table 3-1** User Profile Keywords

Keywords	Description
[main]	A required keyword that identifies the main section. Enter exactly as shown as the first entry in the user profile.
<b>Description</b> = <i>String</i>	This optional keyword describes this user profile. The maximum length is 246 alphanumeric characters.

Table 3-1 User Profile Keywords (continued)

Keywords	Description
<b>Host</b> = <i>IP_Address or hostname</i>	The hostname or IP address of the VPN device you want to connect with. The maximum length of the hostname is 255 alphanumeric characters.
<b>AuthType</b> = {1   3   5}	<p>The authentication type that this user is using.</p> <ul style="list-style-type: none"> <li>• <b>1</b> is preshared keys.</li> <li>• <b>3</b> is a digital certificate using an RSA signature.</li> <li>• <b>5</b> is mutual group authentication</li> </ul> <p>If you select <b>AuthType 1</b> or <b>AuthType 5</b>, you must also configure the <b>GroupName</b> and <b>GroupPwd</b>. To use <b>AuthType5</b>, you must have a root certificate on your VPN Client system. For information on how to install a root certificate automatically on your specific platform, see “<a href="#">Installing the VPN Client.</a>”</p>
<b>GroupName</b> = <i>String</i>	The name of the IPSec group configured on the VPN device that contains this user. The maximum length is 32 alphanumeric characters. This keyword is case sensitive.
<b>GroupPwd</b> = <i>String</i>	The password for the IPSec group that contains this user. The minimum length is 4 alphanumeric characters. The maximum is 32. This keyword is case sensitive and entered in clear text.
<b>encGroupPwd</b> = <i>String</i>	Displays the group password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
<b>Username</b> = <i>String</i>	The name that identifies a user as a valid member of the IPSec group specified in <b>GroupName</b> . The VPN Client prompts the user for this value during user authentication. The maximum length is 32 alphanumeric characters. This keyword is case sensitive and entered in clear text.
<b>UserPassword</b> = <i>String</i>	<p>This password is used during extended authentication.</p> <ul style="list-style-type: none"> <li>• If <b>SaveUserPassword</b> is enabled, the first time the VPN Client reads this password, it is saved in the user profile as <b>encUserPassword</b>, and the clear text version is deleted.</li> <li>• If <b>SaveUserPassword</b> is disabled, the VPN Client deletes the clear text version of the user password in the user profile but it does not create an encrypted version.</li> </ul>
<b>encUserPassword</b> = <i>String</i>	Displays the user password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
<b>SaveUserPassword</b> = {0   1}	<p>Determines if the user password or its encrypted form are valid in the user profile.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, displays the user password in clear text in the user profile and is saved locally.</li> <li>• <b>1</b> displays the user password in the user profile in its encrypted version, and the password is not saved locally.</li> </ul> <p>This value is set in the VPN device, not in the VPN Client.</p>

Table 3-1 User Profile Keywords (continued)

Keywords	Description
<b>EnableBackup</b> = {0   1}	<p>Specifies to use a backup server if the primary server is not available.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, disables the backup server.</li> <li>• <b>1</b> enables the backup server.</li> </ul> <p>You must also specify a <b>BackupServer</b>.</p>
<b>BackupServer</b> = <i>IP_Address or hostname</i>	List of IP addresses or hostnames of backup servers. Separate multiple entries by commas. The maximum length of hostname is 255 alphanumeric characters.
<b>EnableLocalLAN</b> = {0   1}	<p>Allows you to configure access to your local LAN.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, disables local LAN access.</li> <li>• <b>1</b> enables local LAN access.</li> </ul> <p> <b>Note</b> To allow local LAN access, it must be enabled on both the VPN Client and the VPN device you are connecting to.</p>
<b>EnableNAT</b> = {0   1}	<p>Specifies whether or not to enable secure transmission between a VPN Client and a VPN device through a router serving as a firewall, which might also be using the NAT protocol.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, disables IPsec through NAT mode.</li> <li>• <b>1</b> enables IPsec through NAT mode.</li> </ul>
<b>TunnelingMode</b> = {0   1}	<p>Allows you to select which form of NAT transversal is used.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, specifies IPsec over UDP for NAT transparency.</li> <li>• <b>1</b> specifies IPsec over TCP for NAT transparency.</li> </ul> <p>You must also have IPsec through NAT enabled.</p>
<b>TCP TunnelingPort</b> = {0   65535}	Sets which TCP port to use for the cTCP protocol. The default is 10000. You must also have IPsec through NAT enabled and the Tunneling Mode set for IPsec over TCP.
<b>ForceKeepAlives</b> = {0   1}	<p>Allows the VPN Client to keep sending IKE and ESP keepalives for a connection at approximately 20-second intervals so that the port on an ESP-aware NAT/Firewall does not close.</p> <ul style="list-style-type: none"> <li>• <b>0</b>, the default, disables keepalives.</li> <li>• <b>1</b> enables keepalives.</li> </ul>
<b>PeerTimeout</b> = <i>Number</i>	The number of seconds to wait before terminating a connection when the VPN device on the other end of the tunnel is not responding. The range is 30 to 480 seconds. The default is 90.
<b>CertStore</b> = {0   1}	<p>Identifies the type of store containing the configured certificate.</p> <ul style="list-style-type: none"> <li>• <b>0</b> = default, none.</li> <li>• <b>1</b> = Cisco.</li> </ul>
<b>CertName</b> = <i>String</i>	Identifies the certificate used to connect to the VPN device. The maximum length is 129 alphanumeric characters.

**Table 3-1** User Profile Keywords (continued)

Keywords	Description
<b>CertPath</b> = <i>String</i>	The path name of the directory containing the certificate file. The maximum length is 259 alphanumeric characters.
<b>CertSubjectName</b> = <i>String</i>	The qualified Distinguished Name (DN) of the certificate's owner. You can either <i>not</i> include this keyword in the user profile, or leave this entry blank.
<b>CertSerialHash</b> = <i>String</i>	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. You can either <i>not</i> include this keyword in the user profile, or leave this entry blank.
<b>DHGroup</b> = {1   2   5}	<p>Allows a network administrator to override the configured group value used to generate Diffie-Hellman key pairs on a VPN device.</p> <ul style="list-style-type: none"> <li>• 1 = modp group 1</li> <li>• 2 = modp group 2</li> <li>• 5 = modp group 5</li> </ul> <p>The default is 2. The VPN Concentrator configuration for IKE Proposal must match the DHGroup in the VPN Client. If the AuthType is set to 3 (digital certificate), this keyword has no effect on the VPN Client.</p>







## Using the Command-Line Interface

---

This chapter describes common operations using the command-line interface. 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.

For more detailed information about using the VPN Client command-line interface, see the *Cisco VPN Client Administrator Guide*. Also, that user guide contains instructions on how to manage the Certificate Manager application from the command line.

### Displaying a List of Commands

To display a list of available VPN Client commands, locate the directory that contains the VPN Client software and enter the **vpnclient** command at the command line prompt.

The following example shows the command and the information that is displayed:

```
[root@Linux7_1 unity]# vpnclient
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686

Usage:
  vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
                                     [nocertpwd]

  vpnclient disconnect
  vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
  vpnclient notify
```

### Establishing a Connection

This section describes how to establish a VPN connection using the **vpnclient connect** command and optional command parameters.



**Note**

---

If you are connecting to a VPN device by using Telnet or SSH, check to see if the device allows split tunneling. If it does not, you lose connectivity to your VPN device after making a VPN connection.

---

To establish a connection, enter the following command:

```
vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
[nocertpwd]
```

The parameters for the **vpnclient connect** command are described in [Table 4-2](#).

**Table 4-1 Parameters for the vpnclient connect Command**

Parameter	Description
<b>&lt;profile&gt;</b> (required)	The name of the user profile configured for this connection entry (.pcf file). Enter the profile name without the .pcf file extension. If your profile name contains spaces, enclose it in double quotation marks on the command line.
<b>user &lt;username&gt;</b> (optional)	The username configured for this connection entry. If you use this option with the <b>pwd</b> option, the username prompt is suppressed in the authentication dialog box.
<b>{eraseuserpwd   pwd &lt;password&gt;}</b> (optional)	<ul style="list-style-type: none"> <li><b>eraseuserpwd</b> erases the user password that is saved on the VPN Client workstation, forcing the VPN Client to prompt you for a password each time you establish a connection.</li> <li><b>pwd &lt;password&gt;</b> suppresses the password prompt in the authentication dialog box.</li> </ul>
<b>nocertpwd</b> (optional)	Suppresses the prompt for a certificate password and assumes that the password is blank. If you use this option, you cannot set a password for your certificate. For more information, see the "Managing Digital Certificates from the Command Line" in the <i>VPN Client Administrator Guide</i> .



**Note**

If your user profile is configured with the **SaveUserPassword** keyword set to the default, the password is saved locally.

For more information on profiles, see [Chapter 3, "User Profiles."](#)

## Authentication Prompts

Depending on your user profile, you are prompted for the following passwords:

- Group password
- User name
- User password
- Certificate password

If your VPN Client has been configured to use SecurID or RADIUS authentication, you are also prompted for those passwords.

See your administrator for security information.

## Rekeying Issues

When the connection is established, the VPN Client window stays in the foreground to allow the VPN Client to be reauthenticated during a rekey by the VPN device. To send the VPN Client window to the background, press **Ctrl-Z** and enter the **bg** command at the command line prompt.

If the VPN device you are connecting to is configured to support rekeying and you send the VPN Client window to the background, the tunnel disconnects when the first rekey occurs.

The VPN Client responds to rekey triggers based on *time*, not *data*. If you want VPN Client connections rekeyed, you must configure the concentrator so that the IKE proposal is set to rekey every 1800 seconds and IPSec parameters are set to rekey every 600 seconds.

## DNS Server Settings

You can configure the concentrator to send the IP addresses of DNS servers to the VPN Client to use during tunnel sessions.

If the client receives the DNS server settings, it copies the file `/etc/resolv.conf` to a backup file `/etc/resolv.conf.vpnbackup`. When the tunnel closes, the original contents of `/etc/resolv.conf` are restored.

**Note**

---

Refer to the configuration guide for your VPN device for information on DNS server settings.

---

## Disconnecting the VPN Client

This section describes methods for disconnecting the VPN Client.

To disconnect from your session, use one of the following methods:

- Enter the following command:

```
vpnclient disconnect
```

The following example shows the command that disconnects you from your secure connection and the prompts that appear.

```
[root@Linux7_1 clients]# vpnclient disconnect
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686
```

```
Disconnecting the VPN connection.
Your VPN connection has been terminated.
```

- Press **Ctrl-C** while you are in the VPN Client window.

# Displaying VPN Client Statistics

This section describes the VPN Client statistics command **vpnclient stat** and its optional parameters.

To generate status information about your connection, enter the following command:

```
vpnclient stat [reset][traffic][tunnel][route][repeat]
```

If you enter this command without any of the optional parameters, the **vpnclient stat** command displays all status information. The optional parameters are described in [Table 4-2](#).

**Table 4-2** Optional Parameters for the **vpnclient stat** Command

Parameter	Description
<b>reset</b>	Restarts all connection counts from zero.
<b>traffic</b>	Displays a summary of bytes in and out, packets encrypted and decrypted, and packets bypassed and discarded.
<b>tunnel</b>	Displays IPsec tunneling information.
<b>route</b>	Displays configured routes.
<b>repeat</b>	Provides a continuous display, refreshing it every few seconds. To end the display, press <b>Ctrl-C</b> .

## Examples

This section shows examples of output from the different options for the **vpnclient stat** command.

### No Options

The following is a sample output from the **vpnclient stat** command with no options.

```
[root@Linux7_1 clients]# vpnclient stat
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686

VPN tunnel information.
Connection Entry: basic
Client address: 10.10.11.214
Server address: 10.200.20.21
Encryption: 168-bit 3-DES
Authentication: HMAC-SHA
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled

VPN traffic summary.
Time connected: 0 day(s), 00:00.01
Bytes in: 0
Bytes out: 0
Packets encrypted: 0
Packets decrypted: 0
Packets bypassed: 17
Packets discarded: 0
```

```
Configured routes.
Secured   Network Destination  Netmask
          0.0.0.0              0.0.0.0
```

## Reset Option

To reset all connection counters, use the **vpnclient stat reset** command.

```
vpnclient stat reset
Tunnel statistics have been reset.
```

## Traffic Option

The following is a sample output from the **vpnclient stat** command with the traffic option.

```
vpnclient stat traffic

VPN traffic summary
Time connected: 0 day<s>, 00:30:04
Bytes out: 5460
Bytes in: 6090
Packets encrypted: 39
Packets decrypted: 91
Packets bypassed: 159
Packets discarded: 1608
```

## Tunnel Option

The following is a sample output from the **vpnclient stat** command with the tunnel option. The **vpnclient stat tunnel** command shows only tunneling information.

```
vpnclient stat tunnel

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
```

## Route Option

The following is a sample output from the **vpnclient stat** command with the route option.

```
vpnclient stat route

Configured routes
Secured   Network Destination  Netmask  Bytes
*         10.10.02.02         255.255.255.255  17638
*         0.0.0.0             0.0.0.0      18998
```

**Note**

The maximum size of any VPN client statistics is 4,294,967,296. Once the VPN Client software reaches this limit, the statistics rolls back to zero and starts again.

## Event Logging

This section provides information on event logging, including how to capture and view logging information.

## Enabling Logging

You must be a system administrator or have access to the global profile (vpnclient.ini) to enable logging.

To enable logging, set **EnableLog=1**. To disable logging, set **EnableLog=0**.

The global profile, located in /etc/CiscoSystemsVPNClient/vpnclient.ini, must include the following parameters:

```
[main]
BinDirPath=/usr/local/bin
EnableLog=1
[LOG.IKE]
LogLevel=15
[LOG.CM]
LogLevel=3
[LOG.CVPND]
LogLevel=3
[LOG.XAUTH]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=15
[LOG.CLI]
LogLevel=3
[LOG.PPP]
LogLevel=1
[LOG.DIALER]
LogLevel=1
[LOG.FIREWALL]
LogLevel=1
[LOG.GUI]
LogLevel=1
```

The VPN Client for Linux and Solaris supports log levels from 1 (lowest) to 15 (highest).

For more information about the global profile, refer to the *Cisco VPN Client Administrator Guide*.

## Viewing Log Files

To view logging information, enter the following command:

```
/usr/local/bin/ipseclog /directory/clientlog.txt
```

**Note**

If you did not use the default directory `/usr/local/bin` during installation, you must enter logging commands using your chosen path.

When you launch the `ipseclog` application, it appends any previous `ipseclog` files.

To view logging information in real time, enter the following command after you start the `ipseclog`:

```
tail -f /directory/clientlog.txt
```

The `ipseclog` does not automatically go to the background. To send the `ipseclog` to the background, press **Ctrl-Z** and enter the **bg** on the command line, or enter the ampersand symbol (**&**) at the end of the **view** command, as shown in the following example:

```
/usr/local/bin/ipseclog /directory/clientlog.txt &
```

If the `ipseclog` is in the background, you must send it to the foreground before you end the VPN Client application. To send the `ipseclog` to the foreground, enter **fg** on the command line.

## Client Auto Update Messages

When the VPN Client receives an auto-update notification from the VPN remote access device, it logs the notification, but takes no further action.

To receive auto-update messages and other notifications from the network administrator, use the **vpnclient notify** command.

The following example shows the `vpnclient notify` command and an example of an auto-update notification from the VPN device:

```
[root@Linux8 vpnclient]# vpnclient notify
Cisco Systems VPN Client Version 3.7 (Rel)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.18-14 #1 Wed Sep 4 13:35:50 EDT 2002 i686
```

**Notification:**

```
Your network administrator has placed an update of the Cisco Systems VPN
Client at the following location:
http://fake.cisco.com/
```

```
[root@Linux8 vpnclient]
```







---

## A

- aggressive mode [1-5](#)
- algorithms
  - authentication [1-5](#)
  - data compression [1-6](#)
  - encryption [1-6](#)
- authentication
  - algorithms [1-5](#)
  - extended [1-6](#)
  - features [1-6](#)
  - mode [1-6](#)
  - type [3-3](#)

---

## B

- backup server [3-4](#)
- batch files
  - erasing saved password [4-2](#)

---

## C

- certificate
  - distinguished name [3-5](#)
  - hash of contents [3-5](#)
  - name [3-4](#)
  - path name [3-5](#)
  - peer [1-7](#)
  - store [3-4](#)
- command-line interface
  - connect [3-2](#)
  - disconnect [4-3](#)
  - displaying commands [4-1](#)

- logging [4-6](#)
- notify [4-7](#)
- stat [4-4](#)
- commands
  - tar [2-4](#)
  - zcat [2-4](#)
- connection types [1-3](#)

---

## D

- data compression [1-6](#)
- data formats [vii](#)
- delete with reason [1-4](#)
- DHCP request [1-4](#)
- Diffie-Hellman groups [1-6](#)
- disconnecting the VPN client [4-3](#)
- displaying available commands [4-1](#)
- DNS server [1-4](#)
- documentation
  - conventions [vi](#)
  - related [vi](#)

---

## E

- enabling VPN service [2-6](#)
- encrypt group password [3-3](#)
- encryption algorithm [1-6](#)
- encrypt user password [3-3](#)
- eraseuserpwd parameter [4-2](#)
- ESP keepalives [3-4](#)
- extended authentication [1-6](#)

**F**

## features

- authentication [1-6](#)
- IPSec [1-5](#)
- program [1-3](#)
- VPN client [1-2](#)

**G**

- group name [3-3](#)
- group password [3-3](#)

**H**

- hash [3-5](#)
- host name [1-4, 3-3](#)
- hybrid authentication
  - Linux [2-3](#)
  - Solaris [2-3](#)

**I**

- IKE keepalives [1-5, 3-4](#)
- IKE protocols [1-1](#)
- installer contents [2-1](#)
- install script
  - Linux [2-6](#)
  - Solaris [2-8](#)
- introduction [1-1](#)
- IP chains [2-3](#)
- IP protocol [1-3](#)
- IPSec
  - attributes [1-5](#)
  - features [1-5](#)
  - through NAT [3-4](#)

## IPSec group

- name [3-3](#)
- password [3-3](#)

**K**

- keepalives [1-5, 3-4](#)
- kernel version
  - changing [2-4](#)
  - requirements [2-2](#)

**L**

- libraries [2-2](#)
- local LAN access [1-3, 3-4](#)
- logging commands [4-6](#)

**M**

- main mode [1-5](#)
- mode
  - aggressive [1-5](#)
  - authentication [1-6](#)
  - configuration [1-6](#)
  - main [1-5](#)
  - NAT [3-4](#)
  - tunnel encapsulation [1-6](#)
- MTU size [1-4](#)
- mutual authentication
  - Linux [2-3](#)

**N**

- NAT mode [3-4](#)
- NAT transparency [3-4](#)
- NAT transversal [3-4](#)
- network adapters supported [1-1](#)

notifications, from VPN device [1-4](#)  
 notify command [4-7](#)

---

## O

operating systems supported [1-1](#)

---

## P

password  
   group [3-3](#)  
   IPSec group [3-3](#)  
   overriding [4-2](#)  
   string [3-3](#)  
   user profile [3-3](#)  
 peer certificate [1-7](#)  
 peer timeout [3-4](#)  
 platforms not supported [1-1](#)  
 ports  
   TCP [3-4](#)  
 preconfigured keys [2-2](#)  
 prerequisites  
   passwords [2-2](#)  
 profiles [3-1](#)  
 program features [1-3](#)  
 protocols  
   DHCP [1-4](#)  
   IKE [1-1](#)  
   IP [1-3](#)  
   PPP [1-3](#)  
   TCP [3-4](#)  
   UDP [1-4, 2-3](#)

---

## R

Red Hat Software [2-2](#)  
 root certificate  
   installing automatically on Linux [2-3](#)  
   installing automatically on Solaris [2-3](#)

---

## S

SA (security association) [1-4](#)  
 save user password [3-3](#)  
 shared keys  
   authentication type [3-3](#)  
   Diffie-Hellman group [3-5](#)  
 single SA [1-4](#)  
 smart cards [1-7](#)  
 split DNS [1-5](#)  
 split tunneling [1-4, 1-5](#)  
 statistics [4-4](#)  
 subinterfaces limitations [1-1](#)  
 supported VPN devices [1-1](#)  
 system administrator [2-2](#)  
 system requirements [2-2](#)

---

## T

tar command [2-4](#)  
 TCP protocol [3-4](#)  
 terminate connections [1-1](#)  
 transparent tunneling [1-5](#)  
 tunneling  
   encapsulation mode [1-6](#)  
   protocol [1-3](#)  
   split [1-5](#)

---

## U

- UDP protocol [1-4](#)
- UltraSPARC computer [2-4](#)
- uninstalling an old client [2-1](#)
- unpacking the VPN client files [2-4](#)
- user authentication [1-3, 1-6](#)
- user name [3-3](#)
- user password [3-3](#)
- user profiles
  - creating [3-2](#)
  - described [3-1](#)
  - example [3-1](#)
  - location [3-1](#)
  - parameters [3-2](#)

---

## V

- viewing the logging files [4-6](#)
- VPN client
  - defined [1-1](#)
  - features [1-2](#)
- vpnclient connect command [3-2](#)
- vpnclient disconnect command [4-3](#)
- vpnclient stat command [4-4](#)
- VPN devices [1-1](#)

---

## X

- X.509 certificates [1-2](#)
- XAUTH (extended authentication) [1-6](#)

---

## Z

- zcat command [2-4](#)