



## 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.

