



# CHAPTER 1

## 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



### Note

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.

**Note**

---

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 PC <sup>1</sup>	<ul style="list-style-type: none"> <li>Windows 7 32/64-bit</li> <li>Windows Vista 32/64-bit</li> <li>Windows XP 32-bit<sup>2</sup></li> </ul>	<ul style="list-style-type: none"> <li>Microsoft TCP/IP installed. (Confirm via Start &gt; Settings &gt; Control Panel &gt; Network &gt; Protocols or Configuration.)</li> <li>50 MB hard disk space.</li> <li>RAM: <ul style="list-style-type: none"> <li>– 128 MB for Windows XP (256 MB recommended)</li> </ul> </li> </ul>
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 <sup>3</sup>  <b>Note</b> The VPN Client does not support SMP (multiprocessor) or 64-bit processor kernels.	<ul style="list-style-type: none"> <li>32 MB Ram</li> <li>50 MB hard disk space</li> </ul>
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	<ul style="list-style-type: none"> <li>32 MB Ram</li> <li>50 MB hard disk space</li> </ul>
Macintosh computer	Mac OS X, Version 10.4.0 or later	<ul style="list-style-type: none"> <li>50 MB hard disk space</li> <li>PPC or Intel processor.</li> </ul>

1. The VPN Client includes support for dual-processor and dual-core workstations for Windows XP and Windows Vista.
2. 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.
3. Installation of the Linux unified VPN Client works correctly during the kernel module build with Linux kernel 2.2.19 and later (CSCsg98579)

## 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).

**Note**

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](http://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:

**Caution**

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](http://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](http://www.baltimoretechnologies.com))

- Entrust Technologies ([www.entrust.com](http://www.entrust.com))
- Netscape ([www.netscape.com](http://www.netscape.com))
- Verisign, Inc. ([www.verisign.com](http://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](mailto:vpn-client-api-support@cisco.com) so that we can publish the file to you.



---

**Note**

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	<p>Your choice here determines the parameters you see in the following screen. Possible values are:</p> <p>Internal Server/Local</p> <p>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.</p> <p>Additionally, if you specify per-user address assignment, specify the IP address and subnet mask for each user.</p> <p><b>RADIUS</b></p> <p>If you use an external RADIUS user authentication server, specify its IP address or hostname, port number, and server secret or password.</p> <p><b>NT Domain</b></p> <p>If you use an external Windows NT Domain user authentication server, specify its IP address, port number, and Primary Domain Controller hostname.</p> <p><b>SDI</b></p> <p>If you use an external SDI user authentication server, specify its IP address and port number.</p> <p><b>Kerberos/Active Directory</b></p> <p>If you use an external Kerberos/Active Directory authentication server, specify its IP address, port number, and realm.</p>	
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.



**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.

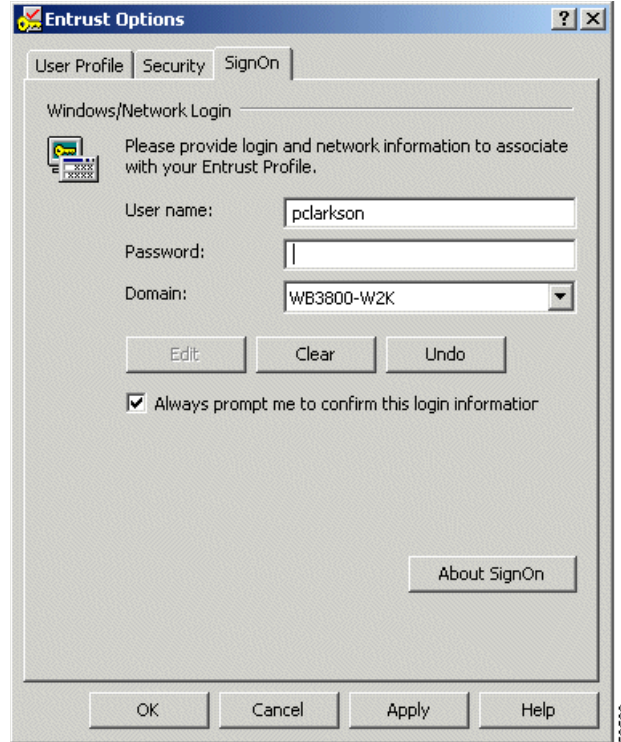
## Configuring Entrust Entelligence for the VPN Client—Windows Only

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 Entrust 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*.

**Note**

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.

**Note**

---

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.

**Note**

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.

**Note**

---

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: <ul style="list-style-type: none"> <li>• IP address for preshared key</li> <li>• Cert DN for certificate authentication.</li> </ul>

## 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 information. 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.



### 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.

## 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.

**Note**

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.



### Note

---

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 through 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 4.7.00.640 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).

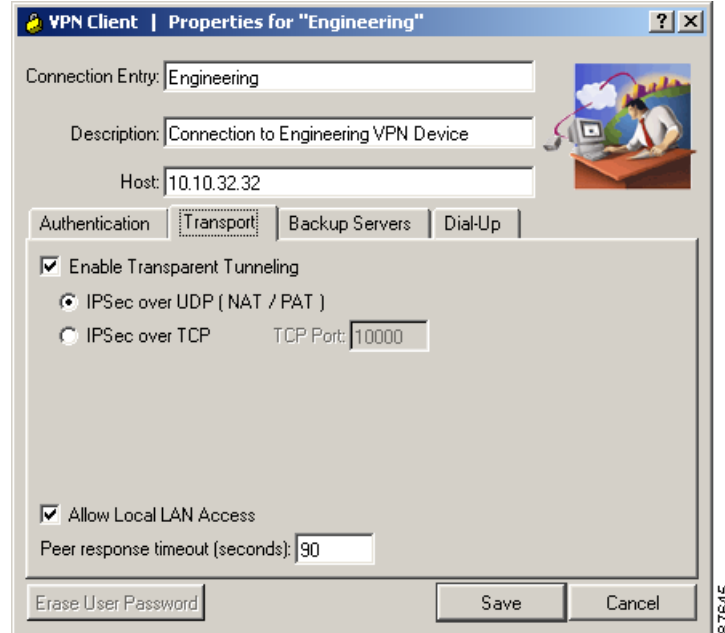
Use the following procedure:

---

**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:
- 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.
  - 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”.



**Note**

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

**Note**

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.

**Note**

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.