

Connecting to a Private Network

This chapter explains how to connect to a private network with the VPN Client.

We assume you have configured at least one VPN Client connection entry as described in "Configuring the VPN Client." To connect to a private network, you also need the following information:

- ISP logon username and password, if necessary.
- User authentication information:
 - - If you are authenticated via the VPN 3000 Concentrator internal server, your username and password.
 - If you are authenticated via a RADIUS server, your username and password.
 - If you are authenticated via an Windows NT Domain server, your username, password, and domain name.
 - If you are authenticated via RSA Data Security (formerly SDI) SecurID or SoftID, your username and PIN.
 - If you use a digital certificate for authentication, the name of the certificate and your username and password. If your private key is password protected for security reasons, you also need this password.

Refer to your entries in "Gathering Information You Need," as you complete the steps described here, which include the following sections:

- Starting the VPN Dialer
- Using the VPN Client to Connect to the Internet via Dial-Up Networking
- Authenticating to Connect to the Private Network
- Connecting with Digital Certificates
- Viewing Connection Status

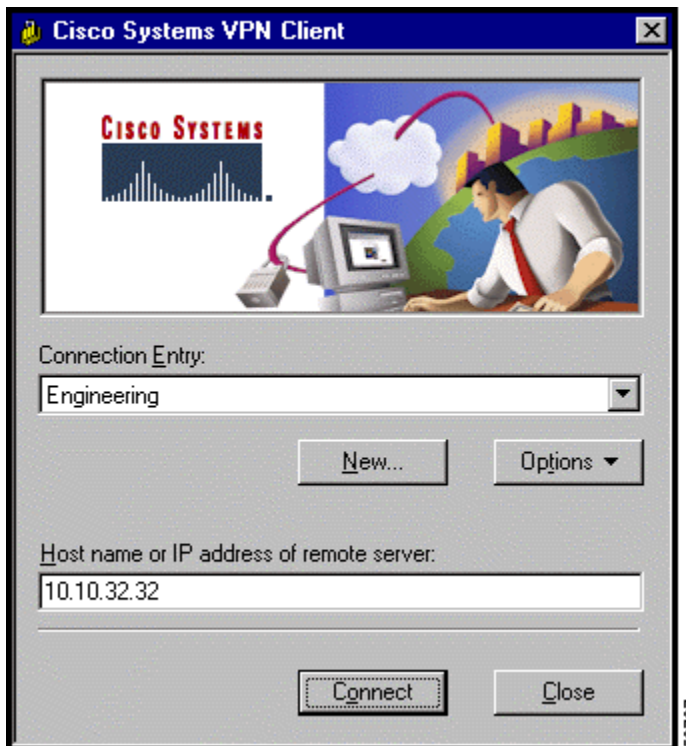
- Closing the VPN Client
- Disconnecting your VPN Client Connection

Starting the VPN Dialer

Step 1 To start the VPN Dialer application, choose **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Dialer displays the VPN Client's main dialog box. (See Figure 4-1.)

Figure 4-1: VPN Dialer Main Dialog Box



Step 2 If necessary, click the **Connection Entry** drop-down menu and choose the desired connection entry.

Connection Procedure

To connect to a private network, perform the following steps:

Step 1 Connect to the Internet, if necessary.

Step 2 Connect to the private network through the Internet.

- Systems with cable or DSL modems are usually connected to the Internet, so no additional action is necessary. Skip to "Authenticating to Connect to the Private Network."
 - Systems with modems or ISDN modems must connect to the Internet via Dial-Up Networking:
 - - If you connect to the Internet via Dial-up Networking, proceed to "Using the VPN Client to Connect to the Internet via Dial-Up Networking."
 - If you must manually connect to the Internet, do it now. When your connection is established, skip to "Authenticating to Connect to the Private Network."
 - If your system is already connected to the Internet via Dial-Up Networking, skip to "Authenticating to Connect to the Private Network."
-

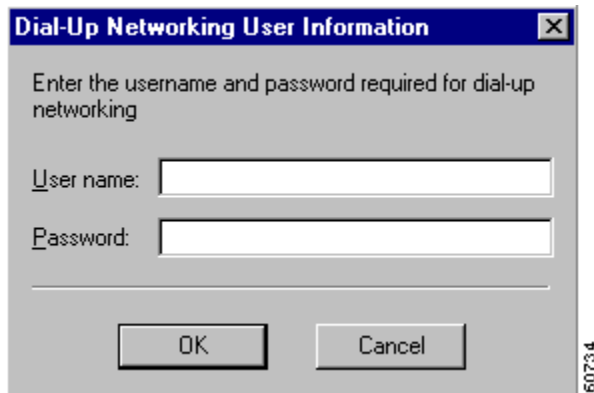
Using the VPN Client to Connect to the Internet via Dial-Up Networking

This section describes how to connect to the Internet via Dial-Up Networking by running only the VPN Client. Your connection entry must be configured with Connect to the Internet via Dial-Up Networking enabled; see "Configuring the VPN Client".

Step 1 Click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

If your credentials are not stored in the RAS database, the **Dial-up Networking User Information dialog box** appears. (See Figure 4-2.) This dialog box varies depending on the version of Windows you are using.

Figure 4-2: Entering User Information



Step 2 Enter your username and password to access your ISP. These entries may be case-sensitive. The Password field displays only asterisks.

Step 3 Click **OK**.

You see the Connection History dialog box. (See Figure 4-3.)

Figure 4-3: Confirming Connections to ISP



When the ISP connection is established, a Dial-Up Networking icon appears in the system tray on the Windows task bar. (See Figure 4-4.)

Figure 4-4: Dial-Up Networking task bar Icon



Authenticating to Connect to the Private Network

This section assumes you are connected to the Internet. If you connect using Dial-Up Networking, verify that its icon is visible in the Windows task bar system tray. (See Figure 4-4.) If not, your Dial-Up Networking connection is not active and you need to establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

The VPN Client starts tunnel negotiation and displays the Connection History dialog box. (See Figure 4-5.)

Figure 4-5: Negotiating Dialog Box



The next phase in tunnel negotiation is user authentication.

User Authentication

User authentication means proving that you are a valid user of this private network. User authentication is optional. Your administrator determines whether it is required.

The VPN Client displays a user authentication dialog box that differs according to the authentication that your IPSec group uses. Your system administrator tells you which method to use.

To continue, refer to your entries in "Gathering Information You Need" and go to the appropriate authentication section that follows.

Authenticating Through the VPN Device Internal Server or RADIUS Server

To display the user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.


Figure 4-6: Authenticating Through an Internal or RADIUS Server



Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 Click **OK**.

 **Note** If you cannot choose the **Save Password** option, your administrator does not allow this option. If you can choose this option, be aware that using it might compromise system security, since your password is then stored on your PC and is available to anyone who uses your PC.

If **Save Password** is checked and authentication fails, your password may be invalid. To eliminate a saved password, click **Options > Erase User Password**.

Proceed to the section "Viewing Connection Status."

Authenticating Through a Windows NT Domain

To display the Windows NT Domain user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

Figure 4-7: Authenticating Through a Windows NT Domain



Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 In the Domain field, enter your Windows NT Domain name, if it is not already there.

Step 4 Click **OK**.

Skip to "Viewing Connection Status."

Changing your Password

Your network administrator may have configured your group for RADIUS with Expiry authentication on the VPN 3000 Concentrator. If this feature is in effect

and your password has expired, a dialog box prompts you to enter and confirm a new password.

After you have tried unsuccessfully to log in three times, you might receive one of the following login messages:

- Restricted login hours
- Account disabled
- No dial-in permission
- Error changing password
- Authentication failure

These messages let you know the cause of your inability to log in. For help, contact your network administrator.

Authenticating Through RSA Data Security (RSA) SecurID (SDI)

RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID. SecurID cards also vary: with some cards, the passcode is a combination of a PIN and a cardcode; with others, you enter a PIN on the card and it displays a passcode. Ask your system administrator for the correct procedure.

Authentication via these methods also varies slightly for different operating systems. If you use an RSA method, the VPN Client displays the appropriate RSA user authentication dialog box. The title bar identifies the connection entry name.

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME)

To display an authentication dialog box asking for your username and passcode, perform the following steps. (See Figure 4-8.) If you are using SoftID, it must be running on your PC.

Figure 4-8: Authenticating through RSA



Step 1 In the **Username field**, enter your username. This entry is case-sensitive.

Step 2 In the Passcode field, enter a SecurID code. With SoftID, you can copy this code from the SoftID window and paste it here. Your administrator will tell you what you need to enter here, depending on the type of token card you are using.

Step 3 After entering the code, click **OK**.

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems)

If you are using SoftID under Windows NT, the VPN Client displays an authentication dialog box asking for your username and PIN. (See Figure 4-9).

Figure 4-9: Authenticating Through SoftID on Windows NT



Step 1 In the Username field, enter your username. This entry is case-sensitive.

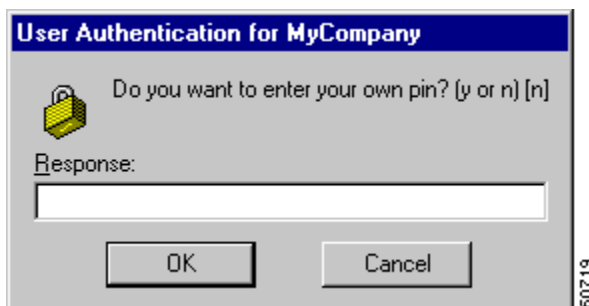
Step 2 In the PIN field, enter your SoftID PIN. The VPN Client gets the passcode from SoftID by communicating directly with SoftID. The SoftID application must be installed but does not have to be running on your PC.

Step 3 After entering the PIN, click **OK**.

RSA New PIN Mode

The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN. (See Figure 4-10.)

Figure 4-10: SecurID New PIN Request



Step 1 Enter your response **y** for yes or **n** for no. No is the default response. Then, click **OK**. What happens next depends on your response.

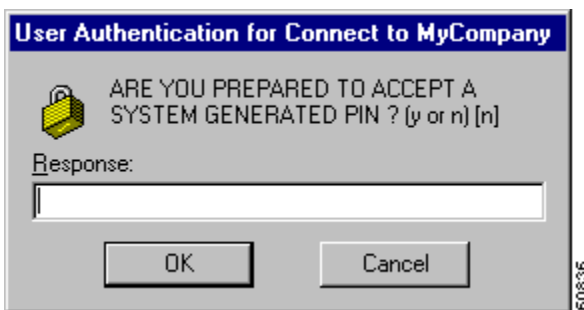
- If you responded yes—Enter your new PIN in the New PIN field and enter it again in the Confirm PIN field. Click **OK**. (See Figure 4-11.)

Figure 4-11: Entering a New PIN Yourself



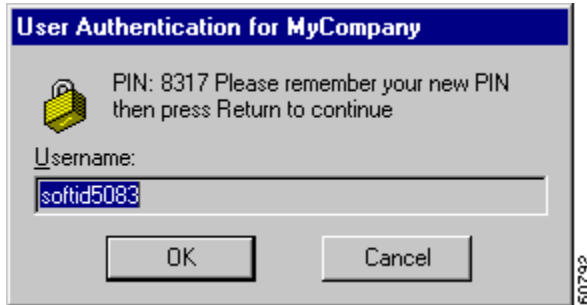
- If you responded no—the authentication program asks if you will accept a system-generated PIN. (See Figure 4-12.)

Figure 4-12: Accepting a PIN from the System



Step 2 To receive a PIN, you must respond **y** for yes and then click **OK**. When you do, the authentication program generates a PIN for you and displays it. (See Figure 4-13.) Be sure to remember your PIN.

Figure 4-13: New PIN Received



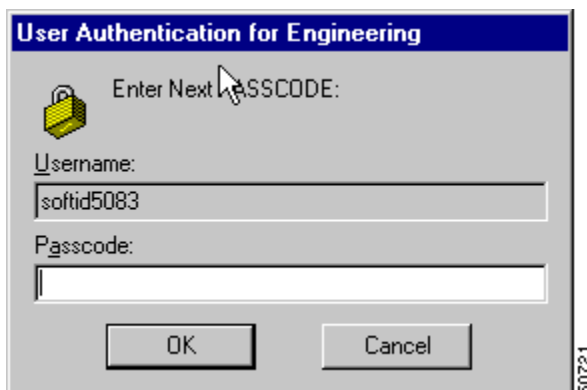
Step 3 To continue, click **OK**.

SecurID Next Cardcode Mode

Sometimes SecurID authentication prompts you to enter the next cardcode from your token card, as in Figure 4-14. SecurID displays this prompt either to resynchronize the token card with the RSA server, or because it noticed several unsuccessful attempts to authenticate with this username.

The SecurID Next Cardcode Mode dialog box might appear. (See Figure 4-14.)

Figure 4-14: Entering the Passcode for SecurID Next Card



In the Passcode field, enter the next code from your token card. This field requires only a cardcode. Do not include your PIN as part of the passcode.


Now continue to "Viewing Connection Status."

Connecting with Digital Certificates

Before you created a connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on your system. If this is not the case, then you need to obtain a digital certificate. In many cases, the network administrator of your organization can provide you with a certificate. If not, then you can obtain one by enrolling with a PKI directly using the Certificate Manager application, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we support the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)
- Entrust PKI™ from Entrust Technologies (www.entrust.com)
- Verisign (www.verisign.com)
- Microsoft Certificate Services in Microsoft Windows 2000 Server
- Cisco Certificate Store

The websites listed in parentheses in this list contain information about the digital certificates that each PKI provides. The easiest way to enroll in a PKI or import a certificate is to use the Certificate Manager (see "Enrolling and Managing Certificates") or Entrust Entelligence (see Entrust documentation).

 **Note** Every time you connect using a certificate, the VPN Client checks to verify that your certificate has not expired. If your certificate is within one month of expiring, the VPN Client displays a message when you attempt to connect or when you use the Properties option. The message displays the certificate common name, the "not before" date, the "not after" date, and the number of days until the certificate expires or since it has expired.

There is one exception to this rule. When you are authenticating with a Microsoft certificate, the VPN Dialer skips the automatic certificate validation process and starts the connection immediately. If there is a problem with the certificate, the connection attempt fails. To obtain information about the failure, look in the connection log file (see "Viewing and Managing the VPN Client Event Log"). To validate the certificate manually, choose Properties >

Authentication > Validate Certificate.

What happens when you press **Connect** can depend on the level of private key protection on your certificate. If your certificate is password protected, you are prompted to enter the password.

Connecting with an Entrust Certificate

This section provides important information about what to expect when connecting with an Entrust certificate under certain conditions.

Accessing Your Profile

If you are not already logged in, you must log in to Entrust Entelligence to access your Entrust Entelligence certificate profile, using the following procedure:

After you choose **Connect** on the VPN Client main dialog box, the Entrust login dialog box appears. (See Figure 4-15.)

Figure 4-15: Logging in to Entrust



Step 1 Choose a profile name from the pull-down menu.

Your network administrator has previously configured one or more profiles for you through Entrust Entelligence. If the software is installed on your system but there are no profiles available, then you need to get a profile from your network

administrator or directly through Entrust. Refer to *Entrust Entelligence Quick Start Guide* for instructions on obtaining a profile. The *VPN Client Administrator Guide* contains supplementary configuration information.

Step 2 After choosing a profile, enter your Entrust password.

Check the Work offline field to use Entrust Entelligence without connecting to the Entrust PKI. If Work offline is checked and you press **OK**, the Entrust wizard displays the message shown in Figure 4-16.

Figure 4-16: Entrust Login Message

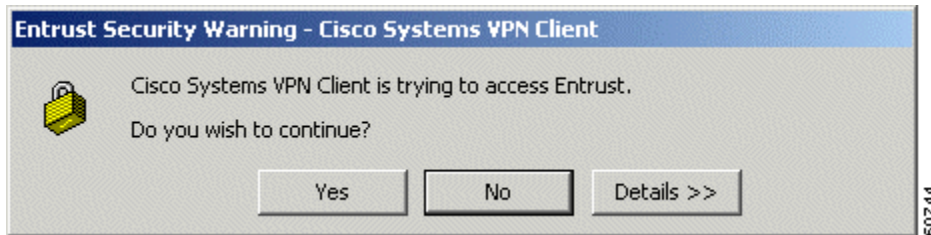


You can ignore this message. Since you are connecting to your organization's private network using an existing certificate profile, you are not interacting with the Entrust PKI. If you see this message, click **OK** to continue.

Step 3 After completing the Entrust Login dialog box (see Figure 4-15), click **OK**.

You may receive a security warning message from Entrust. This warning occurs, for example, when an application attempts to access your Entelligence profile for the first time or when you are logging in after a VPN Client software update. The message happens because Entrust wants to verify that it is acceptable for the VPN Client to access your Entrust profile.

Figure 4-17: Entrust Security Warning



Step 4 At the warning message, click **Yes** to continue.

You can now use your Entrust certificate for authenticating your new connection entry.

Entrust Inactivity Timeout

If you have a secure connection and you see a padlock next to the Entelligence icon in the Windows system tray, Entelligence has timed out. However, you have not lost your connection. If you see the Entelligence icon with an X next to it, you are logged out of Entrust, and you did not have a secure connection initially. To make a new connection, start from the beginning (see "Accessing Your Profile").

Using Entrust SignOn and Start Before Logon Together

Entrust SignOn™ is an optional Entrust application that lets you use one login and password to access Microsoft Windows and Entrust applications. This application is similar to *start before logon*, which is a VPN Client feature that enables you to dial in before logging on to Windows NT. For information about start before logon, see "Starting a Connection Before Logging on to a Windows NT Platform".

If you want to use these two features together, you should make sure you have installed Entrust Entelligence with the Entrust SignOn module before installing the VPN Client. For information about installing Entrust SignOn, refer to Entrust documentation and the *VPN Client Administrator Guide*, Chapter 1.

To use these two features together, follow these steps:

Step 1 Start your system.

When the SignOn option is installed, Entrust displays its own Ctrl Alt Delete dialog box.

Step 2 Click **Ctrl Alt Delete**.

The Entrust Options dialog box and the VPN Dialer login dialog box both pop up. The VPN Dialer dialog box is active.

Step 3 To start your VPN connection, click **Connect** on the VPN Dialer main dialog box.

The Entrust login dialog box becomes active.

Step 4 To log in to your Entrust profile, enter your Entrust password.

The VPN Dialer password prompt dialog box becomes active.

Step 5 Enter your VPN dialer username and password.

The VPN Client authenticates your credentials and optionally displays a banner and/or a notification. Respond to the banner or notification as required. Then the Windows NT logon dialog box is active.

Step 6 To complete the connection, enter your Windows NT logon credentials in the Windows logon dialog box and you are done.

Connecting with a Smart Card or Token

The VPN Client supports authentication with digital certificates through a smart card or electronic token. Several vendors provide smart cards and tokens. For an up-to-date list of those that the VPN Client currently supports, see "Smart Cards Supported". Smart card support is provided through Microsoft Cryptographic API (MS CAPI). Any CryptoService provider you use must support signing with CRYPT_NOHASHOID.

Once you or your network administrator has configured a connection entry that uses a Microsoft certificate provided by a smart card, you must insert the smart card into the receptor. When you start your connection, you are prompted to enter a password or PIN, depending on the vendor. For example, Figure 4-18 shows the authentication prompt from ActivCard Gold.

Figure 4-18: ActivCard Gold PIN Prompt



In above example, you would type your PIN code in the Enter PIN code field and click **OK**.

The next example shows how to log in to eToken from Aladdin. You select the token in the eToken Name column, type a password in the User Password field, and click **OK**.

Figure 4-19: eToken Prompt



Note If your smart card or token is not inserted, the authentication program displays an error message. If this occurs, insert your smart card or token and try again.

Completing the Private Network Connection

After completing the user authentication phase, the VPN Client continues negotiating security parameters and displays a dialog box. (See Figure 4-20.) The title bar identifies the remote Cisco VPN device to which you are connecting.

Figure 4-20: Completing Connection History



If the network administrator of the Cisco VPN device has created a client banner, you see a message designated for all clients connecting to that device; for example, The Documentation Server will be down for routine maintenance on Sunday.

After you complete your connection, the VPN Client minimizes to an icon in the system tray on the Windows task bar.

You are now connected securely to the private network via a tunnel through the Internet, and you can access the private network as if you were an onsite user.

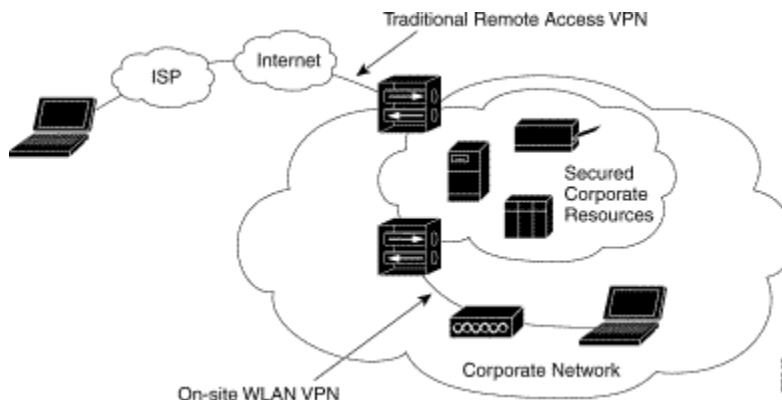
Using Automatic VPN Initiation

Your VPN Client can automatically initiate a VPN connection based on the network to which your machine is connected. The name of this feature is called *auto initiation* for on-site Wireless LANs (WLANs). Auto initiation makes the user experience resemble a traditional wired network in which VPNs secure WLANs. These environments are also known as WLANs.

On-site WLAN VPNs are similar to remote access VPNs with an important distinction. In an on-site wireless VPN environment, enterprise administrators have deployed wireless 802.11x networks in corporate facilities and these networks use VPNs to secure the wireless part of the network link. In this case, if your PC is on a WLAN without VPN, you cannot access network resources. If a VPN exists, your access is similar to what it is with wired Ethernet connections.

[Figure 4-21](#) shows the two different types of VPN access.

Figure 4-21: Remote Access VPN Versus On-Site Wireless Access VPN



In your connection profile, your network administrator can configure a list of up to 64 matched networks (address/submasks) and corresponding connection profiles (.pcf files). When the VPN Client detects that your PC's network address matches one of the addresses in the auto initiation network list, it automatically establishes a VPN connection using the matching profile for that network.

While auto initiation is primarily for an on-site WLAN application, you can also use auto initiation in any situation based on the presence of a specific network. For example, in your home office, you may want to create an entry for your VPN to auto initiate from your corporate PC whenever you are connected to your home network, whether that network is a wireless or a wired LAN.

The VPN Dialer lets you know when your connection is auto initiating and informs you of various stages in the process of an auto initiated connection. You can suspend, resume, disconnect or disable auto initiation. When you disconnect or the connection attempt fails, the VPN Dialer automatically retries auto initiation using a configured interval called the retry interval. From The VPN Dialer Options menu, you can disable auto initiation, and you can change the interval between connection attempts.

Connecting Through Auto Initiation

Typically when you start your wireless system (normally a laptop), your connection initiates automatically. You do not see the VPN Dialer's main dialog. As the connection goes forward, the VPN Dialer displays the dial status screen (see Figure 4-22).

Figure 4-22: Viewing Dial Status of an Auto Initiated VPN Connection



Also, the VPN Dialer displays the authentication dialog such as the one shown in Figure 4-23.

Figure 4-23: Authenticating Auto Initialized Connection



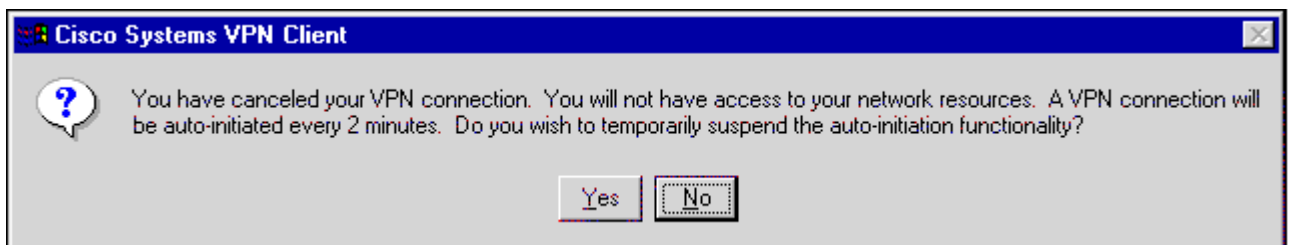
When you enter your authentication information, your connection starts immediately, as you can tell by viewing the closed yellow lock icon in the system tray.

Figure 4-24: Closed Lock—Connected



Or to cancel the connection attempt, click **Cancel** in the Dial Status dialog. When you cancel the connection attempt, the VPN Dialer displays the following message.

Figure 4-25: Canceling Connection Attempt During Authentication



To cancel, click **No**. If you are using the Log Viewer application, in the event log, you see the message "Connection canceled."

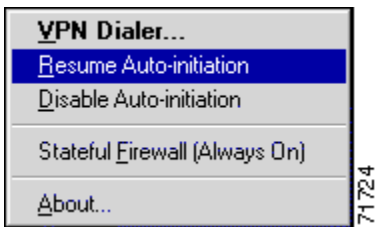
To suspend, click **Yes**; in the event log, you see the message "Auto-initiation has been suspended". When suspended, also in the task bar, you see that the yellow lock icon is now open.

Figure 4-26: Open Lock—Suspended Auto Initiation



To resume auto initiation after canceling, right-click on the open yellow lock icon and select **Resume Auto-initiation** from the menu.(See Figure 4-27).

Figure 4-27: Resuming Auto Initiation

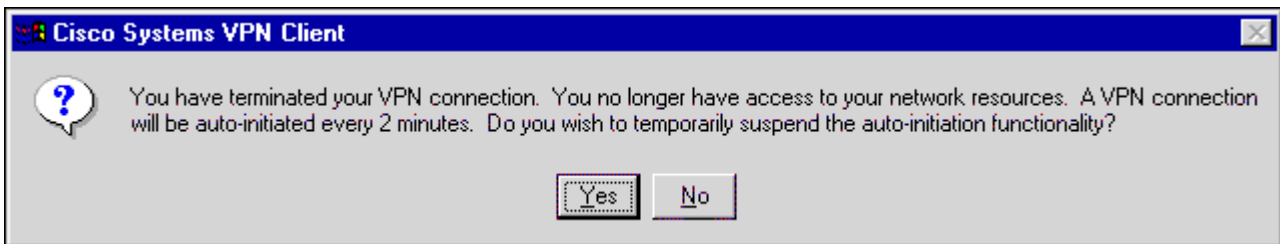


Auto initiation resumes. This is the simplest scenario of what happens during auto initiation. At various points, depending on the actions you take, you see messages, changes in the color of the icon in the system tray, and differences in choices you can make. The rest of this section describes these various alternatives.

Disconnecting Your Session

To disconnect your session, either double-click the lock icon in the system tray and click the **Disconnect** button or right-click the lock and select **Disconnect** from the menu (in the standard way). The VPN Dialer displays the following message. (See Figure 4-28.)

Figure 4-28: Disconnecting Your Session



To suspend auto initiation, click **Yes**. Auto initiation suspends until you resume it, disable it, or log off.

When you click **No**, auto initiation stays in effect and the VPN Dialer automatically retries auto initiation according to the retry interval; for example, every minute.

Changing Option Values While Auto Initiation is Suspended

When auto initiation is suspended, you can change VPN Dialer options as follows:

Step 1 Double-click yellow lock icon in the system tray.

Step 2 Click **Options**. The VPN Dialer displays the Options menu.

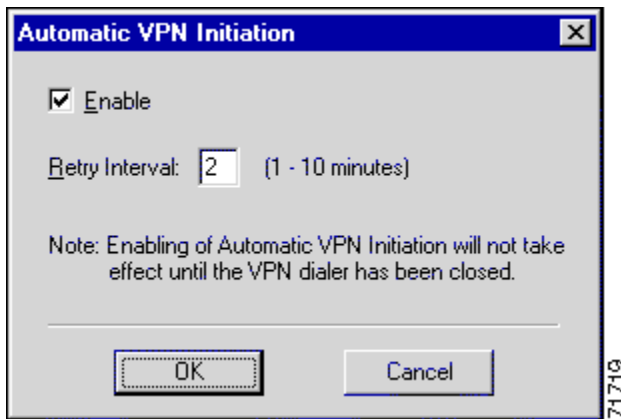
Disabling Auto Initiation

To completely shut down auto initiation, you can disable it through the Options menu by following these steps:


Step 1 Display the VPN Dialer main dialog box and click **Options**.

Step 2 Select **Automatic VPN Initiation**. The VPN Dialer displays the dialog box shown in Figure 4-29.

Figure 4-29: Setting Auto Initiation Parameters



Step 3 Click to remove the check mark from **Enable** and click **OK**. The log displays a message, "Auto-initiation has been disabled," and auto initiation terminates. When you click the dialer icon in the system tray, VPN Dialer is the only option displayed.

 **Note** Unchecking Enable does not remove Automatic VPN Initiation option from the Options menu. This option always shows up in the menu as long as the feature has been configured by your network administrator.

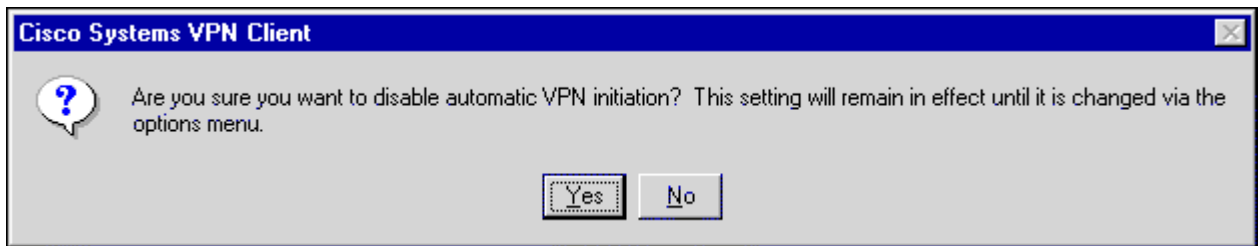
Disabling While Suspended

Alternatively, when auto initiation is suspended and you want to disable it, follow these steps:

Step 1 Right-click on the icon in the system tray.

Step 2 Select **Disable Auto-initiation**. The VPN Dialer displays a warning message (See Figure 4-30.)

Figure 4-30: Disabling an Auto Initiated Connection



Step 3 To completely disable auto initiation and eliminate further automatic retries, click **Yes**. Or to cancel the action and keep auto initiation enabled, click **No**.

Restarting After Disabling Auto Initiation

When you want to restart auto initiation, follow these steps:

Step 1 Launch the **VPN Dialer** from the Start > Programs > Cisco Systems VPN Dialer menu.

Step 2 Click **Options**.

Step 3 Select **Automatic VPN Initiation**.

Step 4 Check **Enable** and click **OK**. The log shows that auto initiation is now in effect. For an example, see Figure 4-31.

Figure 4-31: Auto Initiation Log Messages

15727	14:22:45.721	04/22/02	Sev=Info/6	DIALER/0x63300009
Auto-initiation has been suspended.				
15728	16:24:25.578	04/22/02	Sev=Info/6	DIALER/0x63300009
Auto-initiation has been disabled.				
15729	16:36:09.671	04/22/02	Sev=Info/6	DIALER/0x63300009
Auto-initiation has been enabled.				
15730	16:36:09.671	04/22/02	Sev=Info/6	CM/0x63100036
Auto-initiation condition detected:				
Local IP 10.10.0.32				
Network 10.10.32.32				
Mask 0.0.0.0				
Connection Entry "Engineering"				

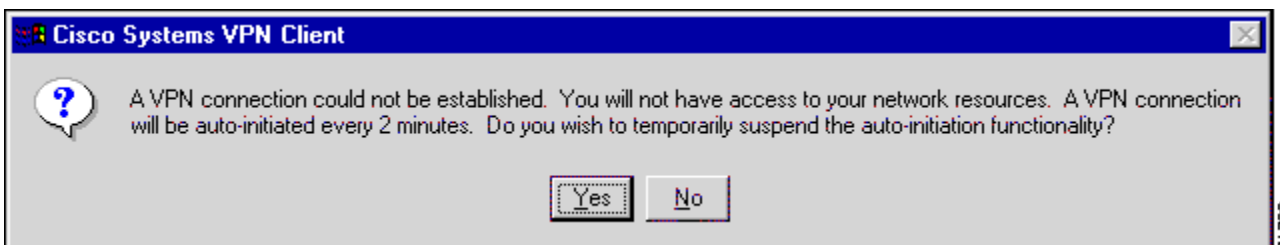
71788

Step 5 Close the VPN Dialer dialog. The Authentication dialog box displays.

Connection Failures

If the auto initiation attempt fails, the VPN Dialer notifies you with a dial status dialog and a warning message.

Figure 4-32: Auto Initiation Failure Message



71792

To suspend auto initiation, click **Yes**. To continue retrying, click **No**. When you click No, the VPN Dialer keeps trying to connect until the connection goes through or you either disable auto initiation or log out.

Summary of Auto Initiation States

This section shows each stage of auto initiation as indicated through the changes in the appearance of the lock icon in the system tray.



Closed lock—Connected. A secure connection is in effect. Note that the closed yellow lock always indicates a secure connection whether or not you are using auto initiation.



Open yellow lock—Not connected. Auto initiation is suspended and waiting for a user action (resuming or disabling).



Open green lock—VPN Dialer is auto initiating a connection. The VPN Dialer is attempting to auto initiate from the Dial Status dialog.




Closed yellow lock with red X over it—Connection terminating. You have chosen to disconnect. The VPN Dialer asks if you want to suspend (see Figure 4-28). (Note that this icon is not specific to auto initiation but occurs any time you choose to disconnect.)



Open Blue Lock— Auto Initiation continues to be suspended with the VPN Dialer's main dialog box displaying. When you click on this lock, VPN Dialer is the only menu choice displayed. If you click **Close**, the VPN Dialer returns to the normal auto initiation suspended state.



Open Red Lock—Auto Initiation is disabling from the suspended state. VPN Dialer displays the Disable warning dialog box (see Figure 4-30) that lets you confirm or retreat.

 **Note** Auto initiation does not connect if the VPN Dialer is opened by any means.

Viewing Connection Status

The VPN Client icon on the task bar



lets you view the status of your private network connection.

- Double-click the icon, or
- Click the icon with the right mouse button and choose **Status** from the pop-up menu.

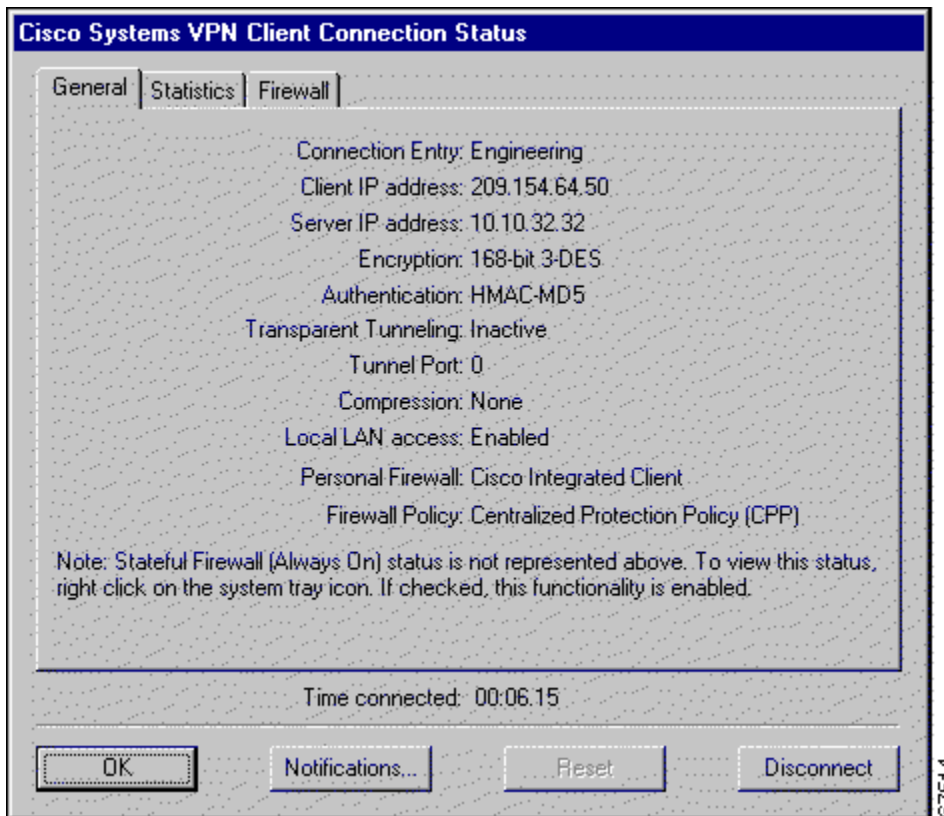
The VPN Client Connection Status dialog box appears. The dialog contains three tabs:

- General (See Figure 4-33.)
- Statistics (See Figure 4-34.)
- Firewall (See Figure 4-35).

General Information

The General tab on the Connection Status dialog box provides IP security information, listing the IPSec parameters that govern the use of this VPN tunnel to the private network.

Figure 4-33: Viewing IPSec Security Information



The parameters are the following:

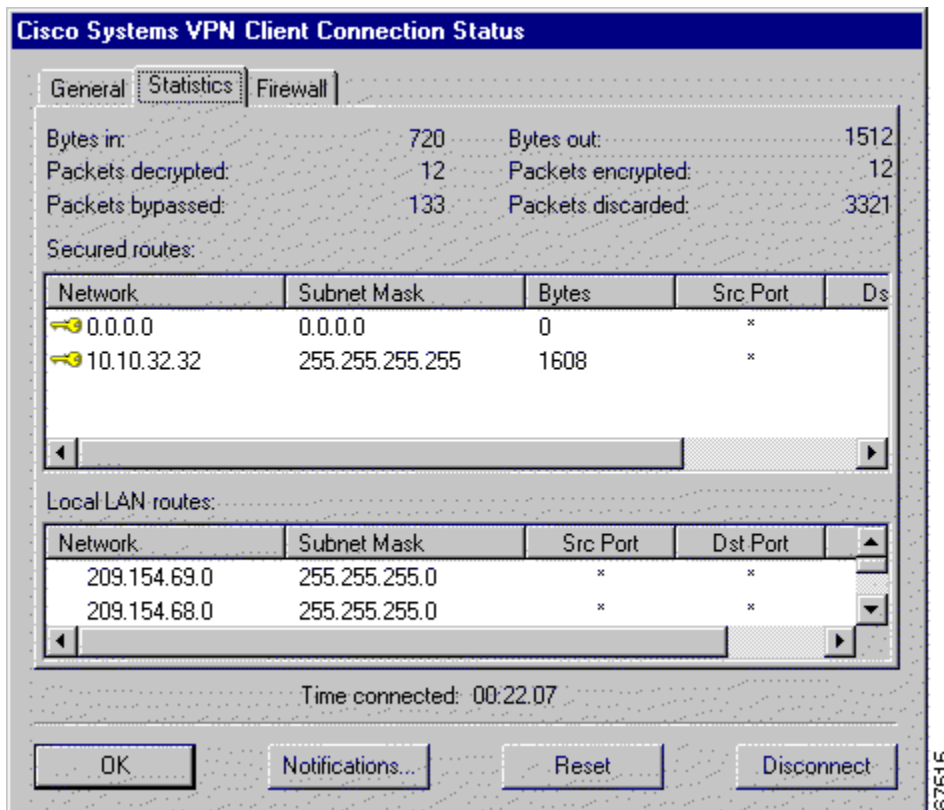
- Connection Entry—The name of the profile you are using to establish the connection.
- Client IP address—The IP address assigned to the VPN Client for the current session.
- Server IP address—The IP address of the VPN device to which the VPN Client is connected.
- Encryption—The data encryption method for traffic through this tunnel. Encryption makes data unreadable if intercepted.
- Authentication—The data, or packet, authentication method used for traffic through this tunnel. Authentication verifies that no one has tampered with data.

- Transparent Tunneling—The status of tunnel transparent mode in the client, either active or inactive.
- Tunnel Port—If Transparent Mode is active, the tunnel port through which packets are passing. This field also identifies whether the VPN Client is sending packets through UDP or TCP. This port number comes from the VPN device. If UDP, the port is negotiated; if TCP the port is preconfigured. If Transparent Tunneling is inactive, then the value of Tunnel Port is zero.
- Compression—Whether data compression is in effect as well as the type of compression in use. Currently, LZS is the only type of compression that the VPN Client supports.
- Local LAN Access—Whether this parameter is enabled or disabled. (For information on configuring this feature, see "Allowing Local LAN Access".)
- Personal Firewall—The name of the firewall that the VPN Client is enforcing, such as the Cisco Integrated Client, Zone Labs ZoneAlarm, ZoneAlarm Pro, BlackICE Defender, and so on.
- Firewall Policy—The firewall policy in use:
 - - AYT (Are You There) enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.
 - Centralized Protection Policy (CPP) or "Policy Pushed" as defined on the VPN Concentrator lets you define a stateful firewall policy that the VPN Client enforces for Internet traffic while a tunnel is in effect. CPP is for use during split tunneling and is not relevant for a tunnel everything configuration. In a tunnel everything configuration, all traffic other than tunneled traffic is blocked during the tunneled connection.
 - Client/Server corresponding to "Policy from Server" (Zone Labs Integrity) on the VPN Concentrator

Statistics

The Statistics tab on the Connection Status dialog box shows statistics for data packets that the VPN Client has processed during the current session or since the statistics were reset. Reset affects only this tab.

Figure 4-34: Viewing Statistics



- Bytes in—The total amount of data received after a secure packet has been successfully decrypted.
- Bytes out—The total amount of encrypted data transmitted through the tunnel.
- Packets decrypted—The total number of data packets received on the port.
- Packets encrypted—The total number of secured data packets transmitted out the port.
- Packets bypassed—The total number of data packets that the VPN Client did not process because they did not need to be encrypted. Local ARPs and DHCP fall into this category.

- Packets discarded—The total number of data packets that the VPN Client rejected because they did not come from the secure VPN device gateway.

Secured Routes

The Secured Routes section lists the IPSec Security Associations (SAs).

In Figure 4-34 under Secured Routes, the columns show the following types of information.

- Key icon—In the first row, you see a key icon at the start of the connection entry. This key shows that the route is secure. The software generates a key as soon as the client needs to send secure data through the tunnel to the networks on the other side. The absence of a key means that the SA is no longer active. The SA may have timed out due to inactivity. Sending data to this network re-establishes the SA, and the key reappears.
- Network—The IP address of the remote private network with which this VPN Client has an SA.
- Subnet Mask—The subnet mask of the IP address for this SA.
- Bytes—The total amount of data this SA has processed. This includes data before encryption as well as encrypted data received.
- Port, Dst Port, and Protocol are for future use.

Local LAN Routes

If active the Local LAN Routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network through an IPSec tunnel. You can access up to 10 networks on the client side of the connection. A network administrator at the central site must configure the networks you can access from the client side. For information on configuring Local LAN Access on the VPN 3000 Concentrator, refer to *VPN Client Administrator Guide*, Chapter 1.

Time Connected


The Statistics tab also displays the time in days, hours, minutes and seconds, that has elapsed since you initiated the connection.

Firewall Tab

The Firewall tab displays information about the VPN Client's firewall configuration.

The VPN Concentrator's network manager sets up the firewall policy under Configuration | User Management | Base Group or Group | Client FW tab. There are three options:

- **Are You There**—The supported personal firewall software on the VPN Client PC controls its own rules. The VPN Client polls the firewall every 30 seconds to make sure it is still running, but does not confirm that a specific policy is enforced.
- **Centralized Protection Policy**—This policy takes advantage of the Cisco Integrated Client. The policy rules are defined on the VPN Concentrator and sent to the VPN Client during each connection attempt. The VPN Client enforces these rules for all non-tunneled traffic while the tunnel is active.
- **Client/Server**—This policy relates to Zone Labs Integrity solution. The policy is defined on the Integrity Server in the private network and sent to the VPN Concentrator, which in turns sends it to the Integrity Agent on the VPN Client PC to implement. Since Integrity is a fully functional personal firewall, it can intelligently decide on network traffic based on applications as well as data.

 **Note** CPP affects Internet traffic only. Traffic across the tunnel is unaffected by its policy rules. If you are operating in tunnel everything mode, enabling CPP has no affect.

The information shown on this tab varies according to your firewall policy.

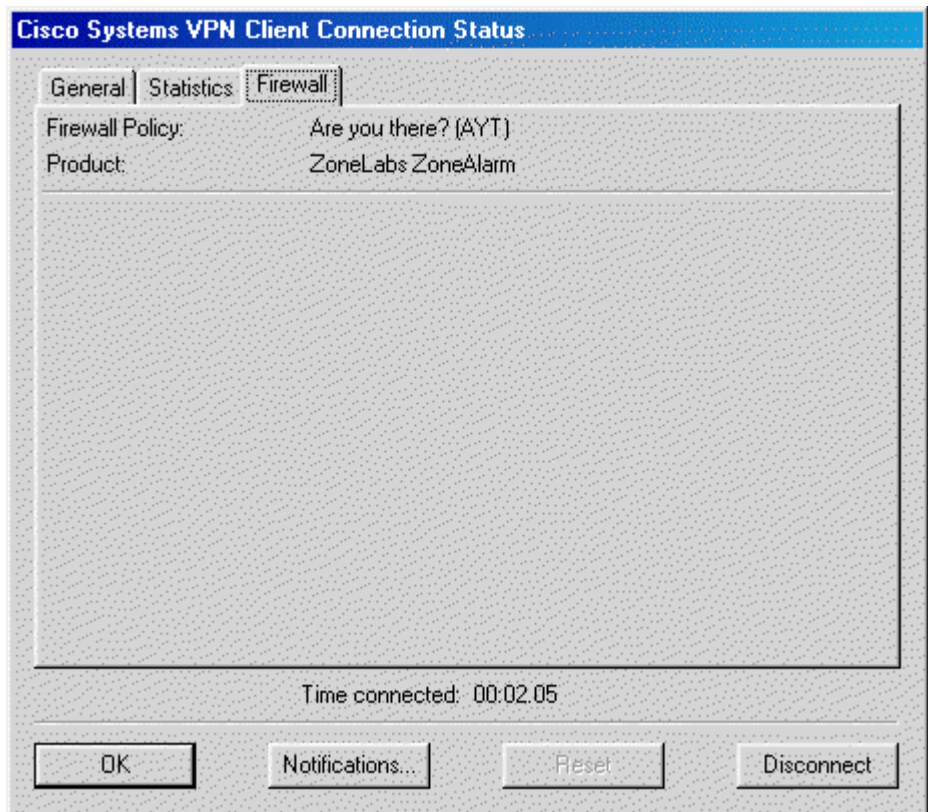
- **AYT**—When the Are You there (AYT) is the supported capability, the Firewall tab shows only the firewall policy (AYT) and the name of the firewall product (see Figure 4-35).

- Centralized Protection Policy (CPP)—When CPP is the supported capability, the Firewall tab includes the firewall policy, the firewall in use, and firewall rules (see Figure 4-36).
- Client/Server—When the Client/Server is the supported capability, the Firewall tab displays the firewall policy as Client/Server, the name of the product as ZoneLabs Integrity Agent, the user ID, session ID, and the addresses and port numbers of the firewall servers (see Figure 4-37).

AYT Firewall Tab

The Firewall tab shows that AYT is running and displays the name of the firewall product that supports AYT.

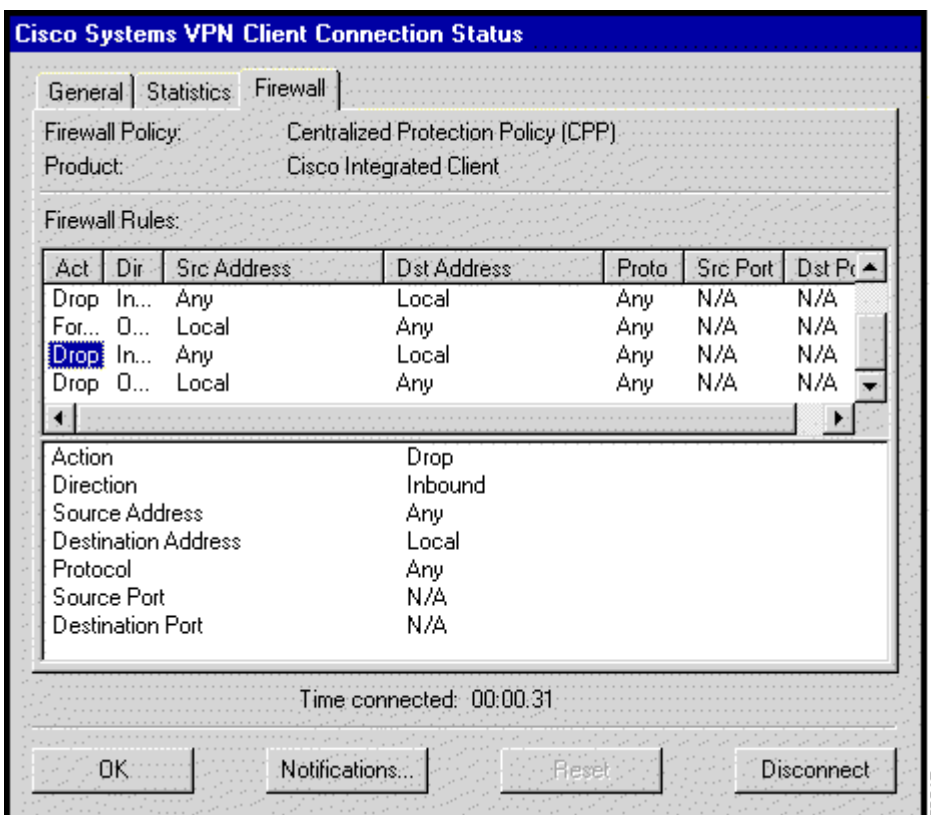
Figure 4-35: Firewall Tab for AYT capability



Centralized Protection Policy (CPP) Using the Cisco Integrated Client

CPP is a stateful firewall policy that is defined on and controlled from the VPN Concentrator. It can add protection for the VPN Client PC and private network from intrusion when split tunneling is in use. For CPP (see Figure 4-36), the Firewall tab shows you the firewall rules in effect.

Figure 4-36: Firewall Tab for CPP



This status screen lists the following information:


- Firewall Policy—The policy established on the VPN Concentrator for this VPN Client.
- Product—Lists the name of the firewall currently in use, such as Cisco Integrated Client, Zone Alarm Pro, and so on.

Firewall Rules

The Firewall Rules section shows all of the firewall rules currently in effect on the VPN Client. Rules are in order of importance from highest to lowest level. The rules at the top of the table allow inbound and outbound traffic between the VPN Client and the secure gateway and between the VPN Client and the private networks with which it communicates. For example, there are two rules in effect for each private network that the VPN Client connects to through a tunnel (one rule that allows traffic outbound and another that allows traffic inbound). These rules are part of the VPN Client software. Since they are at the top of the table, the VPN Client enforces them before examining CPP rules. This approach lets the traffic flow to and from private networks.

CPP rules (defined on the VPN Concentrator) are only for nontunneled traffic and appear next in the table. For information on configuring filters and rules for CPP, see *VPN Client Administrator Guide*, Chapter 1. A default rule "Firewall Filter for VPN Client (Default)" on the VPN Concentrator lets the VPN Client send any data out, but permits return traffic in response only to outbound traffic.

Finally, there are two rules listed at the bottom of the table. These rules, defined on the VPN Concentrator, specify the filter's default action, either drop or forward. If not changed, the default action is drop. These rules are used only if the traffic does not match any of the preceding rules in the table.

 **Note** The Cisco Integrated Client firewall is stateful in nature, where the protocols TCP, UDP, and ICMP allow inbound responses to outbound packets. For exceptions, refer to *VPN Client Administrator Guide*, Chapter 1. If you want to allow inbound responses to outbound packets for other protocols, such as HTTP, a network administrator must define specific filters on the VPN Concentrator.

You can move the bars on the column headings at the top of the box to expand their size; for example, to display the complete words Action and Direction rather than Act or Dir. However, each time you exit from the display and then open this status tab again, you must expand the columns again. Default rules on the VPN Concentrator (drop any inbound and drop any outbound) are always at the bottom of the list. These two rules act as a safety net and are in effect only when traffic does not match any of the rules higher in the hierarchy.

To display the fields of a specific rule, click on the first column and observe the fields in the next area below the list of rules. For example, the window section

underneath the rules in Figure 4-36 displays the fields for the rule that is highlighted in the list.

A firewall rule includes the following fields:

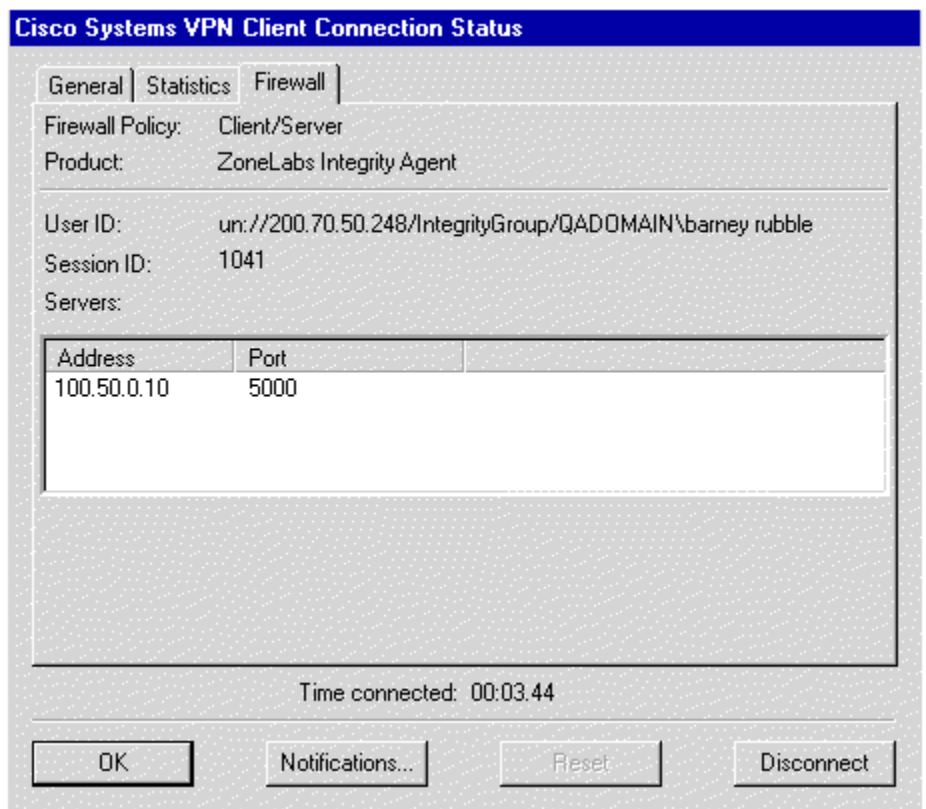
- Action—The action taken if the data traffic matches the rule:
 - - Drop = Discard the session.
 - Forward = Allow the session to go through.
- Direction—The direction of traffic to be affected by the firewall:
 - - Inbound = traffic coming into the PC, also called local machine.
 - Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.
- Source Address—The address of the traffic that this rule affects:
 - - Any = all traffic; for example, drop any inbound traffic.
 - This field can also contain a specific IP address and subnet mask.
 - Local = the local machine; if the direction is Outbound then the Source Address is local.
- Destination Address—The packet's destination address that this rule checks (the address of the recipient).
 - - Any = all traffic; for example, forward any outbound traffic.
 - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).
- Source Port—Source port used by TCP or UDP.

- Destination Port—Destination port used by TCP or UDP.

Client/Server Firewall Tab

When Client/Server is the supported policy, the Firewall tab displays the name of the firewall policy, the name of the product, the user ID, session ID, and the addresses and port numbers of the firewall servers in the private network (see Figure 4-37). Zone Labs Integrity is a Client/Server firewall solution in which the Integrity Server (IS) acts as the firewall server that pushes firewall policy to the Integrity Agent (IA) residing on the VPN Client PC. Zone Labs Integrity can also provide a centrally controlled always on personal firewall.

Figure 4-37: Client/Server Firewall Tab



Firewall Policy—This field shows that Client/Server is the supported policy.

Product—Lists the name of the Client/Server solution currently in use, such as Zone Labs Integrity Client.

User ID—In the format *xx://IP address of the VPN Concentrator/group name and user name*

Where: *xx* can be **un** or **dn**:

un = The gateway-based ID is based on the group and user name.

dn = The gateway-based ID is based on the distinguished name (as is the case when using digital certificates).

The User ID is used to initialize the firewall client.

Session ID—The session ID of the connection between all of the entities. This is used to initialize the firewall client and is helpful for troubleshooting.

Servers—The IP address and port number of each firewall server. For Release 3.6, there is only one.

Resetting Statistics

To reset all connection statistics to zero, click **Reset**. *There is no undo*. Reset affects only the connection statistics, not the other sections of this dialog box.

Closing the VPN Client

You may want to close the VPN Client when it is running on your PC but not connected to a remote network.

To close the VPN Client when it is not connected to a remote network, do one of the following:

- Click **Close** on the VPN Dialer's main dialog box. (See Figure 4-1).
- Press **Esc** on your keyboard.
- Press **Alt-F4** on your keyboard.

Disconnecting your VPN Client Connection

To disconnect your PC from the private network, do one of the following:

- Double-click the VPN Client icon on the Windows task bar. Click **Disconnect** on the Connection Status dialog box. (See Figure 4-33.)

- Click the VPN Client icon with the secondary mouse button and choose **Disconnect** from the pop-up menu.

Your IPSec session ends and the VPN Client closes. You must manually disconnect your dial-up networking connection (DUN).