



## 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 *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

This chapter includes the following major topics:

- [VPN 3000 Series Concentrators Configuration Information](#)
- [Configuring Entrust Entelligence for the VPN Client—Windows Only](#)
- [Setting up the VPN Client for Authentication using Smart Cards—Windows Only](#)
- [Configuring Mutual Authentication](#)

### VPN 3000 Series Concentrators Configuration Information

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

This section covers the following tasks:

- [Configuring a VPN 3000 Concentrator for Remote Access Users](#)
- [Configuring VPN Client Firewall Policy—Windows Only](#)
- [Notifying Remote Users of a Client Update—All VPN Client Platforms](#)
- [Setting up Local LAN Access for the VPN Client](#)
- [Configuring the VPN Concentrator for Client Backup Servers](#)
- [Configuring NAT Traversal for the VPN Client](#)
- [Configuring Automatic Browser Configuration—Windows Only](#)

### Configuring a VPN 3000 Concentrator for Remote Access Users

Before VPN Client users can access the remote network through a VPN 3000 Concentrator, you must complete the following tasks on the VPN 3000 Concentrator:

- 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.

## Completing Quick Configuration

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

Be sure to perform the following tasks.

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



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

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

## Creating an IPSec Group

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


Refer to “User Management” in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*, or the online help, for details on configuring groups.

You may want to set base-group attributes before you create an IPSec group; see the Configuration | User Management | Base Group screen. We suggest you carefully review the General Parameters and IPSec Parameters on that screen. If you use external user authentication, base-group attributes are especially important since they govern all attributes that the external server does not provide.

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

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


- 
- Step 1** Under the Identity tab, enter a Group Name and Password. VPN Client users need these to configure a connection entry and connect via the VPN Client; see “Gathering Information You Need” in Chapter 2 of the *VPN Client User Guide* for your platform.

- Step 2** Next, select a method of authentication. The Type parameter determines the group authentication method, Internal or External. Internal groups are configured on the VPN Concentrator. If you select External, you must configure an external RADIUS server to authenticate and provide appropriate group attributes.
- Step 3** Under the General tab | Tunneling Protocols, be sure IPsec is checked.
- Step 4** Under the IPsec tab | IPsec SA, select **ESP-3DES-MD5** to require Triple-DES authentication. Alternatively, you could choose **ESP-DES-MD5**, which uses DES authentication and provides a minimum level of security. Or, to use AES, select one of the AES protocols, such as **ESP-AES128-SHA**. AES is the most secure.
- 
-  **Note** To create or customize the Security Association (SA), see the Configuration | Policy Management | Traffic Management | Security Associations screens.
- 
- Step 5** Under IPsec > Authentication, choose the method you use for the members of the group; for example, Internal or RADIUS. If you choose an authentication method other than None or Internal, be sure to configure the external authentication server appropriately and supply users with the appropriate information for installing the VPN Client.
- Step 6** To require users to enter a password each time they log in, we suggest that you *not* check Allow Password Storage on Client, which is on the Client Config tab. Not checking this parameter provides greater security.
- Step 7** To add the group, click **Add**, and then save the configuration.
- 

## Creating VPN Client User Profiles

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

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

- Step 1** Enter a User Name, Password, and Verify Password. VPN Client users need a user name and password to authenticate when they connect to the VPN Concentrator; see “Gathering Information You Need” in Chapter 2 of the *VPN Client User Guide* for your platform.
- 
-  **Note** Beginning with Release 4.6.04.x, the VPN Client can accept a pre-shared password of up to 128 characters. The VPN 3000 Concentrator, however, imposes a limit of 32 characters.
- 
- Step 2** Under Group, select the group name you configured under the section “[Creating an IPsec Group](#).”
- Step 3** Carefully review and configure other attributes under General and IPsec. Note that if you are adding a user, the Inherit? checkboxes refer to base-group attributes; if you are modifying a user, the checkboxes refer to the user’s assigned-group attributes.
- Step 4** Click **Add** or **Apply**, and save the configuration.
-

## Configuring VPN Client Users for Digital Certificate Authorization

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

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

Follow these steps:

---

**Step 1** Use the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen to activate an IKE proposal for certificates:

- a. Activate one of the IKE protocols such as CiscoVPNClient-3DES-MD5-RSA-DH5, CiscoVPNClient-3DES-SHA-DSA-DH5, or CiscoVPNClient-AES128-SHA.




---

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

---

- b. If you do not want to modify one of the standard proposals, copy an active proposal and give it a new name; for example, copy the CiscoVPNClient-3DES-MD5-RSA-DH5 and name it “IKE-Proposal for digital certificate use.”
- c. Click Security Associations, which takes you to the next step.

**Step 2** Use the Configuration | Policy Management | Traffic Management | Security Associations screen to create a new SA. You can use the Security Associations link on the IKE Proposals screen.

- a. Add a new SA. For example, name it “Security association for digital certificate use.”
- b. Change the Digital Certificates parameter to identify the VPN 3000 Concentrator's digital certificate. This is the only field that you need to change.

**Step 3** Use the Configuration | User Management | Groups | Add or Modify screen to configure a group for using digital certificates:

- a. To use the Organizational Unit to configure the group, under the Identity tab, enter a group name that is the same as the OU field of the certificate(s) for this group. For example, if the OU in the VPN Client certificate is Finance, you would enter Finance as the group name. The OU is a field of the ASN.1 Distinguished Name (DN). Enter password and verify it.  
or  
Alternatively, you can configure a policy for certificate group matching. To use this approach, go to Configuration | Policy Management | Certificate Group Matching | Policy. For instructions on creating rules, see *VPN 3000 Series Concentrator Reference I: Configuration* for this section or refer to online help.
- b. Under the IPSec tab > IPSec SA, select the IPSec SA you created in step 2; for example, “Security association for digital certificate use.”

- c. Under IPsec tab > Authentication, select the method you use for user authentication; for example, Internal. If you select an external authentication method, such as RADIUS, be sure to configure the external authentication server appropriately and supply users with the appropriate entries for the “Gathering the Information You Need” section in Chapter 2 of the *VPN Client User Guide* for your platform.
  - d. Click **Add** or **Apply**, and save the configuration.
- Step 4** Use the Configuration | User Management | Users | Add or Modify | Identity screen to configure VPN Client users for digital certificates:
- a. As the group name, enter the group you have set up in step 3 as the group parameter; continuing the example, you would enter `Finance`.
  - b. Click **Add** or **Apply**, and save the configuration.
- 

## Connecting with Digital Certificates

Before you create a VPN Client connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on the VPN Client system. If this is not the case, then you need to obtain a digital certificate. You can obtain one by enrolling with a PKI directly using the Certificate Manager feature, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we have tested the following PKIs:

- UniCERT from Baltimore Technologies ([www.baltimoretechnologies.com](http://www.baltimoretechnologies.com))
- Entrust PKI™ 5.0 from Entrust Technologies ([www.entrust.com](http://www.entrust.com))
- Verisign ([www.verisign.com](http://www.verisign.com))
- RSA KEON 5.7 and 6.0
- Microsoft Certificate Services 2.0
- Cisco Certificate Store

The Web sites listed in parentheses in this list contain information about the digital certificates that each PKI provides.

## Configuring VPN Client Firewall Policy—Windows Only

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

This section summarizes how a network administrator can control personal firewall features from a VPN 3000 Concentrator operating as the Secure Gateway communicating policy information to the VPN Client running on a Windows platform.

## Optional versus Required Configuration Option

The VPN Concentrator can require that a VPN Client use a designated firewall configuration or make this configuration optional. Making a designated firewall configuration optional gives a VPN Client user a chance to install the desired firewall on the client PC. When the VPN Client tries to connect, it notifies the VPN Concentrator about any firewalls installed on the client PC. The VPN Concentrator sends back information about what firewall the VPN Client must use. If the firewall configuration is optional, the VPN Concentrator can notify the VPN Client that there is a mismatch but still allow the VPN Client to establish a tunnel. The optional feature thus lets the network administrator of the VPN Client maintain the tunneled connection while obtaining and installing the required firewall.

## Stateful Firewall (Always On)

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

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

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

**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 VPN Concentrator. A network administrator defines this policy on the VPN Concentrator, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the “Always On” option, any more restrictive rules are enforced for Internet traffic while the tunnel is established.

Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. Cisco Integrated Client, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. CPP rules are in effect during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.

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

### Policy Configured on the Remote PC—Personal Firewall Enforcement

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

Currently, the VPN Client supports the following personal firewalls:

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

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

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

**Integrity Server (IS)**—located on a central organization's network, IS maintains policies for the firewall on the remote VPN Client PCs. A network manager defines the policy on the IS, the IS downloads the policy to the Integrity Agent (IA) on the remote PC through a secure tunnel activated through the VPN Concentrator. The IS monitors the PC to ensure enforcement of the policy. The IS also communicates with the VPN Concentrator to establish/terminate connections, exchange session and user information, and report status information.

**Integrity Agent (IA)**—on the remote PC enforces the protection policies it receives from IS and communicates with IS to exchange policy and status information. The IA also communicates with the VPN Client on the remote PC to obtain server addresses and to exchange status information with the VPN Concentrator.

**VPN Concentrator**—provides the means for configuring firewall functionality by group. It reports the IS's IP address and other VPN session-related information to the VPN Client, which passes it on to the IA. The VPN Concentrator also communicates with the IS to establish and terminate sessions, exchange session and user information, and request and acquire authentication status.

VPN Client—on the remote PC gets the IS addresses and information from the VPN Concentrator and passes it to the IA. The VPN Client also gets and reports status information from the IA and terminates sessions.

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

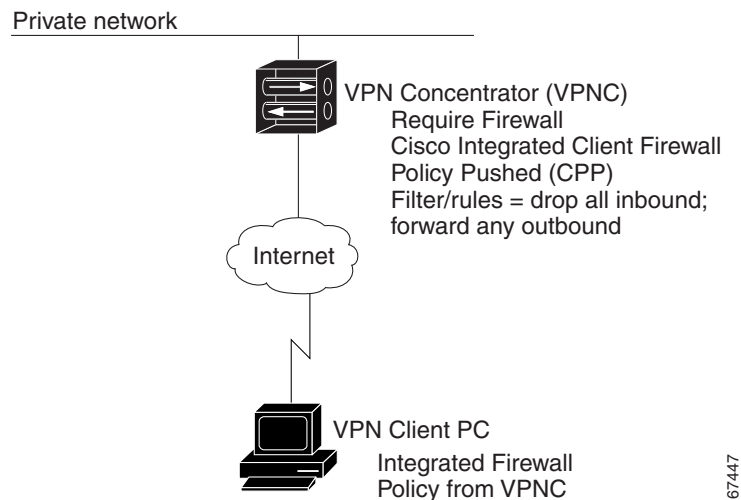
## Firewall Configuration Scenarios

This section shows three sample firewall configurations. Each diagram shows the parameter settings in effect on the VPN Concentrator as well as the firewall product and policy in effect on the VPN Client.

### Cisco Integrated Client

Figure 1-1 shows a typical configuration for Cisco Integrated Client, in which the policy (CPP) is pushed to the VPN Client. This policy blocks inbound traffic from the Internet while split tunneling is in use. Traffic from the private network is not blocked, however.

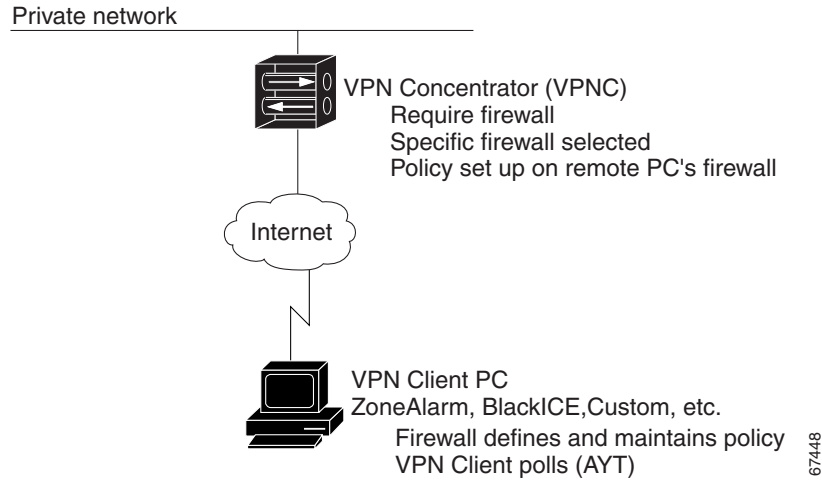
**Figure 1-1 Cisco Integrated Client**



### Remote Firewall

Figure 1-2 shows a configuration in which the policy is set up on a personal firewall on the PC. In this case, Are You There (AYT) is the policy. The VPN Client polls the firewall every 30 seconds to ensure that it is still running and if it is not, the VPN Client terminates the session.

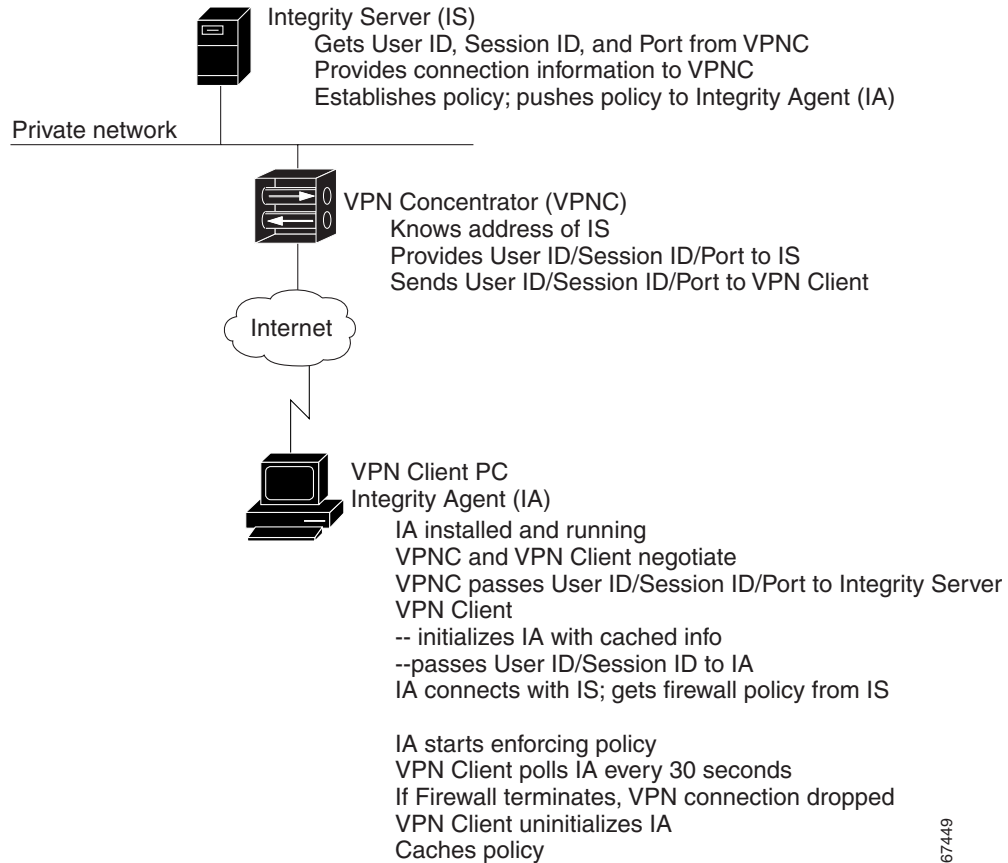
**Figure 1-2 Remote Firewall Determines Policy**



**Client/Server Approach**

Figure 1-3 shows a sample configuration for Zone Labs Integrity.

**Figure 1-3 Client/Server—Integration With Zone Labs Integrity Server**



## Defining a Filter and Rules to Use with Firewalls for CPP

When you want the VPN Concentrator to push the firewall policy to the VPN Client, you must first define the policy on the VPN Concentrator. To do this you need to create a filter and add rules to the filter on the public network. The VPN 3000 Concentrator provides a default filter you can use for CPP by selecting it from the menu. The name of this filter is “Firewall Filter for VPN Client (Default)”. This filter allows all outbound traffic and drops all inbound traffic.

Firewall filters are session filters, rather than packet filters. This means that for an “allow all outbound/drop all inbound” rule, the CPP policy lets inbound responses come from outbound sessions *only* from IP protocols TCP, UDP, and ICMP. These protocols are the only protocols that are “stateful.” Most administrators will want to use a rule that blocks all inbound traffic and either permits all outbound traffic or limits outbound traffic to specific TCP and UDP ports. For complete information on creating filters and adding rules in general, see *VPN 3000 Series Concentrator Reference Volume 1: Configuration*, Configuration | Policy Management | Traffic Management.

### **Example 1-1** Creating a Filter for a Firewall Policy allowing the VPN Client to Act as a Web Server

This example shows step-by-step how to add a filter that allows outbound traffic to any protocol and to allow inbound traffic from HTTP but none of the other protocols. In this way, you can enable your VPN Client to become a Web server.

- 
- Step 1** First, create a rule that allows inbound traffic only from HTTP. To do this, go to Configuration | Policy Management | Traffic Management | Rules.
- Step 2** Click **Add**
- For the Rule Name, enter the name, such as `FW-Allow incoming HTTP`.
  - For Action, choose **Forward**.
  - For Protocol, choose **TCP**.
  - For TCP/UDP Destination Port, choose **HTTP(80)**.
  - Click **Add**.
- Step 3** Next add a filter that drops all inbound traffic except from HTTP but forwards any outbound traffic while connected through a tunnel. To do this, under Traffic Management, click **Filters**.
- Click the **Add Filter** box.
  - Enter the filter name, such as `FW-Allow Incoming HTTP`, and select the defaults for the remaining parameters.
  - Click **Add**, which brings up the Actions screen.
  - On this screen, highlight the rule you made in Step 2 and click **Add** to move it to the Current Rules in Filter column. Do the same for the Any Out (forward/out) rule.
  - Click **Done**.
- Step 4** Save the configuration.
- This filter now is available under Base Group and Groups for you to select for the CPP policy.
-

## Configuring the VPN 3000 Concentrator to Enforce Firewall Usage on the VPN Client

This section shows how to configure the VPN Concentrator to require the VPN Client to enforce the use of a personal firewall on the VPN Client PC. On the VPN 3000 Concentrator side, you configure the Base Group or a specific group of users to enforce a personal firewall policy on the VPN Client side. Use the following general procedure.

- 
- Step 1** To configure firewalls for the Base Group, choose **Configuration | User Management | Base Group** or to configure firewalls for a specific group, choose **Configuration | User Management | Groups**.
- Step 2** To add a firewall, do one of the following:
- For the Base Group, choose the **Client FW** tab.
  - To create a new group for a firewall configuration, click **Add Group** and then click the **Client FW** tab.
  - To add a firewall to an existing group, highlight the group name, click **Modify Group**, and click the **Client FW** tab.
- Step 3** To require a firewall, under the Firewall Setting attribute, choose **Firewall Required**.
- Step 4** Under the Firewall attribute, choose a firewall from the Firewall pull-down menu. If the firewall you are using is not on the list, you must use **Custom**.
- Step 5** Choose the **Firewall Policy**: Policy defined by the remote firewall (AYT) or Policy pushed (CPP). (See the next section.)

For complete information, refer to *VPN 3000 Series Concentrator Reference Volume I: Configuration*, the section “User Management” or the VPN 3000 Concentrator Network Manager’s online help.

---

## Setting up Cisco Integrated Client Firewall (CIC) for CPP

- 
- Step 1** Under Client FW tab on Firewall Setting, choose **Firewall Required**.
- Step 2** On the Firewall pull-down menu, choose **Cisco Integrated Client Firewall**.
- Step 3** On Firewall Policy, click **Policy Pushed** and select a filter that contains firewall policy rules. You can choose the default firewall filter or one that you have configured for a special purpose (see [“Defining a Filter and Rules to Use with Firewalls for CPP”](#)).
- 

## Setting up a Client/Server Firewall —Zone Labs Integrity

- 
- Step 1** Configure firewall policy on the Integrity Server (IS), following Zone Labs documentation.
- Step 2** On the VPN Concentrator, go to Configuration | System | Servers | Firewall Server. For the Zone Labs Integrity Server, enter the host name or IP address and the port number.
- Step 3** Under Configuration | User Management | Base Group or Groups | Client FW tab (see [“Defining a Filter and Rules to Use with Firewalls for CPP”](#)), configure the following:
- a. Firewall Setting = **Firewall Required**
  - b. Firewall = **Zone Labs Integrity**
  - c. Firewall Policy = **Policy from Server**

**Step 4** Save the configuration.

---

## Custom Vendor Codes

On the VPN 3000 Concentrator, you can configure a custom firewall. Currently there are no supported firewall configurations that you cannot choose from the menu on the VPN Concentrator. This feature is mainly for future use. Nevertheless, the following table lists the vendor codes and products that are currently supported.

## Obtaining Firewall Troubleshooting Information

This section describes two ways to obtain information about firewall negotiations: through the IPSec Log or a notification from the VPN Concentrator.

### Examining the IPSec Log

One way to see what is happening during tunnel negotiation between the VPN Client and the VPN Concentrator is to examine messages in the IPSec Log on the VPN Client. You can use the Log Viewer application to do this (for information on using Log Viewer, refer to the *VPN Client User Guide for Windows*, Chapter 5). During tunnel negotiation, the VPN Client initiates the firewall exchange by sending the VPN Concentrator a list of firewalls installed and running on the PC, if any. The VPN Concentrator then sends messages indicating its firewall requirements to the VPN Client.

Following is an example of this exchange.

First, the request from the VPN Client to the VPN Concentrator:

```
36      16:44:39.250  02/28/03  Sev=Info/5
IKE/0x6300005D
Client sending a firewall request to concentrator

37      16:44:39.250  02/28/03  Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).
```

87647

Next, the responses from the VPN Concentrator:

```
47      16:44:40.162  02/28/03  Sev=Info/5
IKE/0x6300005E
Client received a firewall reply from concentrator

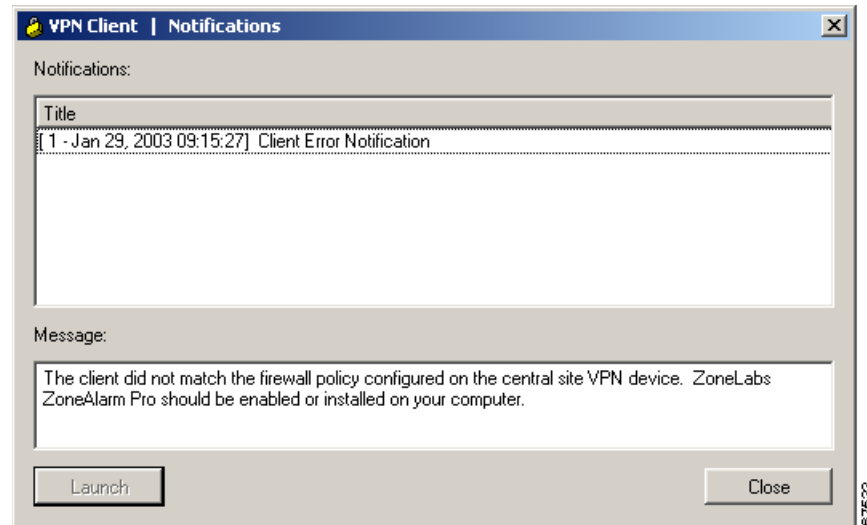
48      16:44:40.162  02/28/03  Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).
```

87648

## Notifications

If the VPN Client and VPN Concentrator firewall configurations do not match, the VPN Concentrator notifies the VPN Client when the VPN Client user attempts to connect. If the firewall configuration is required, the connection attempt fails; if the firewall configuration is optional, the tunnel comes up.

**Figure 1-4 Firewall Mismatch Notification**



## Notifying Remote Users of a Client Update—All VPN Client Platforms

You can notify VPN Client users when it is time to update the VPN Client software on their remote systems. The notification can include a location containing the client update (the update does not happen automatically). Use the Client Update procedure at the VPN 3000 Concentrator to configure a client notification:

- 
- Step 1** To enable Client Update, go to Configuration | System | Client Update and click **Enable**.
  - Step 2** At the Configuration | System | Client Update | Enable screen, check **Enabled** (the default) and then click **Apply**.
  - Step 3** On the Configuration | System | Client Update | screen, click **Entries**.
  - Step 4** On the Entries screen, click **Add**. | The VPN Concentrator Manager, displays the Configuration | System | Client Update | Entries | Add or Modify screen.
  - Step 5** For Client Type, enter the operating systems to notify:
    - Windows includes all Windows based platforms
    - Win9X includes Windows 95, Windows 98, and Windows ME platforms
    - WinNT includes Windows NT 4.0, Windows 2000, and Windows XP platforms
    - Linux
    - Solaris
    - Mac OS X




---

**Note** The VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value Windows includes all Windows platforms, and the value WinNT includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both Windows *and* WinNT. To find out the client types and version information, click on the lock icon at the top left corner of the Cisco Systems VPN Client main window and choose **About VPN Client**.

---

**Step 6** In the URL field, enter the URL that contains the notification.

To activate the Launch button on the VPN Client Notification, the message must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The message can also include the directory and filename of the update, for example, <http://www.oz.org/upgrades/clientupdate>. If you do not want to activate the Launch button for the remote user, you do not need to include a protocol in the message.

**Step 7** In the Revisions field, enter a comma separated list of client revisions that do not need the update because they are already using the latest software. For example, the value 3.6.5 (Rel), 4.0 (Rel) identifies the releases that are compliant; all other VPN Clients need to upgrade.

**Step 8** Click **Add**.

---

The Notification dialog box appears when the remote user first connects to the VPN device or when the user clicks the Notifications button on the Connection Status dialog box. When the notification pops up, on the VPN Client, click **Launch** on the Notification dialog box to open a default browser and access the URL containing the update.

## Setting up Local LAN Access for the VPN Client

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

Before you begin, you should carefully read the section on split tunneling in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*. See the section explaining Configuration | User Management | Groups | Add or Modify | IPSec tab.

Configuring local LAN access involves the following general steps:

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

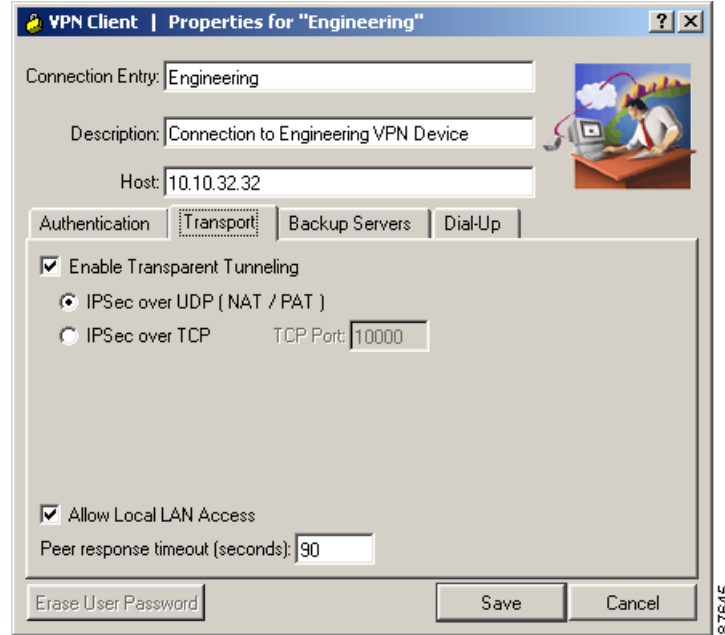
Use the following procedure:

---

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

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

Figure 1-5 Setting the Allow Local LAN Access Parameter on the VPN Client



- Step 2** On the VPN 3000 Concentrator, either add a new group or modify an existing group as follows:
- To configure local LAN access for a specific group, go to Configuration | User Management | Groups.
  - Choose either **Add** to add a new group or **Modify** to enable Local LAN for an existing group.
  - Go to the Client Config tab.
  - At the Split Tunneling Policy attribute, under Value, click the **Tunnel everything** radio button and then click **Allow the networks in list to bypass the tunnel**. This enables local LAN access on the VPN Client.
  - At the Split Tunneling Network List, under Value, choose the network list you have created for local LAN access, if any.

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

For information on creating a network list, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, “Configuration | Policy Management | Traffic Management | Network Lists”.

**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 the VPN Concentrator for Client Backup Servers

This section shows how to configure a group on the VPN Concentrator to automatically push new backup server information to a VPN Client.

- 
- Step 1** On the VPN Concentrator, go to Configuration | User Management | Group.
  - Step 2** To add a new group, click **Add** or to modify an existing group, highlight it in the box and click **Modify**.
  - Step 3** Go to the Client Config tab.
  - Step 4** For IPsec Backup Servers, select **Use List Below** from the drop-down menu.
  - Step 5** Enter a list of up to 10 IPsec backup servers in high to low priority order.
  - Step 6** Type each server address or name on a single line into the IPsec Backup Servers box.
  - Step 7** Click **Apply** and then save the configuration.
- 

## Configuring NAT Traversal for the VPN Client

NAT Traversal (NAT-T) lets the VPN Concentrator establish IPsec tunnels with a VPN Client when there is a NAT device between them. It does this by encapsulating ESP traffic in UDP datagrams, which provides ESP with the port information that NAT devices require.

You can configure NAT-T globally on the VPN Concentrator, which then activates NAT-T for all groups configured on the VPN Concentrator.

### Global Configuration

To configure NAT-T globally, follow these steps on the VPN Concentrator:

- 
- Step 1** Go to Configuration | System | Tunneling Protocols | IPsec | NAT Transparency and check the **IPsec over NAT-T** check box.
  - Step 2** Click **Apply** and then save the configuration.
-

Next configure the following parameters on the VPN Client.

- 
- Step 1** If creating a new connection entry, click **New** under Connection Entries. If modifying an existing connection entry, highlight the entry and click **Modify**. In either case, a properties dialog box displays.
  - Step 2** Open the **Transport** tab.
  - Step 3** Check **Enable Transparent Tunneling** check box.
  - Step 4** Click the **IPSec over UDP (NAT/PAT)** radio button.
- 

## Configuring Automatic Browser Configuration—Windows Only



### Note

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

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

A network administrator configures this setting on the VPN Concentrator. Use the following procedure to configure the browser proxy setting for the VPN Client:

- 
- Step 1** On the VPN Concentrator, go to **Configuration | User Management | Base Group**.
  - Step 2** Click the **Client Config** tab.
  - Step 3** Scroll down to the **Microsoft Client Parameters** section.
  - Step 4** Edit the following sections:
    - a. Select the **IP Proxy Server Policy** method (following the instructions on the screen). Your choices are as follows. These choices are mutually exclusive.
      - Do not modify proxy settings—leaves the proxy setting unchanged
      - No proxy—disables the proxy setting in the VPN Client PC
      - Autodetect proxy—enables automatic detection of the proxy server setting in the VPN Client PC (but does not change it)
      - Use the proxy and server port configured in the IE Proxy Server box. If you choose this option, fill in the remaining boxes in this section of the Client Config tab. IE Proxy Server identity is required.
    - b. In the **IE Proxy Server** box, enter the name of the proxy server, a colon (:), and the port number for clients using Internet Explorer; for example, myproxy.mycompany.com:8080
    - c. In the **IE Proxy Serve Exception List**, enter the addresses or domains that are not to be accessed through a proxy server. This list corresponds to the Exceptions box in the Proxy Settings dialog box in Internet Explorer. You can enter wildcards; for example, www.\*.org or 10.10.\*
    - d. To allow local requests to bypass the proxy server, click **Bypass Proxy Server for Local Addresses**.

**Step 5** Make sure you save the configuration.

---

**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 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.

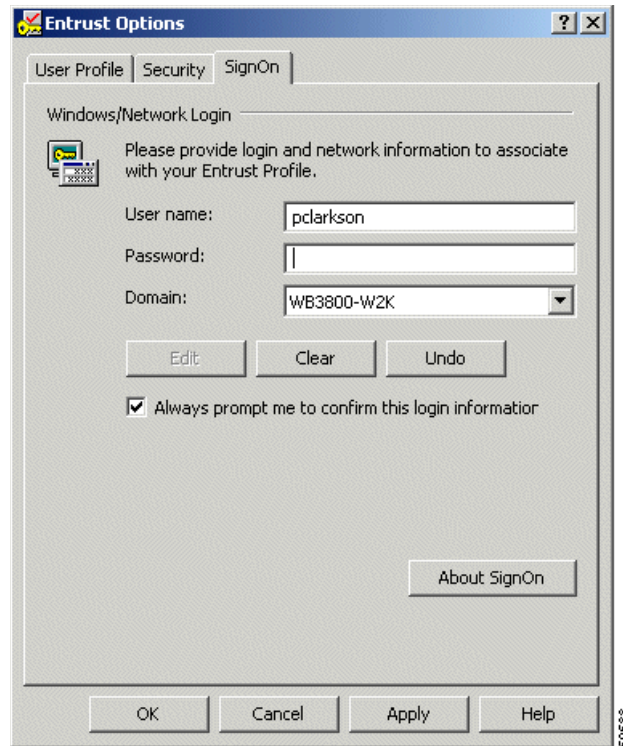
To create an Entrust Entelligence profile, you need the following information:

- 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 1-6](#).)
- b. Make sure that you check **Always prompt me to confirm this login information**. Checking this box causes the Entrust SignOn login dialog box to pause and allow the VPN connection to come up before the remote user enters the NT logon information.

Figure 1-6 Entrust Options SignOn Tab



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

**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 NT, Windows 2000 and Windows XP systems, this directory is `c:\WinNT\System32`. For Windows 9x and Windows ME, the directory is `\Windows\System`.

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

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

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

In general:

- 
- Step 1** Under Key Options, when you are performing web-based certificate enrollment, choose your smart card provider from the pull-down menu.
  - Step 2** For Key usage choose **Signature** and verify that **Create new key set** is selected.
  - Step 3** Install the certificate. The keys are generated on the smart card and a copy of the certificate is stored in the Microsoft store on your PC and listed on the VPN Client Certificates tab.
  - Step 4** Go to the Connection Entry > Modify dialog, and do the following:
    - a. Open the Authentication tab and check the Certificate Authentication radio button
    - b. Display the drop-down Name menu and click the smartcard certificate.
- 

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



## 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.

---

## Configuring Mutual Authentication

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

## Configuring Mutual Group Authentication on the VPN Client System

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

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

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

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

## Configuring Mutual Authentication on the VPN Concentrator

The VPN Concentrator must use the same Certificate Authority (CA) as the VPN Client system for mutual authentication to take place. On the VPN Concentrator side, you must configure the following:

- Step 1** Select an IKE proposal that allows HYBRID mode authentication, such as those listed “[Valid VPN Client IKE Proposals](#)” (table) in Chapter 8 of this manual. For example, in the VPN Concentrator, select HYBRID-AES256-SHA-RSA as the IKE proposal. For information on configuring IKE proposals, see *VPN 3000 Series Concentrator Reference, Volume I, Configuration*, the section on Configuration | Tunneling and Security | IPSec | IKE Proposals:  
([http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a00801f1e36.html#1137591](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1e36.html#1137591))



**Note** IKE proposals that include HYBRID mode authentication are not in the 4.1 Rel release of the VPN 3000 Concentrator. However, you can select them in the VPN 3000 Concentrator release that accompanies Release 4.6.

- Step 2** If the VPN Concentrator does not yet have an identity certificate, you need to enroll with the CA for the certificate. You can find information for doing so in *VPN 3000 Series Concentrator Reference, Volume II, Administration and Monitoring*, the section on Configuration Management:  
([http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_administration\\_guide\\_chapter09186a00801f1dc5.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_administration_guide_chapter09186a00801f1dc5.html)).
- Step 3** Configure an IPSec SA to use an identity certificate to be authenticated with the CA certificate of the VPN Client. You can find information in *VPN 3000 Series Concentrator Reference, Volume I, Configuration*, the section on Configuration | Policy Management | Traffic Management | Security Associations:  
([http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a00801f1dbb.html#1563342](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1dbb.html#1563342))

- Step 4** Configure a VPN Group on the VPN Concentrator to use the new IPsec SA from Step 3. For information on configuring VPN groups, see *VPN 3000 Series Concentrator Reference, Volume I, Configuration*, the section on Configuration | User Management | Groups, IPsec tab:  
([http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a00801f1df7.html#1907522](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1df7.html#1907522).)