Reference Manual for the NETGEAR ProSafe VPN Client

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10015-01
November 2003

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR™ does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Technical Support

Refer to the Support Information Card that shipped with your NETGEAR ProSafe VPN Client.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Contents

Chapter 5
Using the Security Policy Editor

Chapter 6
Using the Certificate Manager

Chapter 7
Using Sessions

Chapter 8
Distributing Customized Profiles

Chapter 9
Troubleshooting

Appendix A
Networks, Routing, and Firewall Basics

Appendix B
Virtual Private Networking

Appendix C
NETGEAR ProSafe VPN Client
to NETGEAR FVS318 or FVM318 VPN Routers

Appendix D
NETGEAR VPN Client
to NETGEAR FVL328 or FWAG114 VPN Router

Glossary

Index

Chapter 1
About This Manual

Thank your for purchasing the NETGEAR ProSafe VPN Client. This chapter describes the target audience, versions, conventions, and features of this manual.

Audience, Versions, Conventions

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, and firewall technologies tutorial information is provided in the Appendices and on the NETGEAR Web site.

This guide uses the following formats to highlight special messages:

➡	Note: This format is used to highlight information of importance or special interest.

This manual is written for the NETGEAR VPN Client according to these versions.:

Table 1-1. Product, Firmware Version, Manual Version, and Publication Date

Product	NETGEAR ProSafe VPN Client
Manual Part Number	202-10015-01
Manual Publication Date	November 2003

➡	Note: Product updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/docs*.

Chapter 2
Introduction

This chapter describes the features of the NETGEAR ProSafe VPN Client.

The NETGEAR ProSafe VPN Client is a remote access and end-point security product that secures communications over the Internet and other public networks to create a virtual private network (VPN) between users. The NETGEAR VPN Client secures data communications sent from a desktop or portable computer across a public or private TCP/IP network. The client protects the office computer user and the home and mobile workforce.

The NETGEAR VPN Client supports secure client-to-gateway or client-to-client communications. For example, employees can telecommute from their homes to the office through the Internet or dial-in connections for secure client-to-gateway communications. Organizations that require a low-cost solution for secure communications among their employees or members across a private LAN, WAN, or individual dial-up connections can use the NETGEAR VPN Client for secure client-to-client communications.

The NETGEAR VPN Client starts automatically when the user's computer starts, and runs transparently at all times behind other software programs. A system tray icon indicates the status of communications for the client.

What's Included?

The NETGEAR ProSafe VPN Client contains two primary components:

- **Security Policy Editor** is where you create, import, and manage connections and their associated proposals that make up your security policy.
- **Certificate Manager** allows users to request and retrieve, import, and store the certificates users receive from certificate authorities (CAs), and to also set the trust policy.

There are also two diagnostic tools:

- **Log Viewer** lists the IKE negotiations that occur during Authentication (Phase 1).
- **Connection Monitor** displays statistical and diagnostic information for each active connection.

What’s in the Box?

The product package should contain the following items:

- NETGEAR ProSafe VPN Client
- *Resource CD (230-10007-01)*, including:
  - — This manual
  - — Application Notes, Tools, and other helpful information
- Warranty and support information card

Chapter 3
Installation

This chapter describes how to install your NETGEAR ProSafe VPN Client.

What You Need Before You Begin

You need to verify that your computer meets the minimum system requirements.

System Requirements

Before installing the NETGEAR ProSafe VPN Client, please make sure that these minimum requirements have been met:

- IBM-compatible computer with Pentium processor or equivalent (not Alpha platforms)
- Compatible operating systems with minimum RAM:

Operating system	Minimum RAM
Microsoft® Windows® 95	16 MB
Windows 98 and Windows NT® Workstation 4.0	32 MB
Windows Me and 2000 Professional	64 MB
Windows XP Home and Professional	64 MB; 128 MB recommended

  Some versions of Windows may ask for the original Windows operating system installation files to complete the installation of the VPN Client driver software

- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- For dial-up connections:
  - Non-encrypting modem
  - Native Microsoft PPP dialer
- For network connections, Ethernet card and connection
- Microsoft Internet Explorer 4.0 or later

Installing

Use the procedure below to install the NETGEAR ProSafe VPN Client.

1. If you're installing this product on Windows NT or Windows 2000 or XP, log on as **administrator** or its equivalent.
2. Run the **setup.exe** file on the installation CD-ROM or in the installation package.
3. Work through the installation wizard. Unless otherwise instructed, accept the defaults.

   Note: The SafeNet VPN Adapter, which supports L2TP, is installed only when these network components are already installed on your computer:

Operating system	**Component**
Windows 95	Dial-Up Networking with the Microsoft Dial-Up Networking 1.3 Upgrade
Windows 98 and Me	Dial-Up Networking
Windows NT	Remote Access Server (RAS)

   Because Windows 2000 and XP use the native Windows L2TP adapter, the SafeNet L2TP adapter isn't installed on computers running these operating systems.
4. When the installation completes, click **Finish**.
5. To complete the client installation, make sure that your computer restarts.

Note: The NETGEAR ProSafe VPN Client lets you configure and switch among multiple profiles for multiple tunnels. You can “Import” predefined configuration profiles. The FVS318.SPD and FVL328.SPD profile files on the NETGEAR ProSafe VPN Client *Resource CD (230-10007-01)* include all the settings identified in the configuration procedures published in these appendices: “NETGEAR ProSafe VPN Client to NETGEAR FVS318 or FVM318 VPN Routers“ on page C-1 and “NETGEAR VPN Client to NETGEAR FVL328 or FWAG114 VPN Router“ on page D-1.

Upgrading

To upgrade to this version of the NETGEAR ProSafe VPN Client, take these steps:

1. Uninstall the current version on your computer through the **Control Panel Add/Remove Programs** application**:**
   a. In the uninstall wizard, on the **Maintenance** dialog box, click **Remove**. This removes all the client product's components, but **not** your security policy.
   b. The **Uninstall Security Policy** dialog box prompts you to delete your IPSec security policy, which includes any certificates and private keys:
      – To keep it, click **No**. You can import this security policy after you install the new version of the NETGEAR ProSafe VPN Client.
      – To delete it, click **Yes**.
   c. When the **Maintenance Complete** dialog box opens, click **Finish**.
   d. To complete the uninstall, make sure that your computer restarts.
2. Install this new version of the NETGEAR ProSafe VPN Client.

Getting Started

The NETGEAR ProSafe VPN Client contains two primary modules:

- **Security Policy Editor** to configure and maintain the security policy
- **Certificate Manager** to request, store, and administer certificates

To learn how to use NETGEAR VPN Client, go to **Start>Programs>NETGEAR ProSafe VPN Client>NETGEAR ProSafe VPN Client Help**.

VPN Client Connection Indicators

The NETGEAR ProSafe VPN Client provides the following three indicators which give you feedback on the status of your wireless connection:

The System Tray (SysTray) resides on one end of the taskbar in the Microsoft Windows desktop.

Table 3-1.

Icon	Explanation
	• The Windows operating system did not start the IREIKE service properly. To start this service, restart your computer. If this icon continues to display, you may need to reinstall the client. or • Your security policy is deactivated—that is, disabled. To reactivate it, go to Reactivate the security polity.
	Your computer is ready to establish connections or transmit data.
	Your computer has established no secure connections and is transmitting unsecured data.
	Your computer has established at least one secure connection, but is transmitting no data.
	Your computer has established at least one secure connection and is transmitting only unsecured data.
	Your computer has established at least one secure connection and is transmitting only secured data.
	Your computer has established at least one secure connection and is transmitting secured and unsecured data.

Uninstalling the NETGEAR ProSafe VPN Client

When you remove NETGEAR ProSafe VPN Client and its components, you have the option to keep your security policy, certificates, and private keys to use when you upgrade or reinstall the client.

Note: Before you upgrade the client, read the readme file and Release Notes provided with the new version.

1. Open the **Control Panel Add/Remove Programs** application.
2. Remove **NETGEAR ProSafe VPN Client**. The details depend on the version of Windows on your computer.
3. Work through the uninstall wizard:
   a. When the **Maintenance** dialog box opens, click **Remove**.

b. When prompted to remove all installed components, click **Yes**.

Note: This does not remove the IPSec security policy, certificates, or private keys.

c. When prompted to remove the IPSec security policy, which includes certificates and private keys, in most cases, click **No**. You can import this policy after you reinstall this client version or upgrade to a newer client version; this can save a lot of time.

d. When the **maintenance complete** message opens, click **Finish**.

   Make sure that the computer restarts; this is required to complete the uninstall.

Keyboard Shortcuts

The client supports standard Windows keyboard shortcuts for accessibility. For a complete list of Windows keyboard shortcuts, refer to the keyboard shortcuts help topics in Windows.

Chapter 4
Configuring L2TP Connections

This chapter describes how to use configure VPN tunnels using the NETGEAR ProSafe VPN Client.

Basic Steps

The client supports Layer 2 Tunneling Protocol (L2TP) connections through a virtual adapter: the SafeNet VPN Adapter. The specific steps required vary with the Windows operating system installed on your computer.

To create and secure an L2TP connection, perform these tasks in the sequence that your network security administrator recommends:

- Configure a network connection to the remote party’s L2TP network server.
- Configure the security policy for L2TP.
- If you are establishing the L2TP or virtual adapter connection over a physical dial-up connection—that is, a modem—add another dial-up connection adapter.

How to Configure an L2TP Dial-Up Network Connection

Configuring a dial-up network connection for L2TP requires you to use the Dial-Up Networking (DUN) features of the Windows operating system. The steps vary by operating system.

For Windows 95/98/Me

1. Create the connection to the other party's L2TP network server:
   a. On the desktop, double-click **My Computer**.
   b. Double-click **Dial-Up Networking**. The **Dial-Up Networking** dialog box opens.
   c. Double-click **Make New Connection**. The **Make New Connection** wizard opens.

d. **Note:** If this is the first dial-up connection for your computer, the **Welcome to Dial-Up Networking** page opens instead. Follow the prompts to start the **Make New Connection** wizard.

e. In the **Type a name for the computer you are using** box, type the name for the connection.

f. In the **Select a device** box, click **SafeNet_VPN x** Adapter, where x is the number of the VPN adapter.

g. Click **Next**.

h. In the **Host name or IP address** box, type the IP address of the remote party's L2TP network server (LNS).

i. Click **Next**.

j. Click **Finish**.

2. Change properties for this connection:

   a. In **My Computer**, double-click **Dial-Up Networking**. The **Dial-Up Networking** dialog box opens.

   b. Right-click the specific connection, and then click **Properties**. The *connection_name* dialog box opens.

   c. On the tabs, locate the settings to change, and then make the changes.

   d. Click **OK** until you return to the **Dial-up Networking** window.

   e. Close the window.

For Windows NT 4.0

1. Double-click **My Computer**.
2. Double-click **Dial-up Networking**. The **Dial-Up Networking** dialog box opens.

   Note: If this is the first dial-up connection for your computer, the **Welcome to Dial-Up Networking** page opens instead. Follow the prompts until the **Dial-Up Networking** dialog box opens.

3. Click **New**. The **New Phonebook Entry** page opens.
4. Click the **Basic** tab.
5. In the **Entry name** box, type the name for the connection.

6. In the **Phone number** box, type the IP address of the remote party's LNS.
7. In the **Dial using** box, click **SafeNet_VPN x** Adapter, where x is the number of the VPN adapter.
8. Click the **Server** tab.
9. Click **OK**.

For Windows 2000

1. On the Windows desktop, click **Start>Settings>Network and Dial-up Connections**. The **Network and Dial-up Connections** window opens.
2. Double-click **Make New Connection**. The **Network Connection Wizard** opens.

   Note: If this is the first dial-up connection for your computer, you may be prompted to provide some preliminary data. Follow the prompts until you return to the **Network Connection Wizard**.
3. On the **Network Connection Type** page, take these steps:
   a. Click **Connect to a private network through the Internet**.
   b. Click **Next**.
4. On the **Select a Device** page, take these steps:
   a. In the **Select the devices to use in this connection** list, as many of the check boxes that apply; you must select at least one. If you're not sure which ones to select, contact your network administrator.
   b. Click **Next**.
5. On the **Public Network** page, take these steps:
   a. Click **Do not dial the initial configuration**.
   b. Click **Next**.
6. On the **Destination Address** page, identify the remote party's L2TP server:
   a. In the **Host name or IP address** box, type the IP address of the remote party's L2TP network server.
   b. Click **Next**.
7. On the **Connection Availability** page, select whether to make this connection available to only you or all others who use your computer:

a. Ask your network administrator which option to select, and then click that option.

b. Click **Next**.

8. On the **Completing the Network Connection Wizard** page, take these steps:

   a. Type the name for this connection; the default is **Virtual Private Connection**.

   b. Click **Finish**.

For Windows XP

1. On the Windows desktop, click **Start>Settings>Network Connections**. The **Network Connections** window opens.
2. Double-click **Make New Connection**. The **Network Connection Wizard** opens.
3. Click **Next**. The **Network Connection Type** page opens.
4. **Note:** If this is the first dial-up connection for your computer, you may be prompted to provide some preliminary data. Follow the prompts until you return to the **Network Connection Wizard**.
5. Click **Connect to the network at my workplace**.
6. Click **Next**. The **Network Connection** page opens.
7. Click **Virtual Private Network connection**.
8. Click **Next**. The **Connection Name** page opens.
9. In the **Workplace** box, type the name for this connection.
10. Click **Next**. The **VPN Server Selection** page opens.
11. Type the hostname or IP address of the remote party's L2TP server.
12. Click **Next**. The **Connection Availability** page opens.
13. For the **Create the connection for** option, accept the default, **Anyone's use**, or click **My use only**.
14. Click **Next**. The **Completing the New Connection Wizard** page opens.
15. If you like, select the **Add a shortcut to this connection to my desktop** check box.
16. Click **Finish**.

How to Configure a Security Policy

1. In the Security Policy Editor, in the **Network Security Policy** list, click the specific secure connection 🔒.
2. In the Remote Party Identity and Addressing group, configure the remote party's information.

   Note: When configuring security for L2TP, the remote party is the L2TP network server (LNS).

   a. In the **ID Type** box at the top of the group, click one of these remote party identifiers:
      - Domain name
      - IP address
      - Email address
      - Distinguished name
      - Any

   b. In the **IP Address** box, type the IP address of the LNS.

   c. In the **Protocol** box, click **UDP**.

   d. In the **Port** box, click **L2TP**.

   e. Unless otherwise instructed, make sure that the **Connect using** check box is clear.
3. Ask the remote party if you need to change the **Port** value to **L2TP** in My Identity.
4. When you configure the Key Exchange (Phase 2) proposal, in the **Encapsulation** box, click **Transport**, which is the typical L2TP connection setting.
5. Click **Save**.

When Using a Modem to Establish the L2TP Connection

Note: If you use a network or broadband connection, such as cable or DSL, to establish an L2TP connection on a network, skip this topic; it doesn't apply. If you have questions, contact your network security administrator.

If you establish the L2TP connection from your computer through a physical dial-up connection—that is, a modem—your computer requires two Microsoft dial-up connections or adapters:

- One for the L2TP connection, which is a virtual connection

- One for the physical dial-up connection

Therefore, you must add another dial-up connection through Windows. The specific steps required to add a second dial-up connection differ among the various Windows operating systems. This is the general procedure:

1. On your computer, in Windows help, look up **network adapters**, **network connections**, or **add a connection**.
2. In **Control Panel**, open the **Network** or **Network and Dial-up Connections** application.
3. Follow the instructions in the help to add another dial-up connection or adapter.

   Note: In Windows 95 and 98, dial-up adapters may be labeled **Dial-Up Adapter** and **Dial-Up Adapter#2 (VPN Support)**.

If you need additional help, contact your network security administrator or IT staff.

Chapter 5
Using the Security Policy Editor

This chapter describes how to use the Security Policy Editor of the NETGEAR VPN Client.

What is the Security Policy Editor?

The Security Policy Editor is the client module in which you (or your network security administrator) create, import, and export security policies. Only one security policy is in effect at any time.

The policy contains connections and proposals that define the address of the remote (or other) party, the security level for the connection, how you identify yourself to the other party, and other attributes concerning the proposals and connections.

The sequence of the connections in the Network Security Policy list in the Security Policy Editor determines the order in which the client tests for a match between an incoming transmission and the proposed policies, and in turn defines the connection's security policy.

There are two ways to open the Security Policy Editor:

- On the Windows desktop, click **Start>Programs>NETGEAR ProSafe VPN Client>Security Policy Editor**.
- Right-click the **NETGEAR ProSafe VPN Client** icon>**Security Policy Editor**.

Basic Steps to Configure a Security Policy

Caution: Before attempting to configure the security policy, check with your network security administrator: your security policy may have been configured when the client was installed.

Table 5-1. Summary of steps

Step	Task
1	• Create one connection that secures all communications, with the option to direct all connections to a specific gateway or • Create multiple connections and specify which ones to secure
2	Select options that apply to all connections in the security policy
3	Identify yourself (the user) through one of these methods: Select the personal certificate Let the client automatically select the personal certificate during IKE negotiation Enter the specific preshared key
4	Select the Phase 1 mode: Main Mode (high security) Aggressive Mode (low security) Manual keys (for troubleshooting only)
5	Add proposals, if needed, and select these options: Encryption algorithm Hash algorithm SA life Key (Diffie-Hellman) group
6	Add proposals, if needed, and select the options for Encapsulated Security Payload (ESP) or Authentication header (AH)
7	Identify backup gateways on the network
8	For network administrators or installers only: Create and deploy a customized client installation package, with the security policy you configured, to users

How to Secure All Connections

You can create a single connection called All Connections in your security policy that secures all IP communications between your computer and every other party.

1. In the Security Policy Editor, click **Options>Secure>All Connections**. A secure connection 🔒 called **All Connections** is added to the **Network Security Policy** list.
2. To route all secure communications from your computer through a specific, secure, IPSec-compliant network gateway, such as a firewall or router, go to Configure a gateway.
3. Click Save.

4. Configure My Identity for this connection.
5. Exit the Security Policy Editor.

How to Configure Global Policy Settings

Global policy settings are program preferences that apply to all secure IP communications. You can change these at any time to match to your security policy.

1. In the Security Policy Editor, click **Options**, and then click **Global Policy Settings**. The **Global Policy Settings** dialog box opens.
2. In the **Retransmit Interval** box, type the length of time, in seconds, that the client waits before resending an IKE protocol packet that has not been responded to. The default is **8** seconds.

   Note: If the client selects a redundant gateway when you know that the primary one is available, try entering a higher number for **Retransmit Interval**.
3. In the **Number of retries** box, type the number of times your computer resends an IKE protocol packet before abandoning the exchange. The default is **3** tries.
4. Status notifications are messages that inform communicating parties what the time-out periods are and whether their security proposals have been accepted or rejected.

   To send these messages, select the **Send status notifications to peer host** check box.
5. An internal network IP address is a virtual IP address assigned to the client user. Remote users can appear as internal users on a private network to, for example, access a WINS server or browse the network.

   To enable remote users to appear as internal users on a private network, select the **Allow to Specify Internal Network Address** check box.

   Note: If you select this check box, you must enter a private internal network IP address when Configuring My Identity.
6. To enable logging the **Log Viewer's** IKE negotiation messages to the **isakmp.log** file in the client's installation directory, select the **Enable logging to a file** check box. This can facilitate remote troubleshooting by allowing a user to send a file with these messages instead of repeatedly freezing and printing the Log Viewer.

   Notes:

- The maximum size for the isakmp.log file is 100 KB. When the client computer, the client, and the IKE service restart and the isakmp.log file size exceeds 100 KB, this isakmp.log file is deleted and a new one created.
- On computers running Windows 95 and 98, when the isakmp.log file size exceeds 64 KB, Notepad prompts the user to try WordPad instead because of the file's size. When the user tries WordPad, however, WordPad prompts the user that it can't open the file because it is in use by another program (the IKE service).

  In this case, to view the file, try one of these options:

  – Rename it, and then open it in WordPad.

  – Open a read-only version of the file in Microsoft Word.

  – Clear the **Enable logging to a file** check box, and then open the file.

7. If you don't use a smart card and reader or similar device to authenticate your identity, skip this step.

   If you do use a smart card and reader or similar device, the client can, when it detects that the smart card or reader is removed, delete active keys and end these communications sessions. This provides extra security. Only connections that use the keys on your smart card are affected.

   To enable this feature, select the **Smart card removal clears keys** check box.

8. Click **OK**.
9. Click **Save**.

How to Configure Other Connections

The security policy includes a connection called Other Connections. This connection, non-secure by default, is designed to allow all non-encrypted IP traffic through and let you to access the Internet and other public networks unsecured.

The client processes connections in the order in which they display in the **Network Security Policy** list. Because Other Connections is the catchall or default rule for communications that don't conform to the proposals for individual connections, it is always last in the connections list.

1. In the Security Policy Editor, click **Options**, point to **Secure**, and then click **Specified Connections**.
2. In the **Network Security Policy** list, click **Other Connections**.

3. In the Connection Security group, click a security level:
   - **Secure** 🔒 secures communications for this connection.
   - **Non-secure** 🔓, the default, allows communications for this connection to pass through unsecured, or not encrypted.
   - **Block** STOP prohibits all communications for this connection from passing through.
4. If you selected **Non-secure** or **Block** in the Connection Security group, the Internet Interface group is available:
   a. In the **Name** list, click the interface for your computer to use to connect to a network. The default, **Any**, lets your computer select any available interface.

      For devices with associated IP addresses, the **IP Addr** box shows the IP address.

   b. In the **Port** box, click the protocol port through which your computer connects to the remote party. The default, **All**, secures all protocol ports.

      The port's standard numeric designation shows next to the **Port** box.
5. Click **Save**.
   a. If you selected **Secure** in the Connection Security group, is your network protected by a secure IPSec-compliant gateway, such as a firewall or router?
      - If it is, go to Configure a gateway.
      - If it is not, continue with the next step.

   b. The **Connection Security** setting determines your next step:
      - If you selected **Secure**, Configure My Identity for this connection.
      - If you selected **Non-secure** or **Block**, you can add and configure connections.

How to Add and Configure a Connection

You can create and configure multiple connections for your security policy.

Before you can configure a connection, make sure that you have identification information for the remote party, such as network IP address, domain name, or email address. If the remote party (user or network) is protected by a secure IPSec-compliant gateway device, obtain that gateway's IP address, too.

1. In the Security Policy Editor, Configure Other Connections.

2. In the **Network Security Policy** list, if the **My Connections** folder does not appear, click **Options**, point to **Secure**, and then click **Specified Connections**.
3. Click (or **Edit>Add Connection**). A highlighted **New Connection** entry displays in the **Network Security Policy** list.
4. Rename the new connection.
5. In the **Connection Security** group, take these steps:

   a. Click the security level:

   - **Secure** secures communications for this connection. This is the default.
   - **Non-secure** allows communications for this connection to pass through unsecured, or not encrypted.
   - **Block** prohibits all communications for this connection from passing through.

   b. When the **Secure** security level is selected, the **Only Connect Manually** check box appears. By default, the check box is clear; this means that the client establishes and terminates connections automatically as needed. You can, however, initiate and end secure sessions manually.

   To require the user to manually establish and terminate all secure sessions using this connection (with the **Connect** and **Disconnect** options on the client icon's shortcut menu), select the **Only Connect Manually** check box.

   If a connection for which the **Only Connect Manually** check box is selected isn't manually connected, traffic that would otherwise go over this connection is bypassed, as though there were no connection configured for this traffic. Traffic that would go over that connection if it were active is instead compared against the remaining connections in the **Network Security Policy** box to determine how to handle it.

6. In the **Remote Party Identity and Addressing** group, in the **ID Type** box at the top of the group, click an identifier for the other party. Boxes become available below the **ID Type** box to enter information about the ID type you selected:

Table 5-2: Remote Party Addressing

ID Type option	In boxes below ID Type box, type…
IP Address	IP address
Domain Name	domain name and IP address
Email Address	email address

IP Subnet	subnet address and mask
IP Address Range	first and last IP addresses for the range
Distinguished Name	IP address To edit a distinguished name, go to edit a distinguished name
Any (default)	IP address

To create a generic security policy for multiple users, select **Any**.

7. In the **Protocol** box, click the protocol for the remote party to use to connect with you. The default, **All**, secures all protocol ports. Selecting the exact protocol port tightens your security policy.

8. If you clicked **UDP** or **TCP** in the **Protocol** box, in the **Port** box, click a protocol port. The standard numeric designation for this port displays next to the **Port** box.

9. Your **Connection Security** selection determines your next step:

   - If you selected **Secure** and a secure IPSec-compliant gateway device, such as a firewall or router, protects the remote user or network, go to Configure a gateway.
   - If you selected **Secure** and the remote user or network is not protected by a secure IPSec-compliant gateway, make sure that the **Connect using** check box is clear.
   - If you selected **Non-secure** or **Block** , the **Internet Interface** group opens:

   a. In the **Name** box, click the interface for your computer to use to connect to a network. The default, **Any**, enables your computer to select any available interface. For devices with associated IP addresses, the read-only **IP Addr** box shows the IP address.

   b. In the **Port** box, click the protocol port for your computer to connect to the remote party through. The default, **All**, secures all protocol ports. The number displayed next to the **Port** box is the port's standard designation.

10. Click **Save**.

11. Configure My Identity for this connection.

How to Enter a Preshared Key

A preshared key is an alphanumeric character string that can be used instead of certificates to authenticate the identity of communicating parties during Phase 1 IKE negotiations. This character string, which can contain from 8 through 255 characters, is called preshared because the remote party needs it before you can communicate with it. Both parties must enter this preshared key in their IPSec-compliant devices, such as a firewall, gateway encryptor, router, or software client. Preshared keys can be included with the security policy when it is exported or included in a customized client installation.

When you use preshared keys, you don't have to deal with CAs and certificates. Preshared keys, however, do not provide the same level of security as certificates.

Before you begin to configure the security policy, decide whether to use certificates or preshared keys.

To use preshared keys instead of certificates for authentication, enter the preshared key when you Configure My Identity for a selected connection.

Note: Preshared keys are not global policy settings; therefore, you must assign the key to each applicable connection individually.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection 🔒.
2. In this connection, click **My Identity**.
3. In the **Select Certificate** box, click **None**.
4. Click **Pre-Shared Key**. The **Pre-shared Key** dialog box opens.
5. Click **Enter Key**.
6. Type the key.
7. Click **OK**.
8. Click **Save**.
9. Complete configuring **My Identity**.

How to Configure a Gateway

When configuring a secure connection—Other Connections, All Connections, or a Specific connection—in the Security Policy Editor, and your network or, for specific connections only, the remote party's network routes secure IP communications through a gateway device, such as a firewall or router, you must identify the gateway and its addressing.

1. In the Security Policy Editor, in the **Network Security Policy** list, click the particular secure connection 🔒.
2. In the right pane, select the **Connect using** check box. When configuring a specific connection, this is in the **Remote Party Identity and Addressing** group.
3. In the adjoining box, click the gateway to use.
4. In the **ID Type** box immediately below the **Connect using** check box, click an identifier for this gateway.

   Note: To create a generic security policy for multiple users, select **Any** (the default).
5. Complete the boxes that become available, based on the gateway identifier you specified in **ID Type:**
   - If you clicked **IP Address**, you can edit the gateway's IP address in a box below the **ID Type** box.
   - If you clicked **Domain Name:**

     a. You can edit the gateway's IP address in a box below the **ID Type** box.

     b. In the box adjacent to the **ID Type** box, select how to specify the gateway: click **Gateway IP Address** or **Gateway Hostname** (DNS name).

     c. In the box below the **Gateway IP Address/Hostname** box, type the value for the selected gateway option.
   - If you clicked **Distinguished Name** or **Any:**

     a. In the box adjacent to the **ID Type** box, select how to specify the gateway: click **Gateway IP Address** or **Gateway Hostname** (DNS name).

     b. In the box below the **Gateway IP Address/Hostname** box, type the value for the selected gateway option.

     To change the distinguished name, go to Edit a distinguished name.
6. Click **Save**.

Configure My Identity

The remote party that you want to communicate securely with uses the information in My Identity to verify that you really are who you indicate that you are. This is done with either a preshared key that you and the remote party have or a certificate. This information also distinguishes you from the remote party during the key exchange process.

The ID types available for identifying yourself in My Identity come from the subject information fields of the personal certificate request that you completed when you requested a personal certificate from a CA.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection.
2. Click **My Identity**.
3. If you are using preshared keys, go to Enter a preshared key.
4. If you are using certificates:
   a. In the **Select Certificate** box, you can specify a personal certificate or let the client select one:
      – To select a particular personal certificate, click that certificate.
      – For the client to select a personal certificate automatically, click **Select automatically during IKE negotiation**, the default for new security policies. This option facilitates creating a policy.

   b. In the **ID Type** box, click the information and format that identifies you to remote parties.

      A box opens below the **ID Type** box with the particular subject information, in the ID type you clicked, from the personal certificate that you selected in the **Select Certificate** box.

      If you selected **Select automatically during IKE negotiation** in the **Select Certificate** box, the default ID type is **Distinguished Name**; each personal certificate contains this.

      Caution: The ID type is a search criterion that the client uses when automatically selecting a certificate. This means that if it doesn't find a personal certificate with the ID type selected, the connection attempt fails.
5. If the **Port** box is enabled, click the protocol port through which your computer will connect to the other party. The default, **All**, secures all protocol ports. Selecting the exact protocol port tightens your security policy.

   The port's standard numeric designation shows next to the **Port** box.

6. In the **Virtual Adapter** box, you can configure the client to use a virtual adapter to handle private IP addressing. If certain programs that work with the client are “IP address-aware,” your computer is assigned a private Windows Internet Naming Service (WINS) server address, or both, you may need to do this.

   In the **Virtual Adapter** box, click an option:

   - **Disabled**—No virtual adapter is used. This is the default.
   - **Required**—When the client tries to launch the connection with the virtual adapter, IP address-aware programs know the assigned address for the virtual adapter and use it as the source IP address. If the launch fails, the connection attempt fails.
   - **Preferred**—Uses the same procedure as **Required** with one exception: if the connection launch using the virtual adapter IP address fails, the client uses address substitution to dynamically change the server IP address throughout the session.

7. If you selected the **Allow to Specify Internal Network Address** check box when you Configured Global Policy Settings, and the **Internal Network IP Address** box opens, type an IP address in it.

8. In the **Internet Interface** group, in the **Name** box, click the interface for your computer to use to connect to a network. The default, **Any**, enables your computer to select any available interface.

   For devices with associated IP addresses, the **IP Addr** box shows the IP address.

   Caution: If the **Name** box contains an entry other than **Any**, do **not** change it. This was configured by your network security administrator. The only instance in which you may need to change this entry is to assist your network security administrator in troubleshooting connection problems.

9. Click **Save**.

Configure Security Policy Connection Options

Before you configure the options for Security Policy in a connection, take these steps:

- Make sure that the connection is secure: In the Connection Security group, click **Secure** 🔒.
- Configure My Identity for this connection.

The Phase 1 negotiation mode selected for Security Policy determines how the security association (SA) is established for each connection through IKE negotiations.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection 🔒.
2. Expand **Security Policy**.
3. In the Select Phase 1 Negotiation Mode group, click an option:
   - **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (Phase 1).
   - **Aggressive Mode** is quicker than Main Mode, because it eliminates several steps when the communicating parties are negotiating authentication (Phase 1).
   - **Use Manual Keys** requires no negotiations; SafeNet recommends using this for troubleshooting only.
4. To activate the perfect forward secrecy (PFS) feature, which requires exchanging independent keying material each time Key Exchange keys are generated, select the **Enable Perfect Forward Secrecy (PFS)** check box.
5. If you selected the **Enable Perfect Forward Secrecy (PFS)** check box, in the **PFS Key Group** list, click a **Diffie-Hellman Group 1**, **2**, or **5**.
6. To set a counter that determines if a packet is unique, select the **Enable Replay Detection** check box.
7. Click **Save**.

The **Phase 1 Negotiation Mode** you selected determines your next step:

- If you selected **Main Mode** or **Aggressive Mode**, configure Authentication (Phase 1).
- If you selected **Use Manual Keys**, configure Key Exchange (Phase 2).

Configure Authentication (Phase 1)

After you configure Security Policy for a secure connection, the next step is to configure authentication proposals for this policy, one connection at a time.

Note: If you are using manual keys, skip this topic, and go to Configure Key Exchange (Phase 2).

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection .
2. For the selected connection, expand **Security Policy**. **Authentication (Phase 1)** and **Key Exchange (Phase 2)** appear.
3. Expand **Authentication (Phase 1)**.
4. Your next step depends on whether you are configuring the first proposal or a subsequent one:
   - For the first proposal, click **Proposal 1**.
   - For subsequent proposals, create a new one from scratch or copy an existing one as a base:
     - To create one from scratch, click **Create New Proposal**.
     - To copy an existing proposal, click the source proposal, and then click **Copy**.
5. In the **Authentication Method and Algorithms** group, select these options for this proposal:
   a. In the **Authentication Method** box, accept the default option, based on how you configured My Identity:
      - If you entered a preshared key, **Pre-Shared Key**
      - If you selected a certificate, **RSA Signatures**

      If your gateway is configured for Extended Authentication (XAUTH), you can select an XAUTH version of the default option.

   b. In the **Encryption Algorithm** box, click an option:
      - For minimal security, **DES**
      - For medium security, **Triple-DES** (the default)
      - For maximum security, **AES-128**, **AES-192**, or **AES-256**

   c. In the **Hash Algorithm** box, click an option:
      - For minimal security, **MD5**
      - For maximum security, **SHA-1** (the default)

d. In the **SA Life** box, click an option. **Unspecified** is the default.

e. If you clicked **Seconds** for **SA Life**, in the adjacent box, type the number of seconds.

f. In the **Key Group** box, click **Diffie-Hellman Group 1**, **Group 2** (the default), or **Group 5**.

6. Click **Save**.

7. Configure Key Exchange (Phase 2).

Configure Key Exchange (Phase 2)

After you add and configure the authentication proposals for Security Policy, the next step is to add and configure the key exchange proposals for that policy, one connection at a time.

1. Configure Authentication (Phase 1).
2. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection 🔒.
3. For the selected connection, expand **Security Policy**. **Authentication (Phase 1)** and **Key Exchange (Phase 2)** appear.
4. Expand **Key Exchange (Phase 2)**. Proposals appear.
5. Your next step depends on whether you are configuring the first proposal or a subsequent one:
   - For the first proposal, click **Proposal 1**.
   - For a subsequent proposal, you can start from scratch or copy an existing one as a base:
     – To start from scratch, click **Create New Proposal**.

     – To copy an existing proposal, click the source proposal, and then click **Copy**.
6. In the **IPSec Protocols** group, configure these options:

   a. In the **SA Life** box, click the measurement unit. Your selection opens various boxes for you to enter additional information.

   Note: If you click **Unspecified**, no boxes are enabled; skip step “b”.

   b. In the enabled boxes, type a value.

   c. In the **Compression** box, click **Deflate**; this value increases the transmission speed.
7. **Encapsulation Protocol (ESP)** and **Authentication Protocol (AH)** are mutually exclusive check boxes. Select the one that meets your requirements:

- To encrypt and authenticate the data, select the **Encapsulation Protocol (ESP)** check box.

a. In the **Encryption Algorithm** box, click an option:

   – For minimal security, **DES**

   – For medium security, **Triple-DES** (the default)

   – For maximum security, **AES-128**, **AES-192**, or **AES-256**

   – For no security, **Null**

b. In the **Hash Algorithm** box, click an option:

   – For minimal security, **MD5**

   – For maximum security, **SHA-1** (the default)

   – DES-MAC

c. In the **Encapsulation** box, accept **Tunnel** (the default) or click **Transport**.

   Note: If you selected the **Connect using** check box and a gateway when you configured All Connections or a specific connection to be secured, **Tunnel** is the only option.

- To ensure that the data has not been altered, select the **Authentication Protocol (AH)** check box.

a. In the **Hash Algorithm** box, click an option:

   – For minimal security, **MD5**

   – For maximum security, **SHA-1** (the default)

b. In the **Encapsulation** box, accept **Tunnel** (the default) or click **Transport**.

   Note: If you selected the **Connect using** check box and a gateway when you configured All Connections or a specific connection to be secured, **Tunnel** is the only option.

8. If, when you configured Security Policy, you selected **Use Manual Keys** in the **Select Phase 1 Negotiation Mode** group, the **Inbound Keys** and **Outbound Keys** buttons are enabled. Go to Enter manual keys.

9. Click **Save**.

Edit a Distinguished Name

When you identify yourself (your computer) or a remote party in a connection, and you select the distinguished name identifier as the ID type, the client typically retrieves your distinguished name information from your personal certificate.

The distinguished name that the remote party identifies itself with must match the distinguished name entered in the Remote Party Identity and Addressing group. Enter the distinguished name exactly as it displays in the remote party's security policy, matching spelling, case, punctuation, and spaces.

1. In the Security Policy Editor, when performing one of these tasks, click **Edit Name:**
   - Configuring a gateway
   - Adding a redundant gateway
   - Adding and configuring a connection
   - Configuring Other Connections

   The **Edit Distinguished Name** dialog box opens.
2. You can enter subject information in LDAP—with distinguished names (DNs) and their relative distinguished name (RDN) components—or non-LDAP (the default) format.

   Warning! Do **not** mix LDAP and non-LDAP format. This information may not translate between the two. Your entry in one format may not display if you select the other format.

   - To use the non-LDAP format, take these steps:

   a. Make sure that the **Enter Name in LDAP Format** check box is clear.

   b. Enter the relevant personal information.

   - To use the LDAP format, take these steps:

   a. Select the **Enter Name in LDAP Format** check box. The box labels change to RDNs.

b. In the **Subject Name in LDAP Format** box, enter the relevant personal information, from specific to general. Preface each type of information with the correct RDN component, and an equals sign (=):

RDN	Information	Example
CN	First and last name	CN=Kerry Smith

OU	Department; there can be multiple OUs	OU=HR
		OU=New York office

O	Company	O=ispname Company
S	State (two-letter abbreviation)	S=MD
C	Country	C=US
postalCode	ZIP or postal code	postalCode=21210
E	Email address	E=ksmith@ispname.com

c. To start a new line to enter another RDN component—for example, to add the **O** after an **OU** on a new line—place the cursor in this box, and then press **<Enter>**.

3. Click **Save**.

Configure and Manage Connections

You can create and configure multiple connections for your security policy.

Before you can configure a connection, make sure that you have identification information for the remote party, such as network IP address, domain name, or email address. If the remote party (user or network) is protected by a secure IPSec-compliant gateway device, obtain that gateway's IP address, too.

Add and Configure a Connection

1. In the Security Policy Editor, configure Other Connections.
2. In the **Network Security Policy** list, if the **My Connections** folder does not appear, click **Options**, point to **Secure**, and then click **Specified Connections**.

3. Click (or **Edit>Add Connection**). A highlighted **New Connection** entry displays in the **Network Security Policy** list.
4. Rename the new connection.
5. In the **Connection Security** group, take these steps:
   a. Click the security level:
      - **Secure** secures communications for this connection. This is the default.
      - **Non-secure** allows communications for this connection to pass through unsecured, or not encrypted.
      - **Block** prohibits all communications for this connection from passing through.

   b. When the **Secure** security level is selected, the **Only Connect Manually** check box appears. By default, the check box is clear; this means that the client establishes and terminates connections automatically as needed. You can, however, Initiate and end secure sessions manually.

      To require the user to manually establish and terminate all secure sessions using this connection (with the **Connect** and **Disconnect** options on the client icon's shortcut menu), select the **Only Connect Manually** check box.

      If a connection for which the **Only Connect Manually** check box is selected isn't manually connected, traffic that would otherwise go over this connection is bypassed, as though there were no connection configured for this traffic. Traffic that would go over that connection if it were active is instead compared against the remaining connections in the **Network Security Policy** box to determine how to handle it.

6. In the **Remote Party Identity and Addressing** group, in the **ID Type** box at the top of the group, click an identifier for the other party. Boxes become available below the **ID Type** box to enter information about the ID type you selected:

ID Type option	**In boxes below ID Type box, type…**
IP Address	IP address
Domain Name	domain name and IP address
Email Address	email address
IP Subnet	subnet address and mask
IP Address Range	first and last IP addresses for the range
Distinguished Name	IP address To edit a distinguished name, go to Edit a distinguished name
Any (default)	IP address

   To create a generic security policy for multiple users, select **Any**.

7. In the **Protocol** box, click the protocol for the remote party to use to connect with you. The default, **All**, secures all protocol ports. Selecting the exact protocol port tightens your security policy.

8. If you clicked **UDP** or **TCP** in the **Protocol** box, in the **Port** box, click a protocol port. The standard numeric designation for this port displays next to the **Port** box.

9. Your **Connection Security** selection determines your next step:
   - If you selected **Secure** 🔒 and a secure IPSec-compliant gateway device, such as a firewall or router, protects the remote user or network, go to Configure a gateway.
   - If you selected **Secure** 🔒 and the remote user or network is not protected by a secure IPSec-compliant gateway, make sure that the **Connect using** check box is clear.
   - If you selected **Non-secure** 🔓 or **Block** STOP, the **Internet Interface** group opens:

   a. In the **Name** box, click the interface for your computer to use to connect to a network. The default, **Any**, enables your computer to select any available interface.

      For devices with associated IP addresses, the read-only **IP Addr** box shows the IP address.

   b. In the **Port** box, click the protocol port for your computer to connect to the remote party through. The default, **All**, secures all protocol ports. The number displayed next to the **Port** box is the port's standard designation.

10. Click **Save**.
11. Configure My Identity for this connection.

Copy a Connection

1. In the Security Policy Editor, in the **Network Security Policy** list, click the connection to copy.
2. Click 📋. A new connection named **Copy of connection name** displays in the **Network Security Policy** list.
3. Rename the copied connection.
4. Press **<Enter>**.
5. Click **Save**.

Move a Connection

The client attempts connections and their proposals in the sequence they appear in the Network Security Policy list in the Security Policy Editor. To change this selection order, you can move a connection up or down in this list.

Note: Other Connections is always the last connection attempted; its place at the bottom of the Network Security Policy list is fixed.

1. In the Security Policy Editor, in the **Network Security Policy** list, click the connection to move.
2. Click ↑ to move the connection up or ↓ to move it down.
3. Click **Save**.

Rename a Connection

1. In the Security Policy Editor, in the **Network Security Policy** list, right-click the connection to rename, and then click **Rename**.
2. Type a new name, with a maximum of 80 alphanumeric characters, for this connection.

3. Press **<Enter>**.
4. Click **Save**.

Delete a Connection

1. In the Security Policy Editor, in the **Network Security Policy** list, click the connection to delete.
2. Click ✕.
3. When a confirmation message opens, click **Yes**.
4. Click **Save**.

Manage Proposals

When you add a connection and configure its Security Policy, the Security Policy Editor provides one proposal (Proposal 1) for Authentication (Phase 1) and Key Exchange (Phase 2). If you need additional proposals, copy one or add one.

Add a Proposal

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection 🔒.
2. Expand **Security Policy** for the secure connection. **Authentication (Phase 1)** and **Key Exchange (Phase 2)** appear.
3. Click the type of proposal to add:
   - Authentication (Phase 1)
   - Key Exchange (Phase 2)
4. Click **Create New Proposal**.
5. Click **Save**.

Copy a Proposal

You can copy proposals for Authentication (Phase 1) or Key Exchange (Phase 2) in the selected connection only. You cannot copy proposals to another phase or connection.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection 🔒.
2. Expand **Security Policy** for the secure connection. **Authentication (Phase 1)** and **Key Exchange (Phase 2)** appear.
3. Depending on the type of proposal you want to copy, click a proposal for **Authentication (Phase 1)** or **Key Exchange (Phase 2)** that you want to copy.
4. Click 📋. The new proposal appears below the copied proposal; its number is the copied proposal incremented by one. Each proposal's number below the new one is incremented by one from before the copy operation. Proposal labels are fixed; you can't change them.

   Example:
   There are four proposals for a connection. You copied Proposal 2; the new proposal is Proposal 3. Proposals 3 and 4 are now Proposals 4 and 5.
5. Click **Save**.

Move a Proposal

The client attempts proposals in the order they are listed, in the particular phase for a connection, in the Network Security Policy list. To change the selection order, you can move a proposal up or down.

When you change a proposal's position in the list, the client renumbers the proposals to maintain sequential numbering. When you have finished moving proposals, make sure that the proposals are in the order you want them tried.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection 🔒.
2. For this secure connection, expand **Security Policy**.
3. Depending on the location of the proposal to move, expand **Authentication (Phase 1)** or **Key Exchange (Phase 2)**.
4. Click the proposal to move.
5. Click ⬆ to move the proposal up or ⬇ to move it down.

6. Repeat steps 4 and 5 as necessary.
7. Click **Save**.

Delete a Proposal

In the Network Security Policy list in the Security Policy Editor, there must be at least one proposal each for Authentication (Phase 1) and Key Exchange (Phase 2).

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection 🔒.
2. Expand **Security Policy** for the secure connection. **Authentication (Phase 1)** and **Key Exchange (Phase 2)** display.
3. Depending on the location of the proposal you want to delete, expand **Authentication (Phase 1)** or **Key Exchange (Phase 2)**. The proposals for the phase display.
4. Click the proposal to delete.
5. Click ☒.
6. When a confirmation message box opens, click **Yes**.
7. Click **Save**.

Manage Redundant Gateways

A redundant gateway is an alternate network access gateway to establish a connection with the client when the primary gateway is busy, offline, or otherwise not available.

Before you can add redundant gateways for a secure connection, you must configure the primary gateway in the Security Policy Editor.

In most cases, use the same security policy information to configure all redundant gateways for a single connection. However, these exceptions must be unique to each device:

- Distinguished name
- IP address
- Preshared key

Each secure connection can have a maximum of 10 redundant gateways, plus the primary. The original secure connection is always the primary gateway.

The client selects the alternates in the sequence in which they are listed for the particular connection in the Network Security Policy list. The client “rolls over” to a redundant gateway only when the primary gateway does not respond. If the client receives a response from the primary gateway, it continues trying to establish a connection.

When the security association (SA) times out, the client tries to connect with the primary gateway. If the primary gateway is busy, it returns to the last active redundant gateway.

Add a Redundant Gateway

1. In the Security Policy Editor, in the **Network Security Policy** list, click the specific secure connection that has a gateway configured—that is, the **Connect using** check box and a gateway are selected.
2. On the toolbar, click **Edit**, point to **Add**, and then click **Redundant Gateway**. The **New Name for RGW X** dialog box, where X is a sequence number from 1 through 10, opens.
3. Type a name for this redundant gateway, and then click **OK**. The new gateway displays below **Security Policy** for this connection in the **Network Security Policy** list.
4. In the **Redundant Gateway Identity and Addressing** group, in the **ID Type** box, click an identifier for this gateway. Boxes become available, based on the identifier you select.

   Note: To create a generic security policy for multiple users, for **ID Type**, click **Any**.
5. Complete the gateway identity-related boxes; for details, go to Configure a gateway.
6. Your next step depends on how My Identity is configured for this connection:
   - If you selected a certificate—in the My Identity group, for **Select Certificate**, a certificate name appears—go to the next step.
   - If you entered a preshared key—in the My Identity group, for **Select Certificate**, **None** appears—take these steps:

   a. Click **Pre-Shared Key**. The **Pre-shared Key** dialog box opens.

   b. Click **Enter Key**.

   c. Enter the key that matches the preshared key in the gateway's configuration.

   d. Click **OK**.
7. Click **Save**.

Copy a Redundant Gateway

A quick way to add redundant gateways to a connection is to copy another redundant gateway in the same connection. You can copy redundant gateway within a connection only, not between connections.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection .
2. Right-click a redundant gateway , and then click **Copy**. The **New Name for RGW X** dialog box, where X is the sequence number, 1 through 10, opens.
3. Type a name for this new connection.
4. Click **OK**.
5. Click **Save**.

Move a Redundant Gateway

When the primary gateway is not available, the client tries redundant gateways in the order in which they appear for a connection in the Network Security Policy list. You can change the selection order by moving a gateway up or down in a connection's list. Redundant gateways can be moved only in their connection.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection .
2. Select a redundant gateway .
3. Click ⬆ to move the gateway up or ⬇ to it down.
4. Repeat steps 2 and 3 as necessary.
5. Click **Save**.

Rename a Redundant Gateway

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection .
2. Right-click a redundant gateway , and then click **Rename**. The **New Name for RGW X** dialog box opens, where X is the sequence number 1 through 10.
3. Type the new name.

4. Click **OK**.
5. Click **Save**.

Delete a Redundant Gateway

1. In the Security Policy Editor, in the **Network Security Policy** list, expand a secure connection 🔒.
2. Click the redundant gateway 🖧 to delete.
3. Click ✕.
4. When a confirmation dialog box opens, click **Yes**.
5. Click **Save**.

Disable Redundant Gateways

You can disable all redundant gateways for a selected secure connection without deleting them. You can also enable them again later.

1. In the Security Policy Editor, in the **Network Security Policy** list, select the specific secure connection 🔒.
2. In the Remote Party Addressing and Identity group, clear the **Connect using** check box.
3. Click **Save**.

Manage the Security Policy

When you export a security policy, the client creates an **.spd** file that contains all the connections, proposals, global policy settings, and My Identity information from the security policy. You can include this security policy file in a customized client installation; make it available to users on a Web site, CD-ROM, or other location or medium; or save it as a backup of your security policy.

1. In the Security Policy Editor, click **File>Export Security Policy**. The **Export Policy To** dialog box opens.
2. In the **Save As** dialog box, navigate to the directory to save this file to and enter the filename. The default location and name is **C:\policy.spd**.

   Note: If you are creating a customized installation, rename this file IPSecPolicy.spd.

3. To password-protect this policy file during the export/import process only, take these steps:
   a. Select the **Protect Exported Policy** check box.
   b. In the **Password** box, enter a password that contains at least eight alphanumeric characters.
   c. In the **Confirm** box, retype the password.
4. To limit or prevent users who Import this policy or install it from changing it, lock it when you export it:
   - To allow users to edit the entire security policy, accept the default, **Policy is unlocked**.
   - To allow users to change only their My Identity settings, click **Policy is partially locked**.
   - To prohibit users from changing anything in the security policy, but let them view it, click **Policy is completely locked**.
5. Click **OK**.
6. Click **Save**.

Edit a Security Policy

After you add and configure connections for a security policy, you can change the options.

1. In the Security Policy Editor, in the **Network Security Policy** list, click a connection; expand secure connections to open the components of the policy to edit.
2. In the right pane, change the particular settings. For details, refer to the help topic on configuring the specific entity you're editing.
3. Click **Save**.

   Note: If secure connections are active, the client prompts you to reset active connections:
   - To reset active connections, which drops and disconnects all active connections and applies the new policy immediately, click **Yes**.
   - To store the changes, but delay saving them until the active connections end, click **No**. Then, when you're ready to put the new policy into effect, reload the security policy.

     Note: If you don't explicitly reload the policy, it goes into effect the next time you log on to Windows or restart your computer.

Import a Security Policy

Caution: When you import a security policy, it overwrites the existing policy on your computer.

1. Obtain the name and location of the policy file to import (an **.spd** file).
2. In the Security Policy Editor, click **File>Import Security Policy**. The **Import Policy From** dialog box opens.
3. Navigate to the **.spd** file to import; when its file name displays in the **File name** box, click **Open**.
4. A policy file can be password-protected and encrypted when it is exported from the client. To import it, you must enter the password used when the policy file was exported.

   If the **Policy Protection Password** dialog box opens, this policy file is password-protected. Unless you enter the password, you can't import the file and policy.

   a. Obtain the password.

   b. In the **Password** box, type the password.

   c. Click **OK**. The **Policy Import** dialog box opens.

   - If the **New policy resets existing connections** check box on the **Policy Management** dialog box in **Security Policy Editor** is selected, the **Reset existing connections** check box on the **Policy Import** dialog box is also selected. This means that the client will reset, or drop, all active connections.
     - If the **New policy resets existing connections** check box on the **Policy Management** dialog box is clear, the **Reset existing connections** check box is also clear.
     - Based on your preference, select or clear the **Reset existing connections** check box; this does not change the **New policy resets existing connections** check box on the **Policy Management** dialog box.
   - When an import confirmation message box opens, click **OK**.

   Note: After the policy is imported, it is no longer encrypted.

Reload the Security Policy

Importing a security policy or editing the existing one makes a new policy available to replace the current one. If you do not reset existing connections, which the client prompts you to do, the new policy does not go into effect (and active connections are not dropped).

When the client doesn't appear to be working properly, try performing this task. It disconnects all connections and loads the current security policy from scratch.

When you're ready to put the new policy into service, which will overwrite the current policy and drop (terminate) any existing connections, take this step:

> Right-click the **client icon**, and then click **Reload Security Policy** or, if there are any active secure communications sessions, **Disconnect All**. All sessions end, and either the current security policy or a new security policy is loaded.

Note: If you don't explicitly reload the policy or reset existing connections, the edited policy or imported policy takes effect the next time you log on to Windows or restart your computer.

Deactivate the Security Policy

To allow all communications to transmit unsecured or not encrypted, you can override or deactivate your security policy. The client continues to run in the background, but secures no communications.

When you deactivate your security policy, you can't communicate with other parties on secure connections unless they also disable their security policy.

You can deactivate the security policy in one of two ways:

- In the Security Policy Editor, take these steps:
    a. Click **Options>Secure>None**. The **Network Security Policy** list and the connections are read-only, but are not deleted.
    b. Click **Save**.
    c. Exit the Security Policy Editor.
- In the Windows system tray, right-click the **icon**, and then click **Deactivate Security Policy**.

In both cases, in a few seconds, the client icon's **Deactivate Security Policy** menu option becomes **Activate Security Policy**, and the icon changes to .

Reactivate the Security Policy

Right-click the **client icon** , and then click **Activate Security Policy**; this option changes to **Deactivate Security Policy**, and the icon changes to .

Configure the Client to Retrieve a New Policy from a Policy Server or Web Address

The client can be configured to periodically check for and then retrieve a new security policy from a Web address, or uniform resource locator (URL). Or, if the client is managed by a policy management application, the client registers with its policy server, and then polls this policy server to look for and retrieve new security policies.

If your client isn't preconfigured with the policy distribution URL or policy server details, your network security administrator must provide these to you.

1. In the Security Policy Editor, click **Options>Policy Management**. The **Policy Management** dialog box opens.
2. Select the **Use Policy Server** check box.
3. By default, the **New policy resets existing connections** check box is clear. This means that the client does **not** drop all connections when it retrieves a new policy.

   For the client to drop all connections when it retrieves this policy, select this check box.
4. In the **Policy Polling Interval (minutes)** box, specify how often the client checks for and retrieves a new policy from the Web address in the **Policy URL** box; type the number of minutes, from **1** through **9999999**, between these checks. The default is **1440** minutes (24 hours).
5. In the Policy Distribution Point group, select where to check for new policies:
   - If it's a policy management application's policy server, take these steps:

   a. Click **Register and retrieve my policy from a VPN Policy Manager**.

   b. In the **Server Name** box, type the policy server’s machine name or IP address.

   c. In the **Server Port** box, type the server’s assigned port number. The default is **389**.

   d. In the **Policy Subtree** box, type the location, typically the organization unit (OU) and organization (O) on the policy server, where security polices are stored. The default is **ou=VPN Client, o=SafeNet**.

   e. The client can register with the policy server with certificates or some other way.

   To register without certificates, in **Perform policy server registration**, accept the default, **without**. Otherwise, click **with**.

   - If it's an URL, take these steps:

   a. **Retrieve my policy from the following URL** (the default).

   b. In the **Policy URL** box, type the Web address, starting with **http://**, to poll.

6. Click **OK**.
7. Click **Save**.

When the client finds and retrieves a new policy for you, a confirmation message box opens.

Register with a Policy Management Application

Perform this task only if your network security administrator instructs you to do so.

The client can be managed by enterprise VPN policy management applications. These products typically serve as the initial and ongoing distribution point (policy server) for the client's security policies.

For the client to check for and retrieve a new security policy from a policy management product's policy server, the location and polling frequency of the LDAP policy server and that there is a policy server must be configured on the Security Policy Editor's Policy Management dialog box.

Obtain the specifics from your network security administrator; your entries must exactly match those expected by the policy management product's LDAP server. Your client may be preconfigured with this information.

Then, if the policy management application requires this step, the client must enroll or register with the management product. This registration may occur automatically when the CA is SCEP-compliant and the client submits a personal certificate request.

1. In the Security Policy Editor, click **File>Register Client**. The **VPN Policy Server Registration** dialog box opens.
2. In the **Name** box (the only one that you must complete), type your name (**CN** is the RDN).
3. In the **Department** box, type your department's name (**OU** is the RDN).
4. In the **Organization** box, type your company's name (**O** is the RDN).
5. In the **State** box, type your company's name (**S** is the RDN).
6. Click **OK**.
7. When a registration confirmation message box opens, click **OK**.

Retrieve a New Policy Manually

When the client is configured to automatically check for and retrieve new security policies from a policy management product or a policy server on a Web site, you can manually check this source for a new or updated policy.

- In the Security Policy Editor, click **File>Retrieve Policy**.

  The client checks the Web address or LDAP server configured on the **Policy Management** dialog box.

  A message box opens confirming the success or failure of the retrieval attempt.

Chapter 6
Using the Certificate Manager

This chapter describes how to configure the advanced features of your NETGEAR ProSafe VPN Client.

What is the Certificate Manager?

The Certificate Manager is the client module where you obtain and manage the certificates you receive from certificate authorities (CAs), set the trust policy, and view certificate revocation lists (CRLs).To learn how to perform all the various certificate-related tasks, refer to the topics in the Certificate Manager book in the help.

The Certificate Manager includes these tabs for you to perform the tasks listed above:

- My Certificates
- Root CA Certificates
- Trust Policy
- CA Certificates
- RA Certificates
- CRLs
- Requests

There are three ways to open the Certificate Manager:

- On the Windows desktop, click **Start>Programs>NETGEAR ProSafe VPN Client**>**Certificate Manager**.
- Right-click the **client icon**, and then click **Certificate Manager**.
- In the Security Policy Editor, click **Options>Certificate Manager**.

Getting Started with the Certificate Manager

If you are using preshared keys for authentication in your VPN, or secure connection, to the other party, you don't have to open the Certificate Manager; skip all the topics in the Certificate Manager book in the help.

If you are using certificates for authentication with the remote party to your VPN, and don't already have a CA and personal certificate, you need to obtain these. However, depending on your network and installed applications and hardware at any particular site, specific tasks may not apply; additional tasks may be required. For details on the tasks to perform, contact your network security administrator.

These are the typical tasks to perform to obtain and manage certificates:

1. Select a CA.
2. Determine its enrollment method; go to CD enrollment methods and procedures.
3. Obtain a CA and personal certificate. There are three methods for doing this:
    - Online enrollment
    - File-based enrollment
    - Through Internet Explorer

    The help contains topics on these methods; go to the **Obtain certificates** book in the **Certificate Manager** book.
4. Manage the various certificates obtained. In the help, go to the **Manage certificates** book in the **Certificate Manager** book.
5. Work with certificate revocation lists (CRLs).
6. Set the trust policy.

What are Certificates?

To set up a VPN, or secure connection, between the client installed on your computer and a remote party, both parties must identify themselves, and then verify that each is really who it indicates it is. One way to do this is with a preshared key that both parties know in advance.

A more secure way to identify the two parties is through certificates. A certificate is an electronic document that contains a public key and is digitally signed by the third-party entity that issued it, called a certificate authority (CA) or certification authority. Because it validates the identities of the two VPN parties, it must be trusted. set the trust policy in the Certificate Manager.

There are two types of CA certificates:

- A root CA certificate is signed by and issued to itself—that is, the issuer and subject are the same.
- A subordinate or intermediate CA certificate is issued by a CA other than itself. A subordinate certificate can be issued by a root CA or another subordinate CA.

Also required for the client user is a personal certificate, which contains information about the user (client) that uniquely identifies it. This is requested by the client, and issued by a subordinate CA.

CAs that support SCEP may also employ a registration authority (RA), which is a network authority that collects and verifies certificate request information for the CA, and then signs responses on behalf of the CA. The CA, however, actually issues the certificates. These CAs may include RA certificates with CA certificates.

CA Enrollment Methods and Procedures

To communicate securely with certificates, you need three certificates issued by a CA:

1. Root CA certificate
2. Subordinate CA certificate

   Note: CAs that support Simple Certificate Enrollment Protocol (SCEP) may employ a registration authority (RA). The CA may include one or more RA certificates with the CA certificate.
3. Personal certificate (and keys)

To obtain certificates, you must enroll with a CA. There are two ways to enroll through the client:

- **Online enrollment**, which uses SCEP. SafeNet recommends this method.
  a. Obtain the CA's certificate server DNS name or IP address to make this request. Follow the instructions for the particular CA.

     You can also obtain personal and CA certificates for IPSec through Microsoft Internet Explorer or an email program.

     Note: To access the Microsoft CSP, Internet Explorer 5.01 or later must be installed on your computer.

  b. Retrieve a CA certificate online.

  c. Request a personal certificate online.

d. Retrieve the personal certificate.

- **Manual (file-based) enrollment**, which requires cutting and pasting text from a text editor. CAs handle this method in various ways; all start with a certificate request file. Follow the instructions provided by the CA.

  These are the typical steps:

  a. Obtain a CA certificate manually.

  b. Import a CA certificate.

  c. Create a certificate request file for a personal certificate.

     The Certificate Manager automatically generates the public/private key pair you need. The public key goes with your request; the private key resides on the hard drive of your computer.

  d. Prepare the personal certificate file to import.

  e. Import the personal certificate file.

Obtain Certificates

With Online (SCEP) Enrollment

CAs that Support SCEP

Simple Certificate Enrollment Protocol (SCEP) allows clients and servers certificates to obtain certificates from CAs online. The listed CAs support SCEP.

Table 6-1.

Certificate Authority	Telephone	Web site
Entrust Technologies, Inc	(972) 943-7300	www.entrust.com
iPlanet	(888) 786-8111	www.iplanet.com
Microsoft Corporation	(425) 882-8080	www.microsoft.com
RSA Security (Keon)	(877) 772-4900	www.rsasecurity.com
VeriSign, Inc.	(650) 961-7500	www.verisign.com

Retrieve a CA Certificate Online

Before you can request a personal certificate online, you must retrieve a CA certificate—root or subordinate—online. For a list of the CAs that offer online retrieval, go to CAs that support SCEP.

When you retrieve a CA certificate online, the CA may also include registration authority (RA) certificates, which you can view or verify in the Certificate Manager.

Note: If you access the Internet through a firewall, make sure that the Use HTTP proxy server for online certificate requests and CRL updates check box check box is selected on the Certificate Settings dialog box in the Security Policy Editor.

1. In the Certificate Manager, click the tab for the CA certificate type to retrieve:
   - For a root CA certificate, **Root CA Certificates**
   - For a subordinate CA certificate, **CA Certificates**
2. Click **Retrieve CA Certificate**. The **Retrieve CA Certificate Online** dialog box opens.
3. In the **CA Domain** box, type the CA's domain name, such as **abc123.com**.
4. In the **Online Certificate Server** box, type the complete URL, including the schema, such as **http://**, of the CA's certificate server.
5. Unless your network security administrator instructs you otherwise, leave the **Place certificate in local machine store** check box selected (the default). This adds the certificate to the store for all users who log on to this computer (local machine).

   Caution! In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store.

6. Click **OK**. In a few seconds, the **Root** or **CA Certificate Store** dialog box opens and prompts you to add the CA certificate to the client's root or CA store, according to the type of CA certificate you retrieved.
7. Click **Yes**. The certificate displays on the appropriate tab, **Root CA Certificates** or **CA Certificates**, in the Certificate Manager. If the retrieved CA certificate included RA certificates, these display on the **RA Certificates** tab.

Configure a CA Certificate

If you did not request your CA certificate online, but the CA you requested it from supports SCEP, before you can request a personal certificate online—that is, through SCEP enrollment—you must change this CA certificate's parameters to make it appear as if you requested it online. When the client is managed by a policy management application, the CA certificate may need to be configured, too.

For root CA certificates, you can also specify whether the certificate is trusted for IP security (IPSec).

1. In Certificate Manager, click the tab for the specific certificate type:
   - For a root CA certificate, Root CA Certificates
   - For a subordinate CA certificate, **CA Certificates**
2. On this tab, click the certificate to configure.
3. Click **Configure**. The **Configuration Parameters** dialog box opens.
4. In the **CA Domain** box, type the CA's domain name, such as **alphabeta.com**.
5. In the **Online Certificate Server** box, type the complete URL, including the schema, such as **http://**, of the CA's certificate server.
6. For Root CA certificates only: To specify that this certificate is trusted for IPSec communications, select the **Trust this certificate for IP security** check box.

   The next time you view or verify this certificate, for **Enh KeyUsage**, **IP security end system** appears as the value.
7. Click **OK**.

Use an HTTP Proxy Server for Online Certificate Requests and CRL Updates

These blocks of IP addresses are reserved for private use by the Internet Assigned Numbers Authority (IANA):

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 171.31.255.255
- 192.168.0.0 through 192.168.255.255

If your network uses an HTTP proxy server to translate private IP addresses to routable IP addresses, you must configure this option and enter the HTTP proxy server's DNS or IP address.

Note: When your computer accesses the Internet through a firewall, before you request and retrieve a CA certificate online, make sure that the **Use HTTP proxy server for online certificate requests and CRL updates** option is selected.

1. In the Security Policy Editor, click **Options>Certificate Settings**. The **Certificate Settings** dialog box opens.
2. Select the **Use HTTP proxy server for online certificate requests and CRL updates** check box.
3. In the **Proxy DNS name or IP address** box, type the DNS or IP address.
4. Click **OK**.
5. Click **Save**.

Import a CA Certificate

In these two situations, you must import a CA certificate into the Certificate Manager:

- As part of obtaining a CA certificate manually, you downloaded a CA certificate to your computer from the CA's Web site
- To obtain a CA certificate file that was exported from the Certificate Manager or a policy management application

1. In the Certificate Manager, click the tab for the certificate type to import:
   - For a root CA certificate, the **Root CA Certificates** tab
   - For a CA certificate, the **CA Certificates** tab

   If the CA certificate you import has RA certificates associated with it, these are imported with the CA certificate.
2. Click **Import Certificate**. The **Import CA Certificate** dialog box opens.
3. Navigate to the certificate file; make sure that its name displays in the **File name** box.

4. Unless your network security administrator instructs you to change it, leave the **Import certificate to local machine store** check box selected (the default).

   Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store (for all users who log on to this computer).

5. Click **Import**.
6. When a confirmation message box opens, click **Yes**.

Select a CSP

You can select a cryptographic service provider (CSP) when requesting a personal certificate, regardless of the method. You can also designate a default CSP to use for all personal certificate requests.

1. In the Security Policy Editor, click **Options>Certificate Settings**. The **Online** or **File-based Certificate Request** dialog box opens.
2. Click **Advanced**. The **Advanced Certificate Enrollment Settings** dialog box opens.
3. Click the specific CSP in the list.
4. If the **Key Size** box is enabled, click the key size to use.
5. To designate the settings on this dialog box as the default for all personal certificate requests, select the **Save as default CSP settings** check box.
6. By default, the **Place certificate and keys in local machine store** check box is clear, which places the imported certificate in your—the logged-on user's—personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

   Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store.

7. Click **OK**.

Request a Personal Certificate

After you retrieve or import a CA certificate, you must request a personal certificate from this CA. If your client was installed with a CA certificate, the Online Certificate Request or File-based Certificate Request dialog box opens automatically the first time your computer restarts after client installation.

When the CA supports SCEP, submit the request online. For CAs that don't support SCEP, create a certificate request to submit to the CA manually.

Note: If you requested your CA certificate manually from CA that supports SCEP, and want to request a personal certificate online, configure the CA certificate before requesting the personal certificate.

1. In the Certificate Manager, click the **My Certificates** tab.
2. Click **Request Certificate**. The **Online Certificate Request** or **File-based Certificate Request** dialog box opens.
3. For online certificate requests only: In the Enrollment method group, make sure that **Online** is selected.
4. In the **Subject Name** group, complete the personal information boxes, as required by the CA.

   Note: To use LDAP format when completing these boxes, select the **Enter Subject Name in LDAP format** check box, and then go to Edit a distinguished name.
5. If this CA requires it, complete at least one box in the **Subject Alternate Name** group, according to the CA's instructions. These boxes may be completed automatically.
6. For online certificate requests only: In the **Online Request Information** group, take these steps:
   a. In the **Challenge Phrase** box, type an alphanumeric character string for the CA to confirm your identity with if you ask to revoke your certificate. The CA makes sure that you are the person the certificate says you are before rescinding your certificate. Record this phrase.

   b. In the **Confirm Challenge** box, retype the challenge phrase.

   c. In the **Issuing CA** list, click the CA you are requesting the certificate from.

      Caution: Make this selection carefully; you can't reverse your decision later.

   In the **Key Generation Options** group, specify whether the private key associated with the personal certificate you're requesting can be exported to, for example, transfer it to another computer or make a backup copy. By default, the private key cannot be exported; the **Generate exportable key** check box is clear. To make the key exportable, select the **Generate exportable key** check box.
7. To select the CSP or assign the default CSP, click **Advanced**.
8. Click **OK**.
   - For online certificate requests only: This submits your request. The **Key Generation** message box opens while the client generates a public/private key pair, and then closes. The **Online Certificate Request** message box opens when the client submits your request.

When the CA receives (accepts) your request, a confirmation message may open; click **OK**.

It may take some time for the CA to approve your request. The client checks the CA at a defined interval for approved personal certificates to retrieve. To change this polling interval, go to Define how often to check for personal certificates to retrieve.

- For file-based certificate requests only: When a message box opens confirming that the certificate request file was created, click **OK**.

  To find out how to send the certificate request file to the CA and receive the certificate file when the CA returns it; this process varies with each CA, contact the specific CA.

Define How Often to Check for and Retrieve New Personal Certificates

For CAs that support SCEP, the client periodically checks for, or polls, the CA's certificate server to look for and retrieve any new personal certificates approved in response to online certificate requests, which display on the Requests tab in the Certificate Manager. You can set the time period between these automatic pools.

1. In the Security Policy Editor, click **Options>Certificate Settings**. The **Certificate Settings** dialog box opens.
2. In the **Online certificate request polling interval (minutes)** box, specify how often the client checks the CA's certificate server for approved personal certificates requests; type the number of minutes, from **1** through **999999**, between polls. The default is **15** minutes.
3. Click **OK**.
4. Click **Save**.

Retrieve a Personal Certificate Manually

After you submit your online request for a personal certificate, the CA must receive the request, and then approve it. Some time may elapse between these two events. The approval creates the personal certificate. The client automatically checks this CA for the approved certificate at the interval defined on the Certificates Setting dialog box in the Certificate Manager, and then retrieves and displays it on the My Certificates tab in the Certificate Manager.

You can check for and retrieve your approved personal certificate manually, too, if you don't want to wait for the client.

1. In the Certificate Manager, click the **Requests** tab.
2. Click **Retrieve**.

Note: If the CA hasn't approved your request yet, a message alerts you of this. Try again later or wait for the client to retrieve it.

3. If the CA has approved your request, the client prompted you to add this personal certificate; click **Yes**. The request is removed from the **Requests** tab, and the retrieved certificate displays on the **My Certificates** tab.

Manage Certificate Requests

View a Certificate Request

You can view the information about a pending request for a CA or personal certificate until you or the client you retrieve a valid certificate, you import one, or you delete the certificate request.

1. In the Certificate Manager, click the **Requests** tab.
2. Click the certificate request to view.
3. Click **View**. A dialog box opens with information about the selected certificate request.
4. To close the certificate request, click anywhere in the dialog box.

Delete a Certificate Request

You can delete a pending certificate request that displays on the Requests tab in the Certificate Manager. When you retrieve or import a valid certificate, the Certificate Manager automatically removes this certificate request.

1. In the Certificate Manager, click the **Requests** tab.
2. Click the specific certificate request.
3. Click **Delete**.
4. When a confirmation message opens, click **Yes**.
5. If prompted to delete the key container, click **Yes**.

With Manual (File-Based) Enrollment

The procedure for obtaining a CA certificate manually varies with each CA. These are the typical steps.

1. On the CA's Web site, complete the registration process.

2. Download the CA certificate from the CA's Web site to your computer through the Internet Explorer certificate management. For details, refer to Windows or Internet Explorer help.
3. In the Certificate Manager, on the **Root CA Certificates** or **CA Certificates** tab (depending on the certificate you're importing), import the CA certificate.
4. To complete the process, follow the instructions from the specific CA.

Note: Before you can request a personal certificate online from this CA, you must configure the CA certificate.

Import a CA Certificate

In these two situations, you must import a CA certificate into the Certificate Manager:

- As part of obtaining a CA certificate manually, you downloaded a CA certificate to your computer from the CA's Web site
- To obtain a CA certificate file that was exported from the Certificate Manager or a policy management application

1. In the Certificate Manager, click the tab for the certificate type to import:
   - For a root CA certificate, the **Root CA Certificates** tab
   - For a CA certificate, the **CA Certificates** tab

   If the CA certificate you import has RA certificates associated with it, these are imported with the CA certificate.
2. Click **Import Certificate**. The **Import CA Certificate** dialog box opens.
3. Navigate to the certificate file; make sure that its name displays in the **File name** box.
4. Unless your network security administrator instructs you to change it, leave the **Import certificate to local machine store** check box selected (the default).

   Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store for all users who log on to this computer.
5. Click **Import**.
6. When a confirmation message box opens, click **Yes**.

Request a Personal Certificate

After you retrieve or import a CA certificate, you must request a personal certificate from this CA. If your client was installed with a CA certificate, the Online Certificate Request or File-based Certificate Request dialog box opens automatically the first time your computer restarts after client installation.

When the CA supports SCEP, submit the request online. For CAs that don't support SCEP, create a certificate request to submit to the CA manually.

Note: If you requested your CA certificate manually from CA that supports SCEP, and want to request a personal certificate online, configure the CA certificate before requesting the personal certificate.

1. In the Certificate Manager, click the **My Certificates** tab.
2. Click **Request Certificate**. The **Online Certificate Request** or **File-based Certificate Request** dialog box opens.
3. For online certificate requests only: In the Enrollment method group, make sure that **Online** is selected.
4. In the **Subject Name** group, complete the personal information boxes, as required by the CA.

   Note: To use LDAP format when completing these boxes, select the **Enter Subject Name in LDAP format** check box, and then go to Edit a distinguished name.
5. If this CA requires it, complete at least one box in the **Subject Alternate Name** group, according to the CA's instructions. These boxes may be completed automatically.
6. For online certificate requests only: In the **Online Request Information** group, take these steps:
   a. In the **Challenge Phrase** box, type an alphanumeric character string for the CA to confirm your identity with if you ask to revoke your certificate. The CA makes sure that you are the person the certificate says you are before rescinding your certificate. Record this phrase.

   b. In the **Confirm Challenge** box, retype the challenge phrase.

   c. In the **Issuing CA** list, click the CA you are requesting the certificate from.

      Caution: Make this selection carefully; you can't reverse your decision later.

In the **Key Generation Options** group, specify whether the private key associated with the personal certificate you're requesting can be exported to, for example, transfer it to another computer or make a backup copy. By default, the private key cannot be exported; the **Generate exportable key** check box is clear. To make the key exportable, select the **Generate exportable key** check box.

7. To select the CSP or assign the default CSP, click **Advanced**.
8. Click **OK**.
   - For online certificate requests only: This submits your request. The **Key Generation** message box opens while the client generates a public/private key pair, and then closes. The **Online Certificate Request** message box opens when the client submits your request.

     When the CA receives (accepts) your request, a confirmation message may open; click **OK**.

     It may take some time for the CA to approve your request. The client checks the CA at a defined interval for approved personal certificates to retrieve. To change this polling interval, go to Define how often to check for personal certificates to retrieve.
   - For file-based certificate requests only: When a message box opens confirming that the certificate request file was created, click **OK**.

     To find out how to send the certificate request file to the CA and receive the certificate file when the CA returns it; this process varies with each CA, contact the specific CA.

Create a Personal Certificate File to Import

After you create and manually submit a personal certificate request file to a CA, and the CA approves the request, this CA returns a certificate to you in an email. You must create a certificate file from the email so that you can Import the personal certificate to the Certificate Manager.

The certificate request approval process varies with each CA. This is an example of the typical process:

1. Submit the personal certificate request file you created, **CertReq.req**, to the CA, according to the instructions the CA or your network security administrator provides.

   When the CA approves your certificate request, it sends you an email that contains the certificate.

   This is a sample email returned by the CA:

Dear Applicant,

Your Administrator has approved your request for an IPSec certificate.

If you have any questions or problems, please contact your Administrator by replying to this email message.

THE COMMON NAME OF THIS CERTIFICATE: Kerry Smith
-----BEGIN CERTIFICATE-----

MIICzCCAmigAwIBAgIQRFfr0rQ4W2xUCfmYzDKCqDANBgkqhkiG9w0BAQQFADCB
zjEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xRzBFBgNVBAsTPkZvciBWZXJpU2ln
biBhdXRob3JpemVkIHRlc3Rpbmcgb25seS4gTm8gYXNzdXJhbmNlcyAoQykgVlMx
OTk4MUcwRQYDVQQLEz53d3cudmVyaXNpZ24uY29tL3JlcG9zaXRvcnkvVGVzdENQ
MA0GCSqGSIb3DQEBBAUAA4GBACBA6T+yqr8xoJfBv2T0P1AcLxG9tjOMuUPELvV
mg4jNB2Jj9oD+iIpEp4yf4NhKq6N3p8vcdXXz2FMxhNMHGAqY8mwKhRAPQrJKnVi
/o9Adoh7SQ3Aoh4ds8CfRcgcrHdQeQBdgszwzRJMTNKP3zj/qvRevIZ/h72MbfWl
gnvK

-----END CERTIFICATE-----

2. Copy the entire certificate, from -----**BEGIN CERTIFICATE**----- through -----**END CERTIFICATE**-----, inclusive.

   Note: When working with Microsoft Certificate Server, copy only the data between -----**BEGIN CERTIFICATE**----- and -----**END CERTIFICATE**-----, not inclusive, and insert a carriage return at the end.

3. Paste the certificate into a text editor, such as Notepad. Do not use a full featured word processor such as MicorSoft Word that will add extra formatting data to the file. Name it **CertReq.der**, and save it to the same drive and directory that the certificate request file, **CertReq.req**, resides in.

4. Import the personal certificate to the Certificate Manager.

Import a Personal Certificate

In these two situations, you must import a personal certificate to the Certificate Manager:

- If you created a personal certificate file from the email that the CA when you manually requested a personal certificate
- To bring a personal certificate file exported from the Certificate Manager (not necessarily in your client) to your client's Certificate Manager

Note: Make sure that you have the password entered to protect the private key when this personal certificate was exported.

1. In the Certificate Manager, click the **My Certificates** tab.
2. Click **Import Certificate**. The **Import Certificate** dialog box opens.
3. In the Import Type group, select the certificate and private key type to import:
   - For online certificate enrollment, click **PKCS12 Personal Certificate**.
   - For older certificate and key types, click **Certificate and Private Key File**.
   - For a manual certificate request, click **Certificate Request Response File**.
4. By default, the **Import certificate to local machine store** check box is clear, which places the imported certificate in your—the logged-on user's—personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

   Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store.
5. The import type you selected determines the boxes available for you to complete:
   - In the **Certificate File** box, type the drive, directory, and file name/file type of the personal certificate or certificate request response file to import or click **Browse** to locate it.

     The default certificate request response filename is **C:\temp_directory_for_OS\Cert.p7r**.
   - In the **Key File** box, type the drive, directory, and file name of the private key file to import or click **Browse** to locate it.
   - In the **Password** box, type the password used when the file was exported.
6. Unless your network security administrator advises you to change it, leave the **Import certificate to local machine store** check box selected (the default).
7. Click **Import**.
8. When the key import confirmation message opens, click **OK**.

   Note: If the import fails, try selecting a different import type.
9. When prompted to add this personal certificate, click **Yes**.

Select a CSP

You can select a cryptographic service provider (CSP) when requesting a personal certificate, regardless of the method. You can also designate a default CSP to use for all personal certificate requests.

1. In the Security Policy Editor, click **Options>Certificate Settings**. The **Online** or **File-based Certificate Request** dialog box opens.
2. Click **Advanced**. The **Advanced Certificate Enrollment Settings** dialog box opens.
3. Click the specific CSP in the list.
4. If the **Key Size** box is enabled, click the key size to use.
5. To designate the settings on this dialog box as the default for all personal certificate requests, select the **Save as default CSP settings** check box.
6. By default, the **Place certificate and keys in local machine store** check box is clear, which places the imported certificate in your—the logged-on user's—personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

   Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store.
7. Click **OK**.

View and Delete Certificate Requests

You can view the information about a pending request for a CA or personal certificate until you or the client you retrieve a valid certificate, you import one, or you Delete the certificate request.

1. In the Certificate Manager, click the **Requests** tab.
2. Click the certificate request to view.
3. Click **View**. A dialog box opens with information about the selected certificate request.
4. To close the certificate request, click anywhere in the dialog box.

You can delete a pending certificate request that displays on the Requests tab in the Certificate Manager. When you retrieve or import a valid certificate, the Certificate Manager automatically removes this certificate request.

1. In the Certificate Manager, click the **Requests** tab.
2. Click the specific certificate request.
3. Click **Delete**.

4. When a confirmation message opens, click **Yes**.
5. If prompted to delete the key container, click **Yes**.

Obtain Certificates Through Internet Explorer

You can use CA and personal certificates obtained outside the client—for example, through Microsoft Internet Explorer or your email program—with the client. In some email programs, personal certificates are called digital IDs.

To obtain certificates through Internet Explorer, go to the Web page the CA or your network security administrator directs you to, and then follow the directions provided. You don't need to go through the client's Certificate Manager to request certificates.

Note: To access the Microsoft CSP, make sure that Internet Explorer 5.01 or later is installed on your computer.

Manage Certificates

When you view a certificate, a new window opens with various certificate attributes, such as its name, serial number, key size, and validity dates.

1. In the Certificate Manager, click the tab for the type of certificate to view:
   - For a personal certificate, **My Certificates**

     By default (the **All** option is selected), the tab lists all personal certificates issued to you and your computer (**Users** and **This machine**).

     – For a list of the personal certificates issued to you, the logged-on user, click **Users**.

     – For a list of the personal certificates issued to your computer (the local machine), click **This machine**.
   - For a root CA certificate, **Root CA Certificates**

     – Clear the **Show only trusted roots** check box; this lists all root CA certificates on the computer.
   - For a subordinate CA certificate, **CA Certificates**
   - For an RA certificate, **RA Certificates**
2. Click the specific certificate to view.

3. Click **View**. A box opens with information about the selected certificate.
4. To close the certificate, click anywhere in this certificate box.

Verify a Certificate

After you import or retrieve a certificate, you can check whether it is valid or verified.

1. In the Certificate Manager, take the steps for the specific certificate type:
   - For a personal certificate:
     - Click the **My Certificates** tab.
     - If the certificate you want to verify isn't listed on the tab, in **Show certificates for**, click **All**. This displays every personal certificate on the computer on the tab.
   - For a root CA certificate:
     - Click the **Root CA Certificates** tab.
     - If the certificate you want to verify isn't listed on the tab, clear the **Show only trusted roots** check box. Every root CA certificate on the computer displays on the tab.
   - For a subordinate CA certificate, click the **CA Certificates** tab.
   - For an RA certificate, click the **RA Certificates** tab.
     - Click the certificate to verify.
     - Click **Verify**. The client checks the validity dates and attempts to check the certificate against its revocation list. A dialog box opens with this information:
   - Current status of the certificate: valid/verified or invalid/not verified, depending on the certificate type
   - If the certificate is invalid or not verified, a brief explanation of why
   - The certificate's contents and attributes, such as its name, serial number, and key size
2. To close this dialog box, click **OK**.

Export a CA Certificate

Exporting a CA certificate copies it to a file to, for example, transfer it to another computer, create a backup copy, or include it in a customized client installation.

When a CA certificate has associated RA certificates, the CA certificate export file also contains these RA certificates.

1. In the Certificate Manager, click the tab for the certificate type to export:
   - For a root CA certificate, the **Root CA Certificates** tab
   - For a subordinate CA certificate, the **CA Certificates** tab
2. Click the certificate to export.
3. Click **Export**. The **Export CA Certificate** dialog box opens.
4. Navigate to the destination drive and directory for the file.
5. In the **File name** box, enter the filename of the certificate you are exporting. The default filename is **C:\temp_directory_path_for_OS\CaCert.cser**.

   Note: If you're creating a customized client installation, accept the default filename.
6. Click **Save**.

Delete a Certificate

Note: When you delete a CA certificate, the client also deletes any associated RA certificates.

1. In the Certificate Manager, take the steps for the specific certificate type:
   - For a personal certificate:
     – Click the **My Certificates** tab.
     – If the certificate to delete isn't listed on the tab, in the Show certificates for group, click **All**. All personal certificates on the computer display on the tab.
   - For a root CA certificate:
     – Click the **Root CA Certificates** tab.
     – Clear the **Show only trusted roots** check box. All root CA certificates on the computer display on the tab.
   - For a subordinate CA certificate, click the **CA Certificates** tab.
   - For an expired RA certificate, the only RA certificates you can directly delete, click the **RA certificates** tab.
     – Click the certificate to delete.
     – Click **Delete**.

  - When a delete confirmation message box opens, click **OK**.

RA Certificates

When you view a certificate, a new window opens with various certificate attributes, such as its name, serial number, key size, and validity dates.

1. In the Certificate Manager, click the tab for the type of certificate to view:
   - For a personal certificate, **My Certificates**

     By default (the **All** option is selected), the tab lists all personal certificates issued to you and your computer (**Users** and **This machine**).
     - For a list of the personal certificates issued to you, the logged-on user, click **Users**.
     - For a list of the personal certificates issued to your computer (the local machine), click **This machine**.
   - For a root CA certificate, **Root CA Certificates**
     - Clear the **Show only trusted roots** check box; this lists all root CA certificates on the computer.
   - For a subordinate CA certificate, **CA Certificates**
   - For an RA certificate, **RA Certificates**
2. Click the specific certificate to view.
3. Click **View**. A box opens with information about the selected certificate.
4. To close the certificate, click anywhere in this certificate box.

After you import or retrieve a certificate, you can check whether it is valid or verified.

1. In the Certificate Manager, take the steps for the specific certificate type:
   - For a personal certificate:
     - Click the **My Certificates** tab.
     - If the certificate you want to verify isn't listed on the tab, in **Show certificates for**, click **All**. This displays every personal certificate on the computer on the tab.
   - For a root CA certificate:
     - Click the **Root CA Certificates** tab.

    - If the certificate you want to verify isn't listed on the tab, clear the **Show only trusted roots** check box. Every root CA certificate on the computer displays on the tab.
  - For a subordinate CA certificate, click the **CA Certificates** tab.
  - For an RA certificate, click the **RA Certificates** tab.
    - Click the certificate to verify.
    - Click **Verify**. The client checks the validity dates and attempts to check the certificate against its revocation list. A dialog box opens with this information:
  - Current status of the certificate: valid/verified or invalid/not verified, depending on the certificate type
  - If the certificate is invalid or not verified, a brief explanation of why
  - The certificate's contents and attributes, such as its name, serial number, and key size

2. To close this dialog box, click **OK**.

Personal Certificates

In these two situations, you must import a personal certificate to the Certificate Manager:

- If you created a personal certificate file from the email that the CA when you manually requested a personal certificate
- To bring a personal certificate file exported from the Certificate Manager (not necessarily in your client) to your client's Certificate Manager

  Note: Make sure that you have the password entered to protect the private key when this personal certificate was exported.

1. In the Certificate Manager, click the **My Certificates** tab.
2. Click **Import Certificate**. The **Import Certificate** dialog box opens.
3. In the Import Type group, select the certificate and private key type to import:
   - For online certificate enrollment, click **PKCS12 Personal Certificate**.
   - For older certificate and key types, click **Certificate and Private Key File**.
   - For a manual certificate request, click **Certificate Request Response File**.
4. By default, the **Import certificate to local machine store** check box is clear, which places the imported certificate in your—the logged-on user's—personal certificate store. Unless your network security administrator instructs you to change it, accept the default.

Caution: In Windows NT and Windows 2000 and XP, you must be logged on as **administrator** or its equivalent to add this certificate to the local machine store (for all users who log on to this computer).

5. The import type you selected determines the boxes available for you to complete:
   - In the **Certificate File** box, type the drive, directory, and file name/file type of the personal certificate or certificate request response file to import or click **Browse** to locate it.

     The default certificate request response filename is **C:\temp_directory_for_OS\Cert.p7r**.
   - In the **Key File** box, type the drive, directory, and file name of the private key file to import or click **Browse** to locate it.
   - In the **Password** box, type the password used when the file was exported.
6. Unless your network security administrator advises you to change it, leave the **Import certificate to local machine store** check box selected (the default).
7. Click **Import**.
8. When the key import confirmation message opens, click **OK**.

   Note: If the import fails, try selecting a different import type.
9. When prompted to add this personal certificate, click **Yes**.

When you view a certificate, a new window opens with various certificate attributes, such as its name, serial number, key size, and validity dates.

1. In the Certificate Manager, click the tab for the type of certificate to view:
   - For a personal certificate, **My Certificates**

     By default (the **All** option is selected), the tab lists all personal certificates issued to you and your computer (**Users** and **This machine**).
     - For a list of the personal certificates issued to you, the logged-on user, click **Users**.
     - For a list of the personal certificates issued to your computer (the local machine), click **This machine**.
   - For a root CA certificate, **Root CA Certificates**
     - Clear the **Show only trusted roots** check box; this lists all root CA certificates on the computer.
   - For a subordinate CA certificate, **CA Certificates**

- For an RA certificate, **RA Certificates**

2. Click the specific certificate to view.
3. Click **View**. A box opens with information about the selected certificate.
4. To close the certificate, click anywhere in this certificate box.

After you import or retrieve a certificate, you can check whether it is valid or verified.

1. In the Certificate Manager, take the steps for the specific certificate type:
   - For a personal certificate:
     – Click the **My Certificates** tab.
     – If the certificate you want to verify isn't listed on the tab, in **Show certificates for**, click **All**. This displays every personal certificate on the computer on the tab.
   - For a root CA certificate:
     – Click the **Root CA Certificates** tab.
     – If the certificate you want to verify isn't listed on the tab, clear the **Show only trusted roots** check box. Every root CA certificate on the computer displays on the tab.
   - For a subordinate CA certificate, click the **CA Certificates** tab.
   - For an RA certificate, click the **RA Certificates** tab.
     – Click the certificate to verify.
     – Click **Verify**. The client checks the validity dates and attempts to check the certificate against its revocation list. A dialog box opens with this information:
   - Current status of the certificate: valid/verified or invalid/not verified, depending on the certificate type
   - If the certificate is invalid or not verified, a brief explanation of why
   - The certificate's contents and attributes, such as its name, serial number, and key size
2. To close this dialog box, click **OK**.

Export a Personal Certificate

Exporting a personal certificate copies it to a file so that you can, for example, transfer it to another computer or create a backup copy.

Caution: The private key is exported with the personal certificate only if, when the personal certificate was requested, the Generate exportable key check box was selected. If this check box was not selected then, you can't export the private key.

1. In the Certificate Manager, click the **My Certificates** tab.
2. Click the personal certificate to export.
3. Click **Export**. The **Export Certificate and Private Key** dialog box opens.
4. In the **File name** box, enter the drive, directory, and filename for the personal certificate file. The default filename is **C:\temp_directory_path_for_OS\Cert.p12**.
5. In the **Password** box, type an alphanumeric password.
6. In the **Confirm Password** box, retype the password. Record it, too; whoever imports this file will need it.
7. Click **Export**.

Delete a Certificate

Note: When you delete a CA certificate, the client also deletes any associated RA certificates.

1. In the Certificate Manager, take the steps for the specific certificate type:
   - For a personal certificate:
     – Click the **My Certificates** tab.
     – If the certificate to delete isn't listed on the tab, in the Show certificates for group, click **All**. All personal certificates on the computer display on the tab.
   - For a root CA certificate:
     – Click the **Root CA Certificates** tab.
     – Clear the **Show only trusted roots** check box. All root CA certificates on the computer display on the tab.
   - For a subordinate CA certificate, click the **CA Certificates** tab.
   - For an expired RA certificate, the only RA certificates you can directly delete, click the **RA certificates** tab.
     – Click the certificate to delete.
     – Click **Delete**.
     – When a delete confirmation message box opens, click **OK**.

Manage Certificate Revocation Lists (CRLs)

A certificate revocation list (CRL) is a list of certificates that the issuing CA rescinded before their expiration dates. This may occur when, for example, a user's name or address changes or the user leaves the company. When you retrieve or import a certificate from a CA, it typically contains a CRL. If it doesn't, you can import one. You can view a CRL on the CRLs tab in the Certificate Manager.

The client can periodically poll, or check for, CA CRL distribution sites and then retrieve the latest CRLs. You must define the site and polling interval.

1. In the Certificate Manager, view a personal certificate.
2. On the certificate, if the **CRL Dist. Point** entry contains an URL, jot down what precedes the **://** in the URL: **http**, **file**, or **ldap**.
3. In the Security Policy Editor, click **Options>Certificate Settings**. The **Certificate Settings** dialog box opens.
4. The **CRL Dist. Point** entry on the personal certificate you just viewed determines your next step:
   - If there was no **CRL Dist. Point** entry, clear the **Enable automatic CRL retrieval** check box.
   - If the **CRL Dist. Point** entry contained an URL, take these steps:
     - Select the **Enable automatic CRL retrieval** check box.
     - In the **CRL retrieval interval (hours)** box, specify how often the client checks for and retrieves new CRLs from the CA; type the number of hours, from **1** through **24**, between these checks. The default is **24** hours.
     - The URL's scheme name determines whether you must complete the **Default LDAP Server for CRLs** box:

Table 6-2:

URL Scheme Name	Definition	Action
file or http	CRLS are published to a Web server. The certificate contains this Web server's address.	Leave the **Default LDAP Server for CRLs** box blank.
ldap	Distinguished name of the distribution point on the LDAP directory server. This doesn't specify the LDAP server for the client to check for CRLs.	In the **Default LDAP Server for CRLs** box, type the LDAP server's IP address, domain name, or complete URL.

5. Click **OK**.
6. Click **Save**.

Import a CRL

If your CA didn't include a CRL in its CA certificate file, you can manually import a CRL to the Certificate Manager.

1. In the Certificate Manager, click the **CRLs** tab.
2. Click **Import CRL**. The **Import CRL** dialog box opens.
3. Navigate to the CRL file to import so that its file name displays in the **File name** box. The file type is typically **.crl**.
4. Click **Import**.
5. Click **Close**.

Update all CRLs Manually

Instead of waiting for the client to check for and retrieve new CRLs automatically at defined intervals, you can manually update all the CRLs.

1. In the Certificate Manager, click the **CRLs** tab.

2. Click **Update All CRLs**.
3. Click **Close**.

View a CRL

1. In the Certificate Manager, click the **CRLs** tab.
2. Click the CRL to view.
3. Click **View**. A dialog box with information about the selected CRL opens.
4. To close this dialog box, click **OK**.

Delete a CRL

If you no longer need the CRL for a particular CA, you can delete it from the Certificate Manager.

1. In the Certificate Manager, click the **CRLs** tab.
2. Click the CRL to delete.
3. Click **Delete**.
4. When a confirmation message box opens, click **OK**.
5. Click **Close**.

Manage the Trust Policy

In the Certificate Manager, when you trust a root CA certificate, the client considers this CA, its subordinate CAs, and the certificates issued by these CAs as valid for IPSec communications, Conversely, when a root CA certificate is not trusted for IPSec sessions, neither are the certificates issued by it or its subordinate CAs.

The trust policy specifies the trusted root CAs:

- Root CAs specifically configured for IPSec communications (the default)

  The client selects this option when it imports a root CA or reinstalls it after you upgrade the client, if you saved your certificates.

  There are two ways to identify a trusted root CA certificate in the Certificate Manager:

  - On the **Configuration Parameters** dialog box, the **Trust this certificate for IP security** check box is selected.
  - When you view or verify the certificates, for **Enh KeyUsage**, the option **IP security end system** appears.
- Root CAs that have issued a personal certificate to any of the computer's users
- All root CAs installed on your computer (the local machine)

The trust policy also applies to personal certificates issued by a CA in the trust hierarchy for remote parties that your security policy allows you to communicate with.

Set the Trust Policy

The trust policy for certificates specifies which root CA certificates the client considers valid for IPSec communications. When you set the trust policy on the Trust Policy tab in the Certificate Manager, the trust policy selected on the Root CA Certificates and Root CA Certificates tabs changes to reflect the Trust Policy tab setting.

1. In the Certificate Manager, click the **Trust Policy** tab.
2. In the Specify which root certificate authorities (CAs) to trust group, select the trust policy:
   - To trust only those root CA certificates configured to be trusted for IPSec sessions, click **Trust specific root CAs**.
   - To trust only root CA certificates that issued a personal certificate to any of the computer's users, click **Trust CAs that have issued a local personal certificate**.
   - To trust all the root CAs installed on your computer, click **Trust all root CAs installed on this computer**

     Caution: Depending on the operating system and Internet Explorer version installed on your computer, there may be at least 100 root CA certificates on your computer. Before you select this option, carefully consider the security ramifications.

   The trust policy you select takes effect immediately.

Set the Trust Policy and View Trusted Root CA Certificates

Typically, you select the trust policy for the client on the Certificate Manager's Trust Policy tab. The Root CA Certificates tab displays the trusted root CA certificates.

You can, however, change the trust policy on the Root CA Certificates tab, and view a real-time list of the trusted root CA certificates. When you change the trust policy on this tab, the client dynamically updates the trust policy selected on the Trust Policy tab.

1. In the Certificate Manager, click the **Root CA Certificates** tab.
2. Select the **Show only trusted roots** check box. Based on the trust policy specified in the **Trust policy--trust these roots for IPSec** group, all the trusted root CA certificates display in the list.

   The **Trust policy--trust these roots for IPSec** options match those on the **Trust Policy** tab, with different labels:

Table 6-3:

Trust policy options:	
Root CA Certificates tab	Trust Policy tab
Configured roots (default)	**Trust specific root CAs** (default)
Issuers of my certs	Trust CAs that have issued a local personal certificate
All roots	Trust all root CAs installed on this computer

   Caution: Depending on the operating system and Internet Explorer version installed on your computer, there may be at least 100 root CA certificates on your computer. Before clicking **All roots**, carefully consider the security ramifications.

3. In the **Trust policy--trust these roots for IPSec** group, click the trust policy option to apply; this takes effect immediately. The list of trusted root CAs is updated to reflect the change.

Chapter 7
Using Sessions

This chapter describes how to perform network management tasks with your NETGEAR ProSafe VPN Client.

Authenticate Yourself

You may be prompted to enter your username and password when you attempt to establish a VPN; enter this information on the dialog box that opens. This is to authenticate who you, the user, are to the network, before the connection is initiated.

Automatically Start and End Secure Sessions

By default, the client automatically establishes and terminates connections, based on the remote party's identity, when needed.

For example, suppose that you want to check your office email from home. The security policy in the client installed on your home computer contains a VPN to access the office network's mail server. When you start your email program at home, and select the proper profile, the client initiates the secure connection behind the scenes. The remote party's identity determines which connection the client selects. All that you'll probably see is a connection logon dialog box, if it's required. After the client connects to the network mail server, you can access your office email.

The connection remains “up” or active until one of these occurs:

- It's dropped by the network, the Internet, or your ISP.
- You turn your computer off.
- When importing or reloading the security policy, you select the **Reset existing connections** option.
- You terminate it manually with the Disconnect or Disconnect All option on the client icon's shortcut menu.

Note: You may be required to start and end secure sessions manually or choose to work with secure connections that way.

Start and End a Secure Session Manually

By default, the client automatically establishes and terminates secure connections—VPNs—based on the remote party's identity. You can, however, directly connect to a specific destination with the **Connect** option on the client icon's shortcut (right-click) menu. Starting the secure connection by selecting this option is analogous to picking up the handset of a telephone and selecting a speed dial number or entering the other party's number to initiate a phone call.

For example, when you're in the office, you connect directly to your corporate network; to access this network remotely, from home or on the road, you must use a VPN connection. With the manual connection feature, you can select the specific connection to use.

If the Only Connect Manually check box check box is selected for a specific connection, the client doesn't automatically initiate or end secure sessions for this connection; you must manually connect and disconnect such sessions.

1. In the Windows system tray, right-click the **client icon**, point to **Connect**, and then click the connection name.
2. To terminate the secure communications session, right-click the **client icon**, click **Disconnect**, and then click the connection name to end.

Chapter 8
Distributing Customized Profiles

A customized installation is the standard client installation package modified to include a security policy, a CA certificate, and perhaps a personal certificate. If preshared keys are to be employed, you can include these instead of CA and personal certificates. Because personal certificates are unique to each individual, a single personal certificate cannot be distributed to multiple users.

Adding these entities to the basic client installation package can facilitate managing corporate security policies for multiple users. You can create multiple customized installations for users with different security needs.

The customized installation package options are presented below.

Create a Customized Installation Containing a Security Policy

1. Configure the security policy for the users.

   Note: If you want users to employ preshared keys instead of certificates, configure one in *My Identity* for the security policy.

2. Export the security policy; name the file **IPSecPolicy.spd**.
3. Add the **IPSecPolicy.spd** file to the **NETGEAR ProSafe VPN Client** installation directory.
4. Deploy this customized installation to users on a network drive, Web site, CD-ROM, or other location or medium, such as a directory or **.zip** or **.exe** file.
5. Make sure that the users have installation instructions and the specific information they need to either use preshared keys or obtain a CA certificate and personal certificate. Help topics describe these tasks.

Create a Customized Installation Containing a Security Policy and a CA Certificate

1. Obtain a CA certificate.
2. Export this CA certificate; name the file CaCert.cser.
3. Configure a security policy.
4. Export the security policy; name the file **IPSecPolicy.spd**.
5. Add the **CaCert.cser** and the **I**PSecPolicy.spd files to the same directory that the **setup.exe** file is located in on the **NETGEAR ProSafe VPN Client** installation media.
6. Deploy this customized installation to users on a network drive, Web page, CD-ROM, or other location/medium as a directory or .zip or .exe file.
7. Tell users how to install the product and perform these tasks:
   a. Add the CA certificate to the Root Store, when prompted.
   b. Complete the online personal certificate request form that opens automatically. They need their domain name and IP address and, if they are allowed to transfer their personal certificate to another computer, they must select the **Generate exportable key** option.

Create a Customized Installation Containing a Security Policy, CA Certificate, and Personal Certificate

Note: Because personal certificates are unique to each individual, a single personal certificate cannot be distributed to multiple users.

1. Obtain a CA certificate.
2. Export the CA certificate; name the file CaCert.cser.
3. Request a personal certificate for each user to receive this customized installation.

   Note: When you create the certificate request, click **Generate exportable key**.
4. Export the personal certificate, which includes the private key; name the file **IPSecCerts.p12**.
5. Configure a security policy.

6. Export the security policy; name the file **IPSecPolicy.spd**.
7. Add the **CaCert.cser**, **IPSecCerts.p12**, and the **IPSecPolicy.spd** files to the same directory that the **setup.exe** file is located in on the **NETGEAR ProSafe VPN Client** installation media.
8. Deploy this customized installation to users on a network drive, Web page, CD-ROM, or other location/medium as a directory or .zip or .exe file.
9. Make sure that users have installation instructions and the password entered when you exported the personal certificates.

Chapter 9
Troubleshooting

System Tray Icons

The client icon displays in the Windows system tray. The icon may change very quickly to reflect the real-time communications status for active connections; it may even appear to blink.

Table 9-1. System Tray Icons

Icon	Explanation
	• The Windows operating system did not start the IREIKE service properly. To start this service, restart your computer. If this icon continues to display, you may need to reinstall the client. or • Your security policy is deactivated—that is, disabled. To reactivate it, go to Reactivate the security policy.
	Your computer is ready to establish connections or transmit data.
	Your computer has established no secure connections and is transmitting unsecured data.
	Your computer has established at least one secure connection, but is transmitting no data.
	Your computer has established at least one secure connection and is transmitting only unsecured data.
	Your computer has established at least one secure connection and is transmitting only secured data.
	Your computer has established at least one secure connection and is transmitting secured and unsecured data.

Remove the Client Icon from the System Tray

Although it is not recommended, the client icon can be removed from the system tray. Typically, this occurs inadvertently. This has no affect on the communications status of active connections.

- In the Windows system tray, right-click the **client icon**, and then click **Remove Icon**.

Restore the Client Icon to the System Tray

If you remove the client icon from the system tray, you can put it back.

1. In Windows Explorer, locate this file on your computer, mostly likely on the C: drive:

   NETGEAR VPN Client installation directory**/Program Files/NETGEAR ProSafe VPN Client/Safecfg.exe**.

2. Double-click the file **Safecfg.exe**. The client icon reappears in the system tray.
3. Exit Windows Explorer.

Log Viewer

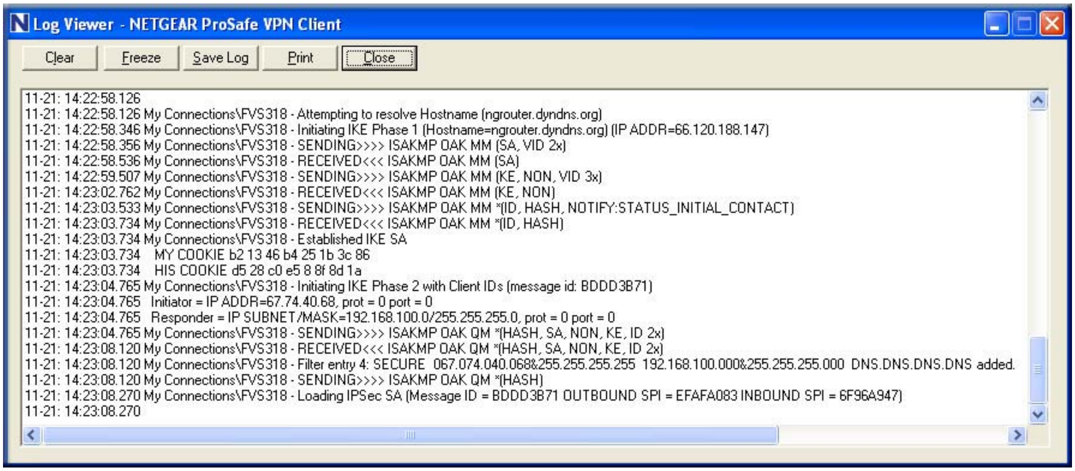
The Log Viewer lists the IKE negotiations that occur during Authentication (Phase 1). These messages can be a helpful diagnostic tool when troubleshooting problems that occur in this phase.

Ongoing negotiations overwrite the messages displayed in the Log Viewer; the client does not save logged messages. To preserve currently displayed messages, you can freeze the log, and then save or print its contents.

You can also save logged messages to the **isakmp.log** file in the client installation directory. You can send the log file to a remote network administrator or customer support center instead of repeatedly freezing and saving the Log Viewer's contents and sending these files.

There are two ways to open the Log Viewer:

- On the Windows desktop, click **Start>Programs>NETGEAR ProSafe VPN Client**>Log Viewer.
- Right-click the **client icon**, and then click **Log Viewer**.



```
11-21: 14:22:58.126
11-21: 14:22:58.126 My Connections\FVS318 - Attempting to resolve Hostname (ngrouter.dyndns.org)
11-21: 14:22:58.346 My Connections\FVS318 - Initiating IKE Phase 1 (Hostname=ngrouter.dyndns.org) (IP ADDR=66.120.188.147)
11-21: 14:22:58.356 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM (SA, VID 2x)
11-21: 14:22:58.536 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM (SA)
11-21: 14:22:59.507 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM (KE, NON, VID 3x)
11-21: 14:23:02.762 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM (KE, NON)
11-21: 14:23:03.533 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
11-21: 14:23:03.734 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
11-21: 14:23:03.734 My Connections\FVS318 - Established IKE SA
11-21: 14:23:03.734    MY COOKIE b2 13 46 b4 25 1b 3c 86
11-21: 14:23:03.734    HIS COOKIE d5 28 c0 e5 8 8f 8d 1a
11-21: 14:23:04.765 My Connections\FVS318 - Initiating IKE Phase 2 with Client IDs (message id: BDDD3B71)
11-21: 14:23:04.765   Initiator = IP ADDR=67.74.40.68, prot = 0 port = 0
11-21: 14:23:04.765   Responder = IP SUBNET/MASK=192.168.100.0/255.255.255.0, prot = 0 port = 0
11-21: 14:23:04.765 My Connections\FVS318 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-21: 14:23:08.120 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-21: 14:23:08.120 My Connections\FVS318 - Filter entry 4: SECURE  067.074.040.068&255.255.255.255  192.168.100.000&255.255.255.000  DNS.DNS.DNS.DNS added.
11-21: 14:23:08.120 My Connections\FVS318 - SENDING>>>> ISAKMP OAK QM *(HASH)
11-21: 14:23:08.270 My Connections\FVS318 - Loading IPSec SA (Message ID = BDDD3B71 OUTBOUND SPI = EFAFA083 INBOUND SPI = 6F96A947)
11-21: 14:23:08.270
```

Freeze the Log Viewer

The client doesn't save logged messages; ongoing negotiations overwrite the messages displayed in the Log Viewer. To preserve the currently displayed messages, you can pause or freeze the log, and then save or print its contents.

Or, to save all the logged messages to a file, enable the file isakmp.log on the **Global Policy Settings** dialog box in the Security Policy Editor.

- In the Log Viewer, click **Freeze**. The button's label changes to **Unfreeze**.

Unfreeze the Log Viewer

When the Log Viewer is frozen or halted, you must unfreeze it to restart the logging and scrolling of IKE negotiation messages in the Log Viewer.

- In the Log Viewer, click **Unfreeze**. The button's label changes to **Freeze**.

Clear Log Viewer Messages

You can't recover the messages that you clear manually from the Log Viewer.

1. In the Log Viewer, click **Clear**.

Save the Log Viewer Messages

1. In the Log Viewer, click **Freeze**.
2. Click **Save Log**.
3. In the **Save As** dialog box, follow the standard Windows Save As procedure. By default, the file is named **IKEx.log**, where x is an incremental number.

Print the messages in the Log Viewer

1. In the Log Viewer, click **Freeze**.
2. Click **Print**.
3. In the **Print** dialog box, follow the standard Windows Print procedure.

Configure Global Policy Settings

Global policy settings are program preferences that apply to all secure IP communications. You can change these at any time to match to your security policy.

1. In the Security Policy Editor, click **Options**, and then click **Global Policy Settings**. The **Global Policy Settings** dialog box opens.
2. In the **Retransmit Interval** box, type the length of time, in seconds, that the client waits before resending an IKE protocol packet that has not been responded to. The default is **8** seconds.

   Note: If the client selects a redundant gateway when you know that the primary one is available, try entering a higher number for **Retransmit Interval**.
3. In the **Number of retries** box, type the number of times your computer resends an IKE protocol packet before abandoning the exchange. The default is **3** tries.
4. Status notifications are messages that inform communicating parties what the time-out periods are and whether their security proposals have been accepted or rejected.

   To send these messages, select the **Send status notifications to peer host** check box.
5. An internal network IP address is a virtual IP address assigned to the client user. Remote users can appear as internal users on a private network to, for example, access a WINS server or browse the network.

To enable remote users to appear as internal users on a private network, select the **Allow to Specify Internal Network Address** check box.

Note: If you select this check box, you must enter a private internal network IP address when configuring My Identity.

6. To enable logging the **Log Viewer's** IKE negotiation messages to the **isakmp.log** file in the client's installation directory, select the **Enable logging to a file** check box. This can facilitate remote troubleshooting by allowing a user to send a file with these messages instead of repeatedly freezing and printing the Log Viewer.

   Notes:

   - The maximum size for the isakmp.log file is 100 KB. When the client's computer, the client, and the IKE service restart and the isakmp.log file size exceeds 100 KB, this isakmp.log file is deleted and a new one created.
   - On computers running Windows 95 and 98, when the isakmp.log file size exceeds 64 KB, Notepad prompts the user to try WordPad instead because of the file's size. When the user tries WordPad, however, WordPad prompts the user that it can't open the file because it is in use by another program (the IKE service).

   In this case, to view the file, try one of these options:

     - Rename it, and then open it in WordPad.
     - Open a read-only version of the file in Microsoft Word.
     - Clear the **Enable logging to a file** check box, and then open the file.

7. If you don't use a smart card and reader or similar device to authenticate your identity, skip this step.

   If you do use a smart card and reader or similar device, the client can, when it detects that the smart card or reader is removed, delete active keys and end these communications sessions. This provides extra security. Only connections that use the keys on your smart card are affected.

   To enable this feature, select the **Smart card removal clears keys** check box.

8. Click **OK**.
9. Click **Save**.

Network Address Translation (NAT)

Network Address Translation (NAT) devices are widely deployed to enable local area networks (LANs) to use a single set of external IP addresses for an entire network.

Remote users commonly encounter NAT devices in home networks, broadband modems (cable and DSL), and hotels. Although an IPSec VPN connection can coexist with NAT devices, IPSec-NAT incompatibilities may occur. To prevent these incompatibilities, the client employs the latest of the emerging standards for NAT-Traversal (NAT-T).

When connecting to a peer (remote) device that implements the same NAT-T standard (there are several), the client automatically detects the presence of the NAT device; you don't have to configure anything. Then, the client and the peer device encapsulate the IPSec packets inside UDP packets; this allows the VPN connection to traverse the NAT device without requiring any changes in the NAT device.

When the client connects to a peer device and detects a NAT device, Log Viewer messages indicate this detection. Here is a sample of these logged messages:

Table 9-1. Sample of NAT Log Messages

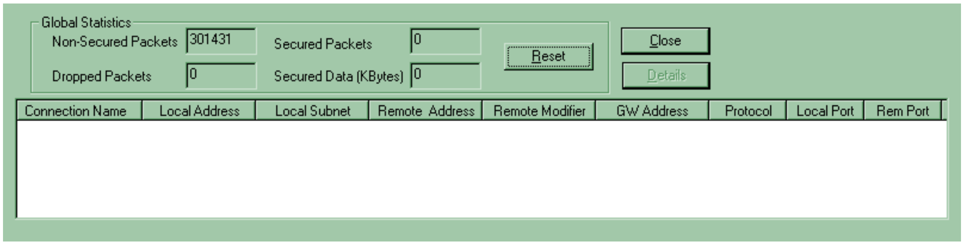
```
10:12:05.371
10:12:05.371 My Connections\NAT-T Demo - Initiating IKE Phase 1 (IP ADDR=65.163.78.79)
10:12:05.371 My Connections\NAT-T Demo - SENDING>>>> ISAKMP OAK MM (SA, VID)
10:12:05.481 My Connections\NAT-T Demo - RECEIVED<<< ISAKMP OAK MM (SA, VID,
VID, VID)
10:12:05.541 My Connections\NAT-T Demo - Peer is NAT-T capable
10:12:05.551 My Connections\NAT-T Demo - SENDING>>>> ISAKMP OAK MM (KE, NON,
NAT-D, NAT-D, VID, VID, VID)
10:12:05.681 My Connections\NAT-T Demo - RECEIVED<<< ISAKMP OAK MM (KE, NON,
CERT_REQ, NAT-D, NAT-D)
10:12:07.164 My Connections\NAT-T Demo - NAT is detected for Client
10:12:07.204 My Connections\NAT-T Demo - Using auto-selected user certificate "nscert1's
SAFENET ENGINEERING ID".
10:12:07.394 My Connections\NAT-T Demo - SENDING>>>> ISAKMP OAK MM *(ID, CERT,
CERT_REQ, CERT_REQ, CERT_REQ, CERT_REQ, SIG,
NOTIFY:STATUS_INITIAL_CONTACT)
10:12:07.594 My Connections\NAT-T Demo - RECEIVED<<< ISAKMP OAK MM *(ID, CERT,
SIG)
10:12:07.784 My Connections\NAT-T Demo - Established IKE SA
10:12:07.784    MY COOKIE e1 d 34 19 b4 4d 0 fc
10:12:07.784    HIS COOKIE 5e e9 de 51 86 5c b2 e0
10:12:07.795 My Connections\NAT-T Demo - Initiating IKE Phase 2 with Client IDs (message
id: A6A0FDA7)
10:12:07.795   Initiator = IP ADDR=10.128.0.2, prot = 0 port = 0
10:12:07.795   Responder = IP SUBNET/MASK=192.168.79.0/255.255.255.0, prot = 0 port = 0
10:12:07.795 My Connections\NAT-T Demo - SENDING>>>> ISAKMP OAK QM *(HASH,
SA, NON, ID, ID)
10:12:07.795 My Connections\NAT-T Demo - RECEIVED<<< ISAKMP OAK QM *(HASH, SA,
NON, NOTIFY:STATUS_RESP_LIFETIME)
10:12:07.795 My Connections\NAT-T Demo - SENDING>>>> ISAKMP OAK QM *(HASH)
10:12:07.795 My Connections\NAT-T Demo - Loading IPSec SA (Message ID = A6A0FDA7
OUTBOUND SPI = 3EB86823 INBOUND SPI = E72195D8)
10:12:07.795
```

Connection Monitor

The Connection Monitor shows statistical and diagnostic information for each active connection. This includes the actual security policy settings configured in the security policy and the security association (SA) information established during Phase 1 IKE negotiations and Phase 2 IPSec negotiations.

To view details for a specific entry, go to View an active connection's details.

- In the Windows system tray, right-click the **client icon**, and then click **Connection Monitor**. The **Connection Monitor** opens.



Global Statistics

Non-Secured Packets: 301431

Secured Packets: 0

Dropped Packets: 0

Secured Data (KBytes): 0

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port

In the **Connection Name** column, the icon that precedes the connection name provides connection information:

Table 9-2: Connection Monitor Terms and Icons

Image	Definition
SA	Connection has only a Phase 1 IKE SA. This occurs when connecting to a secure gateway tunnel or when a Phase 2 IPSec SA or hasn't established yet or fails to establish.
🔑	Connection has a Phase 2 IPSec SA or both a Phase 1 and Phase 2 SA. **Note:** When a single Phase 1 SA to a gateway protects multiple Phase 2 SAs, one Phase 1 connection displays below these Phase 2 SAs entries.
🔑	Client is processing secure IP traffic for that connection.

Notes:

- **Global Statistics** values are not real-time; they are updated every five seconds.
- **Remote Modifier** is either the remote party's subnet mask or the end of the address range when the **ID Type** selected in the **Remote Party Identity and Addressing** group is **IP Address Range**.

The **Security Association Details** dialog box displays IKE (Phase 1) information, IPSec (Phase 2) information, or both for a specific connection entry in the Connection Monitor.

1. In the Connection Monitor, click the specific connection entry.
2. Click **Details**. The **Security Association Details** dialog box opens with a **Phase 1** tab, **Phase 2** tab, or both, based on whether the entry represents a Phase 1 SA, Phase 2 SA, or both.
3. If both tabs appear, click the one with the details to view:
   - To view Authentication (Phase 1) SAs negotiated by IKE, click the **Phase 1** tab.

   Note: Private Addr is the internal IP address.

   - To view Key Exchange (Phase 2) SAs negotiated by IPSec, click the **Phase 2** tab.
4. To exit the dialog box, click **Close**.

Manual keys

Manual keys are IPSec encryption and authentication keys that you type in instead of having the client generate them automatically. They eliminate the need for a certificate or preshared keys and all IKE negotiations during Authentication (Phase 1) and Key Exchange (Phase 2). They are designed to help you determine if secure communications are possible.

Warning! Manual keys are intended for troubleshooting problem connections only. Because the process of distributing these keys is not secure, do not include them in an ongoing security policy.

After you Enable manual keys in the Security Policy Editor, the client makes two buttons available on the right pane when you Configure the Key Exchange (Phase 2) proposal: **Inbound Keys** and **Outbound Keys**. Why two buttons? Because the secure connection between the two parties transmits communications in two directions: incoming and outgoing.

You and the remote party must enter the same keys, but in the reverse order. The key that you enter as an inbound key is entered by the remote party as an outbound key, and vice versa, as this illustration shows:

Your computer		Remote party
inbound key	<-->	outbound key
outbound key	<-->	inbound key

Each direction requires a separate key. The encryption or hash algorithm that you selected when enabling manual keys determines the exact key length. For a list of these key lengths, go to Enter manual keys.

Enable Manual Keys

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the specific secure connection.
2. For this connection, click **My Identity**.
3. In the **Select Certificate** box, in the My Identity group, click **None**.
4. For the selected connection, expand **Security Policy**.
5. In the right pane, in the **Select Phase 1 Negotiation Mode** group, click **Use Manual Keys**.
6. In the **Network Security Policy** list, expand **Key Exchange (Phase 2)**.
7. Click the specific proposal.
8. In the IPSec Protocols group, **Encapsulation Protocol (ESP)** and **Authentication Protocol (AH)** are mutually exclusive check boxes:
   - To encrypt and authenticate the data, select the **Encapsulation Protocol (ESP)** check box.

   a. In the **Encryption Algorithm** box, click an option:

      – For minimal security, **DES**

      – For medium security, **Triple-DES** (the default)

      – For maximum security, **AES-128**, **AES-192**, or **AES-256**

      – For no security, **Null**

      Record your selection; you need it to determine the length of the key for the **ESP Encryption Key** box when entering inbound and outbound keys.

   b. In the **Hash Algorithm** box, click an option:

- For minimal security, **MD5**
- For maximum security, **SHA-1** (the default)
- DES-MAC

Record your selection; you need it to determine the length of the key for the **ESP Authentication Key** box when entering inbound and outbound keys.

c. In the **Encapsulation** box, accept **Tunnel** (the default) or click **Transport**.

Note: If you selected the **Connect using** check box and a gateway when you configured All Connections or a specific connection to be secured, **Tunnel** is the only option.

- To ensure that the data has not been altered, select the **Authentication Protocol (AH)** check box.

a. In the **Hash Algorithm** box, click an option:

- **MD5** for minimal security
- **SHA-1** for maximum security (the default)

Record your selection; you need it to determine the length of the key for the **AH Authentication Key** box when entering inbound and outbound keys.

b. In the **Encapsulation** box, accept **Tunnel** (the default) or click **Transport**.

Note: If you selected the **Connect using** check box and a gateway when you configured All Connections or a specific connection to be secured, **Tunnel** is the only option.

- Make sure that the remote party configures the same options in its VPN software.

9. Enter inbound and outbound manual keys.
10. Click **Save**.

Enter Inbound and Outbound Manual Keys

Before you perform this task, make sure that the particular connection is Enabled for manual keys.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the secure connection 🔒.
2. Expand **Security Policy**.
3. Expand **Key Exchange (Phase 2)**.
4. Click the proposal to enter manuals keys for.

5. In the right pane, click one key type: **Inbound Keys** or **Outbound Keys**. The **Inbound** or **Outbound Keying Material** dialog box opens.
6. In the **Security Parameters Index** box, type the same value, a number with a maximum of 8 digits, the remote party sets for this parameter. The default is **100**.
7. Click **Enter Key**. Specific boxes in the Keys group become available, based on the check box selected in the IPSec Protocols group when manual keys were enabled:

Table 9-3: Inbound and Outbound Keys

Selected Check Box	Enabled Options
Authentication Protocol (AH)	Choose Key Format
	AH Authentication Header
Encapsulation Protocol (ESP)	Choose Key Format
	ESP Encryption Key
	ESP Authentication Key

8. In the **Choose Key Format** box, accept **Binary** (the default) or click **ASCII**.
9. In the available boxes, enter the particular keys. The key length is based on the encryption or hash algorithm selected in the IPSec Protocols group when manual keys were enabled:

Table 9-4: Key Lengths

Algorithm	Key Length:	
	ASCII	Binary
DES	8	16
Triple-DES	24	48
AES-128	128	16
AES-192	192	24
AES-256	256	32
MD5	16	32
SHA-1	20	40

10. Click **OK**.
11. Repeat steps 5 through 10 for the other key type, **Inbound Keys** or **Outbound Keys**.
12. Click **Save**. A yellow key displays in the **client icon** .

Start a Secure Connection with Manual Keys

After you Enable and Enter manual keys for connection troubleshooting, establish a VPN with the remote party using one of these methods:

- From a command prompt, ping the other computer.
- In Windows Explorer, map a drive on the other computer.

Note: Because IKE is not used with manual keys, the client logs no IKE negotiation messages in the Log Viewer.

Disable Manual Keys

When you complete using manual keys for troubleshooting, you can return to the original settings.

1. In the Security Policy Editor, in the **Network Security Policy** list, expand the secure connection you were troubleshooting with manual keys.
2. Are you using certificates or preshared keys?

- If you're using certificates:
  - Click **My Identity**.
  - In the **Select Certificate** box, click a personal certificate. Your original settings are restored.
- If you're using preshared keys:
  - Click **Security Policy**.
  - In the Select Phase 1 Negotiation Mode group, click **Main Mode** or **Aggressive Mode**. Your original settings are restored.

3. Click **Save**.

Appendix A
Networks, Routing, and Firewall Basics

This chapter provides an overview of IP networks, routing, and firewalls.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The NETGEAR ProSafe VPN Client is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The NETGEAR VPN Client supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

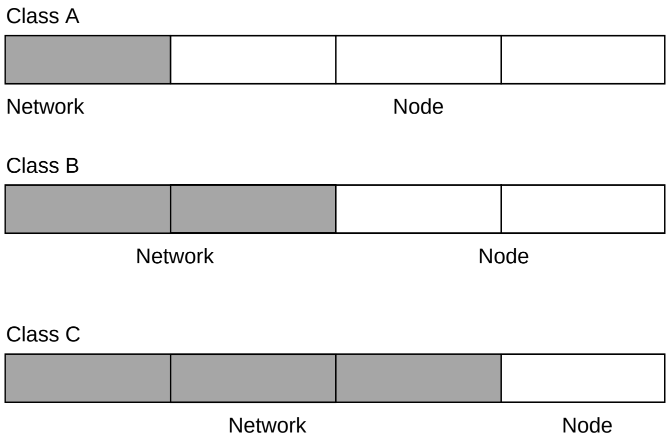


Figure A-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

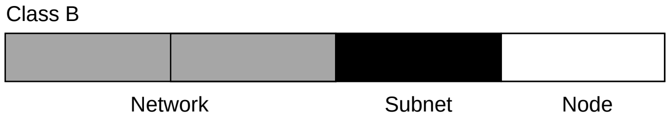


Figure A-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table A-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the mask length formats.

Table A-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Table A-2. Netmask Formats

255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the NETGEAR VPN Client is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The NETGEAR VPN Client employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

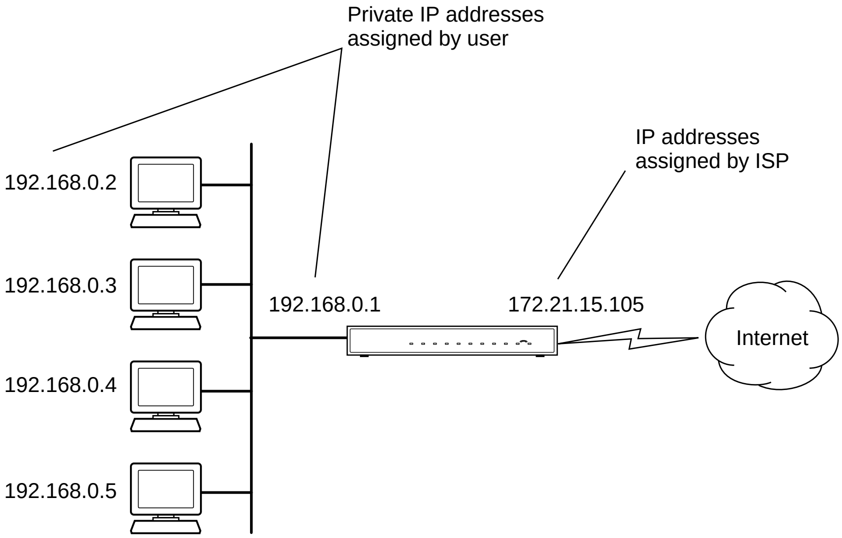


Figure A-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The NETGEAR VPN Client has the capacity to act as a DHCP server.

The NETGEAR VPN Client also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker’s IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Appendix B
Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

A VPN is a shared network where private data is segmented from other traffic so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security, which allows data attackers to tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

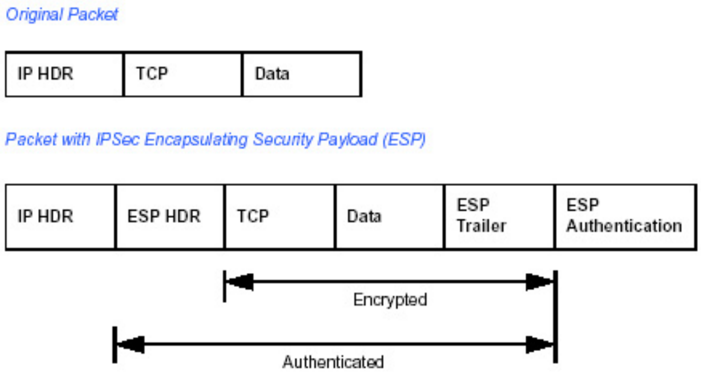


Figure B-1: Original packet and packet with IPSec Encapsulated Security Payload

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

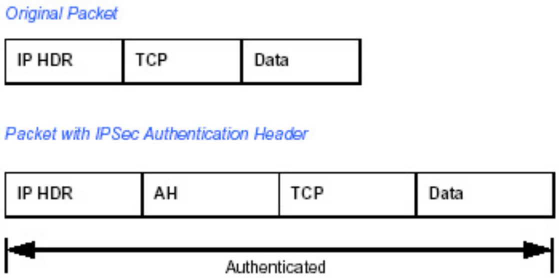


Figure B-2: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.
- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

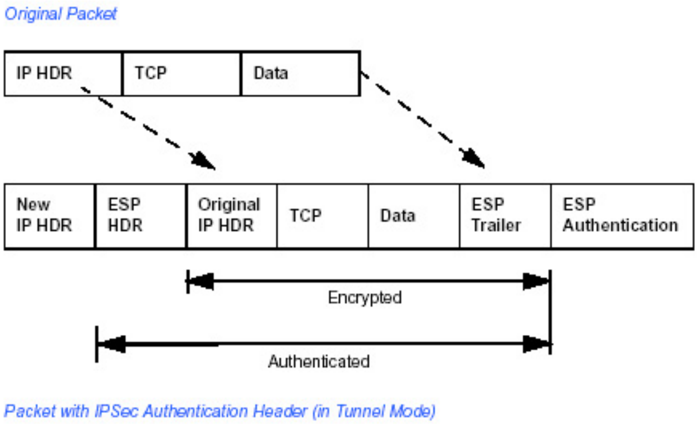


Figure B-3: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. Additional information regarding inter-vendor interoperability may be found at *http://www.vpnc.org/interop.html*.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN. The brief description in this document will help. Other good sources include:

- The NETGEAR VPN Tutorial – http://www.netgear.com/planetvpn/pvpn_2.html
- The VPN Consortium – http://www.vpnc.org/
- The VPN bibliography in “Additional Reading“ on page B-11.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into to the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a “gatekeeper” for each of the computers connected on the Local Area Network behind it.

In most cases, each Gateway will have a “public” facing address (WAN side) and a “private” facing address (LAN side). These addresses are referred to as the “network interface” in documentation regarding the construction of VPN communication. Please note that the addresses used in the example.

Interface Addressing

This TechNote uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

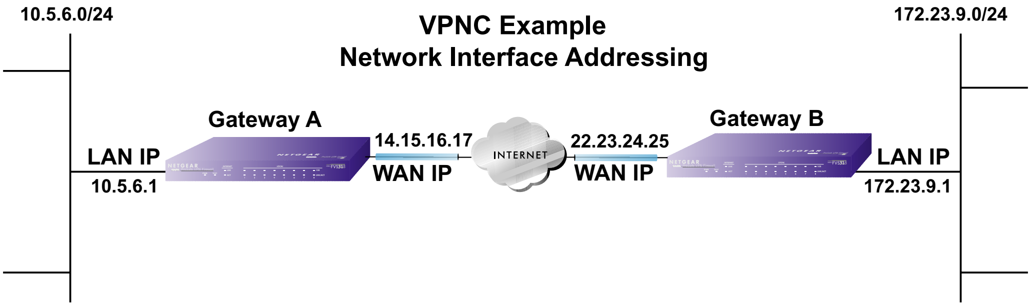


Figure B-4: VPNC Example Network Interface Addressing

It is also important to make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table B-1. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

It will also be important to know the subnet mask of both gateway LAN Connections. Use the worksheet in Appendix A to gather the necessary address and subnet mask information to aid in the configuration and troubleshooting process.

Table B-2. Subnet Addressing

Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

Setting Up a VPN Tunnel Between Gateways

A SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to “trust each other” and communicate securely as they pass information over the Internet.

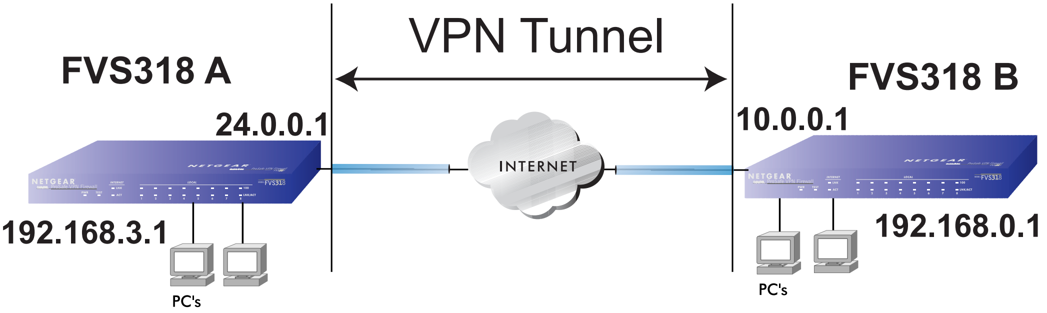


Figure B-5: VPN Tunnel SA

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a “tunnel.” The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.

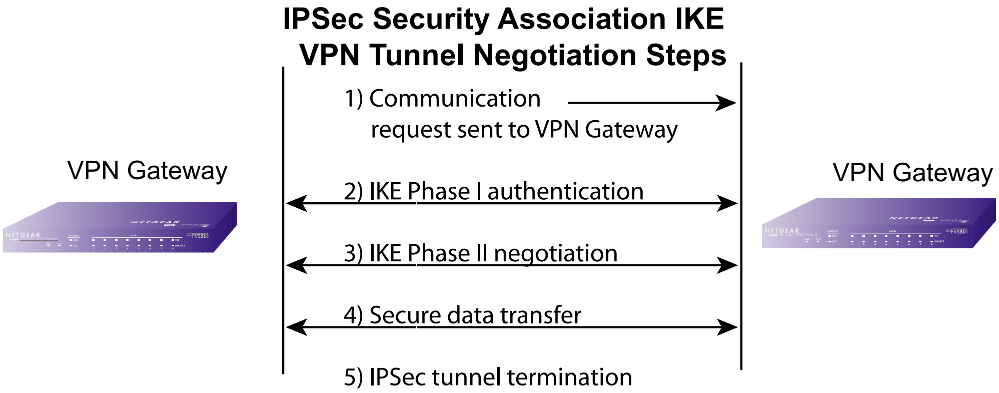

IPSec Security Association IKE
VPN Tunnel Negotiation Steps
1) Communication
request sent to VPN Gateway
VPN Gateway
2) IKE Phase I authentication
VPN Gateway
3) IKE Phase II negotiation
4) Secure data transfer
5) IPSec tunnel termination

Figure B-6: IPSec SA negotiation

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. **IKE Phase I.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
   b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
   c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.
3. **IKE Phase II.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
   b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these TechNote examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN-side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the Netgear gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A vs. Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).
- [RFC 2409] D. Harkins, D.Carrel, Internet Key Exchange (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

Appendix C
NETGEAR ProSafe VPN Client to NETGEAR FVS318 or FVM318 VPN Routers

Follow these procedures to configure a VPN tunnel from a NETGEAR ProSafe VPN Client to an FVS318 or FVM318. This document follows the VPN Consortium interoperability guidelines. The configuration options and screens for the FVS318 and FVM318 are the same.

Configuration Summary

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Assure that there are no firewall restrictions.

Table C-1. Configuration Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		PC/Client-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		November 2003
Model/Firmware Tested:		
	Gateway	FVS318 firmware version 2.2 or FVM318 firmware version 1.1
	Client	NETGEAR ProSafe VPN Client v10.1
IP Addressing:		
	Gateway	Fully Qualified Domain Name (FQDN)
	Client	Dynamic

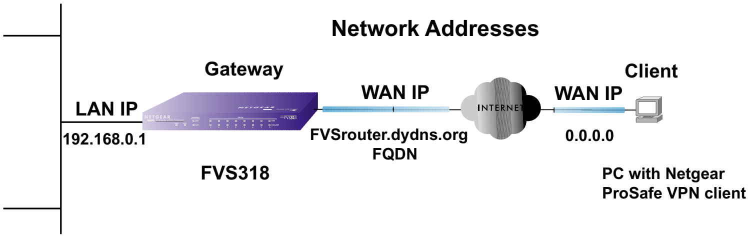


Figure C-1: Addressing and Subnets Used for Examples

The Use of a Fully Qualified Domain Name (FQDN)

Many ISPs provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time which presents a challenge for gateways attempting to establish VPN connectivity.

➡	**Note:** This configuration case study is based on the FVS318 using FQDN. FQDN is the best option when the Internet connection for the FVS318 uses a dynamic IP configuration rather than a static IP configuration. However, the steps below can be used when the FVS318 has a static IP configuration as well.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host name or domain name. It provides a central public database where information (such as email addresses, host names and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a 3rd party service in lieu of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Example DDNS Service Providers include:

Table C-1. Example DDNS Service Providers

DynDNS	www.dyndns.org
TZO.com	netgear.tzo.com
ngDDNS	ngddns.iego.net

In this example, gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **FVSrouter.dyndns.org** for gateway A using the DynDNS service. Client B will use the host name registered with the DDNS Service Provider for gateway A when establishing a VPN tunnel.

In order to establish VPN connectivity, client B must be configured to use a DNS hostname provided by the Gateway A DDNS Service Provider. The following step-by-step procedures assume that you have already registered with a DDNS Service Provider and have the configuration information necessary to set up the gateway and client.

> ➡ **Note:** Product updates are available on the NETGEAR Web site at *www.netgear.com/support/main.asp*. VPNC Interoperability guidelines can be found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 gateway as in the illustration.

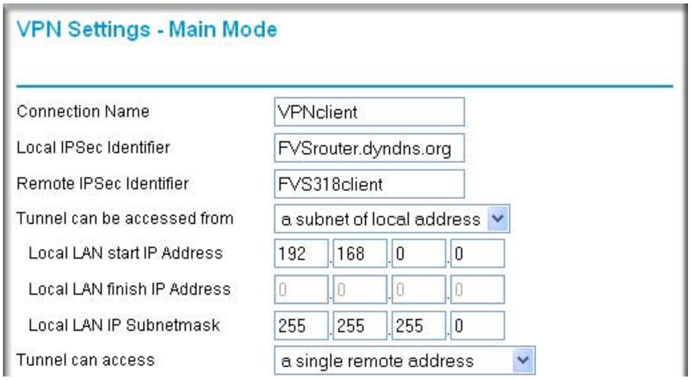
   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**.

   For this example we will assume you set the local LAN address as 10.5.6.1 for the FVS318.

2. Click on the VPN Settings link on the left side of the main menu.

   – *For a FVS318*: Click the radio button of the first available VPN tunnel. Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.

   – *For a FVM318*: Click Add. This will take you to the VPN Settings – Main Mode Menu.



VPN Settings - Main Mode

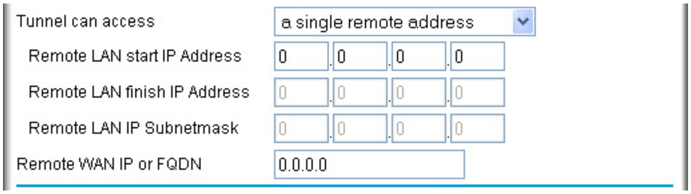
Connection Name	VPNclient
Local IPSec Identifier	FVSrouter.dyndns.org
Remote IPSec Identifier	FVS318client
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	192 . 168 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a single remote address

Figure C-2: NETGEAR FVS318 VPN Settings – Main Mode

- In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **VPNclient**.
- Enter a Local IPSec Identifier for the NETGEAR FVS318 Gateway A. In this example we used **FVSrouter.dyndns.org** as the local identifier.

> **Note:** It is critical that the information entered for the Local IPSec Identifier match exactly what you configure in the NETGEAR VPN Client ID Type menus. Please see "Configure the Connection Network Settings." on page C-7 below.

- Enter a Remote IPSec Identifier name for the remote NETGEAR VPN Client. In this example we used **VPNclient** as the remote identifier.
- Choose "a subnet of local addresses" from the "Tunnel can be accessed from" menu.
- Type the starting LAN IP Address of Gateway A (**192.168.0.0** in our example) in the Local IP Local LAN start IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Local LAN IP Subnetmask field.
- Choose **A Single Remote Address** from the "Tunnel can access" pull-down menu.



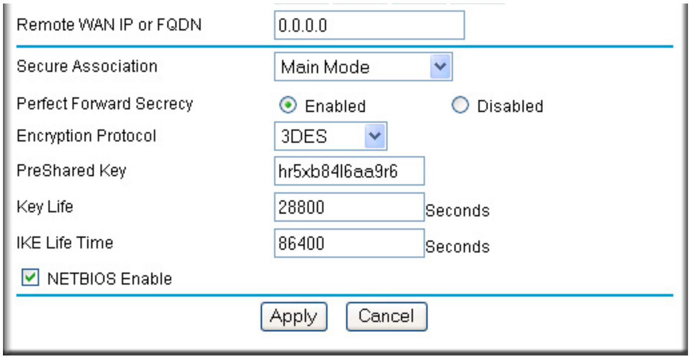
Tunnel can access	a single remote address
Remote LAN start IP Address	0 . 0 . 0 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	0 . 0 . 0 . 0
Remote WAN IP or FQDN	0.0.0.0

Figure C-3: NETGEAR FVS318 VPN Settings – Main Mode

– Type the IP Address of client B (**0.0.0.0** in our example) in the Remote LAN Start IP Address field. Entering 0.0.0.0 as the Remote LAN Start IP Address tells the FVS318 to accept a connection from any IP address. This enables travelling users who will not know the IP address of their connection to use this tunnel. It also allows telecommuters who have a direct connection at their home with a dynamic IP address to use this tunnel.

Note: Entering 0.0.0.0 as the Remote LAN Start IP Address uses two of the available 8 FVS318 tunnels. If you wish to provide a tunnel for home users who are connecting through a home NAT router, use a reserved IP configuration for the PC on the home router. Specifying a reserved IP address for a PC on the home NAT router assures that PC will always receive the same IP address from the DHCP server in the home NAT router. In such a case, you would enter the reserved IP address of the PC for the Remote LAN Start IP Address. To avoid duplicate IP address conflicts, be sure the remote PC IP address is on a different subnet than the FVS318.

– Leave the Remote WAN IP or FQDN address field blank.



Remote WAN IP or FQDN	0.0.0.0	
Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	3DES	
PreShared Key	hr5xb84l6aa9r6	
Key Life	28800	Seconds
IKE Life Time	86400	Seconds
☑ NETBIOS Enable		

Figure C-4: NETGEAR FVS318 VPN Settings – Main Mode

– From the Secure Association drop-down box, select **Main Mode**.

– Next to Perfect Forward Secrecy, select the **Enabled** radio button.

– From the Encryption Protocol drop-down box, select **3DES**.

– In the PreShared Key box, type a unique text string to be used as the shared key between the FVS318 and the VPN client. In this example, we used **hr5xb84l6aa9r6**. You must make sure the key is entered correctly in both the gateway and the client.

– In the Key Life box, enter **28800** seconds.

– In the IKE Life Time, enter **86400** seconds.

   - Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions such as Microsoft Network Neighborhood browsing.

3. Click **Apply** to save all changes. This will return you to the VPN Settings screen.
4. When the screen returns to the VPN Settings, make sure the Enable checkbox is selected.

Step-By-Step Configuration of the NETGEAR VPN Client B

> **Note:** The NETGEAR ProSafe VPN Client has the ability to "Import" a predefined configuration profile. The FVS318.SPD file on the NETGEAR ProSafe VPN Client *Resource CD (230-10007-01)* includes all the settings identified in this procedure.
>
> Whenever importing policy settings, you should first export any existing settings you may have configured to prevent the new imported settings from replacing an existing working configuration.
>
> To import this policy, use the Security Policy Editor File menu to select Import Policy, and select the FVS318.SPD file at D:\Software\Policies where D is the drive letter of your CD-ROM drive.

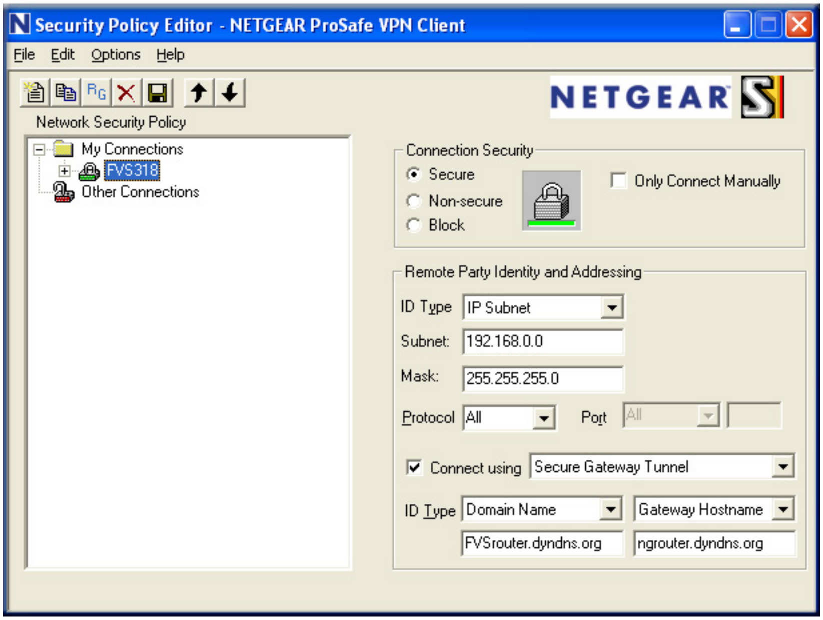
This procedure describes linking a remote PC and a LAN. The LAN will connect to the Internet using an FVS318 with a dynamic address and a dynamic DNS host name. The PC can be directly connected to the Internet through dialup, cable or DSL modem, or other means, and we will assume it has a dynamically assigned IP address.

1. **Install the NETGEAR VPN Client Software on the PC.**

> **Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

- You may need to insert your Windows CD to complete the installation.
- Reboot your PC after installing the client software.

2. Configure the Connection Network Settings.



Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.0.0
Mask: 255.255.255.0
Protocol: All   Port: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name   Gateway Hostname
FVSrouter.dyndns.org   ngrouter.dyndns.org

Figure C-5: Security Policy Editor New Connection

a. Run the Security Policy Editor program and create a VPN Connection.

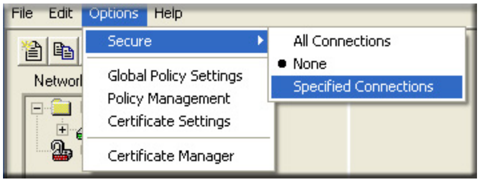


Figure C-6: Security Policy Editor Options menu

Note: If the configuration settings on this screen are not available for editing, go to the Options menu, select Secure, and Specified Options to enable editing of these settings.

From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**. A “New Connection” listing appears. Rename the “New Connection” to **FVS318**.

b. In this example, type **192.168.0.0** in the Subnet field. The network address is the LAN IP Address of the FVS318 with 0 as the last number.

c. Enter **255.255.255.0 i**n the Mask field as the LAN Subnet Mask of the FVS318

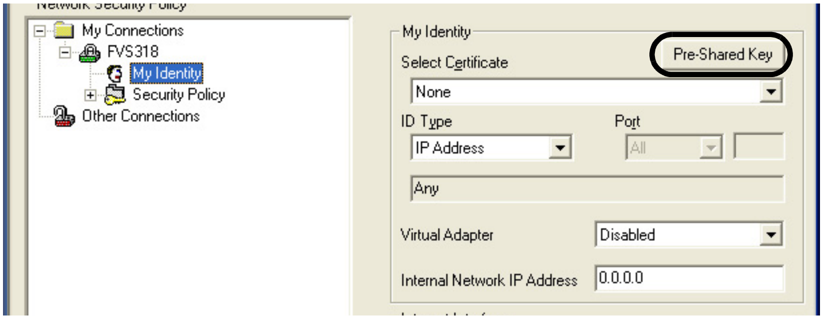
d. Assure that the following settings are configured:

- In the Connection Security box, Secure is selected
- In the ID Type menu, IP Subnet is selected
- In the Protocol menu, All is selected
- The Connect using Secure Gateway Tunnel checkbox is checked

e. In the ID Type menus, select Domain Name and Gateway Hostname. Enter the public FQDN of the FVS318 in the field directly below the ID Type menu. In this example, **FVSrouter.dyndns.org** would be used for both the Domain Name and Gateway Hostname.

3. Configure the Connection Identity Settings.

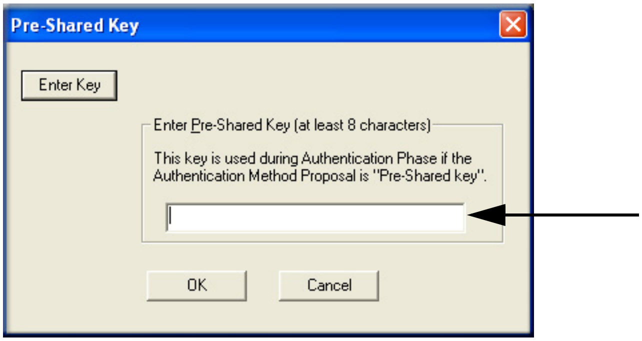
a. In the Network Security Policy list, click the My Identity subheading.



Select Certificate: None
ID Type: IP Address
Port: All
Any
Virtual Adapter: Disabled
Internal Network IP Address: 0.0.0.0

Figure C-7: Connection Identity

b. Click **Pre-Shared Key**.



This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

In this example, enter this pre-shared key in this field: **hr5xb84l6aa9r6**

Figure C-8: Connection Identity Pre-Shared Key

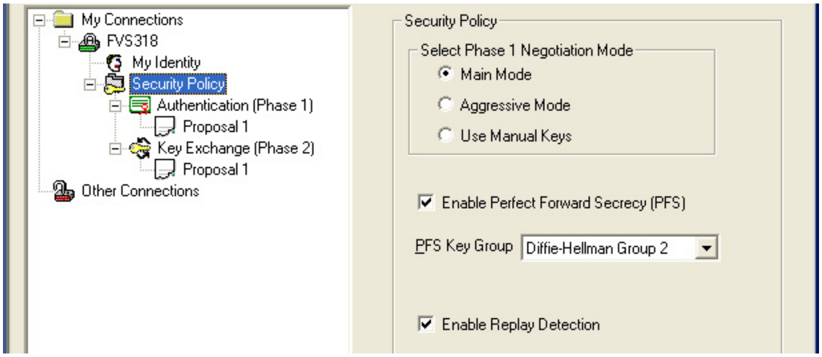
c. Enter the same Pre-Shared Key used in the FVS318 VPN router.

In this example, we used **hr5xb84l6aa9r6.**

d. Click **OK**.

4. Configure the Security Policy Settings.

a. In the Network Security Policy list, click the Security Policy subheading.



Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

Figure C-9: Security Policy

b. For this example, assure that the following settings are configured:

– In the Select Phase 1 Negotiation Mode menu, select **Main Mode**.

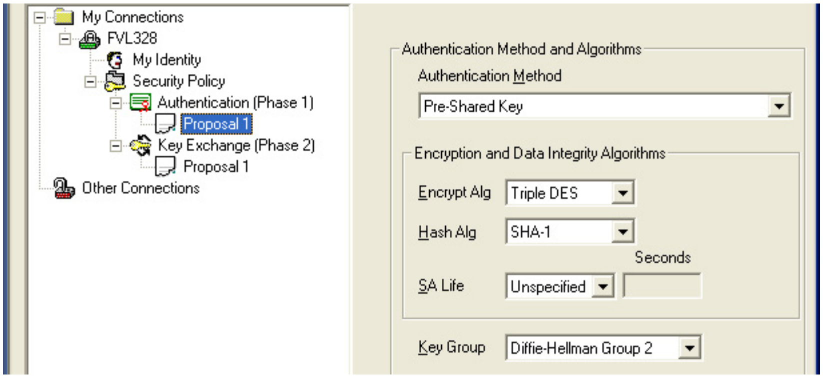
– Check the **Enable Perfect Forward Secrecy (PFS)** checkbox.

– In the PFS Key Group drop-down list, **Diffie-Hellman Group 2**.

– Check the Enable Replay Detection checkbox.

c. Configure the Connection Security Policy

In this step, you will provide the authentication (IKE Phase 1) settings, and the key exchange (Phase 2) settings. The setting choices in this procedure follow the VPNC guidelines.



My Connections
FVL328
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Proposal 1
Other Connections

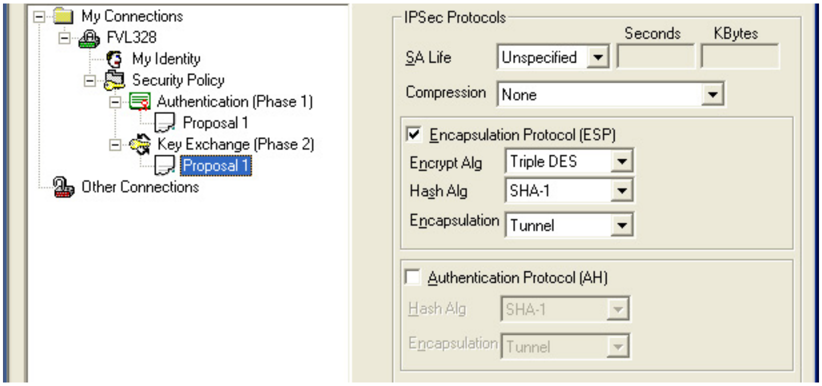
Authentication Method and Algorithms
Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms
Encrypt Alg: Triple DES
Hash Alg: SHA-1
SA Life: Unspecified; Seconds:
Key Group: Diffie-Hellman Group 2

Figure C-10: Connection Security Policy Authentication (Phase 1)

– Configure the Authentication (Phase 1) Settings.

- Expand the Security Policy heading, then expand the Authentication (Phase 1) heading, and click on Proposal 1.
- For this example, assure that the following settings are configured:
  – In the Encrypt Alg menu, select **Triple DES**.
  – In the Hash Alg, select **SHA-1**.
  – In the SA Life, select Unspecified.
  – In the Key Group menu, select **Diffie-Hellman Group 2**.



My Connections
FVL328
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Proposal 1
Other Connections

IPSec Protocols
SA Life: Unspecified; Seconds: ; KBytes:
Compression: None

☑ Encapsulation Protocol (ESP)
Encrypt Alg: Triple DES
Hash Alg: SHA-1
Encapsulation: Tunnel

☐ Authentication Protocol (AH)
Hash Alg: SHA-1
Encapsulation: Tunnel

Figure C-11: Connection Security Policy Key Exchange (Phase 2)

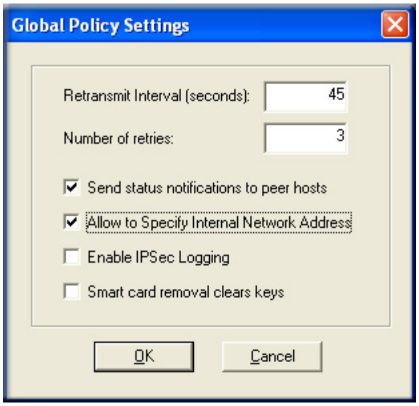
– Configure the Key Exchange (Phase 2).

- Expand the Key Exchange (Phase 2) heading, and click on Proposal 1.

- For this example, assure that the following settings are configured:
  - In the SA Life menu, select Unspecified.
  - In the Compression menu, select None.
  - Check the **Encapsulation Protocol (ESP)** checkbox.
  - In the Encrypt Alg menu, select **Triple DES**.
  - In the Hash Alg, select **SHA-1**.
  - In the Encapsulation menu, select Tunnel.

5. **Configure the Global Policy Settings.**

   a. From the Options menu at the top of the Security Policy Editor window, select Global Policy Settings.



Global Policy Settings

Retransmit Interval (seconds): 45

Number of retries: 3

☑ Send status notifications to peer hosts

☑ Allow to Specify Internal Network Address

☐ Enable IPSec Logging

☐ Smart card removal clears keys

Figure C-12: Security Policy Editor Global Policy Options

   b. Increase the Retransmit Interval period to **45** seconds.

   c. Check the Allow to Specify Internal Network Address checkbox and click **OK**.

6. **Save the VPN Client Settings.**

   From the File menu at the top of the Security Policy Editor window, select Save. After you have the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router’s LAN.

Note: Whenever you make changes to a Security Policy, save them first, then deactivate the security policy, reload the security policy, and finally activate the security policy. This assures that your new settings will take effect.

Testing the VPN Connection

You can test the VPN connection in several ways:

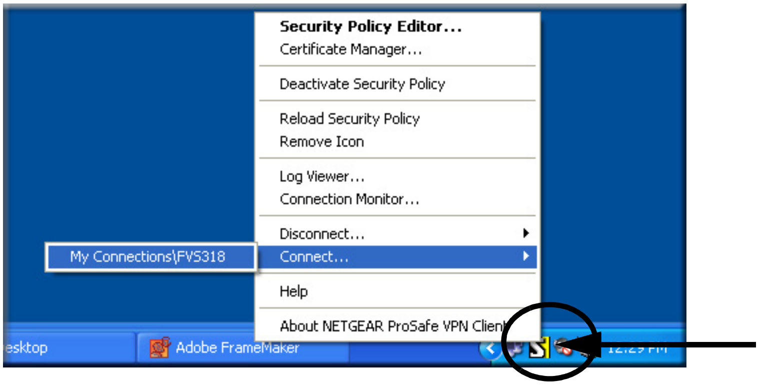
- From the client PC to the FVS318
- From the FVS318 to the client PC

These procedures are explained below.

Note: Virus protection or firewall software can interfere with VPN communications. Be sure such software is not running on the remote PC with the NETGEAR VPN Client and that the firewall settings of the FVS318 do not prevent VPN communications.

From the Client PC to the FVS318

To check the VPN Connection, you can initiate a request from the remote PC to the FVS318 by using the "Connect" option of the NETGEAR VPN Client popup menu.



Right-mouse-click on the system tray icon to open the popup menu.

Figure C-13: Connecting the PC the FVS318 over the VPN tunnel

1. Open the popup menu by right-clicking on the system tray icon.
2. Select **Connect** to open the My Connections list.
3. Choose **FVS318**.

   The NETGEAR VPN Client will report the results of the attempt to connect.

Once the connection is established, you can access resources of the network connected to the FVS318.

Another method is to ping from the remote PC to the LAN IP address of the FVS318. To perform a ping test using our example, start from the remote PC:

1. Establish an Internet connection from the PC.
2. On the Windows taskbar, click the Start button, and then click Run.
3. Type **`ping -t 192.168.0.1`**, and then click OK.

   This will cause a continuous ping to be sent to the first FVS318. After a period of up to two minutes, the ping response should change from “timed out” to “reply.”

   To test the connection to a computer connected to the FVS318, simply ping the IP address of that computer.

Once connected, you can open a browser on the remote PC and enter the LAN IP Address of the FVS318, which is http://192.168.0.1 in this example. After a short wait, you should see the login screen of the FVS318.

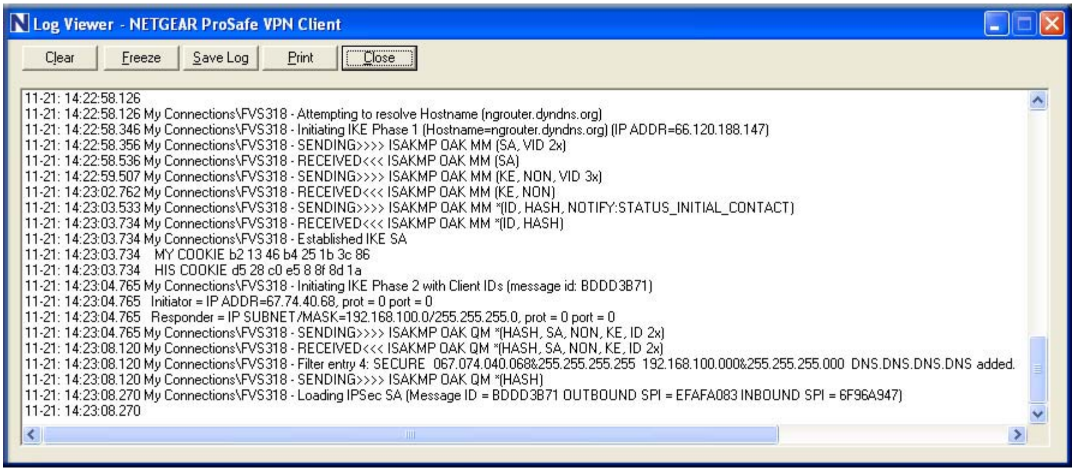
From the FVS318 to the Client PC

You can use the FVS318 Diagnostic utilities to test the VPN connection from the FVS318 to the client PC. Run ping tests from the Diagnostics link of the FVS318 main menu.

Monitoring the VPN Connection from the PC

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR VPN Client Connection Monitor or Log Viewer. To launch these functions, click on the Windows Start button, then select Programs, then NETGEAR ProSafe VPN Client, then either the Connection Monitor or Log Viewer.

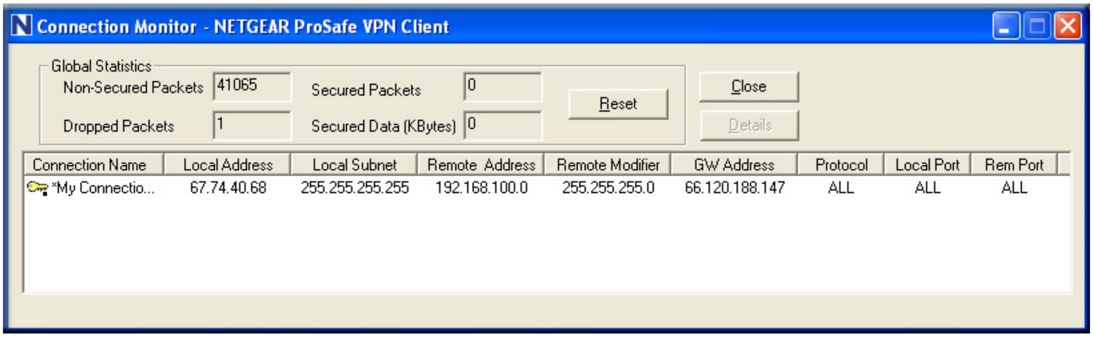
The Log Viewer screen for a successful connection is shown below:



```
11-21: 14:22:58.126
11-21: 14:22:58.126 My Connections\FVS318 - Attempting to resolve Hostname (ngrouter.dyndns.org)
11-21: 14:22:58.346 My Connections\FVS318 - Initiating IKE Phase 1 (Hostname=ngrouter.dyndns.org) (IP ADDR=66.120.188.147)
11-21: 14:22:58.356 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM (SA, VID 2x)
11-21: 14:22:58.536 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM (SA)
11-21: 14:22:59.507 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM (KE, NON, VID 3x)
11-21: 14:23:02.762 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM (KE, NON)
11-21: 14:23:03.533 My Connections\FVS318 - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
11-21: 14:23:03.734 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
11-21: 14:23:03.734 My Connections\FVS318 - Established IKE SA
11-21: 14:23:03.734    MY COOKIE b2 13 46 b4 25 1b 3c 86
11-21: 14:23:03.734    HIS COOKIE d5 28 c0 e5 8 8f 8d 1a
11-21: 14:23:04.765 My Connections\FVS318 - Initiating IKE Phase 2 with Client IDs (message id: BDDD3B71)
11-21: 14:23:04.765   Initiator = IP ADDR=67.74.40.68, prot = 0 port = 0
11-21: 14:23:04.765   Responder = IP SUBNET/MASK=192.168.100.0/255.255.255.0, prot = 0 port = 0
11-21: 14:23:04.765 My Connections\FVS318 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-21: 14:23:08.120 My Connections\FVS318 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-21: 14:23:08.120 My Connections\FVS318 - Filter entry 4: SECURE  067.074.040.068&255.255.255.255  192.168.100.000&255.255.255.000  DNS.DNS.DNS.DNS added.
11-21: 14:23:08.120 My Connections\FVS318 - SENDING>>>> ISAKMP OAK QM *(HASH)
11-21: 14:23:08.270 My Connections\FVS318 - Loading IPSec SA (Message ID = BDDD3B71 OUTBOUND SPI = EFAFA083 INBOUND SPI = 6F96A947)
11-21: 14:23:08.270
```

Figure C-14: Log Viewer screen

A sample Connection Monitor screen for a different connection is shown below:



Global Statistics

Non-Secured Packets: 41065

Secured Packets: 0

Dropped Packets: 1

Secured Data (KBytes): 0

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
*My Connectio...	67.74.40.68	255.255.255.255	192.168.100.0	255.255.255.0	66.120.188.147	ALL	ALL	ALL

Figure C-15: Connection Monitor screen

In this example you can see the following:

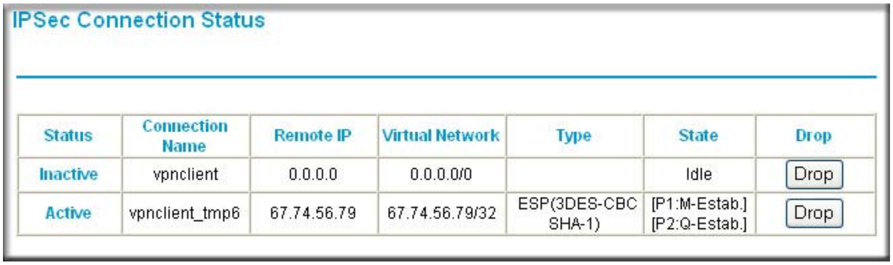
- The FVS318 has a public IP WAN address of 66.120.188.147
- The FVS318 has a LAN IP address of 192.168.100.0
- The VPN client PC has a dynamically assigned address of 67.74.40.68

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

Monitoring the VPN Connection from the FVS318

Information on the status of the VPN client connection can be viewed by opening the FVS318 VPN Status screen. To view this screen, click the Router Status link of the FVS318 main menu, then click the VPN Status button.

The FVS318 VPN Status screen for a successful connection is shown below:



IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Inactive	vpnclient	0.0.0.0	0.0.0.0/0		Idle	Drop
Active	vpnclient_tmp6	67.74.56.79	67.74.56.79/32	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

Figure C-16: FVS318 IPSec Connection Status screen

To view the FVS318 VPN log, click on the Router Status link on the left side of the main menu. Click the Show VPN Logs button. The FVS818 or FVM318 log files should be similar to the example below:

```
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:Receive Packet address:0x13974d4 from 67.74.56.79
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:New State index:1, sno:4
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:quick_inI1_outR1()
Thur, 11/13/2003 10:32:24 - FVS318 IKE:[vpnclient_tmp6] RX << QM_I1 : 67.74.56.79
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:in get_ipsec_spi() spi=3834090c
Thur, 11/13/2003 10:32:24 - FVS318 IKE:[ESP_3DES/AUTH_ALGORITHM_HMAC_SHA1/In
SPI:3834090c,Out SPI:97baddc]
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:responding to Quick Mode
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:****Install INBOUND SA:
Thur, 11/13/2003 10:32:24 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
Thur, 11/13/2003 10:32:24 - FVS318 IKE:[vpnclient_tmp6] TX >> QM_R1 : 67.74.56.79
Thur, 11/13/2003 10:32:24 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for
#4
Thur, 11/13/2003 10:32:26 - FVS318 IPsec:Receive Packet address:0x13974d4 from 67.74.56.79
Thur, 11/13/2003 10:32:26 - FVS318 IPsec:quick_inI2()
Thur, 11/13/2003 10:32:26 - FVS318 IKE:[vpnclient_tmp6] RX << QM_I2 : 67.74.56.79
Thur, 11/13/2003 10:32:26 - FVS318 IPsec:****Install OUTBOUNDSA:
Thur, 11/13/2003 10:32:26 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
Thur, 11/13/2003 10:32:26 - FVS318 IKE:[vpnclient_tmp6] established with 67.74.56.79 successfully
Thur, 11/13/2003 10:32:26 - FVS318 IPsec:inserting event EVENT_SA_EXPIRE, timeout in 28980 seconds
for #4
Thur, 11/13/2003 10:32:26 - FVS318 IPsec:STATE_QUICK_R2: IPsec SA established
End of Log ----------
```

Appendix D
NETGEAR VPN Client
to NETGEAR FVL328 or FWAG114 VPN Router

Follow these procedures to configure a VPN tunnel from a NETGEAR ProSafe VPN Client to an FVL328. This case study follows the VPN Consortium interoperability profile guidelines. The configuration options for the FVS328 and FWAG114 are the same.

Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table D-1. Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		PC/Client-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		November 2003
Model/Firmware Tested:		
	Gateway	NETGEAR FVL328 firmware v 1.4 or FWAG114 firmware v 2.1
	Client	NETGEAR ProSafe VPN Client v10.1
IP Addressing:		
	Gateway	Static IP address
	Client	Dynamic

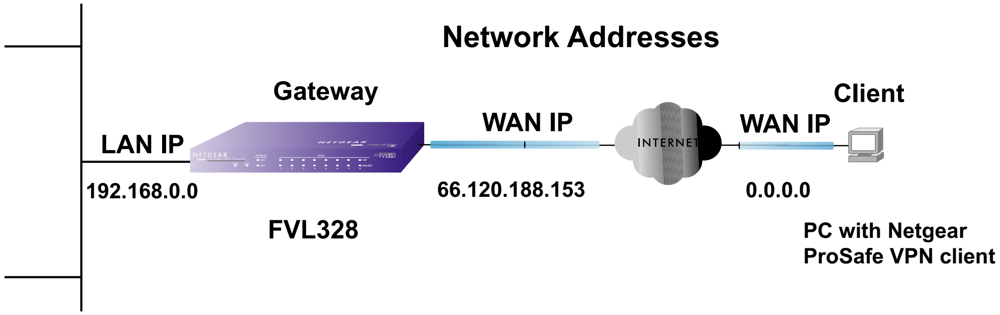


Figure D-1: Addressing and Subnet Used for Examples

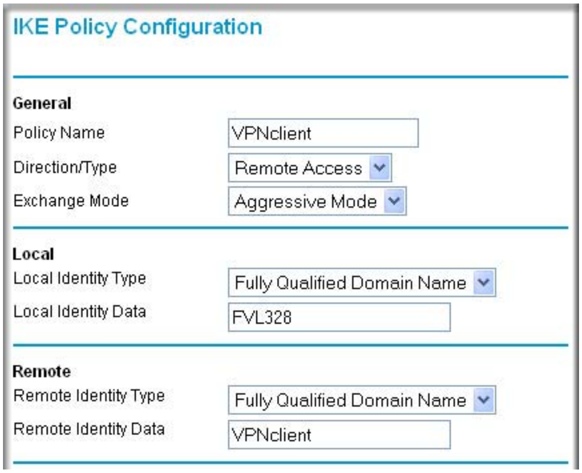
> **Note:** Product updates are available on the NETGEAR Web site at *www.netgear.com/support/main.asp*. VPNC Interoperability guidelines can be found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*.

Step-By-Step Configuration of FVL328 or FWAG114 Gateway

1. Log in to the FVL328 gateway as in the illustration.

   Out of the box, the FVL328 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. Even though the remainder of this document will refer to the FVL328, the login procedures and configuration menu screens are the same for the FVL328 and the FWAG114.

2. Click **IKE Policies** under the VPN menu and click **Add** on the IKE Policies Menu.



IKE Policy Configuration

General	
Policy Name	VPNclient
Direction/Type	Remote Access
Exchange Mode	Aggressive Mode
Local	
Local Identity Type	Fully Qualified Domain Name
Local Identity Data	FVL328
Remote	
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	VPNclient

Figure D-2: NETGEAR FVL328 IKE Policy Configuration

– Enter a descriptive name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example, we used **VPNclient** as the Policy Name.

– From the Direction/Type drop-down box, select **Remote Access**

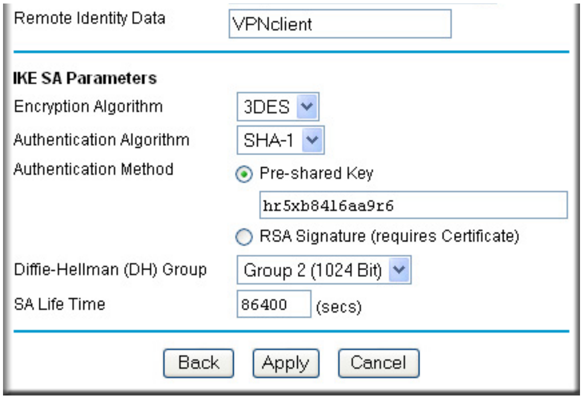
– From the Exchange Mode drop-down box, select **Aggressive Mode**. This will also be selected in the NETGEAR ProSafe VPN Client My Identity ID Type fields, as seen in "Security Policy" on page D-11.

– From the Local Identity drop-down box, select **Fully Qualified Domain Name** (the actual WAN IP address of the FVL328 will also be used in the Connection ID Type fields of the NETGEAR ProSafe VPN Client as seen in "Security Policy Editor New Connection" on page D-9).

– For this example we typed **FVL328** in the Local Identity Data field.

– From the Remote Identity drop-down box, select **Fully Qualified Domain Name**.

– Type **VPNclient** in the Remote Identity Data. This will also be entered in the NETGEAR ProSafe VPN Client My Identity ID Type fields, as seen in "My Identity" on page D-10.



Remote Identity Data: VPNclient

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared Key hr5xb84l6aa9r6 ○ RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

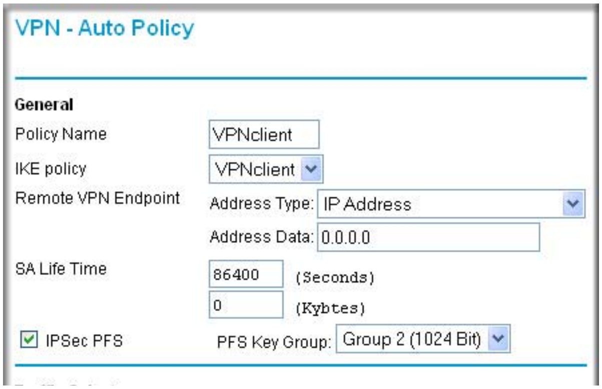
SA Life Time: 86400 (secs)

Figure D-3: NETGEAR FVL328 IKE Policy Configuration

- From the Encryption Algorithm drop-down box, select **3DES**. This will also be selected in the NETGEAR ProSafe VPN Client Security Policy Authentication Phase 1 Proposal 1 Encrypt Alg field, as seen in "Connection Security Policy Authentication (Phase 1)" on page D-12.
- From the Authentication Algorithm drop-down box, select **SHA-1**.This will also be selected in the NETGEAR ProSafe VPN Client Security Policy Authentication Phase 1 Proposal 1 Hash Alg field, as seen in "Connection Security Policy Authentication (Phase 1)" on page D-12.
- From the Authentication Method radio button, select **Pre-shared Key**. This will also be selected in the NETGEAR ProSafe VPN Client Security Policy Authentication Phase 1 Proposal 1 Authentication Method field, as seen in "Connection Security Policy Authentication (Phase 1)" on page D-12.
- In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both the FVL328 and the NETGEAR VPN Client. This will also be selected in the NETGEAR ProSafe VPN Client Security Policy Authentication Phase 1 Proposal 1 Encrypt Alg field, as seen in "Connection Identity Pre-Shared Key" on page D-11.
- From the Diffie-Hellman (DH) Group drop-down box, select **Group 2 (1024 Bit)**. This will also be selected in the NETGEAR ProSafe VPN Client Security Policy Authentication Phase 1 Proposal 1 Key Group field, as seen in "Connection Security Policy Authentication (Phase 1)" on page D-12.
- In the SA Life Time field, type **86400**.

Click **Apply**. This will bring you back to the IKE Policies Menu.The FVL328 IKE Policy is now displayed in the IKE Policies page.

3. Click the **VPN Policies** link under the VPN category on the left side of the main menu. This will take you to the VPN Policies Menu page. Click **Add Auto Policy**. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: VPNclient

IKE policy: VPNclient

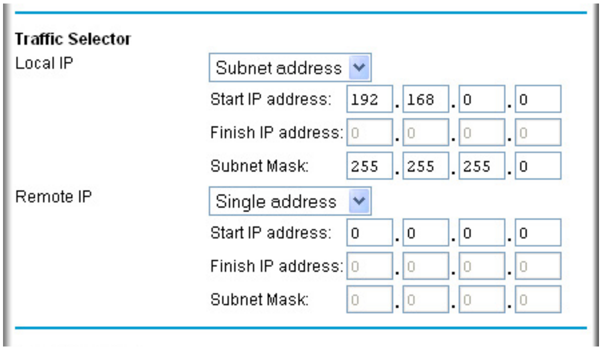
Remote VPN Endpoint: Address Type: IP Address; Address Data: 0.0.0.0

SA Life Time: 86400 (Seconds); 0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Figure D-4: NETGEAR FVL328 VPN – Auto Policy General settings

- – Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used to318 as the Policy Name. In the Policy Name field type **VPNclient**.
- – From the IKE policy drop-down box, select **VPNclient** which is the IKE Policy that was set up in the earlier step.
- – From the Remote VPN Endpoint Address Type drop-down box, select **IP Address**.
- – Type **0.0.0.0** as the Address Data of the client because we are assuming the remote PC will have a dynamically assigned IP address. This will also be entered in the NETGEAR ProSafe VPN Client Internal Network IP Address field, as seen in "My Identity" on page D-10.
- – Type **86400** in the SA Life Time (Seconds) field.
- – Type **0** in the SA Life Time (Kbytes) field.
- – Check the **IPSec PFS** checkbox to enable Perfect Forward Secrecy. This will also be entered in the NETGEAR ProSafe VPN Client Security Policy Enable Perfect Forward Secrecy checkbox, as seen in "Security Policy" on page D-11.
- – From the PFS Key Group drop-down box, select **Group 2 (1024 Bit)**. This will also be entered in the NETGEAR ProSafe VPN Client Security Policy PFS Key Group drop-down selection box, as seen in "Security Policy" on page D-11.



Traffic Selector

Local IP: Subnet address

Start IP address: 192 . 168 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Single address

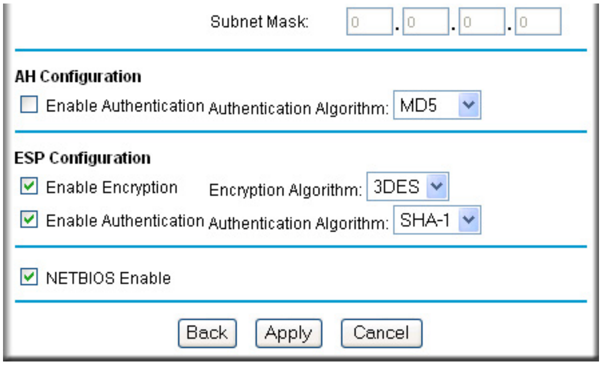
Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Figure D-5: NETGEAR FVL328 VPN – Auto Policy Traffic Selector

- From the Traffic Selector Local IP drop-down box, select **Subnet addresses**. This will also be entered in the NETGEAR ProSafe VPN Client Connection Remote Party Identity and Addressing ID Type field, as seen in “Security Policy Editor New Connection“ on page D-9.
- Type the starting LAN IP Address of the FVL328 in the Local IP Start IP Address field. For this example, we used **192.168.0.0** which is the default LAN IP address of the FVL328**.** This will also be entered in the NETGEAR ProSafe VPN Client Connection Remote Party Identity and Addressing Subnet field, as seen in “Security Policy Editor New Connection“ on page D-9.
- Type the LAN Subnet Mask of the FVL328 (**255.255.255.0** in our example) in the Local IP Subnet Mask field. This will also be entered in the NETGEAR ProSafe VPN Client Connection Remote Party Identity and Addressing Mask field, as seen in “Security Policy Editor New Connection“ on page D-9.
- From the Traffic Selector Remote IP drop-down box, select **Single addresses**.
- Type **0.0.0.0** as the start IP Address of the in the Remote IP Start IP Address field because we are assuming the remote PC will have a dynamically assigned IP address. This will also be entered in the NETGEAR ProSafe VPN Client My Identity Internal Network IP Address field, as seen in “My Identity“ on page D-10.



Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

☐ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption Encryption Algorithm: 3DES

☑ Enable Authentication Authentication Algorithm: SHA-1

☑ NETBIOS Enable

Figure D-6: NETGEAR FVL328 VPN – Auto Policy ESP Configuration

- Select **Enable Encryption** in the ESP Configuration Enable Encryption checkbox. This will also be entered in the NETGEAR ProSafe VPN Client Security Policy Key Exchange (Phase 2) Encapsulation Protocol (ESP) checkbox, as seen in “Connection Security Policy Key Exchange (Phase 2)“ on page D-13.
- From the ESP Configuration Encryption Algorithm drop-down box, select **3DES**. This will also be entered in the NETGEAR ProSafe VPN Client Security Policy Key Exchange (Phase 2) Encrypt Alg field, as seen in “Connection Security Policy Key Exchange (Phase 2)“ on page D-13.
- Select **Enable Authentication** in the ESP Configuration Enable Authentication checkbox. **Note**: Do not confuse this with the Authentication Protocol (AH) option. Using the AH option will prevent clients behind a home NAT router from connecting.
- From the ESP Configuration Authentication Algorithm drop-down box, select **SHA-1**. This will also be entered in the NETGEAR ProSafe VPN Client Security Policy Key Exchange (Phase 2) Hash Alg field, as seen in “Connection Security Policy Key Exchange (Phase 2)“ on page D-13.
- Select **NETBIOS Enable** in the NETBIOS Enable checkbox to enable networking features like Windows Network Neighborhood.

Click **Apply** to save your changes. You will be taken back to the VPN Policies Menu page.

4. When the screen returns to the VPN Policies, make sure the Enable checkbox is selected. Click **Apply** to save your changes.

Step-By-Step Configuration of the NETGEAR VPN Client B

Note: The NETGEAR ProSafe VPN Client has the ability to "Import" a predefined configuration profile. The FVL328.SPD file on the NETGEAR ProSafe VPN Client *Resource CD (230-10007-01)* includes all the settings identified in this procedure.

Whenever importing policy settings, you should first export any existing settings you may have configured to prevent the new imported settings from replacing an existing working configuration.

To import this policy, use the Security Policy Editor File menu to select Import Policy, and select the FVL328.SPD file at D:\Software\Policies where D is the drive letter of your CD-ROM drive.

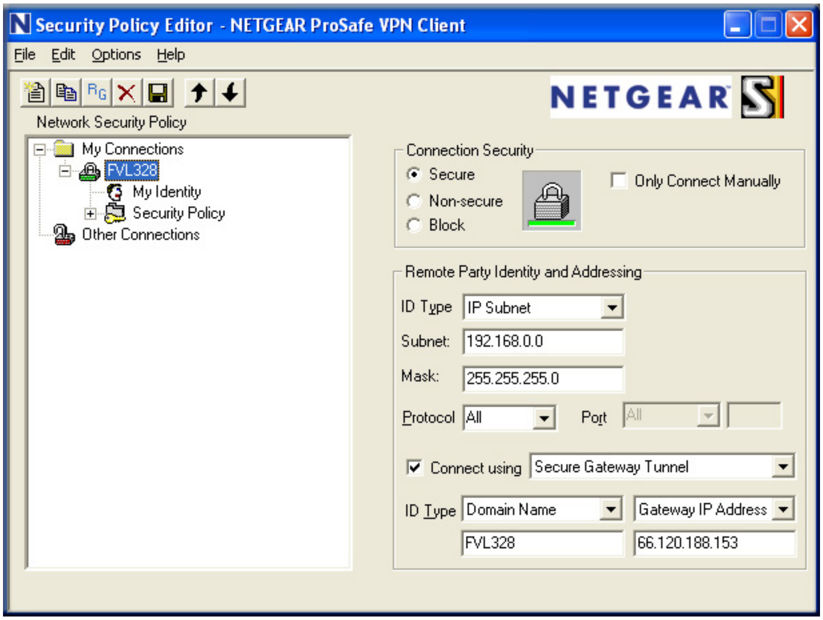
This procedure describes linking a remote PC and a LAN. The LAN will connect to the Internet using an FVL328 with a static IP address. The PC can be directly connected to the Internet through dialup, cable or DSL modem, or other means, and we will assume it has a dynamically assigned IP address.

1. **Install the NETGEAR VPN Client Software on the PC.**

Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

- You may need to insert your Windows CD to complete the installation.
- Reboot your PC after installing the client software.

2. Configure the Connection Network Settings.



Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.0.0
Mask: 255.255.255.0
Protocol: All   Port: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name   Gateway IP Address
FVL328   66.120.188.153

Figure D-7: Security Policy Editor New Connection

a. Run the Security Policy Editor program and create a VPN Connection.

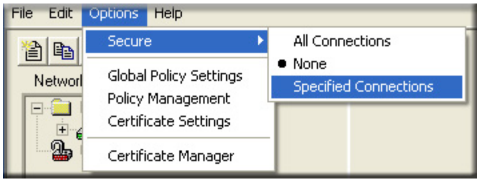


Figure D-8: Security Policy Editor Options menu

Note: If the configuration settings on this screen are not available for editing, go to the Options menu, select Secure, and Specified Options to enable editing of these settings.

From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**. A “New Connection” listing appears. Rename the “New Connection” to **FVL328**.

b. Assure that the following settings are configured:

– In the Connection Security box, Secure is selected

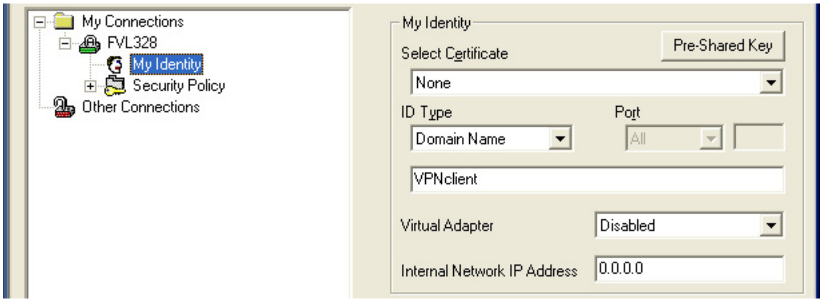
- In the Protocol menu, All is selected
- The Connect using Secure Gateway Tunnel checkbox is checked

c. In this example, select IP Subnet as the ID Type, **192.168.0.0** in the Subnet field (the Subnet address is the LAN IP Address of the FVL328 with 0 as the last number), and **255.255.255.0 i**n the Mask field, which is the LAN Subnet Mask of the FVL328

d. In the ID Type menus, select **Domain Name** and **Gateway IP Address**. Enter **FVL328** in the Domain Name field. In this example, **66.120.188.153** would be used for the Gateway IP Address, which is the static IP address for the FVL328 WAN port.

3. **Configure the Connection Identity Settings.**

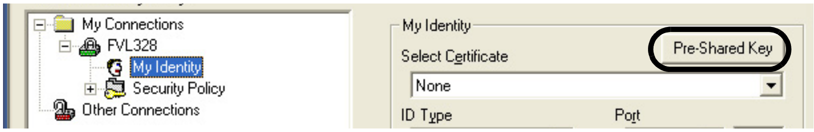
a. In the Network Security Policy list, click the My Identity subheading.



My Identity
Select Certificate: None
ID Type: Domain Name
Port: All
VPNclient
Virtual Adapter: Disabled
Internal Network IP Address: 0.0.0.0

Figure D-9: My Identity

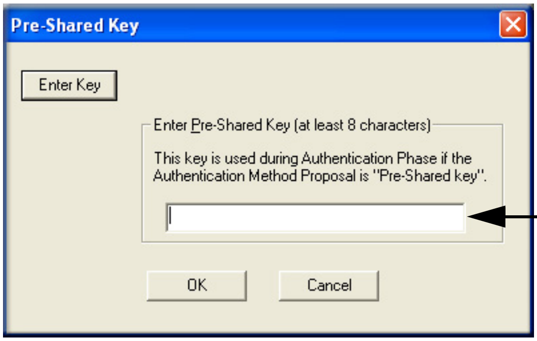
In this example, select Domain Name as the ID Type, and enter **VPNclient**. Also, accept the default Internal Network IP Address of 0.0.0.0.



My Identity
Select Certificate: None
ID Type
Port

Figure D-10: My Identity Pre-Shared Key

b. Click **Pre-Shared Key**.



Pre-Shared Key

Enter Key

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

OK Cancel

In this example, enter this pre-shared key in this field: **hr5xb84l6aa9r6**

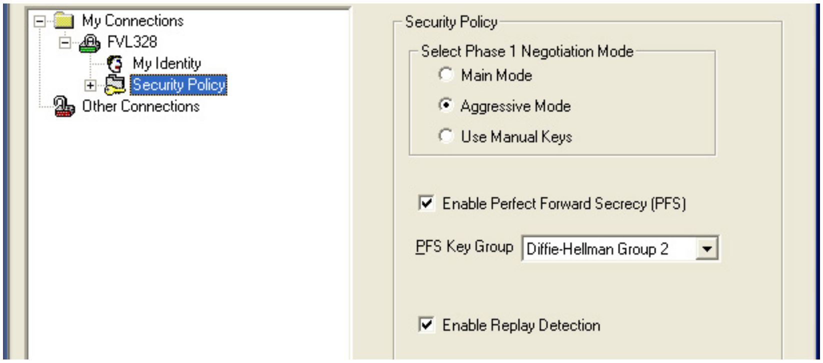
Figure D-11: Connection Identity Pre-Shared Key

c. Enter **hr5xb84l6aa9r6** which is the same Pre-Shared Key entered in the FVL328.

d. Click **OK**.

4. Configure the Connection Identity Settings.

a. In the Network Security Policy list, click the Security Policy subheading.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

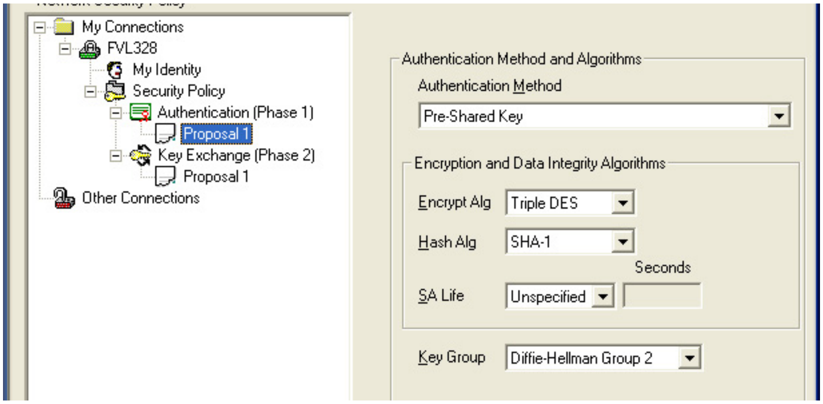
Figure D-12: Security Policy

b. For this example, assure that the following settings are configured:

- In the Select Phase 1 Negotiation Mode menu, select **Aggressive Mode**.
- Check the **Enable Perfect Forward Secrecy (PFS)** checkbox.
- In the PFS Key Group drop-down list, **Diffie-Hellman Group 2**.
- Check the Enable Replay Detection checkbox.

5. Configure the Connection Security Policy

In this step, you will provide the authentication (IKE Phase 1) settings, and the key exchange (Phase 2) settings. The setting choices in this procedure follow the VPNC guidelines.



- My Connections
  - FVL328
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
- Other Connections

Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

Hash Alg: SHA-1

SA Life: Unspecified

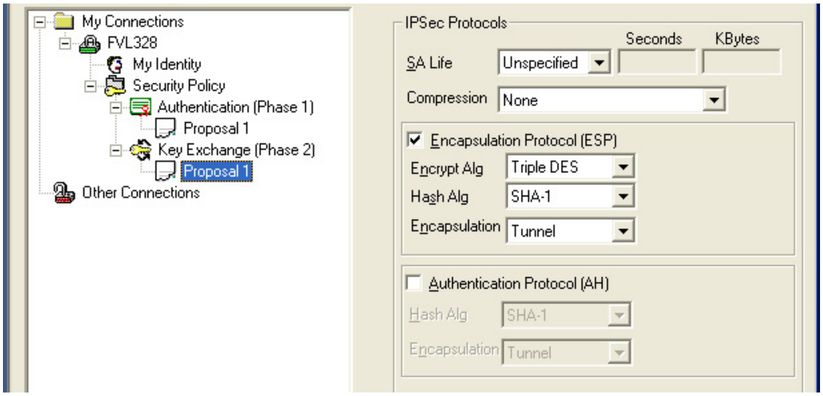
Seconds:

Key Group: Diffie-Hellman Group 2

Figure D-13: Connection Security Policy Authentication (Phase 1)

a. Configure the Authentication (Phase 1) Settings.

- Expand the Security Policy heading, then expand the Authentication (Phase 1) heading, and click on Proposal 1.
- For this example, assure that the following settings are configured:
  - In the Encrypt Alg menu, select **Triple DES**.
  - In the Hash Alg, select **SHA-1**.
  - In the SA Life, select Unspecified.
  - In the Key Group menu, select **Diffie-Hellman Group 2**.



IPSec Protocols

		Seconds	KBytes
SA Life	Unspecified		
Compression	None		

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

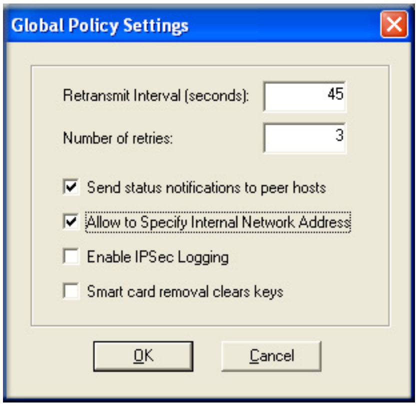
Figure D-14: Connection Security Policy Key Exchange (Phase 2)

b. Configure the Key Exchange (Phase 2).

- Expand the Key Exchange (Phase 2) heading, and click on Proposal 1.
- For this example, assure that the following settings are configured:
  - In the SA Life menu, select **Unspecified**.
  - In the Compression menu, select **None**.
  - Check the **Encapsulation Protocol (ESP)** checkbox.
  - In the Encrypt Alg menu, select **Triple DES**.
  - In the Hash Alg, select **SHA-1**.
  - In the Encapsulation menu, select **Tunnel**.

6. **Configure the Global Policy Settings.**

   a. From the Options menu at the top of the Security Policy Editor window, select **Global Policy Settings**.



Global Policy Settings

Retransmit Interval (seconds): 45

Number of retries: 3

☑ Send status notifications to peer hosts

☑ Allow to Specify Internal Network Address

☐ Enable IPSec Logging

☐ Smart card removal clears keys

Figure D-15: Security Policy Editor Global Policy Options

   b. Increase the Retransmit Interval period to **45** seconds.

   c. Check the Allow to Specify Internal Network Address checkbox and click **OK**.

7. **Save the VPN Client Settings.**

   From the File menu at the top of the Security Policy Editor window, select Save.

   After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router’s LAN.

➡	**Note:** Whenever you make changes to a Security Policy, save them first, then deactivate the security policy, reload the security policy, and finally activate the security policy. This assures that your new settings will take effect.

Testing the VPN Connection

You can test the VPN connection in several ways:

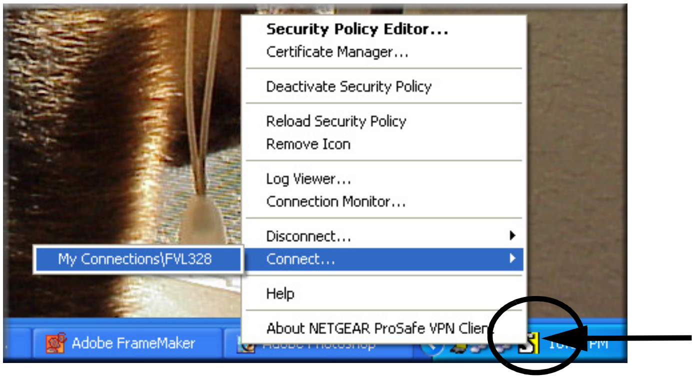
- From the client PC to the FVL328
- From the FVL328 to the client PC

These procedures are explained below.

Note: Virus protection or firewall software can interfere with VPN communications. Be sure such software is not running on the remote PC with the NETGEAR VPN Client and that the firewall features of the FVL328 is not set in such a way as to prevent VPN communications.

From the Client PC to the FVL328

To check the VPN Connection, you can initiate a request from the remote PC to the FVL328 by using the “Connect” option of the NETGEAR VPN Client popup menu.



Right-mouse-click on the system tray icon to open the popup menu.

Figure D-16: Connecting the PC to the FVL328 over the VPN tunnel

1. Open the popup menu by right-clicking on the system tray icon.
2. Select **Connect** to open the My Connections list.
3. Choose **FVL328**.

   The NETGEAR VPN Client will report the results of the attempt to connect.

Once the connection is established, you can access resources of the network connected to the FVL328.

Another method is to ping from the remote PC to the LAN IP address of the FVL328. To perform a ping test using our example, start from the remote PC:

1. Establish an Internet connection from the PC.
2. On the Windows taskbar, click the Start button, and then click Run.
3. Type **`ping -t 192.168.0.1`**, and then click OK.

   This will cause a continuous ping to be sent to the first FVL328. After a period of up to two minutes, the ping response should change from “timed out” to “reply.”

   To test the connection to a computer connected to the FVL328, simply ping the IP address of that computer.

Once connected, you can open a browser on the remote PC and enter the LAN IP Address of the FVL328, which is http://192.168.0.1 in this example. After a short wait, you should see the login screen of the FVL328.

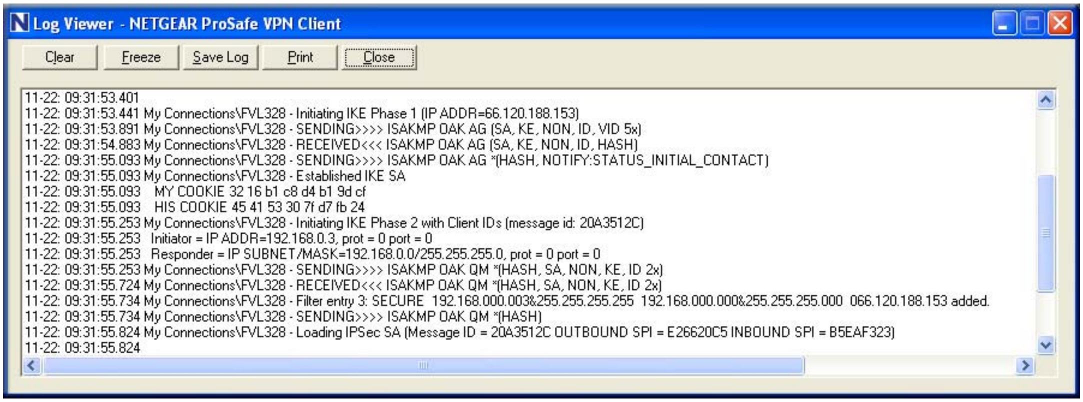
From the FVL328 to the Client PC

You can use the FVL328 Diagnostic utilities to test the VPN connection from the FVL328 to the client PC. Run ping tests from the Diagnostics link of the FVL328 main menu.

Monitoring the PC VPN Connection

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR VPN Client Connection Monitor or Log Viewer. To launch these functions, click on the Windows Start button, then select Programs, then NETGEAR ProSafe VPN Client, then either the Connection Monitor or Log Viewer.

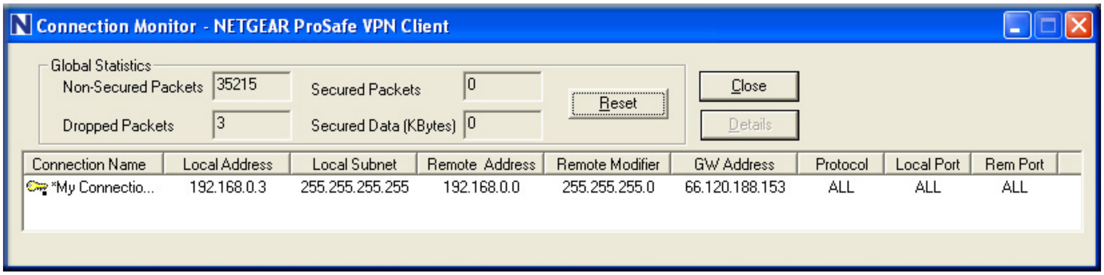
The Log Viewer screen for a successful connection is shown below:



```
11-22: 09:31:53.401
11-22: 09:31:53.441 My Connections\FVL328 - Initiating IKE Phase 1 (IP ADDR=66.120.188.153)
11-22: 09:31:53.891 My Connections\FVL328 - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 5x)
11-22: 09:31:54.883 My Connections\FVL328 - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH)
11-22: 09:31:55.093 My Connections\FVL328 - SENDING>>>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
11-22: 09:31:55.093 My Connections\FVL328 - Established IKE SA
11-22: 09:31:55.093    MY COOKIE 32 16 b1 c8 d4 b1 9d cf
11-22: 09:31:55.093    HIS COOKIE 45 41 53 30 7f d7 fb 24
11-22: 09:31:55.253 My Connections\FVL328 - Initiating IKE Phase 2 with Client IDs (message id: 20A3512C)
11-22: 09:31:55.253   Initiator = IP ADDR=192.168.0.3, prot = 0 port = 0
11-22: 09:31:55.253   Responder = IP SUBNET/MASK=192.168.0.0/255.255.255.0, prot = 0 port = 0
11-22: 09:31:55.253 My Connections\FVL328 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-22: 09:31:55.724 My Connections\FVL328 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-22: 09:31:55.734 My Connections\FVL328 - Filter entry 3: SECURE  192.168.000.003&255.255.255.255  192.168.000.000&255.255.255.000  066.120.188.153 added.
11-22: 09:31:55.734 My Connections\FVL328 - SENDING>>>> ISAKMP OAK QM *(HASH)
11-22: 09:31:55.824 My Connections\FVL328 - Loading IPSec SA (Message ID = 20A3512C OUTBOUND SPI = E26620C5 INBOUND SPI = B5EAF323)
11-22: 09:31:55.824
```

Figure D-17: Log Viewer screen

A sample Connection Monitor screen for a different connection is shown below:



Global Statistics

Non-Secured Packets: 35215

Secured Packets: 0

Dropped Packets: 3

Secured Data (KBytes): 0

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
*My Connectio...	192.168.0.3	255.255.255.255	192.168.0.0	255.255.255.0	66.120.188.153	ALL	ALL	ALL

Figure D-18: Connection Monitor screen

In this example you can see the following:

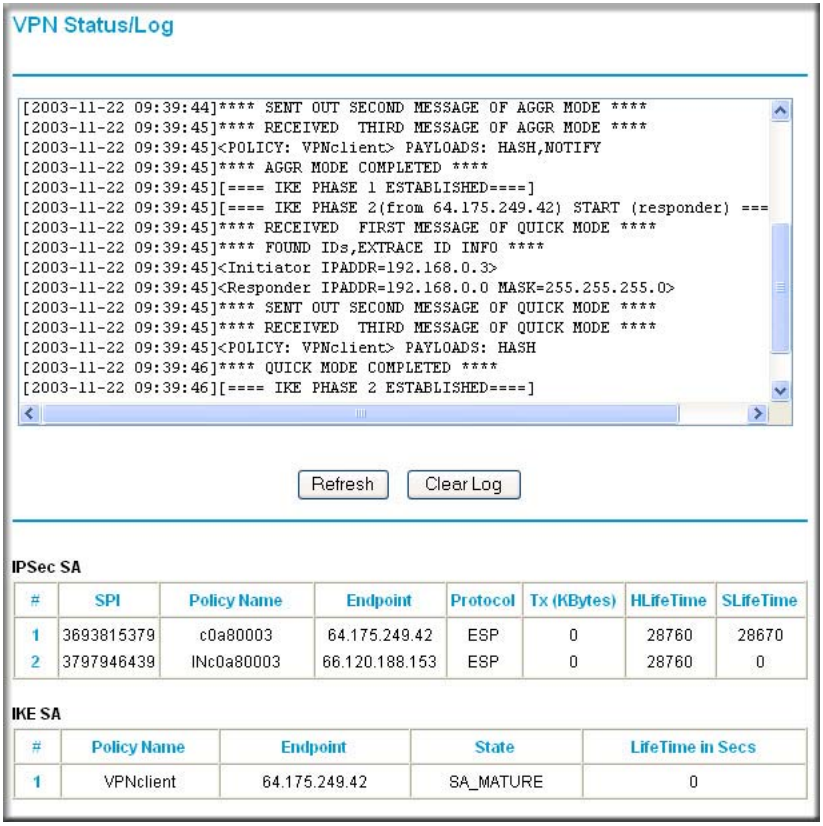
- The FVL328 has a public IP WAN address of 66.120.188.153
- The FVL328 has a LAN IP address of 192.168.0.1
- The VPN client PC is behind a home NAT router and has a dynamically assigned address of 192.168.0.3

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

Viewing the FVL328 VPN Status and Log Information

Information on the status of the VPN client connection can be viewed by opening the FVL328 VPN Status screen. To view this screen, click the VPN Status link of the FVL328 main menu.

The FVL328 VPN Status screen for a successful connection is shown below:



```
[2003-11-22 09:39:44]**** SENT OUT SECOND MESSAGE OF AGGR MODE ****
[2003-11-22 09:39:45]**** RECEIVED  THIRD MESSAGE OF AGGR MODE ****
[2003-11-22 09:39:45]<POLICY: VPNclient> PAYLOADS: HASH,NOTIFY
[2003-11-22 09:39:45]**** AGGR MODE COMPLETED ****
[2003-11-22 09:39:45][==== IKE PHASE 1 ESTABLISHED====]
[2003-11-22 09:39:45][==== IKE PHASE 2(from 64.175.249.42) START (responder) ===
[2003-11-22 09:39:45]**** RECEIVED  FIRST MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]**** FOUND IDs,EXTRACE ID INFO ****
[2003-11-22 09:39:45]<Initiator IPADDR=192.168.0.3>
[2003-11-22 09:39:45]<Responder IPADDR=192.168.0.0 MASK=255.255.255.0>
[2003-11-22 09:39:45]**** SENT OUT SECOND MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]**** RECEIVED  THIRD MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]<POLICY: VPNclient> PAYLOADS: HASH
[2003-11-22 09:39:46]**** QUICK MODE COMPLETED ****
[2003-11-22 09:39:46][==== IKE PHASE 2 ESTABLISHED====]
```

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3693815379	c0a80003	64.175.249.42	ESP	0	28760	28670
2	3797946439	INc0a80003	66.120.188.153	ESP	0	28760	0

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	VPNclient	64.175.249.42	SA_MATURE	0

Figure D-19: FVL328 VPN Status screen

To view the FVL328 VPN log, click on the VPN Status link on the left side of the main menu. The log information should be similar to the example below:

Glossary

Use the list below to find definitions for technical terms used in this manual.

Numeric

3DES

3DES (Triple DES) achieves a high level of security by encrypting the data three times using DES with three different, unrelated keys.

A

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Address Resolution Protocol

An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

AES

Advanced Encryption Standard, a symmetric 128-bit block data encryption technique.
It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

AH

Authentication Header.

API

See “Application Programming Interface” on page 2.

Application Programming Interface

An API is an interface used by an programmer to interface with functions provided by an application.

ARP

See “ADSL” on page 1.

Auto-negotiation

A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.

C

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic_commerce because they guarantee that the two parties exchanging information are really who they claim to be.
the two parties exchanging information are really who they claim to be.

CRL

Certificate Revocation List. Each Certificate Authority (CA) maintains a revoked certificates list.

D

DES

The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. *See* also 3DES.

DHCP

See “Dynamic Host Configuration Protocol.” on page 3.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol.

DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

ESP

Encapsulating Security Payload.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

F

Filtering

The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.

Forwarding

When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Fully Qualified domain Name (FQDN)

A fully qualified domain name consists of a host and domain name, including top-level domain. For example, www.netgear.com is a fully qualified domain name. www is the host, netgear is the second-level domain, and.com is the top level domain. A FQDN always starts with a host name and continues all the way up to the top-level domain name, so www.parc.xerox.com is also a FQDN. Routers can use FQDN to uniquely identify their address on the Internet rather than an IP address.

G

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

I

ICMP

See “Internet Control Message Protocol” on page 5.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IKE

Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

Internet Control Message Protocol

ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol

The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP

See “Internet Protocol” on page 5.

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IPSec

Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.

ISP

Internet service provider.

L

LAN

See “Local Area Network” on page 6.

LDAP

See “Lightweight Directory Access Protocol” on page 6.

Lightweight Directory Access Protocol

A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as e-mail addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Local Area Network

A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC

(1) Media Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

MD5

MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

N

NAT

See “Network Address Translation” on page 7.

NetBIOS

Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

P

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

PKIX

PKIX. The most widely used standard for defining digital certificates.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP

A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP

Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft’s network protocol into Internet packets.

Protocol

A set of rules for communication between devices on a network.

PSTN

Public Switched Telephone Network.

Public Key Infrastructure

PKIX. The most widely used standard for defining digital certificates.
X.509 is actually an ITU Recommendation, which means that it has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both

Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

Q

QoS

See “Quality of Service” on page 9.

Quality of Service

QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RFC

Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

RIP

See “Routing Information Protocol” on page 9.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol

RIP is the routing protocol used by the routed process on Berkeley-derived UNIX systems. Many networks use RIP; it works well for small, isolated, and topologically simple networks.

S

Subnet Mask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

T

TCP/IP

The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

V

VPN

Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.

W

WAN

See “Wide Area Network” on page 10.

Web

Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Index