

# 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

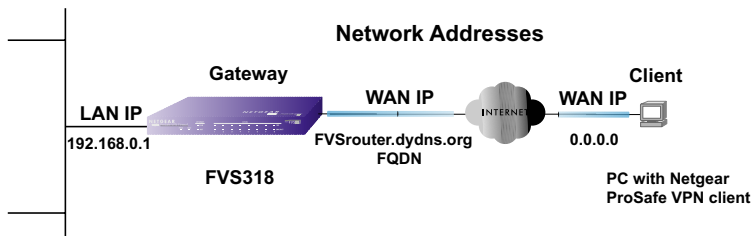


Figure C-1: Addressing and Subnets Used for Examples

## 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 3<sup>rd</sup> 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](http://www.netgear.com/support/main.asp). VPNC Interoperability guidelines can be found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>.

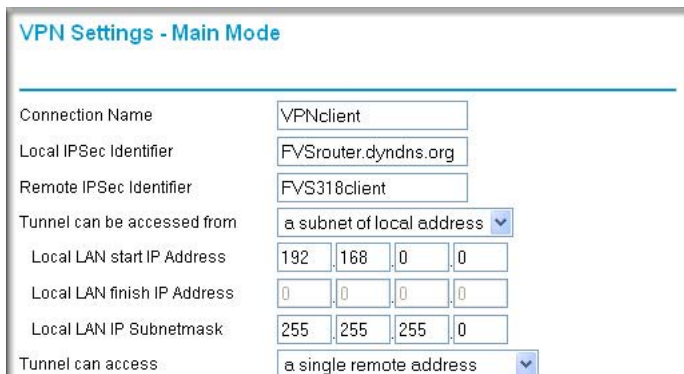
## Step-By-Step Configuration of FVS318 or FVM318 Gateway A

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:

Local IPsec Identifier:

Remote IPsec Identifier:

Tunnel can be accessed from:

Local LAN start IP Address:

Local LAN finish IP Address:

Local LAN IP Subnetmask:

Tunnel can access:

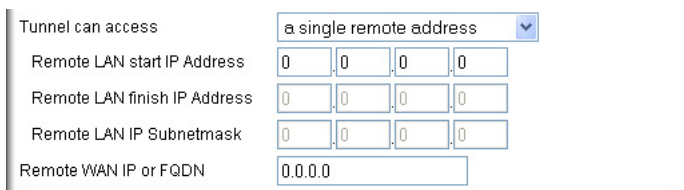
**Figure C-2: NETGEAR FVS318 VPN Settings – Main Mode**

- 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 menu. 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:

Remote LAN start IP Address:

Remote LAN finish IP Address:

Remote LAN IP Subnetmask:

Remote WAN IP or FQDN:

**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	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Encryption Protocol	3DES
PreShared Key	hr5xb84l6aa9r6
Key Life	28800 Seconds
IKE Life Time	86400 Seconds
<input checked="" type="checkbox"/> NETBIOS Enable	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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.

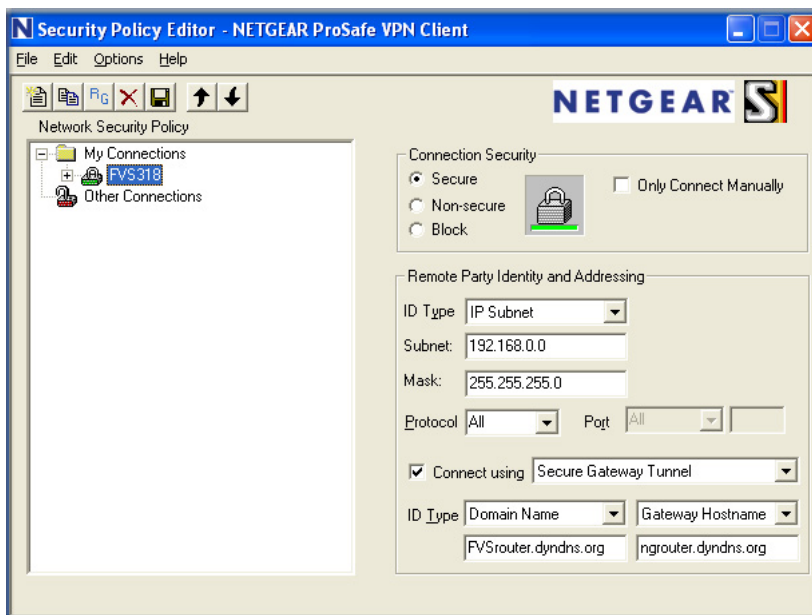
### 1. Install the NETGEAR VPN Client Software on the PC.



**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.

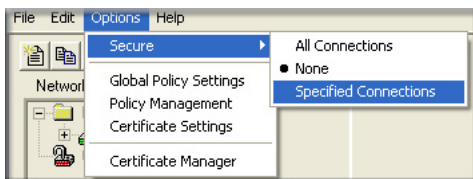
- You may need to insert your Windows CD to complete the installation.
- Reboot your PC after installing the client software.

## 2. Configure the Connection Network Settings.



**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** in 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.

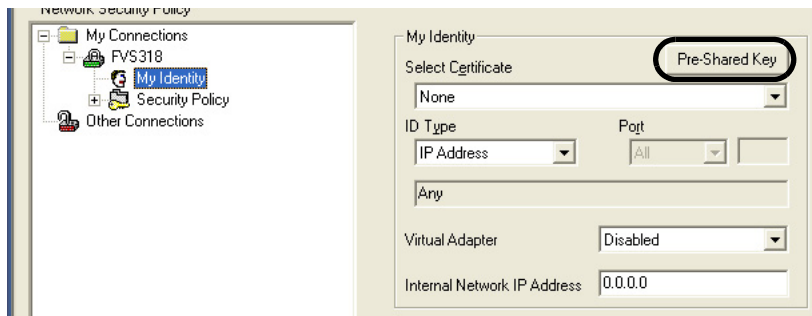
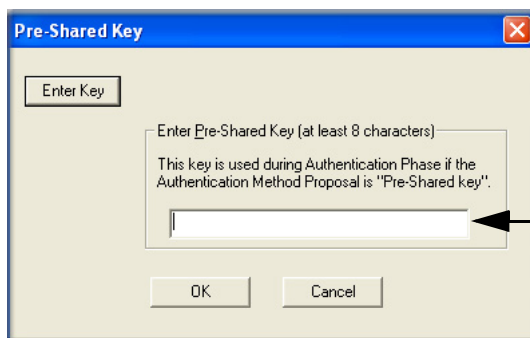


Figure C-7: Connection Identity

- b. Click **Pre-Shared Key**.



In this example, enter this pre-shared key in this field:  
**hr5xb84l6aa9r6**

Figure C-8: Connection Identity Pre-Shared Key

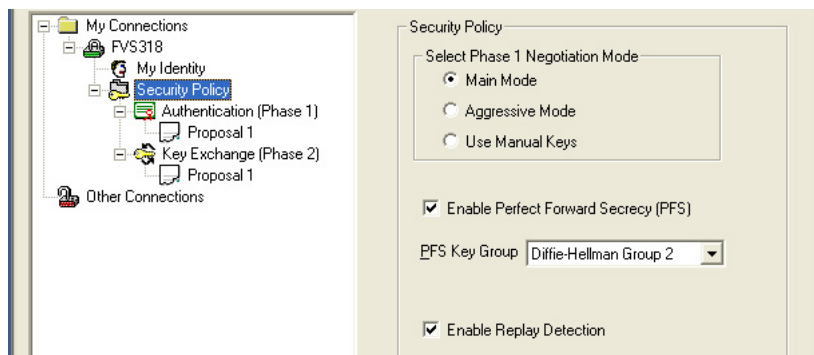
- c. Enter the same Pre-Shared Key used in the FVS318 VPN router.

In this example, we used **hr5xb84l6aa9r6**.

- d. Click **OK**.

#### 4. Configure the Security Policy Settings.

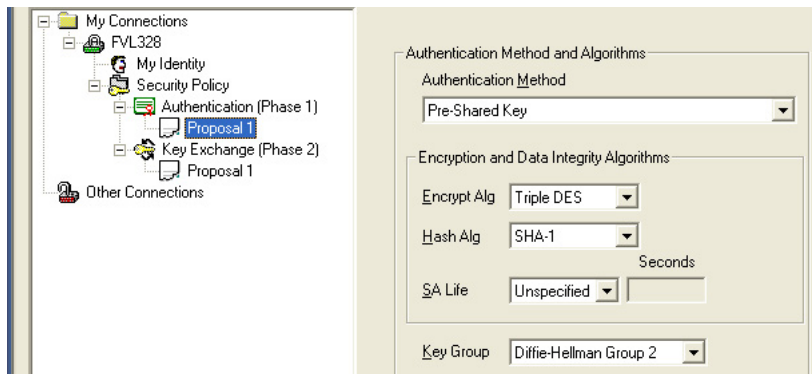
- a. In the Network Security Policy list, click the Security Policy subheading.



**Figure C-9: Security Policy**

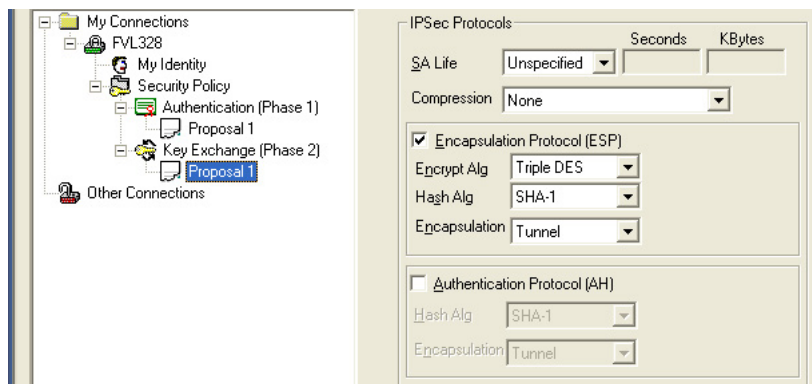
- b. For this example, assure that the following settings are configured:
  - In the Select Phase 1 Negotiation Mode menu, select **Main Mode**.
  - Check the **Enable Perfect Forward Secrecy (PFS)** checkbox.
  - In the PFS Key Group drop-down list, **Diffie-Hellman Group 2**.
  - Check the Enable Replay 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.



**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**.



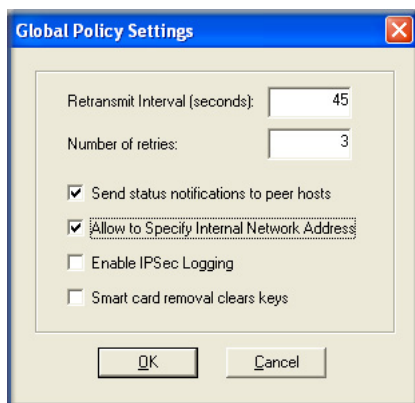
**Figure C-11: Connection Security Policy Key Exchange (Phase 2)**

- 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.



**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

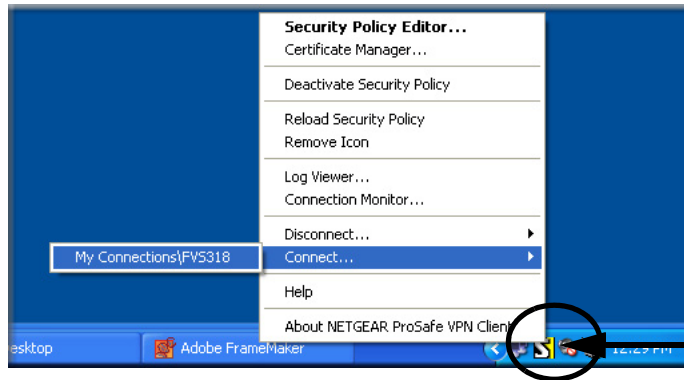
These procedures are explained below.



**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:

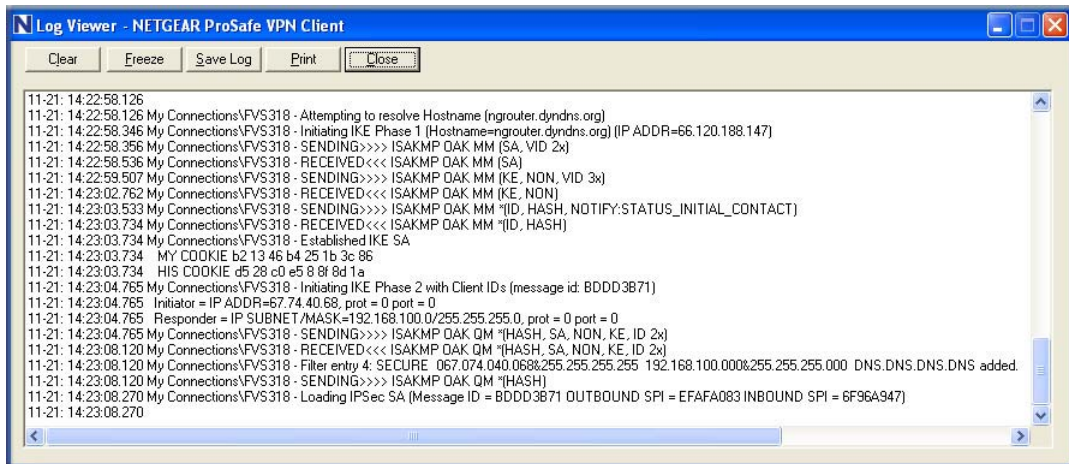
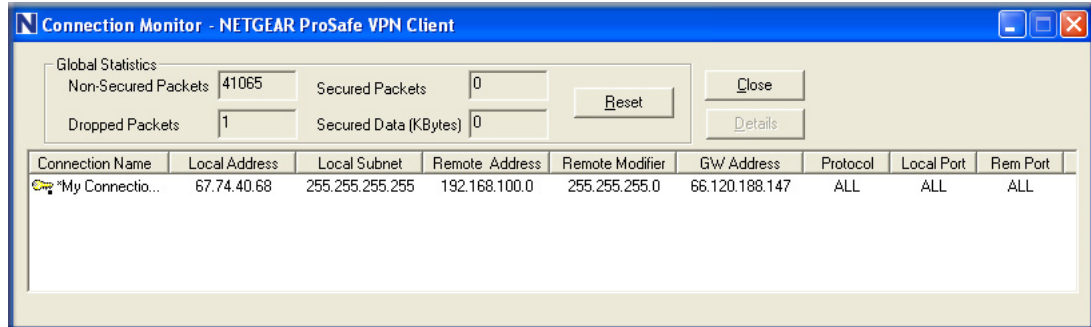


Figure C-14: Log Viewer screen

A sample Connection Monitor screen for a different connection is shown below:



**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:

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Inactive	vpnclient	0.0.0.0	0.0.0.0/0		Idle	<input type="button" value="Drop"/>
Active	vpnclient_tmp6	67.74.56.79	67.74.56.79/32	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	<input type="button" value="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 OUTBOUND SA:
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 -----

```