

Appendix B

NETGEAR VPN Configuration

DG834GSP to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834GSP to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

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 B-1. Profile Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
NETGEAR-Gateway A	Static IP address
NETGEAR-Gateway B	Static IP address

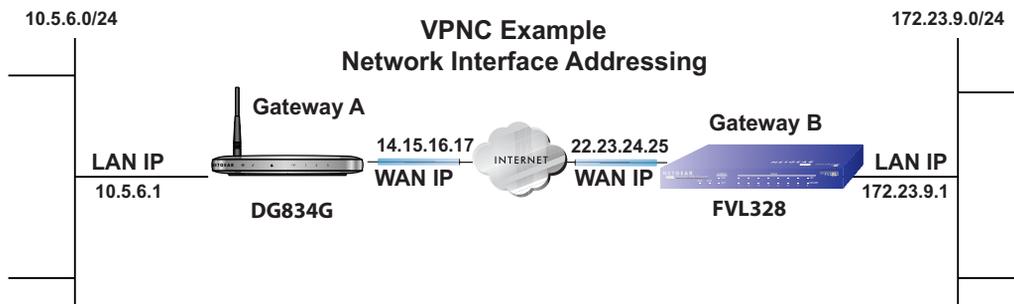


Figure B-1



Note: Product updates are available on the NETGEAR, Inc. web site at <http://kbserver.netgear.com/DG834GSP.asp>.

Step-By-Step Configuration

1. Configure the DG834GSP as in the Gateway-to-Gateway procedures using the VPN Wizard (see “[How to Set Up a Gateway-to-Gateway VPN Configuration](#)” on page 8-21), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

Unit	WAN IP	LAN IP	LAN Subnet Mask
DG834G	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

- a. In Step 1, enter **toFVL328** for the Connection Name.
- b. In Step 2, enter **22.23.24.25** for the remote WAN's IP address.
- c. In Step 3, enter the following:
 - IP Address = **172.23.9.1**
 - Subnet Mask = **255.255.255.0**

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	toFVL328	Auto	10.5.6.1 / 255.255.255.0	172.23.9.1 / 255.255.255.0	3DES

Click VPN Policies under Advanced - VPN to invoke this screen

VPN - Auto Policy

General

Policy Name: toFVL328

Remote VPN Endpoint: Fixed IP Address

Address Data: 66.170.188.152 / 22.23.24.25

NetBIOS Enable
 IKE Keep Alive

Ping IP Address:

Local LAN

IP Address: Subnet address

Single/Start address: 192 . 168 . 0 . 1

Finish address: . 10 . 5 . 6 . 1

Subnet Mask: 255 . 255 . 255 . 0

Remote LAN

IP Address: Subnet address

Single/Start IP address: 192 . 168 . 2 . 1

Finish IP address: . 172 . 23 . 9 . 1

Subnet Mask: 255 . 255 . 255 . 0

IKE

Direction: Initiator and Responder

Exchange Mode: Main Mode

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

Local Identity Type: WAN IP Address

Data: n/a

Remote Identity Type: IP Address

Data: n/a

Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Pre-shared Key: 12345678

SA Life Time: 28800 (Seconds)

Enable PFS (Perfect Forward Security)

Figure B-2

2. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on page 8-21), being certain to use appropriate network addresses for the environment.
 - a. In Step 1, enter **toDG834** for the Connection Name
 - b. In Step 2, enter **14.15.16.17** for the remote WAN's IP address
 - c. In Step 3, enter the following:
 - IP Address = **10.5.6.1**
 - Subnet Mask = **255.255.255.0**

IKE Policies

Policy Table							
#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
<input checked="" type="checkbox"/>	1	toDG834	Main	22.23.24.25	14.15.16.17	3DES	SHA1 Group 2 (1024 Bit)

Buttons: Add, Edit, Delete, Cancel

Click IKE Policies under VPN to invoke this screen

IKE Policy Configuration

General
 Policy Name: jim2in toDG834
 Direction/Type: Both Directions
 Exchange Mode: Main Mode

Local
 Local Identity Type: WAN IP Address
 Local Identity Data: 67.125.91.84
 22.23.24.25

Remote
 Remote Identity Type: Remote WAN IP
 Remote Identity Data: 67.125.91.84
 14.15.16.17

IKE SA Parameters
 Encryption Algorithm: 3DES
 Authentication Algorithm: SHA-1
 Authentication Method: Pre-shared Key

 RSA Signature (requires Certificate)
 Certificate: Group 2 (1024 Bit)
 SA Life Time: 28800 (secs)

Buttons: Back, Apply, Cancel

VPN Policies

#	Enable	Name	Type	Local	Remote	AH	ESP	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	toDG834	Auto	192.168.0.1/255.255.255.0	192.168.0.1/255.255.255.0	Disabled	ESP

Buttons: Edit, Move, Delete, Apply, Cancel, Add Auto Policy, Add Manual Policy

Click VPN Policies under VPN to invoke this screen

VPN - Auto Policy

General
 Policy Name: jim2james
 IKE policy: toDG834
 IKE Keep Alive
 Remote VPN Endpoint: toDG834
 Address Type: IP Address
 Address Data: 67.125.91.84
 SA Life Time: 86400 (seconds)
 PFS key Group: Group 1 (768 Bit)

Traffic Selector
 Local IP:
 Subnet address:
 Start IP address: 192.168.0.1
 Finish IP address: 0.172.23.9
 Subnet Mask: 255.255.255.0
 Remote IP:
 Subnet address:
 Start IP address: 192.168.0.1
 Finish IP address: 0.10.5.6
 Subnet Mask: 255.255.255.0

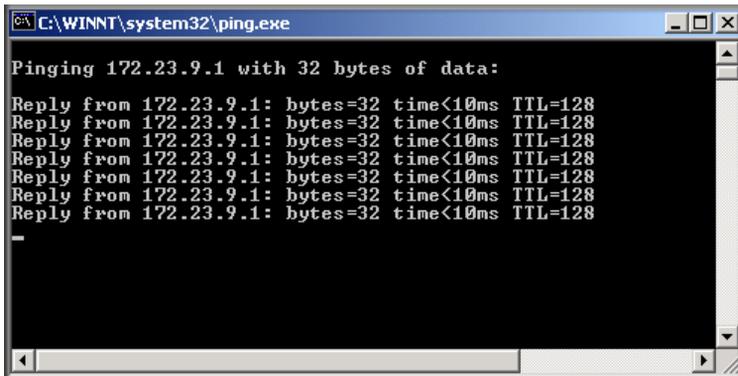
AH Configuration
 Enable Authentication
 Authentication Algorithm: MD5

ESP Configuration
 Enable Encryption
 Enable Authentication
 Encryption Algorithm: 3DES
 Authentication Algorithm: SHA-1

Buttons: Back, Apply, Cancel

Figure B-3

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834GSP.
 - a. Open the command prompt (Start -> Run -> cmd)
 - b. ping 172.23.9.1



```
C:\WINNT\system32\ping.exe
Pinging 172.23.9.1 with 32 bytes of data:
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
```

Figure B-4

	Note: The pings may fail the first time. If this happens, try the pings a second time.
---	---

DG834GSP with FQDN to FVL328

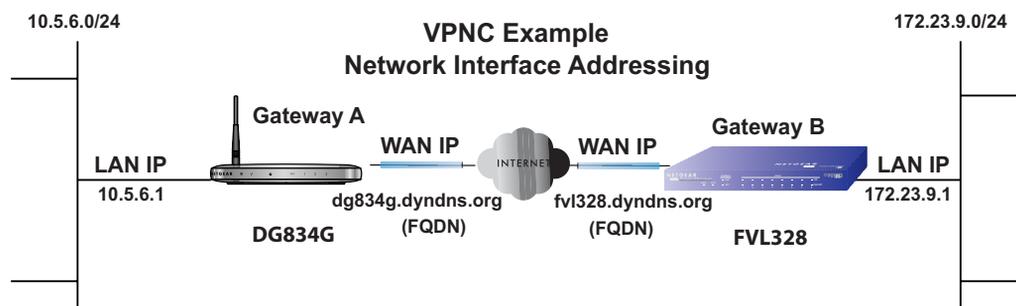
This appendix is a case study on how to configure a VPN tunnel from a NETGEAR DG834GSP to a FVL328 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

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 B-2. Profile Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
NETGEAR-Gateway B	FDQN

**Figure B-5**

Note: Product updates are available on the NETGEAR, Inc. web site at <http://kbserver.netgear.com/DG834GSP.asp>.

The Use of a Fully Qualified Domain Name (FQDN)

Many ISPs (Internet Service Providers) 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.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host 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:

- 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 **dg834g.dyndns.org** for gateway A using the DynDNS service. Gateway B will use the DDNS Service Provider when establishing a VPN tunnel.

In order to establish VPN connectivity Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS hostname to find Gateway A provided by a DDNS Service Provider. Again, 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 gateways.

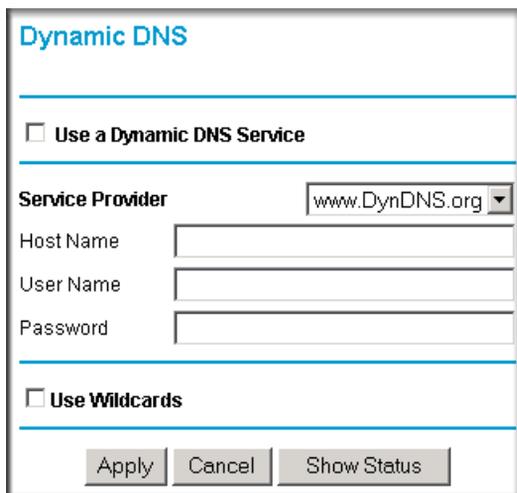
Step-By-Step Configuration

1. Log in to the DG834GSP labeled Gateway A as in the illustration.

Out of the box, the DG834GSP is set for its default LAN address of <http://10.1.1.1> with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. Click on the **Dynamic DNS** link on the left side of the Settings management GUI. This will take you to the Dynamic DNS Menu.

3. On the DG834GSP, configure the Dynamic DNS settings.
 - a. Browse to the Dynamic DNS Setup Screen (see [Figure B-6](#)) in the Advanced menu.



The image shows a web form titled "Dynamic DNS". At the top, there is a checkbox labeled "Use a Dynamic DNS Service". Below this, there is a "Service Provider" dropdown menu with "www.DynDNS.org" selected. Underneath are three text input fields labeled "Host Name", "User Name", and "Password". At the bottom of the form, there is another checkbox labeled "Use Wildcards". At the very bottom, there are three buttons: "Apply", "Cancel", and "Show Status".

Figure B-6

- b. Configure this screen with appropriate account and hostname settings and then click **Apply**.
 - Check the box **Use a Dynamic DNS Service**.
 - Host Name = dg834g.dyndns.org
 - User Name = <user's account username>
 - Password = <user's account password>
- c. Click **Show Status**. The resulting screen should show Update OK: good (see [Figure B-7](#)).



Figure B-7

4. On the FVL328, configure the Dynamic DNS settings. Assume a properly configured DynDNS account.
 - a. Browse to the Dynamic DNS Setup Screen (see [Figure B-8](#)) in the Advanced menu.



Figure B-8

- b. Select the **DynDNS.org** radio button (see [Figure B-8](#)), configure with appropriate account and hostname settings (see [Figure B-9](#)), and then click **Apply**.
 - Host and Domain Name = fv1328.dyndns.org
 - User Name = <user's account username>
 - Password = <user's account password>

Dynamic DNS

Use a dynamic DNS service

None

DynDNS.org [Click here for information](#)

TZO.com [Click here for free trial](#)

ngDDNS [Click here to register](#)

DynDNS

Host and Domain Name

example: yourname.dyndns.org

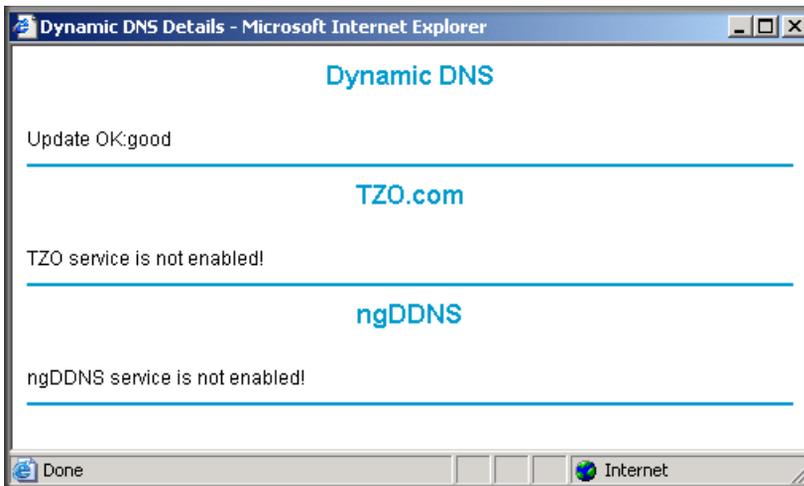
User Name

Password

Use wildcards

Figure B-9

- c. Click **Show Status**. The resulting screen should show Update OK: good (see [Figure B-10](#)).

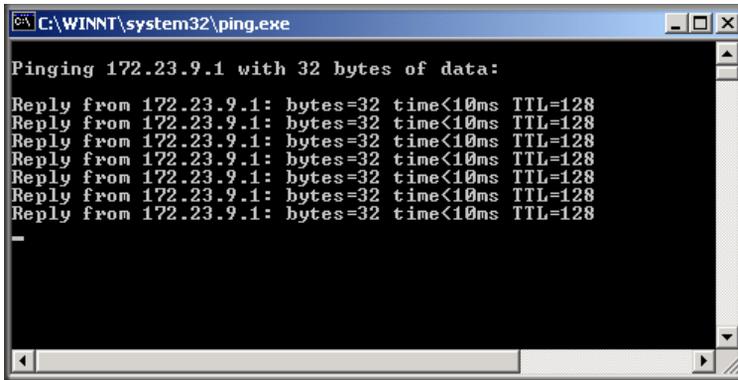
**Figure B-10**

5. Configure the DG834GSP as in the Gateway-to-Gateway procedures using the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration” on page 8-21](#)), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

Device	LAN IP Address	LAN Subnet Mask
DG834GSP	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

- a. In Step 1, enter **toFVL328** for the Connection Name.
 - b. In Step 2, enter **fv1328.dyndns.org** for the remote WAN's IP address.
 - c. In Step 3, enter the following:
 - IP Address = **172.23.9.1**
 - Subnet Mask = **255.255.255.0**
6. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration” on page 8-21](#)), being certain to use appropriate network addresses for the environment.
 - a. In Step 1, enter **toDG834** for the Connection Name.
 - b. In Step 2, enter **dg834g.dyndns.org** for the remote WAN's IP address.
 - c. In Step 3, enter the following:
 - IP Address = **10.5.6.1**
 - Subnet Mask = **255.255.255.0**
7. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834GSP.
 - a. Open the command prompt (Start -> Run -> cmd)
 - b. ping 172.23.9.1



```
C:\WINNT\system32\ping.exe

Pinging 172.23.9.1 with 32 bytes of data:

Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
-
```

Figure B-11



Note: The pings may fail the first time. If this happens, try the pings a second time.

Configuration Summary (Telecommuter Example)

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 B-3. Configuration summary (telecommuter example)

VPN Consortium Scenario:	Scenario 1
Type of VPN:	PC/client-to-gateway, with client behind NAT router
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
Gateway	Fully Qualified Domain Name (FQDN)
Client	Dynamic

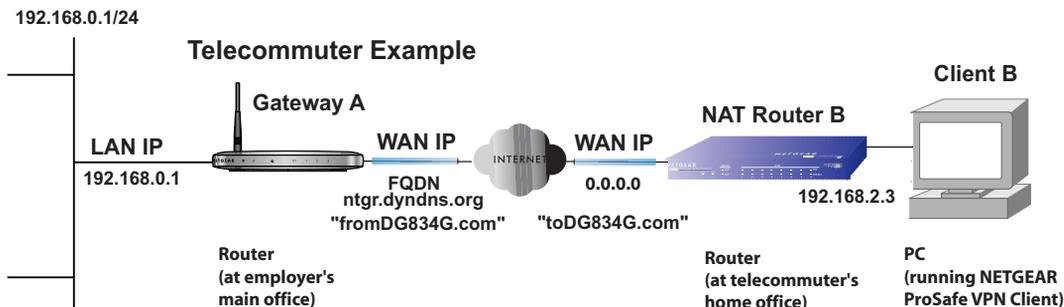


Figure B-12

Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves the following two steps:

- [Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office.](#)

- [Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office](#) configures the NETGEAR ProSafe VPN Client endpoint.

Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office

Follow this procedure to configure a client-to-gateway VPN tunnel by filling out the VPN Auto Policy screen.

1. Log in to the VPN router at its LAN address of <http://10.1.1.1> with its default user name of **admin** and password of **password**. Click the **VPN Policies** link in the main menu to display the VPN Policies screen. Click **Add Auto Policy** to proceed and enter the information.

VPN - Auto Policy

General

Policy Name: fromDG834G ← **fromDG834GSP (in the example) Dynamic IP address**

Remote VPN Endpoint Address Type: Dynamic IP address

Address Data: n/a

NetBIOS Enable

IKE Keep Alive ← **IKE Keep Alive is optional; must match Remote LAN IP Address when enabled (remote PC must respond to pings)**

Ping IP Address: 192 . 168 . 2 . 3

Local LAN

IP Address Subnet address ← **Subnet address**

Single/Start address: 192 . 168 . 0 . 1 ← **192.168.0.1 (in this example) 255.255.255.0**

Finish address:

Subnet Mask: 255 . 255 . 255 . 0

Remote LAN

IP Address Single address ← **Single address**

Single/Start IP address: 192 . 168 . 2 . 3 ← **192.168.2.3 (in this example) (Remote NAT router must have Address Reservation set and VPN Passthrough enabled)**

Finish IP address:

Subnet Mask:

IKE

Direction: Responder only

Exchange Mode: Main Mode ← **Main Mode**

Diffie-Hellman (DH) Group: Auto

Local Identity Type: Fully Qualified Domain Name ← **Fully Qualified Domain Name fromDG834G.com (in this example)**

Data: fromDG834G.com ← **Fully Qualified Domain Name toDG834G.com (in this example)**

Remote Identity Type: Fully Qualified Domain Name ← **Fully Qualified Domain Name toDG834G.com (in this example)**

Data: toDG834G.com

Parameters

Encryption Algorithm: 3DES ← **3DES**

Authentication Algorithm: Auto

Pre-shared Key: 12345678 ← **12345678 (in this example) 3600**

SA Life Time: 3600 (seconds)

Enable PFS (Perfect Forward Security)

Buttons: Back, Apply, Cancel

Figure B-13

- Click **Apply** when done to get the **VPN Policies** screen.



VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	fromDG834G	Auto	192.168.0.1 / 255.255.255.0	192.168.2.3	3DES

Edit Delete

Apply Cancel

Add Auto Policy Add Manual Policy

Figure B-14

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office

This procedure describes how to configure the 54 Mbps ADSL Modem Wireless Router Model DG834GSP. We will assume the PC running the client has a dynamically assigned IP address.

The PC must have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (<http://www.netgear.com>) and select **VPN01L_VPN05L** in the **Product Quick Find** drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.



Note: Before installing the 54 Mbps ADSL Modem Wireless Router Model DG834GSP software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
 - a. You may need to insert your Windows CD to complete the installation.
 - b. If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating “The **NETGEAR ProSafe VPN** Component requires at least one dial-up adapter be installed.” You can disregard this message.
 - c. Install the **IPSec** Component. You may have the option to install either the **VPN Adapter** or the **IPSec Component** or both. The **VPN Adapter** is not necessary.
 - d. The system should show the **ProSafe** icon () in the system tray after rebooting.
 - e. Double-click the system tray icon to open the **Security Policy Editor**.
2. Add a new connection.
 - a. Run the **NETGEAR ProSafe Security Policy Editor** program and create a **VPN Connection**.

- b. From the **Edit** menu of the **Security Policy Editor**, click **Add**, then **Connection**. A **New Connection** listing appears in the list of policies. Rename the **New Connection** so that it matches the **Connection Name** you entered in the **VPN Settings** of the DG834GSP on Gateway A.



Note: In this example, the **Connection Name** used on the client side of the VPN tunnel is **to DG834GSP** and it does not have to match the **VPN_client Connection Name** used on the gateway side of the VPN tunnel (see [Figure B-16](#)) because Connection Names are arbitrary to how the VPN tunnel functions.



Tip: Choose Connection Names that make sense to the people using and administrating the VPN.

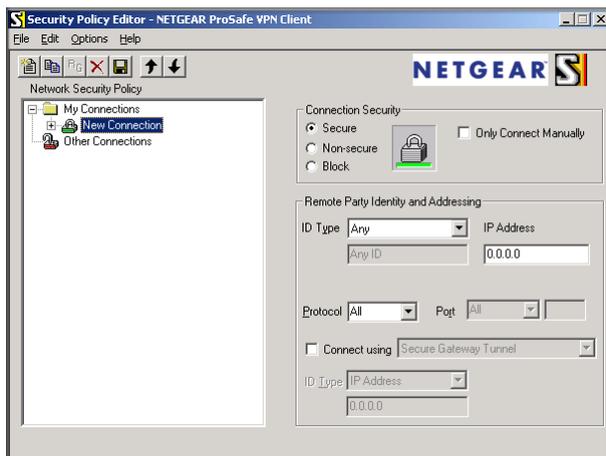


Figure B-15

- b. Click on the **Security Policy** subheading to show the **Security Policy** menu.

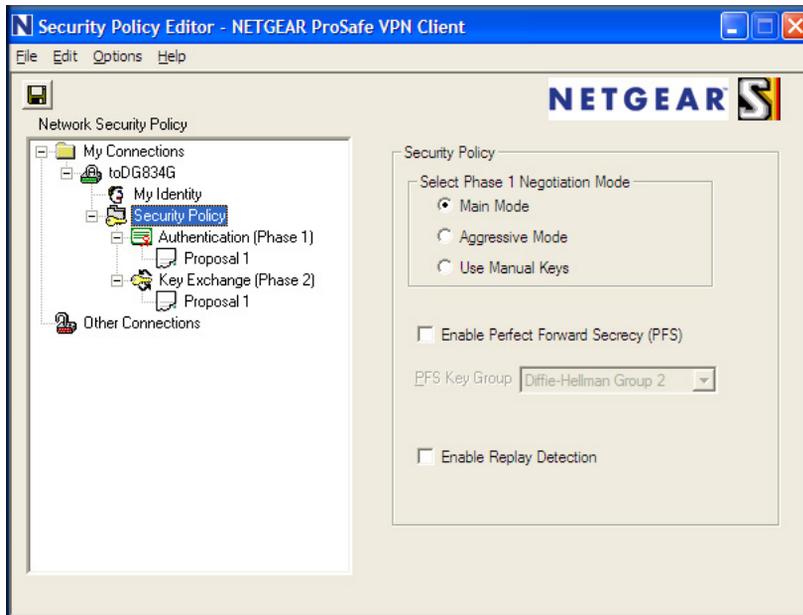


Figure B-17

- c. Select the **Main Mode** in the **Select Phase 1 Negotiation Mode** check box.
4. Configure the **VPN Client Identity**.

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834GSP and either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

- a. In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, click **My Identity**.

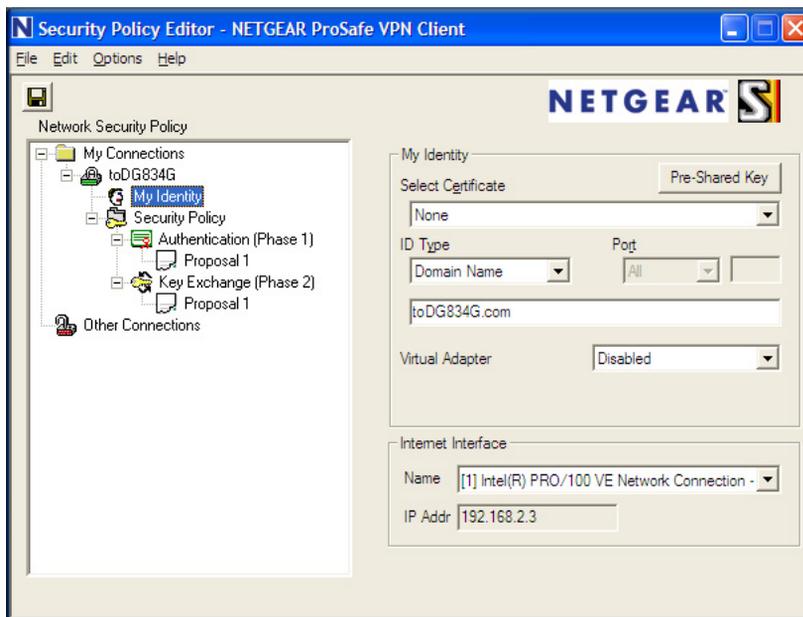


Figure B-18

- b. Choose **None** in the **Select Certificate** menu.
- c. Select **Domain Name** in the **ID Type** menu and enter **toDG834G.com** (in this example) in the box below it. Choose **Disabled** in the **Virtual Adapter** menu.
- d. In the **Internet Interface** box, select **Intel PRO/100VE Network Connection** (in this example, your Ethernet adapter may be different) in the **Name** menu and enter **10.1.2.3** (in this example) in the **IP Addr** box.

- e. Click the **Pre-Shared Key** button.



Figure B-19

- f. In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834GSP's **Pre-Shared Key** and click **OK**. In this example, **12345678** is entered. This field is case sensitive.
5. Configure the **VPN Client Authentication Proposal**.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the VPN router configuration.

 - a. In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, expand the **Security Policy** heading by double clicking its name or clicking on the “+” symbol.
 - b. Expand the **Authentication** subheading by double clicking its name or clicking on the “+” symbol. Then select **Proposal 1** below **Authentication**.

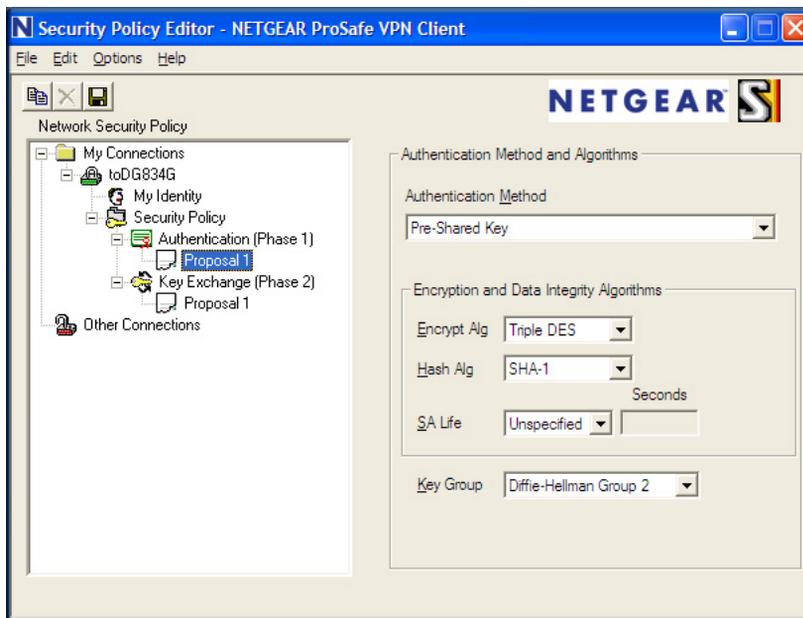


Figure B-20

- c. In the **Authentication Method** menu, select **Pre-Shared key**.
 - d. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.
 - e. In the **Hash Alg** menu, select **SHA-1**.
 - f. In the **SA Life** menu, select **Unspecified**.
 - g. In the **Key Group** menu, select **Diffie-Hellman Group 2**.
6. Configure the **VPN Client Key Exchange Proposal**.

In this step, you will provide the type of encryption (**DES** or **3DES**) to be used for this connection. This selection must match your selection in the VPN router configuration.

- a. Expand the **Key Exchange** subheading by double clicking its name or clicking on the “+” symbol. Then select **Proposal 1** below **Key Exchange**.

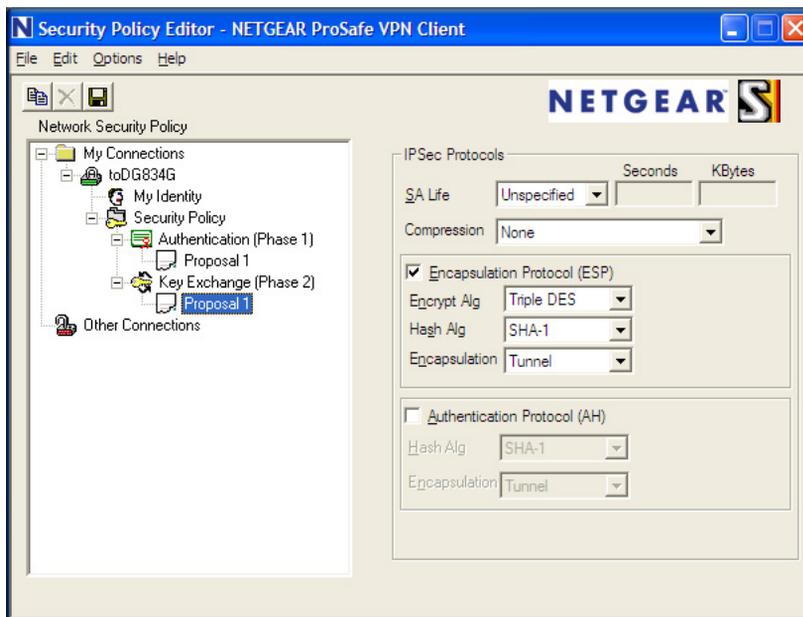


Figure B-21

- b. In the **SA Life** menu, select **Unspecified**.
 - c. In the **Compression** menu, select **None**.
 - d. Check the **Encapsulation Protocol (ESP)** checkbox.
 - e. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.
 - f. In the **Hash Alg** menu, select **SHA-1**.
 - g. In the **Encapsulation** menu, select **Tunnel**.
 - h. Leave the **Authentication Protocol (AH)** checkbox unchecked.
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.

8. Check the **VPN Connection**.

To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the ADSL Modem Wireless Router menu bar (see [Figure B-22](#)). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

- a. Right-click the system tray icon to open the popup menu.
- b. Select **Connect** to open the **My Connections** list.
- c. Choose **toDG834G**.

The 54 Mbps ADSL Modem Wireless Router Model DG834GSP will report the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.



Figure B-22

To perform a ping test using our example, start from the remote PC:

- a. Establish an Internet connection from the PC.
- b. On the **Windows** taskbar, click the **Start** button, and then click **Run**.

- c. Type **ping -t 10.1.1.1**, and then click **OK**.

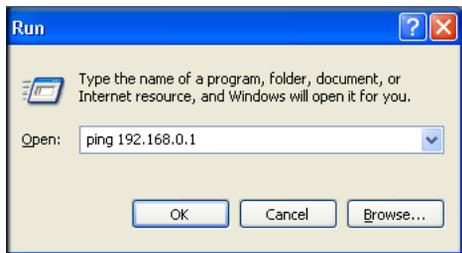


Figure B-23

This will cause a continuous ping to be sent to the VPN router. After between several seconds and two minutes, the ping response should change from **timed out** to **reply**.

```
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

Figure B-24

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another PC already has the VPN router management interface open).



Note: You can use the VPN router diagnostic utilities to test the VPN connection from the VPN router to the client PC. Run ping tests from the **Diagnostics** link of the VPN router main menu.

Monitoring the VPN Tunnel (Telecommuter Example)

Viewing the PC Client's Connection Monitor and Log Viewer

To view information on the progress and status of the VPN client connection, open the 54 Mbps ADSL Modem Wireless Router Model DG834GSP **Log Viewer**.

1. To launch this function, click on the Windows **Start** button, then select **Programs**, then **54 Mbps ADSL Modem Wireless Router Model DG834GSP**, then **Log Viewer**.

	Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.
---	---

2. The **Connection Monitor** screen is shown below:

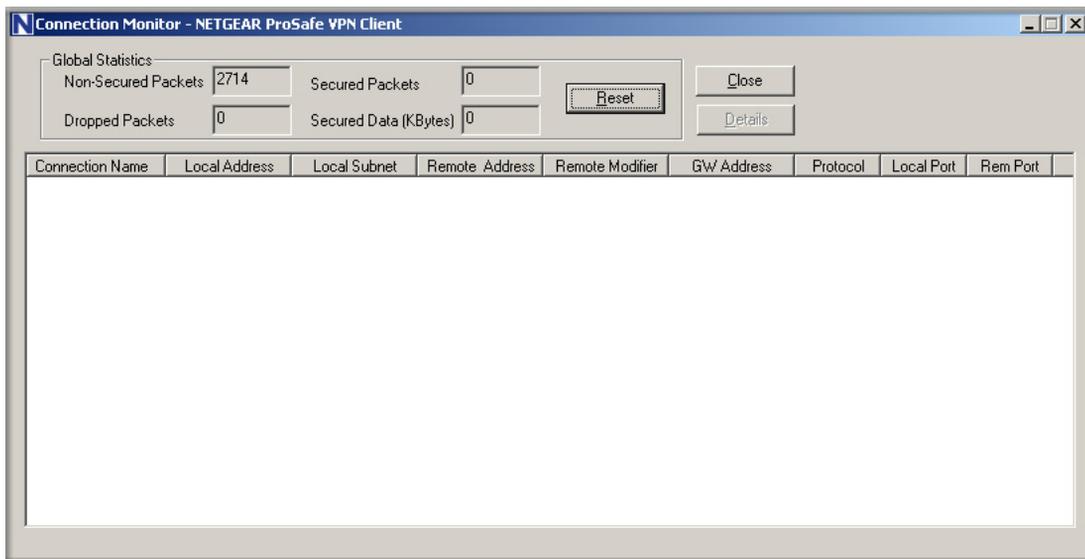


Figure B-25

While the connection is being established, the **Connection Name** field in this menu will show **SA** before the name of the connection. When the connection is successful, the **SA** will change to the yellow key symbol.



Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

Viewing the VPN Router's VPN Status and Log Information

To view information on the status of the VPN client connection, open the VPN router's VPN Status screen by following the steps below:

1. To view this screen, click the **Router Status** link of the VPN router's main menu, then click the **VPN Status** button. The **VPN Status/Log** screen for a connection is shown below:

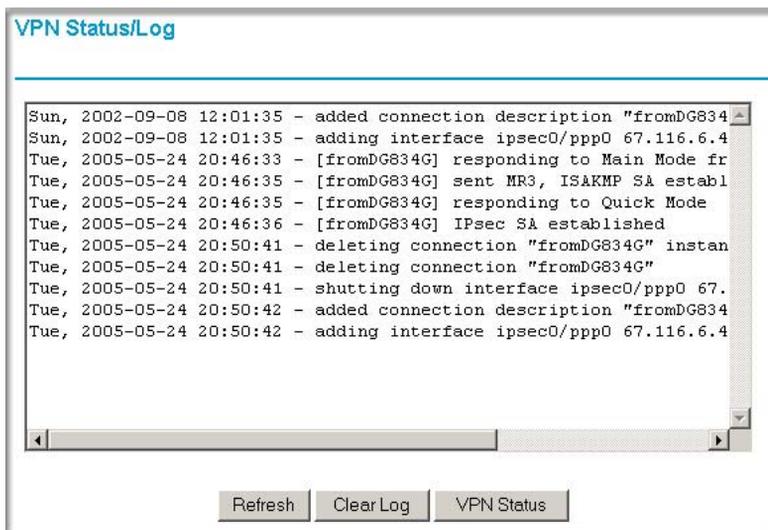
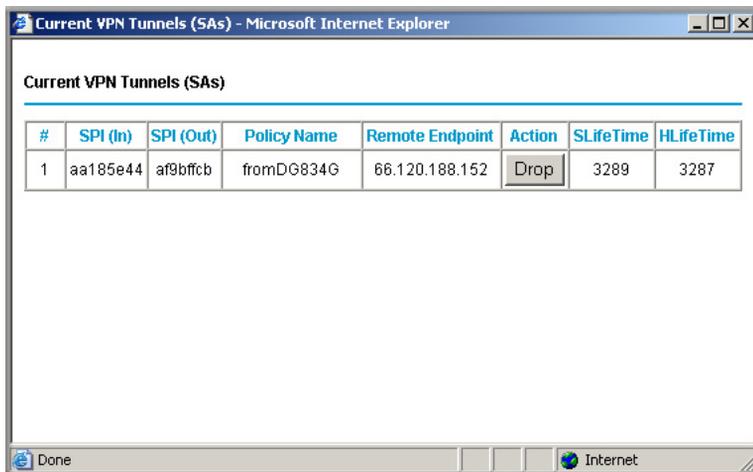


Figure B-26

2. To view the VPN tunnels status, click the **VPN Status** link on the right side of the main menu.



The screenshot shows a web browser window titled "Current VPN Tunnels (SAs) - Microsoft Internet Explorer". The main content area displays a table with the following data:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffc3	fromDG834G	66.120.188.152	Drop	3289	3287

The browser's status bar at the bottom shows "Done" on the left and "Internet" on the right.

Figure B-27

