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

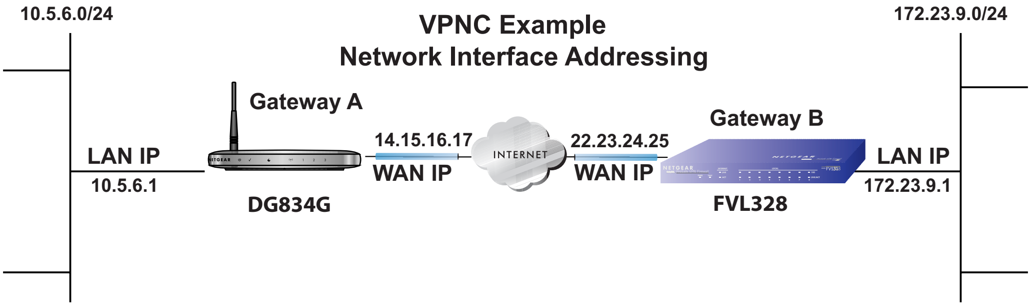


Figure B-1

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:

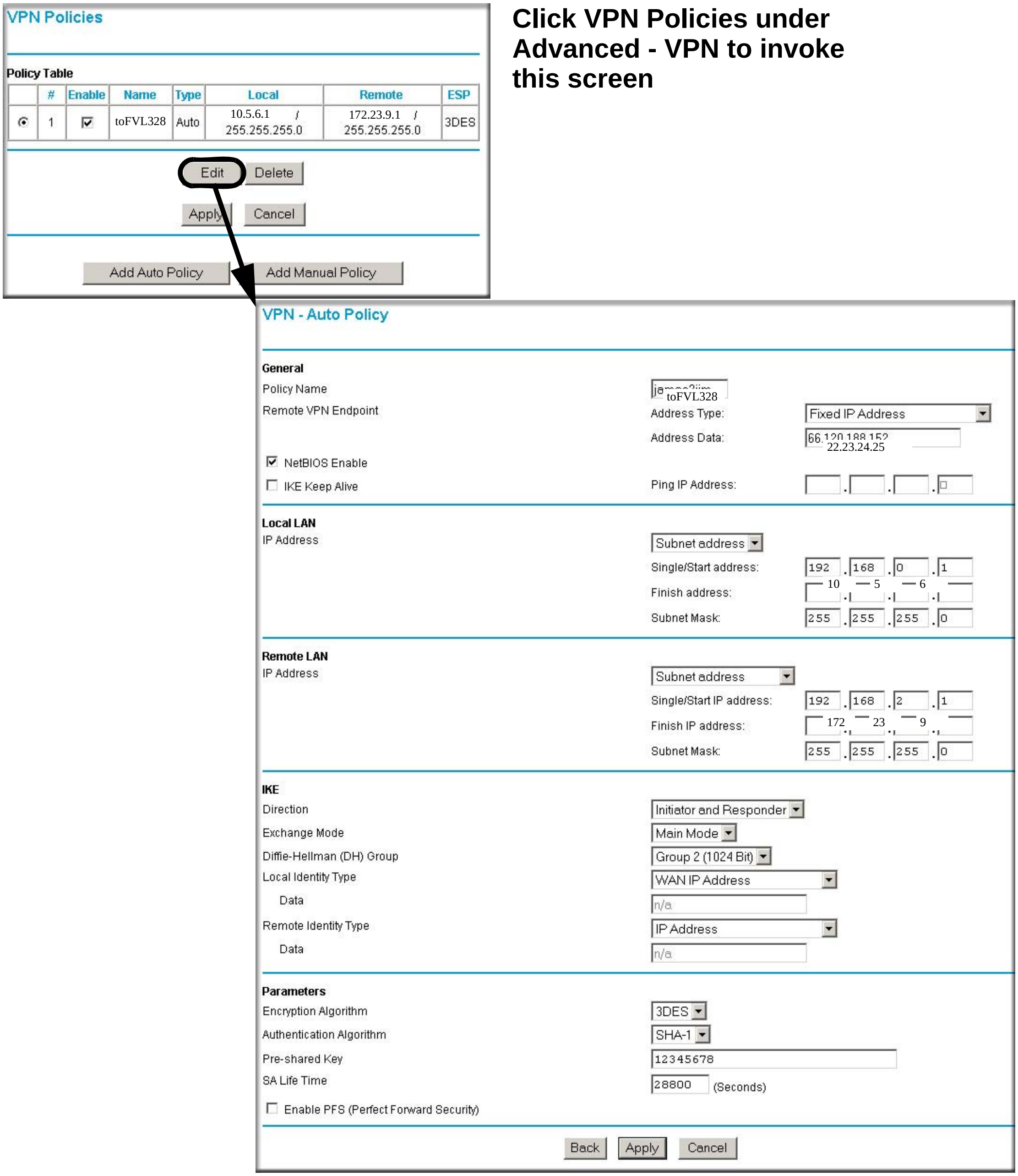
Unit	WAN IP	LAN IP	LAN Subnet Mask
DG834G	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

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**



Click VPN Policies under Advanced - VPN to invoke this screen

VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
●	1	☑	toFVL328	Auto	10.5.6.1 / 255.255.255.0	172.23.9.1 / 255.255.255.0	3DES

VPN - Auto Policy

General

Policy Name	toFVL328		
Remote VPN Endpoint	Address Type:	Fixed IP Address	
	Address Data:	22.23.24.25	
☑ NetBIOS Enable			
☐ IKE Keep Alive	Ping IP Address:	. . . 0	

Local LAN

IP Address	Subnet address	
	Single/Start address:	192 . 168 . 0 . 1
	Finish address:	10 . 5 . 6 .
	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 .
	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

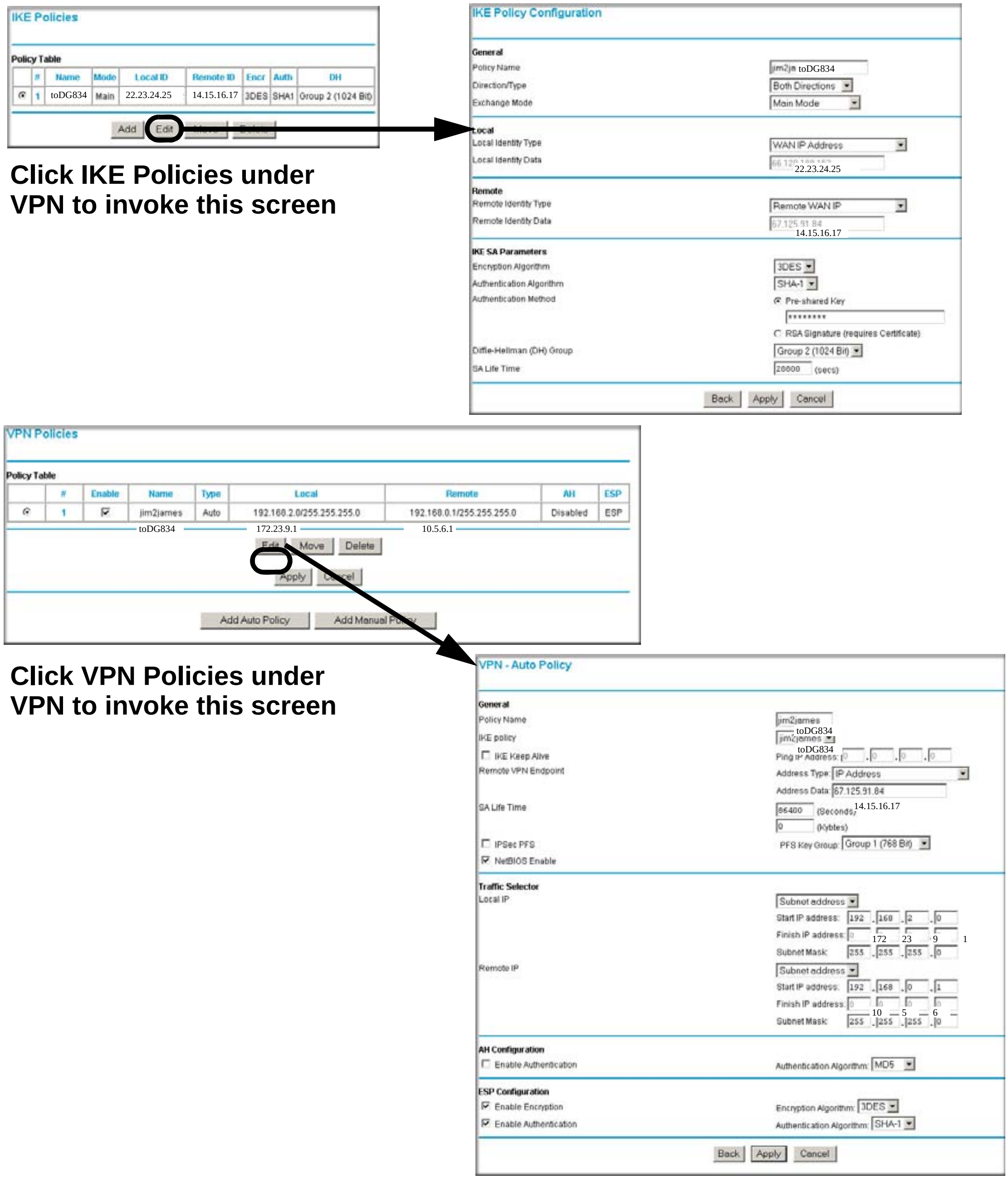
Parameters

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
●	1	toDG834	Main	22.23.24.25	14.15.16.17	3DES	SHA1	Group 2 (1024 Bit)

Click IKE Policies under VPN to invoke this screen

IKE Policy Configuration

General

Policy Name: jim2ja toDG834

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity Type: WAN IP Address

Local Identity Data: 66.12 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)

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

SA Life Time: 28800 (secs)

VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
●	1	☑	jim2james	Auto	192.168.2.0/255.255.255.0	192.168.0.1/255.255.255.0	Disabled	ESP
			toDG834		172.23.9.1	10.5.6.1		

Click VPN Policies under VPN to invoke this screen

VPN - Auto Policy

General

Policy Name: jim2james toDG834

IKE policy: jim2james toDG834

☐ IKE Keep Alive — Ping IP Address: 0 . 0 . 0 . 0

Remote VPN Endpoint — Address Type: IP Address

Address Data: 67.125.91.84 14.15.16.17

SA Life Time: 86400 (Seconds)

0 (Kbytes)

☐ IPSec PFS — PFS Key Group: Group 1 (768 Bit)

☑ NetBIOS Enable

Traffic Selector

Local IP: Subnet address

Start IP address: 192 . 168 . 2 . 0

Finish IP address: 0 172 23 9 1

Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Subnet address

Start IP address: 192 . 168 . 0 . 1

Finish IP address: 0 . 0 . 0 . 0 10 5 6

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

☐ Enable Authentication — Authentication Algorithm: MD5

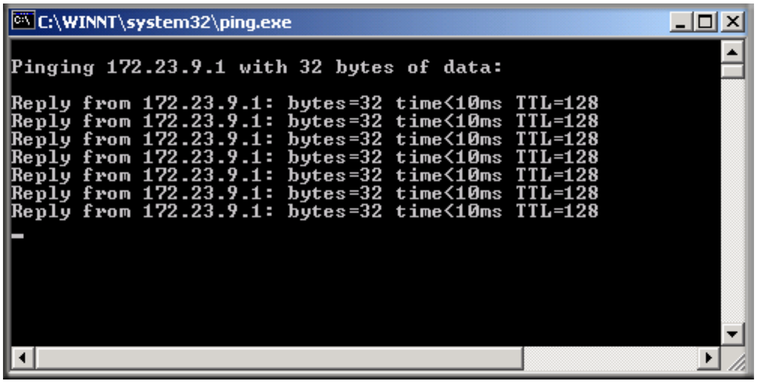
ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

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



```
Pinging 172.23.9.1 with 32 bytes of data:

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

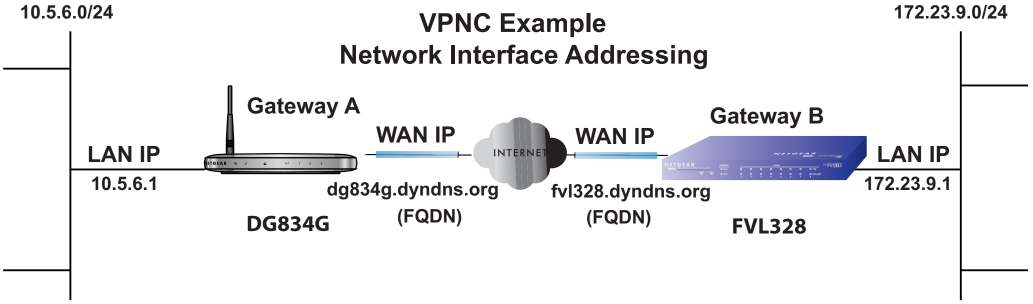


Figure B-5

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

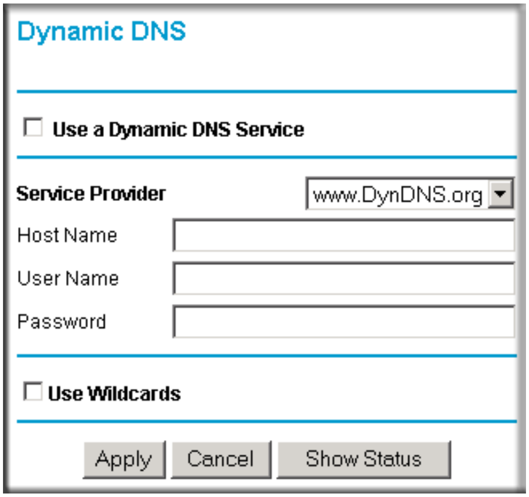
1. Log in to the DG834GSP labeled Gateway A as in the illustration.

   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.



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name:

User Name:

Password:

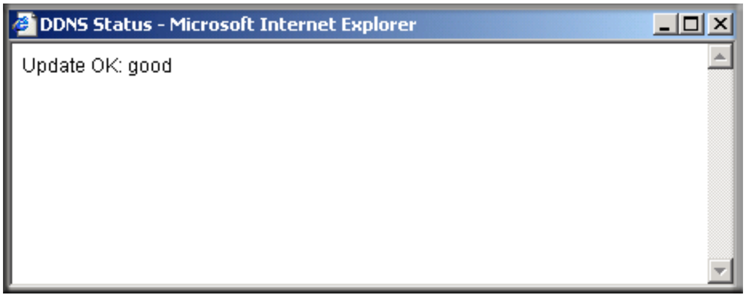
□ Use Wildcards

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).



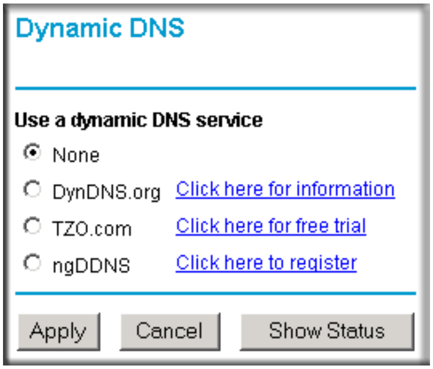
DDNS Status - Microsoft Internet Explorer

Update OK: good

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.



Dynamic DNS

Use a dynamic DNS service

● None

○ DynDNS.org Click here for information

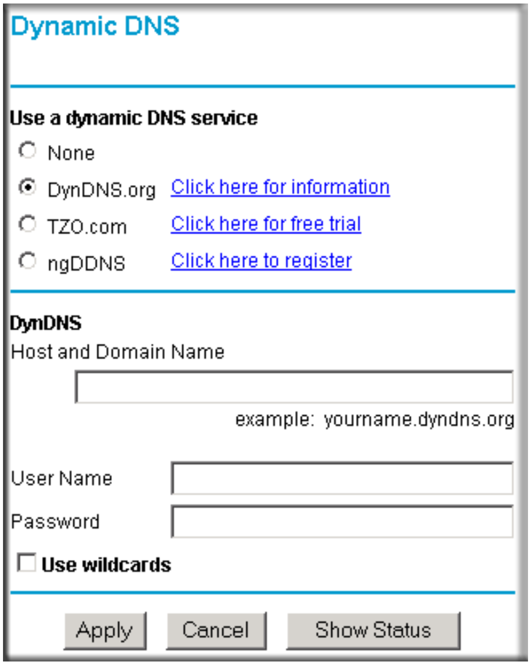
○ TZO.com Click here for free trial

○ ngDDNS Click here to register

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 = fvl328.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

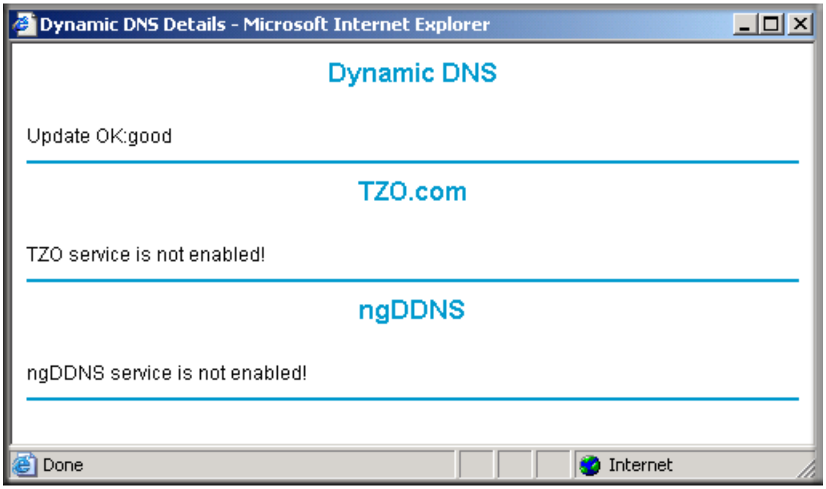
User Name

Password

□ **Use wildcards**

Figure B-9

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



Dynamic DNS Details - Microsoft Internet Explorer

Dynamic DNS

Update OK:good

TZO.com

TZO service is not enabled!

ngDDNS

ngDDNS service is not enabled!

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 **fvl328.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.

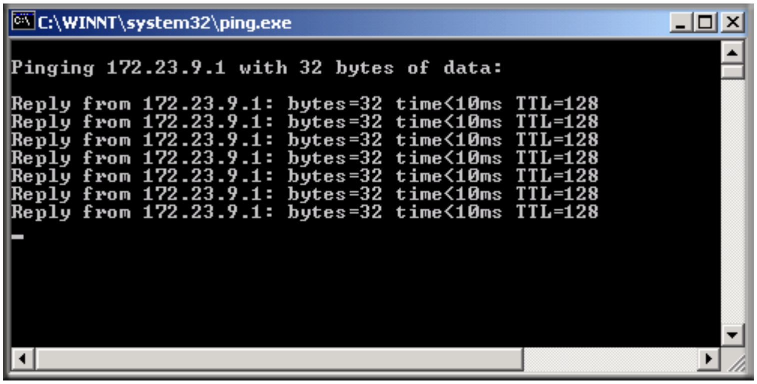
   c. In Step 3, enter the following:

      - 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



```
Pinging 172.23.9.1 with 32 bytes of data:

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

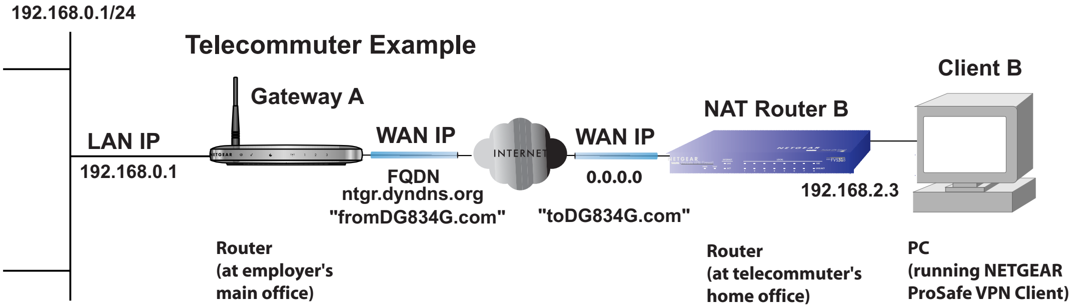


Figure B-12

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:

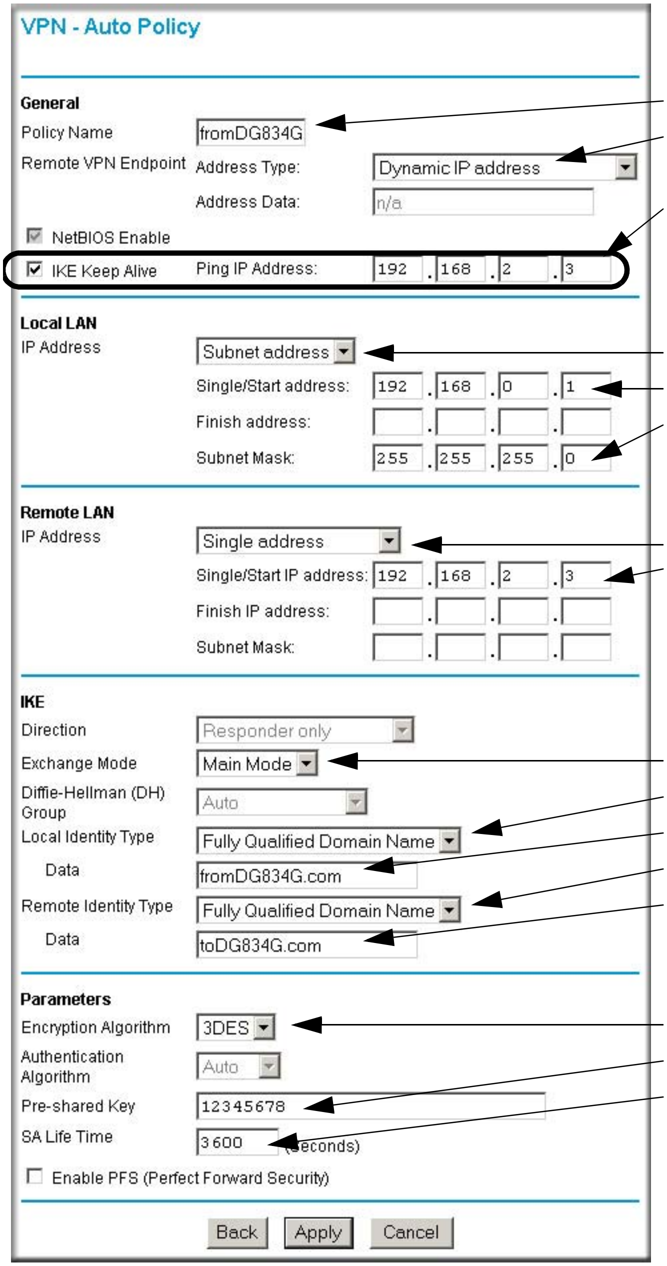
- Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office.

- 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

Remote VPN Endpoint: Address Type: Dynamic IP address; Address Data: n/a

☑ NetBIOS Enable

☑ IKE Keep Alive — Ping IP Address: 192 . 168 . 2 . 3

Local LAN

IP Address: Subnet address

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

Finish address: . . .

Subnet Mask: 255 . 255 . 255 . 0

Remote LAN

IP Address: Single address

Single/Start IP address: 192 . 168 . 2 . 3

Finish IP address: . . .

Subnet Mask: . . .

IKE

Direction: Responder only

Exchange Mode: Main Mode

Diffie-Hellman (DH) Group: Auto

Local Identity Type: Fully Qualified Domain Name

Data: fromDG834G.com

Remote Identity Type: Fully Qualified Domain Name

Data: toDG834G.com

Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: Auto

Pre-shared Key: 12345678

SA Life Time: 3600 (Seconds)

☐ Enable PFS (Perfect Forward Security)

fromDG834GSP (in the example)
Dynamic IP address

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

Subnet address
192.168.0.1 (in this example)
255.255.255.0

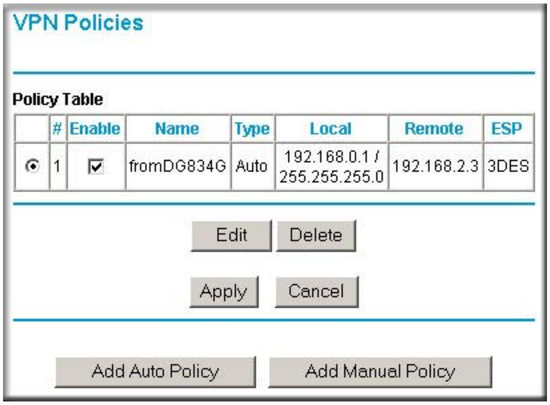
Single address
192.168.2.3 (in this example)
(Remote NAT router must have **Address Reservation** set and **VPN Passthrough** enabled)

Main Mode
Fully Qualified Domain Name
fromDG834G.com (in this example)
Fully Qualified Domain Name
toDG834G.com (in this example)

3DES
12345678 (in this example)
3600

Figure B-13

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



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
●	1	☑	fromDG834G	Auto	192.168.0.1 / 255.255.255.0	192.168.2.3	3DES

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 NETGEA 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 (S) in the system tray after rebooting.

   e. Double-click the system tray icon to open the **Security Policy Editor**.

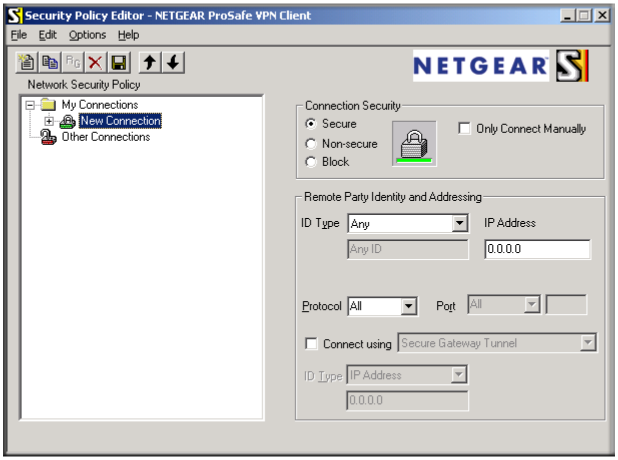
2. Add a new connection.

   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.

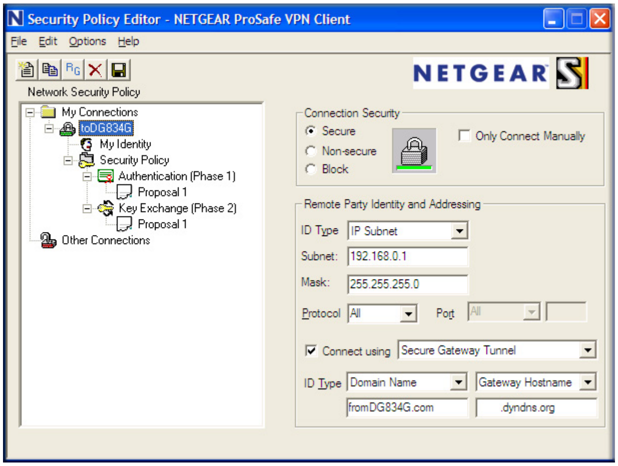
➡	**Tip:** Choose Connection Names that make sense to the people using and administrating the VPN.



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

Remote Party Identity and Addressing
ID Type: Any
Any ID
IP Address: 0.0.0.0
Protocol: All
Port: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Figure B-15



Connection Security

● Secure
○ Non-secure
○ Block

□ Only Connect Manually

Remote Party Identity and Addressing

ID Type: IP Subnet
Subnet: 192.168.0.1
Mask: 255.255.255.0
Protocol: All Port: All

☑ Connect using Secure Gateway Tunnel

ID Type: Domain Name | Gateway Hostname
fromDG834G.com | .dyndns.org

Figure B-16

c. Select **Secure** in the **Connection Security** check-box group.

d. Select **IP Subnet** in the **ID Type** menu.

e. In this example, type **10.1.1.1** in the Subnet field as the network address of the DG834GSP.

f. Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834GSP.

g. Select **All** in the **Protocol** menu to allow all traffic through the VPN tunnel.

h. Select the **Connect using Secure Gateway Tunnel** check box.

i. Select **Domain Name** in the **ID Type** menu below the check box and enter **fromDG834G.com** (in this example).

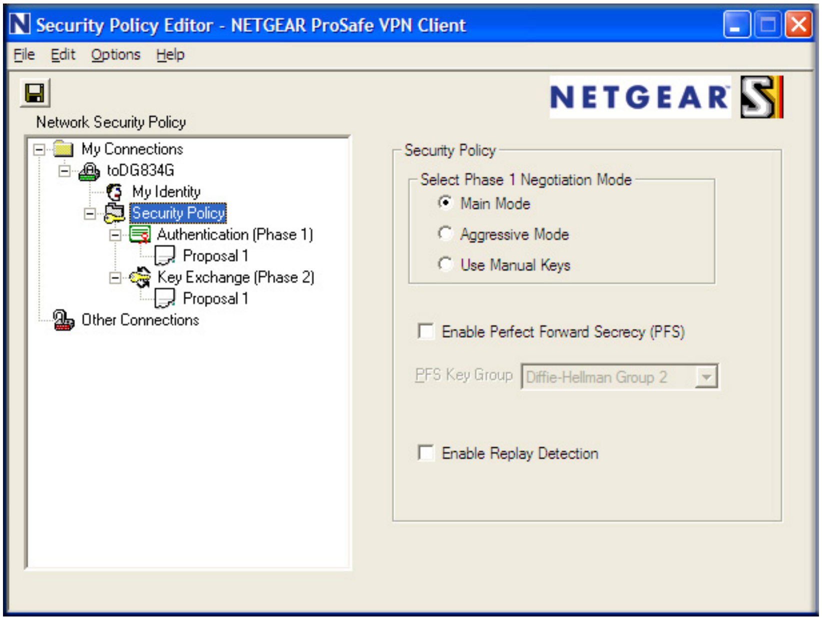
j. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

k. The resulting Connection Settings are shown in Figure B-16.

3. Configure the **Security Policy** in the 54 Mbps ADSL Modem Wireless Router Model DG834GSP software.

   a. In the **Network Security Policy** list, expand the new connection by double clicking its name or clicking on the “+” symbol. **My Identity** and **Security Policy** subheadings appear below the connection name.

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



Network Security Policy

- My Connections
  - toDG834G
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
- Other Connections

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

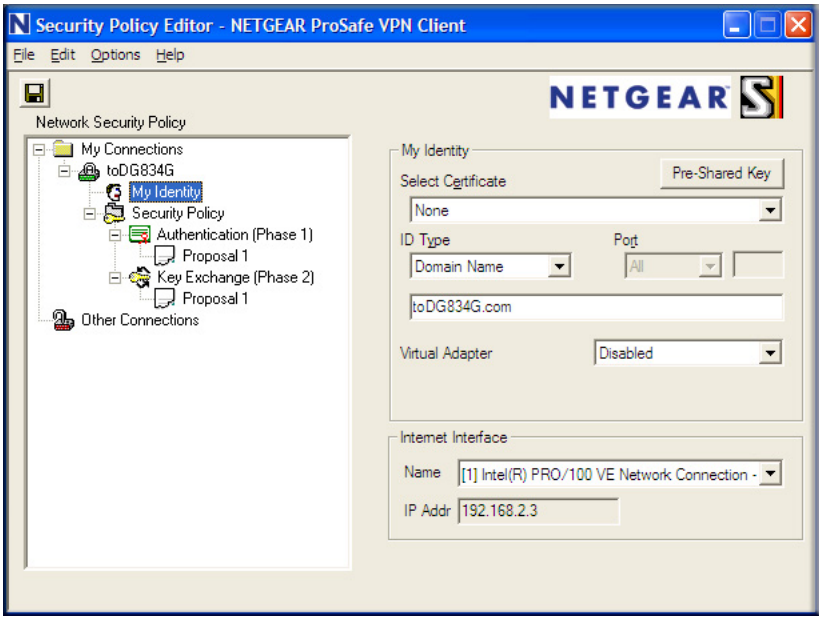
Figure B-17

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**.



Select Certificate: None

ID Type: Domain Name

Port: All

toDG834G.com

Virtual Adapter: Disabled

Name: [1] Intel(R) PRO/100 VE Network Connection -

IP Addr: 192.168.2.3

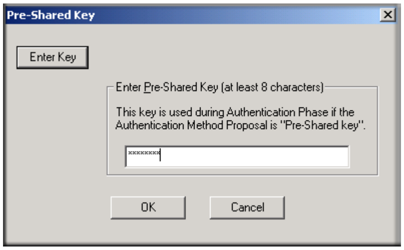
Figure B-18

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.



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".

xxxxxxxx

OK | Cancel

Figure B-19

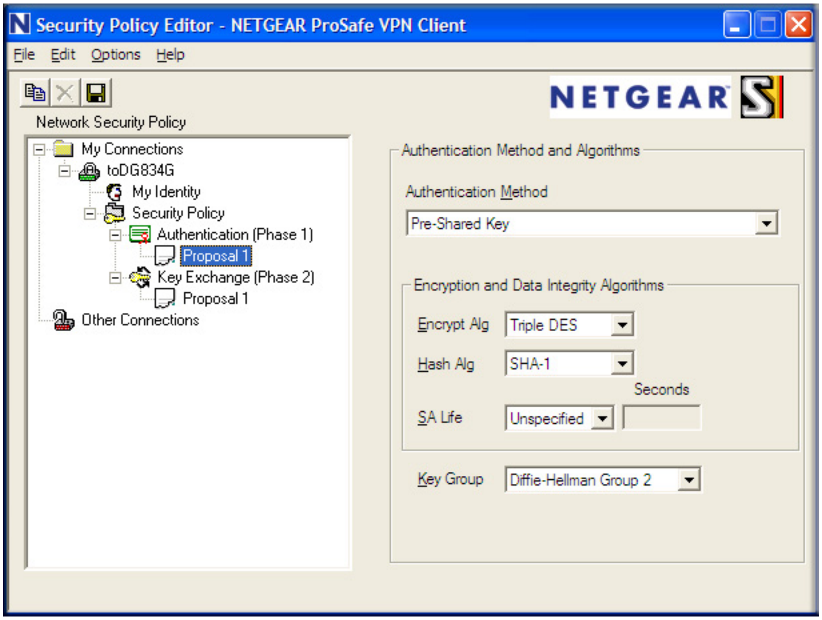
f. In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834GSP's **Pre-Shared Key** and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

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**.



Security Policy Editor - NETGEAR ProSafe VPN Client

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 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**.

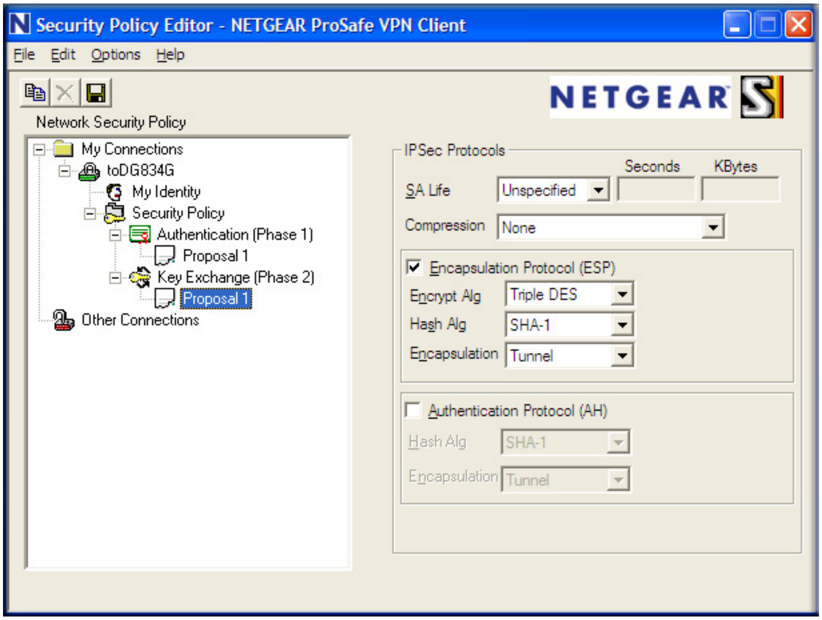
f. In the **SA Life** menu, select **Unspecified**.

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**.



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 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**.

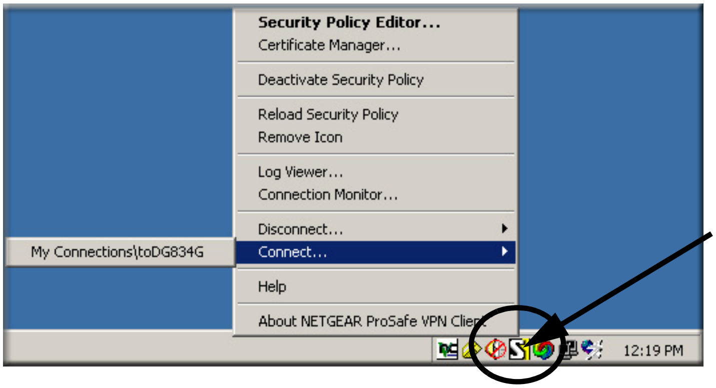
To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the ADSL Modem Wireless Router menu bar (see Figure B-22). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

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.



Right-mouse-click on the system tray icon to open the popup menu.

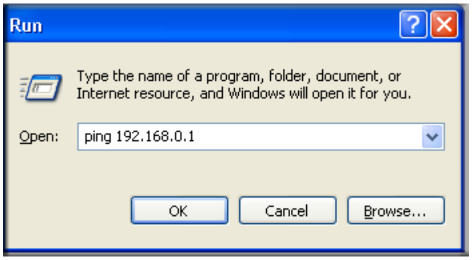
Figure B-22

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**.

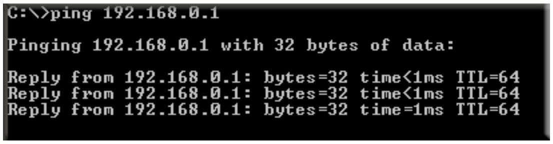
c. Type **ping -t 10.1.1.1**, and then click **OK**.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: ping 192.168.0.1

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)

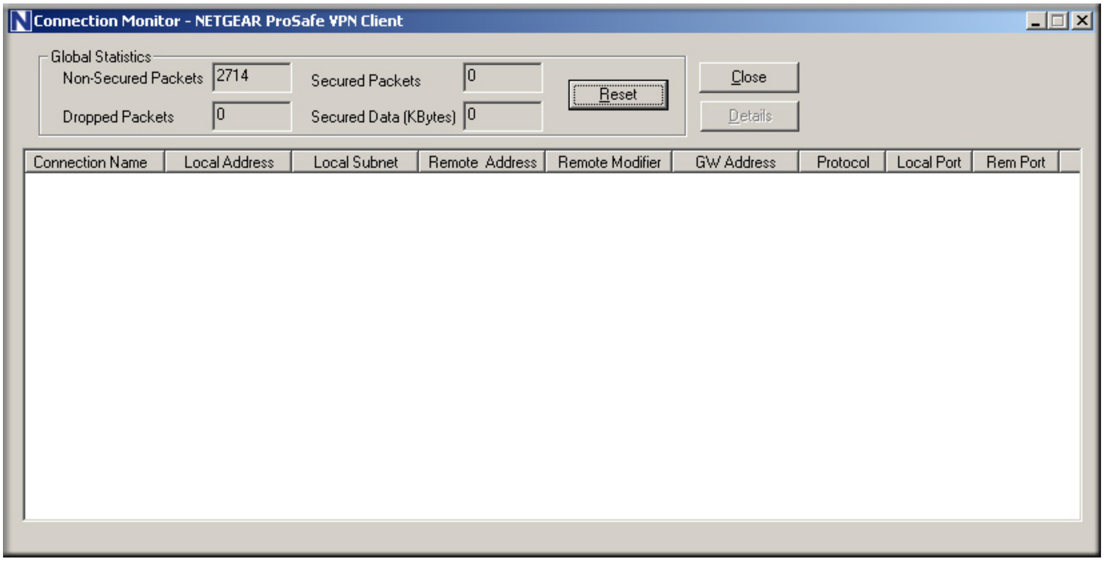
Viewing the PC Client's Connection Monitor and Log Viewer

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:



Connection Monitor - NETGEAR ProSafe VPN Client

Global Statistics

Non-Secured Packets: 2714

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

Figure B-25

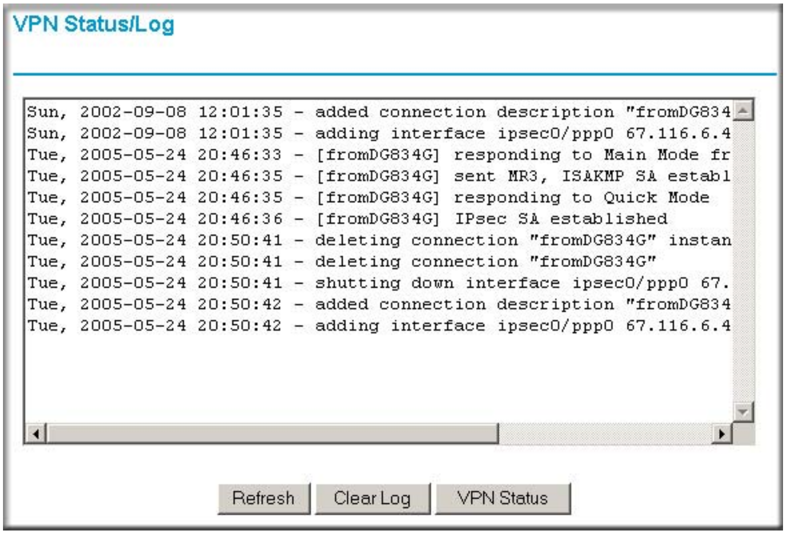
While the connection is being established, the **Connection Name** field in this menu will show **SA** before the name of the connection. When the connection is successful, the **SA** will change to the yellow key symbol.

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:

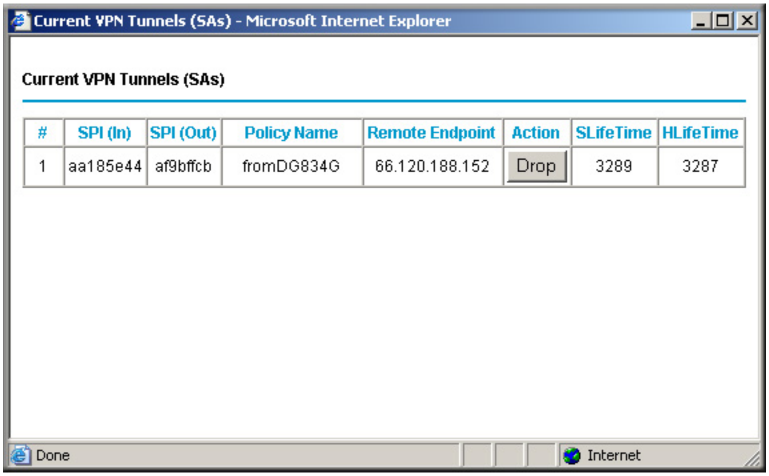
1. To view this screen, click the **Router Status** link of the VPN router's main menu, then click the **VPN Status** button. The **VPN Status/Log** screen for a connection is shown below:



```
Sun, 2002-09-08 12:01:35 - added connection description "fromDG834
Sun, 2002-09-08 12:01:35 - adding interface ipsec0/ppp0 67.116.6.4
Tue, 2005-05-24 20:46:33 - [fromDG834G] responding to Main Mode fr
Tue, 2005-05-24 20:46:35 - [fromDG834G] sent MR3, ISAKMP SA establ
Tue, 2005-05-24 20:46:35 - [fromDG834G] responding to Quick Mode
Tue, 2005-05-24 20:46:36 - [fromDG834G] IPsec SA established
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G" instan
Tue, 2005-05-24 20:50:41 - deleting connection "fromDG834G"
Tue, 2005-05-24 20:50:41 - shutting down interface ipsec0/ppp0 67.
Tue, 2005-05-24 20:50:42 - added connection description "fromDG834
Tue, 2005-05-24 20:50:42 - adding interface ipsec0/ppp0 67.116.6.4
```

Figure B-26

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



Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffcb	fromDG834G	66.120.188.152	Drop	3289	3287

Figure B-27