Note: When NETBIOS is enabled (which it is in the VPNC defaults implemented by the VPN Wizard), automatic traffic will reactivate the tunnel. To prevent reactivation from happening, either disable NETBIOS or disable the policy for the tunnel (see "Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel" on page 7-35).

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the Modem Router.
2. Open the DG834G v3 management interface and click **VPN Policies** to display the VPN Policies screen (Figure 7-39). Select the radio button for the VPN tunnel to be deleted and click the **Delete** button.

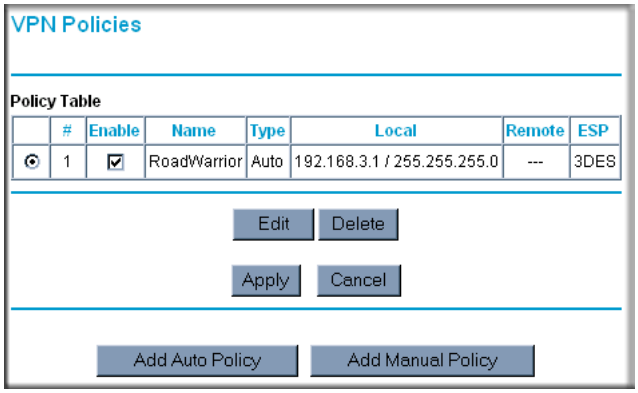


Figure 7-39

How to Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see Table 7-2) are not appropriate for your special circumstances, use one of the following alternatives:

- **Auto Policy**—for a typical automated Internet Key Exchange (IKE) setup, see "Using Auto Policy to Configure VPN Tunnels" on page 7-38. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.
- **Manual Policy**—for a Manual Keying setup in which you must specify each phase of the connection, see "Using Manual Policy to Configure VPN Tunnels" on page 7-48. Manual Policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834G v3 and the corresponding VPN endpoint gateway or client workstation.

Using Auto Policy to Configure VPN Tunnels

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end must match to the inbound VPN settings on other end, and vice versa.

See "Example of Using Auto Policy" on page 7-43 for an example of using Auto Policy.

Configuring VPN Network Connection Parameters

All VPN tunnels on the ADSL Modem Wireless Router require configuring several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios will use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to automatically generate and update the required encryption parameters.

Click the **VPN Policies** link of the main menu, and then click the **Add Auto Policy** button to display the VPN - Auto Policy menu shown in Figure 7-40.

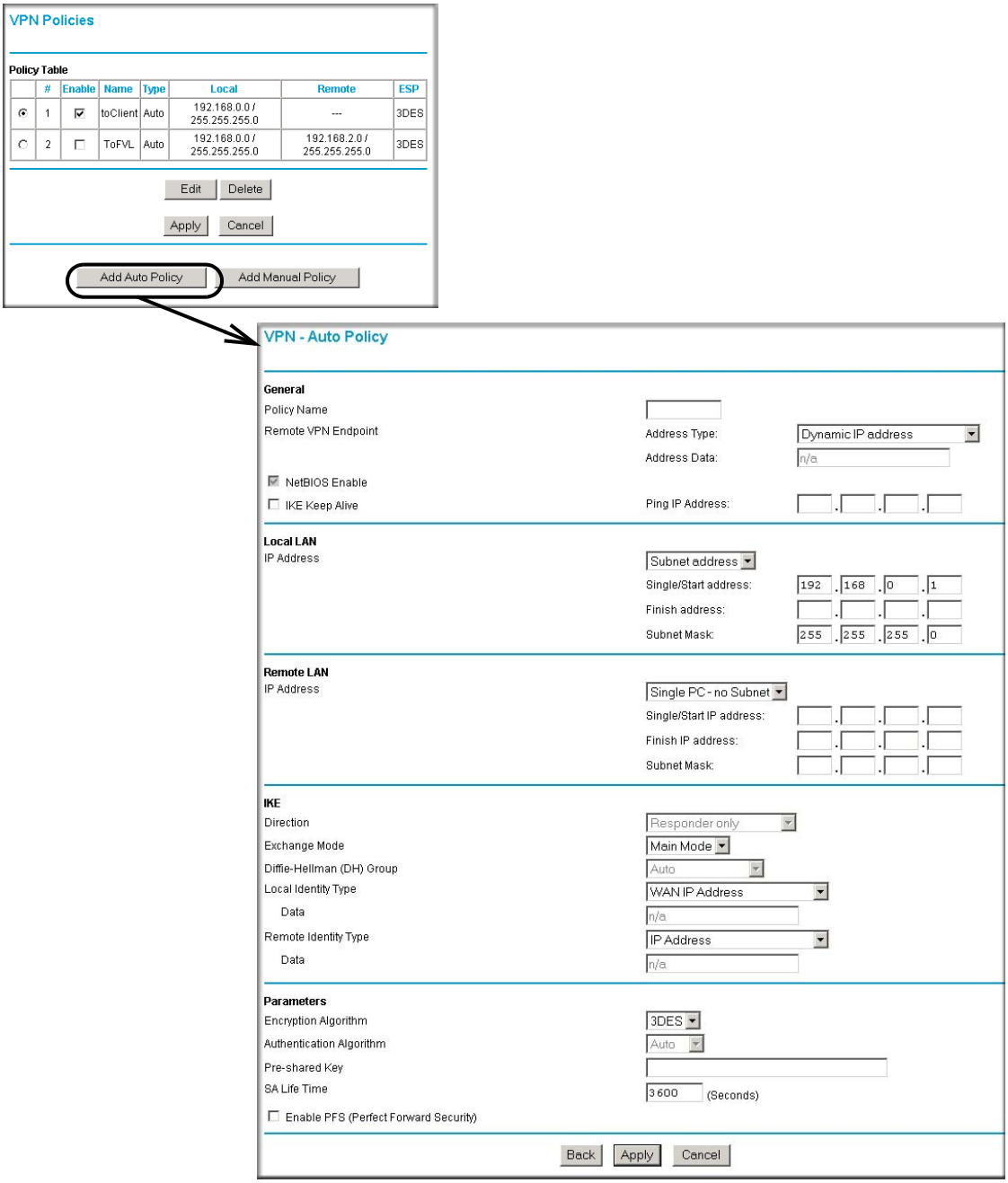

VPN Policies
Policy Table
Enable Name Type Local Remote ESP
1 toClient Auto 192.168.0.0 / 255.255.255.0 --- 3DES
2 ToFVL Auto 192.168.0.0 / 255.255.255.0 192.168.2.0 / 255.255.255.0 3DES
Edit
Delete
Apply
Cancel
Add Auto Policy
Add Manual Policy
VPN - Auto Policy
General
Policy Name
Remote VPN Endpoint
Address Type:
Dynamic IP address
Address Data:
n/a
NetBIOS Enable
IKE Keep Alive
Ping IP Address:
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 PC - no Subnet
Single/Start IP address:
Finish IP address:
Subnet Mask:
IKE
Direction
Responder only
Exchange Mode
Main Mode
Diffie-Hellman (DH) Group
Auto
Local Identity Type
WAN IP Address
Data
n/a
Remote Identity Type
IP Address
Data
n/a
Parameters
Encryption Algorithm
3DES
Authentication Algorithm
Auto
Pre-shared Key
SA Life Time
3600
(Seconds)
Enable PFS (Perfect Forward Security)
Back
Apply
Cancel

Figure 7-40

The DG834G v3 VPN tunnel network connection fields are defined as follows:

General. These settings identify this policy and determine its major characteristics.

- **Policy Name**—Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—If the remote endpoint has a dynamic IP address, select **Dynamic IP address**. No "Address Data" input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

	Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

- **NETBIOS Enable**—check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.
- **IKE Keep-alive**—Enable this if you wish to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when disconnected.

  The Ping IP Address must be associated with the remote endpoint. The remote LAN address must be used. This IP address will be "pinged" periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address must be covered by the remote LAN IP range and must correspond to a device that can respond to ping. The range should be made as narrow as possible to meet this objective.

Local LAN. This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.

Remote LAN. This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single address**—Enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

IKE. **Direction/Type**—this setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- **Responder only**—incoming connections are allowed, but outgoing connections will be blocked.
- **Initiator and Responder**—both incoming and outgoing connections are allowed.

Exchange Mode—ensure the remote VPN endpoint is set to use "Main Mode".

Diffie-Hellman (DH) Group—the Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.

Local Identity Type—select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.

- **WAN IP Address**—your Internet IP address.
- **Fully Qualified Domain Name**—your domain name.
- **Fully Qualified User Name**—your name, E-mail address, or other ID.

Local Identity Data—enter the data for the selection above. (If **WAN IP Address** is selected, no input is required.)

Remote Identity Type—select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.

- **IP Address**—the Internet IP address of the remote VPN endpoint.
- **Fully Qualified Domain Nam**e—the Domain name of the remote VPN endpoint.
- **Fully Qualified User Name**—the name, E-mail address, or other ID of the remote VPN endpoint.

Remote Identity Data—enter the data for the selection above. (If **IP Address** is selected, no input is required.)

Parameters. **Encryption Algorithm**—encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. DES and 3DES are supported.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

Authentication Algorithm—authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

Pre-shared Key—the key must be entered both here and on the remote VPN Gateway.

SA Life Time—this determines the time interval before the SA (Security Association) expires. (It will automatically be re-established as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.

IPSec PFS (Perfect Forward Secrecy)—if enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.

Example of Using Auto Policy

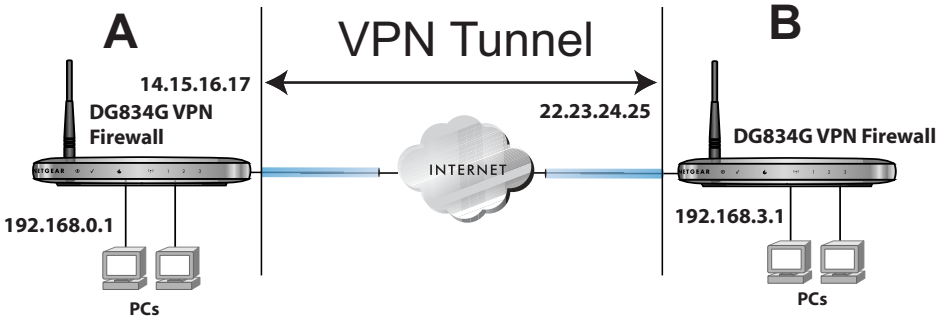


Figure 7-41

1. Set the LAN IPs on each DG834G v3 to different subnets and configure each properly for the Internet. The following settings are assumed for this example:

Table 7-5. VPN Tunnel Configuration Worksheet

Connection Name:	**GtoG**
Pre-Shared Key:	**12345678**
Secure Association -- Main Mode or Manual Keys:	**Main**
Perfect Forward Secrecy -- Enabled or Disabled:	**Disabled**
NETBIOS -- Enabled or Disabled:	**Enabled**
Encryption Protocol -- DES or 3DES:	**3DES**
Authentication Protocol -- MD5 or SHA-1:	**SHA-1**
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	**Group 2**
Key Life in seconds:	**28800 (8 hours)**
IKE Life Time in seconds:	**3600 (1 hour)**

VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
DG834G v3 A	**LAN_A**	**192.168.0.1**	**255.255.255.0**	**14.15.16.17**
DG834G v3 B	**LAN_B**	**192.168.3.1**	**255.255.255.0**	**22.23.24.25**

2. Open the DG834G v3 on LAN A management interface and click on **VPN Policies**.

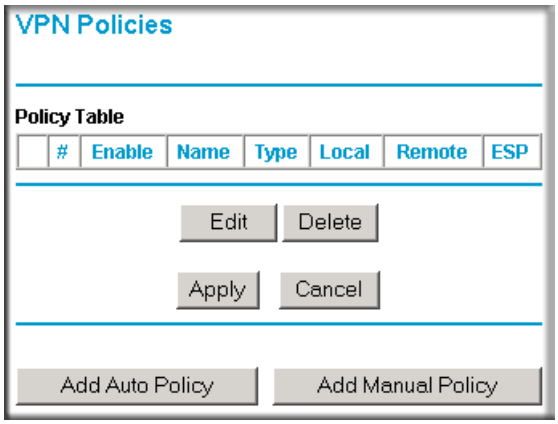


Figure 7-42

3. Click **Add Auto Policy**.
4. Enter policy settings (see Figure 7-43).
   - General
     - Policy Name = GtoG
     - Remote VPN Endpoint Address Type = Fixed IP Address
     - Remote VPN Endpoint Address Data = 22.23.24.25
   - Local LAN – use default setting
   - Remote LAN
     - IP Address = select Subnet address from the pulldown menu.
     - Start IP address = 192.168.3.1
     - 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 = use default setting
     - Remote Identity Type = use default setting
   - Parameters
     - Encryption Algorithm = 3DES

— Authentication Algorithm = MD5

— Pre-shared Key = 12345678

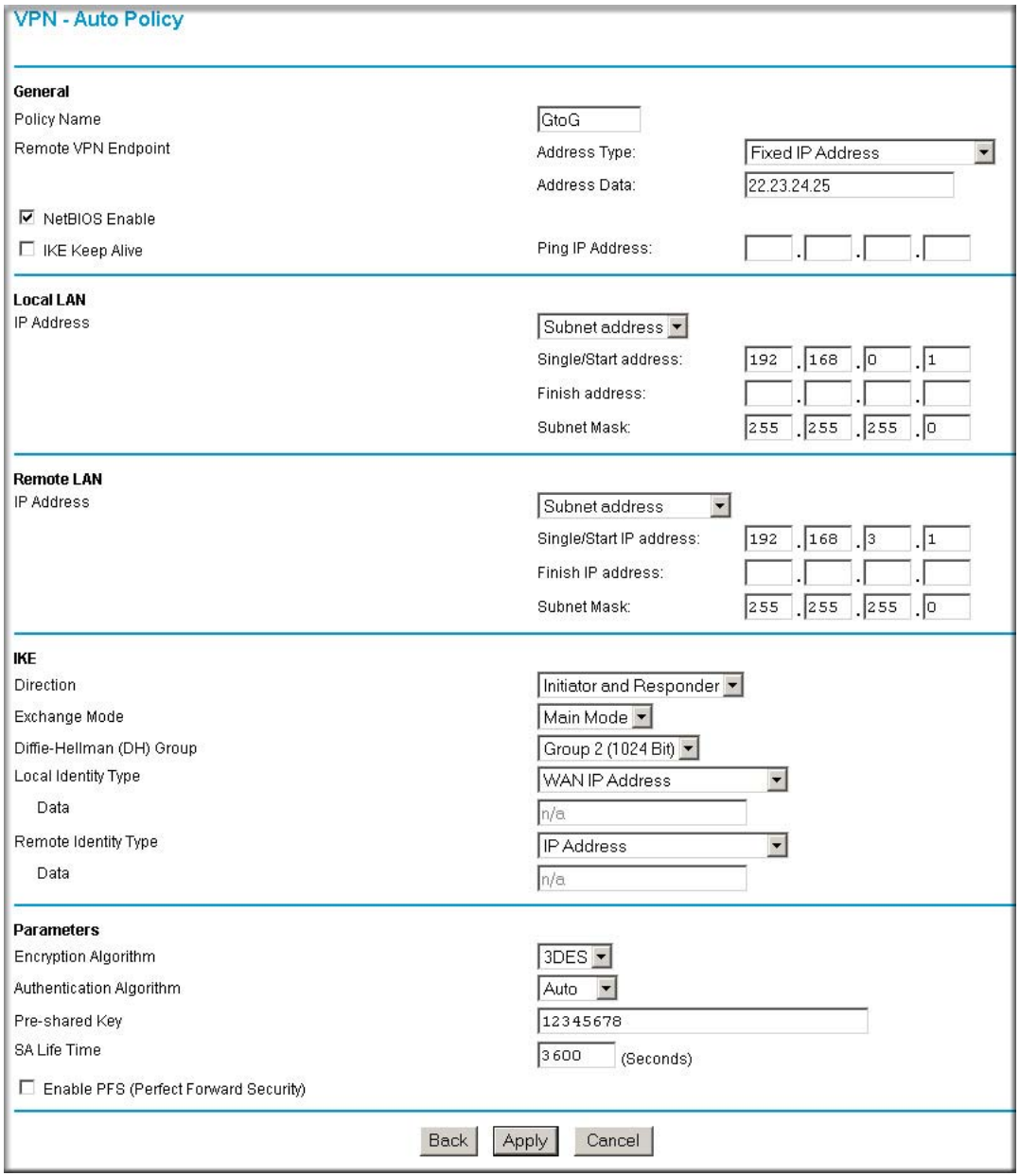


Figure 7-43

5. Click **Apply**. The Get VPN Policies web page is displayed.

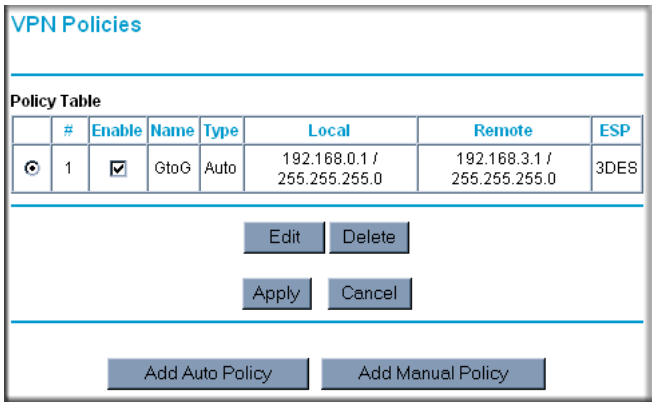


Figure 7-44

6. Repeat for the DG834G v3 on LAN B and pay special attention to use the following network settings as appropriate.
   - General, Remote Address Data (e.g., **14.15.16.17**)
   - Remote LAN, Start IP Address
     - IP Address (e.g, **192.168.0.1**)
     - Subnet Mask (e.g., **255.255.255.0**)
     - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

	Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 7-29 for information on the other ways.

a. Open the DG834G v3 management interface and click on **VPN Status** to display the VPN Status/Log screen (Figure 7-45).

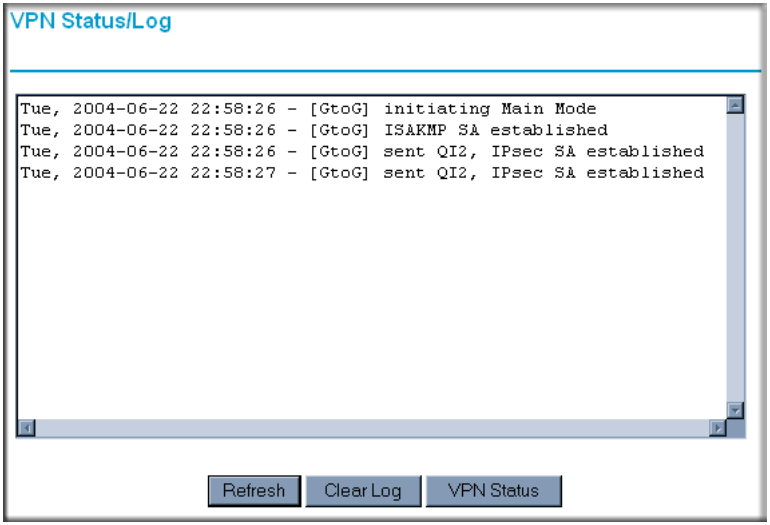


Figure 7-45

b. Click **VPN Status** (Figure 7-45) to display the Current VPN Tunnels (SAs) screen (Figure 7-46). Click on **Connect** for the VPN tunnel you want to activate.

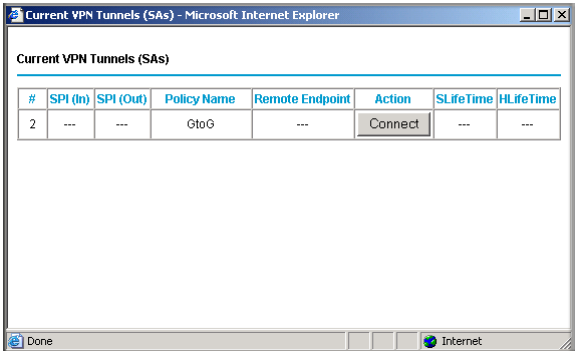


Figure 7-46

c. Review the VPN Status/Log screen (Figure 7-45) to verify that the tunnel is connected.

Using Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you may use Manual Keying, in which you must specify each phase of the connection. A "Manual" VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

Click the **VPN Policies** link of the main menu, and then click the **Add Manual Policy** radio button to display the Manual Keys menu shown in Figure 7-47.

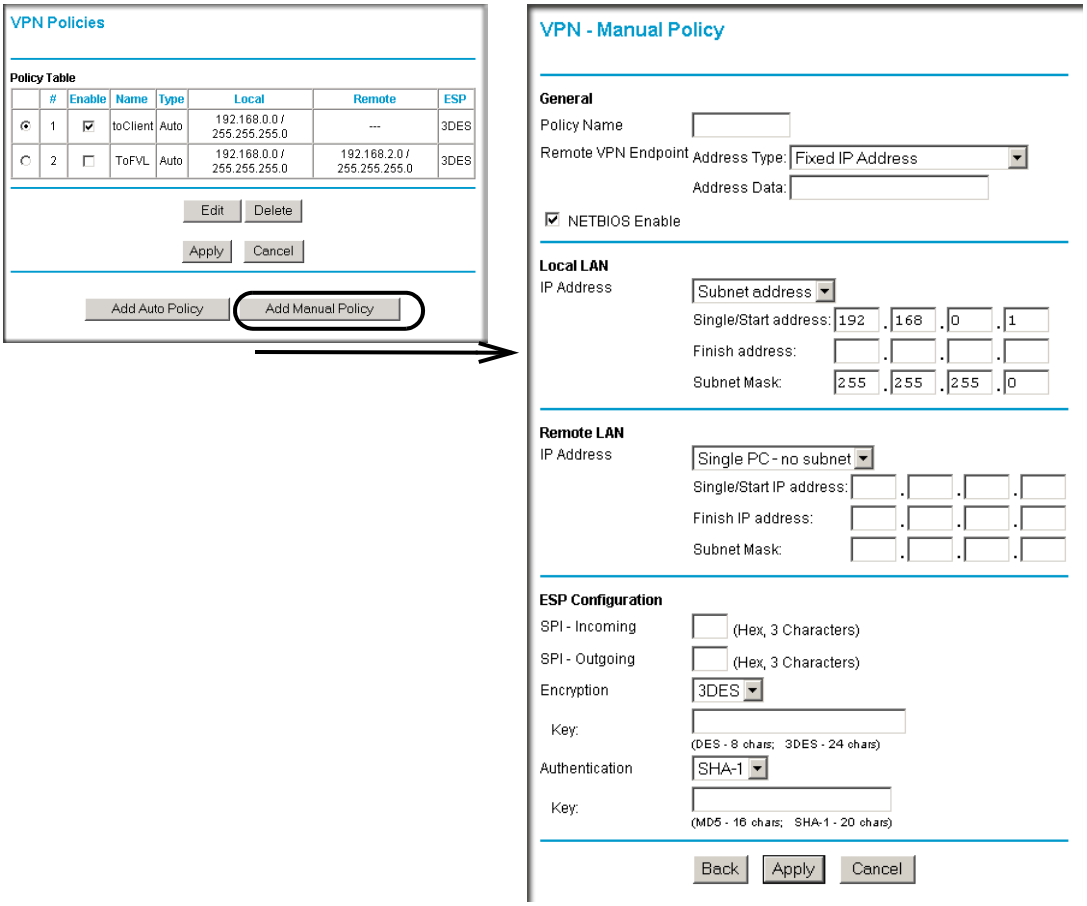


Figure 7-47

General. The DG834G v3 VPN tunnel network connection fields are defined as follows:

- **Policy Name**—enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—select the desired option (IP address or Fully Qualified Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

	Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

- **NETBIOS Enable**—check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.

Local LAN. This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.

Remote LAN. This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.
- **Single address**—enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.

- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

ESP Configuration. ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.

SPI—enter the required security policy indexes (SPIs). Each policy must have unique SPIs. These settings must match the remote VPN endpoint. The "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.

Encryption—select the desired Encryption Algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters and for DES, the keys should be 8 ASCII characters.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

Authentication—select the desired SHA-1 or MD5 Authentication Algorithm, and enter the key in the field provided. For MD5, the keys should be 16 ASCII characters. For SHA-1, the keys should be 20 ASCII characters.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

Chapter 8
Troubleshooting

This chapter gives information about troubleshooting your 54 Mbps ADSL Modem Wireless Router Model DG834G. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?

  Go to "Basic Functioning" on page 8-1.
- I can't access the router's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 8-3.
- I've configured the router but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 8-4.
- I can't remember the router's configuration password.

  Go to "Restoring the Default Configuration and Password" on page 8-9.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 8-9.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on (see "The Router's Front Panel" on page 2-8 for an illustration and explanation of the LEDs).
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
   - **a.** The Test LED is not lit.
   - **b.** The LAN port LEDs are lit for any local ports that are connected.

c. The WAN port LED is lit.

If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

Test LED Never Turns On or Test LED Stays On

When the router is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the router.

If you experience problems with the Test LED:

- Cycle the power to see if the router recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Using the Reset button" on page 8-9.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834G v3.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Preparing a Computer for Network Access" in Appendix C to find your computer's IP address.

	Note: If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Using the Reset button" on page 8-9.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

ADSL link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

Internet LED Green or Blinking Green

If your Internet LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

Internet LED Blinking Amber

If your Internet LED is blinking amber, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the Internet LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green Internet LED, there may be a problem with your wiring. If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

Internet LED Off

If the Internet LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green Internet LED the problem may be one of the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The ADSL Modem Wireless Router uses pins 2 and 3.

Obtaining a WAN IP Address

If your modem router is unable to access the internet, and your Internet LED is green or blinking green, you should determine whether the modem router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser and select an external site such as www.netgear.com.
2. Access the Main Menu of the modem router's configuration at http://192.168.0.1.
3. Under the Maintenance heading check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a Multiplexing Method or Virtual Path Identifier/Virtual Channel Identifier parameter.
  Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.
- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.

- If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See "Troubleshooting PPPoE or PPPoA", below.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

  OR

  Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to the *ADSL Modem Wirelesss Router Setup Manual* (see Table 2-2 on page 2-10).

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the Main Menu of the router at http://192.168.0.1.
2. Under the Maintenance heading, select the **Router Status** link.
3. Click the **Connection Statu**s button.
4. If all of the steps indicate "OK" then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates "Failed", you can attempt to reconnect by clicking **Connect**. The modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you may be using an incorrect Service Name, User Name or Password. There also may be a provisioning problem with your ISP.

	Note: Unless you connect manually, the modem router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your modem router can obtain an IP address but your computer is unable to load any Web pages from the Internet:

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer and verify the DNS address as described in "Preparing a Computer for Network Access" in Appendix C. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer and verify the modem router address as described in "Preparing a Computer for Network Access" in Appendix C.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   ```
   ping 192.168.0.1
   ```

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 8-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

— Check that your PC has the IP address of your router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default modem router as described in "Preparing a Computer for Network Access" in Appendix C.

— Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

— Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to your *ADSL Modem Wirelesss Router Setup Manual* (see Table 2-2 on page 2-10).

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 5-1).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Reset button

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The ADSL Modem Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000
  Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour
  Cause: The router does not automatically sense Daylight Savings Time. In the E-mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A
Technical Specifications

This appendix provides technical specifications for the 54 Mbps ADSL Modem Wireless Router Model DG834G.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V AC @ 1.0A output
Physical Specifications	
Dimensions:	6.9" x 4.7" x 1.1" 175 mm x 119 mm x 28 mm
Weight:	0.7 lbs. 0.3 kg
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	ADSL, ADSL2+, Dual RJ-11, pins 2 and 3,T1.413, G.DMT, G.Lite, ITU Annex A (for the DG834G) or ITU Annex B (for the DG834GB)

Appendix B
NETGEAR VPN Configuration

DG834G v3 to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834G v3 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

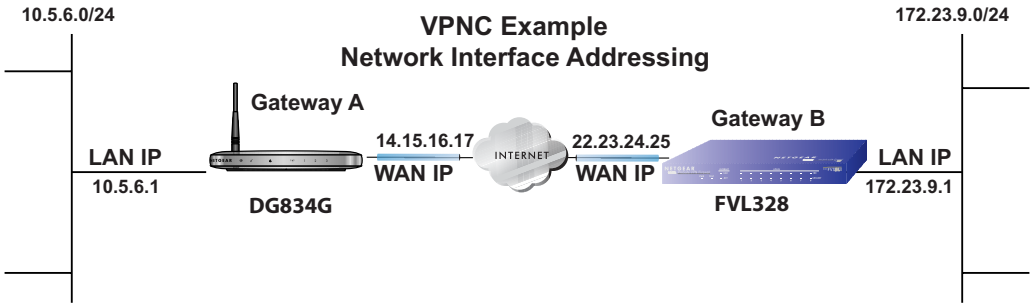


Figure B-1

	Note: Product updates are available on the NETGEAR, Inc. web site at *http://kbserver.netgear.com/DG834G v3.asp*.

Step-By-Step Configuration

1. Configure the DG834G v3 as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-21), being certain to use appropriate network addresses for the environment.

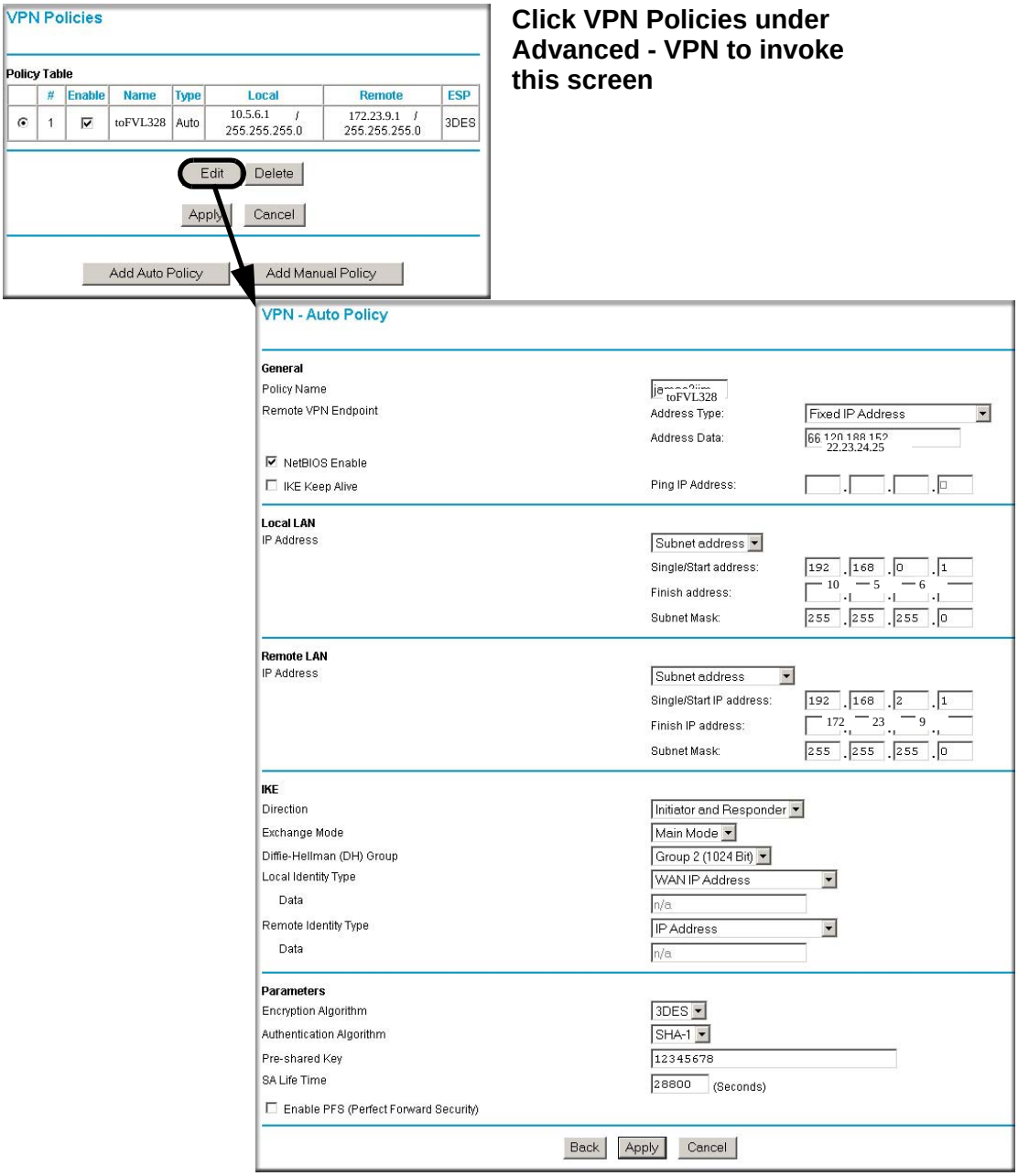
   The LAN Addresses used in this example are as follows:

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

Figure B-2

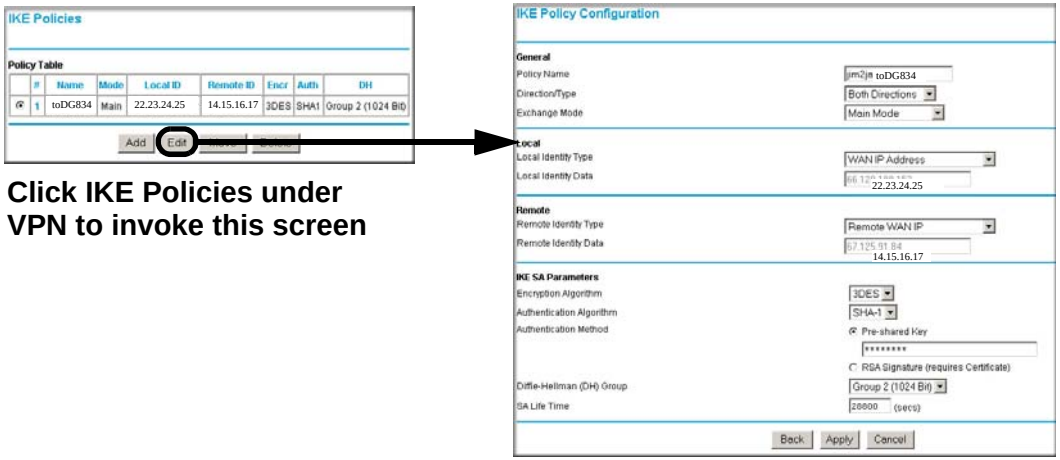
2. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-21), being certain to use appropriate network addresses for the environment.

a. In Step 1, enter **toDG834** for the Connection Name

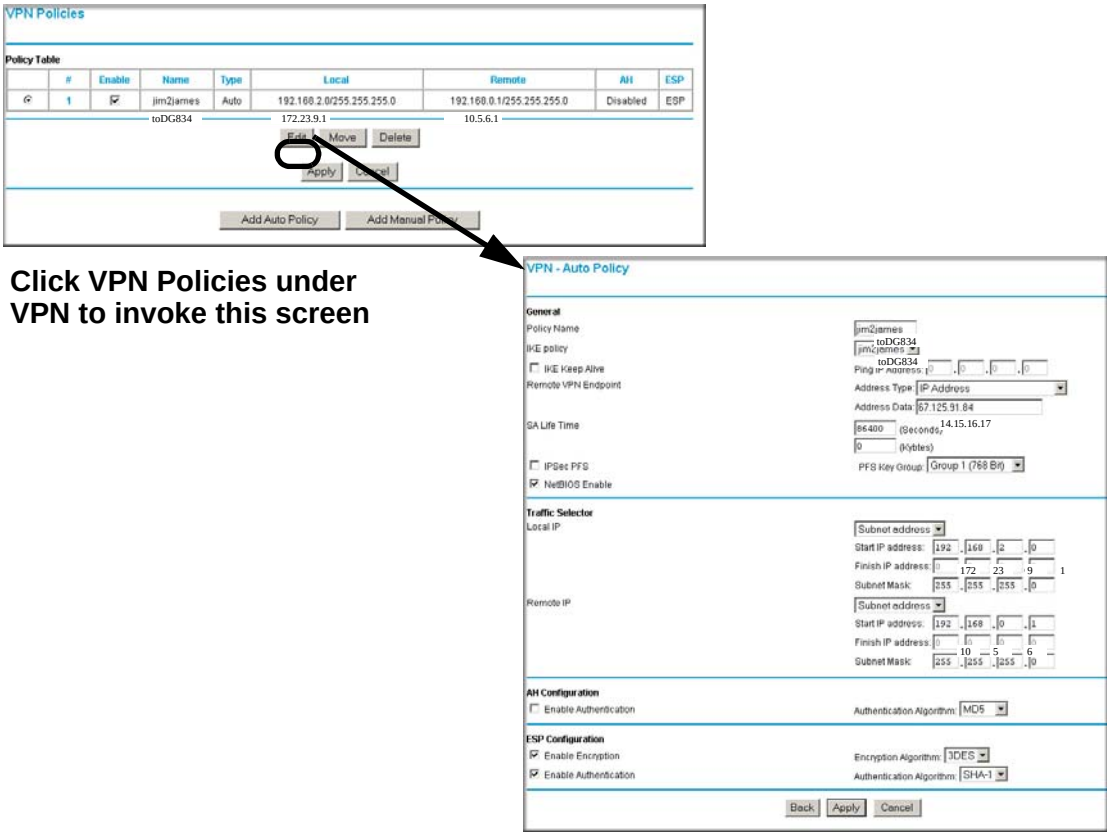
b. In Step 2, enter **14.15.16.17** for the remote WAN's IP address

c. In Step 3, enter the following:

- IP Address = **10.5.6.1**
- Subnet Mask = **255.255.255.0**



Click IKE Policies under VPN to invoke this screen



Click VPN Policies under VPN to invoke this screen

Figure B-3

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834G v3.
   a. Open the command prompt (Start -> Run -> cmd)
   b. ping 172.23.9.1

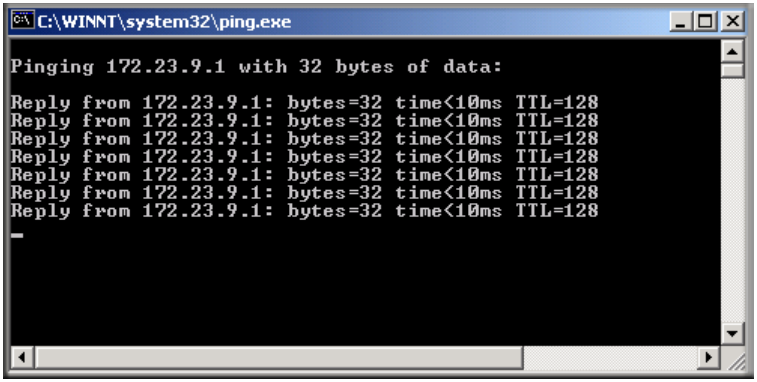


Figure B-4

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

DG834G v3 with FQDN to FVL328

This appendix is a case study on how to configure a VPN tunnel from a NETGEAR DG834G v3 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

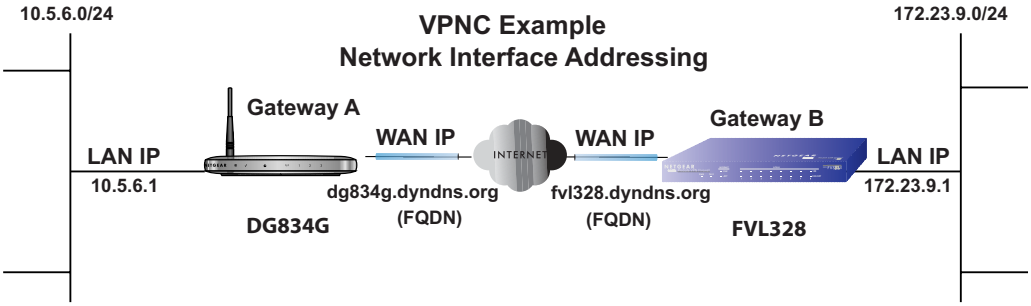


Figure B-5

Note: Product updates are available on the NETGEAR, Inc. web site at *http://kbserver.netgear.com/DG834G v3.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 DG834G v3 labeled Gateway A as in the illustration.

Out of the box, the DG834G v3 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 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 DG834G v3, configure the Dynamic DNS settings.

a. Browse to the Dynamic DNS Setup Screen (see Figure B-6) in the Advanced menu.

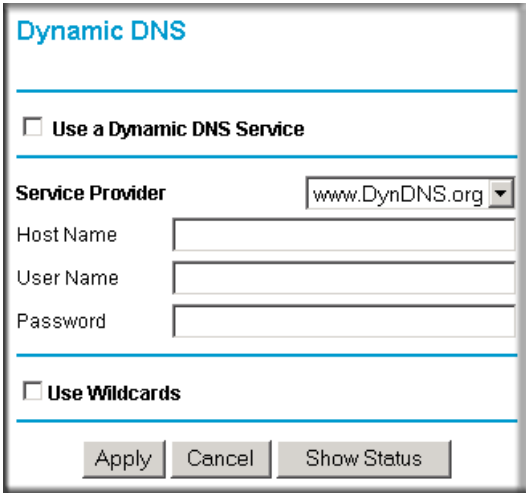


Figure B-6

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).

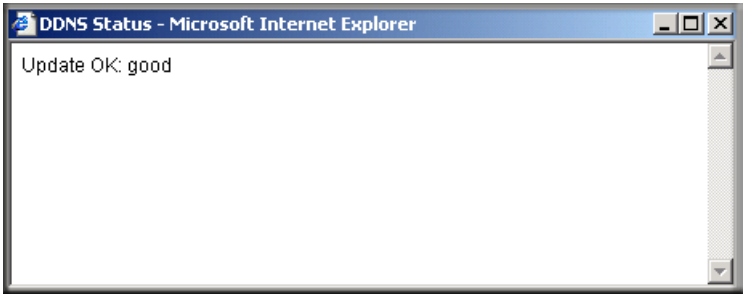


Figure B-7

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.

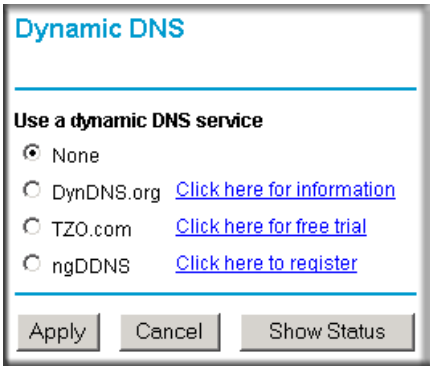


Figure B-8

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 = fvl328.dyndns.org
- User Name = <user's account username>
- Password = <user's account password>

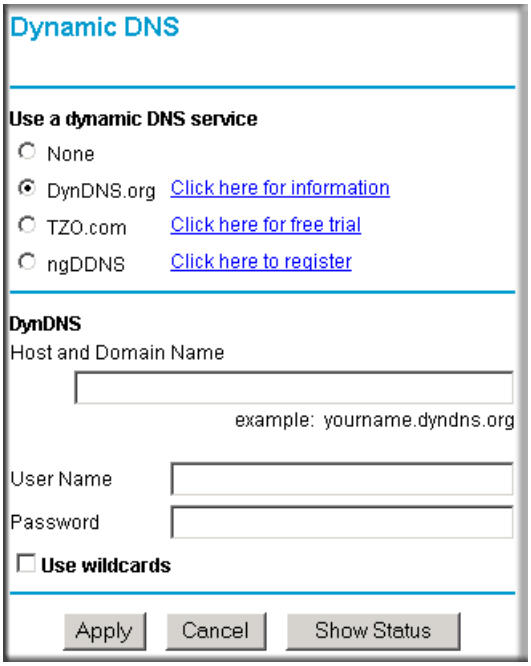


Figure B-9

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

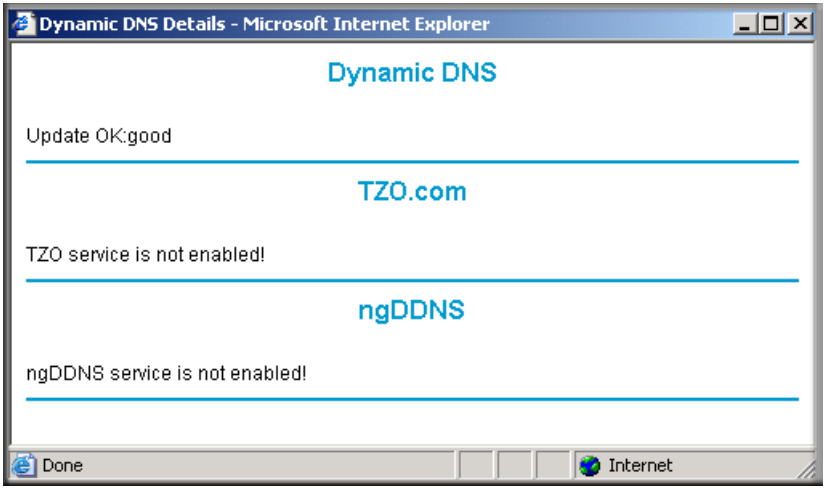


Figure B-10

5. Configure the DG834G v3 as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-21), 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
DG834G v3	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 7-21), 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 DG834G v3.

   a. Open the command prompt (Start -> Run -> cmd)

   b. ping 172.23.9.1

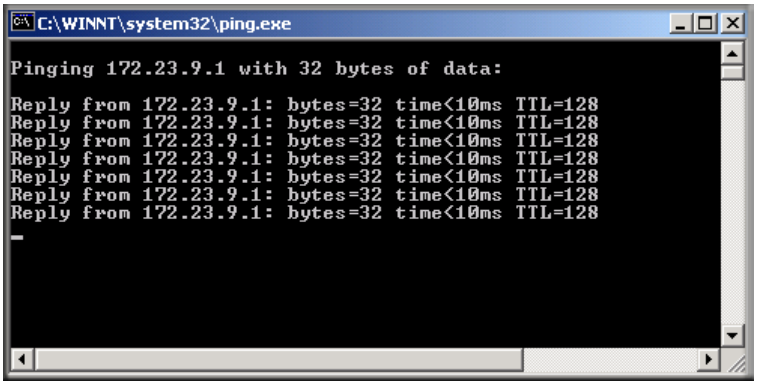


Figure B-11

	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

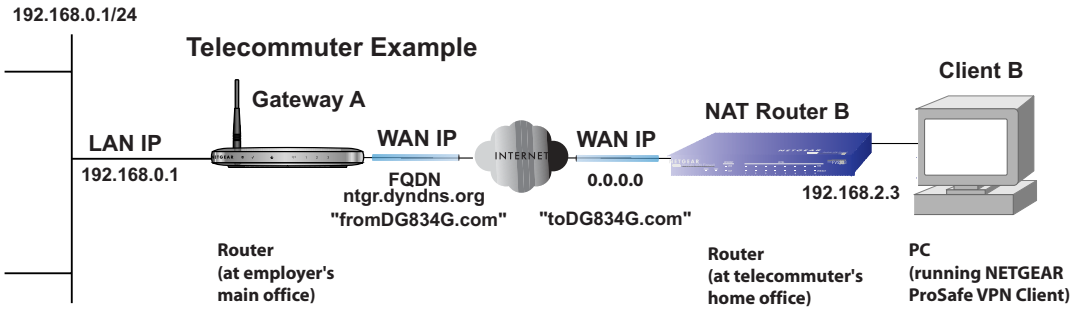


Figure B-12

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://192.168.0.1 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.

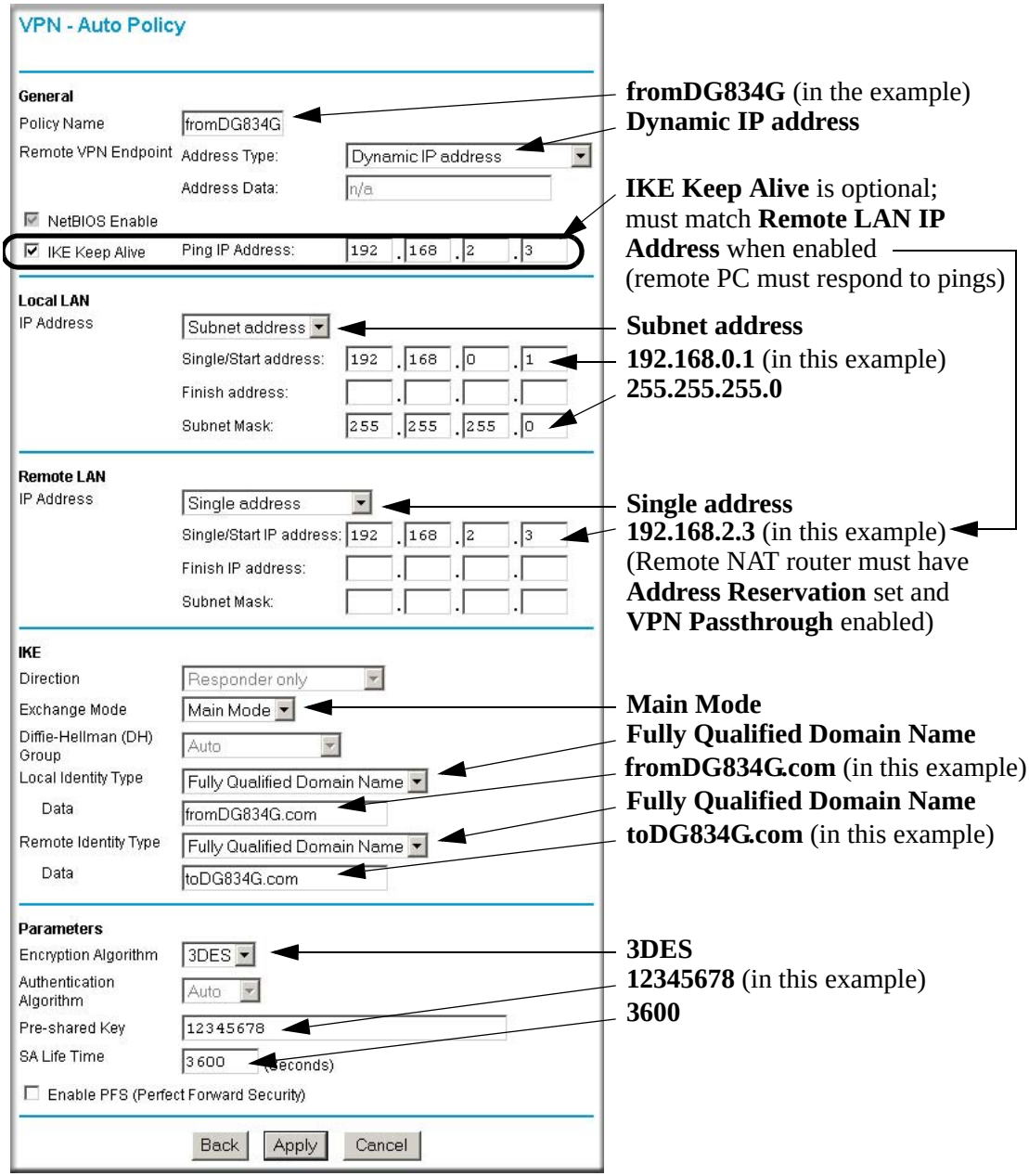

VPN - Auto Policy
General
Policy Name
fromDG834G
Remote VPN Endpoint
Address Type:
Dynamic IP address
Address Data:
n/a
NetBIOS Enable
IKE Keep Alive
Ping IP Address:
192 . 168 . 2 . 3
Local LAN
IP Address
Subnet address
Single/Start address:
192 . 168 . 0 . 1
Finish address:
Subnet Mask:
255 . 255 . 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)
Back
Apply
Cancel
fromDG834G (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.

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 DG834G. 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 DG834G 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 ( ) 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 DG834G v3 on Gateway A.

	Note: In this example, the **Connection Name** used on the client side of the VPN tunnel is **toDG834G** 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.

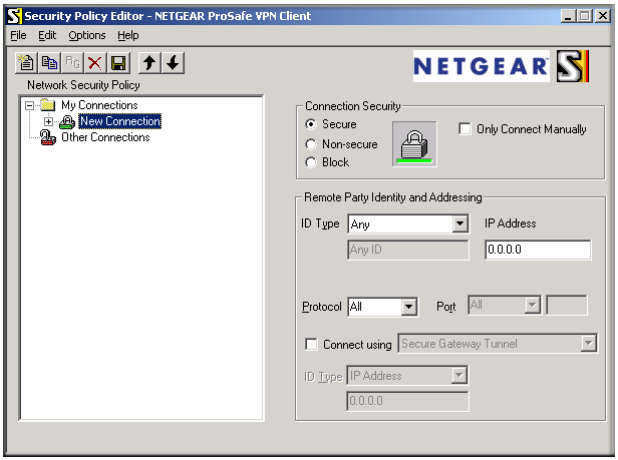


Figure B-15

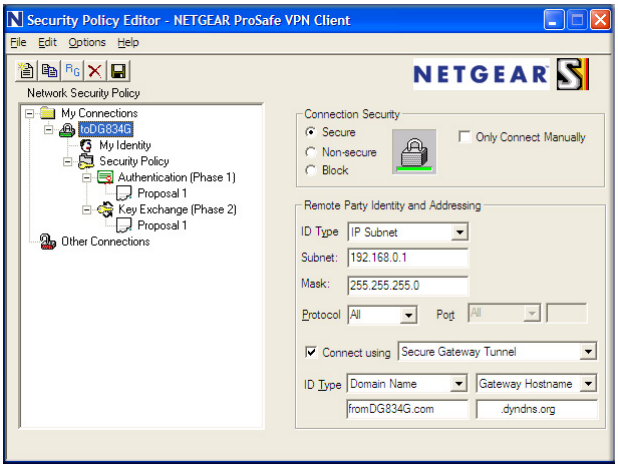


Figure B-16

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

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

e. In this example, type **192.168.0.1** in the Subnet field as the network address of the DG834G v3.

f. Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834G v3.

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 DG834G 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.

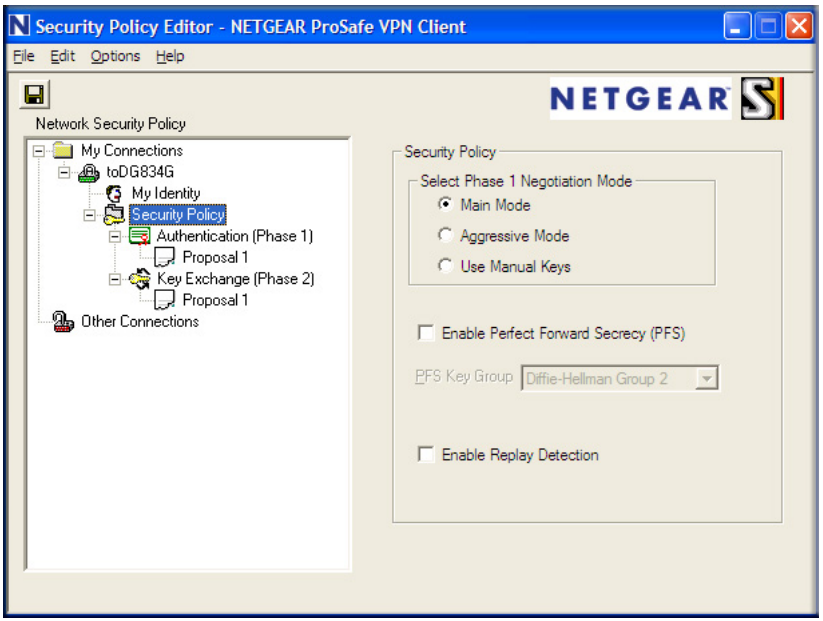


Figure B-17

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 DG834G v3 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**.

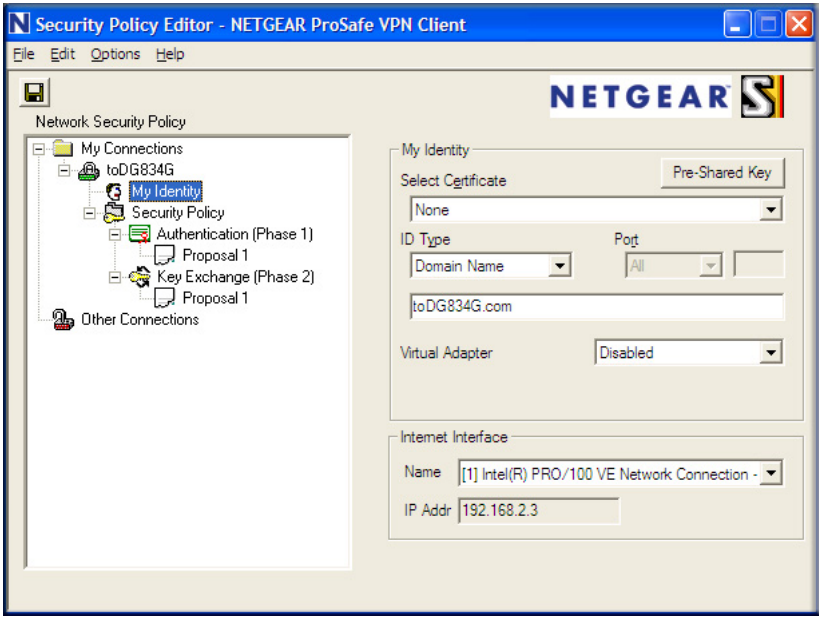


Figure B-18

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 **192.168.2.3** (in this example) in the **IP Addr** box.

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

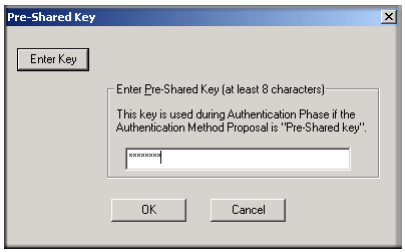


Figure B-19

f. In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834G v3'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**.

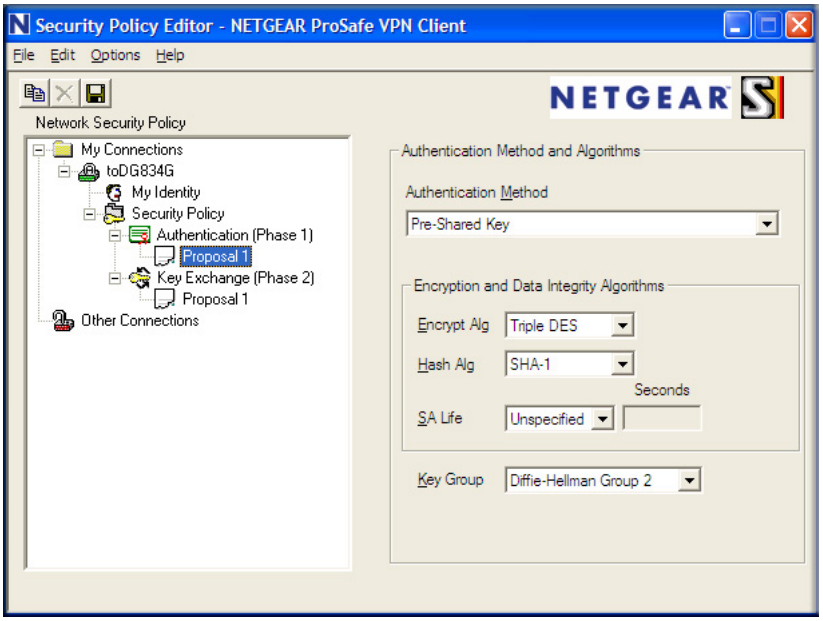


Figure B-20

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**.

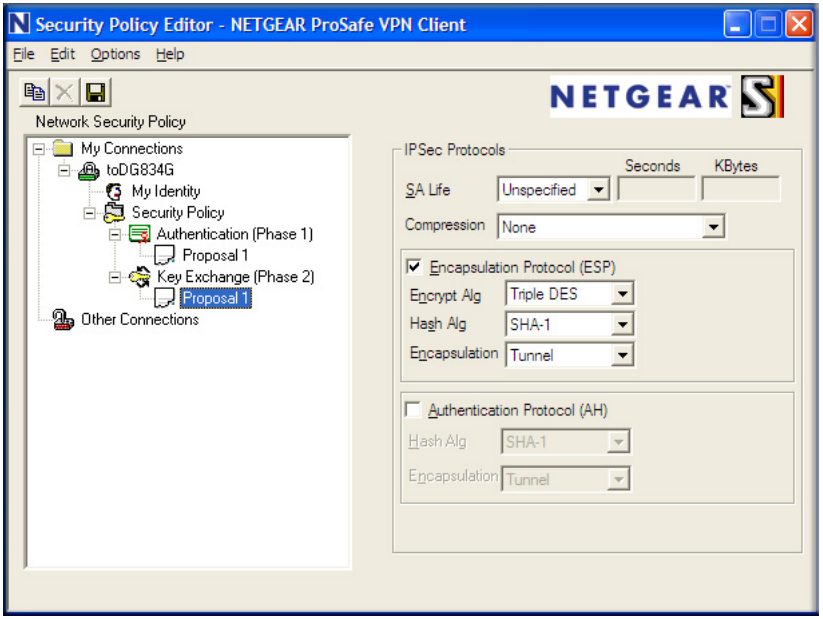


Figure B-21

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**.

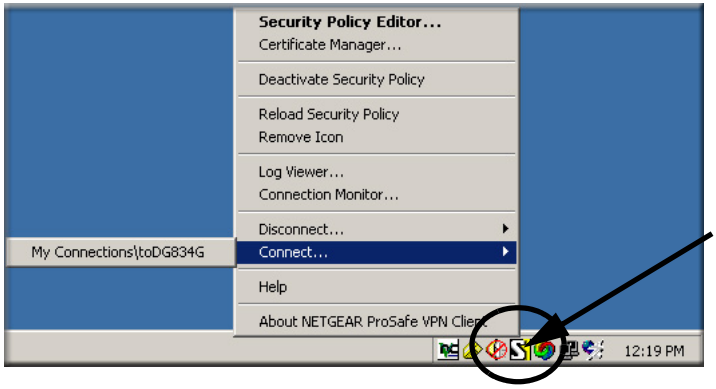
To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the ADSL Modem Wireless Router menu bar (see Figure B-22). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

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 DG834G 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 192.168.0.1**, and then click **OK**.

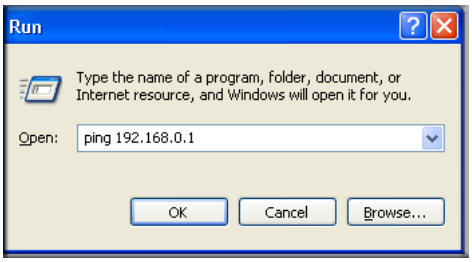


Figure B-23

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**.

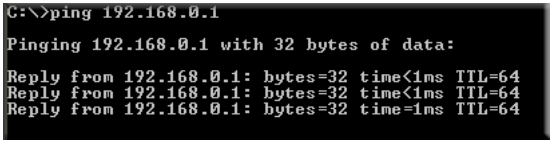


Figure B-24

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 DG834G **Log Viewer**.

1. To launch this function, click on the Windows **Start** button, then select **Programs**, then **54 Mbps ADSL Modem Wireless Router Model DG834G**, 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:

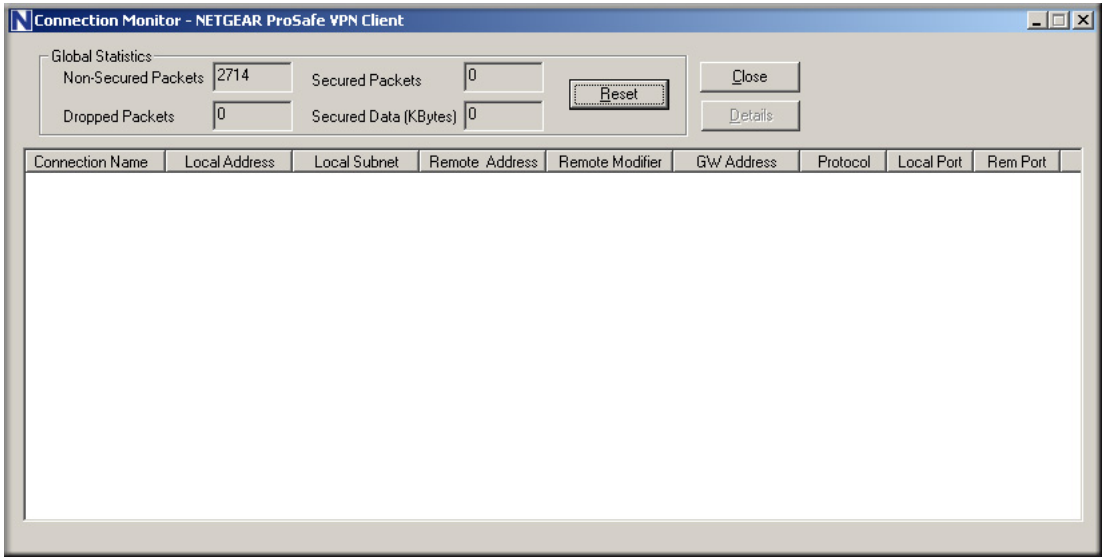


Figure B-25

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:

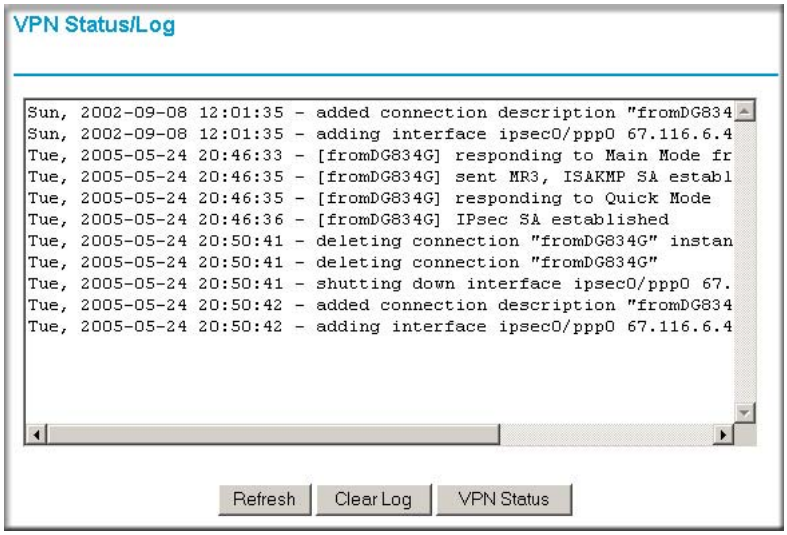
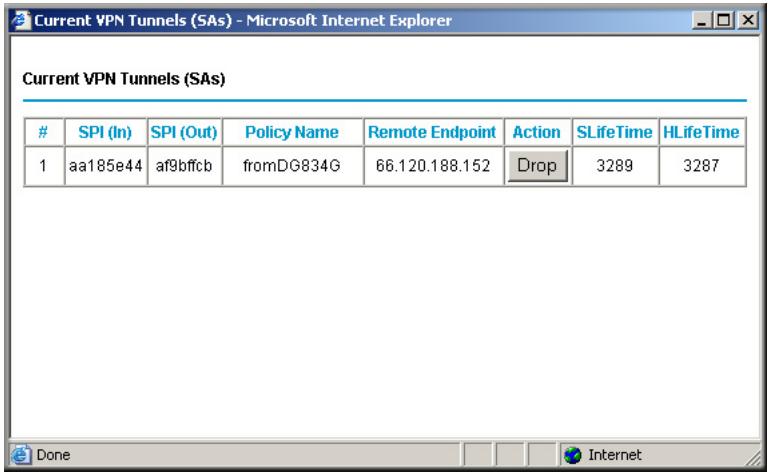


Figure B-26

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



#	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

Appendix C
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm