

Configure IPSec VPN Tunnels With the Wizard

This quick start guide provides basic configuration information about setting up IPSec VPN tunnels by using the VPN Wizard on the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N. For extensive VPN information, see the *Reference Manual*. This quick start guide contains the following sections:

- [VPN Wizard Default Settings and General Information](#)
- [Create an IPv4 Gateway-to-Gateway VPN Tunnel](#)
- [Create an IPv6 Gateway-to-Gateway VPN Tunnel](#)
- [Configure an IPv4 IPSec VPN Connection between a Gateway and a Client](#)
- [For More Information](#)

Note: For more information about the topics covered in this guide, visit the FVS318N support website at <http://support.netgear.com>. You will also find the *Reference Manual* at the support website.

VPN Wizard Default Settings and General Information

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match or mirror each other precisely. The VPN Wizard guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption.

The default IKE policy and VPN policy settings of the VPN Wizard are explained in the following tables:

Table 1. Default IKE policy settings for the VPN Wizard

IKE Policy Settings	Gateway-to-Gateway Tunnels	Gateway-to-Client Tunnels
Exchange mode	Main	Aggressive
ID type	Local WAN IP address	FQDN

Table 1. Default IKE policy settings for the VPN Wizard (continued)

IKE Policy Settings	Gateway-to-Gateway Tunnels	Gateway-to-Client Tunnels
Local WAN ID	Local WAN IP address	remote.com
Remote WAN ID	Not applicable	local.com
Encryption algorithm	3DES	3DES
Authentication algorithm	SHA-1	SHA-1
Authentication method	Pre-shared Key	Pre-shared Key
Key group	DH-Group 2 (1024 bit)	DH-Group 2 (1024 bit)
Life time	8 hours	8 hours

Table 2. Default VPN policy settings for the VPN Wizard

VPN Policy Settings	Gateway-to-Gateway Tunnels	Gateway-to-Client Tunnels
Encryption algorithm	3DES	3DES
Authentication algorithm	SHA-1	SHA-1
Life time	1 hour	1 hour
Key group	DH-Group 2 (1024 bit)	DH-Group 2 (1024 bit)
NetBIOS	Enabled	Disabled

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you have validated the connection, you can use the wizard to create new policies using the domain names, also referred to as fully qualified domain names (FQDNs), for the WAN addresses.

Tip: When using FQDNs and Dynamic DNS (DDNS) service, if the DDNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Tip: To ensure that tunnels stay active, after completing the wizard steps, manually edit the VPN policy to enable keep-alives, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see the “Configure Keep-Alives” section in Chapter 6, “Virtual Private Networking Using IPsec and L2TP Connections,” of the *Reference Manual*.

Create an IPv4 Gateway-to-Gateway VPN Tunnel

➤ To set up an IPv4 gateway-to-gateway VPN tunnel using the VPN Wizard:

1. Select **VPN > IPSec VPN > VPN Wizard**. In the upper right of the screen, the IPv4 radio button is selected by default. The VPN Wizard screen displays the IPv4 settings. (The following screen contains an example.)

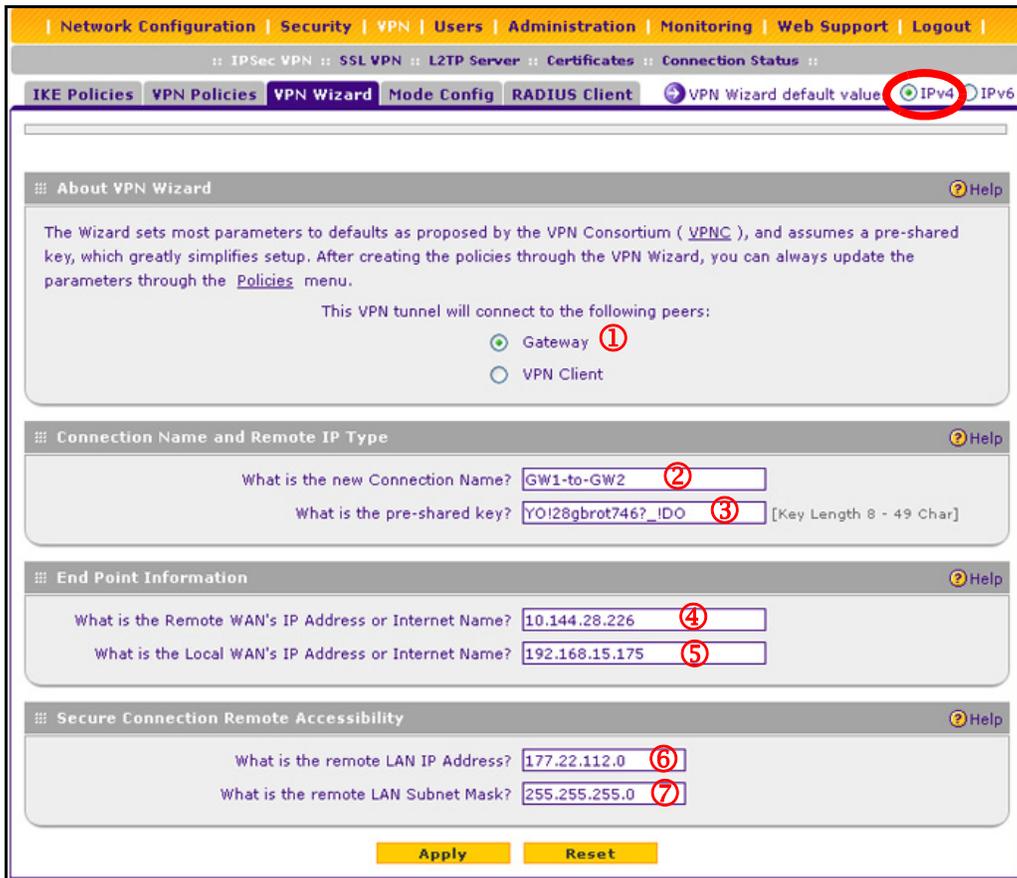


Figure 1.

2. Complete the settings as explained in the following table:

Table 3. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel

#	Setting	Description
About VPN Wizard		
①	This VPN tunnel will connect to the following peers	Select the Gateway radio button. The local WAN port's IP address or Internet name automatically displays in the End Point Information section of the screen.

Table 3. IPSec VPN Wizard settings for an IPv4 gateway-to-gateway tunnel (continued)

#	Setting	Description
Connection Name and Remote IP Type		
②	What is the new Connection Name?	Enter a descriptive name for the connection. (The name is not supplied to the remote VPN endpoint.)
③	What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
End Point Information¹		
④	What is the Remote WAN's IP Address or Internet Name?	Enter the IPv4 address or Internet name (domain name or FQDN) of the WAN interface on the remote VPN tunnel endpoint.
⑤	What is the Local WAN's IP Address or Internet Name?	When you select the Gateway radio button in the About VPN Wizard section of the screen, the IPv4 address of the wireless VPN firewall's active WAN interface is automatically entered.
Secure Connection Remote Accessibility		
⑥	What is the remote LAN IP Address?	Enter the LAN IPv4 address of the remote gateway. Important: The remote LAN IPv4 address needs to be in a different subnet from the local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x but could not be 192.168.1.x. If this information is incorrect, the tunnel fails to connect.
⑦	What is the remote LAN Subnet Mask?	Enter the LAN subnet mask for the remote gateway.

1. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen for IPv4. By default, the VPN policy is enabled.

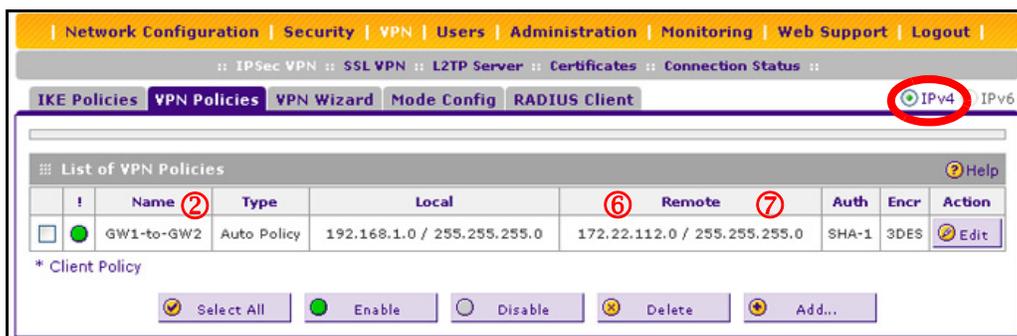


Figure 2.

4. Configure a VPN policy on the remote gateway that allows connection to the wireless VPN firewall.
5. Activate the IPsec VPN connection:
 - a. Select **VPN > Connection Status > IPsec VPN Connection Status**. The IPsec VPN Connection Status screen displays (see the following screen).
 - b. Locate the policy in the table, and click the **Connect** table button. The IPsec VPN connection becomes active.

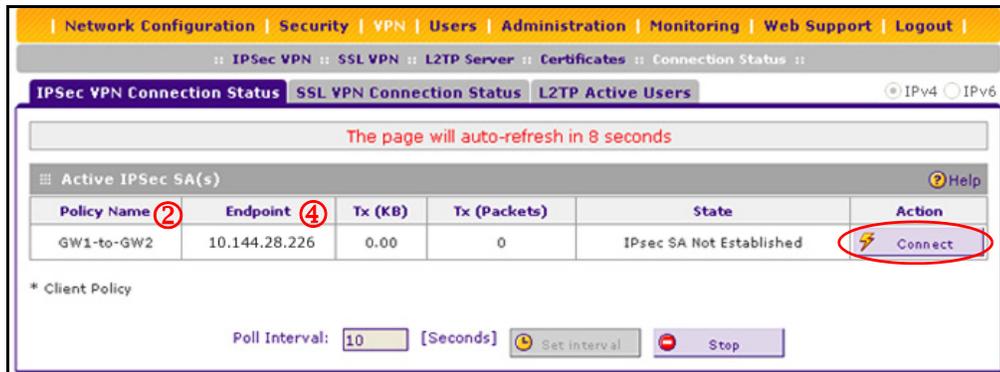


Figure 3.

Create an IPv6 Gateway-to-Gateway VPN Tunnel

- To set up an IPv6 gateway-to-gateway VPN tunnel using the VPN Wizard:
 1. Select **VPN > IPsec VPN > VPN Wizard**.
 2. In the upper right of the screen, select the **IPv6** radio button. The VPN Wizard screen displays the IPv6 settings. (The following screen contains an example.)

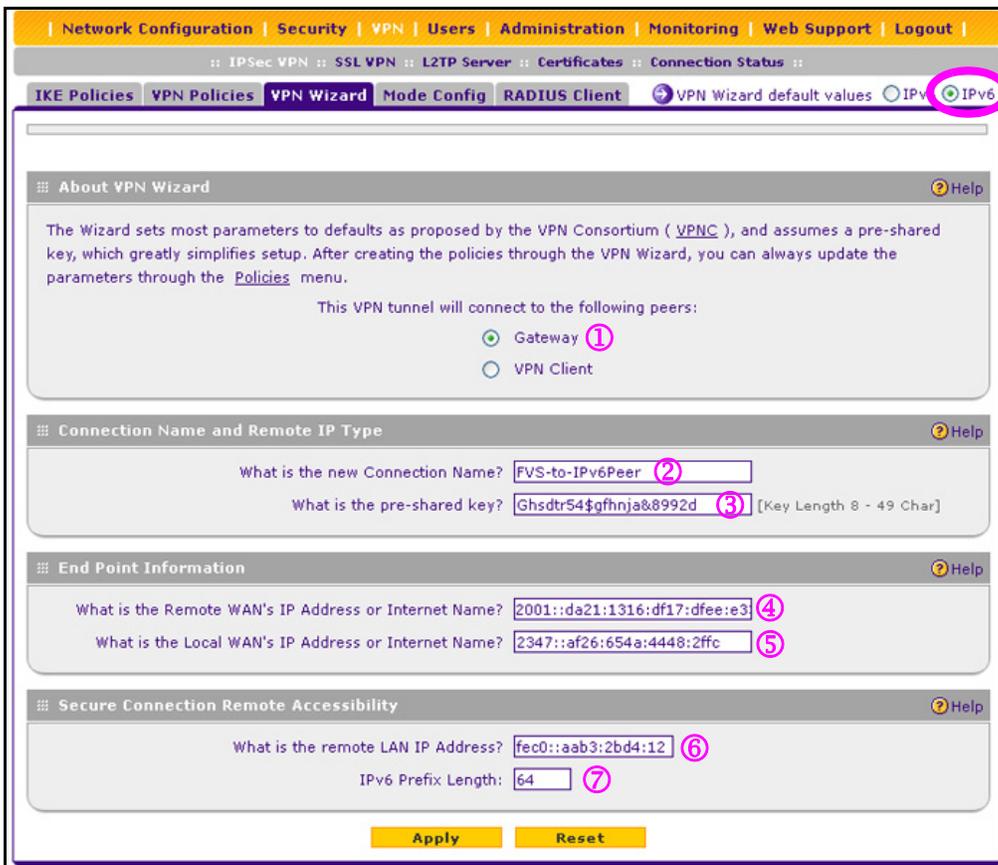


Figure 4.

- Complete the settings as explained in the following table:

Table 4. IPsec VPN Wizard settings for an IPv6 gateway-to-gateway tunnel

#	Setting	Description
About VPN Wizard		
①	This VPN tunnel will connect to the following peers	Select the Gateway radio button. The local WAN port's IP address or Internet name automatically displays in the End Point Information section of the screen.
Connection Name and Remote IP Type		
②	What is the new Connection Name?	Enter a descriptive name for the connection. (The name is not supplied to the remote VPN endpoint.)
③	What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
End Point Information¹		
④	What is the Remote WAN's IP Address or Internet Name?	Enter the IPv6 address or Internet name (domain name or FQDN) of the WAN interface on the remote VPN tunnel endpoint.

Table 4. IPSec VPN Wizard settings for an IPv6 gateway-to-gateway tunnel (continued)

#	Setting	Description
⑤	What is the Local WAN's IP Address or Internet Name?	When you select the Gateway radio button in the About VPN Wizard section of the screen, the IPv6 address of the wireless VPN firewall's active WAN interface is automatically entered.
Secure Connection Remote Accessibility		
⑥	What is the remote LAN IP Address?	Enter the LAN IPv6 address of the remote gateway. Important: The remote LAN IPv6 address needs to be different from the local LAN IPv6 address. For example, if the local LAN IPv6 address is FEC0::1, then the remote LAN IPv6 address could be FEC0:1::1 but could not be FEC0::1. If this information is incorrect, the tunnel fails to connect.
⑦	IPv6 Prefix Length	Enter the prefix length for the remote gateway.

1. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

4. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen for IPv6. By default, the VPN policy is enabled.

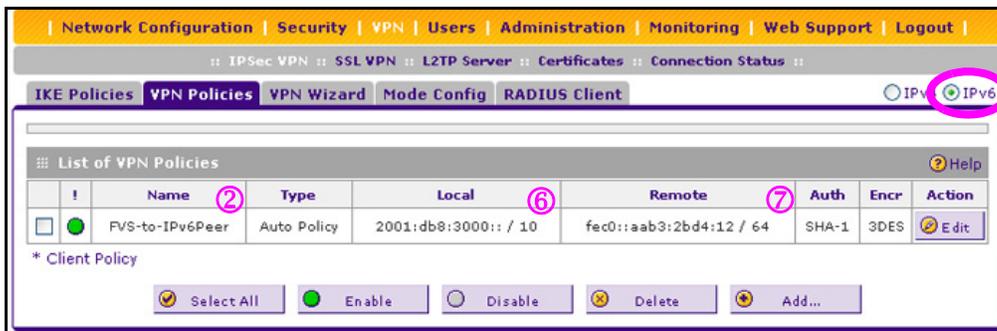


Figure 5.

5. Configure a VPN policy on the remote gateway that allows connection to the wireless VPN firewall.
6. Activate the IPSec VPN connection:
 - a. Select **VPN > Connection Status > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays:

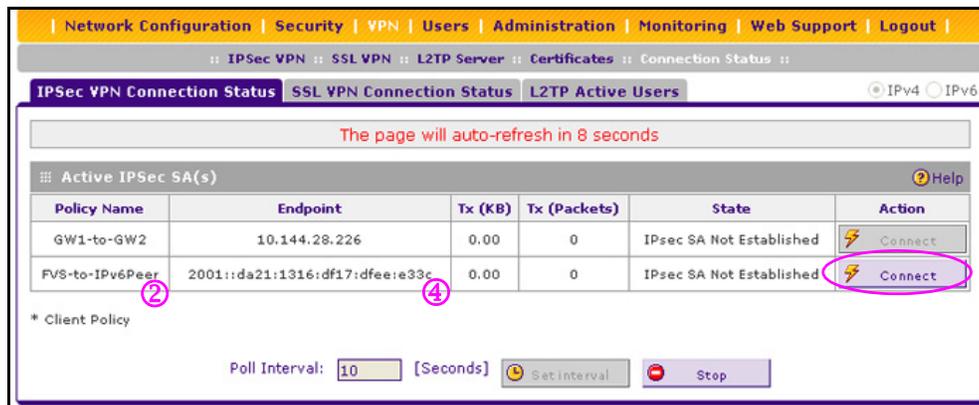


Figure 6.

- b. Locate the policy in the table, and click the **Connect** table button. The IPsec VPN connection becomes active.

Configure an IPv4 IPsec VPN Connection between a Gateway and a Client

- *Configure the Gateway Connection*
- *Configure the VPN Client Connection Using the VPN Client Configuration Wizard*
- *Test the NETGEAR VPN Client Connection*

Note: Although the wireless VPN firewall supports IPv6, the NETGEAR ProSafe VPN Client supports IPv4 only; an upcoming release of the VPN Client will support IPv6.

To set up an IPsec VPN connection between a gateway and a NETGEAR VPN client, first configure the gateway connection, and then configure the VPN client connection.

Configure the Gateway Connection

- **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**
 1. Select **VPN > IPsec VPN > VPN Wizard**. In the upper right of the screen, the IPv4 radio button is selected by default. The VPN Wizard screen displays the IPv4 settings. (The following figure contains an example.)

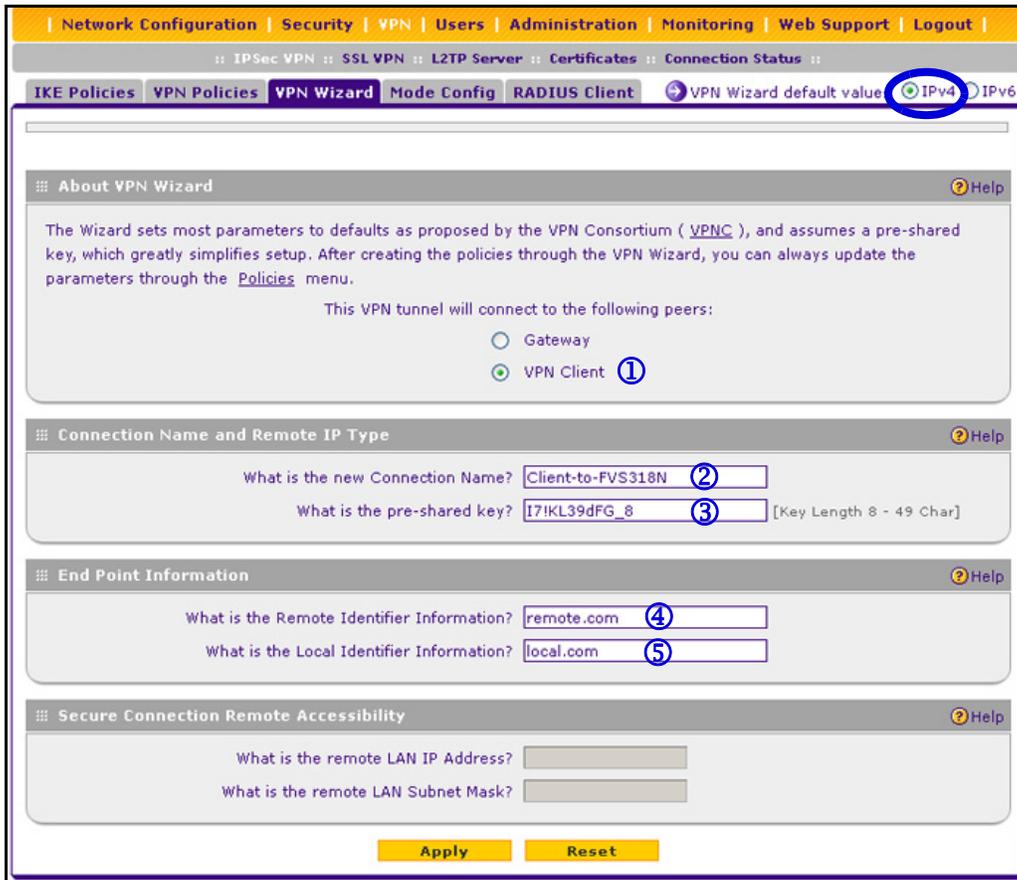


Figure 7.

2. Complete the settings as explained in the following table:

Table 5. IPsec VPN Wizard settings for an IPv4 gateway-to-client tunnel

#	Setting	Description
About VPN Wizard		
①	This VPN tunnel will connect to the following peers	Select the VPN Client radio button. The default remote FQDN (remote.com) and the default local FQDN (local.com) display in the End Point Information section of the screen.
Connection Name and Remote IP Type		
②	What is the new Connection Name?	Enter a descriptive name for the connection. (The name is not supplied to the remote VPN endpoint.)
③	What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.

Table 5. IPSec VPN Wizard settings for an IPv4 gateway-to-client tunnel (continued)

#	Setting	Description
End Point Information¹		
④	What is the Remote Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default remote FQDN (remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN. Note: The remote ID on the wireless VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the wireless VPN firewall and then enter client.com as the local ID on the VPN client.
⑤	What is the Local Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default local FQDN (local.com) is automatically entered. Use the default local FQDN, or enter another FQDN. Note: The local ID on the wireless VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the wireless VPN firewall and then enter router.com as the remote ID on the VPN client.
Secure Connection Remote Accessibility		
	What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
	What is the remote LAN Subnet Mask?	

1. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen for IPv4. By default, the VPN policy is enabled.

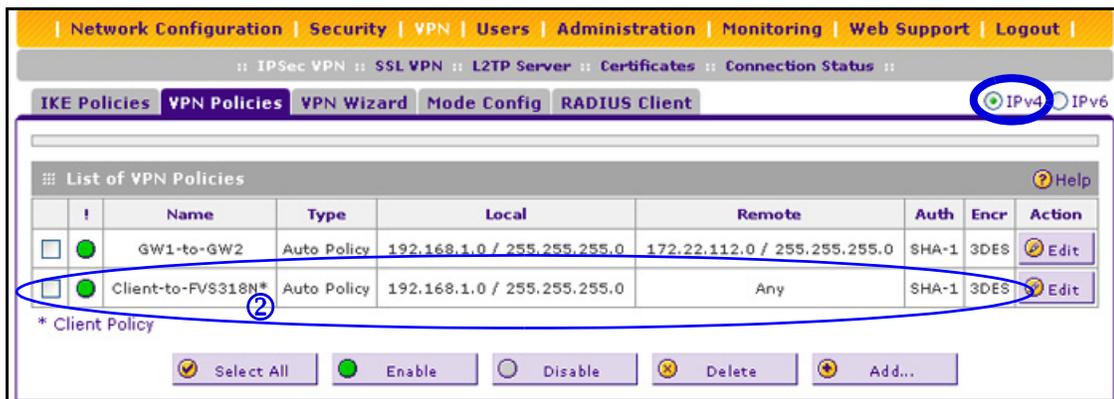


Figure 8.

4. Collect the information that you need to configure the VPN client in your network configuration. You can print the following table to help you keep track of this information (numbers 3, 4, and 5 relate to the same numbers in [Table 5](#) on page 9; numbers 1 and 2 of [Table 5](#) are not applicable; numbers 6 and 7 do *not* relate to any previous samples in this section).

Table 6. Information required to configure the VPN client

#	Component	Enter the information that you collected	Example
③	Pre-shared key		I7!KL39dFG_8
④	Remote identifier information		remote.com
⑤	Local identifier information		local.com
⑥	Router's LAN network IPv4 address		192.168.1.0
⑦	Router's WAN IPv4 address		192.168.15.175

Configure the VPN Client Connection Using the VPN Client Configuration Wizard

Note: Perform these tasks from a computer that has the NETGEAR ProSafe VPN Client installed. If you do not have a VPN client, see <http://www.netgear.com/business/products/software/VPN-client-software/default.aspx>.

The VPN client lets you set up the VPN connection with the integrated Configuration Wizard, which configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the wireless VPN firewall (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to manually enter this information.

- **To use the Configuration Wizard to set up a VPN connection between the VPN client and the wireless VPN firewall:**
 1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays (see the left screen in the following figure).
 2. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (1/3) displays (see the right screen in the following figure).

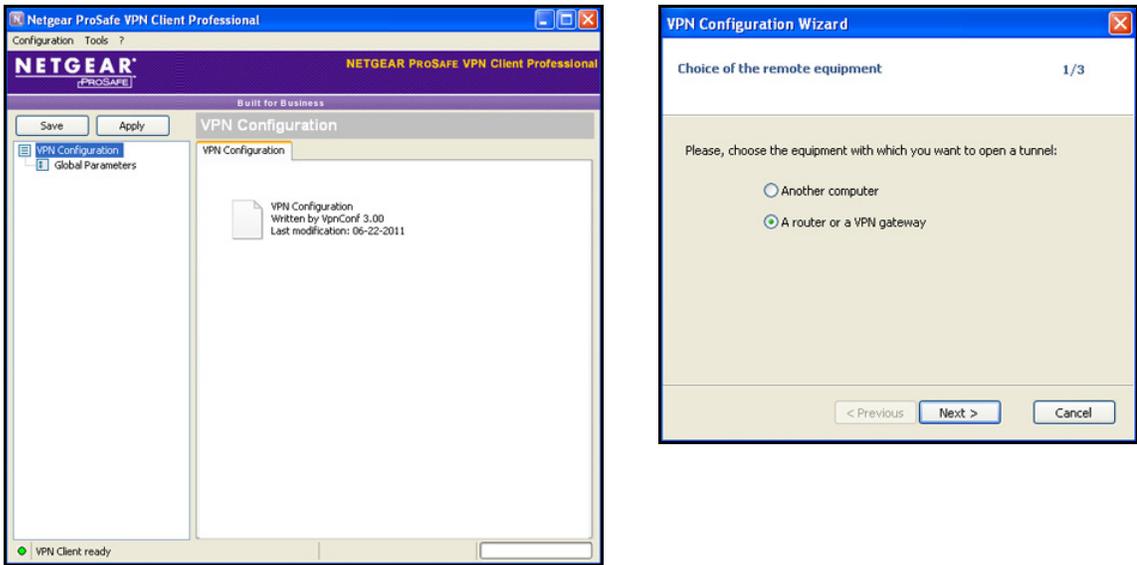


Figure 9.

3. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (2/3) displays (see the left screen in the following figure).

Note: The numbers that are shown in the following figure relate to the numbers that are listed in [Table 6](#) on page 11 and that are explained in [Step 4](#).

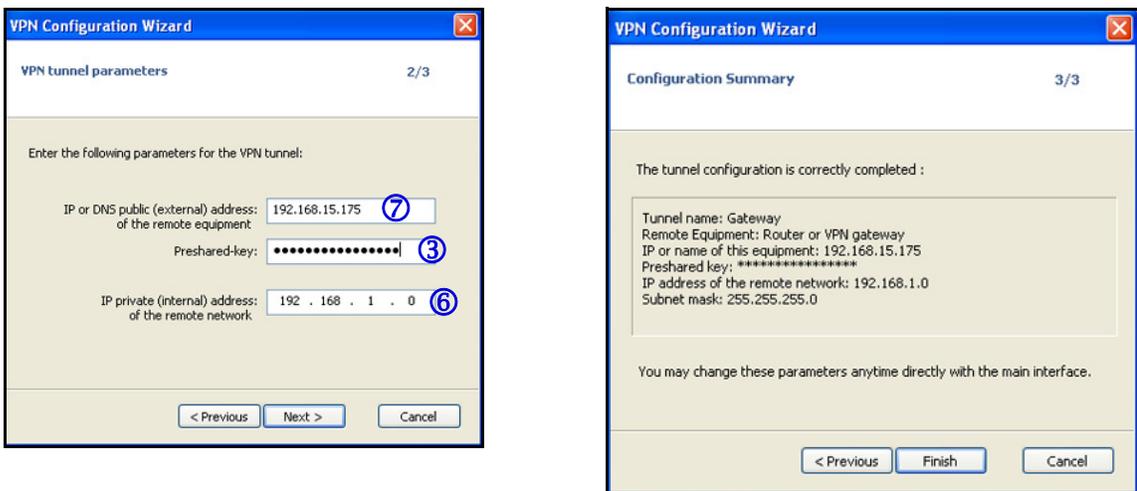


Figure 10.

4. Specify the following VPN tunnel parameters:
 - **IP or DNS public (external) address of the remote equipment.** Enter the remote IP address or DNS name of the wireless VPN firewall. For example, enter **192.168.15.175**. (7)
 - **Preshared-key.** Enter the pre-shared key that you already specified on the wireless VPN firewall. For example, enter **I7!KL39dFG_8**. (3)

- **IP private (internal) address of the remote network.** Enter the remote private IP address of the wireless VPN firewall. For example, enter **192.168.1.0**. (6) This IP address enables communication with the entire 192.168.1.x subnet.
- 5. Click **Next**. The Configuration Summary wizard screen (3/3) displays (see the right screen in *Figure 10* on page 12).
- 6. This screen is a summary screen of the new VPN configuration. Click **Finish**.
- 7. Specify the local and remote IDs:
 - a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
 - b. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

Note: The numbers that are shown in the following figure relate to the numbers that are listed in *Table 6* on page 11 and that are explained in *Table 7*.

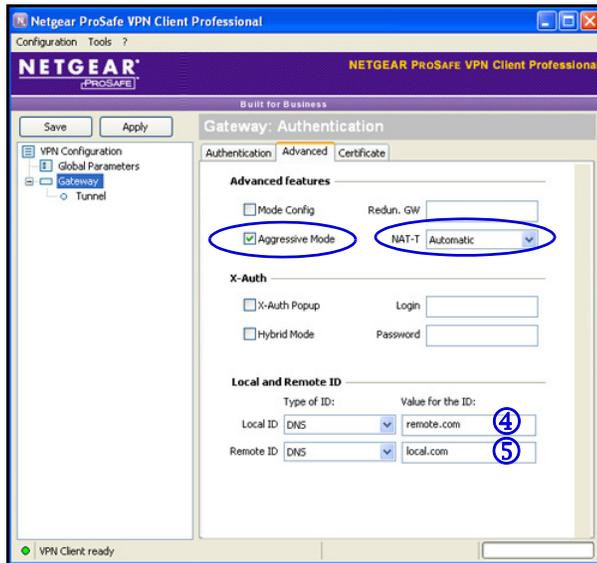


Figure 11.

- c. Specify the settings that are explained in the following table.

Table 7. VPN client advanced authentication settings

#	Setting	Description
Advanced features		
	Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the wireless VPN firewall.
	NAT-T	Select Automatic from the drop-down list to enable the VPN client and wireless VPN firewall to negotiate NAT-T.

Table 7. VPN client advanced authentication settings (continued)

#	Setting	Description
Local and Remote ID		
④	Local ID	As the type of ID, select DNS from the Local ID drop-down list because you specified FQDN in the wireless VPN firewall configuration. As the value of the ID, enter remote.com as the local ID for the VPN client. Note: The remote ID on the wireless VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the wireless VPN firewall and then enter client.com as the local ID on the VPN client.
⑤	Remote ID	As the type of ID, select DNS from the Remote ID drop-down list because you specified an FQDN in the wireless VPN firewall configuration. As the value of the ID, enter local.com as the remote ID for the wireless VPN firewall. Note: The local ID on the wireless VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the wireless VPN firewall and then enter router.com as the remote ID on the VPN client.

8. Configure the global parameters:
 - a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

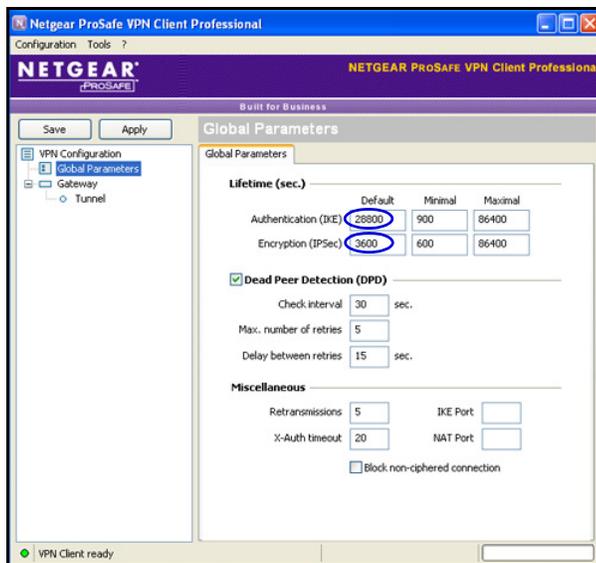


Figure 12.

- b. Specify the default lifetimes in seconds:
 - **Authentication (IKE), Default.** The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the wireless VPN firewall.
 - **Encryption (IPSec), Default.** The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the wireless VPN firewall.
9. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Test the NETGEAR VPN Client Connection

There are many ways to establish a connection. The following procedures assume that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*.

➤ **To establish a connection:**

Right-click the system tray icon (), and select **Open tunnel 'Tunnel'** (see the left screen). When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray (see the right screen).

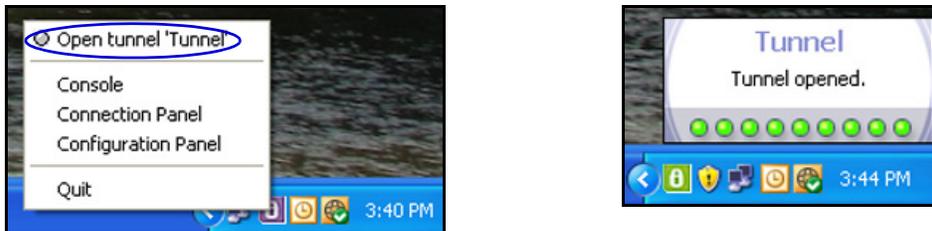


Figure 13.

Once launched, the VPN client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code:

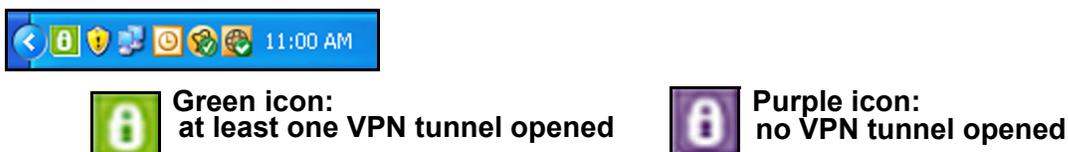


Figure 14.

For More Information

Chapter 6, “Virtual Private Networking Using IPSec and L2TP Connections,” of the *Reference Manual* provides information about the following security topics:

- Managing IPSec VPN policies
- Configuring extended authentication (XAUTH)
- Assigning IPv4 addresses to remote users (Mode Config)
- Configuring keep-alives and Dead Peer Detection (DPD)
- Configuring NetBIOS bridging with IPSec VPN
- Configuring the L2TP server