Configuring IPSec VPNs

This guide describes how to use the Unified Threat Management appliance (UTM) IPSec VPN Wizard to configure the IP security (IPSec) virtual private networking (VPN) feature. This feature provides secure, encrypted communications between your local network and a remote network or computer. For information about other features and for complete configuration steps, see the *ProSecure Unified Threat Management (UTM) Appliance Reference Manua*l at: *http://support.netgear.com*.

This guide contains the following sections:

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match each other precisely. The VPN Wizard guides you through the setup procedure to set the IPSec keys and VPN policies. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that the VPN Wizard uses are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

Be familiar with the following terms:

Dynamic Host Configuration Protocol (DHCP). A protocol for assigning dynamic IP addresses to devices on a network.

Fully Qualified Domain Name (FQDN). A complete address such as myhost.sr1.com

Use the IPSec Wizard to Create a Gateway-to-Gateway VPN Tunnel

Gateway-to-gateway VPN tunnels are used to create secure network to network connections across the Internet.

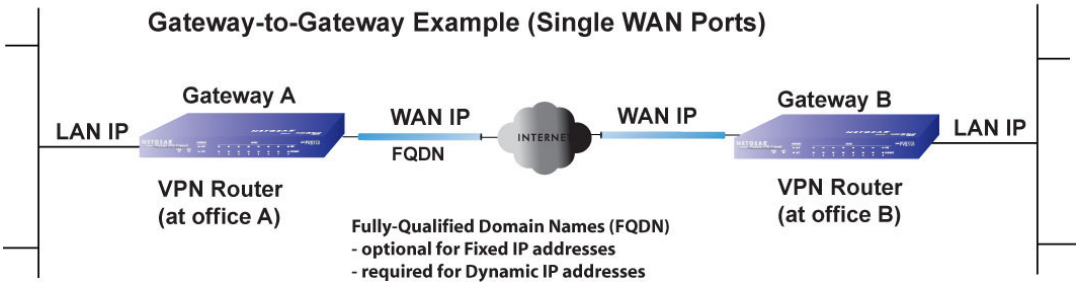
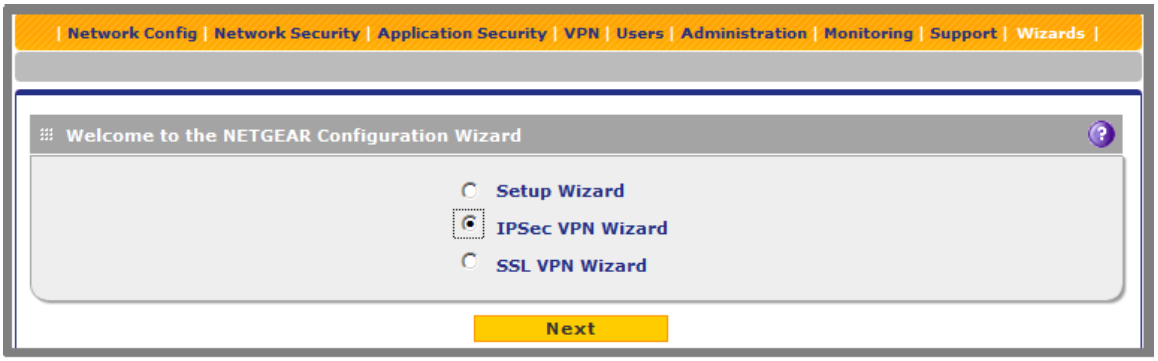


Figure 1. Typical gateway-to-gateway connection

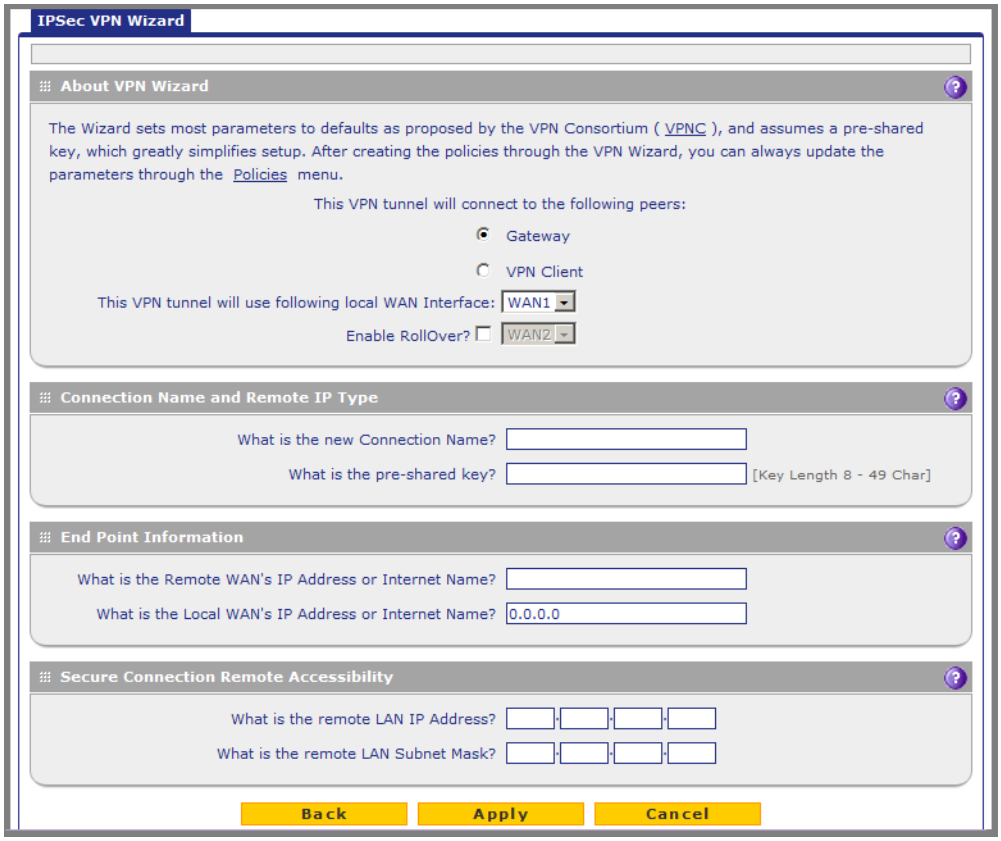
➢ **To set up a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **Wizards** from the main menu. The Welcome to the Netgear Configuration Wizard screen displays:



2. Select the **IPSec VPN Wizard** radio button.
3. Click **Next**. The first IPSec VPN Wizard screen displays.

   The IPSec VPN wizard screen has a drop-down list from which you can select the WAN interface, and a check box to enable VPN rollover. There is another drop-down list to select a WAN interface for VPN rollover. If the UTM is configured to function in WAN auto-rollover mode, you can also use the VPN Wizard to configure VPN rollover.



4. Select the radio buttons and complete the fields as explained in the following table:

Table 1. IPSec VPN Wizard settings for a gateway-to-gateway tunnel

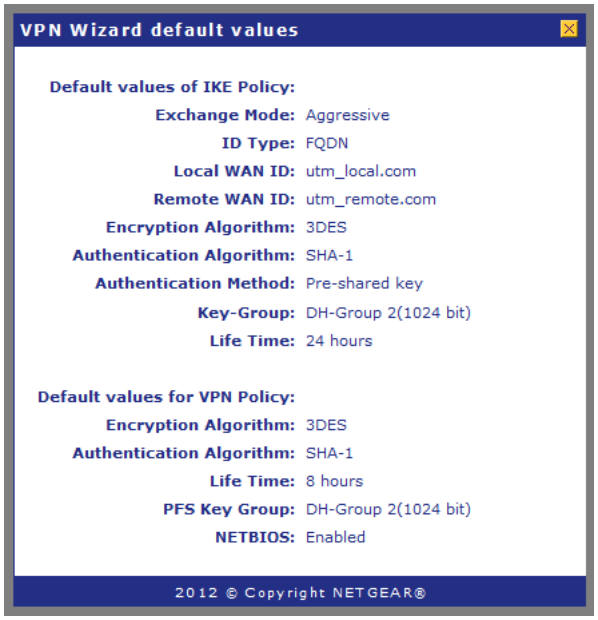
Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port IP address or Internet name displays in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings. The name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key must be entered both here and on the remote VPN gateway. This key must have a minimum length of 8 characters and not exceed 49 characters.

Table 1. IPSec VPN Wizard settings for a gateway-to-gateway tunnel (continued)

Setting	Description
This VPN tunnel uses the following local WAN Interface (multiple WAN port models only)	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	Select the **Enable RollOver?** check box to enable VPN rollover, and then select a WAN interface from the drop-down list to the right of the check box to specify the rollover interface. **Note:** If the multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover address.
End Point Information[a]	
What is the Remote WAN IP Address or Internet Name?	Enter the IP address or Internet name. The name must be a fully qualified domain name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
What is the Local WAN IP Address or Internet Name?	If you select the Gateway radio button in the About VPN Wizard section of the screen, the IP address of the UTM's active WAN interface is automatically entered.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IP address of the remote gateway. **Note:** The remote LAN IP address must be in a different subnet than 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.
What is the remote LAN Subnet Mask?	Enter the LAN subnet mask of the remote gateway.

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

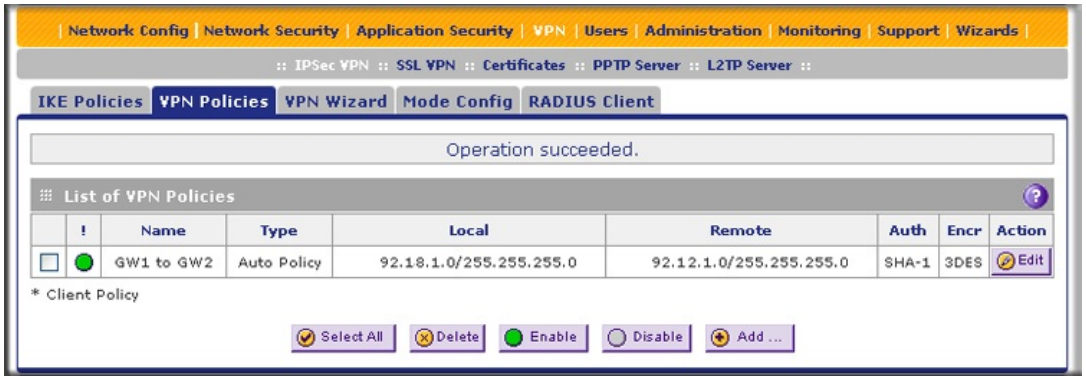
To view the wizard default settings, click the **VPNC** link in the About VPN Wizard panel. A pop-up screen displays (see the following figure), showing the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.



Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alives. This setting periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see the reference manual.

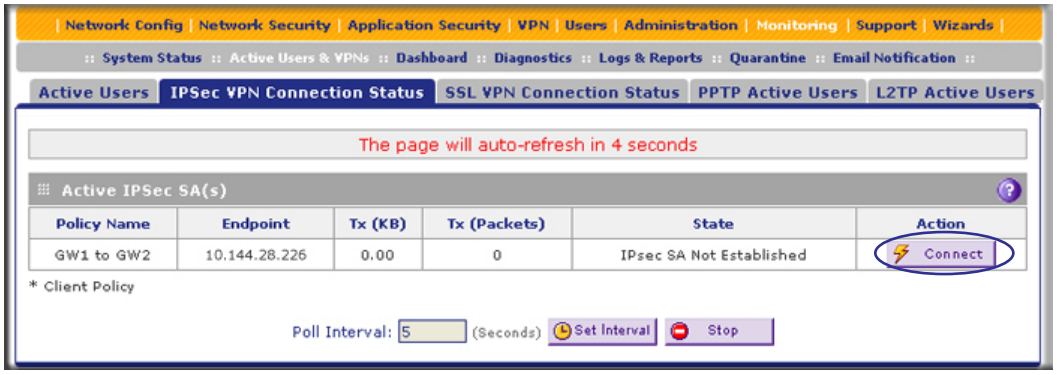
Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you have validated the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

5. 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. By default, the VPN policy is enabled.



6. Configure a VPN policy on the remote gateway that allows connection to the UTM.
7. Activate the IPSec VPN connection:

a. Select **Monitoring > Active Users & VPNs > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays.



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

Note: If you use FQDNs and the Domain Name Server (DNS) service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails. This is because the FQDNs do not resolve to your new address. If you can configure the update interval, set it to an appropriate short time.

Use the IPSec Wizard to Create a Client-to-Gateway VPN Tunnel

Client-to-gateway VPN tunnels are used to create secure connections across the Internet between a network and a computer.

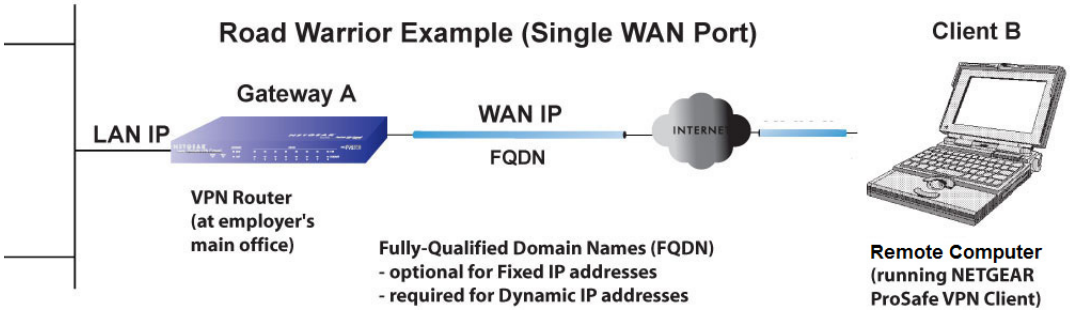
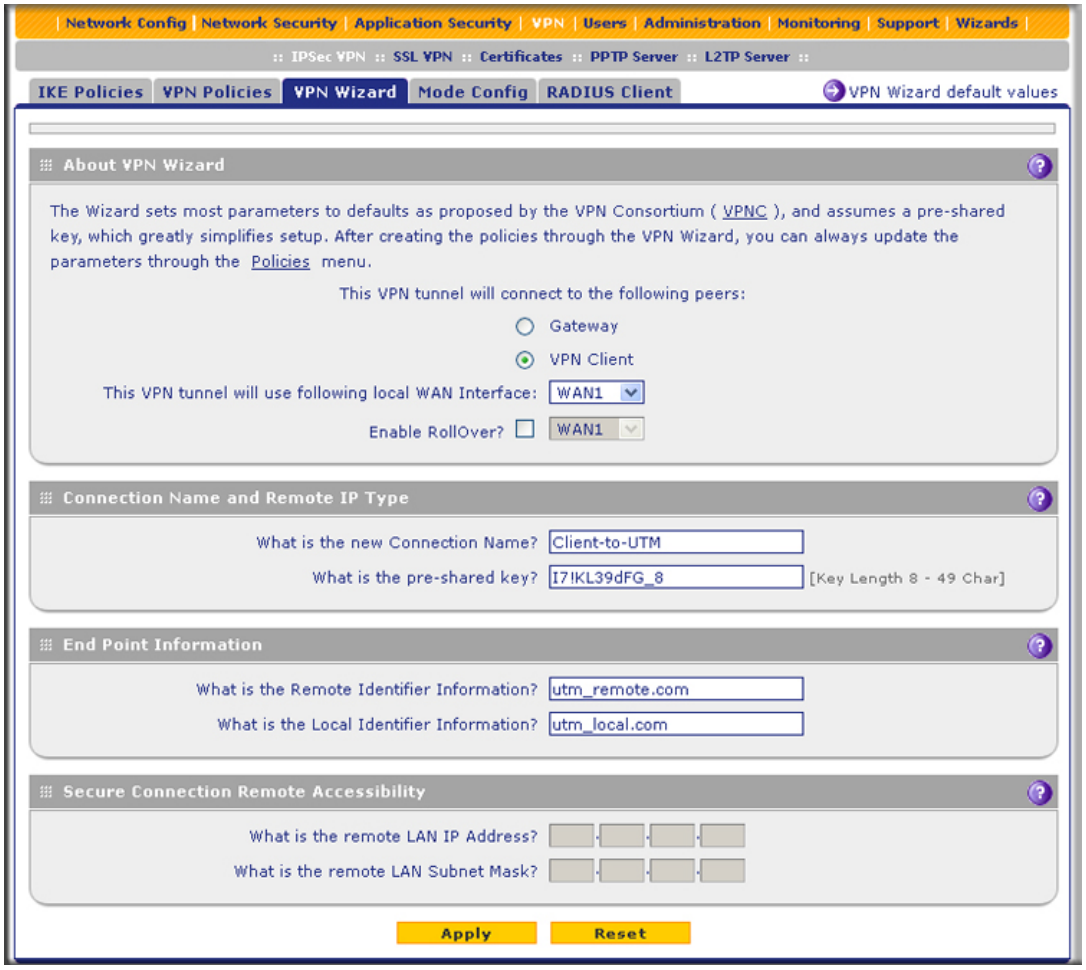


Figure 2. A typical gateway-to-client connection

➢ **To configure a client-to-gateway VPN tunnel:**

1. Make sure the VPN Client radio button is selected.



To display the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right corner of the screen. A pop-up screen displays (see *Figure 4* on page 3), showing the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

2. Select the radio buttons and complete the fields as explained in the following table:

Table 2. IPSec VPN Wizard settings for a client-to-gateway tunnel

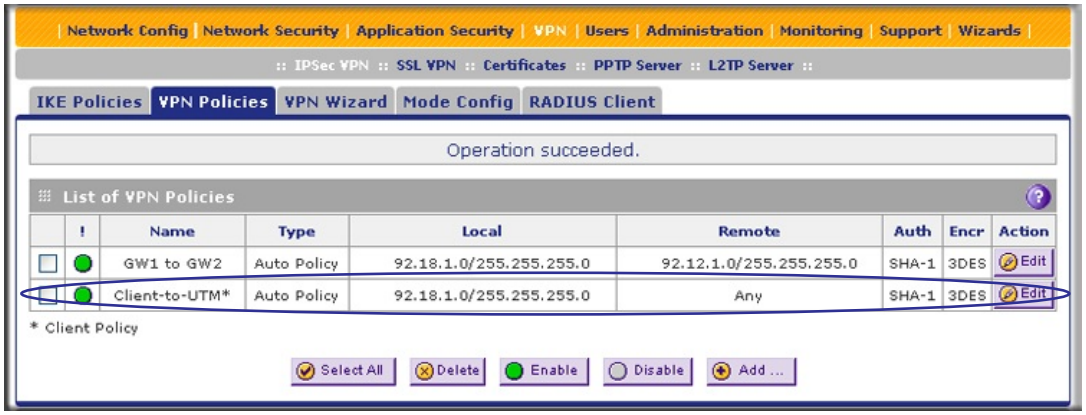
Setting	Description
About VPN Wizard	
This VPN tunnel connects to the following peers	Select the **VPN Client** radio button. The default remote FQDN (utm_remote.com) and the default local FQDN (utm_local.com) display in the End Point Information section of the screen.

Table 2. IPSec VPN Wizard settings for a client-to-gateway tunnel (continued)

Setting	Description
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key must be entered both here and on the remote VPN gateway, or the remote VPN client. This key must have a minimum length of 8 characters and cannot exceed 49 characters.
This VPN tunnel will use following local WAN Interface	Select a WAN interface from the drop-down list to specify which local WAN interface the VPN tunnel uses as the local endpoint.
	Select the **Enable RollOver?** check box to enable VPN rollover, and then select a WAN interface from the drop-down list to the right of the check box to specify the rollover interface. **Note:** If the UTM is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover.
End Point Information[a]	
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 (utm_remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN.
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 (utm_local.com) is automatically entered. Use the default local FQDN, or enter another FQDN.
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?	

a. Both local and remote endpoints must 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. By default, the VPN policy is enabled.



Note: If you use FQDNs and the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails. It fails because the FQDNs do not resolve to your new address. If you can configure the update interval, set it to an appropriate short time.

4. This step is optional. Collect the information to configure the VPN client. You can print the following table to help you track this information.

Table 3. Information required to configure the VPN client

Component	Example	Configuration Information
Pre-shared key	I7!KL39dFG_8	
Remote identifier information	utm_remote.com	
Local identifier information	utm_local.com	
Router LAN network IP address	192.168.1.0	
Router LAN network mask	255.255.255.0	
Router WAN IP address	10.34.116.22	

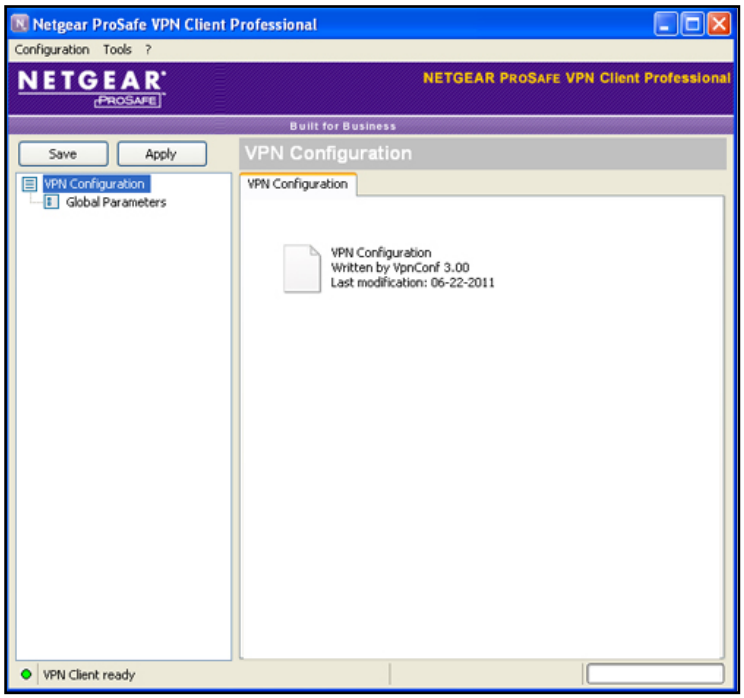
Create a Secure Connection

The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the UTM (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you must enter this information manually.

> **Note:** Perform these tasks from a computer running Windows that has the NETGEAR ProSafe VPN Client installed.

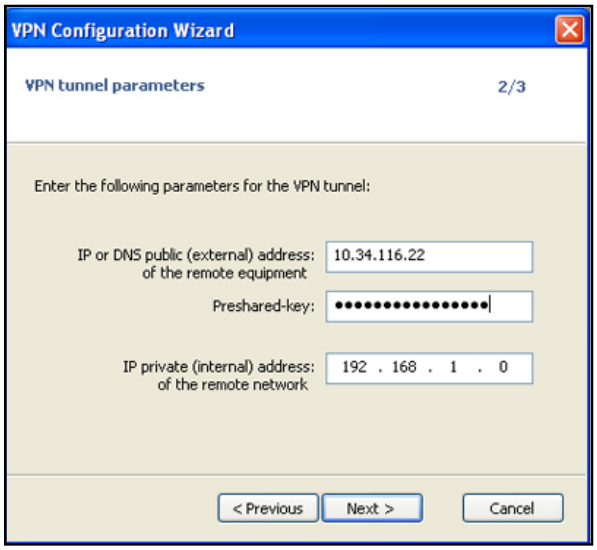
➢ **To set up a VPN connection between the VPN client and the UTM:**

1. Right-click the VPN client icon in your Windows system tray and select **VPN Configuration**. The VPN Configuration Panel displays.



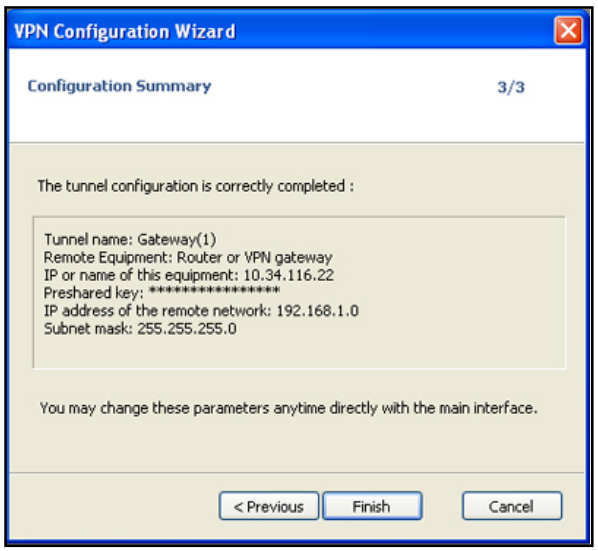
2. From the main menu, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays.

3. Select the **A router or a VPN gateway** radio button and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays.

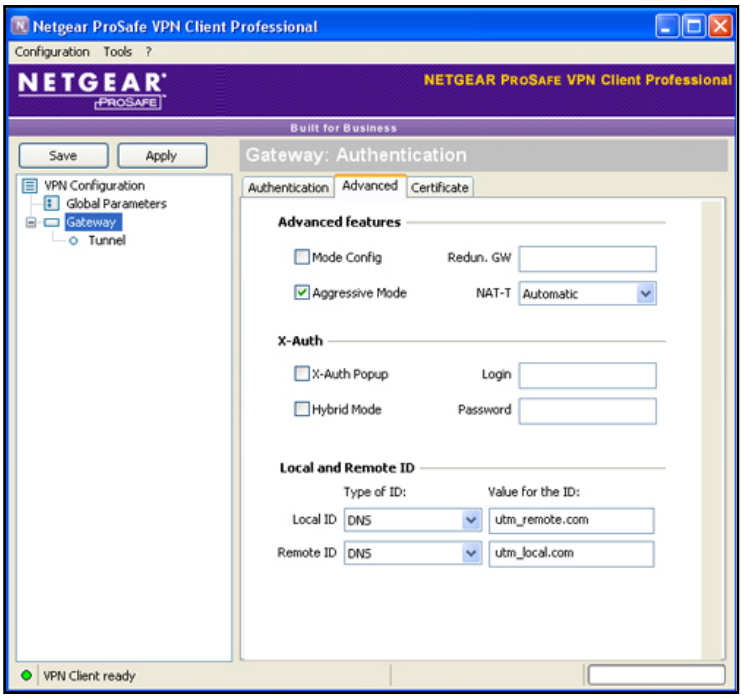


4. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the UTM. For example, enter **10.34.116.22**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the UTM. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the UTM. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.

5. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays. This screen is a summary screen of the new VPN configuration.



6. Click **Finish**.
7. Specify the local and remote IDs:
   a. In the navigation pane click **Gateway** (the default name given to the authentication phase). The Gateway Authentication pane displays with the Authentication tab selected by default.
   b. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.



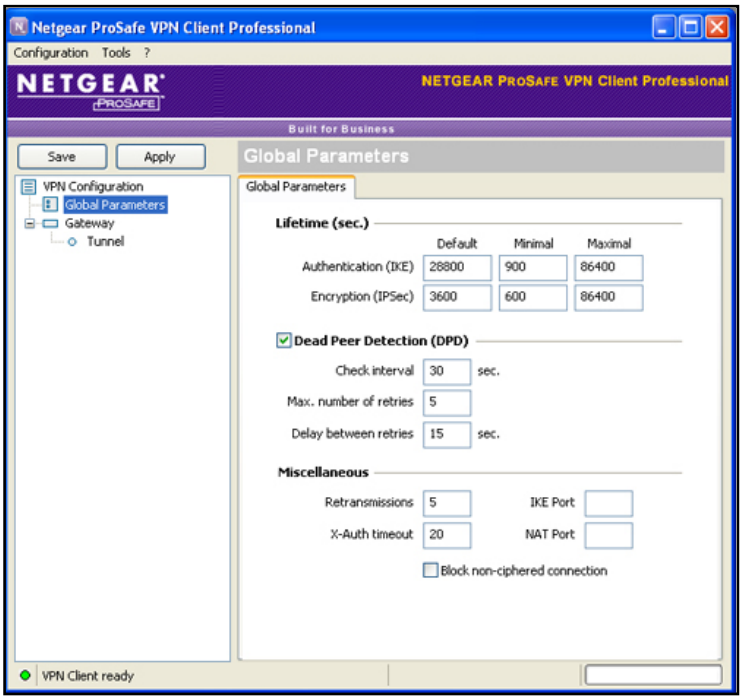
c. Specify the settings that are explained in the following table.

Table 4. 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 UTM.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and UTM to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the UTM configuration. As the value of the ID, enter **utm_remote.com** as the local ID for the VPN client. **Note:** The remote ID on the UTM is the local ID on the VPN client. It is less confusing to configure an FQDN such as client.com as the remote ID on the UTM and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the UTM configuration. As the value of the ID, enter **utm_local.com** as the remote ID for the UTM. **Note:** The local ID on the UTM is the remote ID on the VPN client. It is less confusing to configure an FQDN such as router.com as the local ID on the UTM and then enter router.com as the remote ID on the VPN client.

8. Configure the global parameters:

a. Click **Global Parameters** in the navigation pane. The Global Parameters pane displays.



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 UTM.
- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the UTM.

9. Click **Apply** to use the new settings immediately.
10. Click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

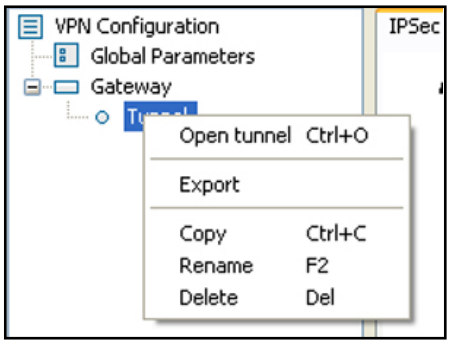
Test the Connection to the VPN CLient

Both the NETGEAR ProSafe VPN Client and the UTM provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a 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*. If you manually set up the connection and changed the names, use *vpn_client* (or any other name that you have configured) as the authentication phase name. Use *netgear_platform* (or any other name that you have configured) as the IPSec configuration name.

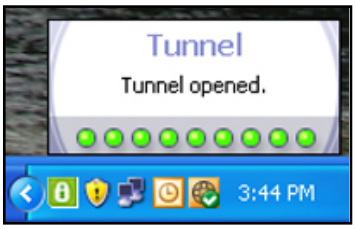
➢ **Use the Configuration screen to establish a connection:**

1. In the navigation pane right-click the **Tunnel** IPSec configuration name.



2. Select **Open tunnel**.

When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:



Once launched, the VPN client displays an icon in the system tray that indicates whether a tunnel is opened, using a color code:

Green icon:
at least one VPN tunnel opened

Purple icon:
no VPN tunnel opened

What to Do Next

You have completed configuring an IPSec VPN network. There are several additional features that can be configured. See the reference manual for procedures for the following:

- Manage IPSec VPN Policies
- Configure Extended Authentication (XAUTH)
- Assign IP Addresses to Remote Users (Mode Config)
- Configure Keep-Alives and Dead Peer Detection
- Configure NetBIOS Bridging with IPSec VPN
- Configure the PPTP Server
- Configure the L2TP Server