Create IPSec VPN Tunnels with the Wizard

ProSecure UTM Quick Start Guide

This quick start guide describes how to use the IPSec VPN Wizard to configure IPSec VPN tunnels on the ProSecure Unified Threat Management (UTM) Appliance. The IP security (IPSec) virtual private networking (VPN) 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 Manual*, available at *http://downloadcenter.netgear.com*.

This quick start guide contains the following sections:

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	IP address or FQDN	FQDN
Local WAN ID	Local WAN IP address or FQDN	utm_local1.com
Remote WAN ID	Remote WAN IP address or FQDN	utm_remote1.com
Encryption algorithm	3DES	3DES

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

IKE Policy Settings	Gateway-to-Gateway Tunnels	Gateway-to-Client Tunnels
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 Dynamic Host Configuration Protocol (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 you use FQDNs and a Dynamic DNS (DDNS) service, if the DDNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails 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 “Configure Keep-Alives” in Chapter 7, “Virtual Private Networking Using IPSec, PPTP, or L2TP Connections,” of the reference manual.

Create a Gateway-to-Gateway VPN Tunnel

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

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays. (The following screen contains an example.)

   The About VPN Wizard section of the VPN Wizard screen shows the following minor differences for the various UTM models:

   - Single WAN port models. No WAN selection drop-down lists and no Enable RollOver check box.
   - Multiple WAN port models. A drop-down list to select the WAN interface, a check box to enable VPN rollover, and another drop-down list to select a WAN interface for VPN rollover. If a multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.

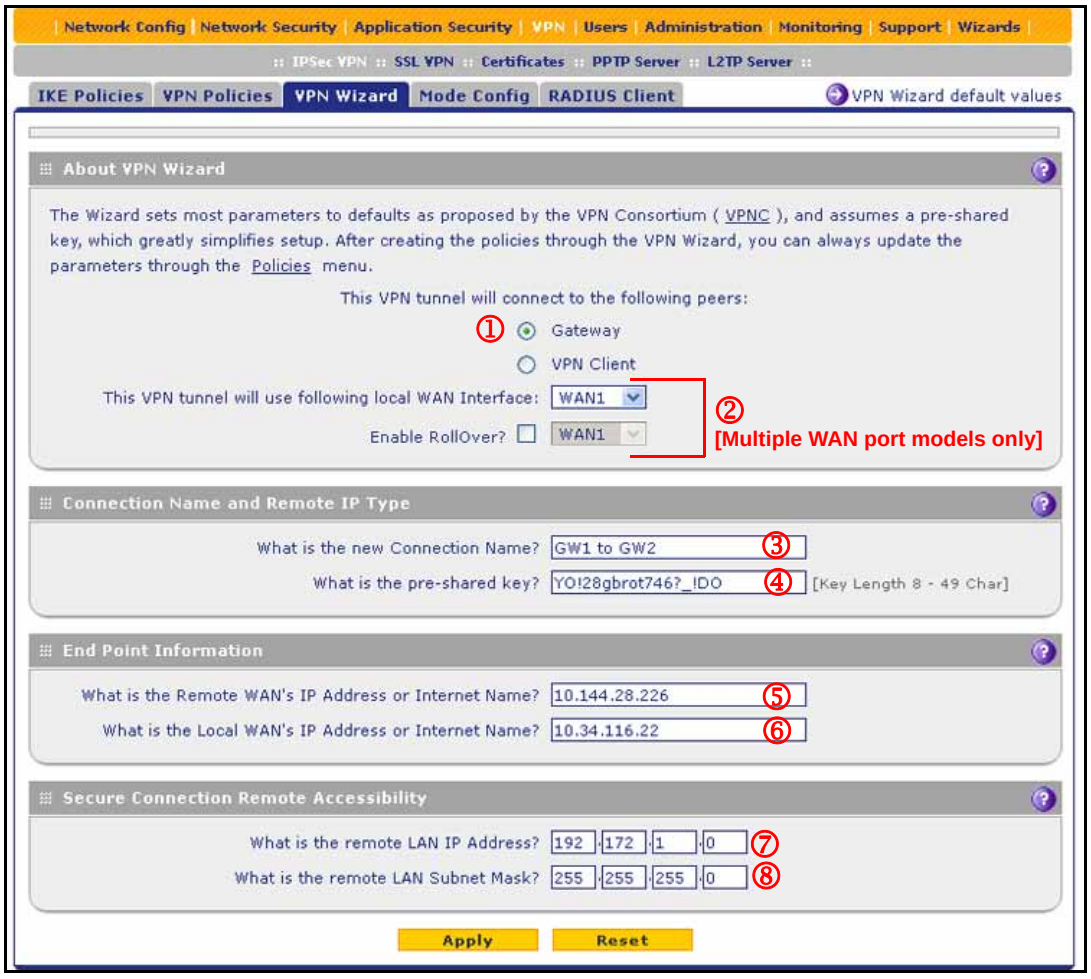

Figure 1.

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

Table 3. IPSec VPN Wizard settings for a 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 displays in the End Point Information section of the screen.
②	This VPN tunnel will use 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 interface to which the VPN rollover should occur. **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 and do not need to configure this manually.
Connection Name and Remote IP Type		
③	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.
④	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 Information[a]		
⑤	What is the Remote WAN's IP Address or Internet Name?	Enter the IP address or Internet name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
⑥	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 IP address of the UTM's active WAN interface is automatically entered.
Secure Connection Remote Accessibility		
⑦	What is the remote LAN IP Address?	Enter the LAN IP address of the remote gateway. **Important:** The remote LAN 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.
⑧	What is the remote LAN Subnet Mask?	Enter the LAN subnet mask of the remote gateway.

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

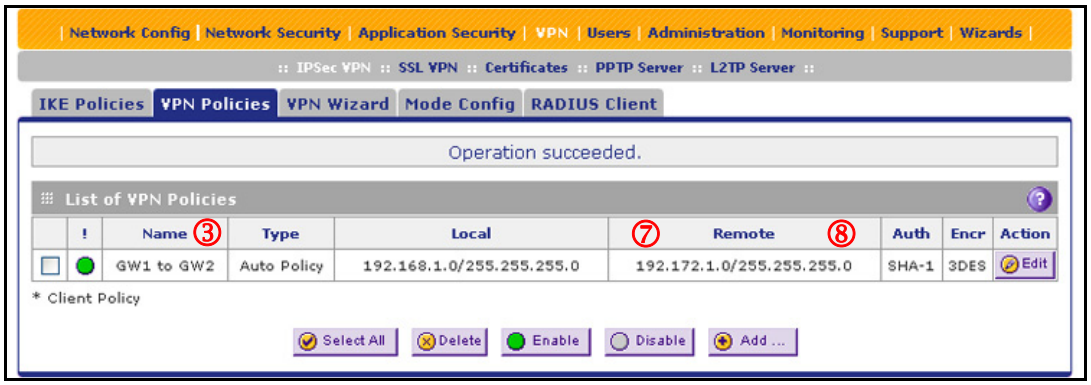

Figure 2.

4. Configure a VPN policy on the remote gateway that allows connection to the UTM.
5. Activate the IPSec VPN connection:
   a. Select **Monitoring > Active Users & VPNs > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays:

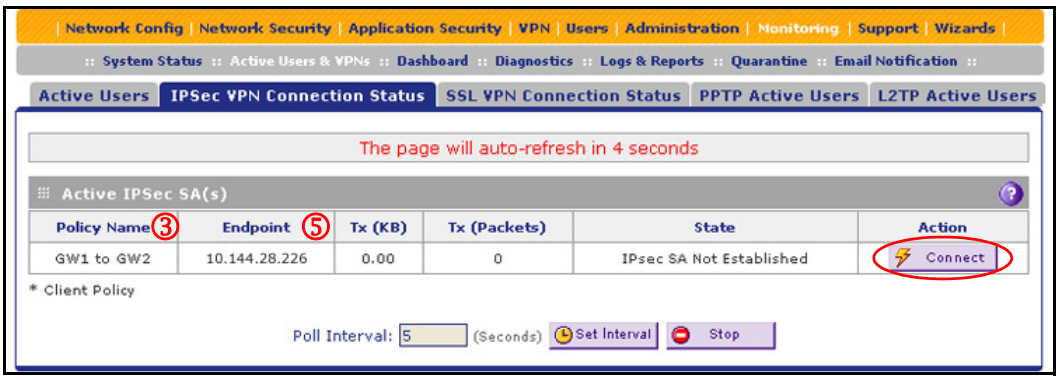

Figure 3.

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

Configure an 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 VPN Client Connection*

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**. The VPN Wizard screen displays. (The following screen contains an example.)

   The About VPN Wizard section of the VPN Wizard screen shows the following minor differences for the various UTM models:

   - Single WAN port models. No WAN selection drop-down lists and no Enable RollOver check box.
   - Multiple WAN port models. A drop-down list to select the WAN interface, a check box to enable VPN rollover, and another drop-down list to select a WAN interface for VPN rollover. If a multiple WAN port model is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure this manually.

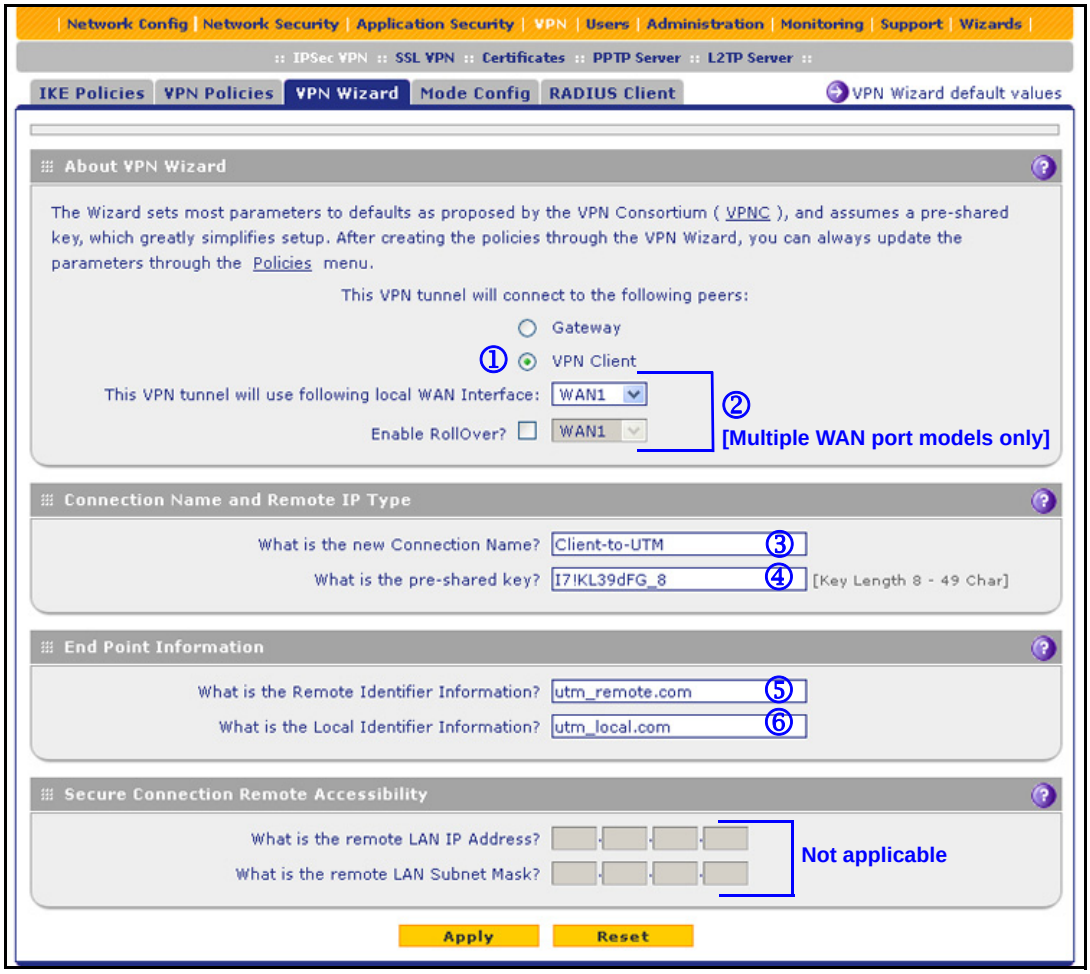

Figure 4.

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

Table 4. IPSec VPN Wizard settings for a client-to-gateway 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 (utm_remote.com) and the default local FQDN (utm_local.com) display in the End Point Information section of the screen.
②	This VPN tunnel will use 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 interface to which the VPN rollover should occur. **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 and do not need to configure this manually.
Connection Name and Remote IP Type		
③	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.
④	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, or the remote VPN client. This key needs to have a minimum length of 8 characters and cannot exceed 49 characters.
End Point Information[a]		
⑤	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.
⑥	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 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. By default, the VPN policy is enabled.

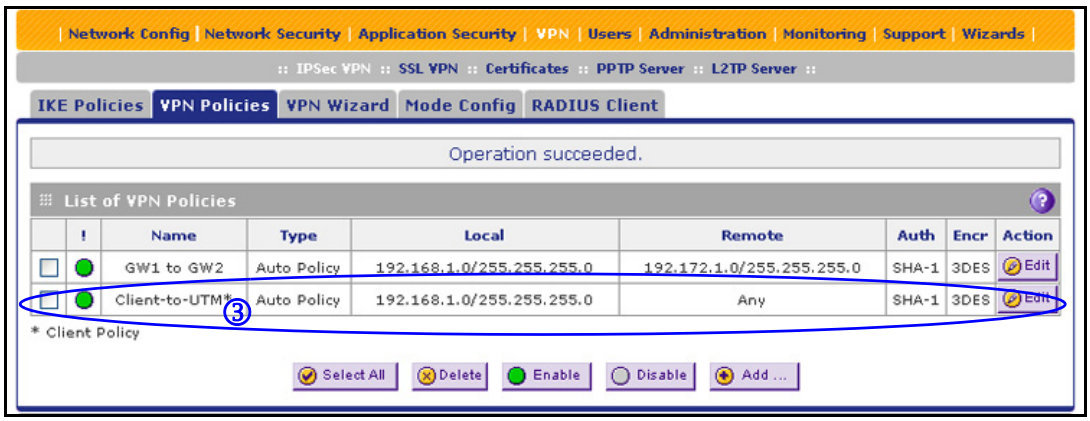

Figure 5.

4. Optional step: Collect the information that you need to configure the VPN client. You can print the following table to help you keep track of this information.

Note: In the following table, numbers ❶, ❷, and ❸ do *not* relate to *Figure 4*, *Figure 5*, and *Table 4*. However, ④, ⑤, and ⑥ do relate to the numbers in *Figure 4*, *Figure 5*, and *Table 4*. These numbers are used in the figures and descriptions in *Configure the VPN Client Connection Using the VPN Client Configuration Wizard* on page 9.

Table 5. Information required to configure the VPN client

#	Component	Information to be collected	Example
❶	Router's LAN network IP address		192.168.1.0
❷	Router's LAN network mask		255.255.255.0
❸	Router's WAN IP address		10.34.116.22
④	Pre-shared key		I7!KL39dFG_8
⑤	Remote identifier information		utm_remote.com
⑥	Local identifier information		utm_local.com

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, visit *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 UTM (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to enter this information manually.

➢ **To use the Configuration Wizard 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 **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 (screen 1of 3) displays (see the right screen in the following figure).

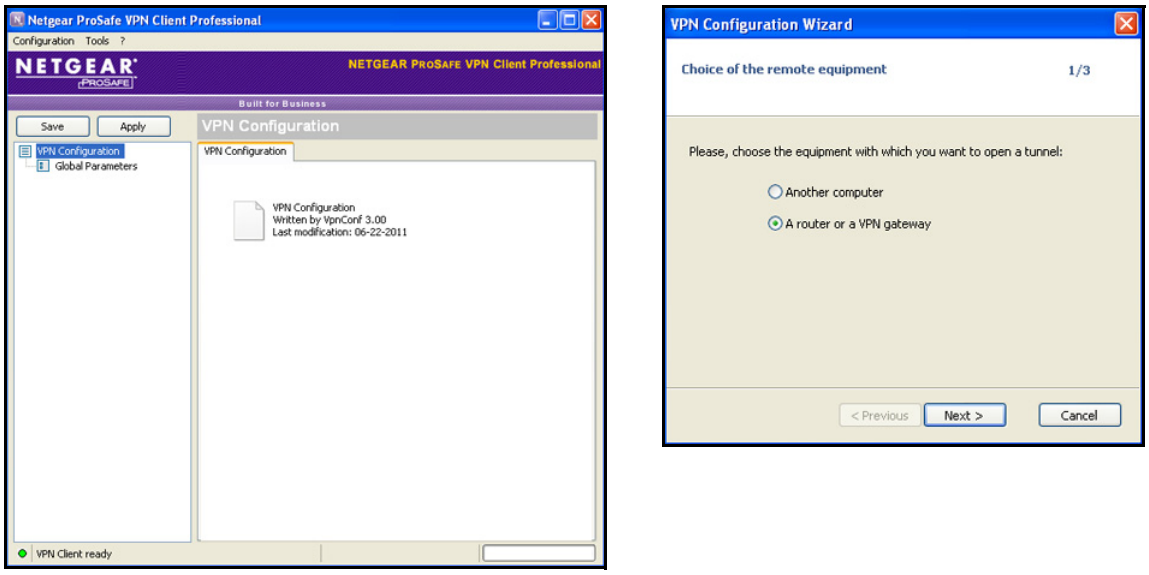

Figure 6.

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 (see the left screen in the following figure; the numbers in the figure refer to the numbers in *Table 5* on page 8 and are described in *Step 4*).

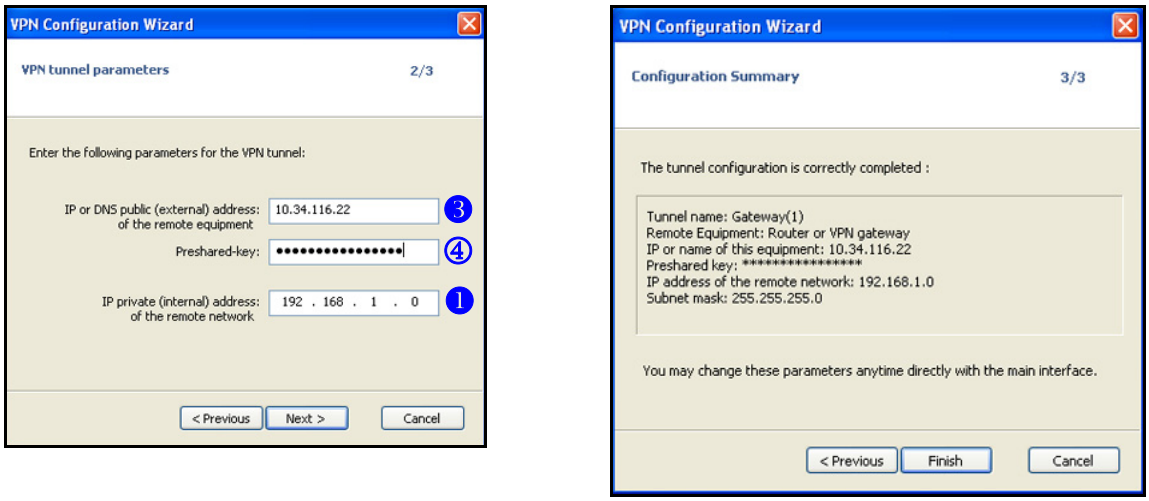

Figure 7.

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**. (❸)
   - **Preshared key**. Enter the pre-shared key that you already specified on the UTM. For example, enter **I7!KL39dFG_8**. (④)
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the UTM. For example, enter **192.168.1.0**. (❶) 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 (see the right screen in *Figure 7*).
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.

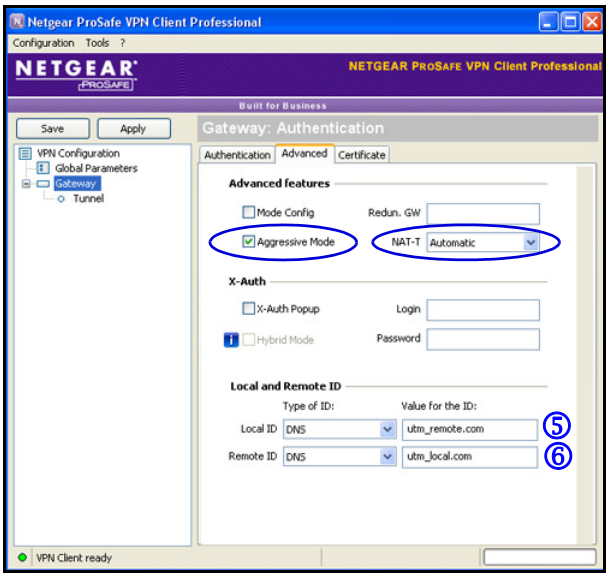

Figure 8.

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

Table 6. 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		
⑤	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 might be 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.
⑥	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 might be 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. In the tree list pane of the Configuration Panel screen, click **Global Parameters**. The Global Parameters pane displays in the Configuration Panel screen.

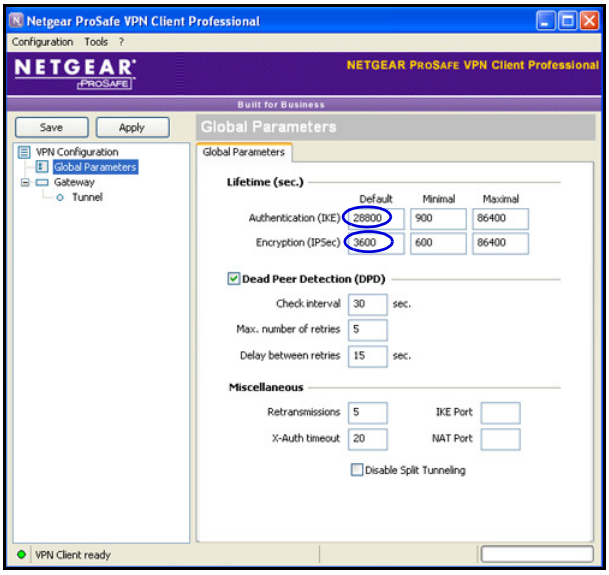

Figure 9.

   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, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Test the 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*. NETGEAR recommends that you test the connection from a computer that is located off-site rather than from a computer that is located behind the UTM.

➢ **To establish a connection:**

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

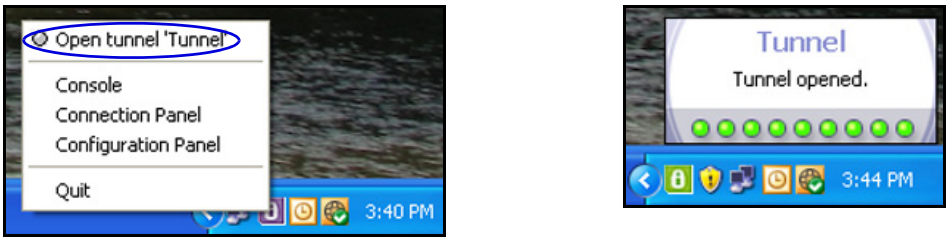

Figure 10.

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

Figure 11.

For More Information

Chapter 7, “Virtual Private Networking Using IPSec, PPTP, or L2TP Connections,” of the reference manual provides information about the following VPN topics:

- Managing IPSec VPN and IKE policies
- Configuring extended authentication (XAUTH)
- Assigning IP addresses to remote users (Mode Config)
- Configuring keep-alives and dead peer detection
- Configuring NetBIOS bridging with IPSec VPN
- Configuring the PPTP server
- Configuring the L2TP server