EnGenius®

Wireless Gigabit VPN Router

EVR100 VPN Configuration Guide

Wireless N VPN Router with Gigabit Switch

V1.0

Table of Contents

Revision History

Version	Date	Notes
1.0	2011/01/10	First Release

1. Introduction

A Virtual Private Network (VPN) provides a secure connection between two remote offices or two users over the public Internet. It provides authentication to secure the encrypted data communicated between the two remote endpoints.

The EVR100 Wireless N Security VPN Router with Gigabit Switch supports Internet Protocol Security **(IPSec)** and Layer 2 Tunneling Protocol (**L2TP over IPSec**) to establish VPN tunnel connections. IPSec VPN tunnels support Site-to-Site tunnels and Client-to-Site tunnels. L2TP over IPSec tunnels provide remote access when connecting Windows native VPN clients.

The EVR100 supports 5 IPSec VPN tunnels, making it ideal for small-office and home-office (SOHO) users. The EVR100 also provides advanced SPI firewall, denial of service (DoS) attack blocking, MAC filtering, and URL filtering to secure high-speed network connections.

This Configuration Guide provides step-by-step instructions for setting up the following three VPN tunnels:

1. IPSec Site-to-Site using two EVR100 routers. See the next page.
2. IPSec Client to Site using TheGreenBow as an IPSec client. See page 32.
3. L2TP over IPSec using Microsoft Windows 7 and Windows Vista as VPN clients. See page 47.

   This Guide ends with the procedure for configuring an Apple Mac VPN client (see page 83).

2. IPSec Site-to-Site

IPSec Site-to-Site VPN tunnels typically are used when two remote locations want to exchange confidential data. To set up an IPSec Site-to-Site VPN tunnel, configure two EVR100 VPN routers to establish a secured channel. The computers connected to the EVR100s can then exchange the data securely using the VPN tunnel.

You can set up the VPN profile by either using a friendly, point-and-click Wizard or entering profile settings manually. To set up your VPN profile in the quickest way possible, use the Wizard (see sections 2.2). If you are a technical user and prefer to set up your VPN profile manually, see sections 2.3 and 2.4.

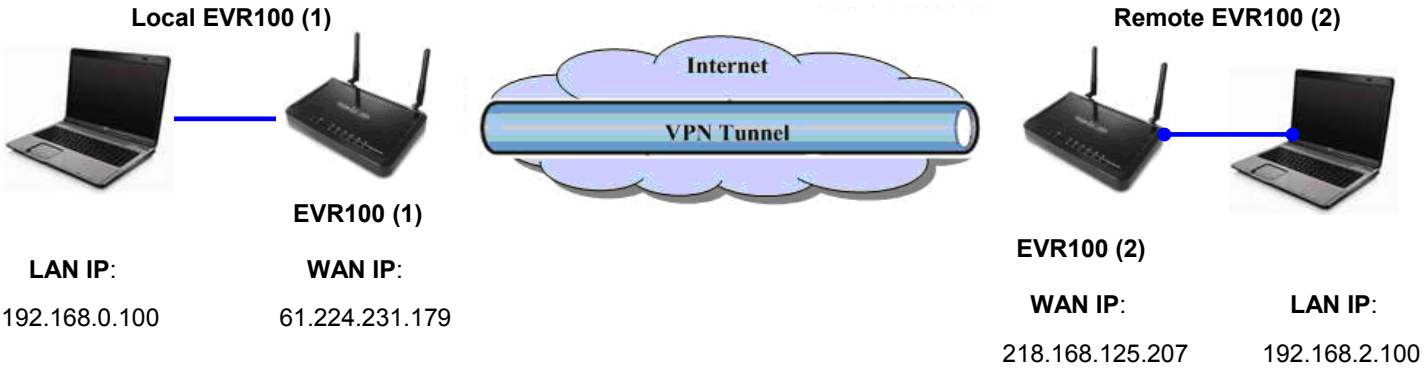
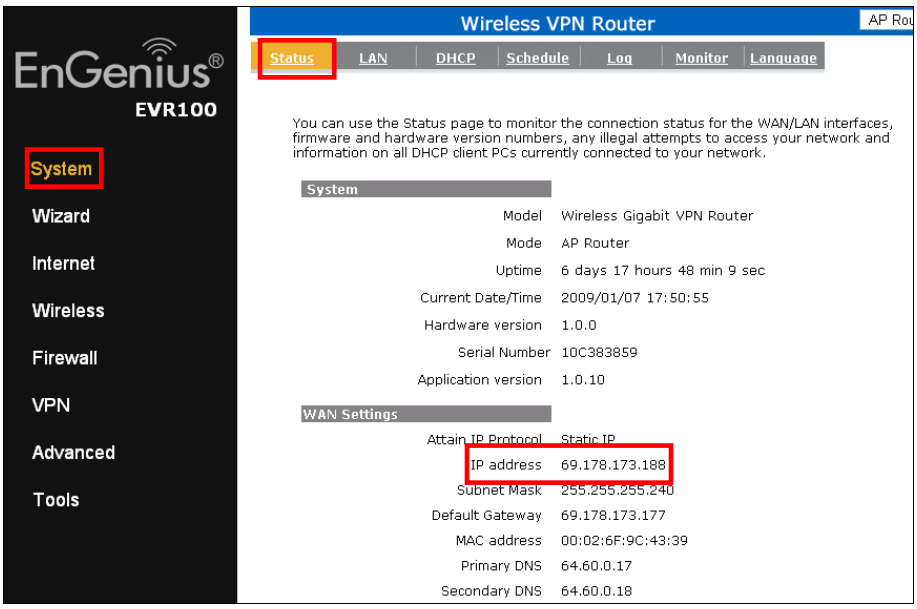


Figure 1. Example of an IPSec Site-to-Site VPN Tunnel

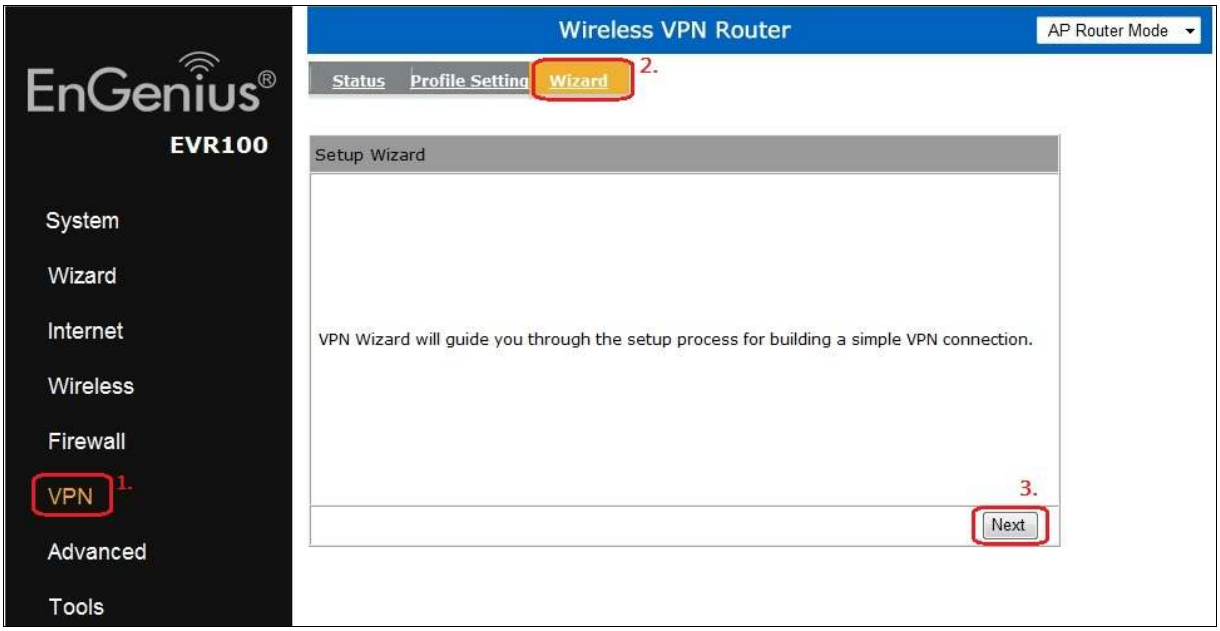
Note: You can find the EVR100 WAN IP under **System > Status**.



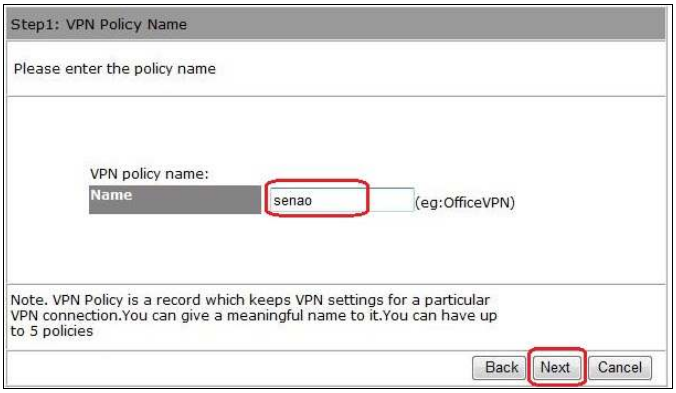
2.1. Using the Wizard to Configure the Local EVR100

This configuration procedure corresponds to the EVR100 (1) in Figure 1.

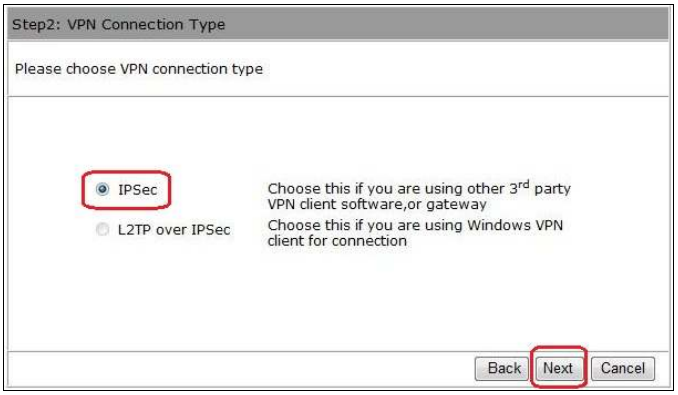
1. In the left-side of the menu, click **VPN**.
2. In the top menu, click **Wizard** to display the Setup Wizard.
3. Click **Next** to create an IPSec Site-to-Site VPN tunnel.



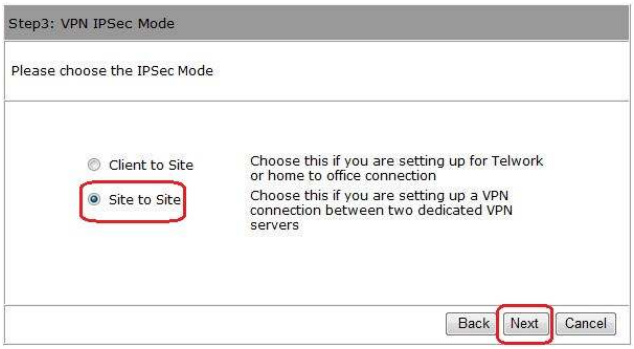
4. In the **Name** field, enter a name for the Site-to-Site VPN tunnel. This name is for reference purposes. Click **Next**.



5. Click **IPSec**, and then click **Next**.



6. Click **Site to Site**, and then click **Next**.



7. Complete the following fields:

Security Gateway Enter the WAN IP of the remote EVR100 (2) to which you want to connect. In Figure 1, this is **EVR100 (2)**.

Remote Address Enter an IP address that is on the same subnet as the LAN IP address of the computer connected behind the remote EVR100 (2). In Figure 1., for example, enter a remote address starting with: 192.168.2.x.

Remote Netmask Type **255.255.255.0**.

Click **Next**.

8. Create the **Shared key** for the local EVR100 (1) VPN, and then click **Next**.

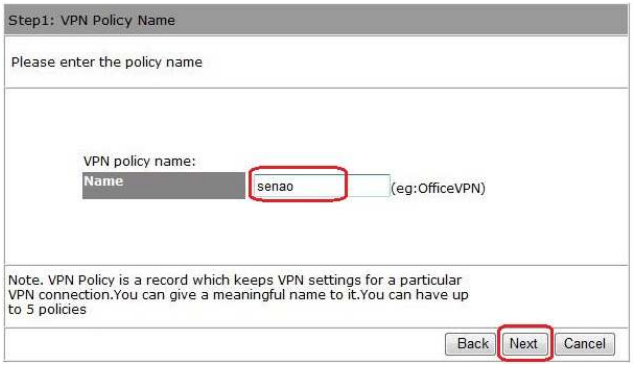
Note: By default, the SA (Security Association) is **ESP-3DES-SHA1**. If desired, you can change it after using the Wizard to add the VPN profile.

9. Check the option below to enable the VPN policy, and then click **Apply** to save the local EVR100 (1) VPN profile. This completes the procedure for configuring your local EVR100 (1) VPN profile.

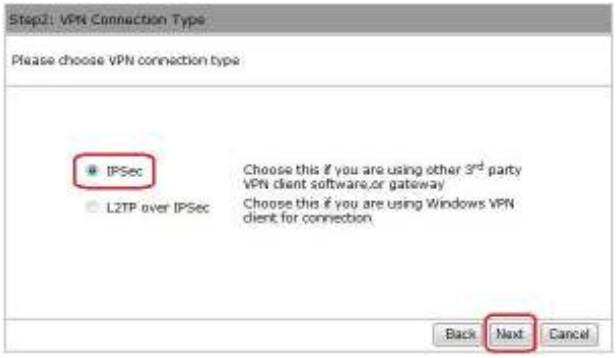
2.2. Using the Wizard to Configure the Remote EVR100

After you configure the local EVR100, use the following procedure to configure the remote EVR100 VPN Profile. This procedure is similar to the one used to configure the local EVR100. This configuration procedure corresponds to the EVR100 (2) in Figure 1. Example of an IPSec Site-to-Site VPN Tunnel.

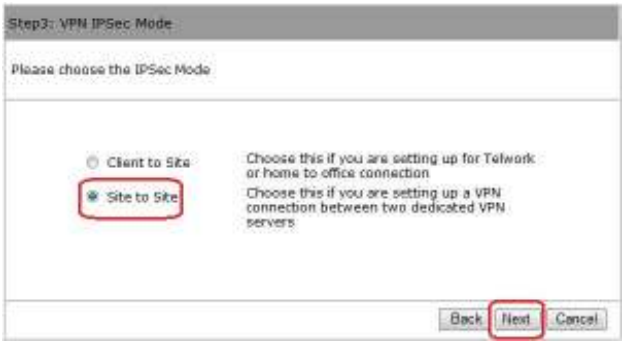
1. Enter the **Name** for the remote EVR100 (2) VPN profile**,** and then click **Next.**



2. Click **IPSec**, and then click **Next**.



3. Click **Site to Site**, and then click **Next**.



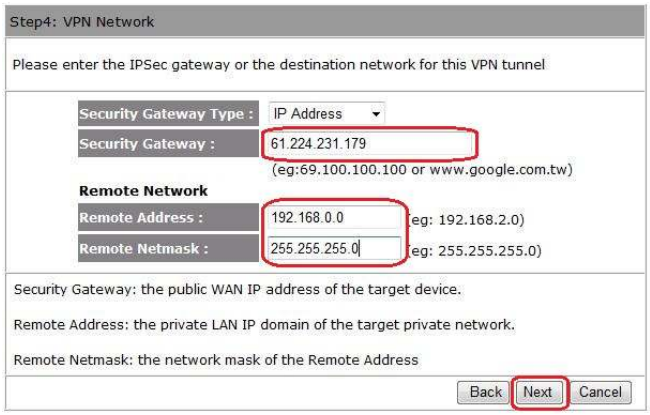
4. Complete the following fields:

Security Gateway Enter the WAN IP of the local EVR100 (1) to which you want to connect. In Figure 1, this is **EVR100 (1)**.

Remote Address Enter an IP address that is on the same subnet as the LAN IP address of the computer connected behind the EVR100 (1). In Figure 1, for example, enter a local address starting with: 192.168.0.x.

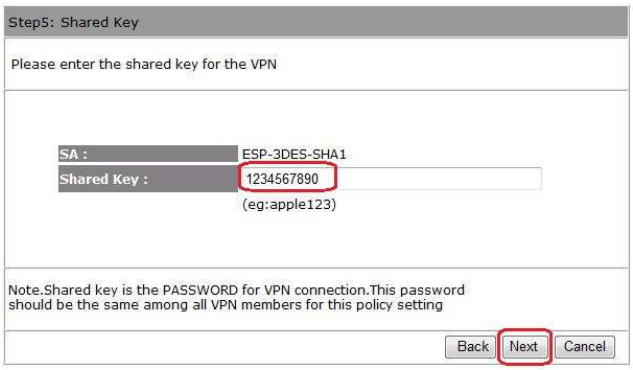
Remote Netmask Type **255.255.255.0**.

Click **Next**.



5. Create the **Shared key** for the remote EVR100 VPN, and then click **Next**.

Note: By default, the SA (Security Association) is **ESP-3DES-SHA1**. If desired, you can change it after using the Wizard to add the VPN profile.



6. Check the option below to enable the VPN policy, and then click **Apply** to save the remote EVR100 VPN profile. This completes the procedure for configuring your remote EVR100 (2) VPN profile.

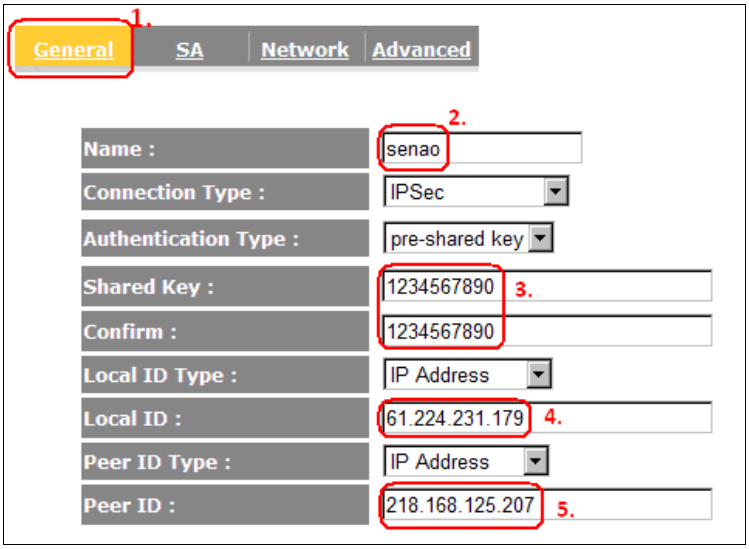
2.3. Configuring the Local EVR100 Manually

The following procedure describes how to manually configure the local EVR100 for an IPSec Site-to-Site VPN tunnel. This configuration procedure corresponds to the EVR100 (1) in Figure1. Example of an IPSec Site-to-Site VPN Tunnel.

1. In left-side of the menu, click **VPN**.
2. In the top menu, click **Profile Setting**.
3. Click **Add** to create an IPSec Site-to-Site VPN tunnel.

4. Complete the following fields:

Name	Enter a name for the local EVR100 (1) VPN profile.
Connection Type	Click **IPSec**.
Shared Key	Create a shared key for the local EVR100 (1) VPN profile and **Confirm** the shared key.
Local ID Type	Select **IP Address**, **Domain Name**, or **E-Mail Address**. Then complete the following fields appropriately.
Local ID	If you selected **IP Address** for **Local ID Type**, enter the WAN IP address of the local EVR100 (1). If you selected **Domain Name** for **Local ID Type**, enter the domain name of the local EVR100 (1). If you selected **E-Mail Address** for **Local ID Type**, enter an email address to identify the local EVR100 (1).
Peer ID Type	Select the same option you chose for **Local ID Type**.
Peer ID	Enter the WAN IP address of the remote EVR100 (2) if you select the IP Address in Peer ID Type. Enter the Domain Name of the remote EVR100 (2) if you select the Domain Name in Peer ID Type. Enter the email address of the remote EVR100 (2) if you select the E-Mail Address in Peer ID Type.

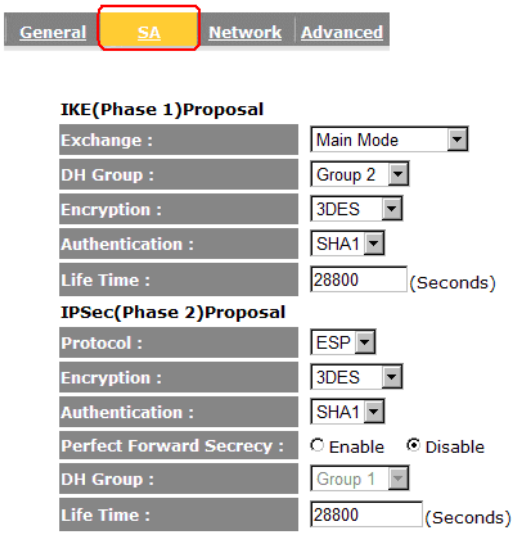


5. Select the appropriate encryption and authentication algorithms for the IKE SA.

Exchange Choices are **Main mode** and **Aggressive mode**. **Main mode** provides higher security at a slower speed than **Aggressive mode**. The default setting is **Main mode**. We recommend you accept this setting.

Encryption Choices are **3DES**, **AES128**, **AES192**, and **AES256**. The default setting is **3DES**. Choose the setting that matches the remote EVR100.

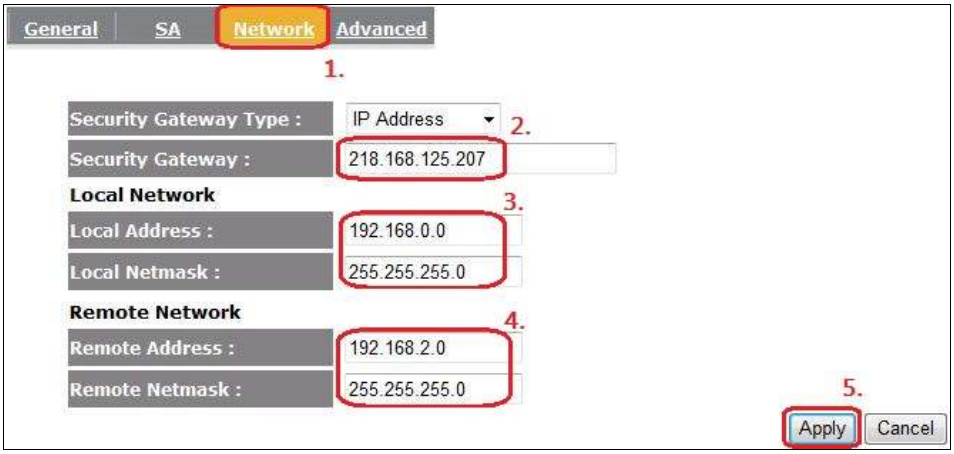
Authentication Choices are **MD5** and **SHA1**. SHA1 provides higher security at a slower speed than MD5. The default setting is **SHA1**. Choose the setting that matches the remote EVR100.



6. Go to the **Network** tab and complete the following settings.

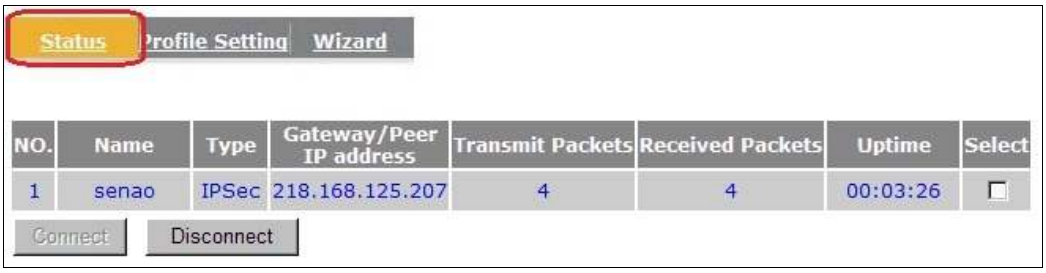
Security Gateway Type	Click **IP Address** or **Domain Name**. Then complete the following fields appropriately.
Security Gateway	If you selected **IP Address** for **Security Gateway Type**, enter the WAN IP address of the remote EVR100 (2). If you selected **Domain Name** for **Security Gateway Type,** enter the domain name of the remote EVR100 (2).
Local Address	Enter an IP address that is on the same subnet of the LAN IP address of the computer connected behind the local EVR100 (1). In Figure 1, for example, the LAN IP address of the local EVR100 (1) is 192.168.0.100.
Local Netmask	Type **255.255.255.0**.
Remote Address	Enter an IP address that is on the same subnet as the LAN IP address of the computer connected behind the remote EVR100 (2). In Figure 1, the LAN IP address of the computer behind the remote EVR100 (2) is 192.168.2.100.
Remote Netmask	Type **255.255.255.0**.

Click **Apply** to save your settings.

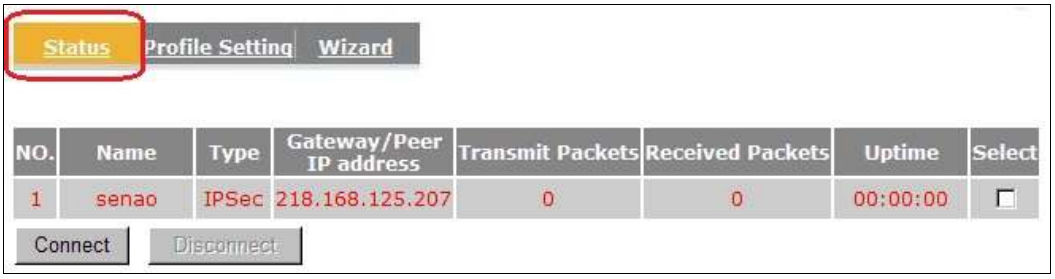


7. Check **Enable**, and then click **Apply** in the **Profile Setting** tab to activate the IPSec Site-to-Site VPN tunnel for EVR100 (1).

8. Go to the **Status** tab to see the VPN tunnel status. **Blue** profiles are configured properly and details are shown for **Transmit Packets**, **Received Packets**, and **Uptime** in tunnels. **Red** profiles indicate profiles have setup problems.



Example of VPN Tunnel Parameters Configured Successfully



Example of VPN Tunnel Parameters Configured Unsuccessfully

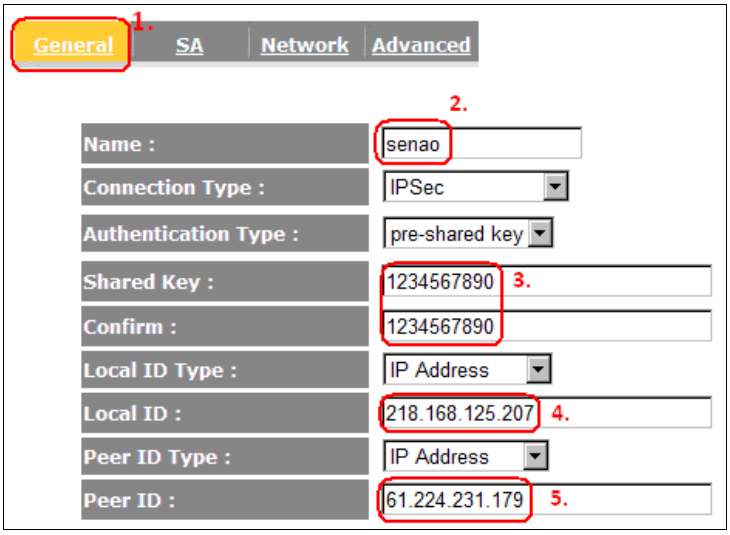
2.4. Configuring the Remote EVR100 Manually

After you configure the local EVR100, use the following procedure to configure the remote EVR100 VPN Profile. This procedure is similar to the one used to manually configure the local EVR100. This configuration procedure corresponds to the EVR100 (2) in Figure 1. Example of an IPSec Site-to-Site VPN Tunnel.

1. In left-side of the menu, click **VPN**.
2. In the top menu, click **Profile Setting** to configure the VPN.
3. Click **Add** to create an IPSec Site-to-Site VPN tunnel.

In the **General tab**, complete the following settings:

Name	Enter a name for the remote EVR100 (2) VPN profile.
Shared Key	Create a shared key for the remote EVR100 (2) VPN profile and **Confirm** the shared key.
Local ID Type	Select **IP Address**, **Domain Name**, or **E-Mail Address**. Then complete the following fields appropriately.
Local ID	If you selected **IP Address** for **Local ID Type**, enter the WAN IP address of the remote EVR100 (2). If you selected **Domain Name** for **Local ID Type**, enter the domain name of the remote EVR100 (2). If you selected **E-Mail Address** for **Local ID Type**, enter an email address to identify the remote EVR100 (2).
Peer ID Type	Select the same option you chose for **Local ID Type**.
Peer ID	Enter the WAN IP address of the local EVR100 (1) to which you want to connect if you select the IP Address in **Peer ID Type**. Enter the Domain Name of the local EVR100 (1) to which you want to connect if you select the Domain Name in Peer ID Type. Enter the email address of the local EVR100 (1) to which you want to connect if you select the E-Mail Address in Peer ID Type.

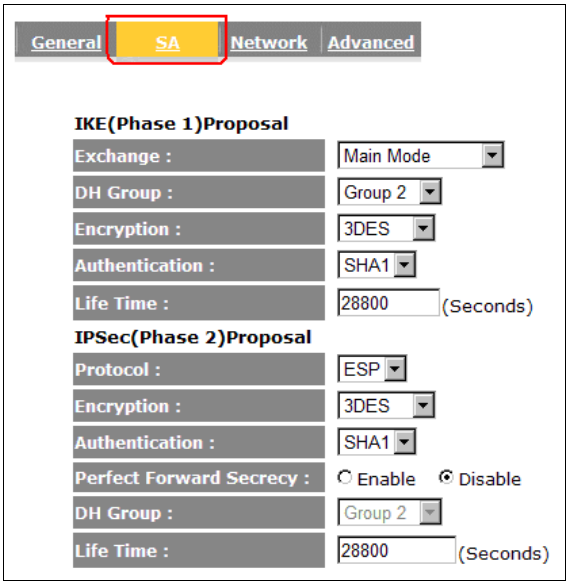


4. Select the appropriate encryption and authentication algorithms for the IKE SA.

Exchange Choices are **Main mode** and **Aggressive mode**. **Main mode** provides higher security at a slower speed than **Aggressive mode**. The default setting is **Main mode**. We recommend you accept this setting. Choose the setting that matches the local EVR100.

Encryption Choices are **3DES**, **AES128**, **AES192**, and **AES256**. The default setting is **3DES**. Choose the setting that matches the local EVR100.

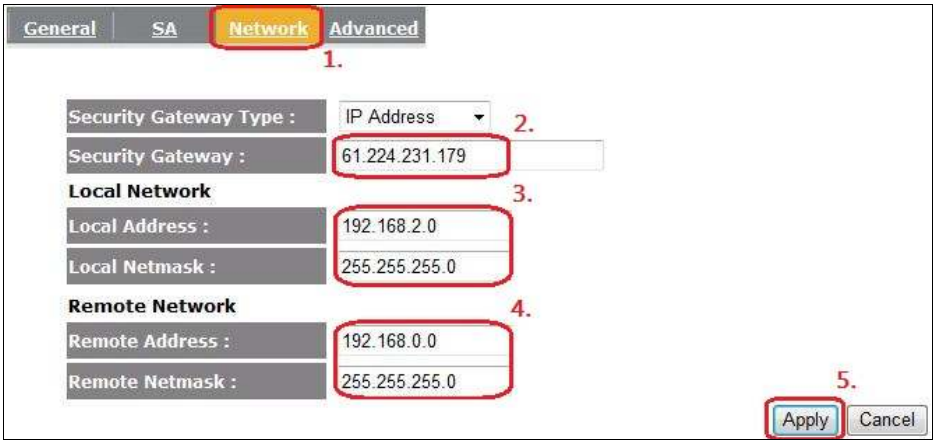
Authentication Choices are **MD5** and **SHA1**. SHA1 provides higher security at a slower speed than MD5. The default setting is **SHA1**. Choose the setting that matches the local EVR100.



5. Go to the **Network** tab and complete the following settings.

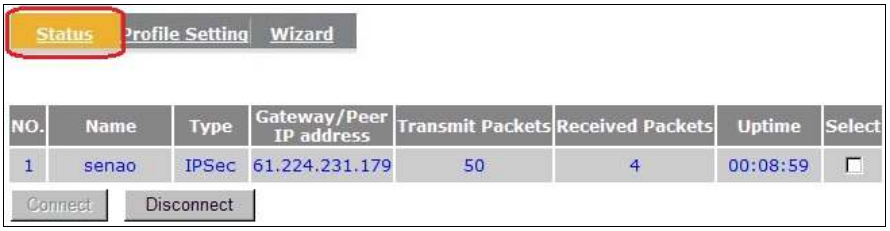
Security Gateway Type	Click **IP Address** or **Domain Name**. Then complete the following fields appropriately.
Security Gateway	If you selected **IP Address** for **Security Gateway Type**, enter the WAN IP address of the local EVR100 (1). If you selected **Domain Name** for **Security Gateway Type,** enter the domain name of the local EVR100 (1).
Local Address	Enter an IP address that is on the same subnet of the LAN IP address of the computer connected behind the remote EVR100 (2). In Figure 1, The LAN IP address of the EVR100 (2) is 192.168.2.100. To be on the same subnet, the IP address must have 192.168.2 as its first three octets (for example, 192.168.2.*x*).
Local Netmask	Type **255.255.255.0**.
Remote Address	Enter an IP address that is on the same subnet as the LAN IP address of the computer connected behind the EVR100 (1). In the example, the LAN IP address of the EVR100 (1) is 192.168.0.100. To be on the same subnet, the IP address must have 192.168.0 as its first three octets (for example, 192.168.0.*x*).
Remote Netmask	Type **255.255.255.0**.

6. Click **Apply** to save your settings.

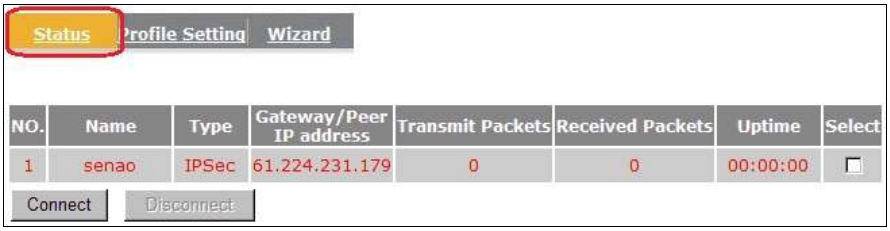


7. Check **Enable** and then click **Apply** in **Profile Setting** field to activate IPSec site-to-site VPN tunnel for the remote EVR100 (2).

8. Go to the **Status** tab to see the VPN tunnel status. **Blue** profiles are configured properly and details are shown for **Transmit Packets**, **Received Packets**, and **Uptime**. **Red** profiles indicate profiles have setup problems.



Example of VPN Tunnel Parameters Configured Successfully



Example of VPN Tunnel Parameters Configured Unsuccessfully

3. IPSec Client-to-Site VPN

IPSec Client-to-Site VPN tunnels are established by connecting third-party VPN clients with EVR100 VPN routers. This chapter provides step-by-step instructions for configuring TheGreenBow, a popular VPN client, with the EVR100. Remote users can access secured, encrypted company data through IPSec Client-to-Site VPN tunnel using a VPN client.

You can set up the IPSec Client-to-Site VPN profile by either using a friendly, point-and-click Wizard or entering profile settings manually. To set up your VPN profile in the quick way possible, use the Wizard (see section 3.1). If you are a technical user and prefer to set up your VPN profile manually, see section 3.2.

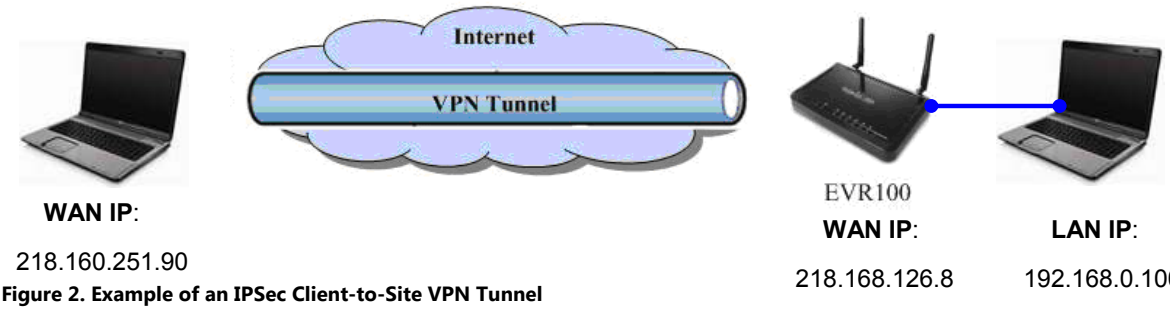
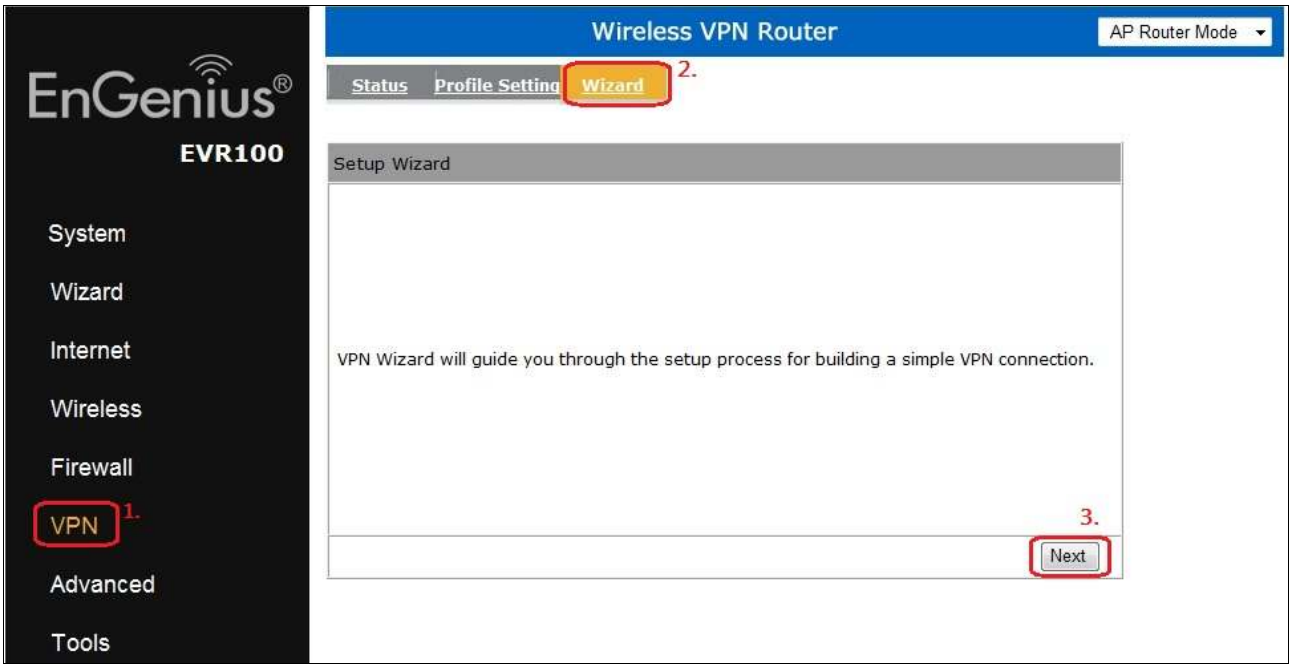


Figure 2. Example of an IPSec Client-to-Site VPN Tunnel

3.1. Using the Wizard to Configure the EVR100

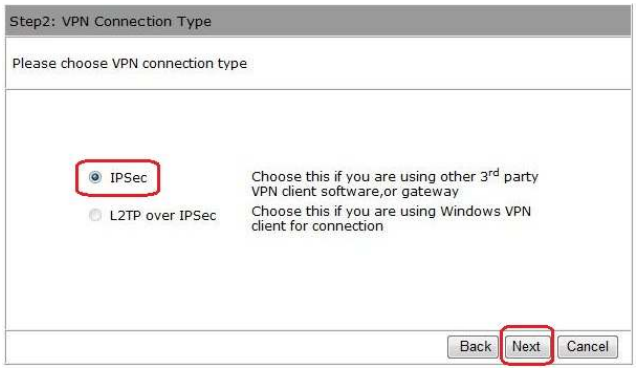
1. In left-side of the menu, click **VPN**.
2. In the top menu, click **Wizard** to add a VPN profile.
3. Click **Next** to create an IPSec Client-to-Site VPN profile.



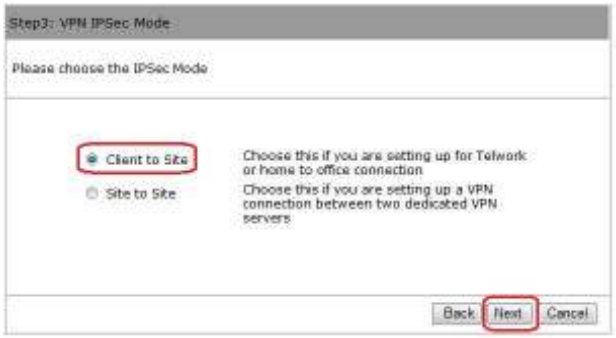
4. In the **Name** field, enter a name for the Client-to-Site VPN tunnel. This name is for reference purposes.

Click **Next**.

5. Click **IPSec,** and then click **Next**.



6. Click **Client to Site**, and then click **Next**.



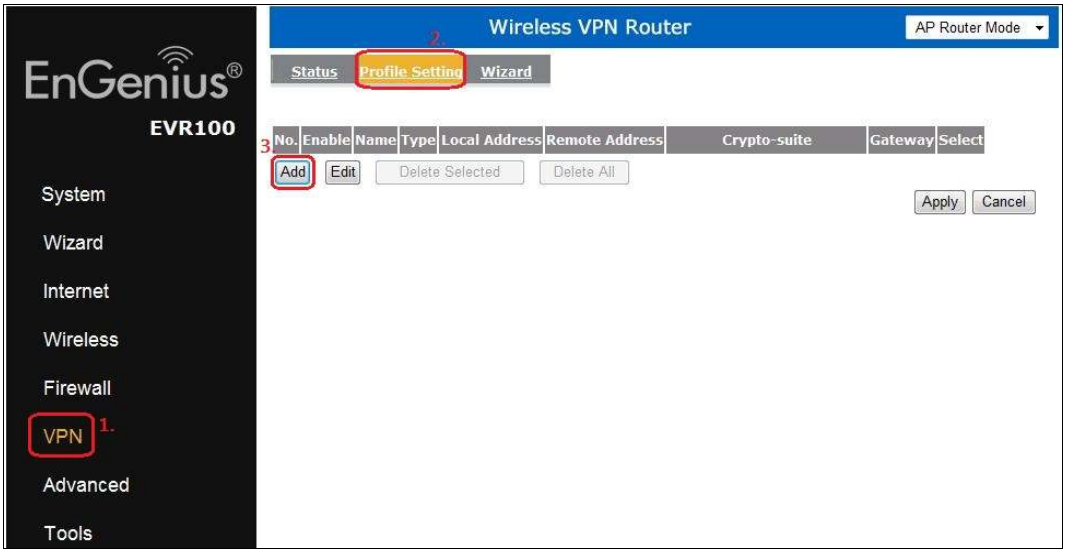
7. Create the **Shared key** for this Client-to-Site VPN tunnel, and then click **Next**.

Note: By default, the SA (Security Association) is **ESP-3DES-SHA1**. If desired, you can change it after using the Wizard to add the VPN profile.

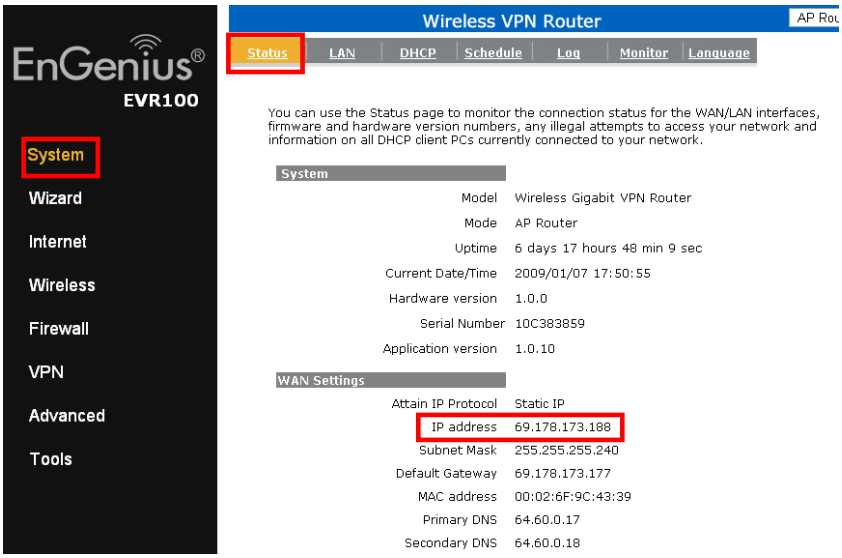
8. Enable the VPN policy, and then click **Apply** to save the Client-to-Site VPN profile.

3.2. EVR100 Manual VPN Profile Setting

1. In left-side of the menu, click **VPN**.
2. In the top menu, click **Profile Setting** to configure VPN Profile Setting.
3. Click **Add** to create a Client-to-Site VPN profile.

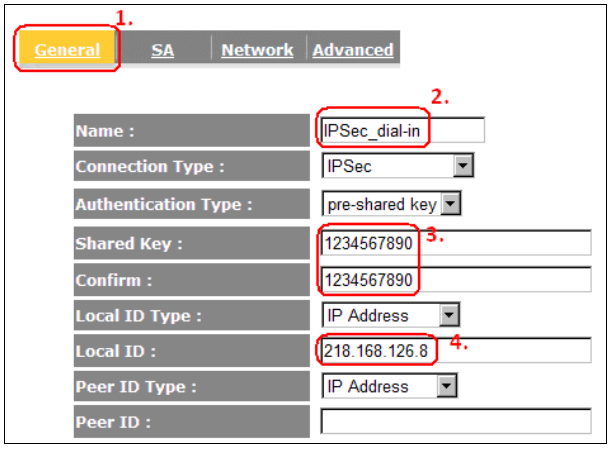


Note: You can find the EVR100 WAN IP settings under **System > Status**.



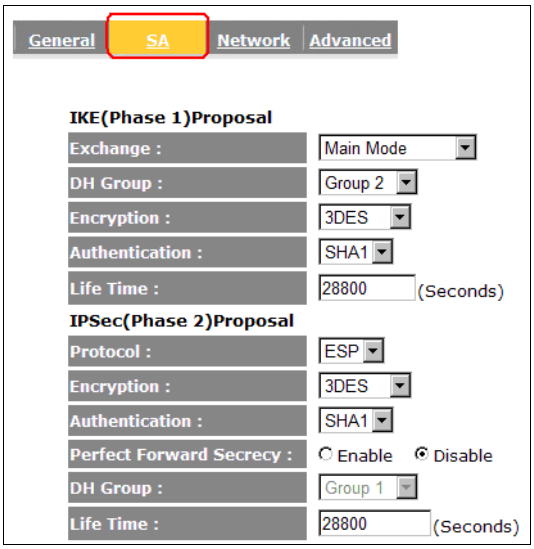
4. Complete the following fields in the **General** tab:

Name	Enter a name for this Client-to-Site VPN profile. This name is for reference purposes.
Connection Type	Click **IPsec**.
Shared Key	Create a shared key for the EVR100 VPN profile and **Confirm** the shared key.
Local ID	If you selected **IP Address** for **Local ID Type**, enter the WAN IP address of the EVR100. If you selected **Domain Name** for **Local ID Type**, enter the domain name of the EVR100. If you selected **E-Mail Address** for **Local ID Type**, enter an email address to identify the EVR100.
Peer ID Type	Leave this field blank.
Peer ID	Leave this field blank.



5. Select appropriate encryption and authentication algorithms for the IKE SA.

Exchange	Choices are **Main mode** and **Aggressive mode**. **Main mode** provides higher security at a slower speed than **Aggressive mode**. The default setting is **Main mode**. We recommend you accept this setting. Choose the setting that matches the local EVR100.
DH Group	Choices are **DH1: 768-bit random number** and **DH2: 1024-bit random number**.
Encryption	Choices are **3DES**, **AES128**, **AES192**, and **AES256**. The default setting is **3DES**.
Authentication	Choices are **MD5** and **SHA1**. SHA1 provides higher security at a slower speed than MD5. The default setting is **SHA1**.

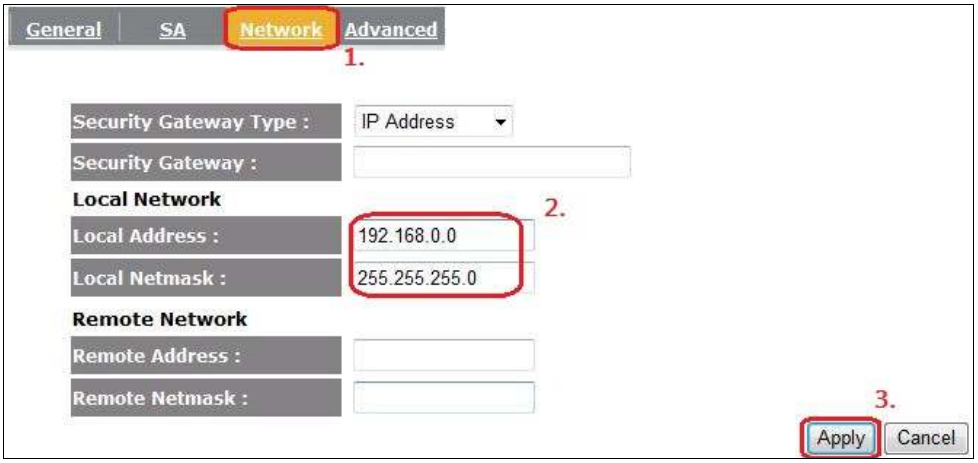


6. Go to **Network** tab and complete **Local Network** only. Leave **Security Gateway Type**, **Security Gateway**, and **Remote Network** blank (these settings are for IPSec Site-to-Site VPN settings).

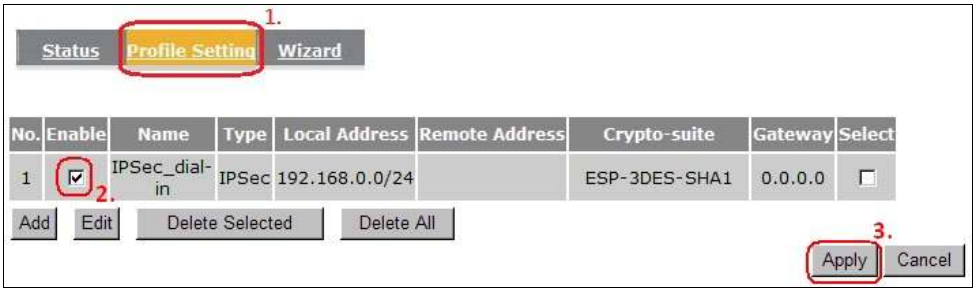
Local Address Enter an IP address on the same subnet of LAN IP address of the computer connected behind EVR100. In Figure 2, the LAN IP address of the EVR100 is 192.168.0.100. To be on the same subnet, the IP address must have 192.168.0 as its first three octets (for example, 192.168.0.*x*).

Local Netmask Type **255.255.255.0**.

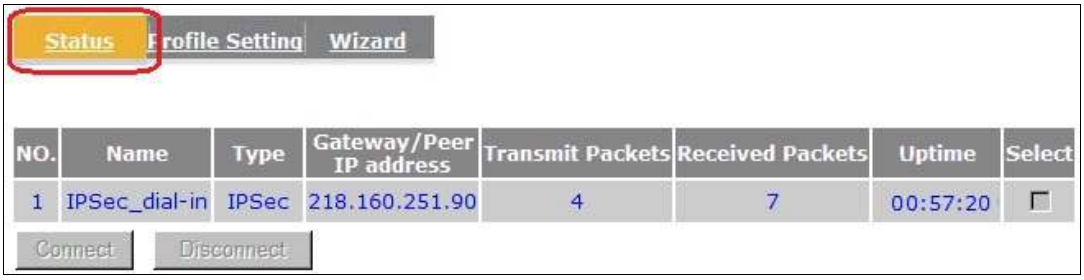
Click **Apply** to save your settings.



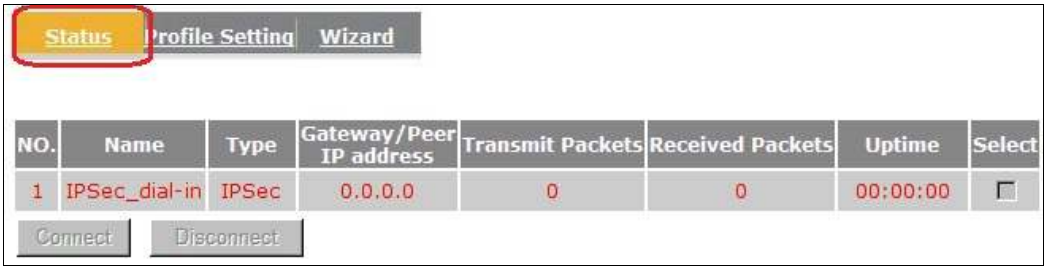
7. Check **Enable**, and then click **Apply** in the **Profile Setting** field to activate IPSec Client-to-site VPN tunnel for the EVR100.



8. Go to the **Status** tab to see the VPN tunnel status. **Blue** profiles are configured properly and details are shown for **Transmit Packets**, **Received Packets**, and **Uptime**. **Red** profiles indicate profiles have setup problems.



Example of VPN Tunnel Parameters Configured Successfully

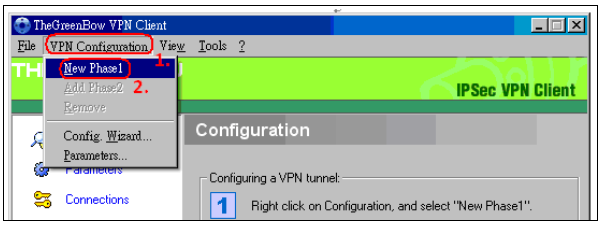


Example of VPN Tunnel Parameters Configured Unsuccessfully

3.3. Configuring TheGreenBow VPN Client

The following procedure describes how to configure TheGreenBow third-party VPN client. If you will use a different VPN client, you can skip this section.

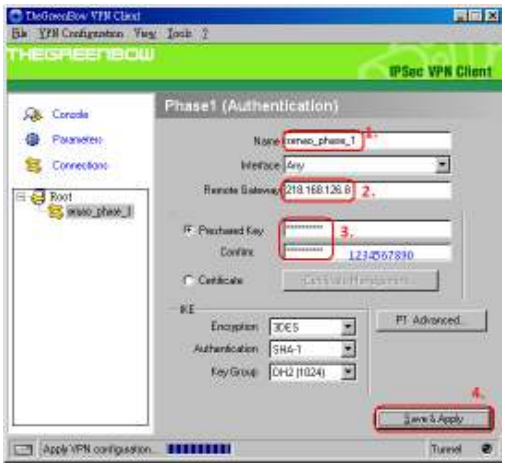
1. Click **VPN Configuration** to add a New Phase1.



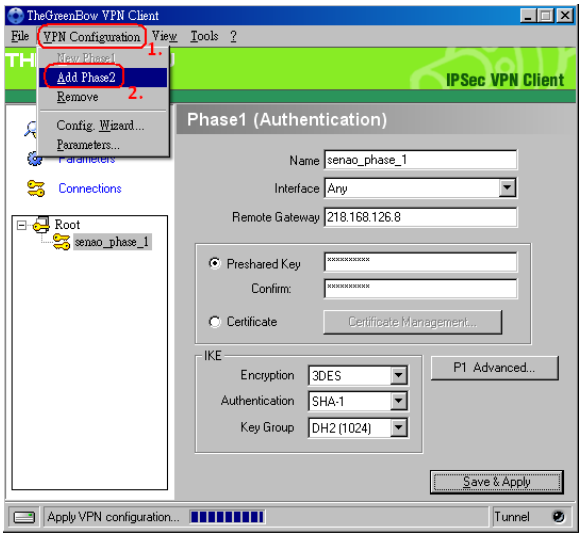
2. Configure the following settings:

Name	Enter a name for the EVR100 VPN tunnel profile. This name is for reference purposes.
Interface	Your computer's IP address appears in this field.
Remote Gateway	Enter the WAN IP of the targeted EVR100.
Pre-shared key	Enter the pre-share key of the targeted EVR100.
Encryption	Select the encryption used by the targeted EVR100.
Authentication	Select the authentication used by the targeted EVR100.
Key Group	Select the DH Group key of the targeted EVR100

Click **Save & Apply**.



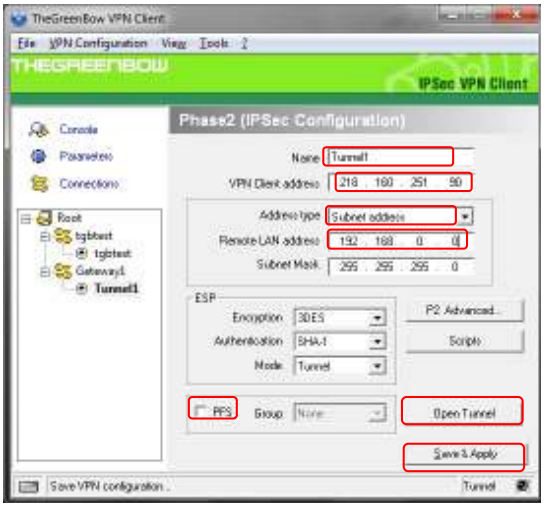
3. On the **VPN Configuration** menu, click **Add Phase2**.



4. Complete the following settings:

Name	Enter a name for the VPN client profile. This name is for reference purposes.
VPN Client Address	Your computer's IP address appears in this field.
Address Type	Select **Subnet address**.
Remote LAN Address/ Subnet Mask	Enter an IP address and subnet mask which is the same subnet as the LAN subnet of the EVR100. In Figure , this LAN subnet is 192.168.0.0/255.255.255.0.
PFS	Uncheck **Perfect Forward Secrecy (PFS)** to disable it
Authentication	Select the authentication used by the targeted EVR100.
Key Group	Select the DH Group key of the targeted EVR100

5. Click **Save & Apply**.
6. Click **Open Tunnel** to enable this tunnel.



The IPSec VPN tunnel connects successfully, as shown in the following figure.

4. L2TP over IPSec

Layer 2 Tunneling Protocol (L2TP) over IPSec is a tunneling protocol where the L2TP tunnel runs on top of an IPSec transport-mode connection. You can use L2TP over IPSec VPNs for routers at remote sites and create a demand-dial connection by connecting with Microsoft Windows' native L2TP Client or Apple Mac L2TP client.

This chapter shows how to set up a L2TP-over-IPSec VPN tunnel by connecting an EVR100 with Microsoft Windows 7 and Vista and Apple Mac L2TP clients.

Note: The EVR100 supports only one L2TP over IPSec VPN tunnel.

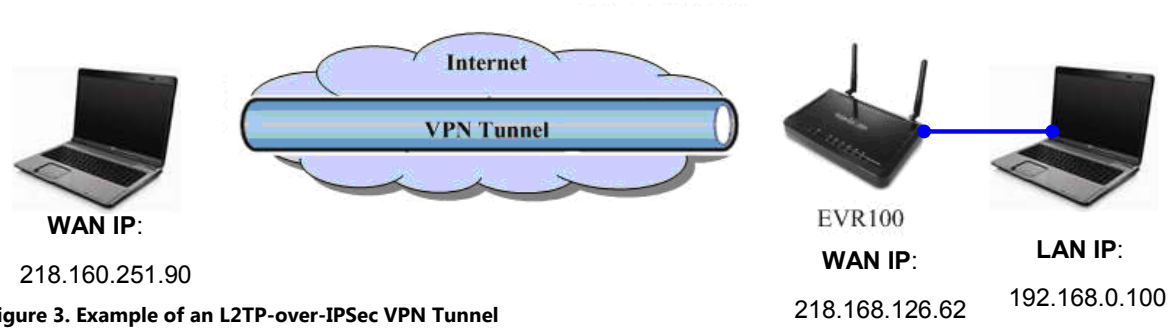
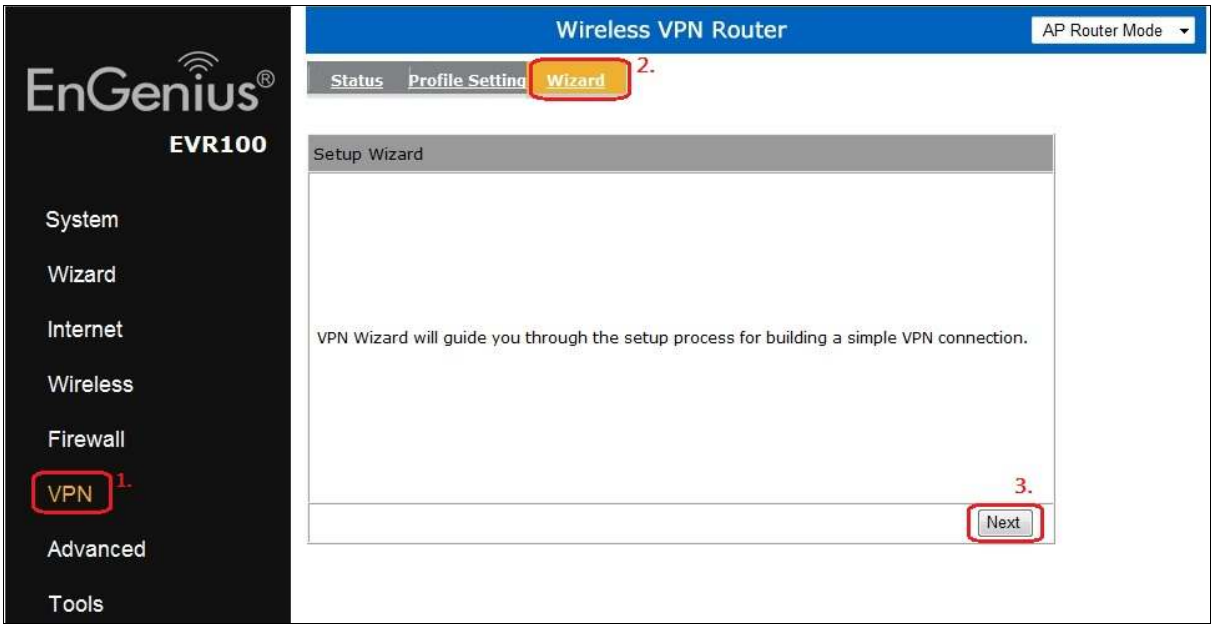


Figure 3. Example of an L2TP-over-IPSec VPN Tunnel

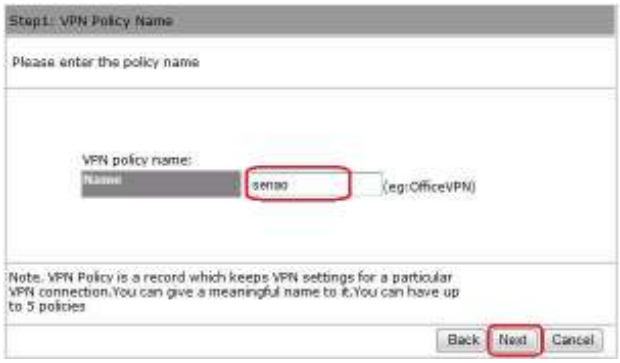
4.1. Using the Wizard to Configure the EVR100

1. In the left-side of the menu, click **VPN**.
2. In the top menu, click **Wizard** to add a VPN profile.
3. Click **Next** to create an L2TP over IPSec VPN profile.



4. In the **Name** field, enter a name for the L2TP over IPSec VPN tunnel. This name is for reference purposes.

5. Click **Next**.

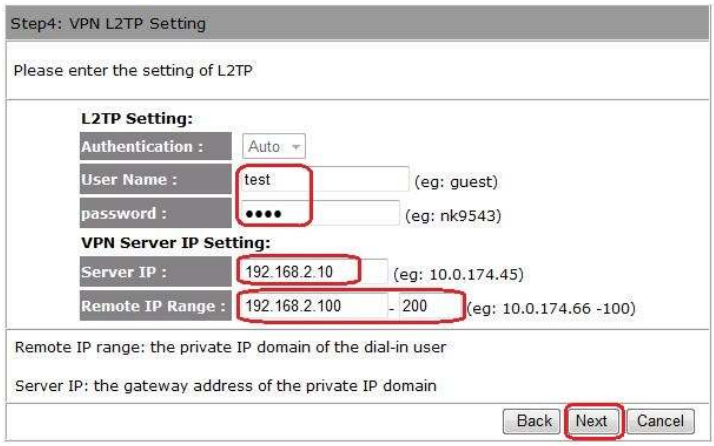


6. Click **L2TP over IPSec**, and then click **Next**.

7. Complete the following fields:

Use Name	Enter a name for the L2TP over IPSec VPN tunnel.
Password	Enter a password for the L2TP over IPSec VPN tunnel.
Server IP	Enter any IP address on a different subnet than the LAN IP address of the computer connected behind the EVR100. In Figure 3, the EVR100 LAN IP address is 192.168.0.100. In this example, you can select any IP address other than 192.168.0.*x*).
Remote IP Range	Enter an IP address range that is on the same subnet as the **Server IP** address you entered in the **Server IP** field, but the range should not include Server IP. For example, if you specified a Server IP address of 192.168.2.10, you can define a **Remote IP Range** of 192.168.2. 100 – 200.

Click **Next**.



8. In the **Shared Key** field, enter the shared key for EVR100 VPN tunnel. Click **Next**.

9. Enable the VPN policy, and then click **Apply** to save the VPN profile.

4.2. Configuring the EVR100 Manually

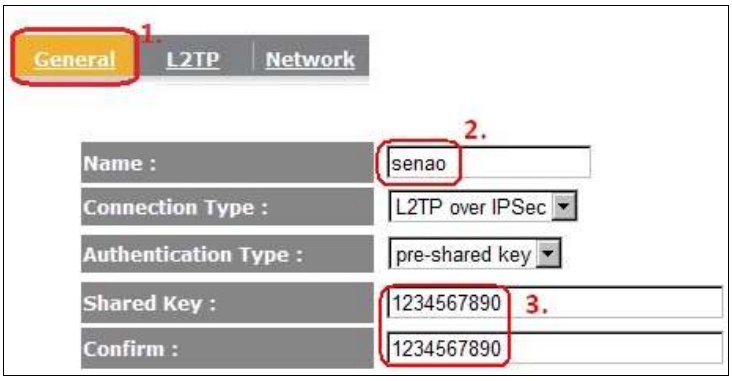
1. In left-side of the menu, click **VPN**.
2. In the top menu, click **Profile Setting** to configure VPN.
3. Click **Add** to create a L2TP over IPSec VPN profile.

4. In the **General** tab, complete the following settings:

Name Enter a name for the L2TP-over-IPSec VPN tunnel.

Connection Type Click **L2TP over IPSec**.

Shared Key Create a shared key for the EVR100 VPN profile and **Confirm** the shared key.

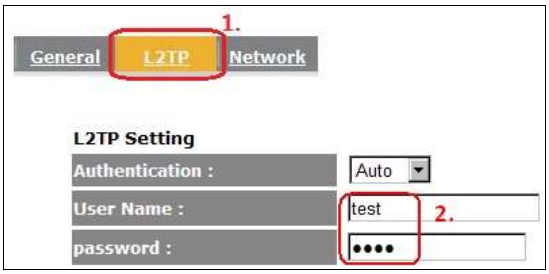


5. Go to the **L2TP** tab and configure the following settings:

Authentication Choices are **CHAP**, **PAP**, and **Auto**. We recommend you use **Auto**.

User Name Enter a user name for the L2TP-over-IPSec VPN tunnel.

Password Enter a password for the L2TP-over-IPSec VPN tunnel.

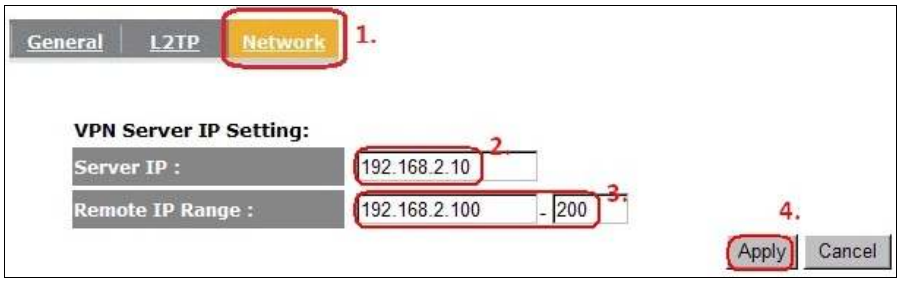


6. Go to the **Network** tab and configure the following settings:

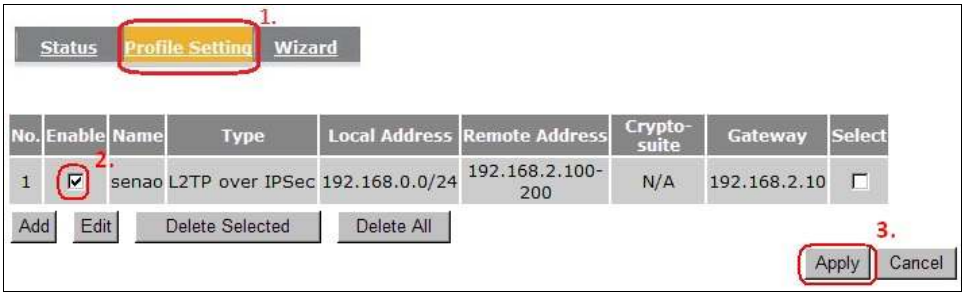
Server IP Enter an IP address on a different subnet than the EVR100 LAN IP address. In the example in Figure 3, the EVR100 LAN IP address is 192.168.0.100. In this example, you can select any IP address other than 192.168.0.x.

Remote IP Range Enter an IP address range that is on the same subnet as the Server IP address you entered in the **Server IP** field. For example, if you specified a Server IP address of 192.168.2.10, you can define a **Remote IP Range** of 192.168.2. 100 – 200.

Click **Apply** to save the whole setting.

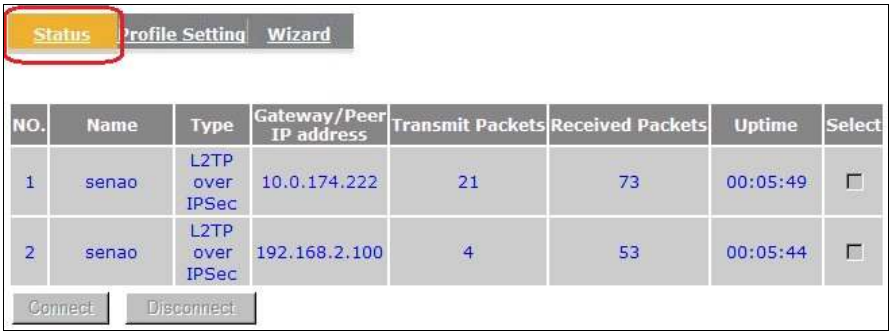


7. Check **Enable**, and then click **Apply** in the **Profile Setting** field to activate the IPSec-over-IPSec VPN tunnel.

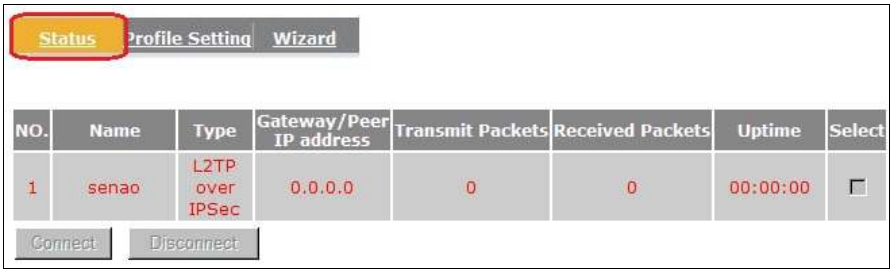


8. Go to the **Status** tab to see the VPN tunnel status. **Blue** profiles are configured properly and details are shown for **Transmit Packets**, **Received Packets**, and **Uptime**. **Red** profiles indicate profiles have setup problems.

Note. If your connection protocol uses L2TP over IPSec dial-in, you cannot disconnect manually through the EVR100.



Example of VPN Tunnel Parameters Configured Successfully

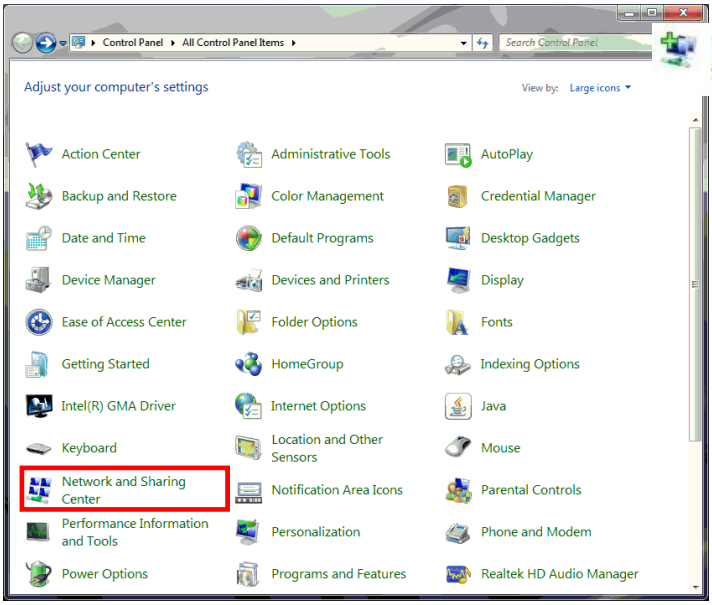


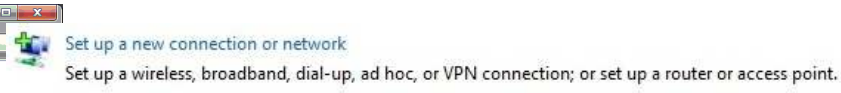
Example of VPN Tunnel Parameters Configured Unsuccessfully

4.3. Configuring a Microsoft Windows 7 VPN Client

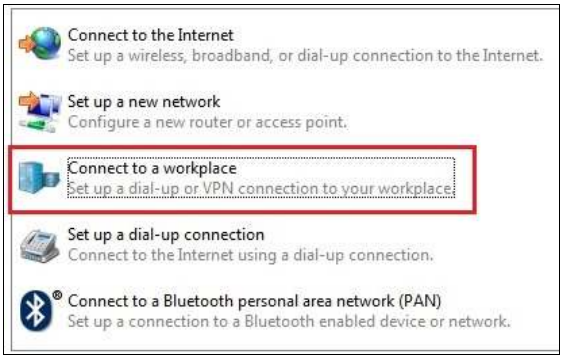
1. Click the **Start** button and open the **Control Panel**.

2. Under **Network and Sharing Center**, select **Set up a new connection or network**.

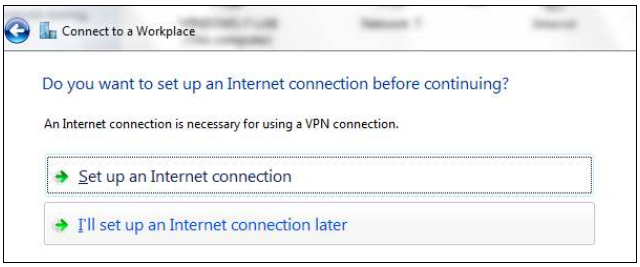




3. Click **Connect to a workplace**, and then click **Use my Internet connection (VPN)**



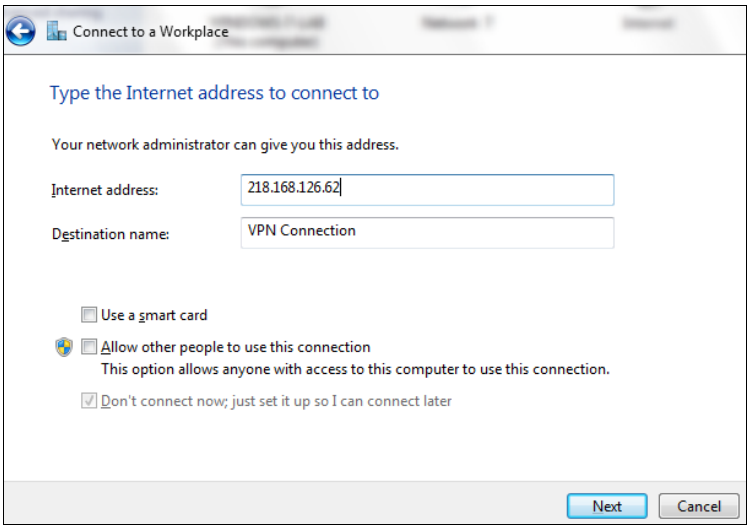
4. We recommend you select **I'll set up an Internet connection later**.



5. Complete the following fields:

Internet Address	Enter the EVR100 WAN IP address.
Destination Name	Enter a name for the VPN client.

6. Click **Next**.



7. Complete the following fields:

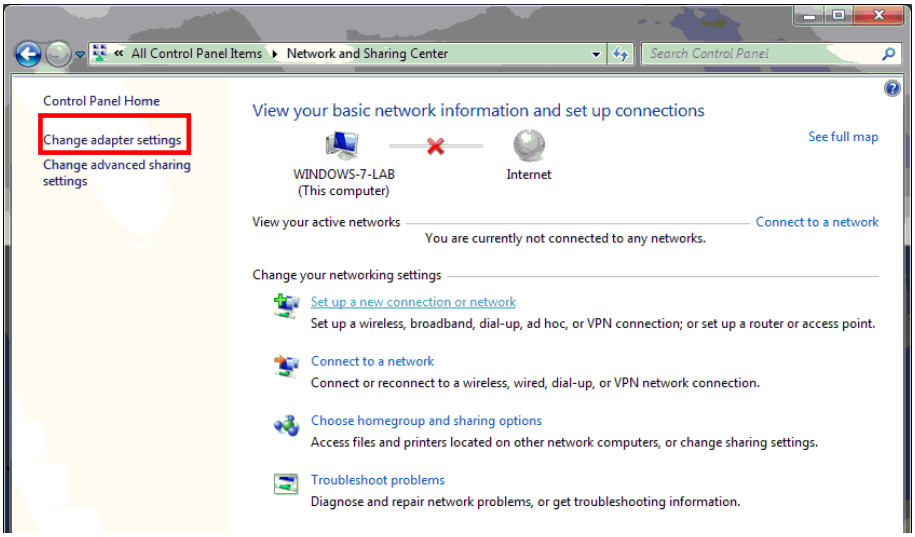
User Name Enter the user name used to log onto the L2TP over IPSec VPN tunnel.

Password Enter the password used to log onto the L2TP over IPSec VPN tunnel.

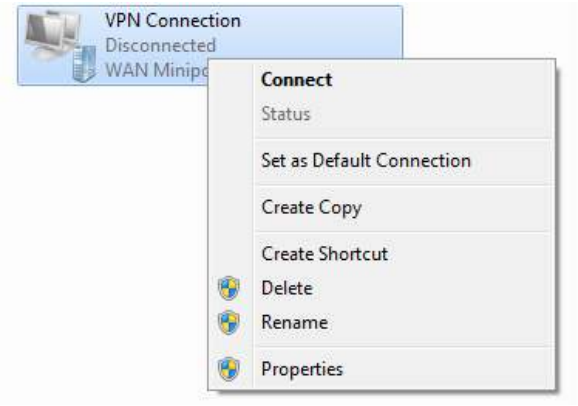
Click **Create**.

8. When the following screen appears, click the **Close** button to close the VPN connection setting.

9. Select **Change adapter settings** on the left side of the screen



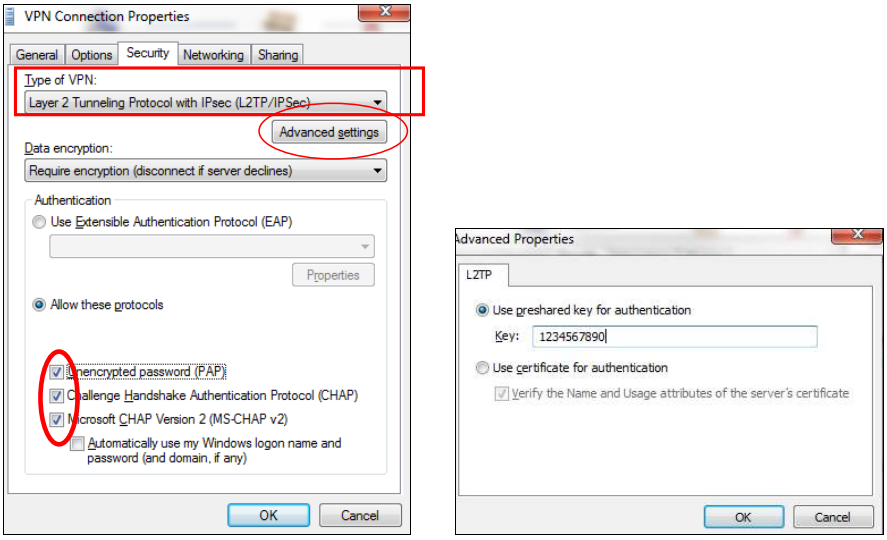
10. Select VPN Connection you just set, right-click VPN Connection, and select **Properties**.



11. Go to the **Security** tab and configure the following settings:

- Under **Type of VPN**, click **Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)**.
- Check **Unencrypted password (PAP)**.
- Check **Challenge Handshake Authentication Protocol (CHAP)**.
- Click **Advanced settings**.

12. In the **Advanced Properties** window, click **Use preshared key for authentication** and enter the preshared key of the target EVR100. Then click **OK**.



13. Go to **Network and Sharing Center** on the bottom-right of the window. Under **VPN Connection**, click **Connect**.

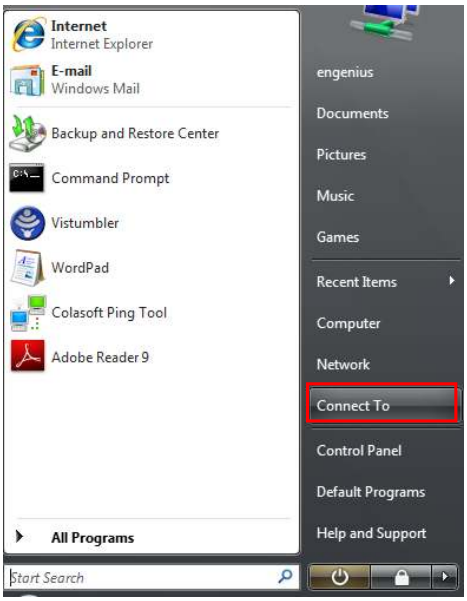
14. Double-click the **VPN Connection**, and then click the **Connect** button.

15. Verify that you can see the VPN Connection has been established. This concludes the procedure for configuring a Microsoft Windows 7 VPN client.

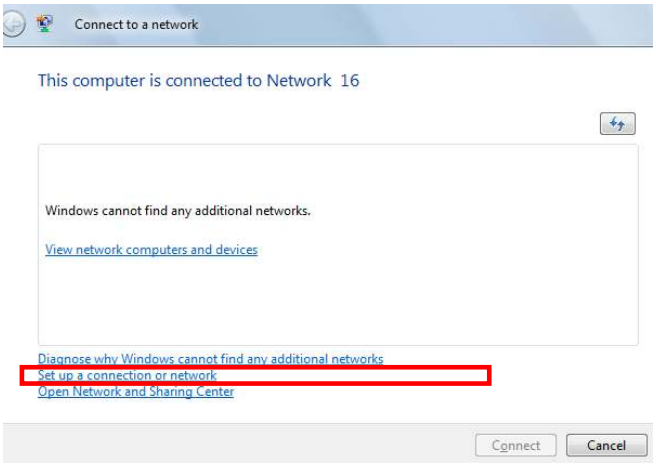
4.4. Configuring a Microsoft Windows Vista VPN Client

The following procedure describes how to configure a Microsoft Windows Vista VPN client.

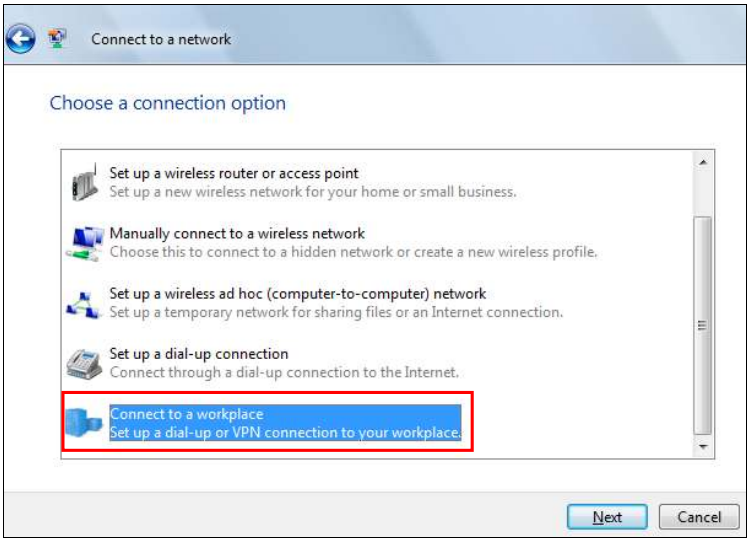
1. Click **Connect To**.



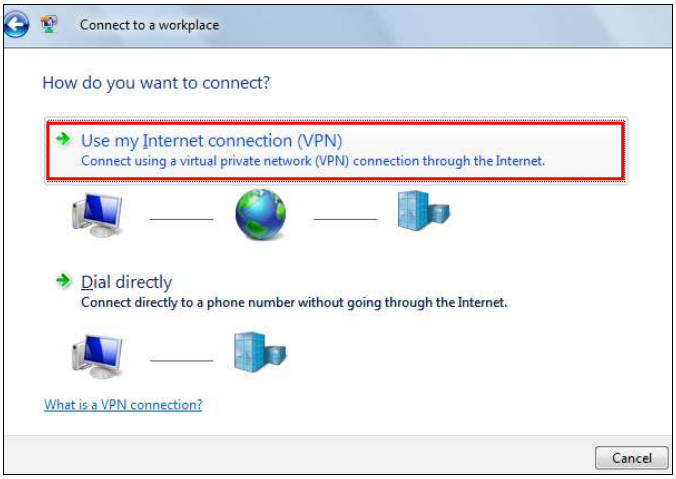
2. Click **Set up a connection or network**.



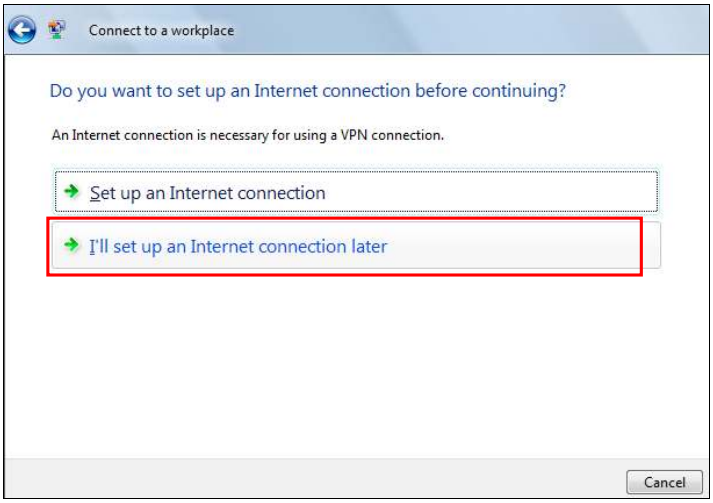
3. Click **Connect to a workplace** to set up a dial-up or VPN connection to your workplace.



4. Click **Use my Internet connection (VPN)**.



5. When the next screen appears select **I'll set up an Internet connection later**.

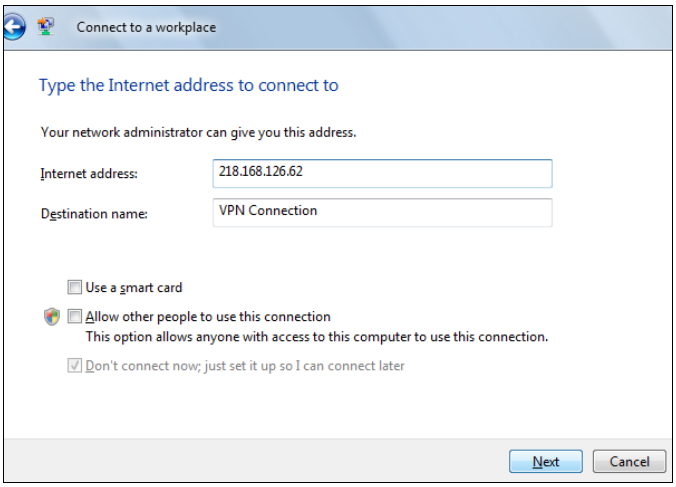


6. Complete the following fields:

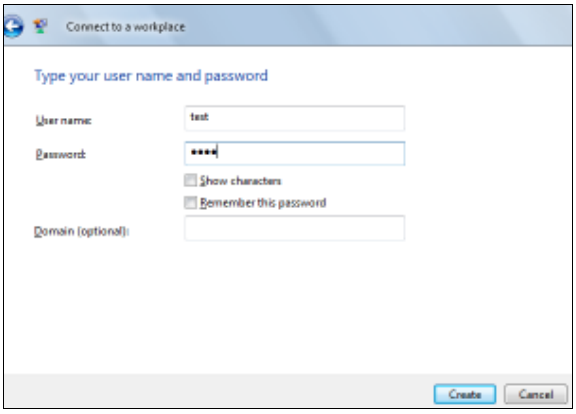
Internet address Enter the WAN IP address of the targeted EVR100.

Destination name Enter a name for the VPN connection.

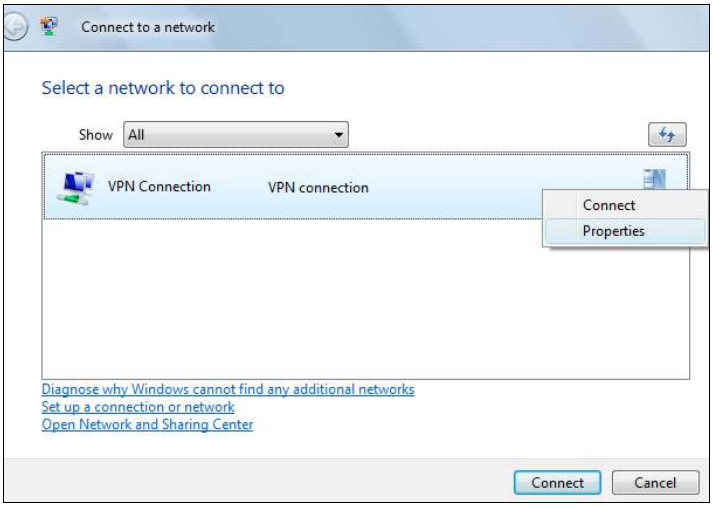
Click **Next**.



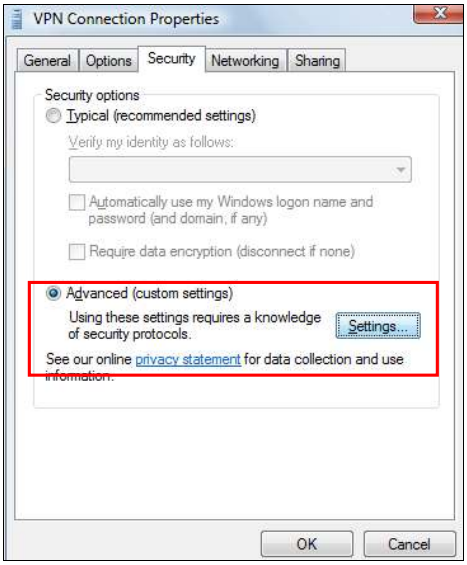
7. When the next screen appears, enter the **User name** and **Password** of the target EVR100. Then click **Create**.



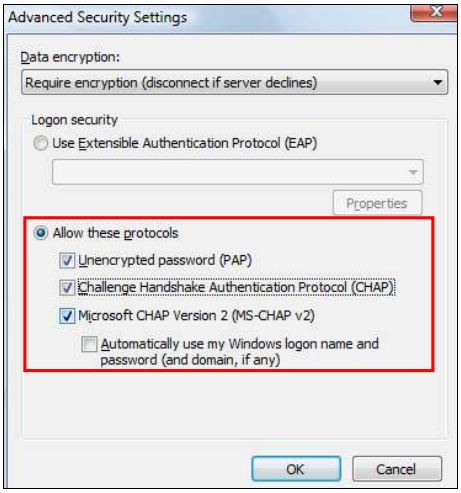
8. Return to **Connect to**. Then right-click **VPN Connection** and select **Properties**.



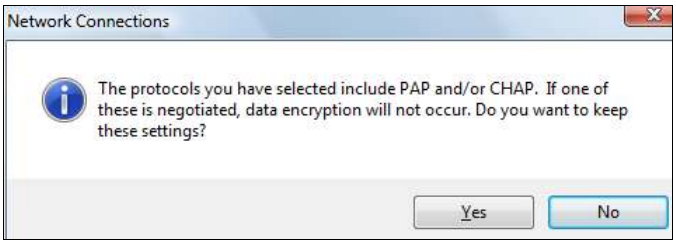
9. Click the **Security** tab, click **Advanced (custom settings)**, and then click **Settings**.



10. Check **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**, and then click **OK**.



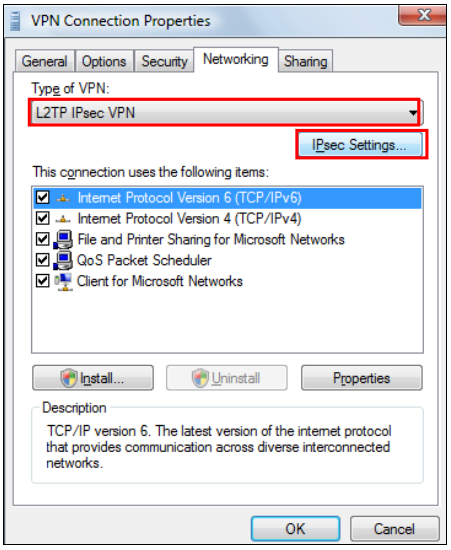
11. When the following window appears, click **Yes**.



12. Go to the **Networking** tab.

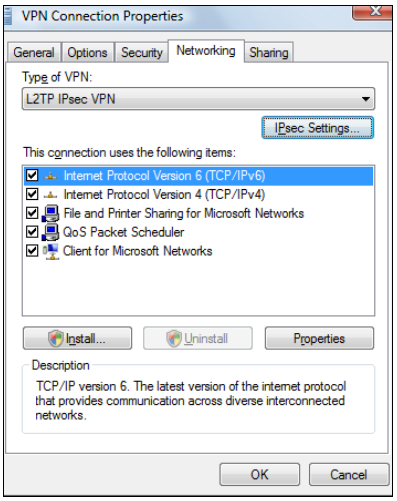
13. Under **Type of VPN**, click **L2TP IPsec VPN**.

14. Click **IPsec Settings**.

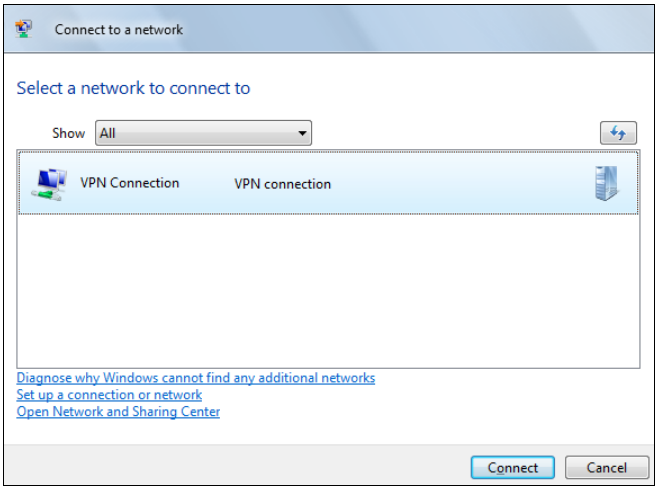


15. In the IPSec Settings window, click **User preshared key for authentication** and enter the preshared key of the target EVR100. Then click **OK**.

16. Click **OK**.



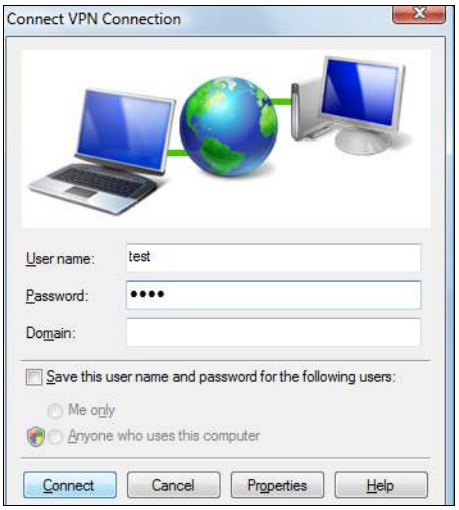
17. Return to **Connect to** and click **VPN Connection** followed by **Connect**.



18. Complete the following fields:

User name	Enter the user name of the target EVR100.
Password	Enter the password of the target EVR100.

19. Click **Connect**. This concludes the procedure for configuring a Microsoft Windows Vista VPN client.

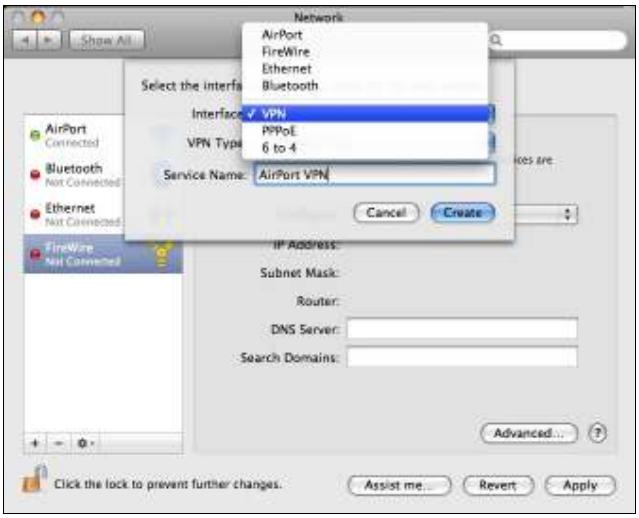


4.5. Configuring an Apple Mac VPN Client

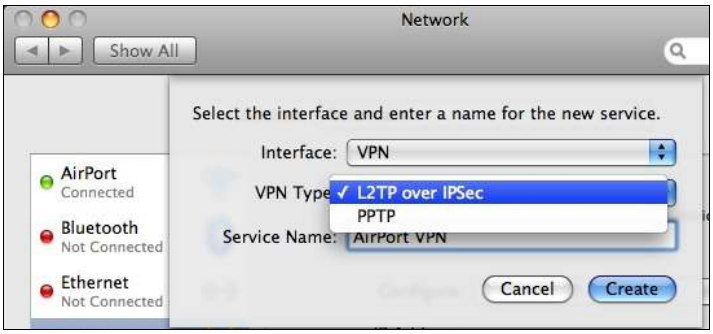
The following procedure describes how to configure an Apple Mac VPN client.

1. Go to **System Preferences**, and then click **Network**.

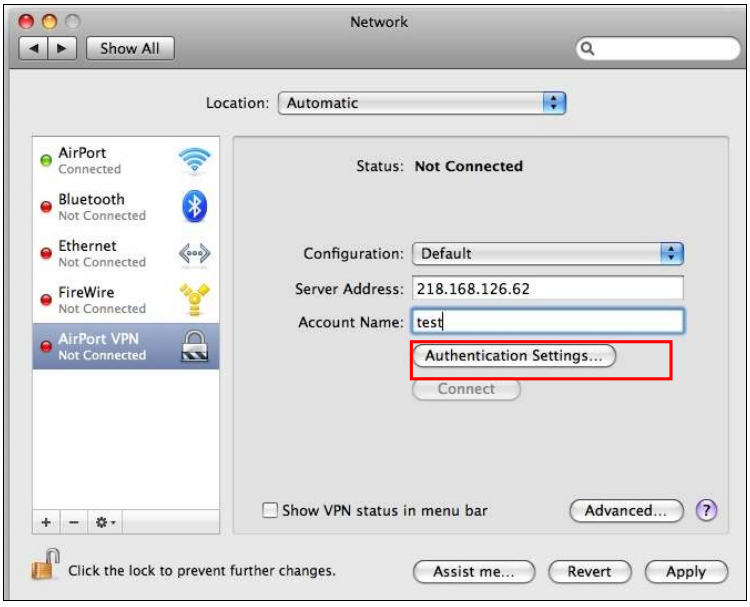
2. Click **+** to create a VPN tunnel. Select **VPN**.



3. For **VPN Type**, click **L2TP over IPSec**.



4. For **Server Address**, enter the WAN IP address of the targeted EVR100
5. For **Account Name**, enter the user name of the targeted EVR100.
6. Click **Authentication Settings**.



7. For **User Authentication: Password**, enter the password of the target EVR100.
8. For **Machine Authentication**: **Shared Secret**, enter the shared key of the target EVR100
9. Click **OK**.

10. Click **Apply** to connect to the VPN.