
Configuring VPNs in the EN-2000

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses configuration of a VPN connection.

Note: VPN configuration requires collection of some information before the actual configuration can be performed. It is important to plan your virtual private network. Before configuring the EN-2000's IPsec VPN tunnels, study the material discussed in [Virtual Private Networks](#) and confer with your network administrator.

See the following sections:

- [Configuring an EN-2000 as a VPN Tunnel Initiator](#)
- [Configuring an EN-2000 as a VPN Tunnel Responder](#)

Note: In the VPN tunnel configuration screens, "left" indicates "local" (that is, it indicates the EN-2000 router) and "right" indicates "remote" (the device at the other end of the connection).

For information about VPNs, see the document [Virtual Private Networks](#). For additional (required) VPN processes, see the following documents:

- [Configuring an EN-2000 Firewall](#)
- [Starting and Tracking VPNs in the EN-2000](#)

5.1 Configuring an EN-2000 as a VPN Tunnel Initiator

- 1 Log into the EN-2000. (For details, see [Logging In](#), on page 2 of the document [Configuring General Settings for the EN-4000](#).)
- 2 On the EN-2000 management system, select the **Network** tab. Then select the **VPN** tab. If necessary, select the **General Settings** tab.
 - ❖ The IPsec VPN Tunnel Table for a VPN Tunnel Initiator is displayed ([Figure 5-1](#)).

Figure 5-1. IPsec VPN Tunnel Table for a VPN Tunnel Initiator

The screenshot shows the 'IPsec -- Tunnels' configuration page. At the top, there's a navigation bar with 'Status', 'System', 'Network', 'Statistics', and 'Logout'. Below that, a sub-menu includes 'Interfaces', 'Firewall', 'Static Routes', 'Load Sharing/Failover', 'QoS', 'Diagnostics', 'Hostnames', 'DHCP and DNS', 'VPN', 'VRRP', and 'Serial'. The main content area is titled 'IPsec -- Tunnels' and includes a brief description of IPsec. Below this is a table of existing tunnels:

Tunnel Name	Left Subnet	Left	Right	Right Subnet	SLE	Tunnel Up	Tunnel Down
OSAT1	192.168.101.0/24	%any	71.16.53.45	0.0.0.0/0	yes		

Below the table are buttons for 'Add IPSEC TUNNEL', 'Edit', and 'Delete'. Further down, there are sections for 'IPsec Defaults' (IKE Lifetime: 72h, KeyLife: 24h, Aggressive: yes, Responder: no) and 'IPsec Actions' (IPsec Start, IPsec Stop, IPsec Restart, Save & Apply).

- 3 On that screen, select the box to **Enable IPsec for this unit.**
- 4 Under the heading **IPsec Tunnels**, do one of the following:
 - a Select the **Edit** button for an existing IPsec VPN tunnel. (The **Edit** button is near the far right of the tunnel's row.)
 - b Select the **Add IPsec Tunnel** button. (The button is below the list of **Tunnel Names**.)
 - ❖ In either case, the IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator is displayed ([Figure 5-2](#)).

Figure 5-2. IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator

The screenshot shows the 'IPsec - Tunnels - (Unnamed Tunnel)' configuration screen. At the top, there's a navigation bar with 'Status', 'System', 'Network', 'Logout', and 'Quickstart'. Below that, a sub-menu includes 'Interfaces', 'Hostnames', 'Static Routes', 'Failover', 'Firewall', 'Diagnostics', 'QoS', 'VPN', and 'VRRP'. The main content area is titled 'IPsec - Tunnels - (Unnamed Tunnel)' and includes a brief description of IPsec. Below this is a form for configuring the tunnel:

Tunnel Name:

Left Subnet: Local Private Subnet(s)
To Reduce to 1 entry, use RESET->SAVE_APPLY and enter new value.

Left: IP of local tunnel endpoint (typically WAN IP, %any for dynamic WANs)

Left ID: Local User Name

Left Firewall: Is the local firewall on or off?

Right: IP of remote tunnel endpoint (typically WAN IP, %any for dynamic WANs)

Right Subnet: Remote Private Subnet(s)
To Reduce to 1 entry, use RESET->SAVE_APPLY and enter new value.

Remote ID: Remote User Name

IPsec startup operations:

Pre-Shared Key:

Buttons:

- 5 Configure the fields on the IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator. Get all values from your network administrator.

Note the following required values for the VPN tunnel initiator:

- Set the **Left** IP address to **%any**.
- Set the **Left Firewall** to **No** (off).
- Set **IPsec Startup Operations** to **Start**.
- Type the **Preshared Key**.

Note: Both sides of the VPN tunnel (initiator and responder) must use the same pre-shared key. Get the key from your network administrator.

The following are sample values.

- **Tunnel Name:** Tunnel_01
 - **Left Subnet:** *a.b.c.0/24* (where *a.b.c* indicates the local private network).
Note: 24 is the IP prefix; its maximum value is 32.
 - **Left ID:** [*a character string*] (representing the local EN-2000)
Note: The VPN tunnel initiator's Left ID must match the VPN tunnel responder's Right ID. In like manner, the initiator's Right ID must match the responder's Left ID.
 - **Right:** *i.j.k.l* (where *i.j.k.l* is the remote router's public IP address)
 - **Right Subnet:** *m.n.p.0/24* (where *m.n.p* indicates the remote private network)
 - **Right [Remote] ID:** [*a character string*] (representing the remote EN-2000)
- 6 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The configuration is saved, and the IPsec VPN Tunnel Table for a VPN Tunnel Initiator is redisplayed (recall [Figure 5-1](#)).
 - 7 On the IPsec VPN Tunnel Table for a VPN Tunnel Initiator, under the heading **IPsec Defaults**, select the **Edit** button (at the far right of the section).
 - ❖ The IPsec Defaults Configuration Screen for a VPN Tunnel Initiator is displayed ([Figure 5-3](#)).

Figure 5-3. IPsec Defaults Configuration Screen for a VPN Tunnel Initiator

The screenshot displays the 'IPsec Defaults' configuration screen. The interface includes a navigation bar at the top with tabs for 'Status', 'System', 'Network', 'Logout', and 'Quickstart'. Below this, there are sub-tabs for 'Interfaces', 'Hostnames', 'Static Routes', 'Failover', 'Firewall', 'Diagnostics', 'QoS', 'VPN', and 'VRRP'. The main content area is titled 'IPsec Defaults' and contains a form for configuring IPsec defaults. The form is organized into sections: 'IPsec Default Configuration' and 'Pass Conn'.

Field	Value
Ike Lifetime	72h
Key Life	24h
ReKey Margin	1h
Keying Tries	2
Key Exchange	Ikev2
Auth	secret
Aggressive Mode	YES
IKE Encryption Protocol	AES256
IKE Authentication Protocol	MD5
IKE DH Group	Group2
ESP Encryption Protocol	AES256
ESP Authentication Protocol	MD5
ESP DH Group	Group2
DPD Action	Restart
DPD Delay	20s
DPD timeout	120s
RE-KEY	NO
RE-AUTH	NO
Responder	NO
Pass Conn type	Pass
Pass Conn Left Subnet	192.168.1.0/24
Pass Conn Right Subnet	192.168.1.0/24
Pass Conn Auth	Never
Pass Conn Startup operations	ROUTE

At the bottom of the screen, there are buttons for 'Back to Overview', 'Reset', 'Save', and 'Save & Apply'.

8 Configure the fields on the IPsec Defaults Configuration Screen for a VPN Tunnel Initiator. Get all values from your network administrator.

Note the following required values for the VPN tunnel initiator:

- Set **Responder** to **No**. (This EN-2000 is the tunnel initiator.)
- Set **Pass Conn Type** to **Pass** (passthrough).
Note: When you select **Pass**, additional fields are displayed.
- Set **Pass Conn Auth** to **Never**.
- Set **Pass Conn Startup Operations** to **Start**.

The following are sample values.

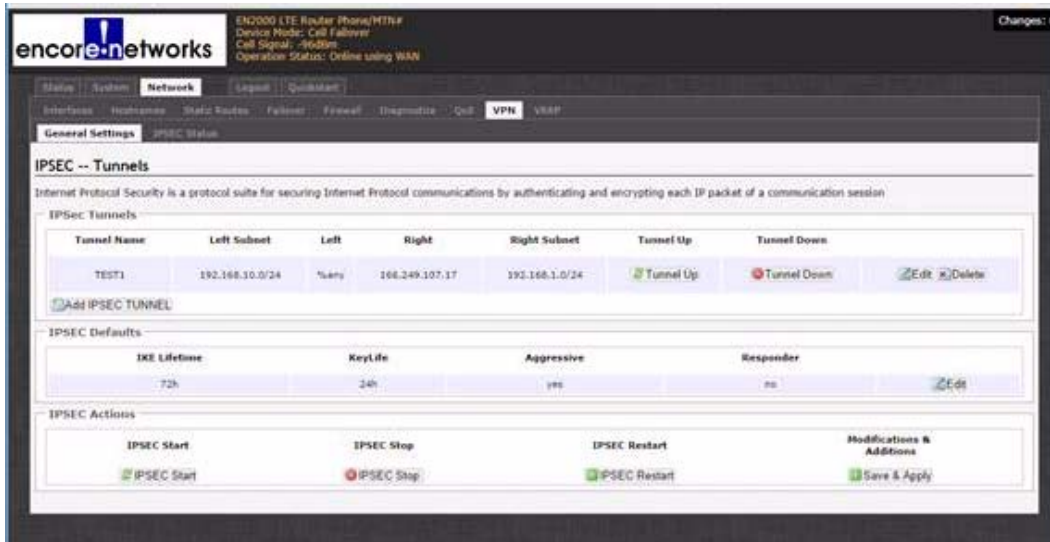
- Phase 1:
 - ◆ **IKE Lifetime:** 72h [72 hours]
 - ◆ **Key Life:** 8h [8 hours]
 - ◆ **ReKey Margin:** 0h [0 hours; thus no kilobytes rekeying]
 - ◆ **Keying Tries:** 2 [the default value]
 - ◆ **Key Exchange:** IKEv1
 - ◆ **Auth** [Authentication]: secret
 - ◆ **Aggressive Mode:** No ("No" indicates use of main mode.)
 - ◆ **IKE Encryption Protocol:** 3DES

- ◆ **IKE Authentication Protocol:** SHA1
- ◆ **IKE DH [Diffie–Hellman] Group:** Group2
- Phase 2 (uses perfect forward secrecy):
 - ◆ **ESP Encryption Protocol:** 3DES
 - ◆ **ESP Authentication Protocol:** SHA1
 - ◆ **ESP DH [Diffie–Hellman] Group:** Group2
 - ◆ **DPD [Dead Peer Detection] Action:** Restart
 - ◆ **DPD [Dead Peer Detection] Delay:** 20s [seconds]
 - ◆ **DPD [Dead Peer Detection] Timeout:** 120s [seconds]
 - ◆ **Re-Key:** No
 - ◆ **Re-Auth:** No
 - ◆ **Pass Conn Left Subnet:** The local LAN subnet
 - ◆ **Pass Conn Right Subnet:** The local LAN subnet
- Note:** The Pass Conn Left Subnet and the Pass Conn Right Subnet must be identical.
- 9 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The configuration is saved, and the IPsec VPN Tunnel Table for a VPN Tunnel Initiator is redisplayed (recall [Figure 5-1](#)).
- 10 On the IPsec VPN Tunnel Table for a VPN Tunnel Initiator, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The EN-2000 has been configured as an IPsec VPN tunnel initiator.

5.2 Configuring an EN-2000 as a VPN Tunnel Responder

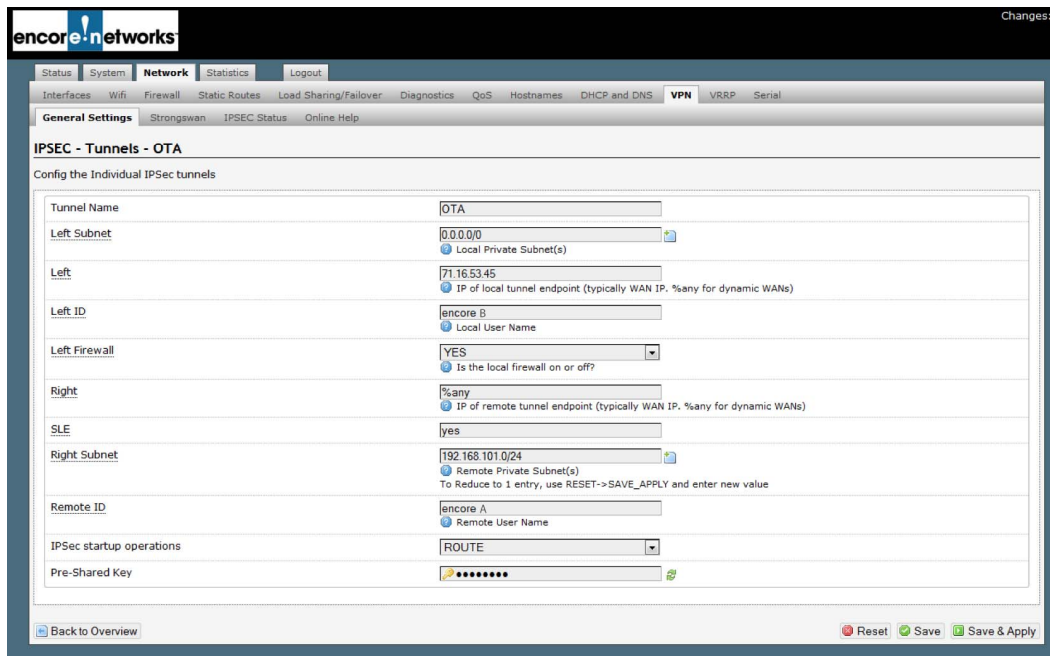
- 1 Log into the EN-2000. (For details, see [Logging In](#), on page 2 of the document [Configuring General Settings for the EN-4000](#).)
- 2 On the EN-2000 management system, select the **Network** tab. Then select the **VPN** tab. If necessary, select the **General Settings** tab.
 - ❖ The IPsec VPN Tunnel Table for a VPN Tunnel Responder is displayed ([Figure 5-4](#)).

Figure 5-4. IPsec VPN Tunnel Table for a VPN Tunnel Responder



- 3 On that screen, select the box to **Enable IPsec for this unit.**
- 4 Under the heading **IPsec Tunnels**, do one of the following:
 - a Select the **Edit** button for an existing IPsec VPN tunnel. (The **Edit** button is near the far right of the tunnel's row.)
 - b Select the **Add IPsec Tunnel** button. (The button is below the list of **Tunnel Names**.)
 - ❖ In either case, the IPsec Tunnel Configuration Screen for a VPN Tunnel Responder is displayed (Figure 5-5).

Figure 5-5. IPsec Tunnel Configuration Screen for a VPN Tunnel Responder



- 5 Configure the fields on the IPsec Tunnel Configuration Screen for a VPN Tunnel Responder. Get all values from your network administrator.

Note the following required values for the VPN tunnel responder:

- Set the **Left Subnet** to **0.0.0.0**.
- Set the **Left IP** address to this EN-2000's WAN IP address.
Note: The VPN tunnel responder's WAN interface must use a static IP address so that it is accessible to the initiator.
- Set the **Left Firewall** to **Yes** (on).
- Set the **Right IP** address to **%any**.
- Set the **Right Subnet** to the subnet of the initiator EN-2000.
- Set **IPsec Startup Operations** to **Route**.
- Type the **Preshared Key**.

Note: Both sides of the VPN tunnel (initiator and responder) must use the same pre-shared key. Get the key from your network administrator.

The following are sample values.

- **Tunnel Name:** Tunnel_01
 - **Left ID:** [*a character string*] (representing the local EN-2000)
Note: The VPN tunnel initiator's Left ID must match the VPN tunnel responder's Right ID. In like manner, the initiator's Right ID must match the responder's Left ID.
 - **Right [Remote] ID:** [*a character string*] (representing the remote EN-2000)
Do not use this sample pre-shared key; it is merely an example. For purposes of demonstration, the sample pre-shared key includes the lowercase letter "l" (ell); do not mistake it for the number "1" (one).
- 6 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The configuration is saved, and the IPsec VPN Tunnel Table for a VPN Tunnel Responder is redisplayed (recall [Figure 5-4](#)).
 - 7 On the IPsec VPN Tunnel Table for a VPN Tunnel Responder, under the heading **IPsec Defaults**, select the **Edit** button (at the far right of the section).
 - ❖ The IPsec Defaults Configuration Screen for a VPN Tunnel Responder is displayed ([Figure 5-6](#)).

Figure 5-6. IPsec Defaults Configuration Screen for a VPN Tunnel Responder

The screenshot displays the 'IPsec Defaults' configuration screen. The interface includes a navigation bar at the top with tabs for 'Status', 'System', 'Network', 'Logout', and 'Quickstart'. Below this, there are sub-tabs for 'Interfaces', 'Hostnames', 'Static Routes', 'Failover', 'Firewall', 'Diagnostics', 'QoS', 'VPN', and 'VRRP'. The main content area is titled 'IPsec Defaults' and contains a form for configuring IPsec defaults. The form is organized into sections: 'IPsec Default Configuration' and 'Pass Conn'.

IPsec Default Configuration

Ike Lifetime	72h
Key Life	24h
ReKey Margin	1h
Keying Tries	2
Key Exchange	Ikev2
Auth	secret
Aggressive Mode	YES
IKE Encryption Protocol	AES256
IKE Authentication Protocol	MD5
IKE DH Group	Group2
ESP Encryption Protocol	AES256
ESP Authentication Protocol	MD5
ESP DH Group	Group2
DPD Action	Restart
DPD Delay	20s
DPD timeout	120s
RE-KEY	NO
RE-AUTH	NO
Responder	NO
Pass Conn type	Pass
Pass Conn Left Subnet	192.168.1.0/24
Pass Conn Right Subnet	192.168.1.0/24
Pass Conn Auth	Never
Pass Conn Startup operations	ROUTE

At the bottom of the screen, there are buttons for 'Back to Overview', 'Reset', 'Save', and 'Save & Apply'.

8 Configure the fields on the IPsec Defaults Configuration Screen for a VPN Tunnel Responder. Get all values from your network administrator.

Note the following required values for the VPN tunnel responder:

- Set **Responder** to **Yes**.
- Set **Pass Conn** to **Pass** (passthrough).
Note: When you select **Pass**, additional fields are displayed.
- Set **Pass Conn Auth** to **Never**.
- Set **Pass Conn Startup Operations** to **Route**.

The following are sample values.

- Phase 1:
 - ◆ **IKE Lifetime:** 72h [72 hours]
 - ◆ **Key Life:** 8h [8 hours]
 - ◆ **ReKey Margin:** 0h [0 hours; thus no kilobytes rekeying]
 - ◆ **Keying Tries:** 2 [the default value]
 - ◆ **Key Exchange:** IKEv1
 - ◆ **Auth** [Authentication]: secret
 - ◆ **Aggressive Mode:** No ("No" indicates use of main mode.)
 - ◆ **IKE Encryption Protocol:** 3DES

- ◆ **IKE Authentication Protocol:** SHA1
- ◆ **IKE DH** [Diffie–Hellman] **Group:** Group2
- Phase 2 (uses perfect forward secrecy):
 - ◆ **ESP Encryption Protocol:** 3DES
 - ◆ **ESP Authentication Protocol:** SHA1
 - ◆ **ESP DH** [Diffie–Hellman] **Group:** Group2
 - ◆ **DPD** [Dead Peer Detection] **Action:** Restart
 - ◆ **DPD** [Dead Peer Detection] **Delay:** 20s [seconds]
 - ◆ **DPD** [Dead Peer Detection] **Timeout:** 120s [seconds]
 - ◆ **Re-Key:** No
 - ◆ **Re-Auth:** No
 - ◆ **Pass Conn Left Subnet:** The local LAN subnet
 - ◆ **Pass Conn Right Subnet:** The local LAN subnet
- Note:** The Pass Conn Left Subnet and the Pass Conn Right Subnet must be identical.
- 9 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The configuration is saved. However, the configuration is not applied until [step 11](#) has been completed.
- 10 Select the **Back to Overview** button.
 - ❖ The IPsec VPN Tunnel Table for a VPN Tunnel Responder is redisplayed (recall [Figure 5-4](#)).
- 11 On the IPsec VPN Tunnel Table for a VPN Tunnel Responder, select the **Save & Apply** button (at the lower right of the screen).
 - ❖ The EN-2000 has been configured as an IPsec VPN tunnel responder.

5.3 The Next Steps

The following items need to be addressed:

- 1 Perform the procedures in the document [Configuring an EN-2000 Firewall](#).
- 2 Then perform the procedures in the document [Starting and Tracking VPNs in the EN-2000](#).

Note: If you wish to study VPNs, see the document [Virtual Private Networks](#).

