# VPNC Scenario for IPsec Interoperability

## EN-4000™ Router

This document presents a configuration profile for IPsec interoperability. The configuration profile conforms to the format recommended by the Virtual Private Network Consortium (VPN Consortium or VPNC).

To prepare the profile, each manufacturer of VPN devices uses its software package to configure the same scenario. Customers can study how each manufacturer configures its router for the sample scenario, and then can get VPN configurations for devices from different manufacturers to operate together.

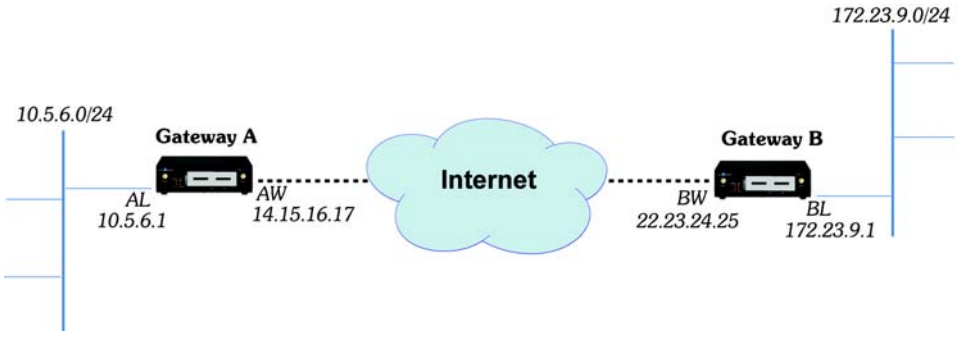
The VPN Consortium (*https://www.vpnc.org/*) developed the scenario. Although the consortium is no longer active, the scenario remains useful.

The EN-4000 supports IPsec interoperability as described in the scenario.

## G.1 Scenario 1: Gateway-to-Gateway VPN with Preshared Secret

Figure G-1 shows a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

Figure G-1. Scenario 1: Gateway-to-Gateway VPN




For information on trademarks, safety, limitations of liability, and similar topics, see *https://www.encorenetworks.com/disclaimer/*.


© 2019 Encore Networks, Inc.
All rights reserved.

VPN Gateway A has the following properties:

- Gateway A connects the private, internal LAN 10.5.6.0/24 to the internet.
- Gateway A's WAN external (internet) interface has the public IP address 14.15.16.17.
- Gateway A's LAN interface has the private IP address 10.5.6.1.

VPN Gateway B has the following properties:

- Gateway B connects the private, internal LAN 172.23.9.0/24 to the internet.
- Gateway B's WAN external (internet) interface has the public IP address 22.23.24.25.
- Gateway B's LAN interface has the private IP address 172.23.9.1.

The following IKEv1 Phase 1 parameters are used in scenario 1:

- Main mode
- 3DES
- SHA-1
- MODP group 2 [Diffie–Hellman Group 2] (1024 bits)
- Preshared secret: hr5xb84l6aa9r6

  **Note:** The preshared secret includes the lowercase letter "l" (ell); do not mistake it for the number "1" (one).
- Security Association lifetime of 28,800 seconds (8 hours), with no kilobytes rekeying

The following IKEv1 Phase 2 parameters are used in scenario 1:

- 3DES
- SHA-1
- ESP tunnel mode
- MODP group 2 [Diffie–Hellman Group 2] (1024 bits)
- Perfect forward secrecy for rekeying
- Security Association lifetime of 3,600 seconds (1 hour), with no kilobytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

## G.2 Configuring the EN-4000 for VPNC Scenario 1

**Caution:** If you configure routers as Gateway A and Gateway B to implement the scenario, make sure those routers are attached only to closed networks.

In this implementation of interoperability scenario 1, Gateway A is an EN-4000 router from Encore Networks, Inc. Gateway B can be an EN-4000, any other Encore Networks VPN device, or another manufacturer's VPN device.

The procedures in the following sections are presented as quick guidelines for configuring an EN-4000 as Gateway A in scenario 1.[1] The entries in the configuration

1. For details of VPN configuration, see *the document The EN-4000™ in IPsec Virtual Private Networks*.

screens reflect the values shown in Figure G-1 and the values listed after that figure. Use this document to work through the configuration of the EN-4000 for scenario 1.

**Note:** Although its configuration is not addressed in this document, Gateway B must be configured to terminate the tunnel that Gateway A initiates.

After Gateway A and Gateway B have been configured for scenario 1, start the tunnel for scenario 1 and monitor it in operation.

## G.2.1 Setting Up, Starting Up, and Logging In

Use the following instructions to set up the EN-4000:[2]

1. Make sure all EN-4000 hardware has been installed. If SIMs are used, make sure they have been installed.
2. Use an Ethernet cable to connect a control console (such as a PC) to a LAN port on the rear of the Gateway A EN-4000. Turn the EN-4000's power on.
3. Open a web browser. Make sure JavaScript is enabled in the browser. Type the IP address for the EN-4000's LAN port (**http://192.168.10.1**) in the browser's address window, and press the **Enter** key. Accept cookies for the management system.
4. Type the user name and password, and select the button to **Log In**.

   **Note:** For EN-4000™ routers, the default user name is **root**. For all other EN™ routers, the default user name is **admin**. In addition:

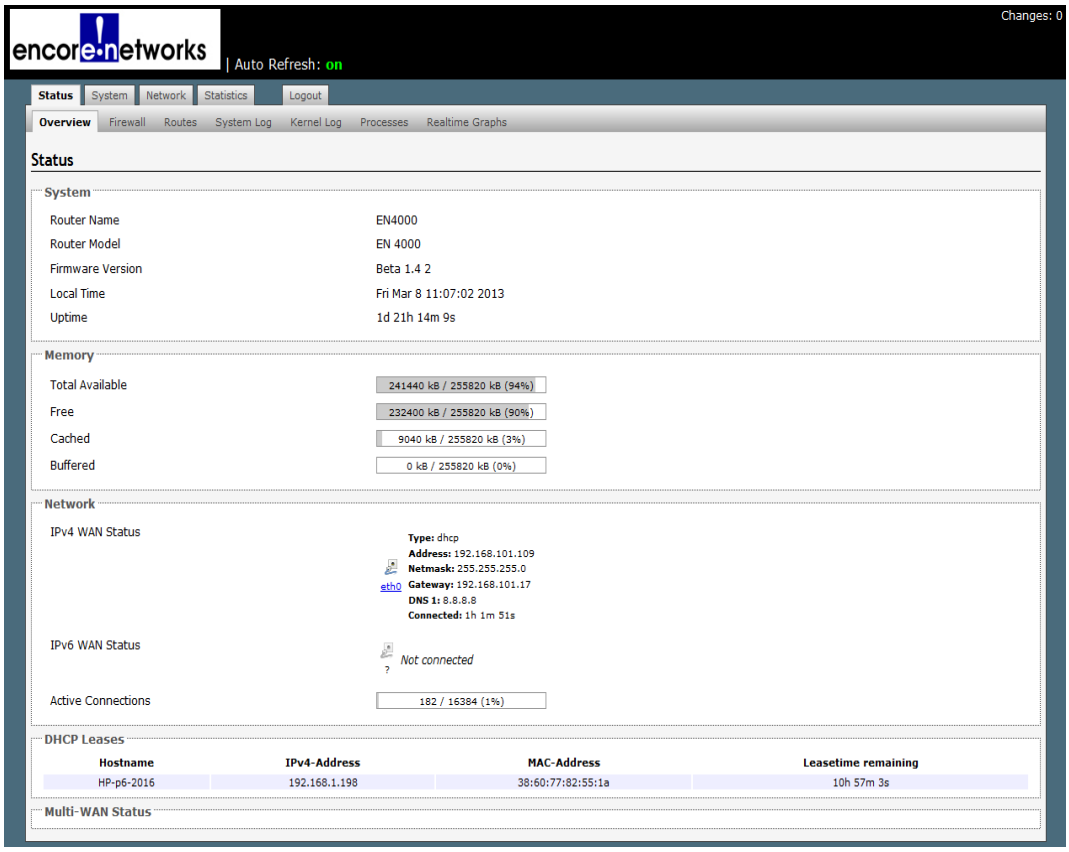
   - Devices shipped before July 09, 2018, use the default password **encore!1**.
   - Devices shipped from the factory on or after July 09, 2018, use a randomly generated default password. That password is contained in information on a sticker on the bottom of the router's chassis. Retain that sticker; you will need that default password if the router must be reset. (For details, see the document *Password Policy for EN™ Routers*.)

   **Note:** Encore Networks, Inc., advises users to change a router's password upon first configuration of the router. Check with your network administrator for all names and passwords.

   ❖ After you complete the log-in, the Status Overview Screen is displayed (Figure G-2).
5. Make sure the EN-4000 has received its basic configuration. And, if you installed any SIM in step 1, activate each new SIM in its carrier network.

2. For more information on EN-4000 installation, see the *EN-4000™ Quick Installation Guide*, at *http://www.encorenetworks.com/documentation.htm/document-catalog/*.

Figure G-2. Status Overview Screen for EN-4000 Management System

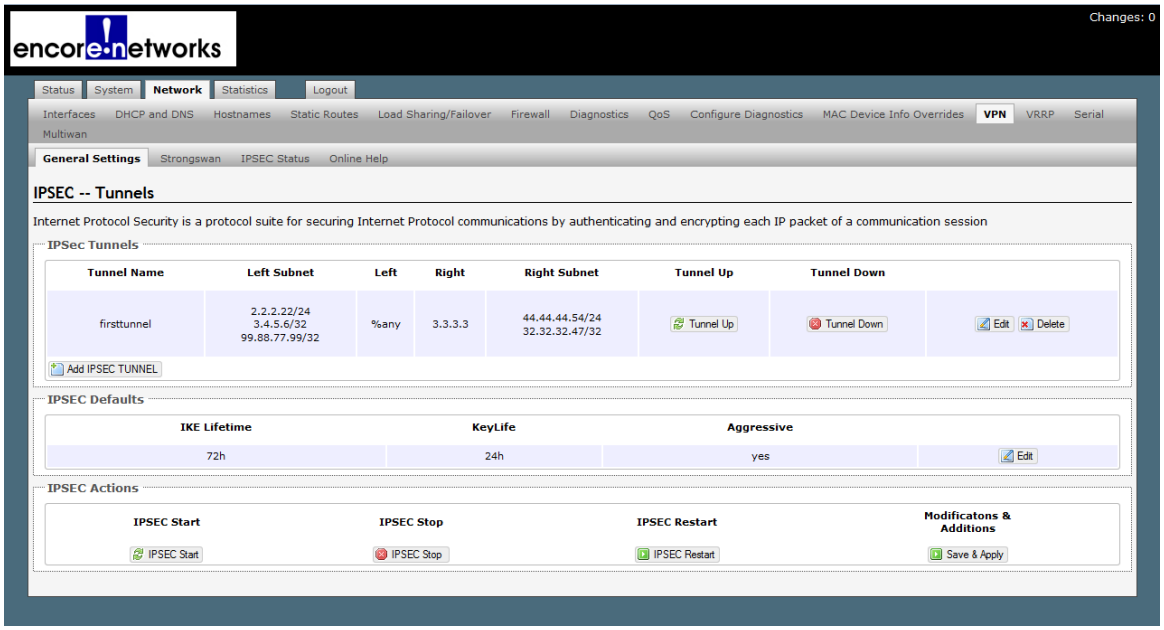



## G.2.2 Configuring an IPsec VPN Tunnel on the EN-4000

1 In the EN-4000's browser-based management system, select the **Network** tab, then the **VPN** tab.

❖ The List of Configured IPsec VPN Tunnels is displayed (Figure G-3).

Figure G-3. List of Configured IPsec VPN Tunnels

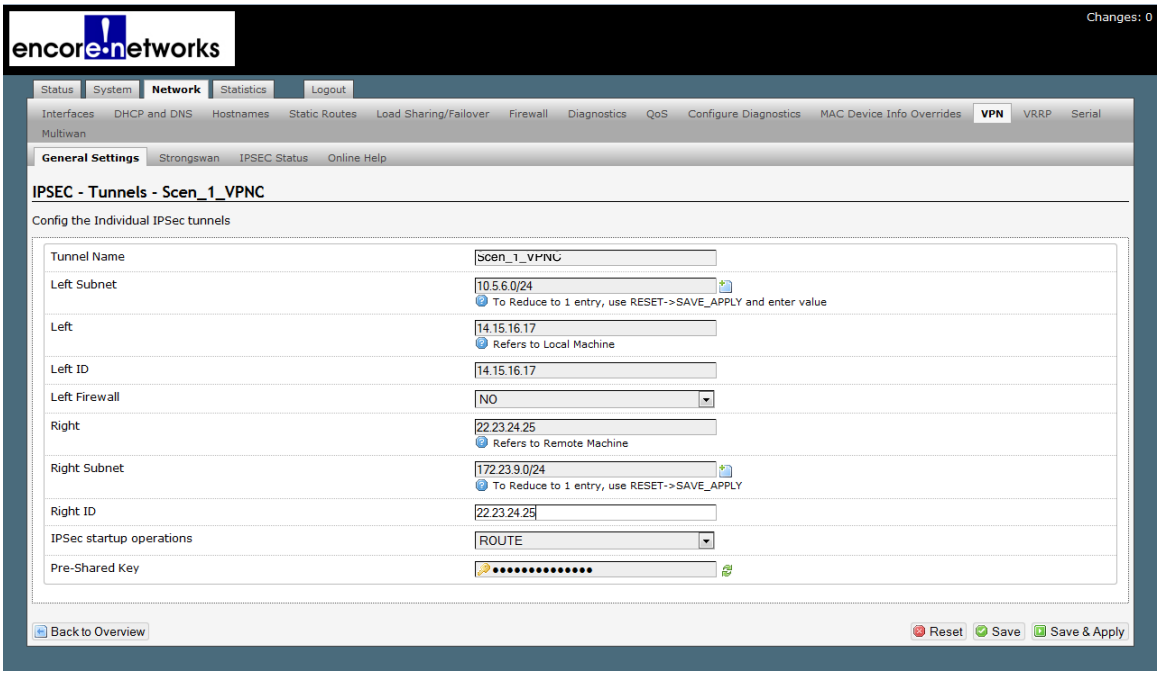


**Note:** In the VPN tunnel configuration screens, "left" indicates "local" (that is, it indicates the EN-4000 router) and "right" indicates "remote" (the device at the other end of the connection).

**2** Select the button **Add IPsec Tunnel** (at left on the screen, below the list of Tunnel Names).

❖ The screen for Configuring an IPsec VPN Tunnel is displayed (Figure G-4).

Figure G-4. Configuring an IPsec VPN Tunnel
for VPNC Scenario 1




**3** On the screen for Configuring an IPsec VPN Tunnel, configure the following:

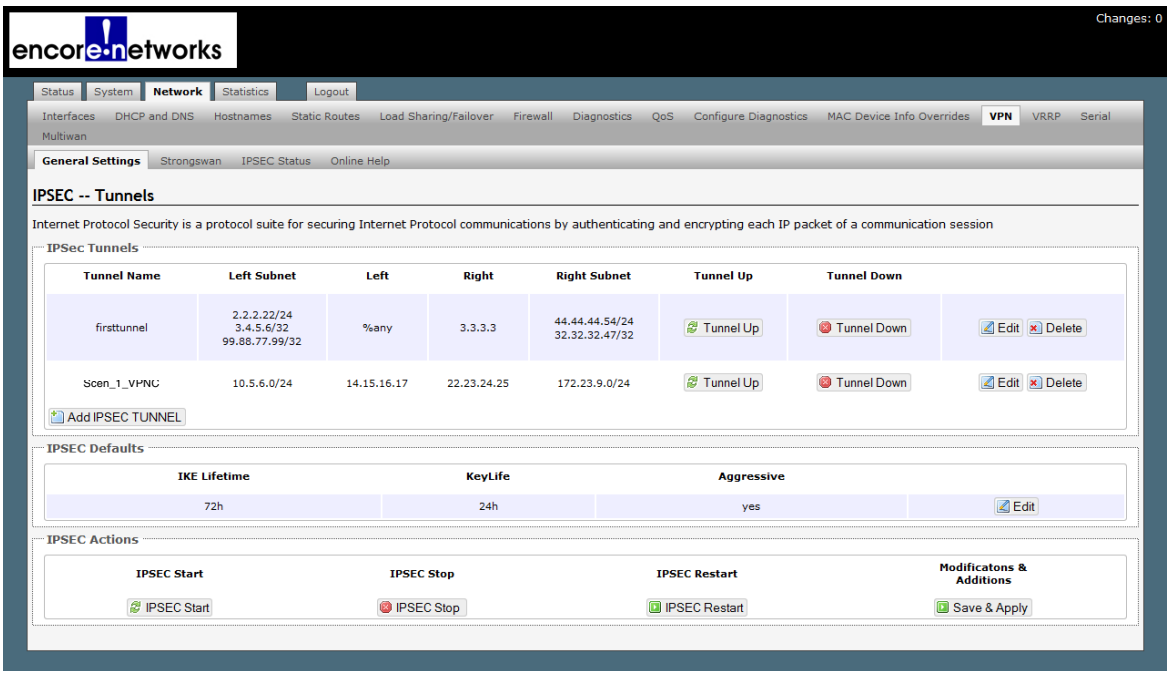
- **Tunnel Name:** Scen_1_VPNC
- **Left Subnet:** 10.5.6.0/24
- **Left** [local EN-4000's public IP address]: 14.15.16.17
- **Left ID:** 14.15.16.17
- **Left Firewall:** NO
- **Right** [remote router's public IP address]: 22.23.24.25
- **Right Subnet:** 172.23.9.0/24
- **Right ID:** 22.23.24.25
- **IPsec Start-Up Operations:** ROUTE
- **Pre-Shared Key:** hr5xb84l6aa9r6

  **Note:** The preshared key includes the lowercase letter "l" (ell); do not mistake it for the number "1" (one).

**4** When you have finished configuring the VPN tunnel, select the **Save & Apply** button (in the lower left corner of the screen).

❖ The new VPN tunnel configuration is saved. The List of Configured IPsec VPN Tunnels is redisplayed. The new tunnel is at the bottom of the list of Tunnel Names (Figure G-5).

Figure G-5. List of Configured IPsec VPN Tunnels
Including the Tunnel Named Scen_1_VPNC




**5** In the List of Configured IPsec VPN Tunnels, you may (if you wish) delete the default IPsec VPN tunnel (named firsttunnel in Figure G-5). (That deletion is **not** required.)

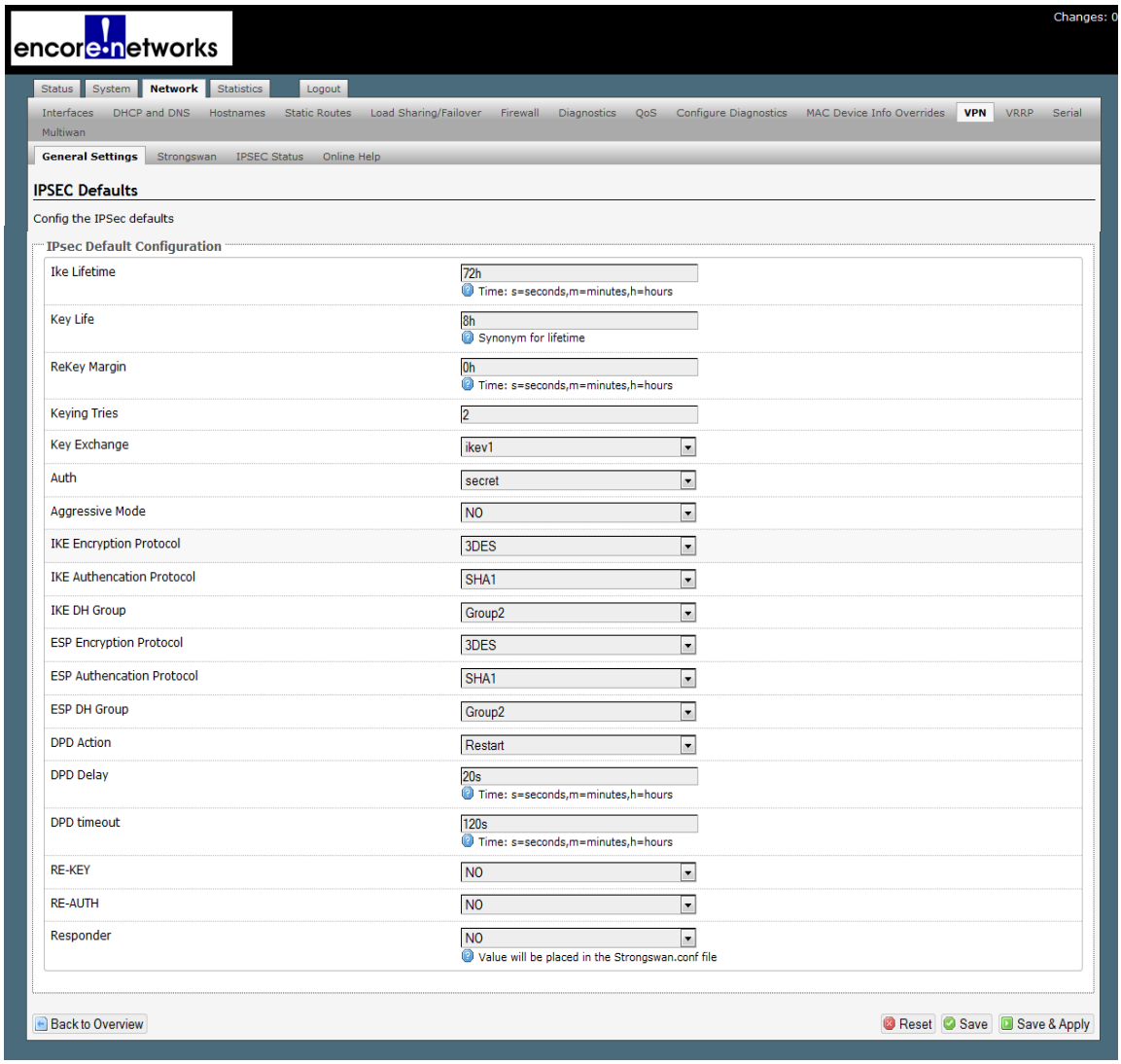
! **Caution:** Do not delete any VPN tunnels that are active or that you intend to use.

**6** On the screen for the List of Configured IPsec VPN Tunnels, select the **Save & Apply** button (under **Modifications and Additions**, at the lower right of the screen).

**7** In the List of Configured IPsec VPN Tunnels, select the **Edit** button at the far right of the row under **IPsec Defaults**.

❖ The screen for Configuring IPsec Defaults is displayed (Figure G-6).

Figure G-6. Configuring IPsec Defaults
for VPNC Scenario 1




**8** On the screen for Configuring IPsec Defaults, configure the following:

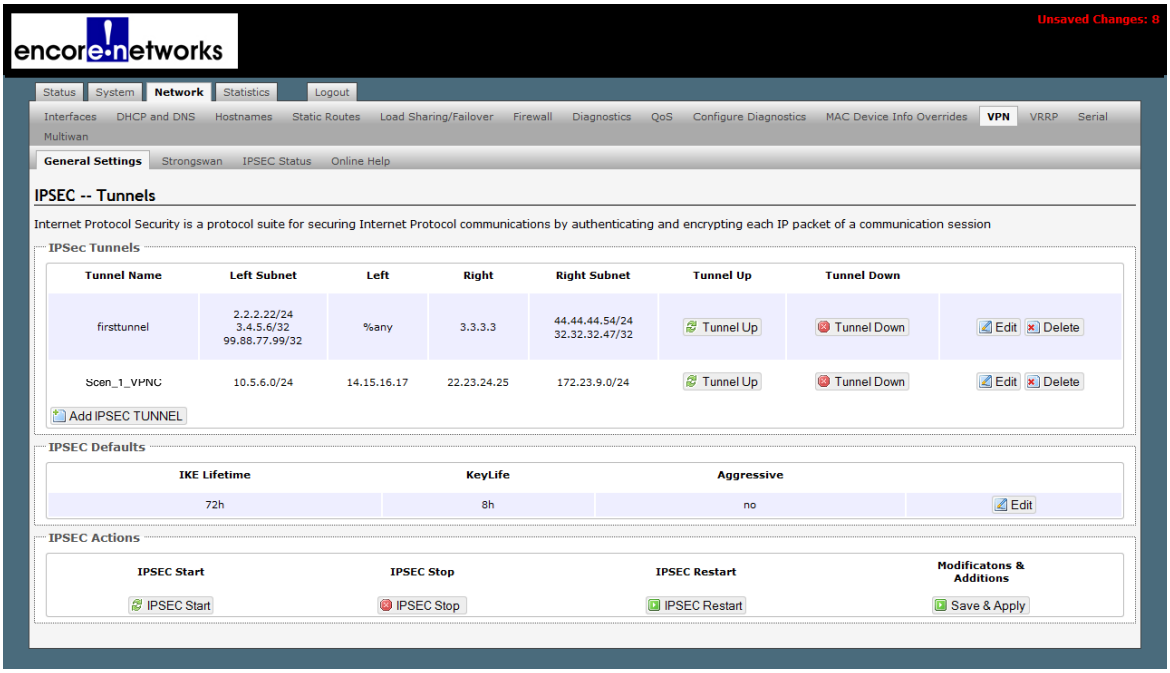
- Phase 1:
  - **IKE Lifetime:** 72h [72 hours]
  - **Key Life:** 8h [8 hours]
  - **ReKey Margin:** 0h [0 hours; thus no kilobytes rekeying]
  - **Keying Tries:** 2 [the default value]
  - **Key Exchange:** IKEv1
  - **Auth** [Authentication]: secret
  - **Aggressive Mode:** No ("No" indicates use of 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
- **Responder:** No (This means that the local EN-4000 will initiate the tunnel.)

**9** When you have finished configuring IPsec defaults, select the **Save & Apply** button in the lower right corner of the screen.

❖ The IPsec defaults are saved, and the List of Configured IPsec VPN Tunnels is redisplayed (Figure G-7).

Figure G-7. List of Configured IPsec VPN Tunnels
with IPsec Defaults for Testing the Tunnel Named Scen_1_VPNC




**10** Do one of the following:

**a** If this is the first IPsec VPN activity since system start-up, select the **IPSEC Start** button (at the lower left of the management window).

**b** If IPsec VPN tunnels are already running, select the **IPSEC Restart** button.

❖ In either case, the new IPsec VPN tunnel is started.

**Note:** To complete the tunnel in VPNC Scenario 1, you must also configure Gateway B.

# G.3 Starting the Tunnel for VPNC Scenario 1

If you performed step 10a or step 10b on page 8, the tunnel is already up, and you may skip this section.

1 In the List of Configured IPsec VPN Tunnels, select the **Tunnel Up** button in the row for the tunnel named Scen_1_VPNC.

❖ The selected VPN tunnel (Scen_1_VPNC) is started.

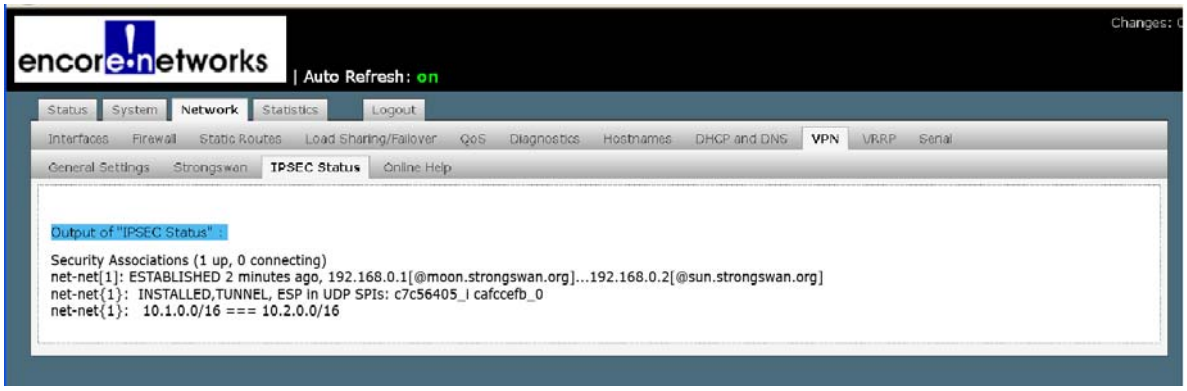
**Note:** To complete the tunnel in VPNC Scenario 1, you must also configure Gateway B.

# G.4 Checking the Connection

**Note:** To complete the tunnel in VPNC Scenario 1, you must also configure Gateway B. The procedure in this section should not be performed until Gateway B has been configured and is ready to connect.

1 In the EN-4000 Management System, select the **Network** tab. Then select **VPN**, **IPsec Status** to see the status of each active IPsec VPN tunnel (Figure G-8). (Active VPN tunnels include tunnels that are up and tunnels that are being brought up.)

Figure G-8. Status of IPsec VPN Tunnels




**Note:** The display lists one or more of the following:

- **NO DATA FOUND:** No IPsec VPN tunnel is active.
- **CONNECTING:** The indicated IPsec VPN tunnels are starting IKEv1's phase 1 (tunnel set-up).
- **INSTALLED:** The indicated IPsec VPN tunnels are starting IKEv1's phase 2 (data transfer).
- **ESTABLISHED:** The indicated IPsec VPN tunnels have finished IKEv1's phase 2 (data transfer) successfully.

If your IPsec VPN tunnel's name (TUNNEL, in Figure G-8) is displayed in the **INSTALLED** line of the IPsec VPN Tunnel Status Screen, then the tunnel has been set up successfully and is exchanging data with Gateway B.

# G.5 Troubleshooting

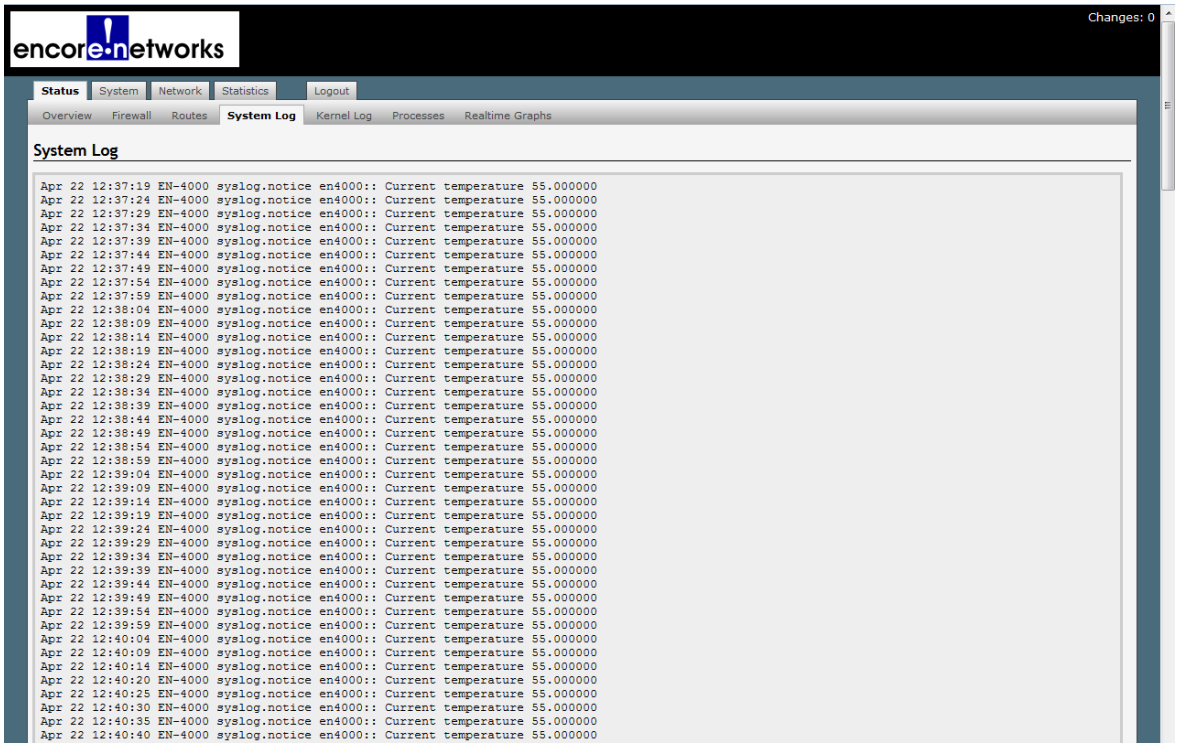
If there is a problem with an IPsec VPN tunnel, do the following:

**1** On the EN-4000 management system, select the **Status** tab; then select the **System Log** tab.

❖ The system log (Figure G-9) is displayed.

**Note:** Your EN-4000's system log will include progressive states of the IPsec VPN tunnels.

Figure G-9. System Log




**2** Do the following:

**a** Find lines about the VPN tunnel in the system log. (The system log includes tunnel names.)

**b** Study those lines to determine the cause of the problem.

**c** Then consider potential resolutions of the problem.