SLE™ in Virtual Private Networks

This document discusses implementation of Encore Networks' Selective Layer Encryption (SLE, patented), a proprietary method of enhancing transmission speed for VPNs over satellite networks.

Satellite networks experience inherent delay in transmission responses. A satellite network's performance enhancing proxy (PEP) reduces that delay, but PEP interferes with VPN security. Encore Networks, Inc., developed SLE to resolve both of those concerns.

See the following:

- *Setting Up SLE on an IPsec VPN Tunnel*
- *Verifying that SLE is Running*

Note: SLE is used only over satellite networks. For information on configuring VPNs over other networks, see *The EN-4000™ in IPsec Virtual Private Networks*.

10.1 Setting Up SLE on an IPsec VPN Tunnel

To use SLE, each end of the IPsec VPN tunnel must be an EN-4000. One EN-4000 initiates the VPN tunnel, and another EN-4000 terminates the tunnel (responds to the request for connection).

This section presents procedures for configuring an IPsec VPN tunnel to use SLE. See the following:

- *Configuring an EN-4000 as a VPN Tunnel Initiator, Incorporating SLE*
- *Configuring an EN-4000 as a VPN Tunnel Responder, Incorporating SLE*
- *Configuring the Firewall for an IPsec VPN Tunnel That Uses SLE*
- *Configuring the Source NAT*

Note: In the EN-4000 management system, the term "left" represents "local," and the term "right" represents "remote." Those designations are always from the point of view of the router being managed—the local ("left") EN-4000.

Version A, November 2014

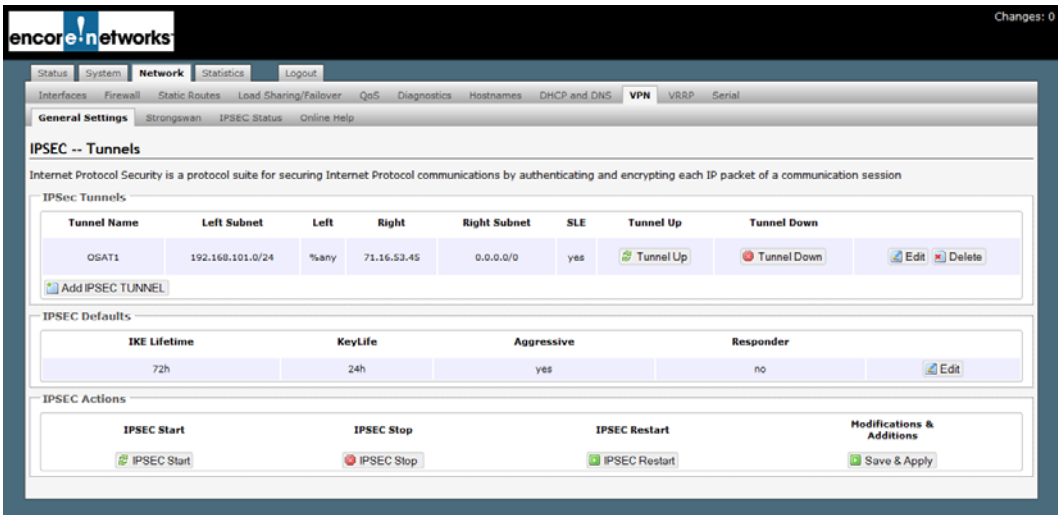
10.1.1 Configuring an EN-4000 as a VPN Tunnel Initiator, Incorporating SLE

1 Log into the EN-4000. (For details, see *Logging In*, on page 2 of the document *Configuring General Settings for the EN-4000*.)

2 On the EN-4000 management system, select the **Network** tab. Then select the **VPN** tab. If necessary, select the **General Settings** tab.

❖ The IPsec VPN Tunnel Screen for a VPN Tunnel Initiator is displayed (Figure 10-1).

Figure 10-1. IPsec VPN Tunnel Screen for a VPN Tunnel Initiator



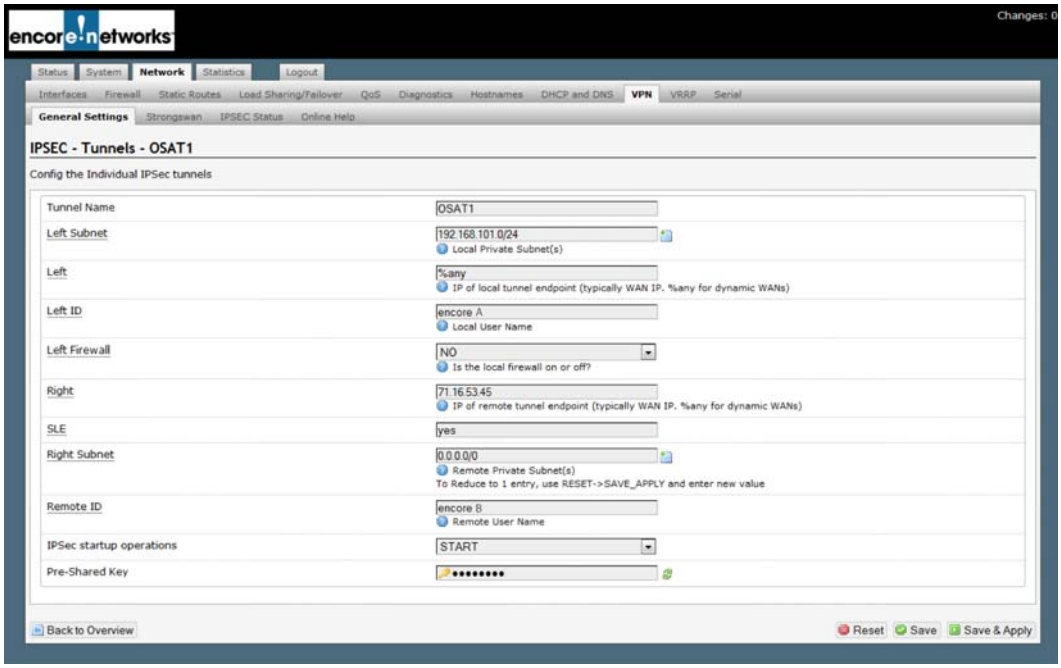
3 Under the heading **IPsec Tunnels**, do one of the following:

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 10-2).

Figure 10-2. IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator



4 Configure the fields on the IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator. Get all values from your network administrator. Note the following:

- Set the **Left** IP address to **%any**.
- Set the **Left Firewall** to **No** (off).
- Set the use of **SLE** to **yes**.
- Set **IPsec Startup Operations** to **Start**.
- Type the **Preshared Key**. (Get the key from your network administrator. The preshared key must be identical for both sides of the IPsec VPN tunnel.)

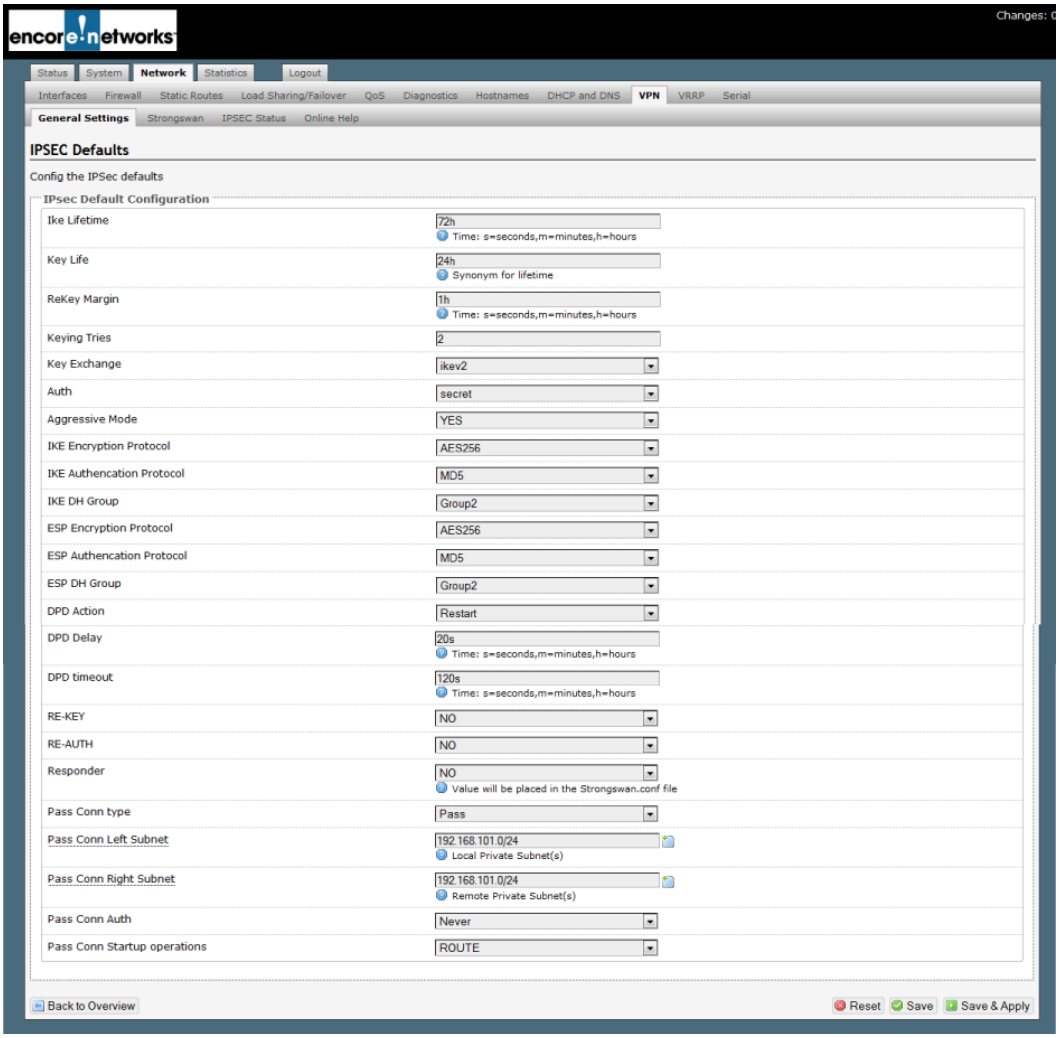
5 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).

❖ The configuration is saved, and the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator is redisplayed (recall Figure 10-1).

6 On the IPsec VPN Tunnel Screen 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 10-3).

Figure 10-3. IPsec Defaults Configuration Screen for a VPN Tunnel Initiator



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

- Set **Responder** to **No**. (This EN-4000 is the tunnel initiator.)
- Set **Pass Conn** to **Pass** (passthrough).
- Set **Pass Conn Auth** to **Never**.
- Set **Pass Conn Startup Operations** to **Route**.

8 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 Screen for a VPN Tunnel Initiator is redisplayed (recall Figure 10-1).

9 On the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator, select the **Save & Apply** button (at the lower right of the screen).

❖ The EN-4000 has been configured as an IPsec VPN (with SLE) tunnel initiator.

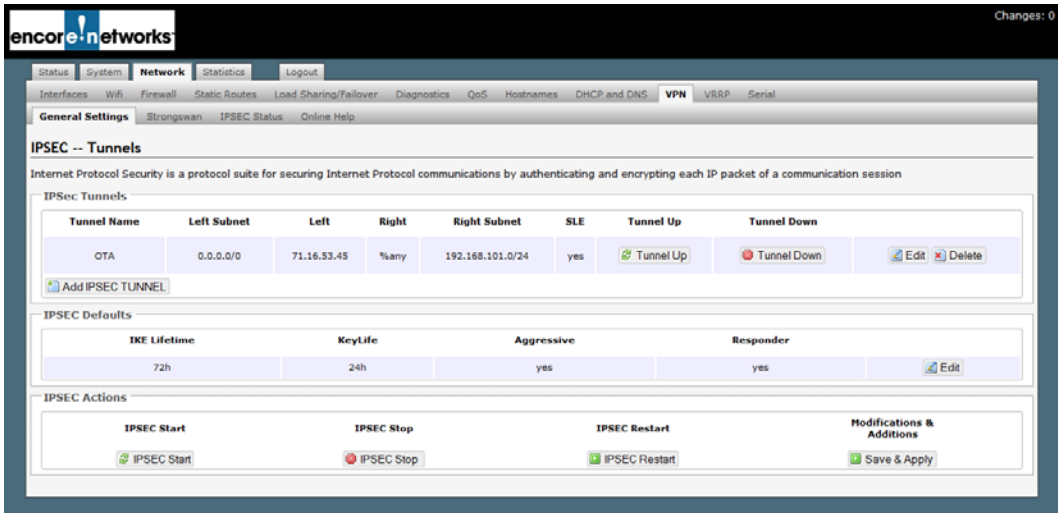
10.1.2 Configuring an EN-4000 as a VPN Tunnel Responder, Incorporating SLE

1 Log into the EN-4000. (For details, see *Logging In*, on page 2 of the document *Configuring General Settings for the EN-4000*.)

2 On the EN-4000 management system, select the **Network** tab. Then select the **VPN** tab. If necessary, select the **General Settings** tab.

❖ The IPsec VPN Tunnel Screen for a VPN Tunnel Responder is displayed (Figure 10-4).

Figure 10-4. IPsec VPN Tunnel Screen for a VPN Tunnel Responder



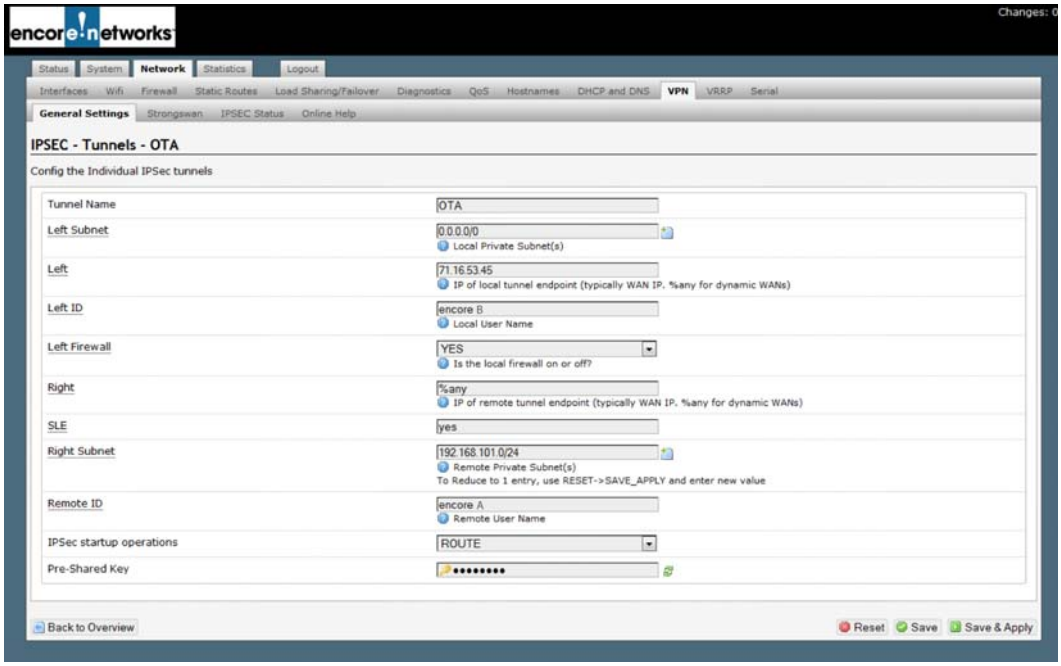
3 Under the heading **IPsec Tunnels**, do one of the following:

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 10-5).

Figure 10-5. IPsec Tunnel Configuration Screen for a VPN Tunnel Responder



4 Configure the fields on the IPsec Tunnel Configuration Screen for a VPN Tunnel Responder. Get all values from your network administrator. Note the following:

- Set the **Left Subnet** to **0.0.0.0**.
- Set the **Left** IP address to this EN-4000's WAN IP address.
- Set the **Left Firewall** to **Yes** (on).
- Set the **Right** IP address to **%any**.
- Set use of **SLE** to **yes**.
- Set the **Right Subnet** to the subnet of the initiator EN-4000.
- Set **IPsec Startup Operations** to **Route**.
- Type the **Preshared Key**. (Get the key from your network administrator. The preshared key must be identical for both sides of the IPsec VPN tunnel.)

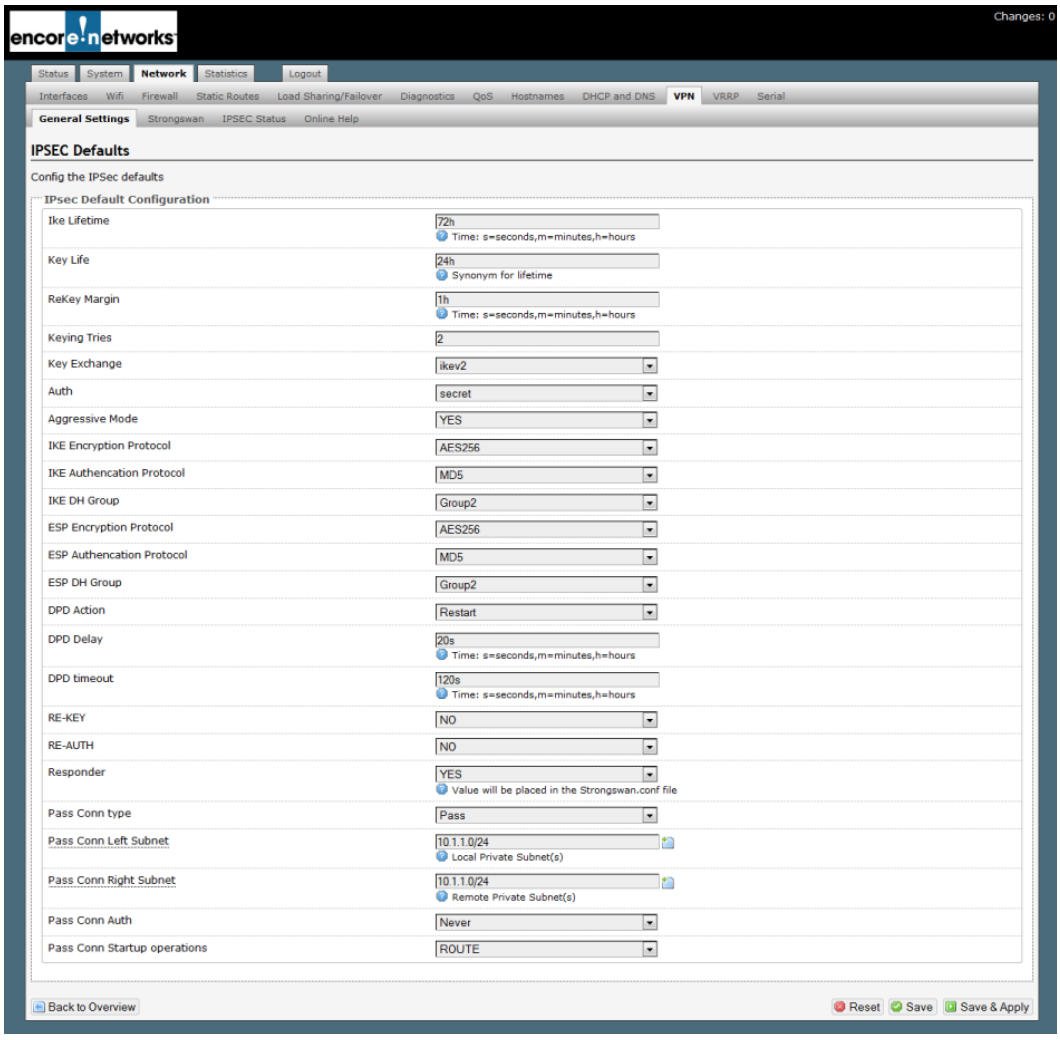
5 When you have finished the configuration, select the **Save & Apply** button (at the lower right of the screen).

❖ The configuration is saved, and the IPsec VPN Tunnel Screen for a VPN Tunnel Responder is redisplayed (recall Figure 10-4).

6 On the IPsec VPN Tunnel Screen 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 10-6).

Figure 10-6. IPsec Defaults Configuration Screen for a VPN Tunnel Responder



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

- Set **Responder** to **Yes**.
- Set **Pass Conn** to **Pass** (passthrough).
- Set **Pass Conn Auth** to **Never**.
- Set **Pass Conn Startup Operations** to **Route**.

8 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 10 has been completed.

9 Select the **Back to Overview** button.

❖ The IPsec VPN Tunnel Screen for a VPN Tunnel Responder is redisplayed (recall Figure 10-4).

10 On the IPsec VPN Tunnel Screen for a VPN Tunnel Responder, select the **Save & Apply** button (at the lower right of the screen).

❖ The EN-4000 has been configured as an IPsec VPN (with SLE) tunnel responder.

10.1.3 Configuring the Firewall for an IPsec VPN Tunnel That Uses SLE

The firewall for the IPsec VPN tunnel is configured on the EN-4000 that is the VPN tunnel responder. See the following:

- *Firewall Zones*
- *Firewall Traffic Rules*

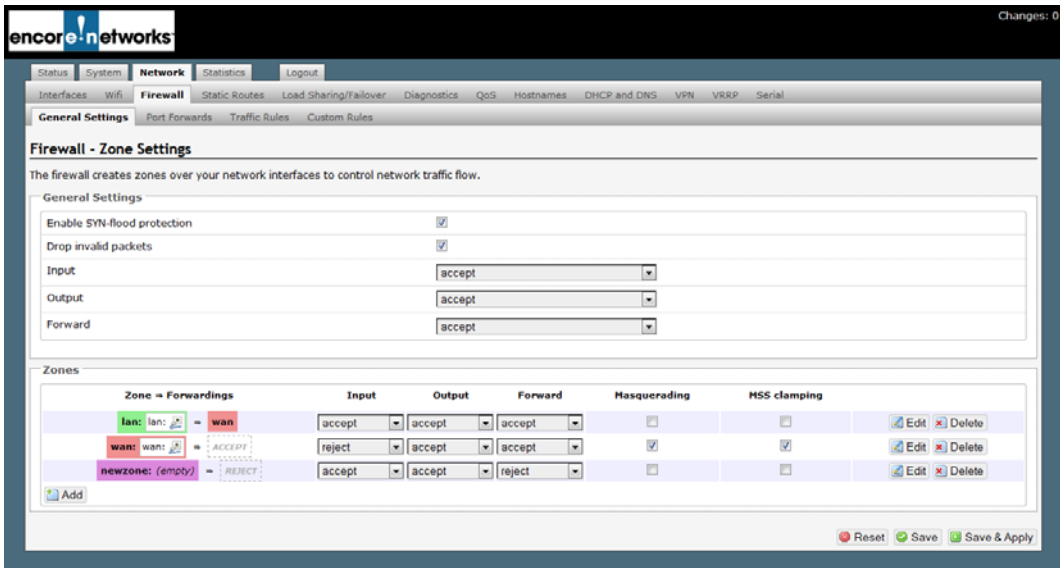
10.1.3.1 Firewall Zones

Some firewall zones require configuration changes to support SLE for IPsec VPNs.

1 On the EN-4000 management system, select the **Network** tab. Then select the **Firewall** tab. If necessary, select the **General Settings** tab.

❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is displayed (Figure 10-7).

Figure 10-7. Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder

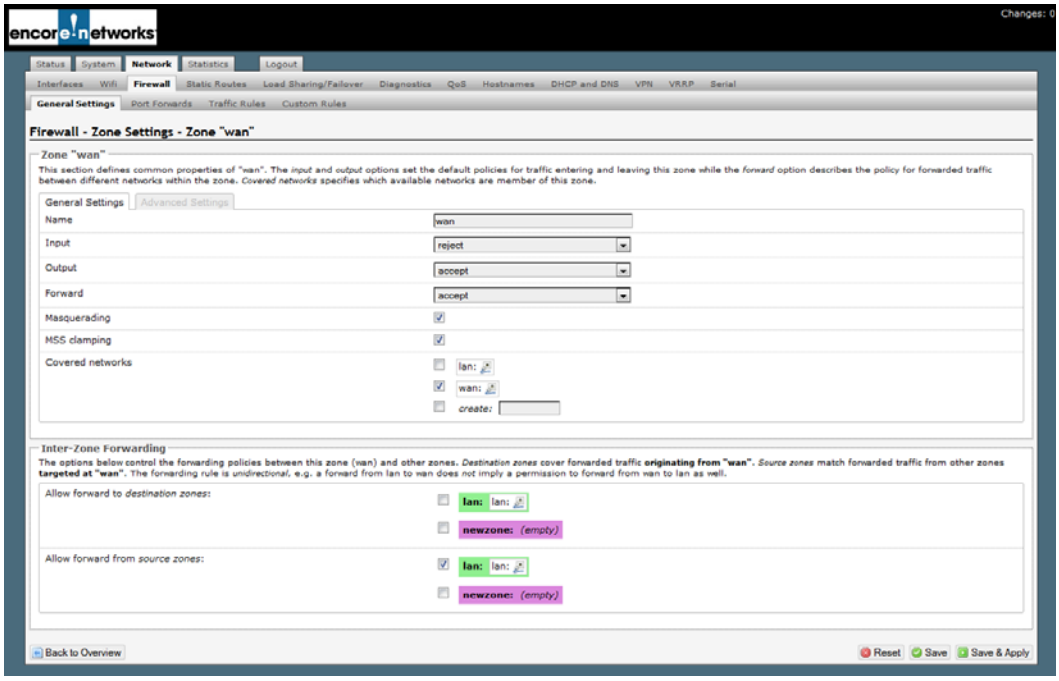


2 For this example, select the **Edit** button in the row for the WAN zone.

Note: In general, select the **Edit** button for each zone for which **Masquerading** is selected (by default).

❖ The General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder is displayed (Figure 10-8).

Figure 10-8. General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder



3 On the General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder, configure the following:

- Under the heading **General Settings**:
  - Set **Input** to **Reject**.
  - Set **Output** to **Accept**.
  - Set **Forward** to **Accept**.
  - Enable **Masquerading**.
  - Enable **MSS Clamping**.
  - For **Covered Networks**, select **WAN**.
- Under the heading **Interzone Forwarding**:
  - For **Allow Forward for Source Zones**, select the source zone **LAN**.

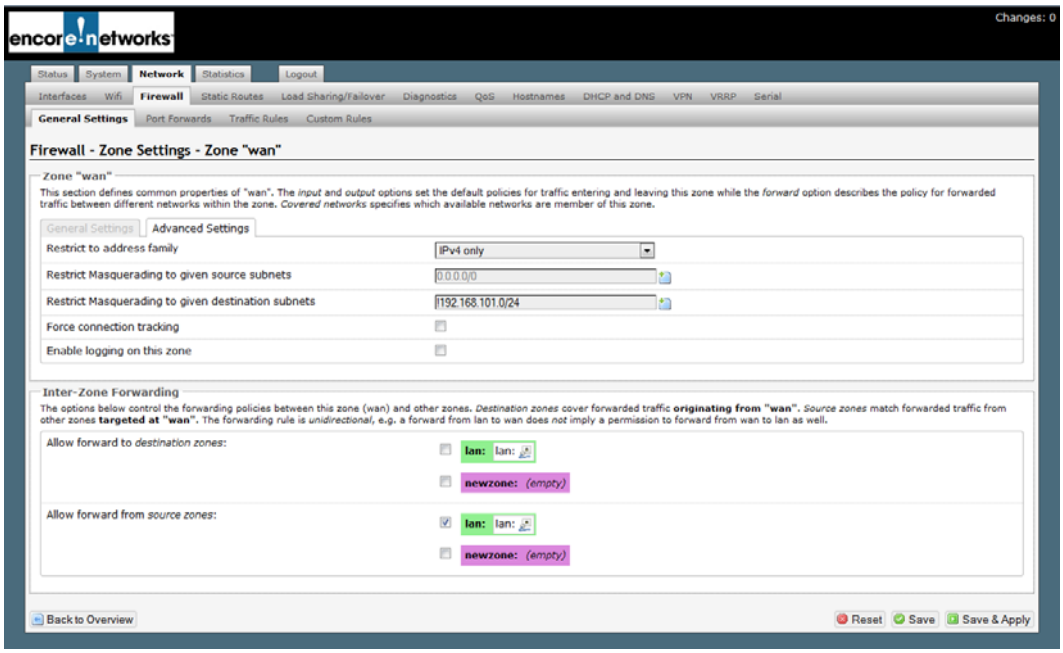
4 When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).

Note: If masquerading is enabled for the zones of interest under firewall configuration, then, for IPsec to work properly, packets destined for the right subnet cannot be masqueraded. Step 5 through step 7 resolve that concern.

5 Then select the **Advanced Settings** tab on the General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder.

❖ The Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder is displayed (Figure 10-9).

Figure 10-9. Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder



6 On the Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder, configure the following:

a Under the heading **Zone WAN**:

i Set **Restrict to Address Family** to **IPv4 Only**.

ii Set **Restrict Masquerading to Given Source Subnets** to **0.0.0.0/0**.

iii Set **Restrict Masquerading to Given Destination Subnets** to **!*a.b.c.d/e***, where the exclamation point (**!**) indicates not to masquerade the IP address, and *a.b.c.d/e* represents the subnet for the remote EN-4000.

❖ This turns off masquerading for the VPN tunnel.

Note: The initiator must also disable masquerading for this connection. After you finish the current procedure, see *Disabling Masquerading on the VPN Tunnel Initiator*, on page 12.

b If you wish to exempt an additional destination subnet, select the **Add** button beside the that field, and repeat substep 6.a.iii.

c Under the heading **Interzone Forwarding**:

◆ For **Allow Forward from Source Zones**, select **LAN**.

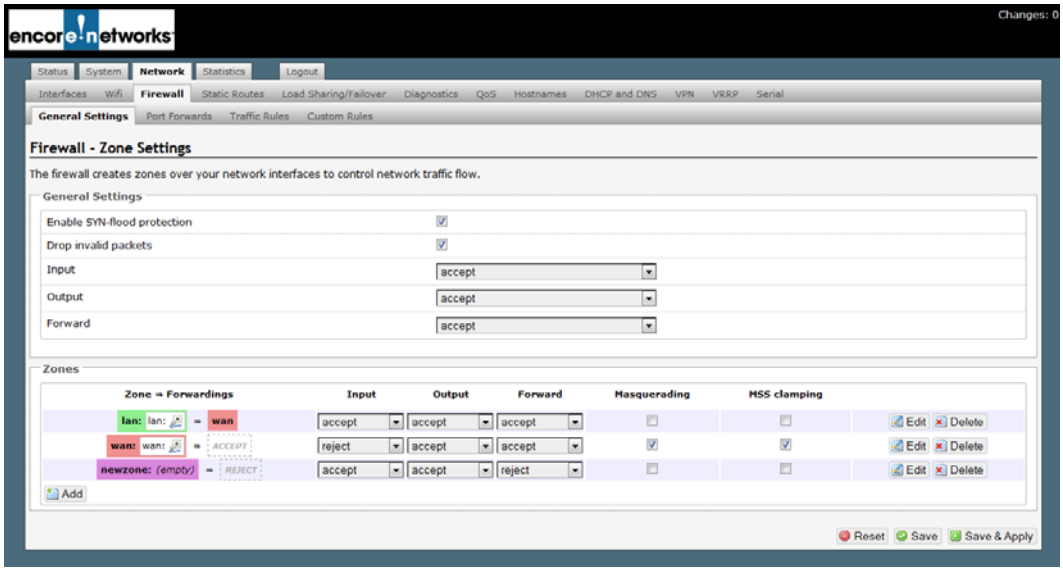
7 When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).

❖ Masquerading for the subnet has been disabled, so that VPNs will work properly.

8 Then select the **Back to Overview** button.

❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is redisplayed (Figure 10-10).

Figure 10-10. Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder



9 On that screen, make sure the following settings are observed:

- Under the heading **General Settings**:
  - Select **Enable SYN-Flood Protection**.
  - Select **Drop Invalid Packets**.
  - Set **Input** as **Accept**.
  - Set **Output** as **Accept**.
  - Set **Forward** as **Accept**.
- Under the heading **Zones**:
  - The **LAN** zone is configured to forward to the **WAN** zone. **Input**, **Output**, and **Forward** for that forwarding zone are all set to **accept**.
  - Verify that the **WAN** zone has the following settings:
    - **Input: reject**
    - **Output: accept**
    - **Forward: accept**
    - Uses **Masquerading**
    - Uses **MSS Clamping**

Note: You can also configure the **newzone** if the EN-4000 will use that zone; possibilities are for 802.11 wireless, GigE, or Ethernet. Consult your network administrator for configuration information.

10 When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).

❖ The configuration is saved.

11 Select the **Back to Overview** button.

❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is redisplayed (recall Figure 10-7).

12 On that screen, select the **Save and Apply** button.

❖ The configuration is saved and applied (restarting the firewall).

10.1.3.2 Disabling Masquerading on the VPN Tunnel Initiator

There are two ways to disable masquerading on the initiator of the VPN tunnel, depending on the initiator's right subnet.

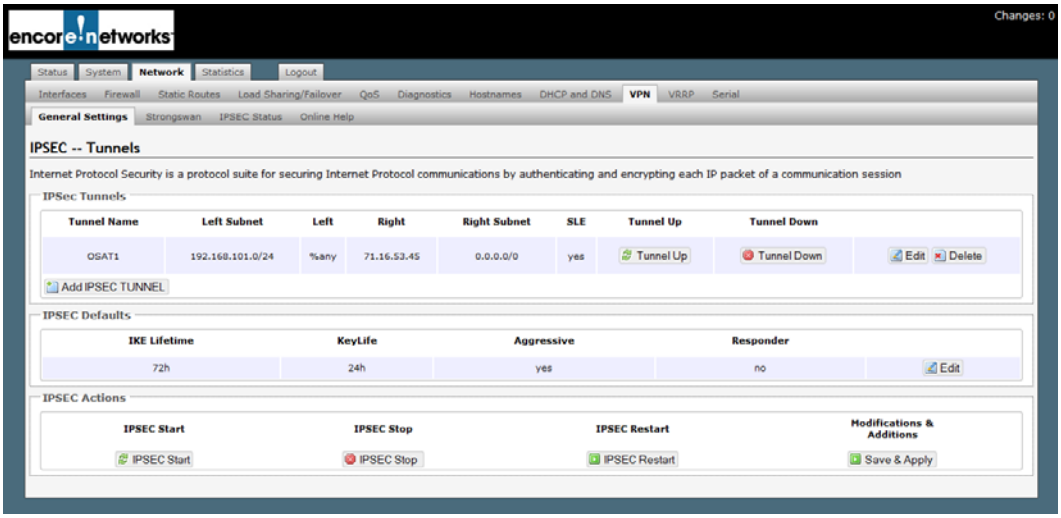
! **Caution:** Do only one of the following:

- If the tunnel initiator's right subnet is 0.0.0.0/0, perform only step 1.
- If the tunnel initiator's right subnet is not 0.0.0.0/0, perform only step 2.

---

1 If the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator specifies a **Right Subnet** of **0.0.0.0/0**, indicating all remote locations (as shown in Figure 10-11), do the following:

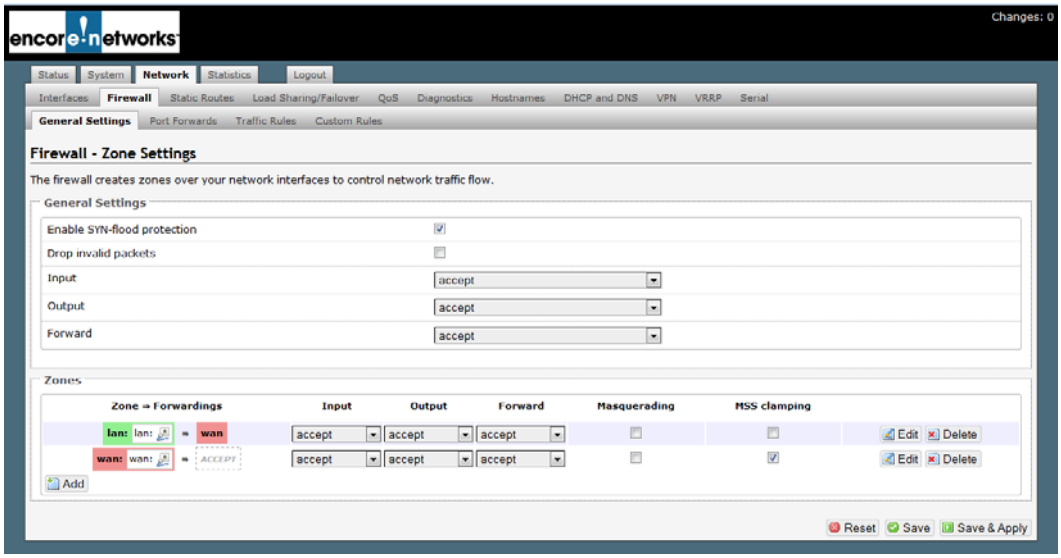
Figure 10-11. IPsec VPN Tunnel Screen for a VPN Tunnel Initiator



a Select the **Network** tab; then select the **Firewall** tab.

❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator is displayed (Figure 10-12).

Figure 10-12. Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator



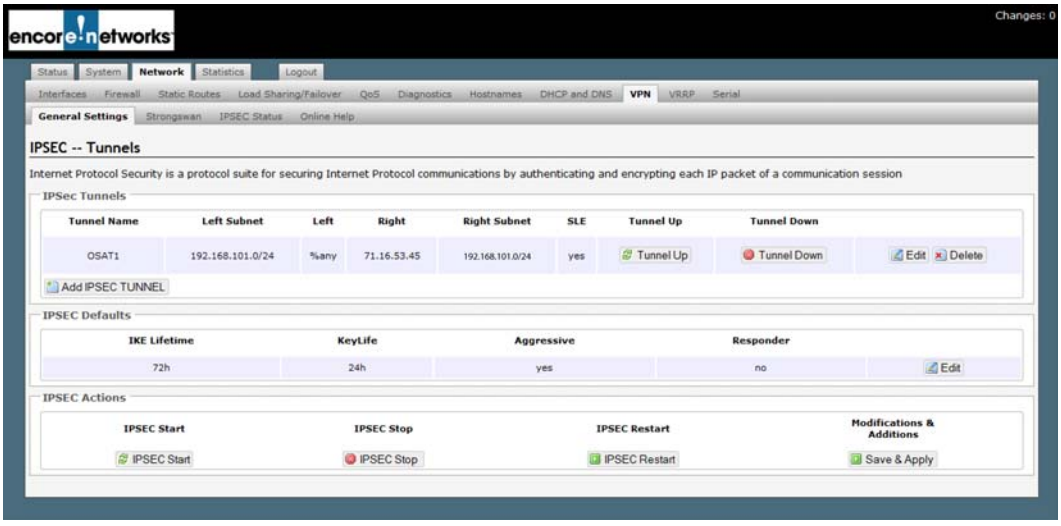
b On the Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator, make sure **Masquerading** is NOT checked for any **Zone Forwarding**.

c On that same screen, select the **Save & Apply** button.

d Go to *Firewall Traffic Rules*, on page 15.

2 If the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator specifies a **Right Subnet** of ***f.g.h.i/j*** other than 0.0.0.0/0 (in Figure 10-13, the sample right subnet is 192.168.101.0/24), do the following:

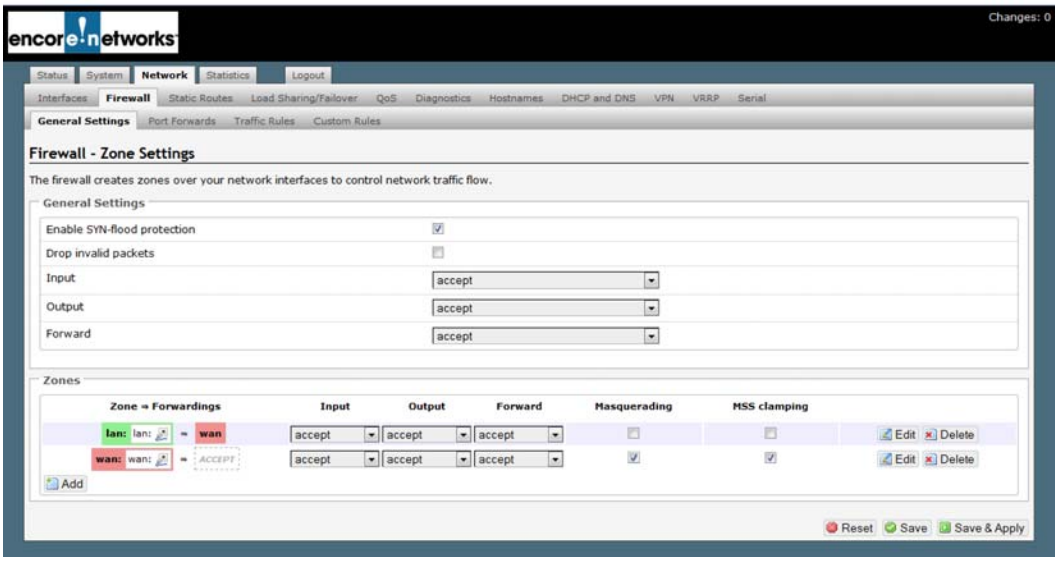
Figure 10-13. IPsec VPN Tunnel Screen for a VPN Tunnel Initiator



a Select the **Network** tab; then select the **Firewall** tab.

❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator is displayed (Figure 10-14).

Figure 10-14. Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator

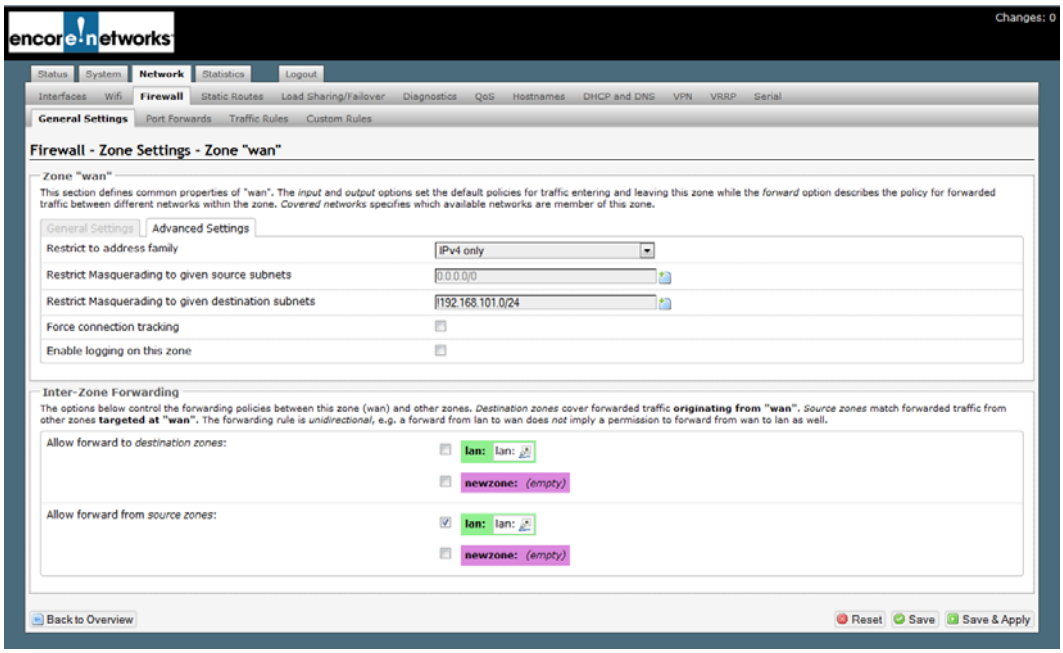


b On the Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator, check **Masquerading** for the WAN **Zone** (the lower **Zone** in Figure 10-14).

c On that same screen, select the **Edit** button for the WAN **Zone**.

❖ The Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator is displayed (Figure 10-15).

Figure 10-15. Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator



d On the Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator, specify **!*f.g.h.i/j*** in the field **Restrict Masquerading to Given Destination Subnets**, to indicate not to use masquerading for that subnet.

Note: Make sure the exclamation point is followed by the right subnet (remote subnet) ***f.g.h.i/j*** shown on the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator (recall Figure 10-13).

e Select the **Save & Apply** button.

f On that same screen, select the **Back to Overview** button.

g On the overview screen, select the **Save & Apply** button.

h Go to *Firewall Traffic Rules*, on page 15.

10.1.3.3 Firewall Traffic Rules

For SLE to work on this IPsec VPN tunnel, we need to add and update firewall rules on the server side (responder side) of the IPsec VPN tunnel.

Note: Do not configure these rules on the initiator of the VPN tunnel.

1 On the EN-4000 management system, select the **Network** tab. Then select the **Firewall** tab and the **Traffic Rules** tab.

❖ The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder is displayed (Figure 10-16).

Figure 10-16. Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder

The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder lists several rules for monitoring traffic. We will briefly address its rules for IPsec VPNs.

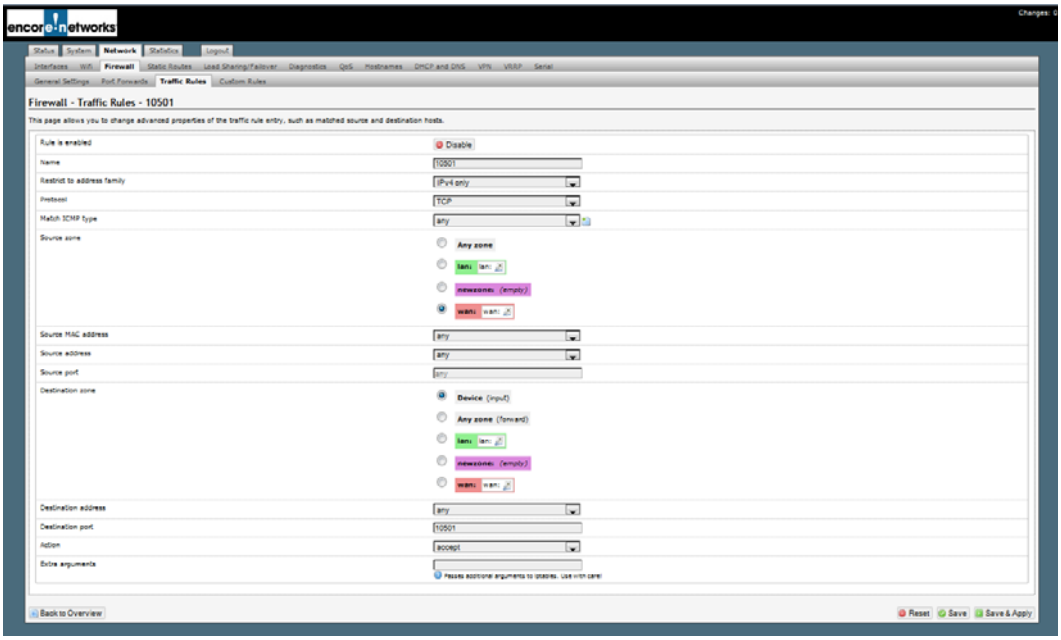
2 Do the following to add a firewall traffic rule to allow the responder side of an SLE VPN tunnel to accept all traffic on TCP port 10501 from any IP address in the WAN:

a Under the heading **Open ports on router**, type the name **TCP_10501**. (Any name can be entered for a firewall rule; this choice of name reminds us of the port number.)

b Then select the **Add** button.

❖ The Firewall Rule Configuration Screen for SLE in VPNs is displayed (Figure 10-17).

Figure 10-17. Firewall Rule Configuration Screen for SLE in VPNs
TCP_10501



c Configure the fields on this screen:

- Set **Restrict to address family** to **IPv4 only**.
- Set the **Protocol** to **TCP**.
- Leave **Match ICMP type** at **any**.
- Make sure the **Source Zone** shows that the **WAN** port is selected.
- Leave the **Source MAC address**, **Source address**, and **Source port** at **any**.
- For **Destination Zone**, select **Device**.
- Leave the **Destination Address** at **any**.
- For **Destination Port**, type the port number **10501**.
- Make sure the **Action** is to **accept** the packets.
- Leave the **Extra Arguments** field blank.

d Select the **Save & Apply** button.

❖ The rule is saved.

e Select the **Back to Overview** button.

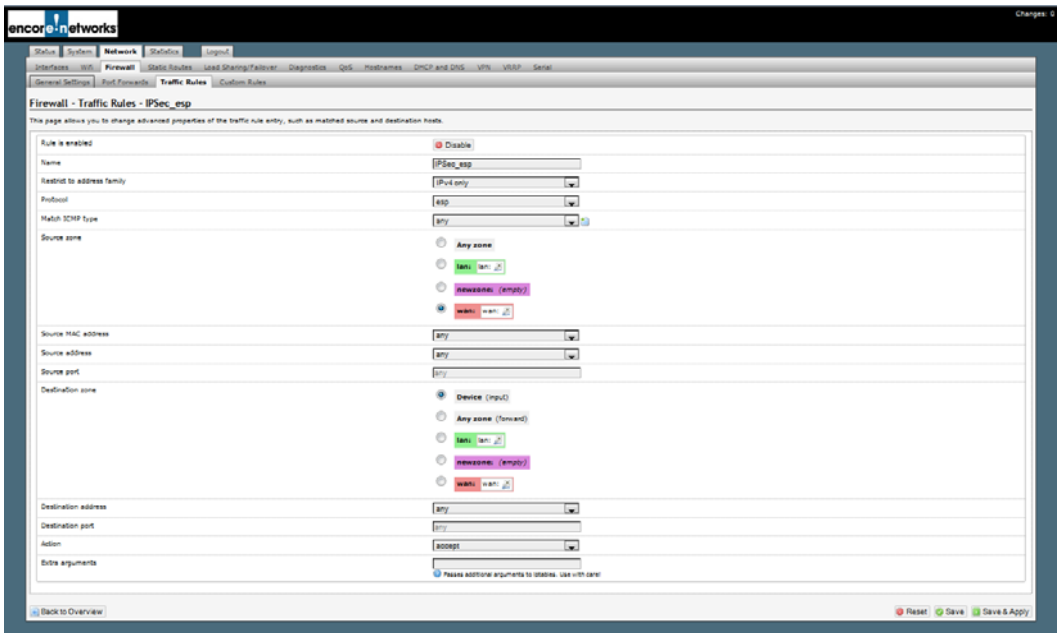
❖ The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder is redisplayed (recall Figure 10-16).

3 Repeat the procedure in step 2 for each of the following protocols:

- ESP protocol (see Figure 10-18).

  Note: For the **Destination Port**, specify **any**.

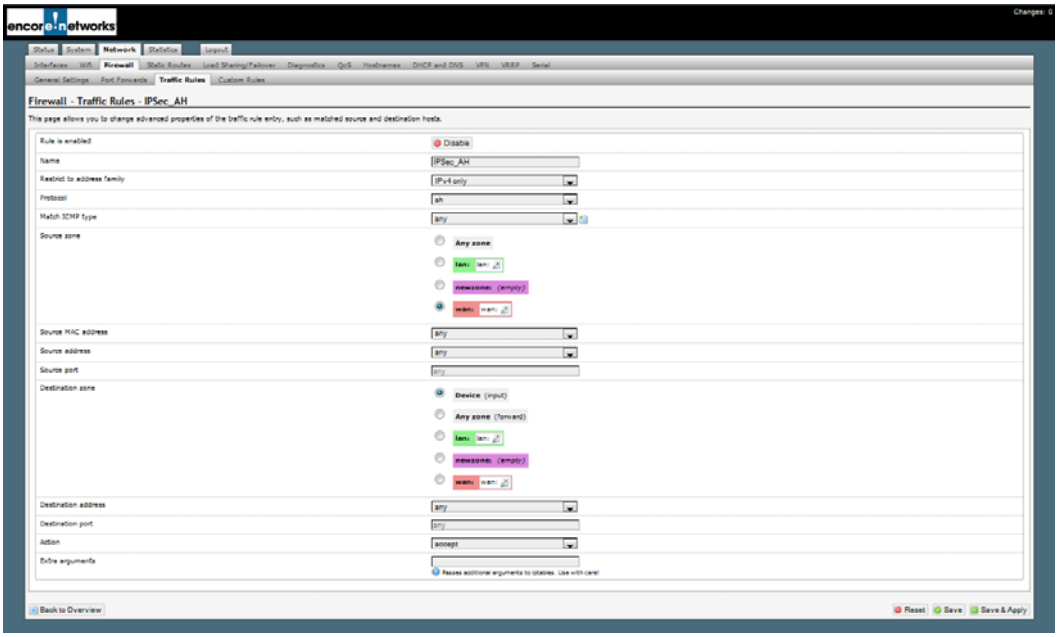
Figure 10-18. Firewall Rule Configuration Screen for VPNs
ESP protocol



- AH protocol (see Figure 10-19).

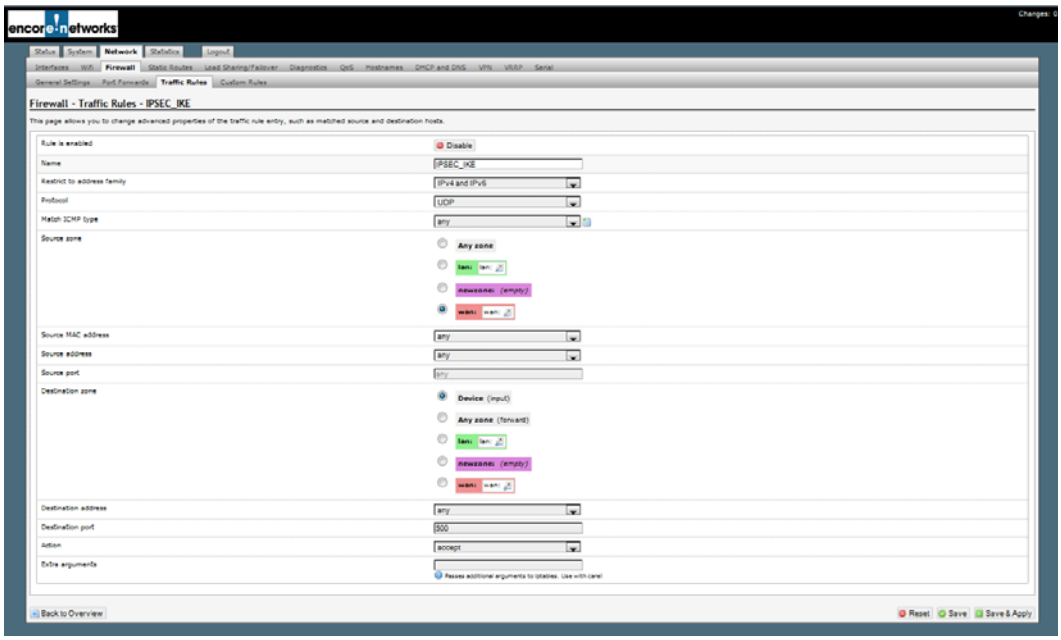
  Note: For the **Destination Port**, specify **any**.

Figure 10-19. Firewall Rule Configuration Screen for VPNs
AH protocol



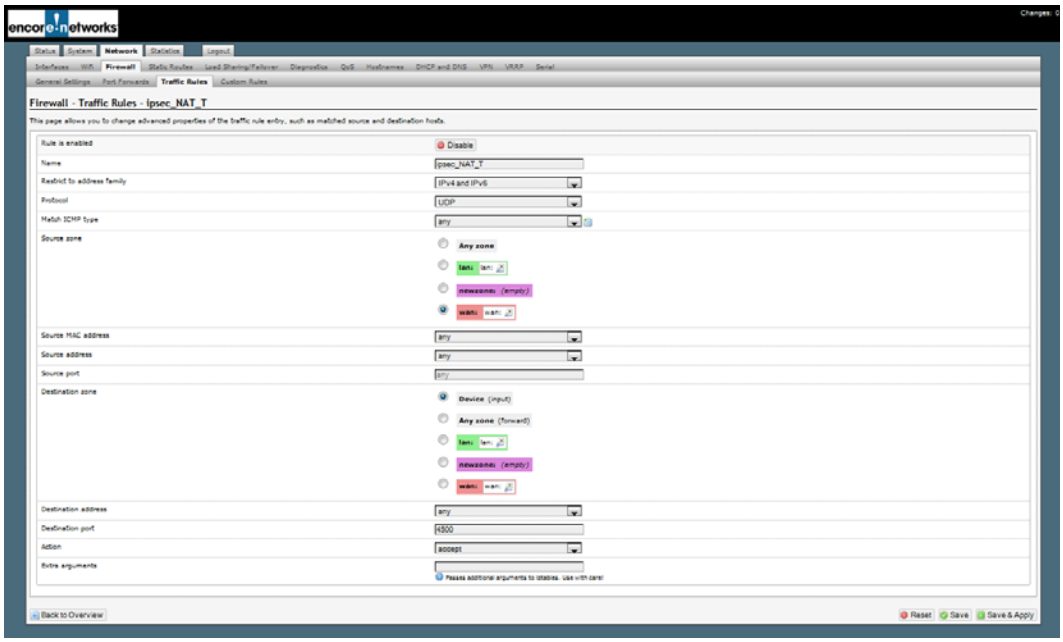
- IKE, UDP port 500 (see Figure 10-20).

Figure 10-20. Firewall Rule Configuration Screen for VPNs
IKE



- IPsec_NAT_T, UDP port 4500 (see Figure 10-21).

Figure 10-21. Firewall Rule Configuration Screen for VPNs
IPsec_NAT_T



10.1.4 Configuring the Source NAT

1 On the Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder (recall Figure 10-16), under the heading **New Source NAT** (near the bottom of the screen), type a **Name** for a new network address translation (NAT) rule.

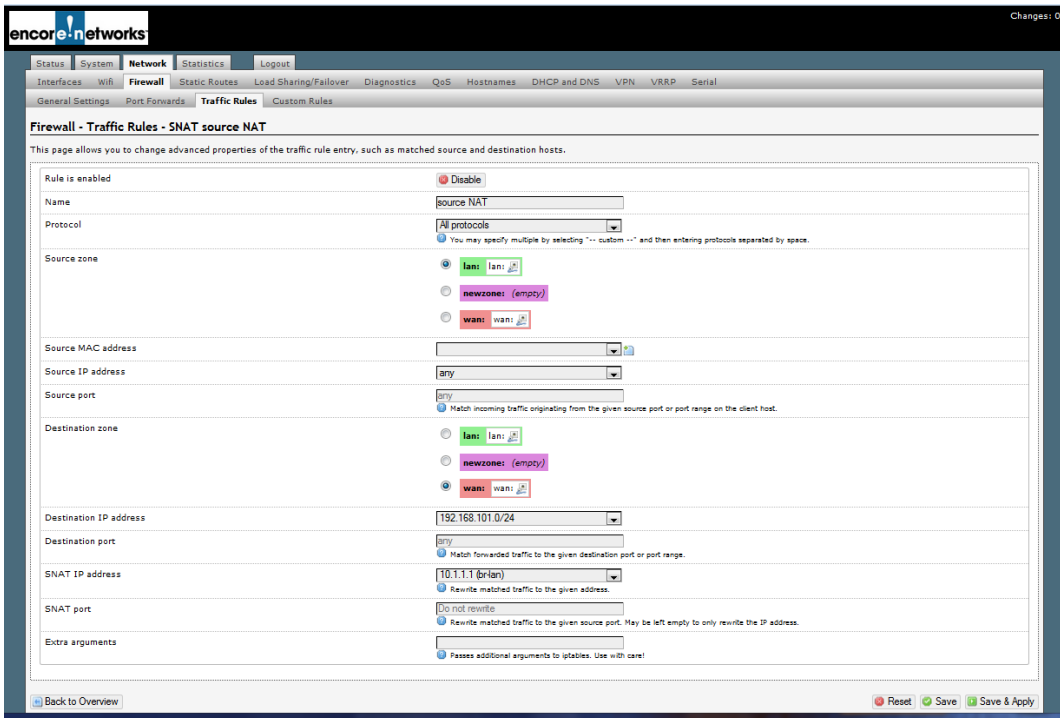
2 Make sure the following settings are used:

- **Source zone: LAN**
- **Destination zone: WAN**
- **To source IP: 10.1.1.1 (br-lan)**, selected from the field's pulldown menu

3 Then select the **Add and Edit** button.

❖ The VPN Responder's Firewall Traffic Rules Screen for a Source NAT is displayed (Figure 10-22).

Figure 10-22. VPN Responder's Firewall Traffic Rules Screen for a Source NAT



4 On that screen, make sure the following values are entered:

- **Protocol: All protocols**
- **Source zone: LAN**
- **Source IP address: any**
- **Source port: any**
- **Destination zone: WAN**
- **Destination IP address:** subnet for left (local) router
- **Destination port: any**
- **SNAT** (Source NAT) **IP address: 10.1.1.1 (br-lan)**, selected from the field's pulldown menu

5 Select the **Save & Apply** button.

6 Then select the **Back to Overview** button.

❖ The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder (recall Figure 10-16) is redisplayed.

7 On that screen, select the **Save & Apply** button.

❖ Firewall rules for the Source NAT are configured and implemented.

10.2 Verifying that SLE is Running

You can add a command to determine whether SLE is running.

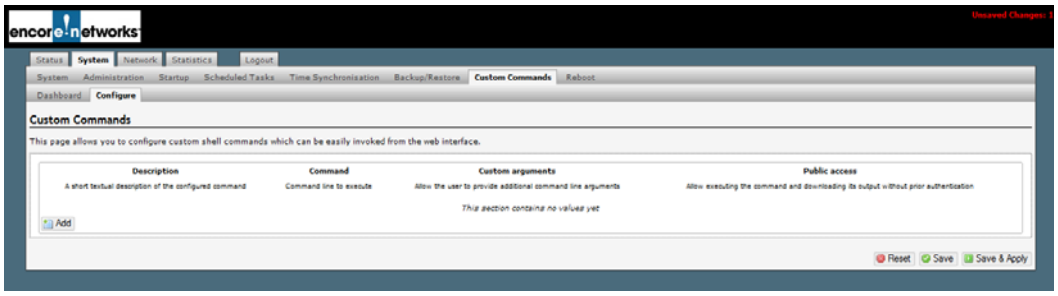
Note: Add this command to both EN-4000 routers (the initiator and the responder) in the VPN connection.

1 On the EN-4000 management system, select the **System** tab. Then select the **Custom Commands** tab.

2 Select the tab to **Configure** a command.

❖ The Custom Command Configuration Screen is displayed (Figure 10-23).

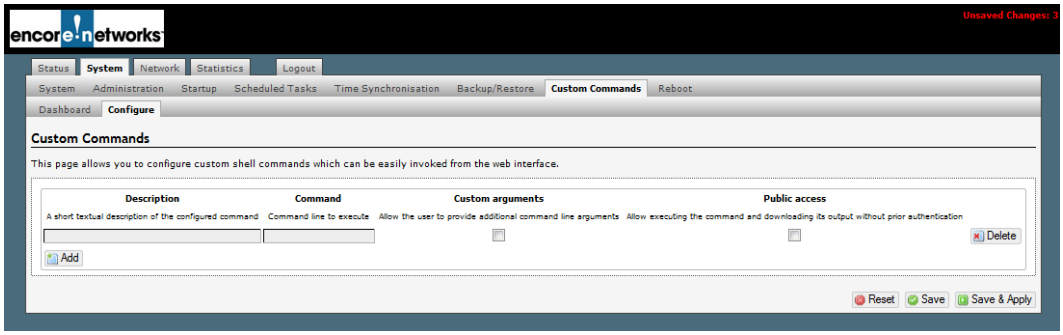
Figure 10-23. Custom Command Configuration Screen
Empty



3 Select the **Add** button (in the lower left of the screen).

❖ The Custom Command Configuration Screen to Add a Record is displayed (Figure 10-24).

Figure 10-24. Custom Command Configuration Screen to Add a Record



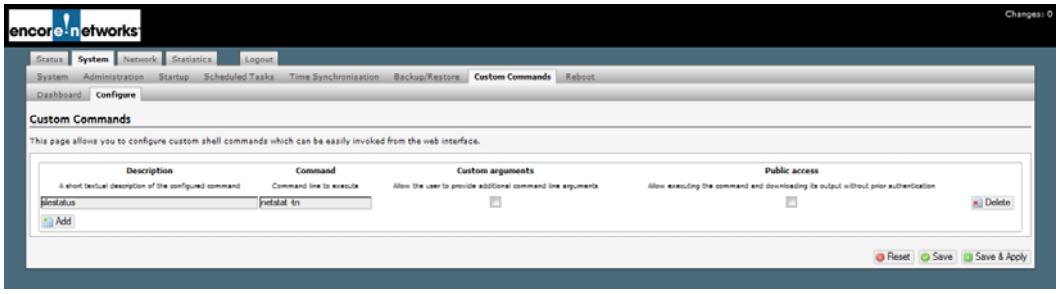
4 On that screen, enter the following values (as shown in Figure 10-25):

a In the **Description** field, type the name **slestatus**.

b In the **Command** field, type the following command:

netstat -tn

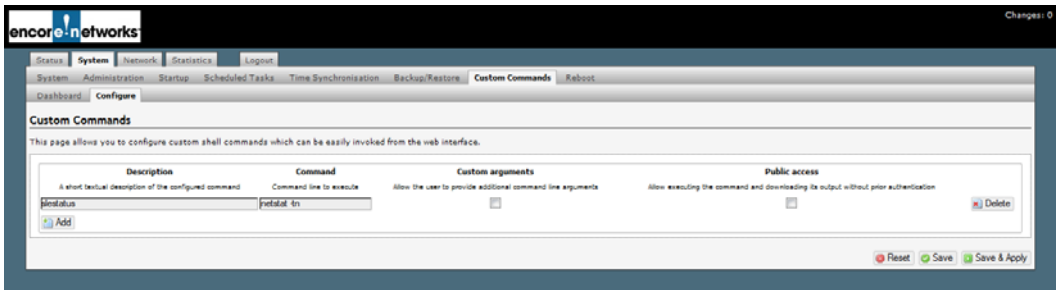
Figure 10-25. Custom Command Configuration Screen with One Entry Not Yet Saved as a Record



5 Select **Save & Apply**.

❖ The Custom Command Configuration Screen with One Record is redisplayed (Figure 10-26). The screen now represents a table (with one record, showing the new command).

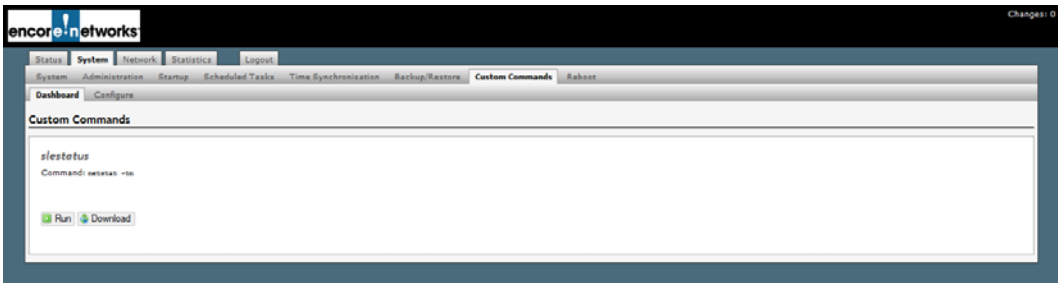
Figure 10-26. Custom Command Configuration Screen with One Record



6 On the Custom Command Configuration Screen, select the **Dashboard** tab.

❖ The Custom Command Dashboard is displayed (Figure 10-27).

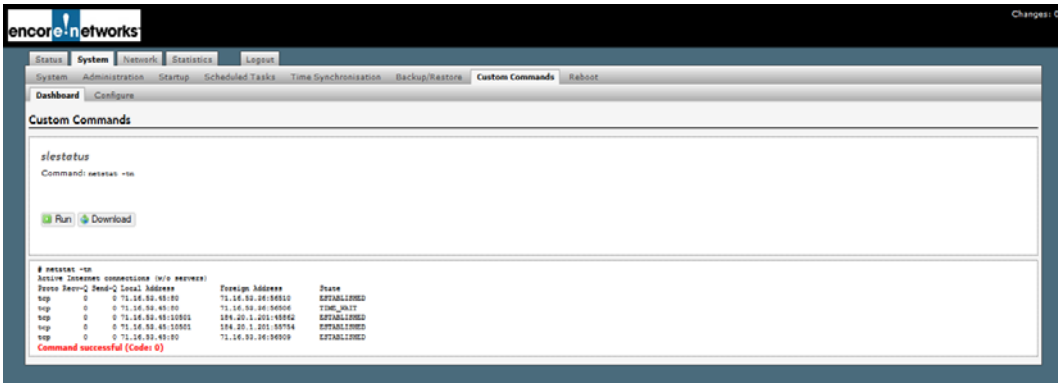
Figure 10-27. Custom Command Dashboard



7 On the Custom Command Dashboard, select the command that you configured. (If there is only one command on the dashboard, that command is automatically selected.) Then select the **Run** button.

❖ The routine checks for SLE operation and generates a report (Figure 10-28).

Figure 10-28. Report for Selected Custom Command
SLE Status



8 In the report listing, look for port number **10501**. The port should be in the **Established** state.

Note: There might be times when the VPN tunnel is attempting to connect but has not yet been established, so the report would not show an entry for port 10501. In that case, perform step 9.

9 If no entry for port 10501 is listed, rerun the command after few minutes to ensure that SLE is actually running.