
Configuring the EN-2000's VPN Firewall

This document discusses implementation of firewall rules to support IPsec VPN transmissions in the EN-2000. It presents procedures for configuring the firewall for an IPsec VPN tunnel. See the following:

- [Configuring the Firewall for an IPsec VPN Tunnel](#)
- [Configuring the Source NAT](#)

Note: In the EN-2000 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-2000.

Also see the following documents:

- [Configuring IPsec VPNs in the EN-2000](#)
- [Starting and Tracking VPNs in the EN-2000](#)
- [Virtual Private Networks](#)

10.1 Configuring the Firewall for an IPsec VPN Tunnel

The firewall for the IPsec VPN tunnel is configured on the EN-2000 that is the VPN tunnel responder. See the following:

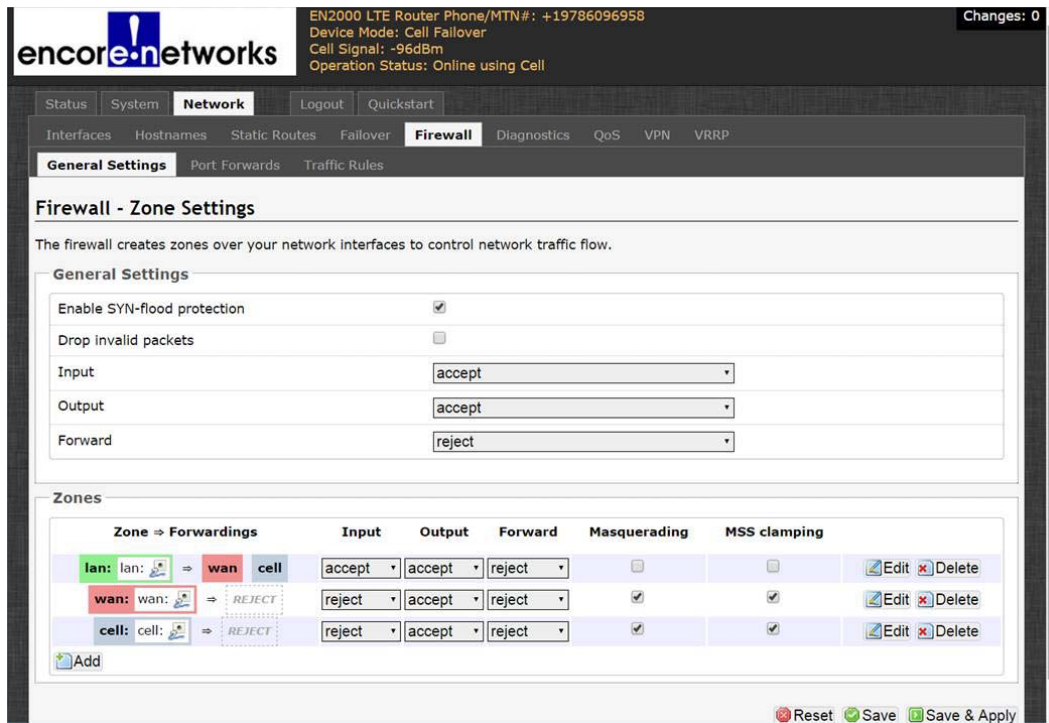
- [Firewall Zones](#)
- [Firewall Traffic Rules](#)

10.1.1 Firewall Zones

Some firewall zones require configuration changes to support IPsec VPNs.

- 1 On the EN-2000 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 10-1](#)).

Figure 10-1. Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder

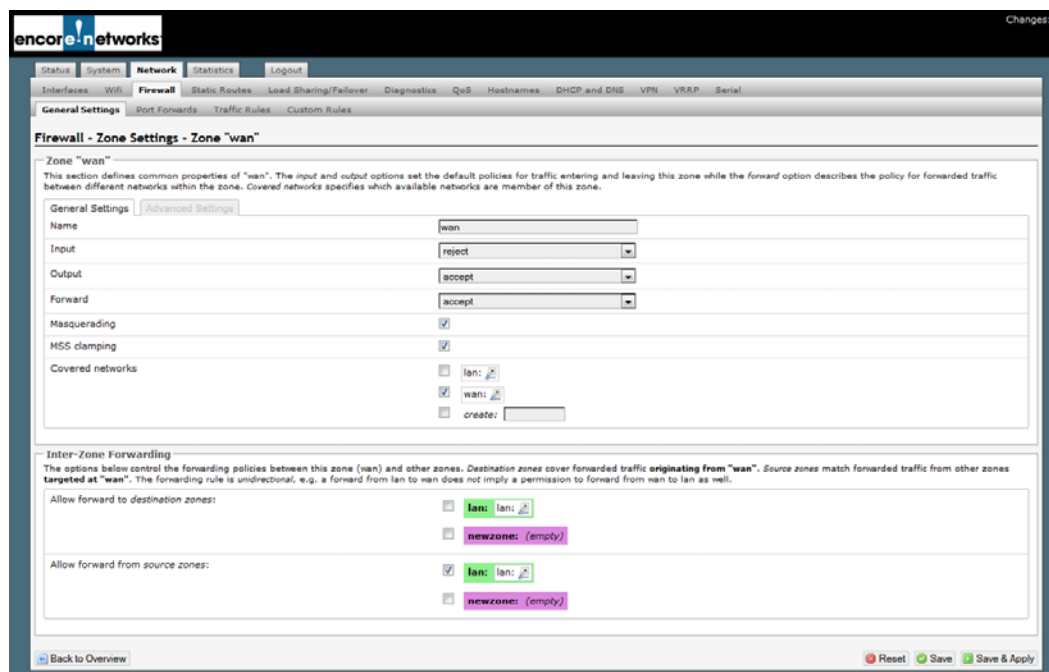


- 2 For this example, select the **Edit** button in the row for the WAN zone.

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

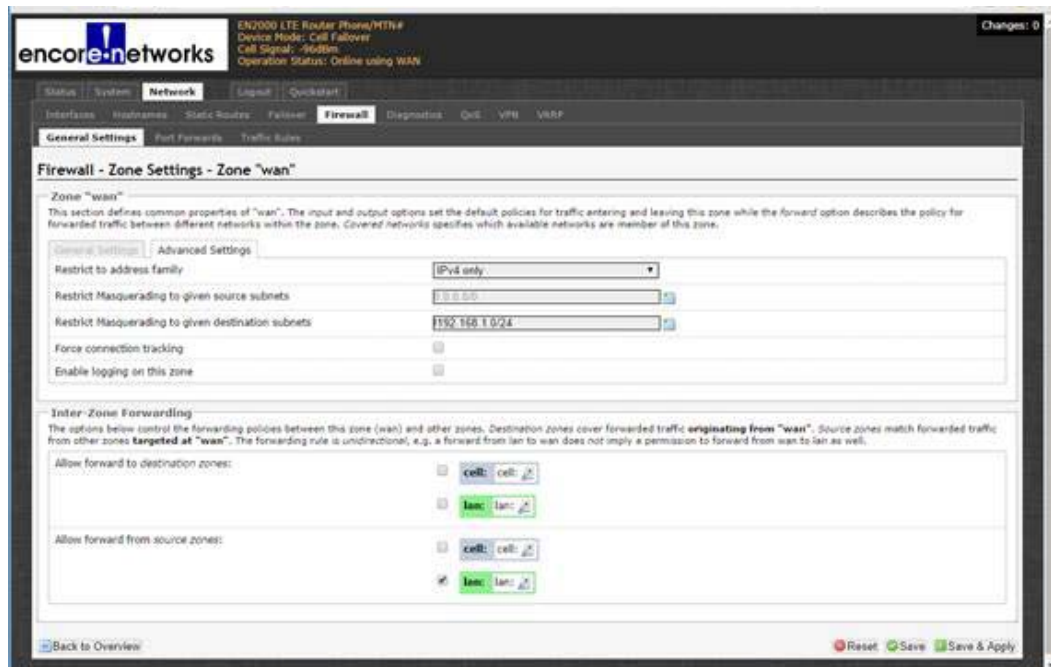
- ❖ The General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder is displayed (Figure 10-2).

Figure 10-2. General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder



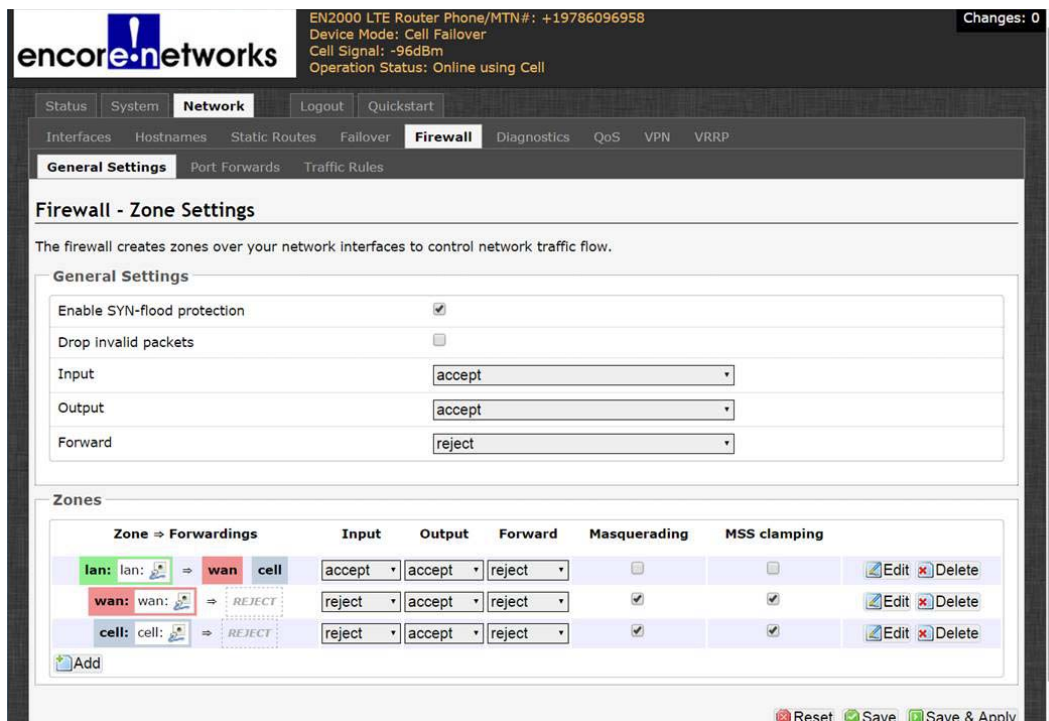
- 3 On the General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder, configure the following:
 - Under the heading **General Settings**:
 - ◆ Set **Input** to **Reject**.
 - ◆ Set **Output** to **Accept**.
 - ◆ Set **Forward** to **Accept**.
 - ◆ Enable **Masquerading**.
 - ◆ Enable **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 10-3](#)).

Figure 10-3. 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-2000.
 - ❖ 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 5.
 - 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 10-4](#)).

Figure 10-4. 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-2000 will use that zone; possibilities are for 5 GHz 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 10-1](#)).
- 12 On that screen, select the **Save and Apply** button.
- ❖ The configuration is saved and applied (restarting the firewall).

10.1.2 Disabling Masquerading on the VPN Tunnel Initiator

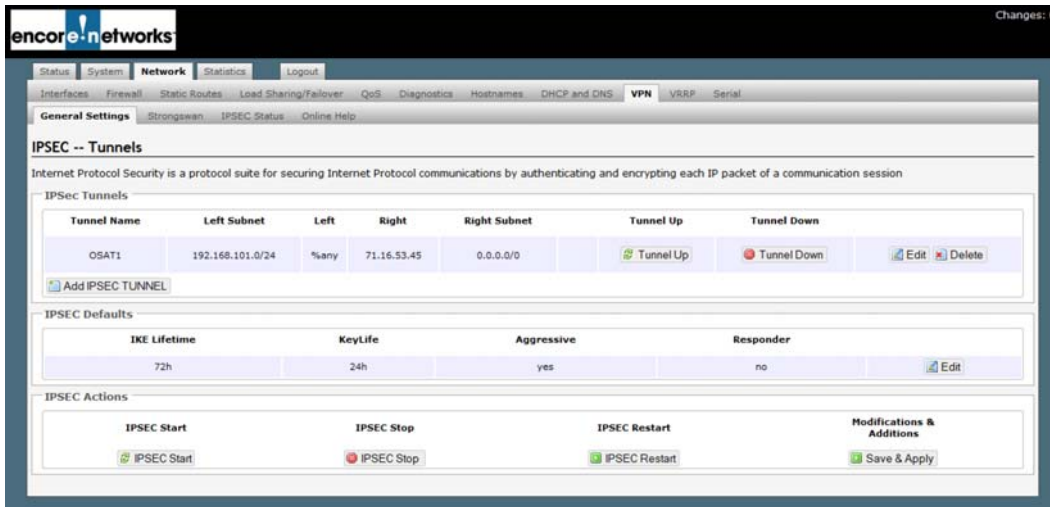
There are two ways to disable masquerading on the initiator of the VPN tunnel, depending on the initiator's right subnet.

! **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](#).

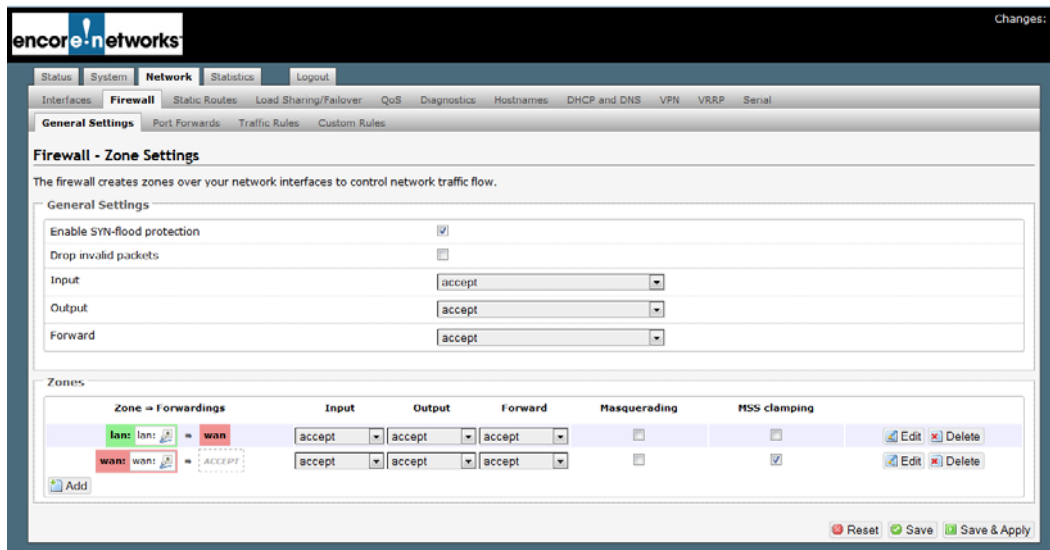
-
- 1 If the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator specifies a **Right Subnet** of **0.0.0.0/0**, indicating all remote locations (as shown in [Figure 10-5](#)), do the following:

Figure 10-5. IPsec VPN Tunnel Screen for a VPN Tunnel Initiator
Right Subnet 0.0.0.0/0



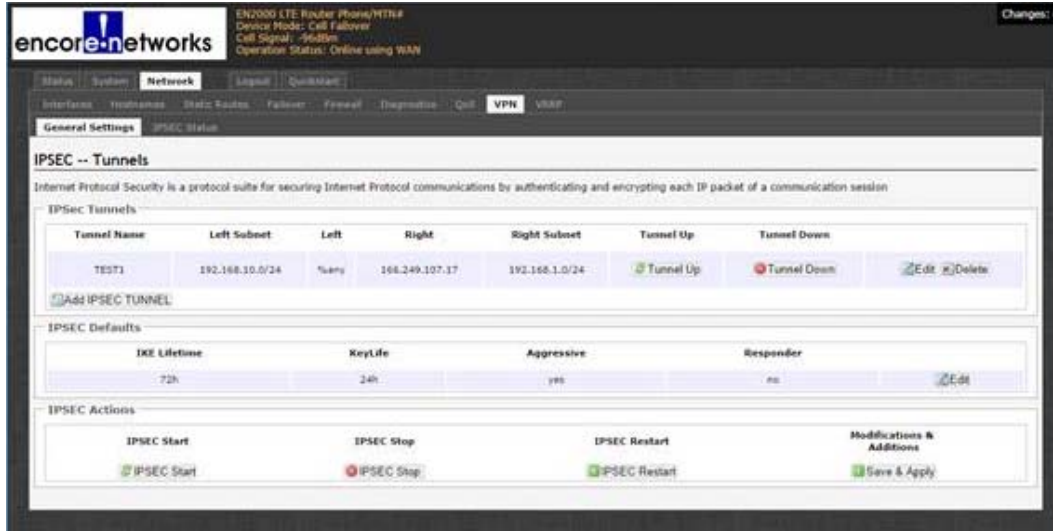
- a Select the **Network** tab; then select the **Firewall** tab.
- ❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator is displayed (Figure 10-6).

Figure 10-6. Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator
Right Subnet 0.0.0.0/0



- 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 8.
- 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 10-7](#), the sample right subnet is 192.168.101.0/24), do the following:

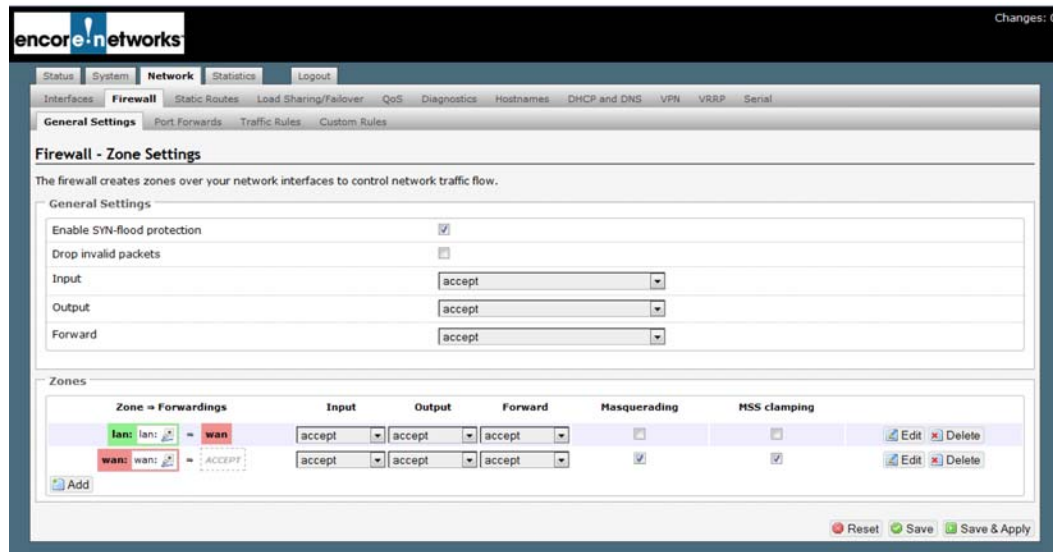
Figure 10-7. IPsec VPN Tunnel Screen for a VPN Tunnel Initiator
Right Subnet Not 0.0.0.0/0



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

- ❖ The Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator is displayed (Figure 10-8).

Figure 10-8. Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator
Right Subnet Not 0.0.0.0/0

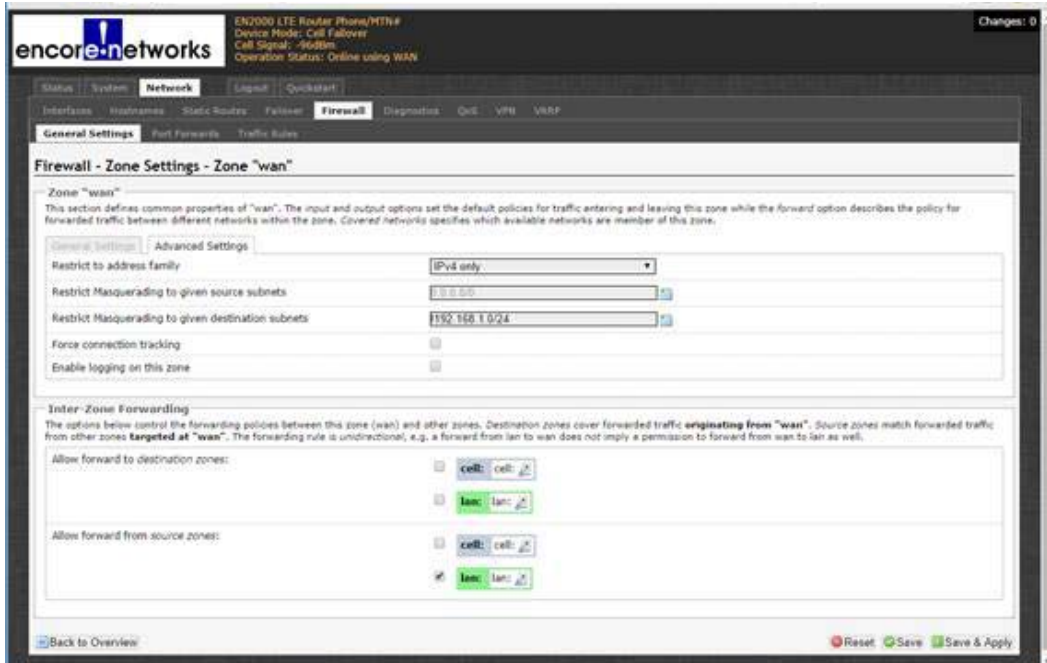


b On the Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator, check **Masquerading** for the WAN Zone (the lower Zone in Figure 10-8).

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 10-9).

Figure 10-9. 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 an exclamation point precedes the right subnet (remote subnet) **f.g.h.i/j** shown on the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator (recall [Figure 10-7](#)).

- 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 8.

10.1.3 Firewall Traffic Rules

For 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-2000 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 10-10](#)).

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

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From any host in any zone To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-TCP-HTTPS	IPv4-TCP From any host in any zone To any router IP at port 443 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-TCP-SSH	IPv4-TCP From any host in any zone To any router IP at port 22 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-Ping	IPv4-ICMP with type echo-request From any host in any zone To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
IPsec_csp	IPv4 IPSEC ESP From any host in any zone To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Auth_Header	IPv4-IPSEC-AH From any host in any zone To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
IPSEC_IKE	IPv4-UDP From any host in cell To any router IP at port 500 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Ipsec_NAT_T	IPv4-UDP From any host in cell To any router IP at port 4500 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	-- Please choce	Do not rewrite

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 for the ESP protocol, to allow the responder side of a VPN tunnel to accept traffic on the TCP port from any IP address in the WAN:
 - a Under the heading **Open ports on router**, type the name **ESP protocol**. (Any name can be entered for a firewall rule; this choice of name reminds us of the function.)
 - b Then select the **Add** button.
 - ❖ The Firewall Rule Configuration Screen for VPNs is displayed (Figure 10-11).

Figure 10-11. Firewall Rule Configuration Screen for VPNs
ESP protocol

The screenshot shows the 'Firewall - Traffic Rules - IPsec_esp' configuration page. The rule is enabled. The configuration is as follows:

- Name:** IPsec_esp
- Restrict to address family:** IPv4 only
- Protocol:** esp
- Match ICMP type:** any
- Source zone:** wan (selected)
- Source MAC address:** any
- Source address:** any
- Source port:** any
- Destination zone:** Device (input) (selected)
- Destination address:** any
- Destination port:** any
- Action:** accept
- Extra arguments:** (blank)

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

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**, leave the port number as **any**.
- 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 10-10](#)).

3 Repeat the procedure in [step 2](#) for each of the following protocols:

- AH protocol (see [Figure 10-12](#)).

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

Figure 10-12. Firewall Rule Configuration Screen for VPNs
AH protocol

Firewall - Traffic Rules - Auth_header

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled Disable

Name: Auth_header

Restrict to address family: IPv4 only

Protocol: ah

Match ICMP type: any

Source zone: Any zone (selected), cell, lan, wan

Source MAC address: any

Source address: any

Source port: any

Destination zone: Device (input) (selected), Any zone (forward), cell, lan, wan

Destination address: any

Destination port: any

Action: accept

Extra arguments:

Passes additional arguments to iptables. Use with care!

Buttons: Back to Overview, Reset, Save, Save & Apply

- IKE, UDP port 500 (see [Figure 10-13](#)).

Figure 10-13. Firewall Rule Configuration Screen for VPNs
IKE

Firewall - Traffic Rules - IPSEC_IKE

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled Disable

Name: IPSEC_IKE

Restrict to address family: IPv4 only

Protocol: UDP

Match ICMP type: any

Source zone: Any zone (selected), cell, lan, wan

Source MAC address: any

Source address: any

Source port: any

Destination zone: Device (input) (selected), Any zone (forward), cell, lan, wan

Destination address: any

Destination port: 500

Action: accept

Extra arguments:

Passes additional arguments to iptables. Use with care!

Buttons: Back to Overview, Reset, Save, Save & Apply

- IPsec_NAT_T, UDP port 4500 (see [Figure 10-14](#)).

Figure 10-14. Firewall Rule Configuration Screen for VPNs
IPsec_NAT_T

Firewall - Traffic Rules - ipsec_NAT_T

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled Disable

Name: ipsec_NAT_T

Restrict to address family: IP4 only

Protocol: UDP

Match ICMP type: any

Source zone:

- Any zone
- cell: cell
- lan: lan
- wan: wan

Source MAC address: any

Source address: any

Source port: any

Destination zone:

- Device (input)
- Any zone (forward)
- cell: cell
- lan: lan
- wan: wan

Destination address: any

Destination port: 4500

Action: accept

Extra arguments: Passes additional arguments to iptables. Use with care!

[Back to Overview](#)

10.2 Configuring the Source NAT

- 1 On the Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder (recall [Figure 10-10](#)), 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 10-15](#)).

Figure 10-15. VPN Responder's Firewall Traffic Rules Screen for a Source NAT

The screenshot shows the 'Firewall - Traffic Rules - SNAT source NAT' configuration page. The rule is currently disabled. The configuration details are as follows:

- Rule is enabled:** (Disabled)
- Name:** source NAT
- Protocol:** All protocols
- Source zone:** lan: lan: 192.168.101.0/24
- Source MAC address:** (empty)
- Source IP address:** any
- Source port:** any
- Destination zone:** wan: wan: 192.168.101.0/24
- Destination IP address:** 192.168.101.0/24
- Destination port:** any
- SNAT IP address:** 10.1.1.1 (br-lan)
- SNAT port:** Do not rewrite
- Extra arguments:** (empty)

Buttons at the bottom include 'Back to Overview', 'Reset', 'Save', and 'Save & Apply'.

- 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 10-10](#)) is redisplayed.
- 7 On that screen, select the **Save & Apply** button.
 - ❖ Firewall rules for the Source NAT are configured and implemented.

