Configuring EN™ Routers for OpenVPN®

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses configuration of an OpenVPN® connection.[1]

If the EN™ router is using the latest version of firmware, OpenVPN® is included in the router's functions. Depending on the firmware in your router, screens displayed may differ slightly from screens shown in this document.

> **Note:** To upgrade an EN™ router's firmware image, follow the instructions in Section E.3.2.2, *Loading a Software Upgrade*, on page 11 of the document *EN-2000 System Administration*. (Those instructions for upgrading firmware apply to all EN™ Routers.)

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 OpenVPN® connections, confer with your network administrator.

See the following sections:

- Section 5.1, *Network Interfaces*, on page 2
- Section 5.2, *Alternate Creation of a VPN Interface*, on page 6
- Section 5.3, *List of OpenVPN® Instances*, on page 9
- Section 5.4, *Configuring an OpenVPN® Connection*, on page 10. This section includes the router's assignment of an OpenVPN® server or client certificate, depending on the router's role in the OpenVPN® connection.

  Note: For certificate information, see the document *Generating Certificates for OpenVPN® Connections*.

[1] OpenVPN® uses transport layer security (TLS, successor to secure socket layers, SSL). For information about VPNs that use IP security (IPsec), see one of the following documents:
- *Configuring IPsec VPNs in the EN-1000™*
- *Configuring IPsec VPNs in the EN-2000™*
- *The EN-4000™ in IPsec Virtual Private Networks*

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

- Section 5.5, *Firewall Configuration for OpenVPN®*, on page 16
- Section 5.6, *More Information*, on page 18

Note: The VPN client in the OpenVPN® connection needs three certificates for the VPN connection; the VPN server in the OpenVPN® connection needs four certificates.

To create and authenticate customized certificates for OpenVPN®, see the document *Generating Certificates for OpenVPN® Connections*. After the certificates have been generated for your OpenVPN® connections, the certificates can be downloaded to the EN™ router. (That download is described in step 11 on page 14 through page 15 of Section 5.4, *Configuring an OpenVPN® Connection*, in the current document.)

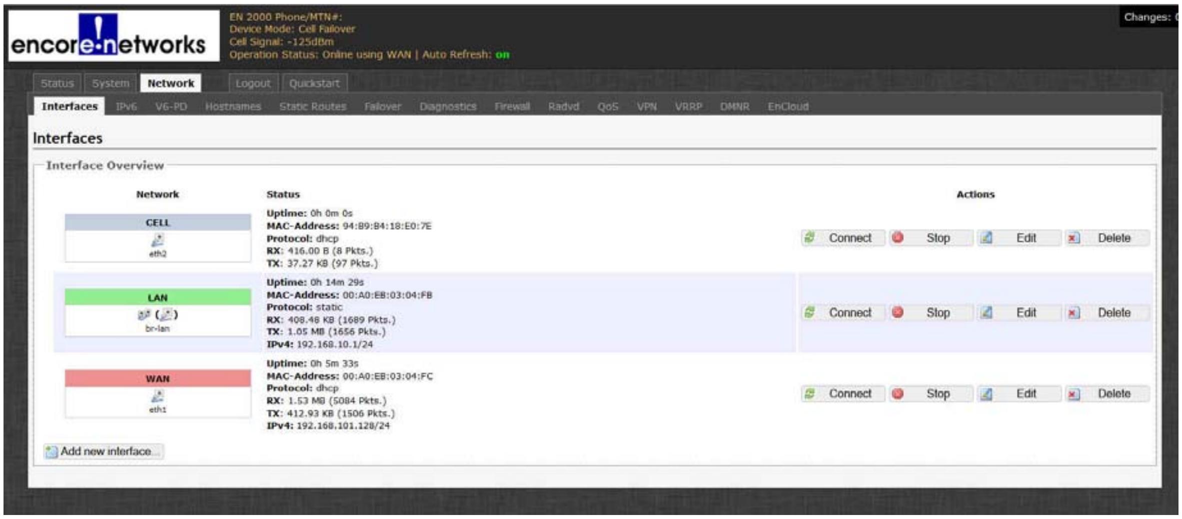
5.1 Network Interfaces

First, create a VPN interface:

1 Log into your EN™ Router. Select the tab **Network**; then select the tab **Interfaces**.

❖ The List of Network Interfaces is displayed (Figure 5-1).

Figure 5-1. List of Network Interfaces



EN 2000 Phone/MTN#:
Device Mode: Cell Failover
Cell Signal: -125dBm
Operation Status: Online using WAN | Auto Refresh: on

Interfaces

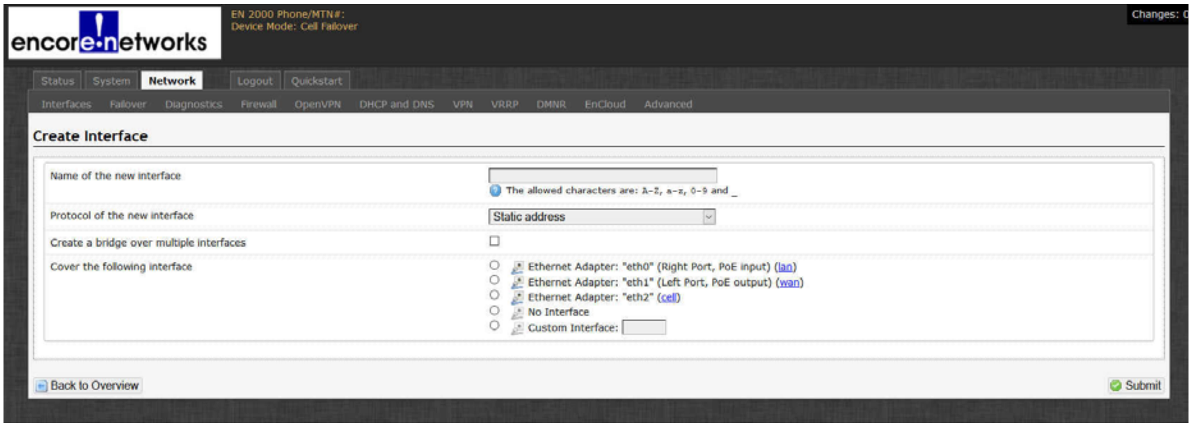
Interface Overview

Network	Status	Actions
CELL eth2	**Uptime:** 0h 0m 0s **MAC-Address:** 94:B9:B4:18:E0:7E **Protocol:** dhcp **RX:** 416.00 B (8 Pkts.) **TX:** 37.27 KB (97 Pkts.)	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 0h 14m 29s **MAC-Address:** 00:A0:EB:03:04:FB **Protocol:** static **RX:** 408.48 KB (1689 Pkts.) **TX:** 1.05 MB (1656 Pkts.) **IPv4:** 192.168.10.1/24	Connect Stop Edit Delete
WAN eth1	**Uptime:** 0h 5m 33s **MAC-Address:** 00:A0:EB:03:04:FC **Protocol:** dhcp **RX:** 1.53 MB (5084 Pkts.) **TX:** 412.93 KB (1506 Pkts.) **IPv4:** 192.168.101.128/24	Connect Stop Edit Delete

2 Select the button to **Add New Interface** (at the lower left corner of the screen).

❖ The screen to Create a Network Interface is displayed (Figure 5-2).

Figure 5-2. Create a Network Interface

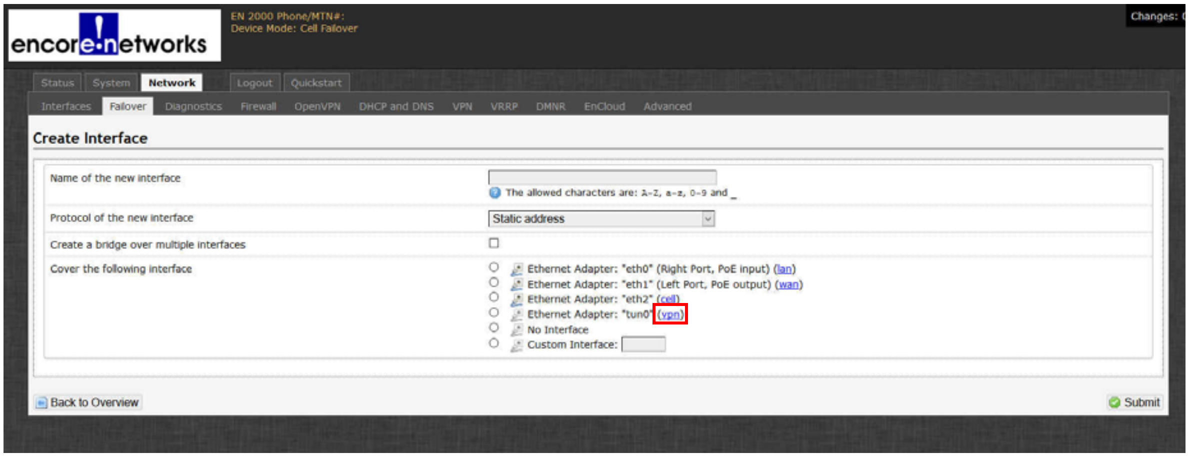


Create Interface

Name of the new interface	The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface	Static address
Create a bridge over multiple interfaces	□
Cover the following interface	○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan) ○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan) ○ Ethernet Adapter: "eth2" (cell) ○ No Interface ○ Custom Interface:

Note: The screen might include **vpn** (surrounded by a red rectangle in Figure 5-3) in the screen's list to **Cover the Following Interface**. If that is the case, go to Section 5.2, *Alternate Creation of a VPN Interface*, on page 6.

Figure 5-3. Create a New Interface, VPN Listed



Create Interface

Name of the new interface	The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface	Static address
Create a bridge over multiple interfaces	□
Cover the following interface	○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan) ○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan) ○ Ethernet Adapter: "eth2" (cell) ○ Ethernet Adapter: "tun0" (vpn) ○ No Interface ○ Custom Interface:

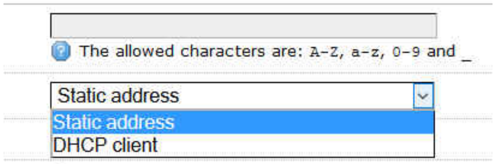
3 If the screen to Create a Network Interface does not include **vpn** (recall Figure 5-2), assign the following values:

• **Name of new interface:**	**VPN1**	(Use any unique name.)
• **Custom Interface:**	**tun0**	(Use any unique name.)
• **Protocol for the new interface:**	**Unmanaged**	(This value is required.)

4 Do one of the following:

a If the interface protocol option **unmanaged** is not listed (Figure 5-4), go to Section 5.2, *Alternate Creation of a VPN Interface*, on page 6.

Figure 5-4. List of Interface Protocol Options
(Option for "unmanaged" not listed)

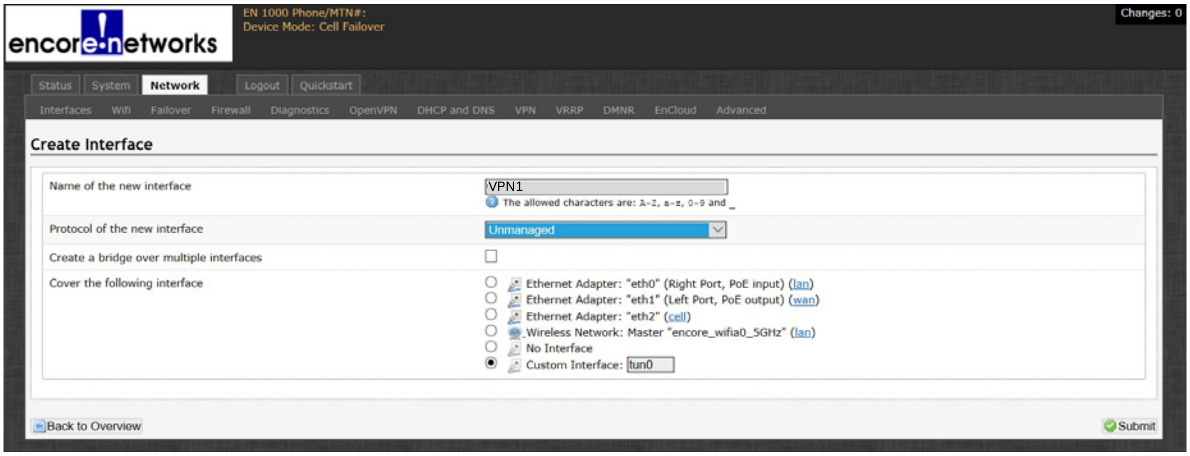


The allowed characters are: A-Z, a-z, 0-9 and _

b If the list of interface protocol options (Figure 5-4) includes the option **unmanaged**, select it.

❖ The screen to Create a Network Interface is displayed. Figure 5-5 indicates that the protocol interface is **unmanaged**.

Figure 5-5. Network Interface Ready for Submission



EN 1000 Phone/MTN#:
Device Mode: Cell Failover

Create Interface

Name of the new interface: VPN1
The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Unmanaged

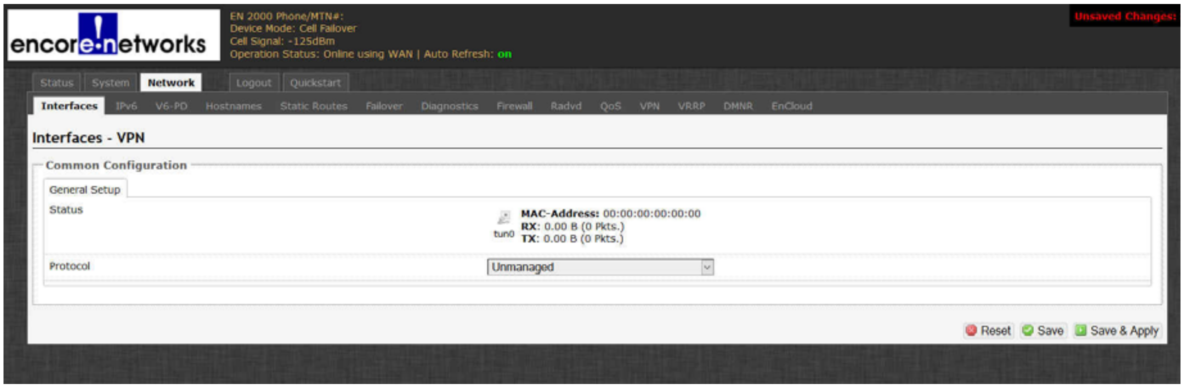
Create a bridge over multiple interfaces: □

Cover the following interface:
○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan)
○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan)
○ Ethernet Adapter: "eth2" (cell)
○ Wireless Network: Master "encore_wifia0_5GHz" (lan)
○ No Interface
● Custom Interface: tun0

5 Select the screen's button to **Submit** the interface (in the lower right corner of the screen).

❖ The screen develops the interface and presents it for confirmation (Figure 5-6).

Figure 5-6. Confirmation Screen for New Interface



EN 2000 Phone/MTN#:
Device Mode: Cell Failover
Cell Signal: -125dBm
Operation Status: Online using WAN | Auto Refresh: on

Interfaces - VPN

Common Configuration

Status: tun0 **MAC-Address:** 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol: Unmanaged

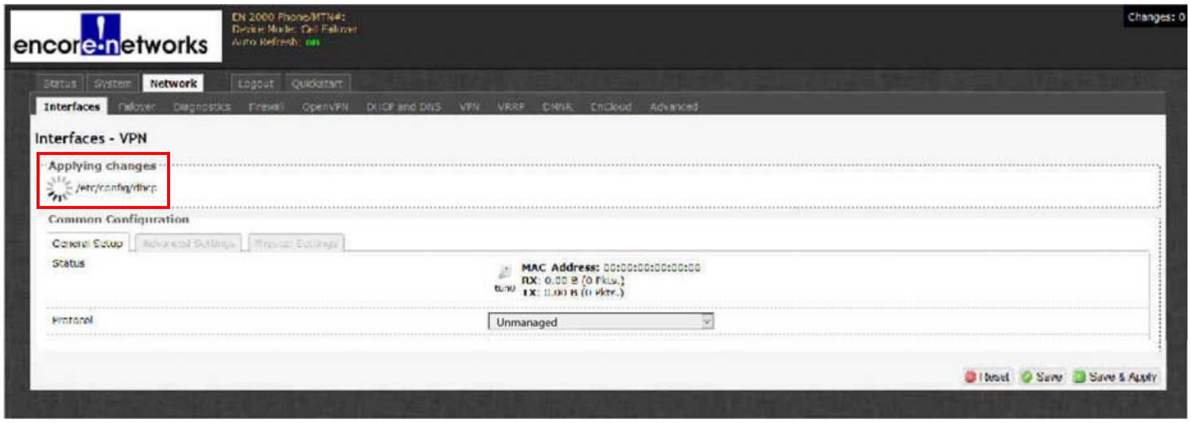
Note: The values displayed on the confirmation screen at this point are merely placeholders.

- If the EN™ Router is being configured as a *server*, the tunnel will show an IP address after the VPN configuration has been completed. The VPN tunnel's IP address will reflect the server's configured IP address.
- If the EN™ Router is being configured as a *client*, the IP address for the tunnel interface will show up only when the VPN tunnel is up.

6 After review of the new interface's values, select the **Save & Apply** button.

❖ The EN™ system creates the interface. (Note the spinning circle near the upper left of Figure 5-7, under **Applying changes**.)

Figure 5-7. Creating an Interface



EN 2000 Phone/MTN#:
Device Mode: Cell Failover
Auto Refresh: on

Interfaces - VPN

Applying changes
/etc/config/dhcp

Common Configuration

Status: tun0 MAC Address: 00:00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

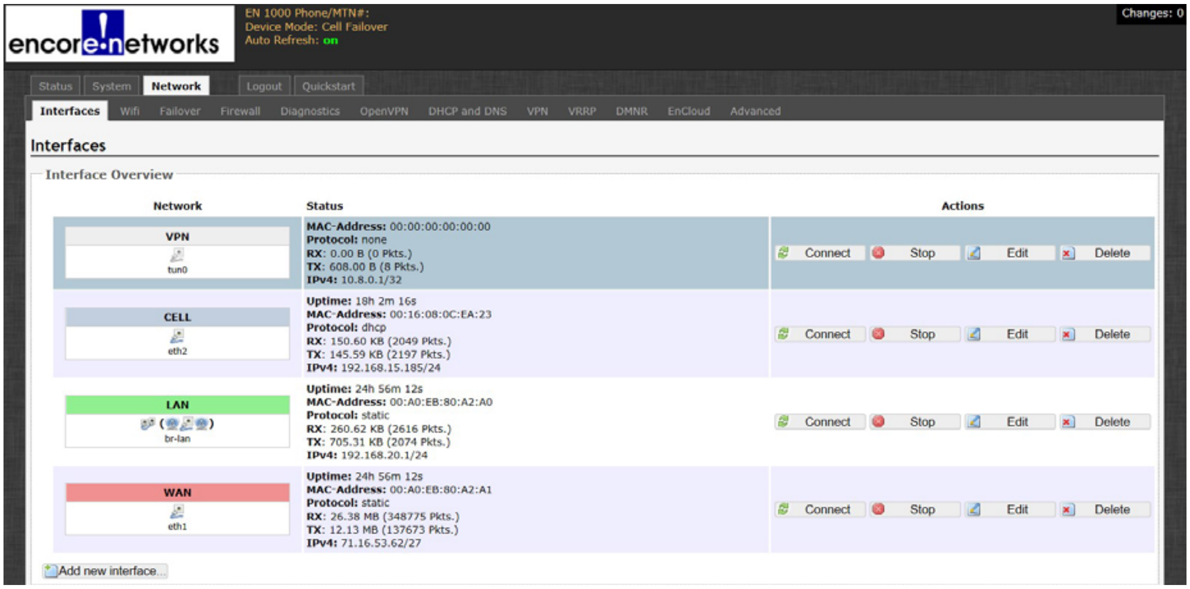
Protocol: Unmanaged

- ❖ After the circle quits spinning, the interface confirmation screen is displayed again.

7 After the interface confirmation screen is displayed again, select the tabs **Network**, **Interface**.

- ❖ The List of Network Interfaces is redisplayed, including the VPN interface you just created (in the top row of Figure 5-8).

Figure 5-8. List of Network Interfaces



EN 1000 Phone/MTN#:
Device Mode: Cell Failover
Auto Refresh: on

Interfaces

Interface Overview

Network	Status	Actions
VPN tun0	**MAC-Address:** 00:00:00:00:00:00 **Protocol:** none **RX:** 0.00 B (0 Pkts.) **TX:** 608.00 B (8 Pkts.) **IPv4:** 10.8.0.1/32	Connect Stop Edit Delete
CELL eth2	**Uptime:** 18h 2m 16s **MAC-Address:** 00:16:08:0C:EA:23 **Protocol:** dhcp **RX:** 150.60 KB (2049 Pkts.) **TX:** 145.59 KB (2197 Pkts.) **IPv4:** 192.168.15.185/24	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 24h 56m 12s **MAC-Address:** 00:A0:EB:80:A2:A0 **Protocol:** static **RX:** 260.62 KB (2616 Pkts.) **TX:** 705.31 KB (2074 Pkts.) **IPv4:** 192.168.20.1/24	Connect Stop Edit Delete
WAN eth1	**Uptime:** 24h 56m 12s **MAC-Address:** 00:A0:EB:80:A2:A1 **Protocol:** static **RX:** 26.38 MB (348775 Pkts.) **TX:** 12.13 MB (137673 Pkts.) **IPv4:** 71.16.53.62/27	Connect Stop Edit Delete

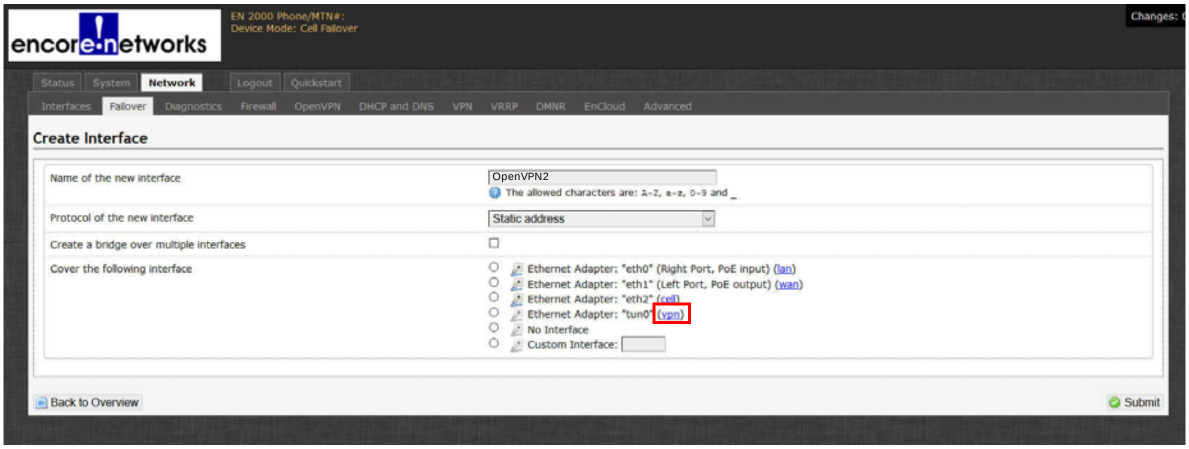
8 Study Section 5.3, *List of OpenVPN® Instances*, on page 9. Then proceed to Section 5.4, *Configuring an OpenVPN® Connection*, on page 10.

5.2 Alternate Creation of a VPN Interface

If the screen to Create a Network Interface does not include the interface protocol **unmanaged** (recall Figure 5-4, on page 3), follow the steps in this section to create a VPN interface.

1 Type the **Name of the new interface**—for example, **OpenVPN2** (Figure 5-9). (Use any unique name.)

Figure 5-9. Create a New Interface, VPN Listed



Create Interface

Name of the new interface: OpenVPN2
The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Static address

Create a bridge over multiple interfaces: □

Cover the following interface:
○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan)
○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan)
○ Ethernet Adapter: "eth2" (cell)
○ Ethernet Adapter: "tun0" (vpn)
○ No Interface
○ Custom Interface:

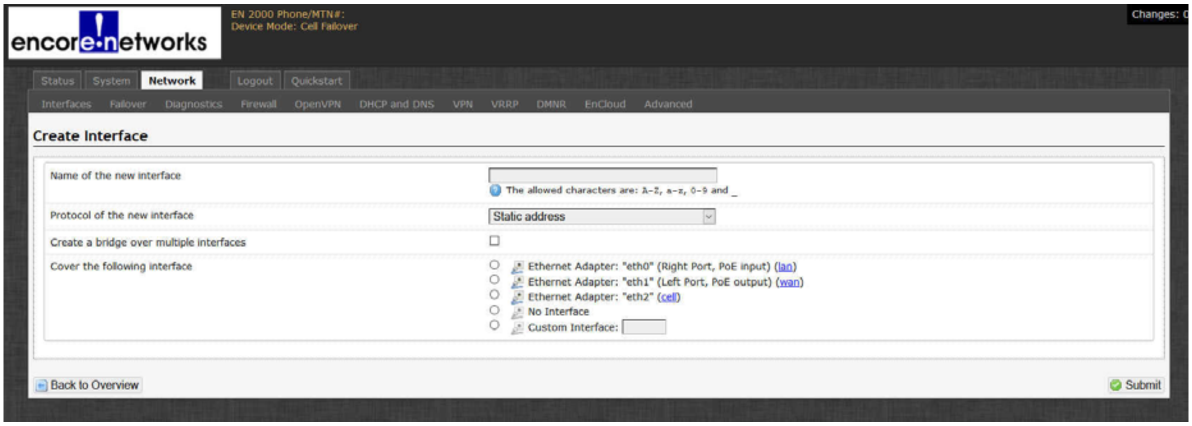
2 Do one of the following:

a If the screen includes **vpn** (surrounded by a red rectangle in Figure 5-9) in its list to **Cover the Following Interface**, select the checkbox for that interface.

❖ The Common Configuration Screen for interfaces is displayed (Figure 5-12, on page 7). The upper left title for that screen shows **Interfaces - VPN**. Go to step 3, on page 7.

b If the screen does not includes **vpn** in its list to **Cover the Following Interface** (Figure 5-10), enter an interface type (for example, **tun0**) in the field **Custom Interface**.

Figure 5-10. Initial Screen to Create Interface
(No unmanaged protocol available)



Create Interface

Name of the new interface:
The allowed characters are: A-Z, a-z, 0-9 and _

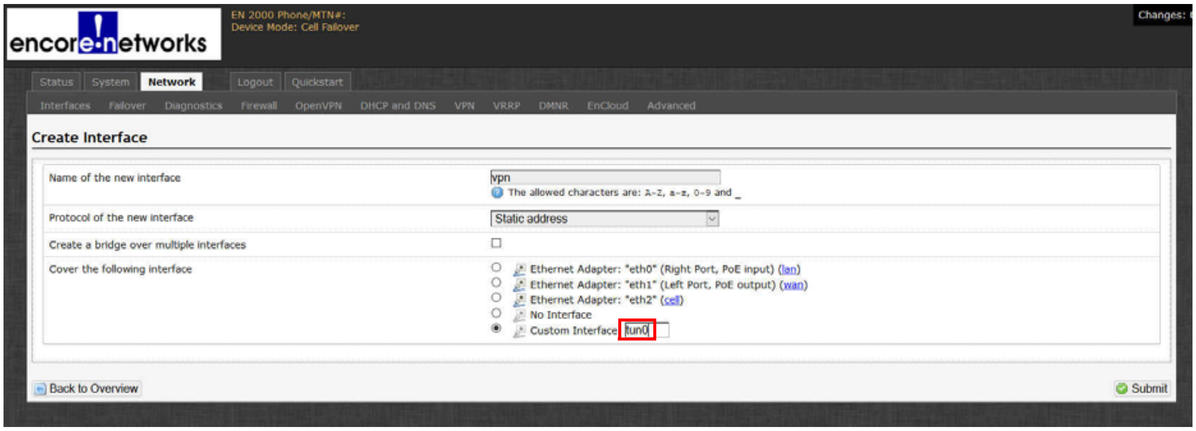
Protocol of the new interface: Static address

Create a bridge over multiple interfaces: □

Cover the following interface:
○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan)
○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan)
○ Ethernet Adapter: "eth2" (cell)
○ No Interface
○ Custom Interface:

Note: Figure 5-11 shows the interface type **tun0**.

Figure 5-11. Creating a Custom Interface



EN 2000 Phone/MTN#:
Device Mode: Cell Failover

Create Interface

Name of the new interface: vpn
The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Static address

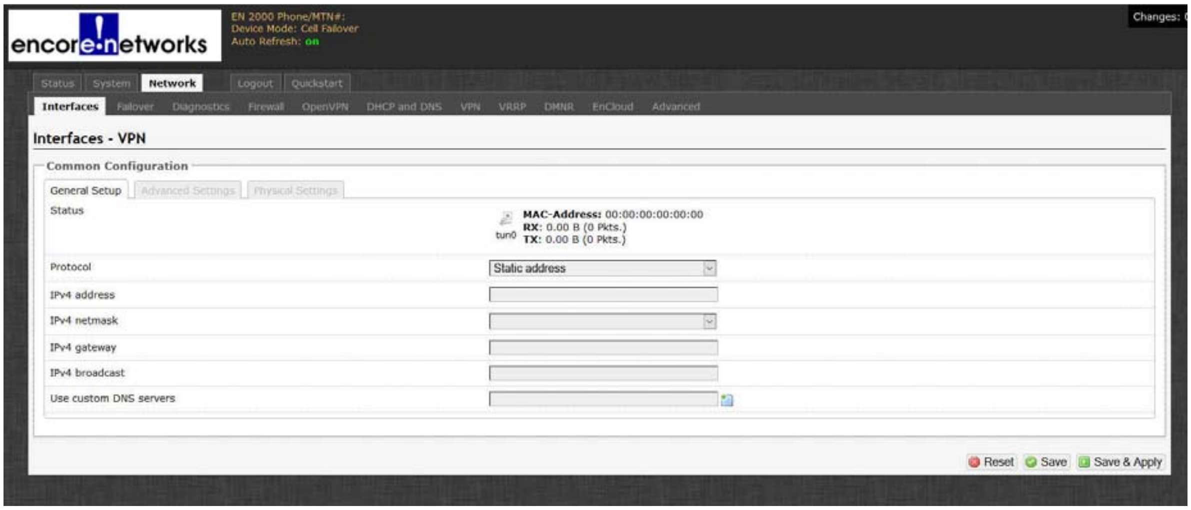
Create a bridge over multiple interfaces: □

Cover the following interface:
- ○ Ethernet Adapter: "eth0" (Right Port, PoE input) (lan)
- ○ Ethernet Adapter: "eth1" (Left Port, PoE output) (wan)
- ○ Ethernet Adapter: "eth2" (cell)
- ○ No Interface
- ● Custom Interface: tun0

c Select the button to **Submit** the interface (at the lower right corner of the screen).

❖ The Common Configuration Screen for interfaces is displayed (Figure 5-12). The upper left title for the screen shows **Interfaces - VPN**. Continue to step 3.

Figure 5-12. Common Configuration Screen



EN 2000 Phone/MTN#:
Device Mode: Cell Failover
Auto Refresh: on

Interfaces - VPN

Common Configuration

Status: tun0 **MAC-Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 0.00 B (0 Pkts.)

Protocol: Static address

IPv4 address

IPv4 netmask

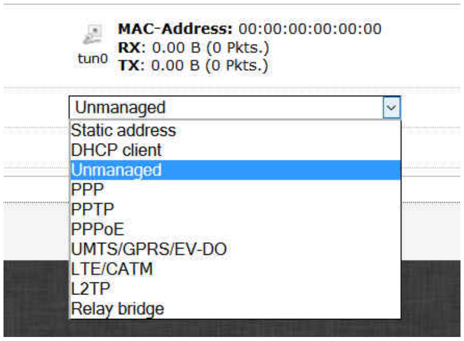
IPv4 gateway

IPv4 broadcast

Use custom DNS servers

3 On the Common Configuration Screen, select the dropdown button for the **Protocol** field. In the dropdown list, select **Unmanaged** (Figure 5-13).

Figure 5-13. List of Interface Protocols

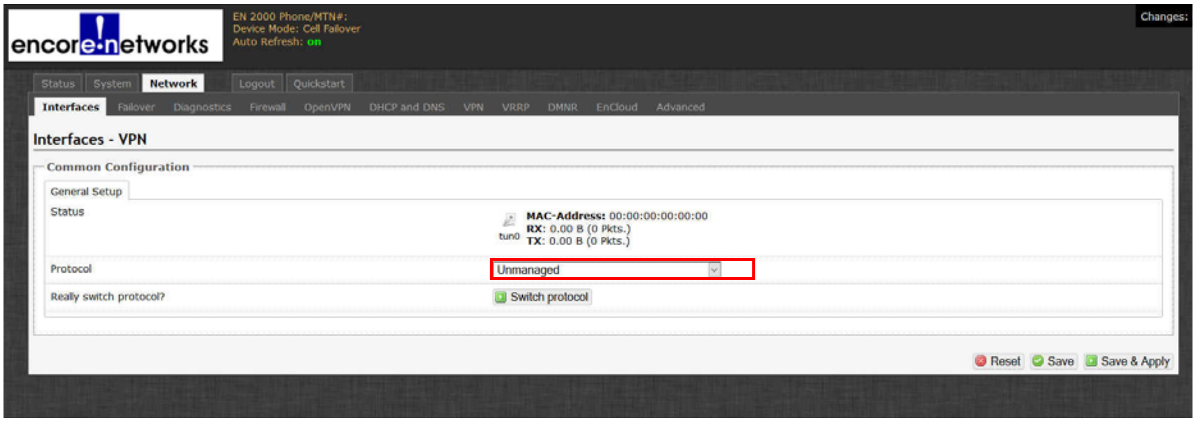


tun0 **MAC-Address:** 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Unmanaged

- ❖ The Common Configuration Screen is updated to reflect the selected interface protocol (Figure 5-14).

Figure 5-14. Common Configuration Screen, Updated



Interfaces - VPN

Common Configuration

Status: tun0 **MAC-Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 0.00 B (0 Pkts.)

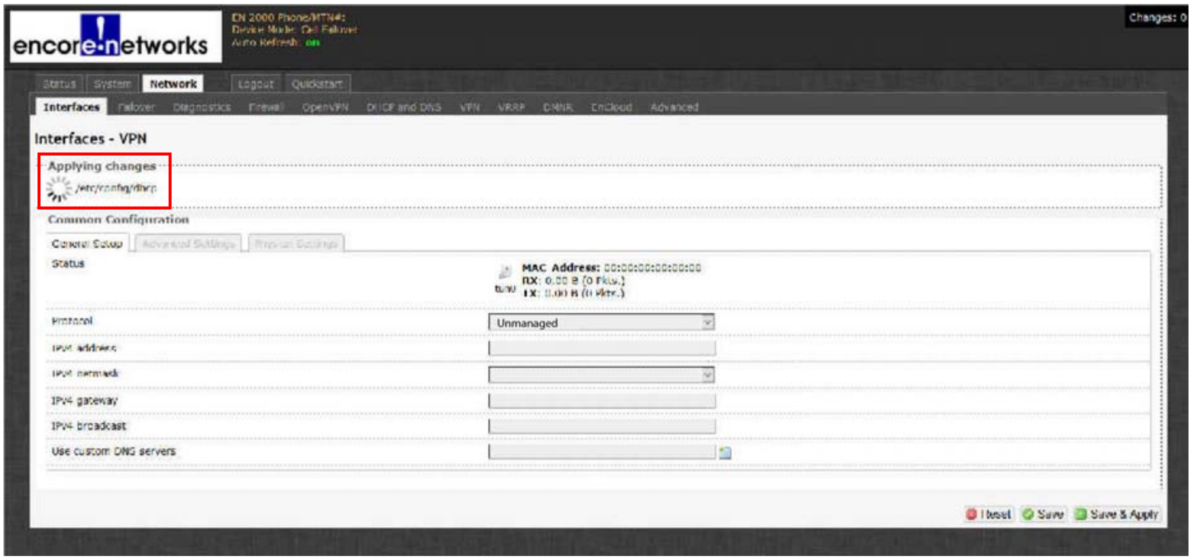
Protocol: Unmanaged

Really switch protocol?

4 After review of the new interface’s values, select the **Save & Apply** button (in the lower right corner of the screen).

- ❖ The EN™ system creates the interface. (Note the spinning circle near the upper left of Figure 5-15, under **Applying changes**.)

Figure 5-15. Creating an Interface



Interfaces - VPN

Applying changes

/etc/config/dhcp

Common Configuration

Status: tun0 **MAC Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 0.00 B (0 Pkts.)

Protocol: Unmanaged

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

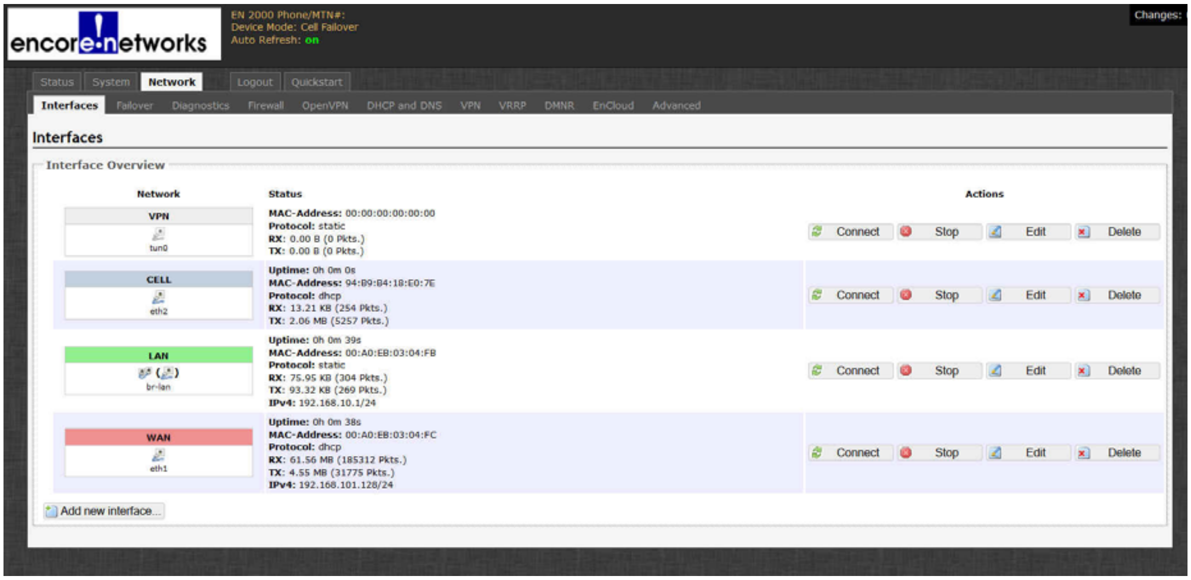
Use custom DNS servers

- ❖ After the circle quits spinning, the interface confirmation screen is displayed again.

5 After the interface confirmation screen is displayed again, select the tabs **Network**, **Interface**.

- ❖ The List of Network Interfaces is redisplayed, including the VPN interface you just created (in the top row of Figure 5-16).

Figure 5-16. Revised List of Network Interfaces



EN 2000 Phone/MTN#:
Device Mode: Cell Failover
Auto Refresh: on

Interfaces

Interface Overview

Network	Status	Actions
VPN tun0	**MAC-Address:** 00:00:00:00:00:00 **Protocol:** static **RX:** 0.00 B (0 Pkts.) **TX:** 0.00 B (0 Pkts.)	Connect Stop Edit Delete
CELL eth2	**Uptime:** 0h 0m 0s **MAC-Address:** 94:B9:B4:18:E0:7E **Protocol:** dhcp **RX:** 13.21 KB (254 Pkts.) **TX:** 2.06 MB (5257 Pkts.)	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 0h 0m 39s **MAC-Address:** 00:A0:EB:03:04:FB **Protocol:** static **RX:** 75.95 KB (304 Pkts.) **TX:** 93.32 KB (269 Pkts.) **IPv4:** 192.168.10.1/24	Connect Stop Edit Delete
WAN eth1	**Uptime:** 0h 0m 38s **MAC-Address:** 00:A0:EB:03:04:FC **Protocol:** dhcp **RX:** 61.56 MB (185312 Pkts.) **TX:** 4.55 MB (31775 Pkts.) **IPv4:** 192.168.101.128/24	Connect Stop Edit Delete

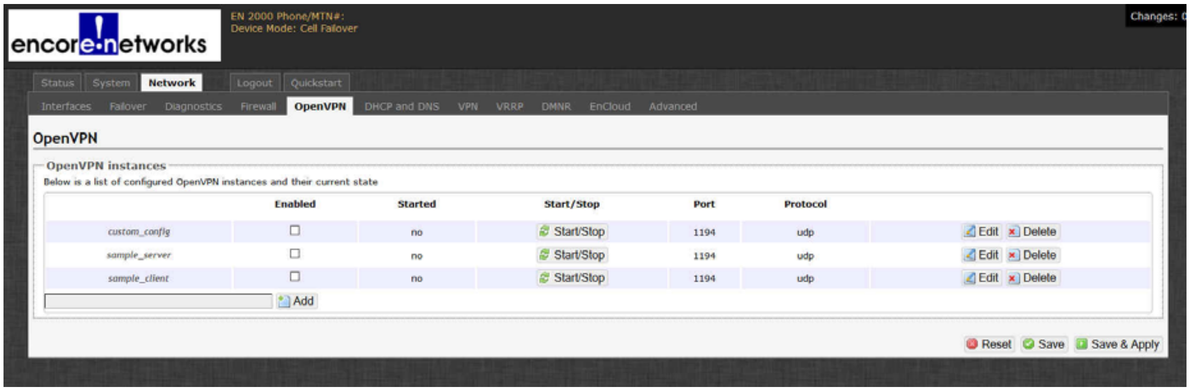
6 Study *Section 5.3, List of OpenVPN® Instances*, on page 9. Then proceed to *Section 5.4, Configuring an OpenVPN® Connection*, on page 10.

5.3 List of OpenVPN® Instances

1 On the EN™ Router management screen, select the **Network** tab; then select the **OpenVPN** tab.

❖ The List of OpenVPN Instances is displayed (Figure 5-17).

Figure 5-17. List of OpenVPN Instances



EN 2000 Phone/MTN#:
Device Mode: Cell Failover

OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	□	no	Start/Stop	1194	udp	Edit Delete
sample_server	□	no	Start/Stop	1194	udp	Edit Delete
sample_client	□	no	Start/Stop	1194	udp	Edit Delete

Note: The List of OpenVPN Instances includes default instances. Use an appropriate default instance as a template to configure new OpenVPN® connections. See *Section 5.4, Configuring an OpenVPN® Connection*, on page 10.

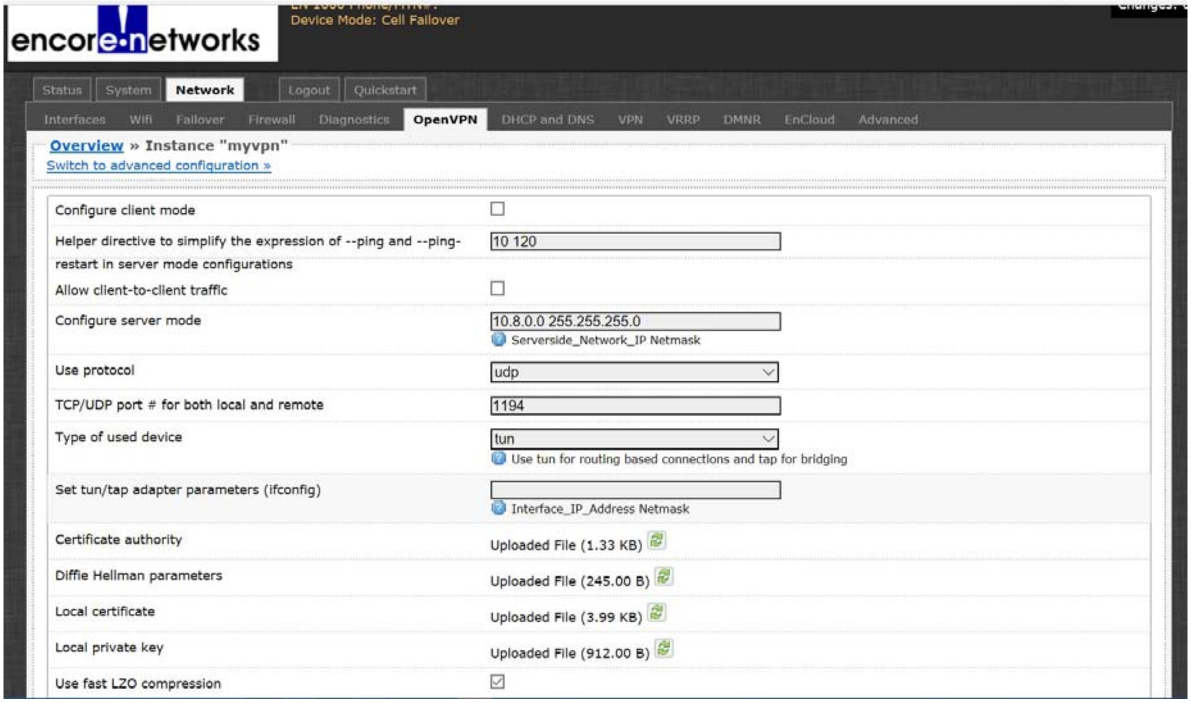
5.4 Configuring an OpenVPN® Connection

After a VPN interface is created (in Section 5.1, *Network Interfaces*, starting on page 2, or in Section 5.2, *Alternate Creation of a VPN Interface*, starting on page 6), you can configure parameters for an OpenVPN® connection.[2]

1 To create a new OpenVPN® connection, select the **Edit** button at the end of the row for the default instance *custom_config* in the List of OpenVPN Instances (recall Figure 5-17, on page 9).

2 The Screen for Basic Configuration of OpenVPN Connections is displayed (Figure 5-18).

Figure 5-18. Screen for Basic Configuration of OpenVPN Connections



Configure client mode	□
Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations	10 120
Allow client-to-client traffic	□
Configure server mode	10.8.0.0 255.255.255.0 Serverside_Network_IP Netmask
Use protocol	udp
TCP/UDP port # for both local and remote	1194
Type of used device	tun Use tun for routing based connections and tap for bridging
Set tun/tap adapter parameters (ifconfig)	 Interface_IP_Address Netmask
Certificate authority	Uploaded File (1.33 KB)
Diffie Hellman parameters	Uploaded File (245.00 B)
Local certificate	Uploaded File (3.99 KB)
Local private key	Uploaded File (912.00 B)
Use fast LZO compression	☑

3 Confer with your network administrator for the values to enter on the Screen for Basic Configuration of OpenVPN Connections. Determine whether the EN™ router will be the server or the client in this OpenVPN® connection.

[2] Configuration files (on Windows: *.ovpn; on other platforms: *.conf) can be generated for OpenVPN® servers and clients. To study the process and to review sample .conf files, see one of the following:

- *https://openvpn.net/community-resources/creating-configuration-files-for-server-and-clients/*
- *https://github.com/OpenVPN/openvpn/blob/master/sample/sample-config-files/server.conf*
- *https://github.com/OpenVPN/openvpn/blob/master/sample/sample-config-files/client.conf*

Encore Networks, Inc., recommends configuration as described in the current document, to more closely reflect your organization’s connection needs.

4 Do one of the following:

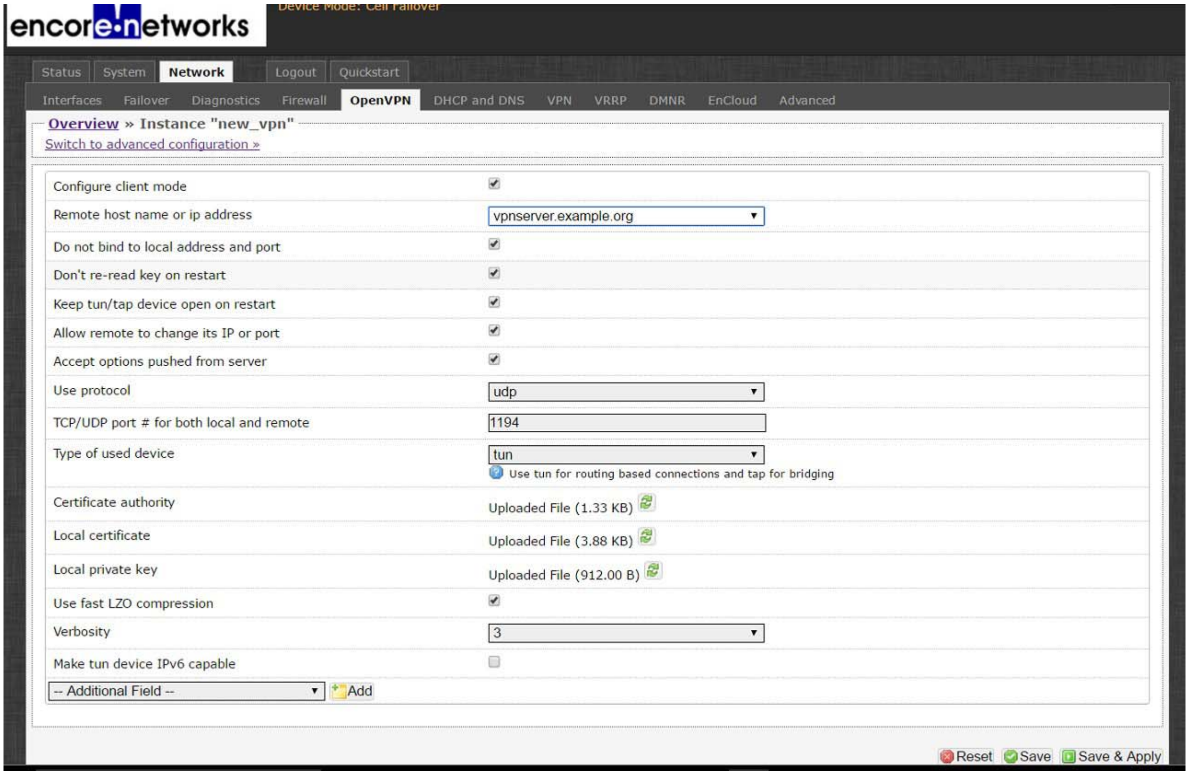
a To configure the server’s side of the OpenVPN® connection, leave the box to **Configure Client Mode** unchecked. (That empty checkbox is at the top of the list of fields in Figure 5-18, above.)

❖ The screen displays parameters for the server.

b To configure the client’s side of the OpenVPN® connection, check the box to **Configure Client Mode**. (That selected checkbox is at the top of the list of fields in Figure 5-19, below.)

❖ The screen displays parameters for the client.

Figure 5-19. Basic Configuration of OpenVPN Client Connection



Overview » Instance "new_vpn"
Switch to advanced configuration »

Configure client mode	☑
Remote host name or ip address	vpnserver.example.org
Do not bind to local address and port	☑
Don't re-read key on restart	☑
Keep tun/tap device open on restart	☑
Allow remote to change its IP or port	☑
Accept options pushed from server	☑
Use protocol	udp
TCP/UDP port # for both local and remote	1194
Type of used device	tun Use tun for routing based connections and tap for bridging
Certificate authority	Uploaded File (1.33 KB)
Local certificate	Uploaded File (3.88 KB)
Local private key	Uploaded File (912.00 B)
Use fast LZO compression	☑
Verbosity	3
Make tun device IPv6 capable	□
-- Additional Field --	Add

5 After you have configured the basic parameters for an OpenVPN® connection, select the line to **Switch to Advanced Configuration** (near the upper left corner of the screen).

❖ The Advanced Configuration Screen is displayed (Figure 5-20).

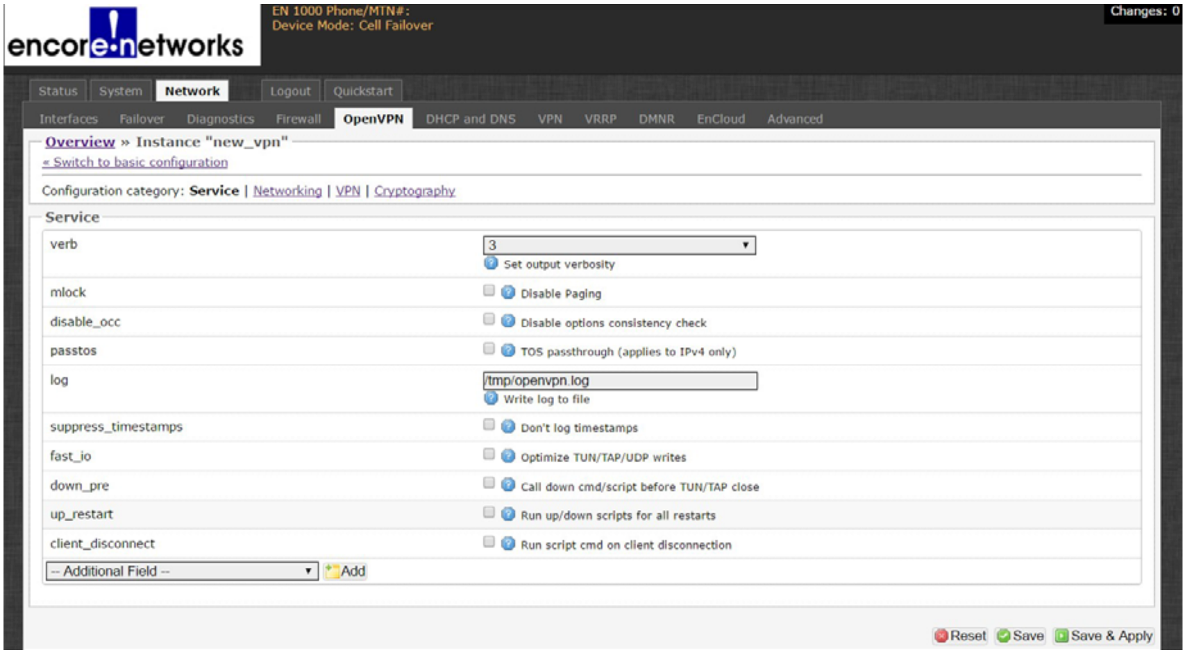
Note: Information entered on the screens for basic configuration will automatically populate some information on the screens for advanced configuration.

OpenVPN Advanced Configuration screens differ for the client and for the server.

This side of the OpenVPN® connection (server or client) must fill out advanced information for this side of the connection. The other side of the connection (client or server) must configure corresponding information.

The Advanced Configuration screen has four parts. Configuration of **Service** is selected in Figure 5-20.

Figure 5-20. Advanced Configuration of OpenVPN Client Connection: Service



Overview » Instance "new_vpn"

« Switch to basic configuration

Configuration category: **Service** | Networking | VPN | Cryptography

Service

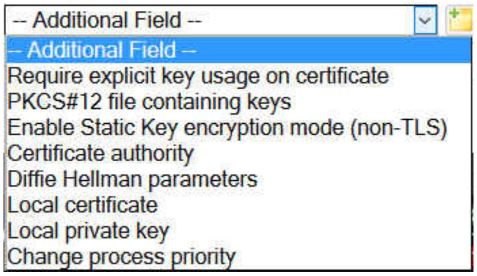
verb	3 ▾ Set output verbosity
mlock	□ Disable Paging
disable_occ	□ Disable options consistency check
passtos	□ TOS passthrough (applies to IPv4 only)
log	/tmp/openvpn.log Write log to file
suppress_timestamps	□ Don't log timestamps
fast_io	□ Optimize TUN/TAP/UDP writes
down_pre	□ Call down cmd/script before TUN/TAP close
up_restart	□ Run up/down scripts for all restarts
client_disconnect	□ Run script cmd on client disconnection

-- Additional Field -- ▾ Add

6 On the Advanced Configuration screen for service, fill out additional information for the OpenVPN® configuration.

Note: Select the **Additional Field** button (in the lower left corner of the advanced screen) to see a list of parameters that can be added to this section of the advanced configuration (sample shown in Figure 5-21).

Figure 5-21. Optional Parameters for OpenVPN Configuration

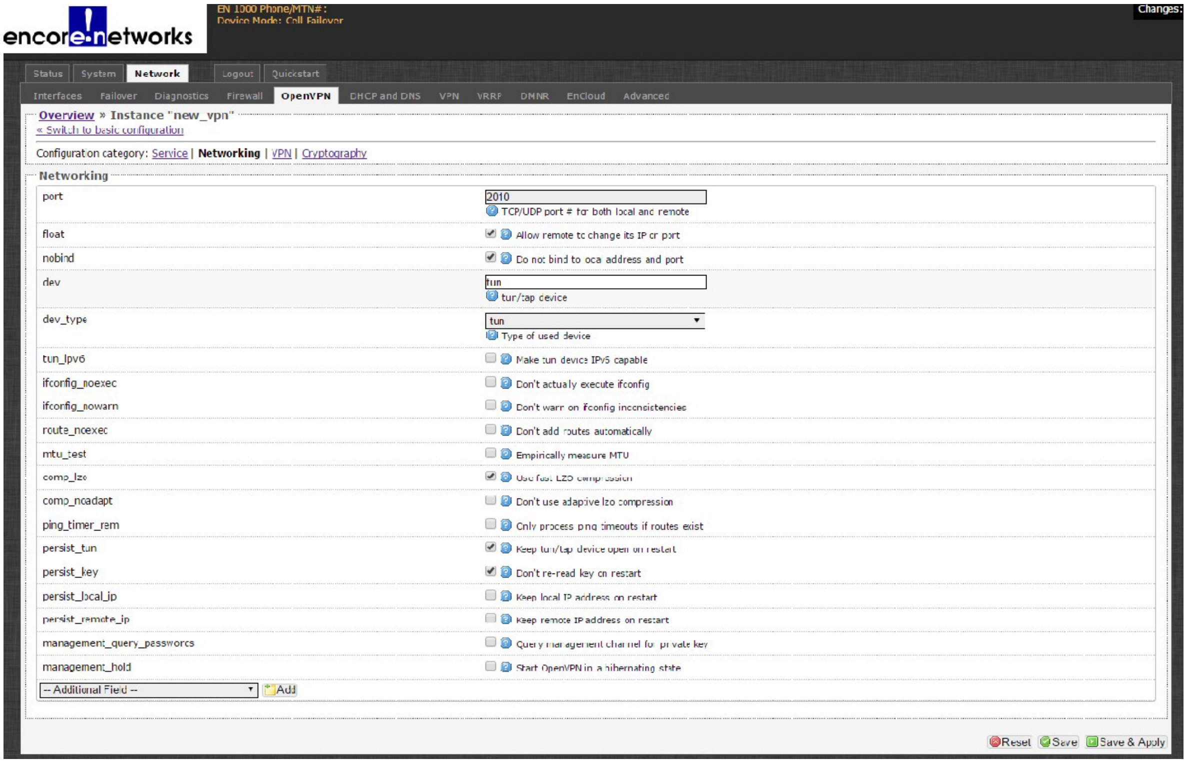

-- Additional Field --
-- Additional Field --
Require explicit key usage on certificate
PKCS#12 file containing keys
Enable Static Key encryption mode (non-TLS)
Certificate authority
Diffie Hellman parameters
Local certificate
Local private key
Change process priority

7 Enter configuration information for each additional parameter that you select.

8 Near the upper left corner of the OpenVPN screen, select each part of the Advanced Configuration (**Service**, **Networking**, **VPN**, and **Cryptography**) as needed to continue the configuration.

Note: Figure 5-22 displays advanced networking options for the server connection.

Figure 5-22. Advanced Configuration of OpenVPN Server Connection: Networking



EN 1000 Phone/MTN#:
Device Mode: Cell Failover
Changes:
Status | System | Network | Logout | Quickstart
Interfaces | Failover | Diagnostics | Firewall | OpenVPN | DHCP and DNS | VPN | VRRP | DMNR | EnCloud | Advanced

Overview » Instance "new_vpn"
« Switch to basic configuration

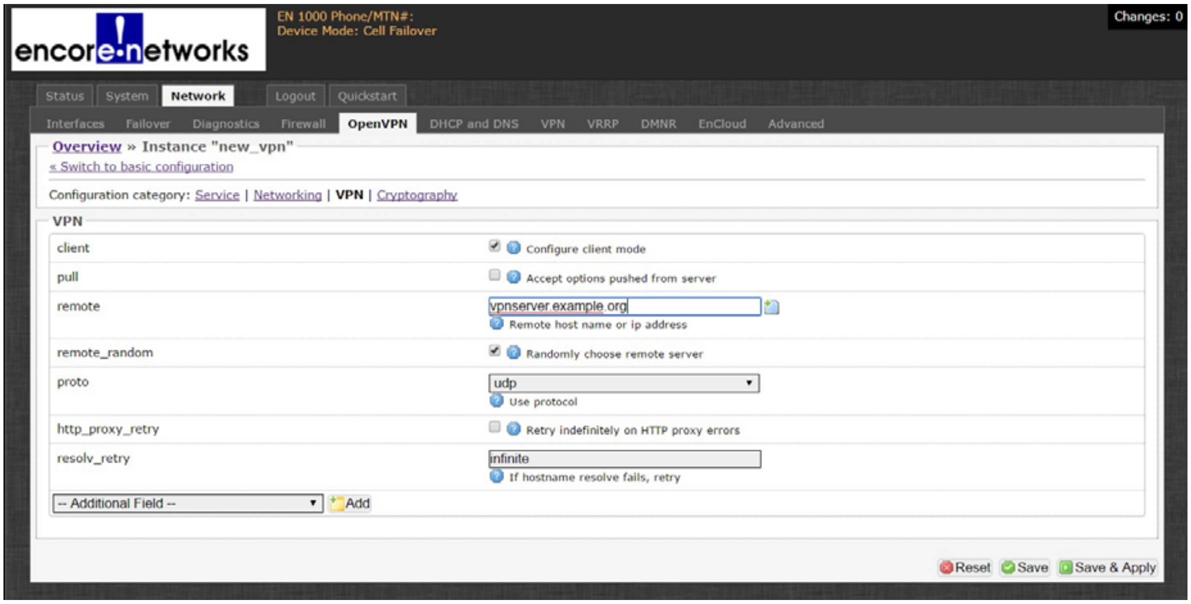
Configuration category: Service | **Networking** | VPN | Cryptography

Networking

port	2010 TCP/UDP port # for both local and remote
float	☑ Allow remote to change its IP or port
nobind	☑ Do not bind to local address and port
dev	tun tun/tap device
dev_type	tun Type of used device
tun_ipv6	□ Make tun device IPv6 capable
ifconfig_noexec	□ Don't actually execute ifconfig
ifconfig_nowarn	□ Don't warn on ifconfig inconsistencies
route_noexec	□ Don't add routes automatically
mtu_test	□ Empirically measure MTU
comp_lzo	☑ Use fast LZO compression
comp_noadapt	□ Don't use adaptive lzo compression
ping_timer_rem	□ Only process ping timeouts if routes exist
persist_tun	☑ Keep tun/tap device open on restart
persist_key	☑ Don't re-read key on restart
persist_local_ip	□ Keep local IP address on restart
persist_remote_ip	□ Keep remote IP address on restart
management_query_passwords	□ Query management channel for private key
management_hold	□ Start OpenVPN in a hibernating state

Note: OpenVPN Advanced Configuration screens differ for the client and for the server (client screen shown in Figure 5-23).

Figure 5-23. Advanced Configuration of OpenVPN Client Connection: VPN Parameters



EN 1000 Phone/MTN#:
Device Mode: Cell Failover
Changes: 0
Status | System | Network | Logout | Quickstart
Interfaces | Failover | Diagnostics | Firewall | OpenVPN | DHCP and DNS | VPN | VRRP | DMNR | EnCloud | Advanced

Overview » Instance "new_vpn"
« Switch to basic configuration

Configuration category: Service | Networking | **VPN** | Cryptography

VPN

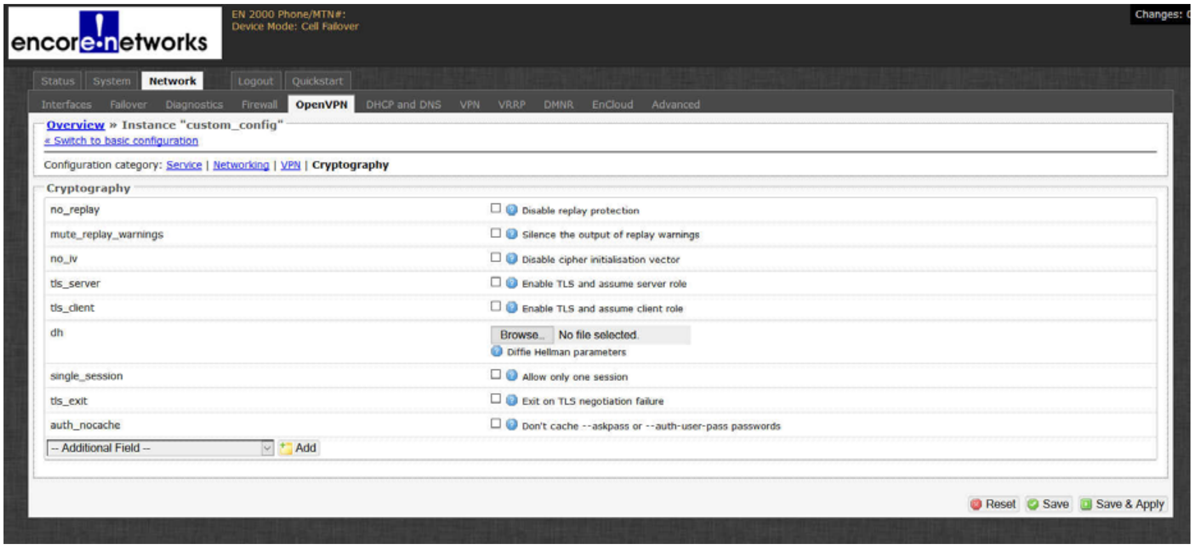
client	☑ Configure client mode
pull	□ Accept options pushed from server
remote	vpnserver.example.org Remote host name or ip address
remote_random	☑ Randomly choose remote server
proto	udp Use protocol
http_proxy_retry	□ Retry indefinitely on HTTP proxy errors
resolv_retry	infinite If hostname resolve fails, retry

9 On the screen for OpenVPN server configuration, select **Cryptography**.

❖ The server's advanced configuration screen for cryptography is displayed (Figure 5-24).

Note: The Advanced Configuration screens for Cryptography are identical for the client and for the server, except for the certificates needed.

Figure 5-24. Advanced Configuration of OpenVPN Server Connection: Cryptography



Overview » Instance "custom_config"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

no_replay	□ Disable replay protection
mute_replay_warnings	□ Silence the output of replay warnings
no_iv	□ Disable cipher initialisation vector
tls_server	□ Enable TLS and assume server role
tls_client	□ Enable TLS and assume client role
dh	Browse... No file selected. Diffie Hellman parameters
single_session	□ Allow only one session
tls_exit	□ Exit on TLS negotiation failure
auth_nocache	□ Don't cache --askpass or --auth-user-pass passwords

-- Additional Field -- Add

10 On the screen for Advanced Configuration of OpenVPN Server Connection: Cryptography, select one of the following:

- **TLS server: Enable TLS [Transport Layer Security] and assume server role.**

❖ Parameters for the server are displayed. Go to Step 11.

- **TLS client** (as shown in Figure 5-25 for client screen): **Enable TLS [Transport Layer Security] and assume client role.**

❖ Parameters for the client are displayed. Go to Step 11.

11 Do the following:

a Select the **Additional Field** list (recall Figure 5-21, on page 12) to add the certificate fields to the screen.

b In that list, select certificates appropriate to the side of the connection (client or server) that this router supports.

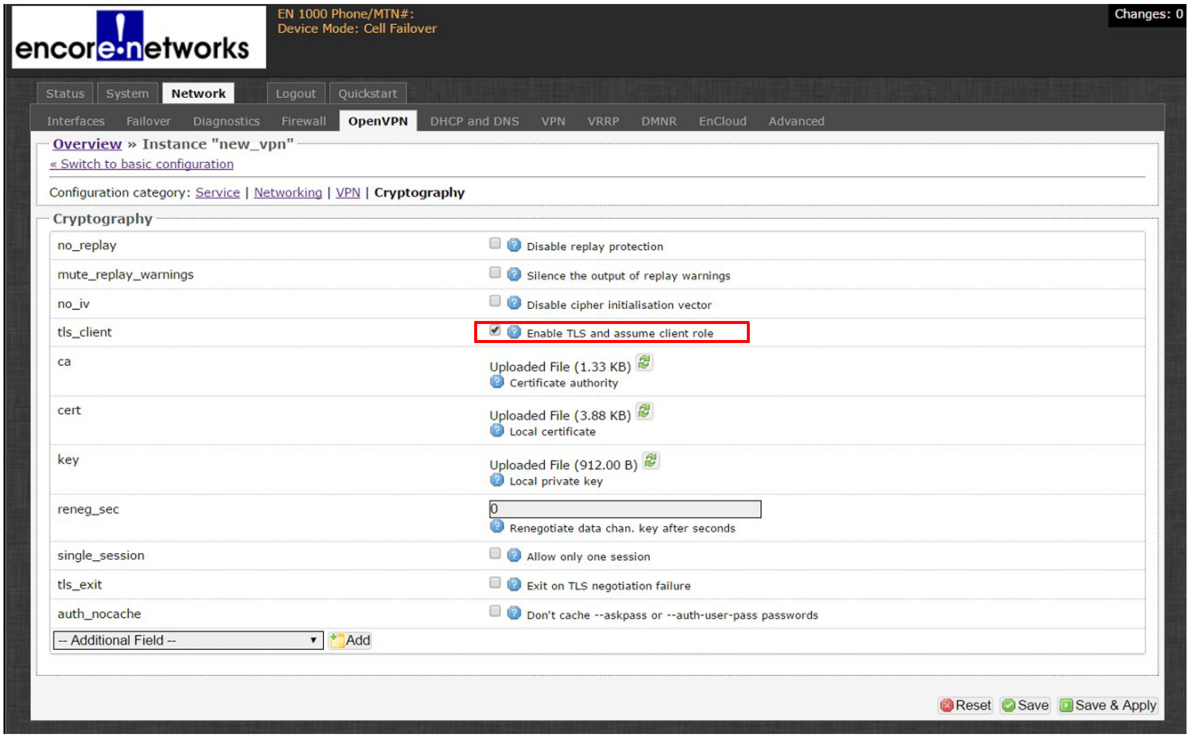
❖ The certificates are added to the screen.

Note: OpenVPN® certificates are generated in a management computer; see the document *Generating Certificates for OpenVPN® Connections*. Download the certificates from that computer to the EN™ router.

Note: As shown in Figure 5-25, the transport layer security client (**TLS client**) in the OpenVPN® connection needs the following certificate entities:

- **ca:** certificate authority
- **cert:** client certificate
- **key:** client key

Figure 5-25. Advanced Configuration of OpenVPN Client Connection: Cryptography



Overview » Instance "new_vpn"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

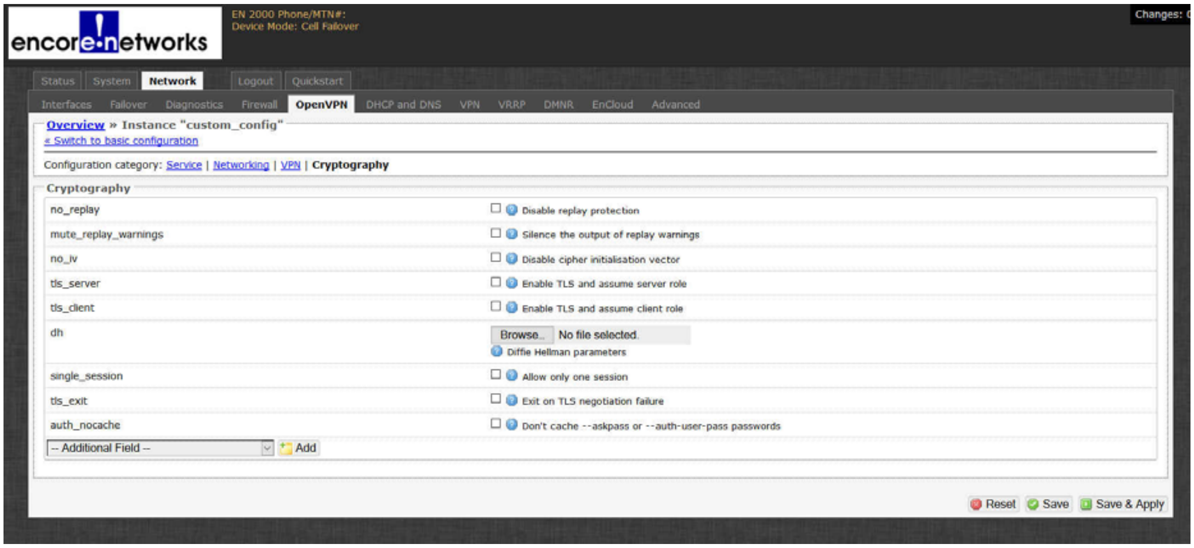
no_replay	□ Disable replay protection
mute_replay_warnings	□ Silence the output of replay warnings
no_iv	□ Disable cipher initialisation vector
tls_client	☑ Enable TLS and assume client role
ca	Uploaded File (1.33 KB) Certificate authority
cert	Uploaded File (3.88 KB) Local certificate
key	Uploaded File (912.00 B) Local private key
reneg_sec	0 Renegotiate data chan. key after seconds
single_session	□ Allow only one session
tls_exit	□ Exit on TLS negotiation failure
auth_nocache	□ Don't cache --askpass or --auth-user-pass passwords
-- Additional Field --	Add

If you are configuring the **TLS server** in the OpenVPN® connection, add the following certificate entities:

- **ca:** certificate authority
- **cert:** server certificate
- **key:** server key
- **dh:** Diffie–Hellman key-exchange parameters

Note: Figure 5-26 includes the **dh** certificate field, but the certificate itself has not been downloaded yet. Select the field, and browse your computer's \easy-rsa directory to select the dh certificate to download to the EN™ Router.

Figure 5-26. Add Server Certificate for Diffie–Hellman (dh) Parameters



Overview » Instance "custom_config"

« Switch to basic configuration

Configuration category: Service | Networking | VPN | **Cryptography**

Cryptography

no_replay	□ Disable replay protection
mute_replay_warnings	□ Silence the output of replay warnings
no_iv	□ Disable cipher initialisation vector
tls_server	□ Enable TLS and assume server role
tls_client	□ Enable TLS and assume client role
dh	Browse... No file selected. Diffie Hellman parameters
single_session	□ Allow only one session
tls_exit	□ Exit on TLS negotiation failure
auth_nocache	□ Don't cache --askpass or --auth-user-pass passwords
-- Additional Field --	Add

12 When you have finished configuring the VPN connection, select the button to **Save & Apply** the configuration (in the lower right corner of the screen).

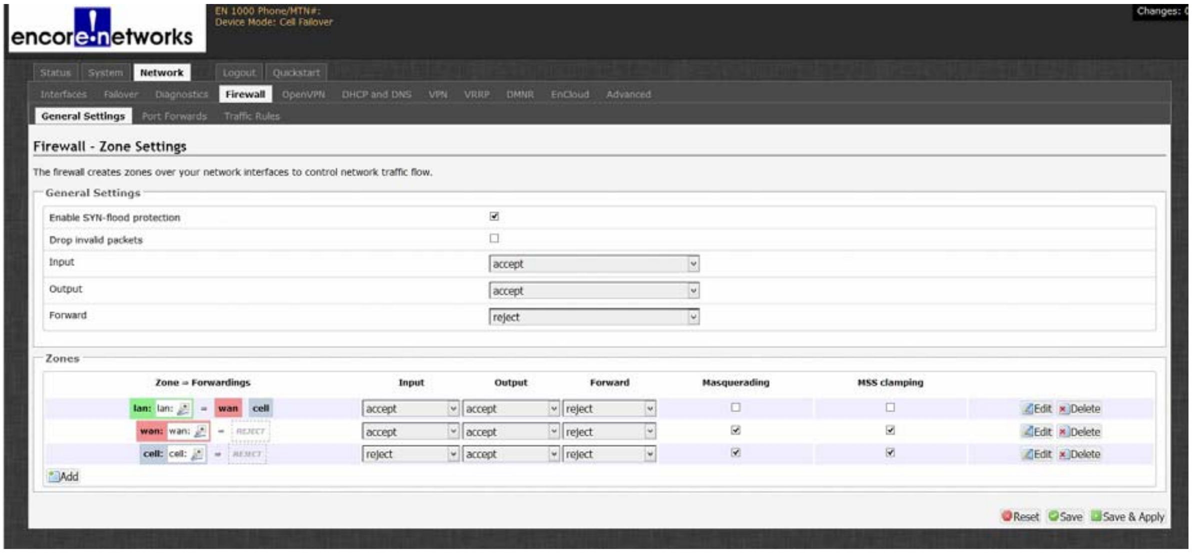
❖ The new OpenVPN® connection is displayed in the List of OpenVPN Instances.

5.5 Firewall Configuration for OpenVPN®

1 On the management configuration screen, select the tab **Network**; then select the tab **Firewall**. If necessary, select the tab **General Settings**.

❖ The screen for General Firewall Settings is displayed (Figure 5-27).

Figure 5-27. General Firewall Settings



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection	☑
Drop invalid packets	□
Input	accept
Output	accept
Forward	reject

Zones

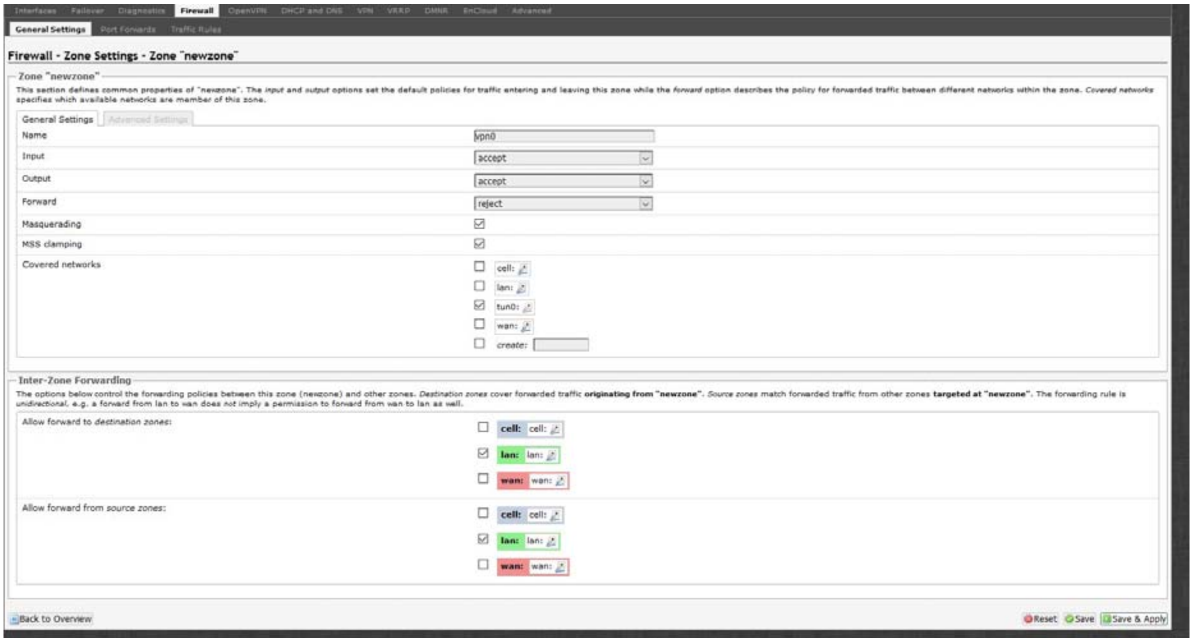
Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan cell	accept	accept	reject	□	□	Edit Delete
wan: wan: ⇒ REJECT	accept	accept	reject	☑	☑	Edit Delete
cell: cell: ⇒ REJECT	reject	accept	reject	☑	☑	Edit Delete

Note: We need to add a zone for the OpenVPN® tunnel that we created in *Section 5.4, Configuring an OpenVPN® Connection*, on page 10.

2 Select the **Add** button (near the lower left corner of the General Firewall Settings screen).

❖ The screen for a New Firewall Zone is displayed (Figure 5-28).

Figure 5-28. New Firewall Zone



Firewall - Zone Settings - Zone "newzone"

Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

Name: vpn0
Input: accept
Output: accept
Forward: reject
Masquerading: ☑
MSS clamping: ☑
Covered networks: ☐ cell: ☐ lan: ☑ tun0: ☐ wan: ☐ *create:*

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from "newzone"**. *Source zones* match forwarded traffic from other zones **targeted at "newzone"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*: ☐ cell: cell: ☑ lan: lan: ☐ wan: wan:

Allow forward from *source zones*: ☐ cell: cell: ☑ lan: lan: ☐ wan: wan:

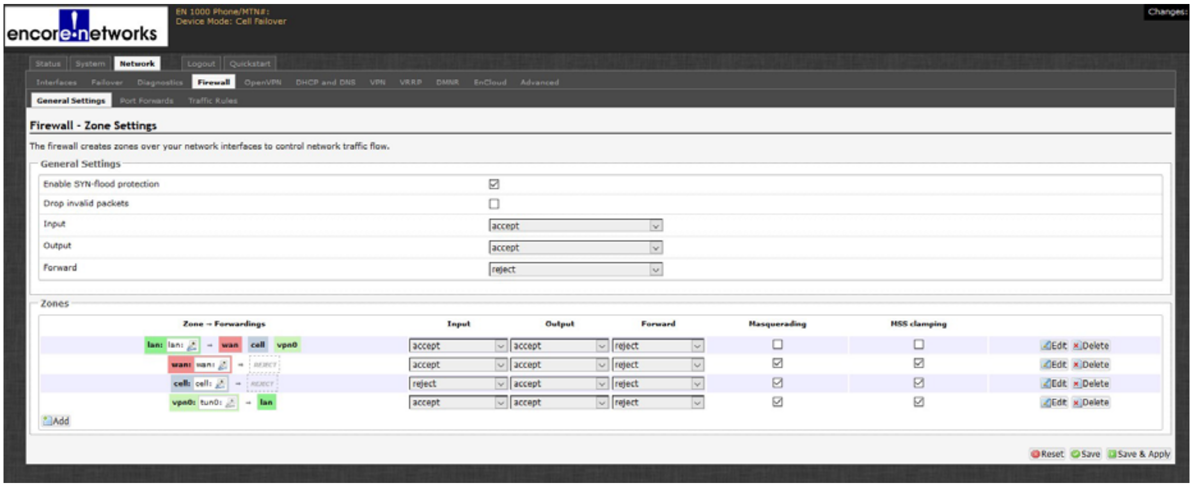
3 Configure the following settings for the new firewall zone:

• **Name**	**vpn0** (use any unique name)	
• **Input**	**accept**	
• **Output**	**accept**	
• **Forward**	**reject**	
• **Masquerading**	**on** (checked)	
• **MSS Clamping**	**on** (checked)	
• **Covered Networks**	cell	off (unchecked)
	lan	off (unchecked)
	tun0	**on** (checked)
	wan	off (unchecked)
	create (leave blank)	
• **Allow Forward to Destination Zones**	cell	no (unchecked)
	lan	**yes** (checked)
	wan	no (unchecked)
• **Allow Forward from Source Zones**	cell	no (unchecked)
	lan	**yes** (checked)
	wan	no (unchecked)

4 When you have configured the settings for the new zone, select the button to **Save & Apply** (in the lower right corner of the screen).

❖ The new firewall zone is saved, and the screen for General Firewall Settings is redisplayed (Figure 5-29). The new zone is included in the list of zones.

Figure 5-29. General Firewall Settings



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection	☑
Drop invalid packets	□
Input	accept
Output	accept
Forward	reject

Zones

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → wan cell vpn0	accept	accept	reject	□	□	Edit Delete
wan: wan: → REJECT	accept	accept	reject	☑	☑	Edit Delete
cell: cell: → REJECT	reject	accept	reject	☑	☑	Edit Delete
vpn0: tun0: → lan	accept	accept	reject	☑	☑	Edit Delete

5 Select the button to **Save & Apply** (in the lower right corner of the screen).

❖ The firewall settings are saved and are put into use immediately.

5.6 More Information

For a list of documents for OpenVPN® connections over EN routers, see *Reference Manual for OpenVPN® on EN™ Routers*.