

EN-4000<sup>™</sup> Reference Manual Document G

# VPNC Scenario for IPsec Interoperability

EN-4000<sup>™</sup> 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 Although the consortium is no longer active, the scenario remains useful.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

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 "I" (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.<sup>1</sup> The entries in the configuration

<sup>1.</sup> 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:<sup>2</sup>

- 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<sup>TM</sup> routers, the default user name is **root**. For all other  $EN^{TM}$  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.

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

Status     Overview     Firewall     Routes     System Log     Process       Status     System     Router Name     EN4       Router Name     EN4       Router Model     EN4       Firmware Version     Beta       Local Time     Fri M       Uptime     1d 2       Memory     Total Available       Free     22       Cached     Buffered       IPv4 WAN Status     En4       IPv6 WAN Status     2	ses Realtime Graphs 4000 4000 4000 4000 23 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 41440 k8 / 255820 k8 (94%) 3940 k8 / 255820 k8 (9%) 9040 k8 / 255820 k8 (9%)
System           System         ENAL           Router Name         ENAL           Router Madel         ENAL           Firmware Version         Betz           Local Time         Fri N           Uptime         1d 2           Memory         Total Available           Free         22           Cached         Enfered           Buffered         IPv4 WAN Status	4000 4000 a 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 41440 k8 / 255820 k8 (94%) 32400 k8 / 255820 k8 (9%) 9040 k8 / 255820 k8 (9%)
Status         System         Router Name       EN4         Router Model       EN 4         Firmware Version       Betz         Local Time       Fri N         Uptime       1d 2         Memory       1d 2         Total Available       22         Free       22         Cached       Buffered         Buffered       2         Network       1Pv4 WAN Status         IPv6 WAN Status       2         7       7	4000 4000 (a 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 141440 k8 / 255820 k8 (94%) 19040 k8 / 255820 k8 (9%) 9040 k8 / 255820 k8 (9%)
System Router Name EN4 Router Model EN4 Router Model EN4 Firmware Version Bet Local Time Fri N Uptime 1d 2 Memory Total Available 22 Free 22 Cached 2 Buffered 22 Cached 2 Buffered 22 IPv4 WAN Status 2 IPv6 WAN Status 2	4000 4000 (a 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 41440 k8 / 255820 k8 (94%) 9040 k8 / 255820 k8 (9%) 9040 k8 / 255820 k8 (9%)
Router Name     EN4       Router Model     EN       Firmware Version     Betz       Local Time     Fri N       Uptime     1d 2       Memory     22       Total Available     22       Free     22       Cached     24       Buffered     24       Network     24       IPv4 WAN Status     24       Pv6 WAN Status     24	4000 4000 (a 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 
Router Model     EN 4       Firmware Version     Betz       Local Time     Fri M       Uptime     1d 2       Memory     1d 2       Total Available     2       Free     22       Cached     2       Buffered     2       Network     2       IPv4 WAN Status     4th       1Pv6 WAN Status     2	4000 ia 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 41440 k8 / 255820 k8 (94%) 9040 k8 / 255820 k8 (9%) 0 k8 / 255820 k8 (9%)
Firmware Version Beta Local Time Fri M Uptime 1d 2 Memory Total Available 2 Free 2 Cached 2 Buffered 2 Network 1 IPv4 WAN Status 2 IPv6 WAN Status 2 7	ia 1.4 2 Mar 8 11:07:02 2013 21h 14m 9s 241440 k8 / 255820 k8 (94%) 252400 k8 / 255820 k8 (96%) 9040 k8 / 255820 k8 (9%) 0 k8 / 255820 k8 (9%)
Local Time Fri M Uptime 1d 2 Memory Total Available 2 Free 2 Cached 2 Buffered 2 Network IPv4 WAN Status	Mar 8 11:07:02 2013 21h 14m 9s 241440 kB / 255820 kB (94%) 292400 kB / 255820 kB (96%) 9940 kB / 255820 kB (9%)
Uptime 1d 2 Memory Total Available 2 Free 2 Cached  Buffered  IPv4 WAN Status IPv6 WAN Status  2	21h 14m 9s 241440 k8 / 255820 k8 (94%) 222400 k8 / 255820 k8 (90%) 9040 k8 / 255820 k8 (9%)
Memory Total Available 22 Free 22 Cached Buffered Network IPv4 WAN Status IPv6 WAN Status 2	241440 kB / 255820 kB (94%) 282400 kB / 255820 kB (90%) 9040 kB / 255820 kB (9%) 0 kB / 255820 kB (9%)
Total Available 2 Free 2 Cached 9 Buffered 9 Network 1 IPv4 WAN Status 2 IPv6 WAN Status 2 7	X41440 kB / 255820 kB (94%) 232400 kB / 255820 kB (96%) 9040 kB / 255820 kB (9%) 0 kB / 255820 kB (9%)
Free 22 Cached 9 Buffered 9 Network 1 IPv4 WAN Status 9 IPv6 WAN Status 9	232400 kB / 255820 kB (90%) 9040 kB / 255820 kB (9%) 0 kB / 255820 kB (0%)
Cached Buffered Network IPv4 WAN Status IPv6 WAN Status	9040 kB / 255820 kB (3%) 0 kB / 255820 kB (0%)
Buffered  Network  IPv4 WAN Status  IPv6 WAN Status  2	0 kB / 255820 kB (0%)
Network IPv4 WAN Status IPv6 WAN Status	0.897 255020 88 (0.8)
- Network IPv4 WAN Status IPv6 WAN Status	
IPv4 WAN Status	
IPv6 WAN Status	Type: dhcp
IPv6 WAN Status	Address: 192.168.101.109
IPv6 WAN Status	0 Gateway: 192.168.101.17
IPv6 WAN Status	DNS 1: 8.8.8.8 Connected: 1h 1m 51s
?	
	Not connected
Active Connections	
Active connections	182 / 16384 (176)
DHCP Leases	
Hostname IPv4-Address	MAC-Address Leasetime remaining

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).

atus System Network	Statistics							
erfaces DHCP and DNS	Hostnames Static Route	s Load St	aring/Failover	Firewall Diagnostics	OoS Configure Diago	stics MAC Device Info	Overrides VPN VRRP Seria	
ltiwan			iannig, rano ran	in chair bhaghballab	Quo configure blagite			
neral Settings Strongsv	van IPSEC Status Onlir	ne Help						
FC Tunnels								
met Protocol Security is a	protocol suite for securing	) Internet P	rotocol comm	unications by authentica	ting and encrypting each I	P packet of a communic	ation session	
Sec Tunnels								
Tunnel Name	Left Subnet	Left	Left Right Right Sub		Tunnel Up	Tunnel Down		
2.2.2.22/24 firsttunnel 3.4.5.6/32 9 99.88.77.99/32		%any	%any 3.3.3.3 44.44.44.54/24 32.32.32.47/32		👸 Tunnel Up		Z Edit X Delete	
Add IPSEC TUNNEL								
SEC Defaults								
IKE	Lifetime		Key	Life	Aggressi	ve		
72h			24h		yes		Z Edit	
PSEC Actions								
TDEEC Start		IDEEC	Stop		IDEEC Doctort		Modificatons &	
IFSEC Start		IFSEC	Stop		IFSLC Restart		Additions	
@ IDSEC Start		IPSEC	Stop		IPSEC Restart		Save & Apply	

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	

cor <mark>e-n</mark> etworks	Ch
Status System Network Statistics Logout	
Interfaces DHCP and DNS Hostnames Static Routes Multiwan	Load Sharing/Failover Firewall Diagnostics QoS Configure Diagnostics MAC Device Info Overrides VPN VRRP Serial
General Settings Strongswan IPSEC Status Online H	elp
PSEC - Tunnels - Scen_1_VPNC	
onfig the Individual IPSec tunnels	
Tunnel Name	Scen_1_vrnc
Left Subnet	10.5.6.0/24
Left	14.15 16.17   Refers to Local Machine
Left ID	14.15.16.17
Left Firewall	NO
Right	22 23 24 25 @ Refers to Remote Machine
Right Subnet	17223.9.0/24
Right ID	22 23 24.25
IPSec startup operations	ROUTE

- **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 "I" (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

ncor	r <mark>e n</mark> etwor	ks						Chan
Status	System Networ	k Statistics Lo	ogout					
Interfac	ces DHCP and DNS	Hostnames Static	Routes Load Sha	ring/Failover Fire	ewall Diagnostics Q	oS Configure Diagnos	stics MAC Device Info Ov	verrides <b>VPN</b> VRRP Serial
Multiwa	in la ur	10050 01 1	0 ľ. u I					
PSEC -	Tunnels	a protocol suite for se	curing Internet Pro	otocol communicati	ons by authenticating	and encrypting each IF	packet of a communicati	on session
IPSec	c Tunnels Tunnel Name	Left Subnet	Left	Right	Right Subnet	Tunnel Up	Tunnel Down	
	firsttunnel	2.2.22/24 3.4.5.6/32 99.88.77.99/32	%any	3.3.3.3	44.44.44.54/24 32.32.32.47/32	🖉 Tunnel Up	Tunnel Down	Z Edit X Delete
	Scen_1_VPNC	10.5.6.0/24	14.15.16.17	22.23.24.25	172.23.9.0/24	🖉 Tunnel Up	Unnel Down	Z Edit Delete
📩 Ad	dd IPSEC TUNNEL							
IPSEC	C Defaults							
	IKE	Lifetime		KeyLife		Aggressive		
		72h		24h		yes		Edit
IPSEC	C Actions							
	IPSEC Sta	rt	IPSEC	Stop		IPSEC Restart		Modificatons & Additions
	Ø IPSEC St	art	() IPSEC	C Stop		IPSEC Restart		Save & Apply

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 intendto 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

atus System Network Statistics Logo		
terfaces DHCP and DNS Hostnames Static Ro	es Load Sharing/Failover Firewall Diagnostics QoS Con	nfigure Diagnostics MAC Device Info Overrides <b>VPN</b> VRRP Set
Strongswan IFSEC status	петер	
SEC Defaults		
nng the IPSec defaults		
Psec Default Configuration	70b	
	Image: Time: s=seconds,m=minutes,h=hours	-
Key Life	8h	]
	Ø Synonym for lifetime	
ReKey Margin	0h	1
Keying Tries	2	1
Key Exchange	ikev1	
Auth	secret	]
		د ٦
		3
	JDES 💌	1
IKE Authencation Protocol	SHA1	
IKE DH Group	Group2	]
ESP Encryption Protocol	3DES 💌	]
ESP Authencation Protocol	SHA1	3
ESP DH Group	Group2	
DPD Action	Restart	1
DPD Delay	20s	
	Time: s=seconds,m=minutes,h=hours	
DPD timeout	120s	1
RE-KEY	NO	л
RE-MITH		3
		3
Responder	NO Value will be placed in the Stronoswan.con	nf file

- **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).





	ks						
Status System Networ	k Statistics Lo	ogout					
Interfaces DHCP and DNS Hostnames Static Routes			ring/Failover Fire	wall Diagnostics Q	oS Configure Diagnos	tics MAC Device Info Ov	errides <b>VPN</b> VRRP Serial
fultiwan							
General Settings Strongs	swan IPSEC Status	Online Help					
SEC Tunnels							
ernet Protocol Security is a IPSec Tunnels	a protocol suite for sec	curing Internet Pro	tocol communicati	ons by authenticating	and encrypting each IF	packet of a communicati	on session
Tunnel Name	Left Subnet	Left	Right	Right Subnet	Tunnel Up	Tunnel Down	
firsttunnel	2.2.2.22/24 3.4.5.6/32 99.88.77.99/32	%any	3.3.3.3	44.44.44.54/24 32.32.32.47/32	🖉 Tunnel Up	Tunnel Down	Edit Delete
Scen_1_VPNC	10.5.6.0/24	14.15.16.17	22.23.24.25	172.23.9.0/24	🖉 Tunnel Up	Tunnel Down	Edit Edit
Add IPSEC TUNNEL							
IPSEC Defaults							
IKE	Lifetime		KeyLife		Aggressive		
72h			8h		no		Z Edit
IPSEC Actions							
IPSEC Star	t	IPSEC	Stop		IPSEC Restart		Modificatons & Additions
# IPSEC Start			Stop		IPSEC Restart		Save & Apply

- **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.

 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
0		5	0

Status System Network Statistics Logout	
Overview Firewall Routes System Log Kernel Log Processes Realtime Graphs	
System Log	
Apr 22 12:37:19 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:24 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:29 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:34 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:39 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:44 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:49 EN-4000 Sysleg.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:54 EN-4000 Syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:37:59 EN-4000 system.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:04 EN-4000 System.notice en4000:: Current temperature 55.000000	
Apr 22 12:38:09 EN-4000 System. Active en4000:: Current temperature 55.000000	
Apr 22 12:33:14 EN-4000 system.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:19 EN-4000 system.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:24 EN-4000 System.notice en4000:: Current temperature 55.000000	
Apr 22 12:38:29 EN-4000 Syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:34 EN-4000 system.notice en4000:: Current temperature 55.000000	
Apr 22 12:38:39 EN-4000 syslog.notice en4000:: Current temperature 55.000000	
Apr 22 12:38:44 EN-4000 Sysled.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:49 EN-4000 System.notice en4000:: Current temperature 55.000000	
Apr 22 12:33:54 EN-4000 system.notice en4000:: Current temperature 55.000000	
Apr 22 12:36:59 EN-4000 System.notice en4000:: Current temperature 55.000000	
Apr 22 12:39:04 EN-4000 System of the endoor: Current temperature 55.000000	
Apr 22 12:39:09 EN-4000 System notice en4000: Current temperature 55.000000	
Apr 22 12:35:14 EN-4000 system notice en4000: Current temperature 55.00000	
Apr 22 12:33:15 EN 4000 sysleg.notice entuous: current temperature 33.00000	
Apr 22 12:39:21 EN-4000 sysley indice entropy, cultering temperature 55.000000	
Apr 22 12:39:25 EN-1000 System of the antion of the temperature 55,000000	
Apr 22 12:35:35 EN 4000 gyplog.notice en4000: Current temperature 55.00000	
Apr 22 12:35:35 4 EN-4000 gyalog notice en4000; current temperature 55,00000	
hr 22 12:30:40 FN-4000 system notice enforts temperature 55,000000	
Apr 22 12:30:54 EN-4000 suslag notice en4000: Current temperature 55 000000	
In 2 12:30:52 FN-4000 system notice en4000: Current temperature 55,000000	
ar 22 12:40:14 EN-4000 system outine endout: Current temperature 55,000000	
Apr 22 12:40:09 EN-4000 syalad notice en4000:: Current temperature 55,000000	
Apr 22 12:40:14 EN-4000 syslog notice en4000:: Current temperature 55,000000	
Apr 22 12:40:20 EN-4000 syslag.notice en4000:: Current temperature 55,000000	
Apr 22 12:40:25 EN-4000 syslog.notice en4000:: Current temperature 55,000000	
Apr 22 12:40:30 EN-4000 syslog.notice en4000:: Current temperature 55,000000	
Apr 22 12:40:35 EN-4000 syslog.notice en4000:: Current temperature 55,000000	
Apr 22 12:40:40 EN-4000 syslog.notice en4000:: Current temperature 55.000000	

- 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.