

SLE[™] in Virtual Private Networks

his 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.

Changes:

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

terfaces Firewall S	tatic Routes Load Shari	ng/Failover	OoS Diagnost	ics Hostnames D	HCP and DN	S VPN VRRP	Serial	
eneral Settings Stro	ngswan IPSEC Status	Online Hel	p					
SEC Tunnels								
ernet Protocol Security	is a protocol suite for se	curing Inte	rnet Protocol com	munications by authe	enticating a	nd encrypting each I	P packet of a communication	n session
IPSec Tunnels								
Tunnel Name	Left Subnet	Left	Right	Right Subnet	SLE	Tunnel Up	Tunnel Down	
OSAT1	192.168.101.0/24	%any	71.16.53.45	0.0.0.0/0	yes	Tunnel Up	Cunnel Down	Z Edit 💌 Delete
Add IPSEC TUNNEL								
IPSEC Defaults								
TKE Life	etime	K.	wlife	Agore	ssive		Responder	
72	h		24h	уе	s		no	🛃 Edit
IPSEC Actions								
IPSEC S	tart		IPSEC Stop		19	SEC Restart		Additions &
# IPSEC	Start		IPSEC Stop		IPSEC Restart			Save & Apply

- **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 I Psec 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

	Logon		_
erfaces Firewall Static Routes Load Si	saring/Failover QoS Diagnostics Hostnames DHCP and D	DNS VPN VRRP Serial	-
neral Settings Strongswan IPSEC Stat	us Online Help		
EC - Tunnels - OSAT1			
ig the Individual IPSec tunnels			
unnel Name	OSAT1		
eft Subnet	192.168.101.0/24		
	Local Private Subnet(s)		
eft	%any P of local tunnel endopint (typ	vnically WAN IP. Namy for dynamic WANs)	
eft ID		The set of	
	 Local User Name 		
eft Firewall	NO		
	Is the local firewall on or off?	P	
sight	71.16.53.45		
	IP of remote tunnel endpoint (t	(typically WAN IP. %any for dynamic WANs)	
LE	yes		
light Subnet	0.0.0/0		
	To Reduce to 1 entry, use RESET-	T->SAVE_APPLY and enter new value	
emote ID	encore 8		
	Remote User Name		
PSec startup operations	START		
re-Shared Key	2	3	

- **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

atus System Network Statistics Logout			
terfaces Firewall Static Routes Load Sharing/Failo	ver QoS Diagnostics Hostnames DHCP	and DNS VPN VRRP Serial	
neral Settings Strongswan IPSEC Status Online	: Help		
EC Defaults			
ng the IPSec defaults			
vsec belaut configuration			
	Time: s=seconds,m=minu	es,h=hours	
Key Life	24h		
ReKey Margin	16		
	Time: s=seconds,m=minu	es,h=hours	
(eying Tries	2		
(ey Exchange	ikev2	•	
iuth	secret	•	
ggressive Mode	YES		
KE Encryption Protocol	AES256	-	
KE Authencation Protocol	MD5	•	
KE DH Group	Group2		
SP Encryption Protocol	AES256	•	
SP Authencation Protocol	MD5	-	
SP DH Group	Group2	•	
PPD Action	Restart	•	
PD Delay	20s		
	Time: s=seconds,m=minu	es,h=hours	
PD timeout	120s Time: s=seconds,m=minu	es,h=hours	
E-KEY	NO	-	
IE-AUTH	NO	•	
Responder	NO Value will be placed in the	Strongswan.conf file	
Pass Conn type	Pass	•	
ass Conn Left Subnet	192.168.101.0/24 Local Private Subnet(s)		
Pass Conn Right Subnet	192.168.101.0/24 Remote Private Subnet(s)	1	
Pass Conn Auth	Never	•	
Pass Conn Startup operations	ROUTE	•	

- 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

atus System Netw	ork Statistics	Logout						
terfaces Wifi Firew	all Static Routes	Load Sharing/Failor	ver Diagn	ostics QoS Hostname	s DHC	P and DNS VPN	VRRP Serial	
eneral Settings Stro	ngswan IPSEC Stat	us Online Help			_			
EC Tunnels								
ernet Protocol Security	is a protocol suite fo	r securing Interne	t Protocol o	ommunications by authe	nticating	and encrypting e	wh IP packet of a communicat	tion session
PSec Tunnels					in the second	and and puty a		
Tunnel Name	Left Subnet	Left	Right	Right Subnet	SLE	Tunnel Up	Tunnel Down	
OTA	0.0.0/0	71.16.53.45	%any	192.168.101.0/24	yes	S Tunnel Up	United Tunnel Down	Edit 🗶 Delete
Add IPSEC TUNNEL								
PSEC Defaults								
IKE Life	etime	KeyL	ife	Aggres	sive		Responder	
72	h	24	1	yes			yes	🛃 Edit
DEEC Actions								
PSEC ACTIONS								
IPSEC S	tart	16	SEC Stop			IPSEC Restart		Additions &
di mono	Claud	-	DEEC Plan			DEEC Destert		Cours & Annaly

- 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 I Psec 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

aufacus W.S. Erenall Static Doutes 10	ad Charges/Tailoury Dissection OoC Mestasmen	DHCD and DNG NON MODO Ca	int .
meral Settings Strongswan IPSEC Status	Online Help	DECEMBER OF SEC.	
EC - Tunnels - OTA			
fig the Individual IPSec tunnels			
funnel Name	OTA		
.eft Subnet	0.0.0.0/0	1	
eft	71.16.53.45 IP of local tunnel endpoint	(typically WAN IP. %any for dynamic W	(ANs)
.eft ID	encore B		
.eft Firewall	YES Is the local firewall on or o	e off?	
light	%any 🔕 IP of remote tunnel endpo	int (typically WAN IP. %any for dynamic	: WANs)
SLE	yes		
light Subnet	192.168.101.0/24 Remote Private Subnet(s) To Reduce to 1 entry, use RE	SET->SAVE_APPLY and enter new value	
Remote ID	encore A		
PSec startup operations	ROUTE	•	
Pre-Shared Key	<i>"</i>	ø	

- **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

tus System Network Statistics Logout			
erfaces Wifi Firewall Static Routes Load Sharing/Fai	lover Diagnostics QoS Hostnames DHCP a	and DNS VPN VRRP Serial	
neral Settings Strongswan IPSEC Status Online Help			
EC Defaults			
in the IDSec defaults			
2sec Default Configuration			
ke Lifetime	72h 77 Time: s=seconds,m=minutes,h=ho	iours	
iey Life	24h 🥥 Synonym for lifetime		
teKey Margin	1h Time: s=seconds,m=minutes,h=ho	iours	
leying Tries	2		
ey Exchange	ikev2		
uth	secret	•	
ggressive Mode	YES		
KE Encryption Protocol	AES256	•	
KE Authencation Protocol	MD5		
KE DH Group	Group2		
SP Encryption Protocol	AES256		
SP Authencation Protocol	MD5	-	
SP DH Group	Group2	•	
PD Action	Restart	•	
PD Delay	20s ② Time: s=seconds,m=minutes,h=ho	ours	
PD timeout	120s ime: s=seconds,m=minutes,h=ho	iours	
E-KEY	NO		
E-AUTH	NO	•	
tesponder	YES Value will be placed in the Strongsv	swan.conf file	
lass Conn type	Pass		
lass Conn Left Subnet	10.1.1.0/24 2 Local Private Subnet(s)		
ass Conn Right Subnet	10.1.1.0/24 Remote Private Subnet(s)		
ass Conn Auth	Never	•	
ass Conn Startup operations	ROUTE		

- 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

Statistics with Statistics		o's section of		ourse and ourse area	a second and a	
terfaces With Firewall Static Routes L	oad Sharing/Failover	Diagnostics (205 Hostnames	DHCP and DNS VP	VRRP Senal	
eneral Settings Port Forwards Traffic Rules	Custom Rules					
ewall - Zone Settings						
firewall creates zones over your network inte	rfaces to control netv	vork traffic flow.				
eneral Settings						
Enable SYN-flood protection		V				
Drop invalid packets		V				
Input		accent				
Distort		accept				
Jupu		accept				
Forward		accept				
ones						
Zone Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: 🗾 🗕 wan	accept -	accept	 accept 			🛃 Edit 💌 Delete
wan: wan: 🔬 🖷 ACCEPT	reject 💌	accept	 accept 	▼	V	🛃 Edit 💌 Delete
newzone: (empty) = REJECT	accept	accept	 reject 			🛃 Edit 💌 Delete
Add						

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

atus System Network Statistics Logout			
terfaces Wifi Firewall Static Routes Load Sharing/	ailover Diagnostics QoS Hostnames D	ICP and DNS VPN VRRP Serial	
eneral Settings Port Forwards Traffic Rules Custom R	les		
ewall - Zone Settings - Zone "wan"			
one "wan"			
his section defines common properties of "wan". The input and etween different networks within the zone. Covered networks sp	l output options set the default policies for traffic ecifies which available networks are member of t	ntering and leaving this zone while the forward option is zone.	describes the policy for forwarded traffic
General Settings Advanced Settings			
Name	wan		
Input	reject		
Output	accept		
Forward	accept		
Masquerading	V		
MSS clamping	×.		
Covered networks	🔲 lan: 🖉		
	🗹 🛛 wan: 者		
	create:		
nter-Zone Forwarding he options below control the forwarding policies between this z proted at "wan". The forwarding rule is unidirectional, e.g. a for	one (wan) and other zones. Destination zones cov prward from Ian to wan does not imply a permissi	r forwarded traffic originating from "wan". Source zone n to forward from wan to lan as well.	is match forwarded traffic from other zones
Allow forward to destination zones:	🔲 lan: lan: 🔎		
	newzone: (empty		
Allow forward from source zones:	🗹 Ian: Jan: 🗾		
	newzone: (empty		

- **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

encor <mark>e¹n</mark> etworks ⁻	Chai
Status System Network Statistics Logout	
Interfaces Wifi Firewall Static Routes Load Sharing/Failover Diagn	pnostics QoS Hostnames DHCP and DNS VPN VRRP Serial
General Settings Port Forwards Traffic Rules Custom Rules	
Firewall - Zone Settings - Zone "wan"	
Zone "wan"	
This section defines common properties of "wan". The <i>input</i> and <i>output</i> options set traffic between different networks within the zone. Covered networks specifies whi	et the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded thich available networks are member of this zone.
General Settings Advanced Settings	
Restrict to address family	IPv4 only
Restrict Masquerading to given source subnets	0 0 0 0 0
Restrict Masquerading to given destination subnets	1192.168.101.0/24
Force connection tracking	
Enable logging on this zone	
Inter-Zone Forwarding The options below control the forwarding policies between this zone (wan) and oth other zones targeted at "wan". The forwarding rule is unidirectional, e.g. a forw	ther zones. Destination zones cover forwarded traffic originating from "wan" . Source zones match forwarded traffic from ward from lan to wan does not imply a permission to forward from wan to lan as well.
Allow forward to destination zones:	🗈 lan: 🔝
	newzone: (empty)
Allow forward from source zones:	🗷 lan: 🔝
	newzone: (empty)
Back to Overview	🥝 Reset 🖉 Save 🗔 Save & App

- 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.
 - 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

ocore networks					Changes
Interfaces Wife Firewall Statis Pourles I	oad Sharino/Failovar Diagontics	OoS Notosmer	DHCP and DNS VPN	VPPP Sarial	
General Settings Port Forwards Traffic Pules	Custom Dules	203 Hostianies	DHCP and DHS VPH	VKKP Serial	
Firewall - Zone Settings	Caston Haros				
The firewall creates zones over your network inte	rfaces to control network traffic flow				
General Settings					
Enable SYN-flood protection	V				
Drop invalid packets	V				
Input	accept				
Output	accept				
Forward	accept				
			_		
Zones					
Zone ⇒ Forwardings	Input Output	Forward	Masquerading	MSS clamping	
lan: lan: 🗾 🗕 wan	accept 📼 accept	accept			🛃 Edit 💌 Delete
wan: wan: 🔊 😁 ACCEPT	reject 💌 accept	• accept •	V	V	🛃 Edit 💌 Delete
newzone: (empty) = REJECT	accept 💌 accept	💌 reject 💌			🗹 Edit 💌 Delete
Add 🔝					
				٢	Reset Save Save Apply

- **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, perform only step 1.
- If the tunnel initiator's right subnet is not 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**, 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

ncore [!] networks				Change
Status System Network Statistics Logout				
Interfaces Firewall Static Routes Load Sharing/Failover QoS D	Diagnostics Hostnames	DHCP and DNS VPN	VRRP Serial	
General Settings Port Forwards Traffic Rules Custom Rules				
Firewall - Zone Settings				
The firewall creates zones over your network interfaces to control netwo	rk traffic flow.			
General Settings				
Enable SYN-flood protection	V			
Drop invalid packets				
Input	accept	-		
Output	accept	-		
Forward	accept			
Zone → Forwardings Input Ou	itput Forward	Masquerading	MSS clamping	
lan: lan: 🖉 🔹 wan accept 💌 accept	t 💌 accept			Edit 🗶 Delete
wan: wan: 🖉 = Accept 💌 accept	t 💌 accept		V	🖪 Edit 💌 Delete
* Add				
				🛢 Reset 🧉 Save 🛄 Save & Apply

- **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:

tus System Netwo	statistics L	ogout						
erfaces Firewall St	atic Routes Load Shari	ng/Failover	Qo5 Diagnosti	cs Hostnames D	HCP and D/	NS VPN VRRP	Serial	
neral Settings Stro	ngswan IPSEC Status	Online Hel	P/					
C Tunnels								
net Protocol Security i	s a protocol suite for se	curing Inte	met Protocol com	nunications by authe	nticating a	and encrypting each I	P packet of a communicatio	n session
Sec Tunnels					8			
Tunnel Name	Left Subnet	Left	Right	Right Subnet	SLE	Tunnel Up	Tunnel Down	
OSAT1	192.168.101.0/24	%any	71.16.53.45	192.168.101.0/24	yes	S Tunnel Up	Tunnel Down	Edit 🙁 Delete
Add IPSEC TUNNEL								
SEC Defaults								
IKE Life	time	Ke	yLife	Aggre	ssive		Responder	
72	ic. (3	24h	ye	s		no	🛃 Edit
SEC Actions								
IPSEC St	art		IPSEC Stop		1	PSEC Restart		Modifications & Additions
(# man.	0		DOCTO Chan		100	IDOEC Dested		Cours & Annaly

- 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).

Go to Table of Contents

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

atur Gustern Network Statistics	Inset					
erfaces Firewall Static Routes La neral Settings Port Forwards Traffi	c Rules Custom Rules	QoS Diagno	itics Hostnames D	ICP and DNS VPN V	RRP Serial	
firewall creates zones over your netwo eneral Settings	ork interfaces to contro	l network trai	fic flow.			
nable SYN-flood protection		V				
Drop invalid packets Input		8	accept 💌			
		ac				
Output		accept				
Forward		ac	accept 💌			
Zones						
Zone - Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: 🧾 🛥 wan	accept 💌	accept	★ accept ★		8	Edit 💌 Delete
wan: wan: 🧾 🖷 ACCEPT	accept 💌	accept	• accept •	9		🔀 Edit 📧 Delete
Add						

- **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

Interfaces Wifi Firewall Static Routes Load Sharing/Failow	ar Diagnostics QoS Hostnames	DHCP and DNS VPN	VRRP Serial	
General Settings Port Forwards Traffic Rules Custom Rules				
rewall - Zone Settings - Zone "wan"				
Zone "wan" This section defines common properties of "wan". The input and output traffic between different networks within the zone. Covered networks sy General Settings Advanced Settings	options set the default policies for traffic e pecifies which available networks are mem	ntering and leaving this zon- ber of this zone.	e while the forward option de	scribes the policy for forwarded
Restrict to address family	IPv4 only			
Restrict Masquerading to given source subnets	0.0.0/0	2		
Restrict Masquerading to given destination subnets	1192.168.101.0/24	<u>*</u>		
Force connection tracking	8			
Enable logging on this zone	8			
Inter-Zone Forwarding The options below control the forwarding policies between this zone (w other zones targeted at "wan". The forwarding rule is unidirectional, Allow forward to destination zones:	in) and other zones. Destination zones cov e.g. a forward from lan to wan does not in lan: lan: ja newzone: (empty)	er forwarded traffic origina ply a permission to forward	ting from "wan". Source z I from wan to lan as well.	ones match forwarded traffic from
Allow forward from source zones:	Ian: Ian: Ian: Ian: Ian: Ian:			

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

atus System	Network Statistics	Logout			_			_
terfaces Wifi	Firewall Static Routes	Load Sharing/Failover Diagnostics QoS Hostnames	DHCP and DNS VPN V	/RRP Serial		-	-	
eneral Settings	Port Forwards Traffic Rule	s Custom Rules			-	-	-	-
ewall - Traffic	c Rules							
fic rules define p	olicies for packets traveling	between different zones, for example to reject traffic between	certain hosts or to open	WAN ports on the router.				
raffic Rules								
Name		Match		Action	Enable	Sort		
		IPv4-UDP						
DHCP-Renew		From any host in wan To any router IP at port 66 on this device		Accept input	V	• •	🛃 Edit	X Delet
Allena Diese		IPv4-ICMP		Annual forward			2 E-JA	Delet
Allow-Ping		To any host in any zone		Accept rormana			L'UIL	Delet
Allow-HTTP		IPv4-TCP From any host in any zone		Accept input	1		🛃 Edit	E Delet
		To any router IP at port 80 on this device IPvd-TCP						
Allow-HTTPS		From any host in any zone		Accept input	1	•	🛃 Edit	× Delet
		IPed-TCP						-
Allow-SSH		From any host in wan To any router 0º at port 22 on this device		Accept input		••	🛃 Edit	× Delet
Allow-DHCPv6		IPv6-UDP From IP range FE80:0:0:0:0:0:0:0:0/10 in was with source post 547		Accept input			Z Edit	× Delet
		To IP range FE80:0:0:0:0:0:0:0:0/10 at port 546 on this device		consider subset		ک ک	and most	
Allow-	rvo-aumr with types echo-request, ed	 reply, destination-unreachable, packet-loo-big, time-exceeded, bad-header, unknov neighbour-solicitation, router-advertisement, neighbour-advertisement 	in-neader-lype, rouler-solicitation,	Accept input and limit to 1000 pkts.	7		Edit	× Delet
ICMPv6-Input		From any host in wan To any router IP on this device		per second	-	20	and mont	
Allow-ICMPv6-	IPv6-ICMP with types echo-re	uest, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-heade From any host in wan	v, unknown-header-type	Accept forward and limit to 1000			🖉 Edit	× Delet
Forward		To any host in any zone		pkts. per second	_		and most	
Enforce- ILA-Border-Src		From IP range FC00:0:0:0:0:0:0/7 in any zone		Refuse forward		•	🛃 Edit	× Delet
t dans		To any heat in way IPv6-TCP+UDP						
Enforce- LA-Border-Dest		From any host in any zone To 2P renne EC00-0-0-0-0-0-0/2 in year		Refuse forward	1	٠	🔏 Edit	× Delet
10501		IPv4-TCP		Arrest insul	121			Delet
10501		From any host in wan To any router IP at port 10301 on this device		Accept Input			Eat	× Delet
5000		Any TCP From any host in any zone		Accept forward		• •	🛃 Edit	× Delet
		To any host in any zone						
IPSec_esp		From any host in wan		Accept input	1	• •	🛃 Edit	× Delete
		To any router IP on this device IPv4-IPSEC-AM			_			
IPSec_AH		From any host in wan To any router IP on this device		Accept input	1	* *	🛃 Edit	× Delete
IPSEC IKE		Any UDP From any boot in wan		Accept input	V		Edit	
		To any router IP at port 500 on this device		Security subsc		ك ك	and mont	00.00
ipsec_NAT_T		Any UDP From any host in wan		Accept input	V	•	🗾 Edit	🗶 Delet
		To any router 39 at port 4500 on this device						
pen ports on ro	uter:							
Name	Protocol	ternal port						
New input rule	TCP+UDP 💌	tal Add						
ton former to the								
Name	Source zone Des	tination zone						
New forward rule	lan 💌 war	Add and edit						
ource NAT	cific form of masquarading	which allows fine orained control over the source TD used for out-	noing traffic, for exemple i	n man multiple WAN addresses to is	sternel	subnetz		
ame	terre room or masqueraoing i	Match	yong danig tor example t	Aria Aria Aria Aria Aria Aria Aria Aria	tion	a sheat	Fee	ble Sort
		This section contains no	values yet					
New source NAT:								
Name	Source zone Destination	zone To source IP To source port						
New SNAT rule	an 💌 wan	Please cho						

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 $${\rm TCP}_{-}10501$$

us System Network Statistics Logout		
ofaces W/I Firewall Static Routes Load Sharing/Fallover	Disprestics QeS Hestnames DHCP and DNS VPN VRRP Serial	
eral Settings Port Forwards Traffic Rules Custom Rules		
wall - Traffic Rules - 10501		
sage allows you to change advanced properties of the traffic rule entry	, such as matched source and destination hosts.	
ule is enabled	@ Disable	
arra	10801	
estrict to address family	iPv4 only	
lesete	TCP v	
ton ICMP type	any 💌 🔁	
turge zone	C Any zone	
	Data and A	
	ewzone (empty)	
	👻 wats wat: 🔉	
surce MAC address	ary 🐷	
ource address	any 🐷	
surce port	147Y	
estination zone	Device (input)	
	Any zone (forward)	
	newsone: (empty)	
	want want 2	
ssination address	ary 🔽	
estination port	10501	
flor.	accept	
its arguments		
	 These encodes experiments in presents, vol. 107-1280. 	

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

core networks		Chary
Interfaces Wit Firewall Static Routes Load Sharing/Fallover D	agnostics QoS Hostnames DMCP and DNS VPN VILIAP Serial	
General Settings Fort Forwards Traffic Rules Custom Rules		
Firewall - Traffic Rules - IPSec esp		
This page allows you to change advanced properties of the traffic rule entry, so	if as matched source and destination hosts.	
Rule is enabled	0 Disable	
Name	(PSec_esp	
Restrict to address family	IPv4 only	
Protocol	esp 🐙	
Metch ICMP type	ary 🗶	
Source zone	Any zone	
	newzone: (empty)	
	🗶 water water 🖉	
Source MAC address	any 💌	
Source address	any 💌	
Source port	ary .	
Destination zone	Device (input)	
	Any zone (forward)	
	O Intel Int. 7	
	v newzone (empty)	
	🔍 wati vati 者	
Destination address	any 🐷	
Destination port	ary .	
Action	accept tessors	
Extra argumenta	Paulus Antificat and marks to interior Una	
	W Frank Review in prime in contrast, will REVEN	
Bark to Duarview		Basat C Sava D Sava & Annu
and the second sec		A unter A once R once which

• AH protocol (see Figure 10-19).

Note: For the Destination Port, specify any.

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

eral Settings Port Forwards Traffic Rules Custom Rules		
wall - Traffic Rules - IPSec_AH		
age allows you to change advanced properties of the traffic rule entry	such as matched source and destination hosts.	
vie is enabled	Oisable	
sme	IP\$ec_AH	
estrict to address family	IPv4 only	
1000	ah 🖉	
etch SCMP type	any 🗶 📷	
Surge some	Any zone	
	C Inni Inni 2	
	The sector of th	
surce MAC address	ary 🐷	
surce address	atty 🐷	
hog source	ary .	
estination zone	Device (input)	
	Any zone (forward)	
	C Ians (an: 2)	
	menane: (empty)	
estination address	any 💌	
estination port	ary	
alon	accept	
tra argumenta		

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

Figure 10-20. Firewall Rule Configuration Screen for VPNs

IKE

faces W/6 Firewall Static Routes Load Sharing/Failover	Diagnostics QoS Hostnames DHCP and DNS VPN VRRP Serial	
al Settings Port Forwards Traffic Rules Custom Rules		
vall - Traffic Rules - IPSEC_IKE		
ege allows you to change advanced properties of the traffic rule entry,	such as matched source and destination hosts.	
e is enabled	0 Disable	
me.	PSEC_KE	
strict to address family	IPv4 and IPv6	
čacol	UDP 🗨	
toh ICMP type	any 💌 📜	
Jone Jone	C Any zone	
	ewzone: (empty)	
	🔍 water water Z	
iros MAC address	any 💌	
inter address	Μγ 🐷	
ures port	(My	
cination zone	Device (input)	
	Any space (forward)	
	O market	
	newsones (empty)	
	U WARE HARE &	
tination address	εγ 🐙	
Enation port	800	
54	accept y	
a arguments		

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



terfaces W/L Firewall Static Routes Load Sharing/Fallover	Disproxition QuS Hostnames DHCP and DNS VPN VRRP Serial	
eral Settings Port Forwards Traffic Rules Custom Rules		
wall - Traffic Rules - ipsec_NAT_T age allows you to change advanced properties of the traffic rule entry.	such as matched source and destination hosts.	
ule is enabled	© Disable	
lame	psec_NAT_T	
estrict to address family	IPv4 and IPv6	
ntacal	UDP 💌	
latuh ICMP type	ary 💌 🗊	
ource zone	O Are rear	
	newsones (empty)	
	🖲 wats wats Z	
ource MAC address	ary 🐷	
jource address	any 🔤	
ource port	any	
estination zone	Device (input)	
	Any zone (forward)	
	D Inter M	
	V wat wat g	
estination address	any 🐙	
Jestination port	4500	
eten	accept	
txtra argumenta	Passes additional arguments to totables. Use with carel	

Go to Table of Contents

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

erfaces Wifi Firewall Static Boutes Load Sharing/Failov	er Diagnostics QoS Hostnames DHCP and DNS VPN VRRP Serial
neral Settings Port Forwards Traffic Rules Custom Rules	
wall - Traffic Bules - SNAT source NAT	
page allows you to change advanced properties of the traffic rule er	ntry, such as matched source and destination hosts.
ule is enabled	© Disable
lame	source NAT
rotocol	All protocols
iource zone	lant lant <u>j</u> !
	newzone: (empty)
iource MAC address	
iource IP address	any 💌
iource port	any Of the second se
Destination zone	🔘 Jan: Tan: 🚈
	O newzone: (empty)
	🔍 wan: 🖉
Destination IP address	192.168.101.0/24
Destination port	Stry State forwarded traffic to the given destination port or port range.
NAT IP address	10.1.1.1 (brian)
NAT port	Do not rewrite Rewrite metched buffic to the given source port. May be left empty to only rewrite the IP address.
xtra arguments	Passes additional arguments to iptables. Use with care!

- 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

encor <mark>e n</mark> et	works				Um	saved Changes
Status Syste System Adr Dashboard	em Network Statistics Logo ministration Startup Scheduled Task Configure	t Time Synchronisation	Backup/Restore Custom Commands R	Reboot		
Custom Com This page allows	imands I you to configure custom shell commands	which can be easily invoked	from the web interface.			
A short te	Description solual description of the configured command	Command Command line to execute	Custom arguments Alex the user to provide additional command t	ine arguments	Public access Alow executing the command and downloading its output without prior authentication	
Add			This section contains no valu	lues yet		
					Save Save Save	ive & Apply

- **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

Logout ed Tasks Time Synchronisation mands which can be easily invoked	Backup/Restore Custom Commands	Reboot	
Command ommand line to execute Allow the user to	Custom arguments provide additional command line arguments Allow	Public access executing the command and downloading its output without prio	r authentication
			× Delete
	Logout d Tasks Time Synchronisation mands which can be easily invoked Command mmand line to execute Allow the user to	Logout d Tasks Time Synchronisation Backup/Restore Custom Commands mands which can be easily invoked from the web interface. Command Custom arguments mmand line to execute Allow the user to provide additional command line arguments Allow	Logout d Tasks Time Synchronisation Backup/Restore Custom Commands Reboot mands which can be easily invoked from the web interface. Command Custom arguments Public access mmands ine to execute Allow the user to provide additional ammand line arguments Allow executing the command and downloading to output without pro

- 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

Status System Network Statistics	ogout			
System Administration Startup Scheduled	Tasks Time Synchronisation	n Backup/Restore Custom Commands Reboot		
Dashboard Configure				
Curton Commands				
Description	Command	Custom arguments	Public access	
			Alow executing the command and downloading its output without prior authentication	
A short textual description of the configured command	Command line to execute	Allow the user to provide additional command line arguments	Allow executing the command and downloading its output without prior authentication	
A short textual description of the configured command Restatus	Command line to execute Instatut In	Allow the user to provide additional command line arguments	Alow executing the command and downloading its output without prior authentication	E) Delete
A short textual description of the configured command plostatus	Command line to execute	Allow the user to provide additional command line arguments	Allow executing the command and downloading its output without prior authentication	🛋 Delete

- 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

encor <mark>e¹n</mark> etworks ⁻				Changes:
Status System Network Statistics Log	sut.			
System Administration Startup Scheduled Tax	ks Time Synchronisation	Backup/Restore Custom Commands Reboot		
Dashboard Configure				
Custom Commands				
This page allows you to configure custom shell command	is which can be easily invoke	d from the web interface.		
Description	Command	Custom arguments	Public access	
A short textual description of the configured command	Command line to execute	Allow the user to provide additional command line arguments	Allow executing the command and downloading its output without prior authentication	
plestatus	netstat 4n			🛋 Delete
Add 1				
			Beset Save	Save & Apply

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

encor <mark>e.n</mark> etworks [.]	Changes: 0
Status System Network Statistics Logout	
System Administration Startup Scheduled Tasks Time Synchronisation Ba	ickup/Restore Custom Commands Reboot
Dashboard Configure	
Custom Commands	
- destatue	
Command: setstas -te	
🛙 Run 🗯 Download	
L	

- 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

encor <mark>e n</mark> etworks				Changes
Status System Network System Administration S Dashbeard Configure Custom Commands	Statistics Lopout itartup Scheduled Tasks T	me Synchronisation Backup/Restore	Custom Commands	Rabor
slestatus Command: sessas -tn Run 🌢 Download				
# messax -un Antire Internet consections /W Press Recr-2 Send-2 lead Not 0 0 0 11.45.814 Nop 0 0 11.45.814 Command successful (Coder 0)	/* servers) ess Decign Address 5:00 71.10.52.44:56510 5:0001 10.40.01.00:16842 5:15001 10.40.1.00:16842 5:15001 10.40.1.00:168784 5:2500 72.16.33.44:56509	Šuss Efialies Stalies Efialies Efialies Efialies Efialies Efial		

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.