

Configuring IPsec VPNs in the EN-2000™

ne of the principal features of routers is their support of virtual private networks (VPNs). This document discusses configuration of a VPN connection.

Note: 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 the EN-2000's IPsec VPN tunnels, study the material discussed in Virtual Private Networks and confer with your network administrator.

See the following sections:

- Configuring an EN-2000 as a VPN Tunnel Initiator
- Configuring an EN-2000 as a VPN Tunnel Responder

Note: In the VPN tunnel configuration screens, "left" indicates "local" (that is, it indicates the EN-2000 router) and "right" indicates "remote" (the device at the other end of the connection).

For information about VPNs, see the document Virtual Private Networks. For additional (required) VPN processes, see the following documents:

- Configuring the EN-2000's VPN Firewall
- Starting and Tracking VPNs in the EN-2000

9.1 Configuring an EN-2000 as a VPN Tunnel Initiator

- 1 Log into the EN-2000. (For details, see *Logging In*, on page 2 of the document Using the EN-2000's Management System.)
- 2 On the EN-2000 management system, select the **Network** tab. Then select the VPN tab. If necessary, select the General Settings tab.
 - The IPsec VPN Tunnel Table for a VPN Tunnel Initiator is displayed (Figure 9-1).

Figure 9-1. IPsec VPN Tunnel Table for a VPN Tunnel Initiator

tatus System Netwo	ork Statistics L	ogout						
rfaces Firewall St	atic Routes Load Shari	ng/Failover	QoS Diagnosti	cs Hostnames D	HCP and D	NS VPN VRRP	Serial	
eral Settings Stron	gswan IPSEC Status	Online Help						
Tunnels								
net Protocol Security i Sec Tunnels	s a protocol suite for se	curing Interr	net Protocol comm	nunications by authe	enticating	and encrypting each	IP packet of a communication	on session
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	2 Tunnel Up	Tunnel Down	🛃 Edit 💌 Delete
Add IPSEC TUNNEL								
SEC Defaults								
IKE Lifetime		KeyLife		Aggre	Aggressive		Responder	
72h		2	24h ye		s		no	🛃 Edit
PSEC Actions								
IPSEC Start		IPSEC Stop		IPSEC Restart			Modifications & Additions	
di IDREC Start		IPSEC Stop			PSEC Restart			

- 3 On that screen, select the box to Enable IPsec for this unit.
- 4 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 9-2).

Core-networks		Cha
Status System Network Logout Quickstart		
Interfaces Hostnames Static Routes Failover Firewal	Diagnostics QoS VPN VRRP	
General Settings IPSEC Status		
Sec - Tunnels - (Unnamed Tunnel)		
nfig the Individual IPSec tunnels		
Tunnel Name		
Left Subnet	192.168.1.0/24 Cost Private Submat(s) To Reduce to 1 endpy, use RESET->SAVE_APPLY and enter new value	
Left	1.1.1.2 IP of local tunnel endpoint (typically WAN IP. % any for dynamic WANs)	
Left ID	encorenetworks.com	
Left Firewall	NO v Is the local firewall on or off?	
Right	1.1.1.2 IP of remote tunnel endpoint (typically WAN IP. % any for dynamic WANs)	
<u>Right Subnet</u>	0.0.0.0/0 10 Remote Private Submet(s) To Reduce to 1 entry, use RESET-> SAVE_APPLY and enter new value	
Remote ID	encore Remote User Name	
IPSec startup operations	START	
Pre-Shared Key	<i>»</i>	
Back to Oversian		Recet R Save & An

Figure 9-2. IPsec Tunnel Configuration Screen for a VPN Tunnel Initiator

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

Note the following required values for the VPN tunnel initiator:

- Set the Left IP address to %any.
- Set the Left Firewall to No (off).
- Set IPsec Startup Operations to Start.
- Type the Preshared Key.

Note: Both sides of the VPN tunnel (initiator and responder) must use the same pre-shared key. Get the key from your network administrator.

The following are sample values.

- Tunnel Name: Tunnel_01
- Left Subnet: *a.b.c.*0/24 (where *a.b.c* indicates the local private network). Note: 24 is the IP prefix; its maximum value is 32.
- Left ID: [*a character string*] (representing the local EN-2000) Note: The VPN tunnel initiator's Left ID must match the VPN tunnel responder's Right ID. In like manner, the initiator's Right ID must match the responder's Left ID.
- **Right:** *i.j.k.l* (where *i.j.k.l* is the remote router's public IP address)
- **Right Subnet:** *m.n.p.*0/24 (where *m.n.p* indicates the remote private network)
- Right [Remote] ID: [a character string] (representing the remote EN-2000)
- 6 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 Table for a VPN Tunnel Initiator is redisplayed (recall Figure 9-1).
- 7 On the IPsec VPN Tunnel Table 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 9-3).

Go	to	Tab	le
of	Cor	iten	ts

Defaults			
the IPSec defaults			
ec Default Configuration	PHK.		
Linetime	Time: s=seconds,m=mir	vCes,h=hours	
y Life	24h Synonym for lifetime		
Key Margin	Ih	fan ha ba a	
ying Tries	2		
y Exchange	[kev2		
th	secret	•	
gressive Mode	YES	*	
E Encryption Protocol	AE\$256	•	
E Authencation Protocol	MD5	•	
E DH Group	Group2	•	
P Encryption Protocol	AE\$256	•	
P Authencation Protocol	MD5	•	
P DH Group	Group2		
D Action	Restart	•	
D Delay	[20s		
0 timesut	Time: s=seconds,m=mir	utes, he hours	
a sumayar	Time: s=seconds,m=min	utes, his hours	
-KEY	NO	×	
AUTH	NO	¥	
sponder	NO Value will be placed in the	Strongswan.conf file	
ass Conn type	Pass		
ass Conn Left Subnet	192.168.1.0/24	net(s)	
ass Conn Right Subnet	192.168.1.0/24	ubnet(s)	
ass Conn Auth	Never		
ass Conn Startup operations	ROUTE		

Figure 9-3. IPsec Defaults Configuration Screen for a VPN Tunnel Initiator

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

Note the following required values for the VPN tunnel initiator:

- Set Responder to No. (This EN-2000 is the tunnel initiator.)
- Set Pass Conn Type to Pass (passthrough).

Note: When you select Pass, additional fields are displayed.

- Set Pass Conn Auth to Never.
- Set Pass Conn Startup Operations to Start.

The following are sample values.

- 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
 - Pass Conn Left Subnet: The local LAN subnet
 - Pass Conn Right Subnet: The local LAN subnet

Note: The Pass Conn Left Subnet and the Pass Conn Right Subnet must be identical.

- **9** 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 Table for a VPN Tunnel Initiator is redisplayed (recall Figure 9-1).
- 10 On the IPsec VPN Tunnel Table for a VPN Tunnel Initiator, select the **Save &** Apply button (at the lower right of the screen).

The EN-2000 has been configured as an IPsec VPN tunnel initiator.

9.2 Configuring an EN-2000 as a VPN Tunnel Responder

- 1 Log into the EN-2000. (For details, see *Logging In*, on page 2 of the document *Using the EN-2000's Management System*.)
- 2 On the EN-2000 management system, select the **Network** tab. Then select the **VPN** tab. If necessary, select the **General Settings** tab.
 - The IPsec VPN Tunnel Table for a VPN Tunnel Responder is displayed (Figure 9-4).

Figure 9-4. IPsec VPN Tunnel Table for a VPN Tunnel Responder

Concernering	Operation S	Catus: Online	uning WAN				
Linter Trainers Nets	rock Ligner 50						
Eriterfanns Healthamad				VPN VENP			
General Settings	S Status						
PSEC Tunnels							
nternet Protocal Security in TPSec Tumnels	a protocol suite for seco	aring Interne	t Protocol communicatio	ons by authenticating and	l encrypting each IP pa	cket of a communication set	alan
Tunnel Name	Left Subset	Left	Right	Right Subset	Tunnel Up	Tunnel Down	
TESTI	192.168.10.0/24	Naty	166-249-107-17	192.168.1.0/24	S Tunnel Op	Tunnel Down	Edit M Delete
Add IPSEC TUNNEL							
IPSEC Defaults							
INE LA	etime	Ke	yLife	Aggressive		Responder	
72	h		24h	245			(LEda
IPSEC Actions							
IPSEC Start		IPSEC Stop		IPSEC Restart		Modifications & Additions	
E IPSEC Start		O PSEC Stor		D PSEC Restart		Biave & Apply	

- 3 On that screen, select the box to Enable IPsec for this unit.
- 4 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 9-5).

Figure 9-5. IPsec Tunnel Configuration Screen for a VPN Tunnel Responder

stus System Network Statistics	Logour	
terfaces Wifi Firewall Static Routes L	Jad Shanng/Failover Diagnostics QoS Hostnames DHCP and DNS VPN VRRP Senal	
cheral Settings Strongswan (Poce Statu	Vouis rep	
EC - Tunnels - OTA		
fig the Individual IPSec tunnels		
funnel Name	ATO	
.eft Subnet	00000	
	Local Private Subnet(s)	
Left	71.16.53.45	
	IP of local tunnel endpoint (typically WAN IP. %any for dynamic WANs)	
left ID	encore B	
off Eirourall		
CELT IN EWON	Is the local firewall on or off?	
Right	Sanv	
	IP of remote tunnel endpoint (typically WAN IP. %any for dynamic WANs)	
SLE	yes	
Right Subnet	192.168.101.0/24	
	Remote Private Subnet(s) To Reduce to 1 entry, use REFET > SAVE APRIX and actes new value	
Pomoto ID	to Reade to 1 entry, the REALTY SAVE_APTER and enter new value	
Nelloce ID	<pre>@ Remote User Name</pre>	
IPSec startup operations	ROUTE	
Pre-Shared Key	2	

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

Note the following required values for the VPN tunnel responder:

- Set the Left Subnet to 0.0.0.0.
- Set the Left IP address to this EN-2000's WAN IP address.

Note: The VPN tunnel responder's WAN interface must use a static IP address so that it is accessible to the initiator.

- Set the Left Firewall to Yes (on).
- Set the **Right** IP address to **% any**.
- Set the Right Subnet to the subnet of the initiator EN-2000.
- Set IPsec Startup Operations to Route.
- Type the Preshared Key.

Note: Both sides of the VPN tunnel (initiator and responder) must use the same pre-shared key. Get the key from your network administrator.

The following are sample values.

- Tunnel Name: Tunnel_01
- Left ID: [a character string] (representing the local EN-2000)

Note: The VPN tunnel initiator's Left ID must match the VPN tunnel responder's Right ID. In like manner, the initiator's Right ID must match the responder's Left ID.

- **Right [Remote] ID**: [*a character string*] (representing the remote EN-2000) Do not use this sample pre-shared key; is it merely an example. For purposes of demonstration, the sample pre-shared key includes the lowercase letter "I" (ell); do not mistake it for the number "1" (one).
- 6 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 Table for a VPN Tunnel Responder is redisplayed (recall Figure 9-4).
- 7 On the IPsec VPN Tunnel Table 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 9-6).

ec Defaults			
fig the IPSec defaults			
Psec Default Configuration			
Ike Lifetime	72h 🕥 Time: seseconds.meminutes.h	ehours	
Key Life	24h Synonym for ilfetime		
ReKey Margin	1h Q Time: s=seconds,m=minutes,h	ahous	
Keying Tries	2		
Key Exchange	[kev2		
Auth	secret	*	
Aggressive Mode	TYES		
IKE Encryption Protocol	AES256	-	
IKE Authencation Protocol	[MD5		
IKE DH Group	Group2	•	
ESP Encryption Protocol	AES256		
ESP Authencation Protocol	MD5	-	
ESP DH Group	Group2		
DPD Action	Restart		
DPD Delay	20s Ime: s=seconda,m=minutes,1	*hours	
DPD timeout	120s Q Time: s=seconds,m=minutes,*	nhours	
RE-KEY	NO		
RE-AUTH	NO		
Responder	NO Value will be placed in the Strong	gs×sn.conf file	
Pass Conn type	Pass		
Pass Conn Left Subnet	192.168.1.0/24 Local Private Subnet(;))	
Pass Conn Right Subnet	192.168.1.0/24 Remote Private Subn	et(s)	
Pass Conn Auth	Never	•	
Pass Conn Startup operations	ROUTE		

Figure 9-6. IPsec Defaults Configuration Screen for a VPN Tunnel Responder

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

Note the following required values for the VPN tunnel responder:

- Set Responder to Yes.
- Set Pass Conn to Pass (passthrough).

Note: When you select Pass, additional fields are displayed.

- Set Pass Conn Auth to Never.
- Set Pass Conn Startup Operations to Route.

The following are sample values.

- 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
 - Pass Conn Left Subnet: The local LAN subnet
 - Pass Conn Right Subnet: The local LAN subnet

Note: The Pass Conn Left Subnet and the Pass Conn Right Subnet must be identical.

- **9** 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 11 has been completed.
- 10 Select the Back to Overview button.
 - The IPsec VPN Tunnel Table for a VPN Tunnel Responder is redisplayed (recall Figure 9-4).
- 11 On the IPsec VPN Tunnel Table for a VPN Tunnel Responder, select the **Save** & Apply button (at the lower right of the screen).
 - ✤ The EN-2000 has been configured as an IPsec VPN tunnel responder.

9.3 The Next Steps

The following items need to be addressed:

- 1 Perform the procedures in the document *Configuring the EN-2000's VPN Firewall.*
- **2** Then perform the procedures in the document *Starting and Tracking VPNs in the EN-2000*.

Note: If you wish to study VPNs, see the document Virtual Private Networks.