

Configuring the EN-2000's VPN Firewall

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

- Configuring the Firewall for an IPsec VPN Tunnel
- Configuring the Source NAT

Note: In the EN-2000 management system, the term "left" represents "local," and the term "right" represents "remote." Those designations are always from the point of view of the router being managed-the local ("left") EN-2000.

Also see the following documents:

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

10.1 Configuring the Firewall for an IPsec VPN Tunnel

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

- Firewall Zones
- Firewall Traffic Rules

10.1.1 Firewall Zones

Some firewall zones require configuration changes to support IPsec VPNs.

- On the EN-2000 management system, select the **Network** tab. Then select the 1 Firewall tab. If necessary, select the General Settings tab.
 - The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is displayed (Figure 10-1).

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

erfaces Hostnames Static Routes Failover Firewall Diagnostics QoS VPN VRRP neral Settings Port Forwards Traffic Rules ewall - Zone Settings hrewall creates zones over your network interfaces to control network traffic flow. eneral Settings nable SYN-flood protection rop invalid packets nput accept int accept Zone ⇒ Forwardings Input Output Forward Masquerading MSS clamping Inc: [an: [an: [a]] = wan cell accept → [reject →] [] [] [] [] [] [] [] [] [] [] [] [] [erfaces Hostnames Static Routes Failover				
Port Forwards Traffic Rules wall - Zone Settings Image: Setting settin		FILE AND DISTRIBUTIONS	OoS VPN VE		
wall - Zone Settings irewall creates zones over your network interfaces to control network traffic flow. eneral Settings nable SYN-flood protection Image: Synonymetric synonymetri synonyme	neral Settings Port Forwards Traffic Rules				
wall - Zone Settings irewall creates zones over your network interfaces to control network traffic flow. eneral Settings nable SYN-flood protection or op invalid packets input accept utput accept orward reject ones Zone ⇒ Forwardings Input output accept • inspect • ones • inspect					
Inewall creates zones over your network interfaces to control network traffic flow.	wall - Zone Settings				
aneral Settings hable SYN-flood protection rop invalid packets uput accept t accept t a	irewall creates zones over your network interface	s to control network traffi	c flow.		
nable SYN-flood protection rop invalid packets uput accept v utput accept v reject v reje	eneral Settings				
rop invalid packets	nable SYN-flood protection				
put accept · · utput accept · · prward reject · · mes Zone → Forwardings Input Output Forward Masquerading MSS clamping Ian: Ian: ♪ → wan cell accept · reject · @ @ @Edit x Delete wan: wan: ♪ → REFECT reject · @ @ @Edit x Delete	rop invalid packets				
utput accept • orward reject •	put	accept		*	
orward reject • Torward reject • Torward Nasquerading MSS clamping Ian: lan: 2 → wan cell accept • reject • Wan: wan: 2 → REFECT reject • Celt * Delete	utput	accept		•	
Zone ⇒ Forwardings Input Output Forward Masquerading MSS clamping Ian: lan: lan: lan: lan: lan: lan: lan: l	prward	reject		•	
Zone > Forwardings Input Output Forward Masquerading MSS clamping Ian: Ian: * > wan cell accept • reject • Image: Cell * Image: Cell * wan: wan: * > REFECT reject • Image: Cell * Image: Cell * Image: Cell *					
Zone > Forwardings Input Output Forward Masquerading MSS clamping Ian: Ian: * * wan cell accept * reject * Image: * Image: * MSS clamping wan: * * * REJECT reject * Image: * <th>ones</th> <th></th> <th></th> <th></th> <th></th>	ones				
Ian: lan: : :> wan cell accept • reject • Image: Cell * Celete wan: wan: : :> :> REJECT reject • accept • reject • Image: Cell * Celete	Zone ⇒ Forwardings Input	Output Forward	Masquerading	MSS clamping	
wan: w	lan: lan: 💒 ⇒ wan cell accept •	accept • reject •			Edit Delete
	wan: wan: 🖉 🔿 REJECT	accept • reject •	۲	2	ZEdit Delete
cell: cell: ≱ ⇒ REJECT reject v reject v reject v @ @Edit ★Delete	~			(a)	
cell: cell: * = PETECT reject v accent v reject v	wan: wan: A REJECT reject	accept • reject •	۲	×	

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

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

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

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

tus System Network Statistics Logout		
erfaces Wifi Firewall Static Routes Load Sharing/Failo	ver Diagnostics QoS Hostnames DHCP and DNS VPN VRRP Serial	
neral Settings Port Forwards Traffic Rules Custom Rules		
wall - Zone Settings - Zone "wan"		
one "wan"		
is section defines common properties of "wan". The input and out tween different networks within the zone. Covered networks specifi	put options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forward es which available networks are member of this zone.	ed traffic
General Settings Advanced Settings		
lame	wan	
nput	reject	
Dutput	accept	
orward	accept	
tasquerading	V	
tSS clamping	Z	
Covered networks	lan: 🧾	
	🕅 wan: 🖉	
	create:	
Iter-Zone Forwarding e options below control the forwarding policies between this zone geted at "wan". The forwarding rule is unidirectional, e.g. a forwa	(wan) and other zones. Destination zones cover forwarded traffic eriginating from "wan" . Source zones match forwarded traffic from o Id from Ian to wan does not imply a permission to forward from wan to Ian as well.	ther zones
llow forward to destination zones:	🔲 lan: lan: 🔊	
	newzone: (empty)	
llow forward from source zones:	🗹 lan: lan: 🖉	
	newzone: (emply)	

- **3** On the General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder, configure the following:
 - Under the heading General Settings:
 - Set Input to Reject.
 - Set Output to Accept.
 - Set Forward to Accept.
 - Enable Masquerading.
 - Enable MSS Clamping.
 - For Covered Networks, select WAN.
 - Under the heading Interzone Forwarding:
 - For Allow Forward for Source Zones, select the source zone LAN.
- **4** When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).

Note: If masquerading is enabled for the zones of interest under firewall configuration, then, for IPsec to work properly, packets destined for the right subnet cannot be masqueraded. Step 5 through step 7 resolve that concern.

- **5** Then select the **Advanced Settings** tab on the General Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder.
 - The Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder is displayed (Figure 10-3).

ncore-networks	ning WIN		Changes:
Status Vyolee Network Light Qolkatar	Disposition Oct. VHI VARP		
General Settings Fort Personale Tradic Julies			
Firewall - Zone Settings - Zone "wan"			
Zone "wath" This section defines common properties of "wath". The input and out forwarded traffic between different networks within the pone. Given	put options set the default policies for tra of networks specifies which available net	ffic antening and leaving this zone while the forward i works are member of this zone.	option describes the policy for
General Bettings Advanced Settings	2000/01/1	1017	
Restrict to address family	IPv4 only	•	
Restrict Masquerading to given source subnets	5.0.0.05	1	
Restrict Masquerading to given destination subnets	192 168 1 0/24	10	
Force connection tracking	0		
Enable logging on this zone			
Inter Zone Forwarding The options below control the forwarding policies between this zone from other zones targeted at "was". The forwarding rule is under	(wan) and other zones. Destination zone ectional, e.g. a forward from lan to wan d	s cover forwarded traffic originating from "wan" . oes not imply a permission to forward from wan to ia	lource zones match forwarded traffic in as well.
Allow forward to destination zones:	🗉 cell: cell: 🖉		
	D Inc Inc A		
Allow forward from source zones:	D celt cel: 2		
	8 less lats gt		

Figure 10-3. Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Responder

- Go to Table of Contents
- 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-2000.
 - This turns off masquerading for the VPN tunnel.

Note: The initiator must also disable masquerading for this connection. After you finish the current procedure, see *Disabling Masquerading on the VPN Tunnel Initiator*, on page 5.

- **b** If you wish to exempt an additional destination subnet, select the **Add** button beside the that field, and repeat substep 6.a.iii.
- c Under the heading Interzone Forwarding:
 - For Allow Forward from Source Zones, select LAN.
- 7 When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).
 - Masquerading for the subnet has been disabled, so that VPNs will work properly.
- 8 Then select the Back to Overview button.
 - The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is redisplayed (Figure 10-4).

cor <mark>e•n</mark> etworks	Device Mode: Cell Signal: -9 Operation Sta	Cell Failove GdBm tus: Online	using Cell	00090958		Chang	
atus System Network L terfaces Hostnames Static Route eneral Settings Port Forwards rewall - Zone Settings	ogout Quick 25 Fallover Traffic Rules	Start Firewall	Diagnostics	QoS VPN VF	RRP		
firewall creates zones over your net General Settings	work interfaces	to control i	network traffic	flow.			
Enable SYN-flood protection							
Drop invalid packets							
Input		accept	accept •				
Output		accept			•		
Forward			reject •				
lones							
Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan: lan: 🗾 ⇒ wan cell	accept •	accept •	reject •			ZEdit Delete	
wan: wan: 🚂 ⇒ REJECT	reject •	accept •	reject •			ZEdit Delete	
and an Ind	reject •	accept ·	reject •			ZEdit Delete	
cell: cell: 💒 ⇒ REJECT							

Figure 10-4. Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder

- **9** On that screen, make sure the following settings are observed:
 - Under the heading General Settings:
 - Select Enable SYN-Flood Protection.
 - Select Drop Invalid Packets.
 - Set Input as Accept.
 - Set Output as Accept.
 - Set Forward as Accept.
 - Under the heading **Zones**:
 - The LAN zone is configured to forward to the WAN zone. Input, Output, and Forward for that forwarding zone are all set to accept.
 - Verify that the **WAN** zone has the following settings:
 - Input: reject
 - Output: accept
 - Forward: accept
 - Uses Masquerading
 - Uses MSS Clamping

Note: You can also configure the **newzone** if the EN-2000 will use that zone; possibilities are for 5 GHz 802.11 wireless, GigE, or Ethernet. Consult your network administrator for configuration information.

- **10** When you have finished configuring the screen, select the **Save & Apply** button (in the lower right corner of the screen).
 - The configuration is saved.
- **11** Select the **Back to Overview** button.
 - The Firewall Zone Settings Screen for the IPsec VPN Tunnel Responder is redisplayed (recall Figure 10-1).
- 12 On that screen, select the Save and Apply button.
 - The configuration is saved and applied (restarting the firewall).

10.1.2 Disabling Masquerading on the VPN Tunnel Initiator

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

- Caution: Do only one of the following:
- If the tunnel initiator's right subnet is 0.0.0/0, perform only step 1.
- If the tunnel initiator's right subnet is not 0.0.0.0/0, perform only step 2.
- 1 If the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator specifies a **Right Subnet** of **0.0.0/0**, indicating all remote locations (as shown in Figure 10-5), do the following:

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

tus System Netwo	ork Statistics	ogout					
erfaces Firewall St	atic Routes Load Sharin	g/Failover	QoS Disgnosti	cs Hostnames DHCP a	nd DNS VPN VRRP	Serial	
neral Settings Stron	gswan IPSEC Status	Online Held					
EC Tunnels							
amet Protocol Security is	s a protocol suite for se	curing Inter	net Protocol com	nunications by authentical	ing and encrypting each I	P packet of a communicat	ion session
PSec Tunnels							
Tunnel Name	Left Subnet	Left	Right	Right Subnet	Tunnel Up	Tunnel Down	
OSAT1	192.168.101.0/24	%any	71.16.53.45	0.0.0.0/0	2 Tunnel Up	Tunnel Down	Edit 💌 Delete
Add IPSEC TUNNEL							
IPSEC Defaults							
IKE Life	IKE Lifetime KeyLife		yLife	Aggressive		Responder	
72h		1	24h	yes no		no	Edit
IPSEC Actions							
IPSEC Start IPSEC Sto		IPSEC Stop	IPSEC Restart			Modifications & Additions	
A DECC Stat		DREC Stop		IPSEC Restart		Sava & Anniv	

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

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

tus System Nelwork Statistics	Logout				
erfaces Firewall Static Routes L	oad Sharing/Failover QoS	Diagnostics Hostnames	DHCP and DNS VPN V	RRP Serial	
neral Settings Port Forwards Traff	c Rules Custom Rules				
wall - Zone Settings					
irewall creates zones over your netwo	ork interfaces to control ne	work traffic flow.			
eneral Settings					
nable SYN-flood protection					
rop invalid packets					
nout		accont			
-poc		accept			
lutput		accept	•		
orward		accept			
ones					
Zone Forwardings	Input	Output Forward	Masquerading	MSS clamping	
lan: lan: 🚂 📼 wan	accept 💌 ac	cept 💌 accept			🛃 Edit 💌 Delete
wan: wan: 🔝 🖷 ACCEPT	accept 💌 ac	cept 💌 accept		V	🛃 Edit 💌 Delete
Add					

- **b** On the Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator, make sure **Masquerading** is NOT checked for any **Zone Forwarding**.
- c On that same screen, select the Save & Apply button.
- d Go to Firewall Traffic Rules, on page 8.
- 2 If the IPsec VPN Tunnel Screen for a VPN Tunnel Initiator specifies a Right Subnet of *f.g.h.i/j* other than 0.0.0/0 (in Figure 10-7, the sample right subnet is 192.168.101.0/24), do the following:

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

Icore-networks								
Internet Settings Network	rock [Linguid] () Dista Raides - Falles C Théon	umoart r - Yeneel	Degradue - Quil	VPH VIAP				
PSEC Tunnels								
itemit Protocol Security i TPSec Tunnels	a protocol suite for sec	uring Interne	t Protocol communicatio	ns by authenticating and	encrypting each IP pa	dust of a communication set	alon	
Tunnel Name	Left Subnet	Left	Right	Right Subset	Tannel Up	Tannel Down		
теата	192.168.10.0/24	Sars	168-249.107-37	192-168-1-0/24	2 Tunnel Up	Tunnel Down	Edit #Delete	
Add IPSEC TUNNEL								
IPSEC Defaults								
DOE Lifetime		ReyLife		Aggressive		Responder		
72	72h 24h		24h			- 14	(CEdit	
IPSEC Actions								
IPSEC Start		IPSEC Stop		IPSEC Restart		Modifications & Additions		

- a Select the Network tab; then select the Firewall tab.
 - The Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator is displayed (Figure 10-8).

Figure 10-8. Firewall Zone Settings Screen for the IPsec VPN Tunnel Initiator Right Subnet Not 0.0.0/0

atus System Network Statistics	Logout					
terfaces Firewall Static Routes	Load Sharing/Failover Q	Diagnostic	s Hostnames Di	HCP and DNS VPN VI	URP Serial	
eneral Settings Port Forwards Tra	ffic Rules Custom Rules					
ewall - Zone Settings						
firewall creates zones over your net	work interfaces to control	network traffic	flow.			
Seneral Settings						
Enable SYN-flood protection		V				
Drop invalid packets						
Input		accep	ot	•		
Output		accep	ot			
Forward		accer	ot			
		100000				
lones						
Zone - Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: 🧾 🗕 wan	accept 💌	accept	accept 💌		8	Edit 🗶 Delete
wanz wan: 🖉 🗕 ACCEPT	accept 💌	accept 💽	accept .	S	(V)	🛃 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 10-8).
- c On that same screen, select the Edit button for the WAN Zone.
 - The Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator is displayed (Figure 10-9).

Go to Table

Figure 10-9. Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator

ncore-networks	hrthw aling WAN	Changes:
Status Vestor Network (agent Questanat) Interface Restrance State Scates Falser Firewall General Settings Puri Parwark, Turlin Jaire	Disgonation Quil VPB VBBP	
irewall - Zone Settings - Zone "wan"		
Zone "Wan" This section defease common properties of "wan". The input and out forwarded traffic between deflerent networks within the pine. Given	put options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for of hetrophic specifies which evaluable networks are member of this zone.	
Restrict to address family	Pvd only *	
Restrict Masquerading to given source subnets	0.0.05	
Restrict Masquerading to given destination subnets	192 168 1 0/24	
Force connection tracking	1/2 / / / / / / / / / / / / / / / / / /	_
Enable logging on this zone		
Inter-Zone Forwarding The options below soutrol the forwarding policies between this gone from other zones targeted at "wan". The forwarding rule is unifor	(man) and other zones. Destination zones cover forwarded traffic originating from "wast ". Source zones match forwarded t ectional, e.g. a forward from lar to wan does oct mark a permassion to forward from was to fair as well.	traffic
Allow forward to destination zones:	cett out g tage face g	
Allow forward from source zones:	E colt [colt 2]	

d On the Advanced Firewall Settings Screen for the WAN Zone of the VPN Tunnel Initiator, specify **!***f.g.h.i/j* in the field **Restrict Masquerading to Given Destination Subnets**, to indicate not to use masquerading for that subnet.

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

- e Select the Save & Apply button.
- f On that same screen, select the Back to Overview button.
- g On the overview screen, select the Save & Apply button.
- h Go to Firewall Traffic Rules, on page 8.

10.1.3 Firewall Traffic Rules

For this IPsec VPN tunnel, we need to add and update firewall rules on the server side (responder side) of the IPsec VPN tunnel.

Note: Do not configure these rules on the initiator of the VPN tunnel.

- 1 On the EN-2000 management system, select the **Network** tab. Then select the **Firewall** tab and the **Traffic Rules** tab.
 - The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder is displayed (Figure 10-10).

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

fic rules define po	licies for pack	ets traveling bei	tween different zones, for exa	mple to reject traffic betwe	en certain	hosts o	r to open WAN po
he router.							
raffic Rules							
Name		Ma	tch	Action	Enable	Sort	
llow-DHCP- Renew	,	IPv4 From any hos fo any router IP st p	-UDP It in any zone out 55 on this device	Accept input	8	• •	Ecit Delete
Allow-TCP- HTTPS	т	IPv4 From any bar o any mater 1P at p	-TCP © In any zone at 443 on this device	Accept input		• •	Ecit Delete
Allow-TCP- SSH	1	IPv4 From any hose To any router IP at p	-TCP it in any zone iort 22 on this device	Accept input	8		Ecit Delete
Allow-Ping		IFv4-ICMP with t From any hose To any router J	ype echio-request st in any zone P on this device	Accept input	2	•	Edit Delete
IPSec_csp		IPv4 IP From any hos To any router I	SEC ESP It in any zone P on this device	Accept input	8		Ecit Delete
uth_header		IPv4-IP From any hos To any router &	SEC-AH Is in any zone P on this device	Accept input	8	•	ZEdit Delete
IPSEC_IKE	т	IPv4 From any o any nouter IP at p	-UDP host in cell art 500 on this device	Accept input	8		Ecit Delete
osec_NAT_T	Te	From any From any outer IP at po	-UDP host in cell int 4500 on this device	Accept input	8	••	Edit Delete
Open ports on router: Name	Protocol	External port					
New input rule	TCP+UDP		Add 🔛				
New forward rule: Name	Source zone	Destination zone					
New forward rule	lan	wan	Add and edit				
ource NAT urce NAT is a specific fo bnets.	orm of masqueradi	ng which allows <mark>f</mark> ine	grained control over the source IP use	d for outgoing traffic, for example to	map multiple	WAN ad	dresses to internal
lame			Match		Act	ion	Enable Sort
			This section contains no vali	ues vet			
New source NAT:	ource zone D	estination zone	To source IP To source port				
New SNAT rule lan	• Wa	an 💌 🖂	Please choo · Do not rewrite	Add and edit			

The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder lists several rules for monitoring traffic. We will briefly address its rules for IPsec VPNs.

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

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

	(Basi 141)	
ule is enabled	(Disable	
ame	IPSec_esp	
estrict to address family	IPv4 only	
rotocol	esp	
fatch ICMP type	any 🔻 🏠	
iource zone	Any zone cell:	
ource MAC address	any 🔻	
ource address	any	
iource port	any	
vestination zone	 ● Device (input) ● Any zone (forward) ● cell: cell: <i>j</i> ● Ian: lan: <i>j</i> ● wan:: wan:: <i>j</i> 	
Destination address	any	
Destination port	any	
lction	accept	
extra arguments	Passes additional arguments to iptables. Use with carel	

- c Configure the fields on this screen:
 - Set Restrict to address family to IPv4 only.
 - Set the Protocol to TCP.
 - Leave Match ICMP type at any.
 - Make sure the **Source Zone** shows that the **WAN** port is selected.
 - Leave the Source MAC address, Source address, and Source port at any.
 - For Destination Zone, select Device.
 - Leave the Destination Address at any.
 - For Destination Port, leave the port number as any.
 - Make sure the Action is to accept the packets.
 - Leave the Extra Arguments field blank.
- d Select the Save & Apply button.
 - The rule is saved.
- e Select the Back to Overview button.
 - The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder is redisplayed (recall Figure 10-10).

- **3** Repeat the procedure in step 2 for each of the following protocols:
 - AH protocol (see Figure 10-12).

Note: For the Destination Port, specify any.

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

s page allows you to change advanced properties of the tr	mic rule entry, such as matched source and destination nosts.	
Rule is enabled	() Disable	
Name	Auth_header	
Restrict to address family	IPv4 only	
Protocol	ah 🔻	
Match ICMP type	any 🔻 📷	
Source zone	 Any zone cell: cell: <a> lan: <a> want: <a> 	
Source MAC address	any	
Source address	any	
Source port	any	
Destination zone	Device (input) Any zone (forward) cell: c	
Destination address	any 🔻	
Destination port	any.	
Action	accept 🔹	
Extra arguments	Passes additional arguments to iptables. Use with care!	

• IKE, UDP port 500 (see Figure 10-13).



s page allows you to change advanced properties of the tr	amic rule entry, such as matched source and destination nosts.	
Rule is enabled	ODisable Disable	
Name	IPSEC_IKE	
Restrict to address family	IPv4 only 🔻	
Protocol	UDP *	
Match ICMP type	any 🔹	
Source zone	 Any zone cell: cell: lan: lan: wan: wan: 	
Source MAC address	any 🔻	
Source address	any	
Source port	any	
Destination zone	 Device (input) Any zone (forward) cell: cell: <u>js</u> ion: ian: <u>js</u> wan: <u>wan: js</u> 	
Destination address	any •	
Destination port	500	
Action	accept	
Extra arguments	Passes additional arguments to iptables. Use with carel	

• IPsec_NAT_T, UDP port 4500 (see Figure 10-14).

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

e is enabled	ØDisable	
ne	ipsec_NAT_T	
trict to address family	IPv4 only	
tocol	UDP	
tch ICMP type	any 🔻	
iource zone	Any zone	
	● con: ≥= ● fan: [an:]]	
	wan: wan:	
irce MAC address	any	
irce address	any 🔻	
irce port.	any	
estination zone	Device (Input) Any zone (forward) cell: cell: js	
	vvan: van: 2	
tination address	any	
tination port	4500	
ion	accept	
ra arguments	Passes additional arguments to iptables. Use with care!	

10.2 Configuring the Source NAT

- 1 On the Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder (recall Figure 10-10), under the heading **New Source NAT** (near the bottom of the screen), type a **Name** for a new network address translation (NAT) rule.
- 2 Make sure the following settings are used:
 - Source zone: LAN
 - Destination zone: WAN
 - To source IP: 10.1.1.1 (br-lan), selected from the field's pulldown menu
- 3 Then select the Add and Edit button.
 - The VPN Responder's Firewall Traffic Rules Screen for a Source NAT is displayed (Figure 10-15).

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

ncor <mark>e¹n</mark> etworks ⁻		Change
Status System Network Statistics Logout Interfaces Wif Firewall Statistics Logout General Settings Port Forwards Traffic Rules Custom Rules Firewall - Traffic Rules - SNAT source NAT	astics QoS Hostnames DHCP and DNS VPN VRRP Serial	
This page allows you to change advanced properties of the traffic rule entry, such as	matched source and destination hosts.	
Rule is enabled	@ Disable	
Name	source NAT	
Protocol	All protocols Vou may specify multiple by selecting * custom* and then entering protocols separated by space.	
Source zone	lan: lan: <u>p</u> newzone: (emoty) wan: wan: <u>p</u>	
Source MAC address		
Source IP address	any	
Source port	any Match incoming traffic originating from the given source port or port range on the client host.	
Destination zone	Ian: [an:]] newzone: (empty) wan: wan:]]	
Destination IP address	192.168.101.0/24	
Destination port	any Match forwarded traffic to the given destination port or port range.	
SNAT IP address	10.1.1.1 (prian) Rewrite matched traffic to the given address.	
SNAT port	Do not rewrite Rewrite matched traffic to the given source port. May be left empty to only rewrite the IP address.	
Extra arguments	Passes additional arguments to iptables. Use with care!	
Back to Overview		Reset Save Save Save & Apply

- 4 On that screen, make sure the following values are entered:
 - Protocol: All protocols
 - Source zone: LAN
 - Source IP address: any
 - Source port: any
 - Destination zone: WAN
 - Destination IP address: subnet for left (local) router
 - Destination port: any
 - **SNAT** (Source NAT) **IP address: 10.1.1.1 (br-lan)**, selected from the field's pulldown menu
- 5 Select the Save & Apply button.
- 6 Then select the **Back to Overview** button.
 - The Firewall Traffic Rules Screen for an IPsec VPN Tunnel Responder (recall Figure 10-10) is redisplayed.
- 7 On that screen, select the Save & Apply button.
 - Firewall rules for the Source NAT are configured and implemented.