SonicOS

#### Hub and Spoke TZ170 VPNs with Checkpoint NG

### Introduction

This technote will detail all steps to get a Hub and Spoke setup between the SonicWALL SonicOS Enhanced and the Checkpoint NG. Within this setup the Checkpoint NG will be the HUB and 2 TZ170 units will be the Spokes.

### **Versions Used**

- SonicOS 2.5.0.2 Enhanced on both TZ170 units
- Checkpoint FW-1 NGAI

### Sample Diagram



### Tasklist

#### On the SonicWALL units:

- Create new network objects and groups
- Create new VPN Policy for the Check Point FW-1 NG
- Specify Destination Network(s), IKE Phase 1 and Phase 2 properties

#### On FireWall-1 NG:

- Create local(Check Point) LAN network objects and group
- Create remote(SonicWALL's) LAN network objects
- Create new Interoperable Device objects
- Edit the Check Point Gateway object
- Verify the Topology
- Manually define VPN Domain
- Create new VPN Star Community
- Edit VPN Star community properties
- Verify Security Rules
- Verify Address Translation Rules

#### Testing

- Verify that traffic flows through the tunnel.
- Verify that applications function properly through the tunnel.
- Verify that the tunnel can reestablish if either side is disconnected.
- Verify that the network map and documentation match the running configuration.



### **Before You Begin**

If you have not already done so, set up a management system connecting to the SonicWALL's internal LAN interface. The SonicWALL should already be configured for internet access; if not, do this before completing any further steps. The Check Point FireWall-1 NG server is also assumed to be properly configured for internet access.

### **Setup Steps**

#### SonicWALL Setup Side Alice

Log into the SonicWALL's Management GUI using a current web browser.

SONICWALL	1	COMPREHENSIVE INTERNET SECURITY*
ſ	Name:	odmin
		Login

The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.

System	SONICWALL	Contraction in the second				
Network	System Retwork	Network > Address Objects				
🕿 Interfaces	stefans     von fatters & LB     zans	Address Croups Weyther CALABERS CORD	MADREN CREED 🥤 DATALEADREN CONTR			
💼 🗰 WAN Failover & LB	B DND B Address Directs	- Disame	Address Detail	Type	2440	Cosfigure
- Zonoo	Bi Houting	III. III LAN Babriets		Graup		形態
Zones	AND AND	FI (S WAN Submets		Greup		A-8
📠 DNS	DeCP Saver	TO IS CRIZ SUBRIS		Orange		务商
👼 Address Objects.	B P Helper	T IS ATWOOD		Graup		外班
	and the second second	E 🗑 Allistatiza P		Greup		余音
Routing *		F B englet_group		Greup		208
💼 NAT Policies		-C. IN GROUP HAT THOME		GUILE		学生
-		Attont				
		Address Objects				
💼 DHCP Server		E Store	Address Datail	Type	Zean	Cosfigere
📖 ID Halsay		E LAN Privary IP	192 168 168 168/255 255 255-255	Most	LAN	2018
		E LAN PERMY Subret	192 160 100 0/255 265 255 0	Notwork	LAPE	外族
💼 Web Proxy		IT YOU Prinay P	ZM PA 98, 110256 255 259 255	PERSI	TANK	958
		III YAAN Primary Salariet	207.68.91.64/255.251.255.224	Notwork	WWW	务的
Fireusell		E 321P	102 160 100 3055 251 255 266	Howt	VMMPU	先准
Firewall		E District	192 168 190/0259 255 253 0	Network	YWW	95.85
VPN		E RenadeAccess Networks	01000000	Notvreite	NP1R	90.81
		E VHOND® CHARAS	0000000	Nanwers.	VPH	0.8
Users			102 100 100 0010 201 201 0	Address for	VER	2018
Eccurity Ecruicos	Preval	T and the dree	192 160 109 00255 255 255 0	Names	11002	20 B
Security Services	VITI	C Invincent.org	192 160 225 0/255 255 255 0	Network	NTH.	208
Log	Users Security Security	E senewalijiss	192 166 H60 0/255 255 255 0	Norwen	LAN	8.6
Help	Log Leb	Add and a second				
Logout	Logar Statut: Roady	(The state of the state)				



Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects.

🖉 Add Address Object - Microsoft Internet Explorer 🔔 🔲 🗙					
Name:	checkpoint_lan				
Zone Assignment:	VPN 💌				
Туре:	Network				
Network:	192.168.170.0				
Netmask:	255.255.255.0				
Ready					
TREADY					
	OK Cancel				

Name: checkpoint\_lan Zone Assignment: VPN Type: Network Network: 192.168.170.0 Netmask: 255.255.255.0 Click 'OK' to finish.

🚰 Add Address Object	- Microsoft Internet Explorer 💶 🗙
Name:	Side_Bob_lan
Zone Assignment:	VPN 💌
Туре:	Network
Network:	10.234.234.0
Netmask:	255.255.255.0
Ready	
Incluy	
	OK Cancel

Name: Side\_Bob\_lan Zone Assignment: VPN Type: Network Network: 10.234.234.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects. The 'Name;" is "checkpoint\_group"

Add Address Object Group - Microsoft Internet Explore	er 📃 🗙
Name: checkpoint_group	checkpoint_lan Side_Bob_Lan
Ready	
	OK Cancel

Select the "checkpoint\_lan" object and 'Ctrl' or 'Shift' click to select the "Side\_Bob\_lan" object. Click the right arrow button to add both objects to the group.



From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for the Check Point FireWall-1.

System					
Network	VPN > Settings		VPN Policy Wizard	Apply	Cancel
Wireless Firewall	VPN Global Settings				
Settings Advanced	Vique Firewall Identifier: 0006B1067	7100			
DHCP over VPN	VPN Policies			Items 1	to 4 (of 4) 🖏 🕁 🗅
Local Certificates	📕 # Name	Gateway Destination:	Crypto Suite	Enable	Configure
CA Certificates	1 WAN GroupVPN		ESP 3DES HMAC SHA1 (IKE)		2000
	2 LAN GroupVPN		ESP 3DES HMAC SHA1 (IKE)		2000
	3 DMZ GroupVPN		ESP 3DES HMAC SHA1 (IKE)	П	2000
	4 WLAN GroupVPN		ESP 3DES HMAC SHA1 (IKE)		2000
					Delete All
Users ecurity Services Log Witzerds	Add Delete Add a new entry 4 Policies Defined, U Policies Enabled,	14 Maximum Policies Allowed			

The 'VPN Policy' window will then appear. On the 'General' tab page, 'Security Policy' section, select "IKE using Preshared Secret" from the 'IPSec Keying Mode:' dropdown box.

3	VPN Policy - Mic	rosoft Internet E	xplorer				
	General	Network	Proposals	Advanced			
	Security P	olicy					
	IPSec Keving	Mode:		IKE using Pre	shared Secre		
	Name:			to Checkpoint			
	IPSec Primar	y Gateway Name (	or Address:	67.115.118.94		_	
	IPSec Second	Jary Gateway Nan	ne or Address:	0.0.0.0		_	
	Shared Secre	t		HaRdI to Gue	:55 Al1c3	_	
	Local IKE ID (	(optional):	SonicWA	LL Identifier 💌	HUB-TEST		_
	Peer IKE ID (0	optional):	IP Addres	33 -	192.168.170	0.1	_
	Ready						
					OK	Cancel	Help

Name: "to\_checkpoint"

IPSec Primary Gateway Name or Address: 67.115.118.94

Shared Secret: HaRd!\_to\_Gue55\_Al1c3

Local IKE ID: SNWL Identifier HUB-TEST (the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG)

Peer IKE ID: IP Address 192.168.170.1



Next select the 'Network' tab.

<b>8</b>   1	/PN Policy - Microsoft Internet Explorer
[	General Network Proposals Advanced
	Local Networks
	Choose local network from list
	C Local network obtains IP addresses using DHCP through this VPN Tunnel
	© Any address
	Destination Networks
	C Lies this VDN Turned as default youts for all interpret traffic
	Operations when indimensional and internet training     Destination patwork obtains IP addresses using DHCP through this VPN Turned
	Chapter destination network form list
	Ready
	OK Cancel Help

In the 'Local Networks' section, select the radio button next to 'Choose local network from list' and select "LAN Primary Subnet" from the dropdown box.

In the 'Destination Networks' section, select the radio button next to 'Choose destination network from list' and select "checkpoint\_group" from the dropdown box.

Next select the 'Proposals' tab. The default values should be correct, except the 'Life Time'; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.

<b>@</b> )1	PN Policy - Microsoft Internet Explore	:r		
	General Network Pr	posals Advanced		
	IKE (Phase 1) Proposal			
	Exchange:	Aggressive Mode		
	DH Group:	Group 5		
	Encryption:	3DES		
	Authentication:	SHA1	•	
	Life Time (seconds):	3600		
	Ipsec (Phase 2) Proposal			
	Protocol:	ESP		
	Encryption:	3DES		
	Authentication:	SHA1		
	Enable Perfect Forward Secrecy			
	DH Group:	Group 2		
	Life Time (seconds):	3600		
	Ready			
		OK	Cancel Help	



IKE (Phase 1) Proposal

Exchange: Aggressive Mode DH Group: Group 5 Encryption: 3DES Authentication: SHA1 Life Time (seconds): 3600

#### **Ipsec (Phase 2) Proposal**

Protocol: ESP Encryption: 3DES Authentication: SHA1 DH Group Group 2 Life Time (seconds): 3600 Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.

'PN Policy - Micr	osoft Internet E	plorer		
General	Network	Proposals Advanced		
Advanced	Settings			
🔽 Enable Ke	ep Alive			
🗖 Require a	uthentication of \	PN clients by XAUTH		
User grou	ip for XAUTH use	s: 🛛Select a user group		
🗖 Enable W	indows Networki	g (NetBIOS) Broadcast		
🗖 Enable Mu	ulticast			
Apply NAT	Policies			
Translate	d Local Network:	Select Translated Local Network	<b>V</b>	
Translate	d Remote Netwo	ĸ 🛛 Select Translated Remote Network	-	
Management	/ia this SA:	🗖 НТТР 🗖 НТТРЗ		
User login via	this SA:	🗖 НТТР 🗖 НТТРЗ		
Default LAN G	ateway (optional)	0.0.0.0	_	
VPN Policy bo	und to:	Zone WAN 🔽		
200du				
(COUY				
			Cancel	Help

Make sure that the option Enable Keep Alive is checked. All other options can be left as they are. Click the OK button.

This completes the settings on the SonicWALL TZ170 installed on Side Alice. Now, we will setup the Check Point unit we will setup the TZ170 unit at Side Bob.



#### SonicWALL Setup Side Bob

Log into the SonicWALL's Management GUI using a current web browser.



The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.

System	SONICWALL					
Network	System Feitwork	Network > Address Objects				
🕿 Interfaces	<ul> <li>Mathematical</li> <li>Mathematical</li> <li>Mathematical</li> <li>Context</li> </ul>	Address Croups Weyther CALABERS CORD	n Address Otrects 🦿 Datale Address Otarcia			
💼 🛛 WAN Failover & LB	M DND	E B Name	Address Detail	Tasar	Zane	Cosfigere
👼 Zones	Bi Houting	E E LAN Babriets		Graup.		50.8
Zones	BE NAT Passies	TO SE WARD BORNAGE		Greup		20.8
💼 DNS	Dettit Saver	TT IS CRIZ SUBRETS		Orange		务组
🛲 Address Objects	B P Heber	E B AIWON P		Ormp		新教
	Const Lower	T 🗄 Allidation P		Ontup		免疫
📷 Routing 🏠		☐ El englek_getue		Greup		98
💼 NAT Policies		E Bienackperrigroup		Grag		<b>外市</b>
		AlfGroup				
ARP ARP		Address Objects				
💼 DHCP Server		P-Passage	Address Data	Total	2000	Confirmen
ma ID Listeren		E LAUPSMONIP	192 188 168 168055 254 254 255	Host	LARI	20.8
IP Helper		E LANF Smary Subret	192 188 189 0/255 265 255 0	Noteste	LAN	2019
💼 Web Proxy		IT WRIPPINAVP	201 14:01 10:00 200 200 200	Hast	TWNE	20.8
		T matt Primary Saturet	207.00.01.64/255.255.255.224	Notwork	WWW	影響
Cincrus II		E 121P	102 180 100 3055 251 255 256	Hout	VMM	先者
Firewall		# Distrut	192 168 180.0259 255 259 0	Network	THE	908
UPN		E RenadeAccess Networks	0.0.0000.0.0	Notvente	NP16	958
*114		E Ver Det D* Chieres	04060600	Raidweak	VEH	908
Users		T english_ster	192.166.100.0/255.255.255.0	Hervisite	LAN	90.8
		In christipath( Jan	102 160 170 0/255 264 255 0	haidweite	14.11	9.8
Security Services	VIII	To anglah_dree	192100108202552552550	planete te	DWE	0.8
1.00	Users	C Invincent in	122 100 225 0035 255 255 0	Pactore and	1.000	0.9
LOG	Decisity Decision	C. second jax	142166.0004055.255.255.0	NINVER	LW1	0.8
Help	Log	and the second second second				
	Logavi	Act a way abben (dat)				
Logout	Statute: Ready					

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects.



🚰 Add Address Object	- Microsoft Internet Explorer 💶 🗙
Name:	checkpoint_lan
Zone Assignment:	VPN 🔽
Type:	Network
Network:	192.168.170.0
Netmask:	255.255.255.0
Roadu	
Ready	
	OK Cancel

Name: checkpoint\_lan Zone Assignment: VPN Type: Network Network: 192.168.170.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Name:	Side_Alice_Lan
Zone Assignment:	VPN
Туре:	Network
Network:	180.10.10.0
Netmask:	255.255.255.0
Roadu	

Name: Side\_Alice\_lan Zone Assignment: VPN Type: Network Network: 180.10.10.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects. The 'Name;" is "checkpoint\_group"

Edit Address Object Group - Microsoft Intern	et Explorer
Name: checkpoint_group	<ul> <li>checkpoint_lan</li> <li>Side_Alice_Lan</li> <li></li> </ul>
Ready	
	OK Cancel

Select the "checkpoint\_lan" object and 'Ctrl' or 'Shift' click to select the "Side\_Alice\_lan" object. Click the right arrow button to add both objects to the group.

From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for the Check Point FireWall-1.



System					
Network	VPN > Settings		VPN Policy Wizard	Apply	Cancel
Wireless Firewall	VPN Global Settings				
VPN	Enable VPN				
Settings	Unique Firewall Identifier: 0006B1	0671D0			
Ndvanced DHCP over VPN L2TP Server	VPN Policies			Items 1	to 4 (of 4) 🖸 🕽 🖉
Local Certificates	📕 # Name	Gateway Destinations	Crypto Suite	Enable	Configure
A Certificates			ESP ODES HMAC SHA1 (IVE)	Г	2010
	1 WAN GroupVPN		Edi Spedrimno drini (ne)		
	1 WAN GroupVPN     2 LAN GroupVPN		ESP 3DES HMAC SHA1 (KE)		888
	1 WAN GroupVPN      2 LAN GroupVPN      3 DMZ GroupVPN		ESP 3DES HMAC SHA1 (KE) ESP 3DES HMAC SHA1 (KE)	П	\$18 \$18 \$18 \$18 \$18 \$18 \$18 \$18 \$18 \$18
	1 WAN GroupVPN     2 LAN GroupVPN     3 DMZ GroupVPN     4 WLAN GroupVPN		ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)		\$8 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
Users	1 WAN Group/PN     2 LAN Group/PN     3 DMZ Group/PN     4 WLAN Group/PN     Add		ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)	6 6 6	NO B NO NO B NO NO B NO Calato All
Users courity Services	1 WAN Group/PN     2 LAN Group/PN     3 DMZ Group/PN     4 WILAN Group/PN     Add. Colorie     fadd a new entry	_	ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)	C C C	N B P N B P N B P Letter All
Users countly Services Log Wizands	1 WAN GroupVPN     2 LAN GroupVPN     3 DMZ GroupVPN     4 WILAN GroupVPN     Add	led, 14 Maximum Policies Allowed	ESP 3DES HIMAC SHAT (INE) ESP 3DES HIMAC SHAT (INE) ESP 3DES HIMAC SHAT (INE)	C C	Delete All

The 'VPN Policy' window will then appear. On the 'General' tab page, 'Security Policy' section, select "IKE using Preshared Secret" from the 'IPSec Keying Mode:' dropdown box.

VPN Policy - Microsoft Internet Explo	rer				
General Network F	roposals	Advanced			
Security Policy					
IDDae Vaving Mada		IVE using Rea	abarad Court		
hisma:		The Checknoist	snared Secret		
IPOec Primary Gateway Mame or A	idea.e.e.	10_CHECKPOIN		_	
IP Sec Primary Gateway Name of A	Juress.	67.115.118.94		_	
IPSec Secondary Gateway Name o	r Address:	0.0.0.0		_	
Shared Secret		HaRdI_to_Gue	-55_B0b	_	
Local IKE ID (optional):	SonicWA	LL Identifier 🗾	HUB-TEST		_
Peer IKE ID (optional):	IP Addres	ss 💌	192.168.170.	1	
Ready					
		_	OK	Cancel	Help
				0.000	

Name: "to\_checkpoint" IPSec Primary Gateway Name or Address: 67.115.118.94 Shared Secret: HaRd!\_to\_Gue55\_B0b Local IKE ID: SNWL Identifier HUB-TEST (the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG) Peer IKE ID: IP Address 192.168.170.1



Next select the 'Network' tab.

MPN Policy - Microsoft Internet Explorer	
General Network Proposals Advanced	
Local Networks	
Choose local network from list LAN Primary Subnet	
C Local network obtains IP addresses using DHCP through this VPN Tunnel	
C Any address	
Destination Networks	
C Use this VPN Tunnel as default route for all Internet traffic	
C Destination network obtains IP addresses using DHCP through this VPN Tunnel	
Choose destination network from list _ checkpoint_group	
Ready	
OK Cancel	Help

In the 'Local Networks' section, select the radio button next to 'Choose local network from list' and select "LAN Primary Subnet" from the dropdown box.

In the 'Destination Networks' section, select the radio button next to 'Choose destination network from list' and select "checkpoint\_group" from the dropdown box.

Next select the 'Proposals' tab. The default values should be correct, except the 'Life Time'; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.

VPN Policy - Microsoft Internet Exp	alorer		
General Network	Proposals Advanced		
IKE (Phase 1) Proposa			
Exchange:	Aggressive Mode		
DH Group:	Group 5	•	
Encryption:	3DES		
Authentication:	SHA1		
Life Time (seconds):	3600		
Tanana (Dhana D) Daanaa			
Ipsec (Phase 2) Propos	idi		
Protocol:	ESP	•	
Encryption:	3DES	¥	
Authentication:	SHA1		
Enable Perfect Forward Sec	recy		
DH Group:	Group 2	¥.	
Life Time (seconds):	3600		
Ready			
	_	OK Cancel	Help
		- Cancer	

IKE (Phase 1) Proposal Exchange: Aggressive Mode DH Group: Group 5 Encryption: 3DES Authentication: SHA1 Life Time (seconds): 3600



Ipsec (Phase 2) Proposal Protocol: ESP Encryption: 3DES Authentication: SHA1 DH Group Group 2 Life Time (seconds): 3600 Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.

Advanced Settings		
Enable Keep Alive		
Require authentication of VPN of	lients by XAUTH	
User group for XAUTH users:	Select a user group	
Enable Windows Networking (N	letBIOS) Broadcast	
Enable Multicast		
Apply NAT Policies		
Translated Local Network:	Select Translated Local Network	
Translated Remote Network:	Select Translated Remote Network	
Management via this SA:	Г НТТР Г НТТРЗ	
User login via this SA:	F HTTP F HTTPS	
Default LAN Gateway (optional):	0.0.0	
VPN Policy bound to:	Zone WAN	

Make sure that the option Enable Keep Alive has been checked. All other options can be left as they are. Click the OK button.

This completes the settings on the SonicWALL TZ170 installed on Side Bob.



#### Check Point FireWall-1NG Setup

Log into SmartDashboard.

Welcome to Check Point SmartDashboard					
🔲 <u>D</u> emo Mode	Basic (Firewall)				
● <u>U</u> ser Name	admin				
C Certificate:					
Password:	*****				
<u>S</u> martCenter Server:	192.168.170.1				
Read Only	More Options >>				
<u>         0</u> K	Quit				

Before the VPN can be setup it is necessary to create Network Objects for all devices and networks. To create the network objects, first click on 'Manage' on the top of the SmartDashboard. Then click on 'Network Objects...' from the drop down box.

The wanherten.com - Check Point	imartDa	shboard - Standard						
Elle Edit Yew Manage Rules	le Edit Yew Manage Bules Bolicy Search Window Help							
] 🖬 Ə   X 🖷 🛍 ] 🏪 4	2 例 6	N   🗉   🖳 🖞	°≕ <u>–</u> – – ×	👻 🏜 🖪 🖽				
] 88 X 🖂   隆 🔳 😂	24 <mark>8</mark> 4		10 X					
₽ <u></u>	Sec.	curity 🗮 Address Tra	nslation 🛛 📇 SmartDel	iense 🛛 🔨 VPN Manaj	ger 🛛 🛗 Desktop Securi	ty		
Retwork Objects     Direck Point	NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	-
Ordes     Interoperable Devices	ŀ	∼ EncDomain HubG	← EncDomain.Spok	* Any Traffic	~ EncryptedService	Encrypt8Continue	- None	
Hetworks     Groups	·	∼ MemberGWs Enc	∼ MemberOWs.Enc	* Any Traffic	∼ EncryptedService	Encrypt&Continue	- None	
Dynamic Objects	-	Accept VPN traffic	rule (configured fro	m the community)				
	· -	* Any	🔆 Member Gatewar	🔆 HUB-TEST	<ul> <li>Encrypted Servic</li> </ul>	🔂 accept	🔳 Log	
	1	Hecc_P FamPoeters	💦 opmodule	* Any Traffic	TOP CPM	🔂 accept	Log	
	⊪—				microsoft-ds-udp		_	- 1
	2	cpmodule	* Any	* Any Traffic	* Any	accept	Log	_
	3	* Any	TZ170	* Any Traffic	TOP https	🔂 accept	🔳 Log	
	4	* Any	VanHertenServe	* Any Traffic	TOP ftp TOP http	nccept	Log	
	5	* Any		* Any Traffic	VEO_OBSERVER	💮 accept	🔲 Log	
	6	4 CP_LAN	blocked_P	* Any Traffic	* Any	🖲 drop	Log	
	7	+ CP_LAN	* Any	* Any Traffic	* Any	😨 accept	Log	
	0	* Any	* Any	* Any Traffic	* Any	🖲 drop	Log	÷
	•	,						<u>ا</u>
For Help, press F1	,			va	nherten.com Rei	d/Write NUM		

The 'Network Objects' window will then appear. The first object to create is for the LAN subnet of the Checkpoint FW, it's likely that these object already exist as they are used as the base for most rules. To create the LAN object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Network' from the dropdown box.

Network Objects			×
Network objects: Show: All		▼ More >>	
AuxiliaryNet         blocked_P         +       CP_LAN         cpmodule       2         DMZNet		_	
<u>N</u> ew	<u>R</u> emove	<u>E</u> dit	1
<u>C</u> lose	Actions	<u>H</u> elp	

New	Remove
Check Point	· •
Node	•
Interoperat	ole Device
Network	N
Domain	KS -
OSE Device	
Group	+
Logical Serv	/er
Address R.a	nge
Dynamic Ob	oject
VoIP Domai	ns 🕨



The 'Network Properties' window will then appear.

Network Properties -	CP_LAN		×
General NAT			
<u>N</u> ame:	CP_LAN		
Network Address:	192.168.170.0		
Net <u>M</u> ask:	255.255.255.0		
<u>C</u> omment:			
Color:			
Broadcast addre	SS: C Not included		
	OK Cancel	Help	

In this window, enter the object:

Name: CP\_LAN Network Address: 192.168.170.0 Net Mask: 255.255.255.0

The next network objects to create are for the LAN of the SonicWALL appliance at Side Alice and for the LAN of the SonicWALL appliance at Side Bob.

From the 'Network Objects' window, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Network...' from the dropdown box.

Here we create the Network Object for the LAN of Side Alice. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network\_Alice Network Address: 180.10.10.0 Net Mask: 255.255.255.0

Network Properties	- Network	_Alice		×
General NAT				
<u>N</u> ame:	Network_	_Alice		
Network Addres	s: 180.10.1	0.0		
Net <u>M</u> ask:	255.255.	255.0		
Comment:				
Cojor:		•		
Broadcast add	ress: ON	lot included		
	OK	Cancel	Help	



Here we create the Network Object for the LAN of Side Bob. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network\_Bob Network Address: 10.234.234.0 Net Mask: 255.255.255

Network Properties	Network_Bob	×
General NAT		
<u>N</u> ame:	Network_Bob	
Network Address:	10.234.234.0	
Net <u>M</u> ask:	255.255.255.0	
Comment:		
Color:		
Broadcast addre	© Ngt included	
	OK Cancel	Help

Next, edit the 'Check Points' network object. It should be named the same as the machine name then press the edit button. If it does not exist, create it under 'New' > 'Check Point' > 'Gateway...' and proceed to the next step.

Network Objects	×		
Network objects:		New Remove	E dit
Show: Check Points		Check Point 🔹 🕨	Gateway
The comodule		Node 🕨	Hast
		Interoperable Device	Gateway Cluster
		Network	Embedded Device
		Domain	Externally Managed Ga
		OSE Device	Externally Managed Ho
		Group 🕨	
		Logical Server	
<u>New <u>R</u>emove <u>E</u>dit</u>		Address Range	
Chara Antinua I Hala		Dynamic Object	
Liose Actions Help		VoIP Domains	



The 'Check Point Gateway' page will appear. On 'General Properties', verify the 'IP Address' and that both 'FireWall-1' and 'VPN-1 Pro' are selected. In this example, the 'IP Address' is "192.168.170.1". When finished, click 'Topology' on the left hand side.

heck Point Gateway - cp	module	×
General Properties	Check Point Gateway - General Properties	
NAT 	Name: jcpmodule	
Remote Access     Authentication	IP Address:   192.168.170.1	
Logs and Masters     Capacity Optimization		
Advanced     Advanced	Check Point Products	
	Version: NG with Application Intelligence Version	
	Type: Check Point Enterprise/Pro	
	Firewall       Image: Construction of the server         SecureClient Policy Server       SecureClient Software Distribution Server         Primary Management Station       Image: Construction         Additional Products:       Image: Construction         Web Server       Secure Internal Communication         Communication       DN:         Communication       DN:	
	OK Cancel Help	

On 'Topology', verify the network addresses of the 'internal' and 'external' networks listed under the 'Topology' section. If nothing is populated in the topology fields, click 'Get Topology...'

Crementary reperiors	Topology
Topology NAT	Get
VPN Remote Access Authentication Loga and Masters Capacity Optimization Advanced	Name     IP-Address     Nameda Mada     P-Addresses behavior transfer       620     6524     6524     6524     6524     6524       611     671     151     119     255     255     255     External       61     671     151     119     255     255     255     External       641     Edk     Bemove     Add     Edk     Bemove

In this example: External network: "67.115.118.94" Net mask : "255.255.255.255" Internal network: "192.168.170.1" Net mask: "255.255.255.0" (internal is also referred to as 'This Network').

In the 'VPN Domain' section select 'Manually defined' and select the previously created "CP\_LAN" Network Object with the dropdown menu. When this is done you can close this page by pressing the OK button.



It is needed to create also Interoperable Network objects for the both SonicWALL appliances. Go to 'Manage' > 'Network Objects' now the Network Objects window will then appear. To create the 'Interoperable Device' object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Interoperable Device' ...' from the dropdown box. The 'Interoperable Device' window will then appear.



In this window, under 'General Properties' enter Name: SNWL\_Alice IP Address: 207.88.91.77 Next click 'Topology' on the left hand side.



On the 'Topology' page, under the 'VPN Domain' section, select 'Manually defined' and select the previously created "Network\_Alice" Network Object with the dropdown menu. Click on 'OK' to finish.

An Interoperable Device Object needs also to be created for Side Bob. Go to 'Manage' > 'Network Objects' now the Network Objects window will then appear. To create the 'Interoperable Device' object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Interoperable Device' ...' from the dropdown menu.

VEN	<u>G</u> et			
	Name If	<sup>o</sup> Address	Network Mask	IP Addresses behind interfac
	•			<b>)</b>
	<u>A</u> dd	Edit	<u>R</u> emove	
	VPN Domai	n	d Gataway based on T	analagu information
	VPN Domain C All IP Ac	n Idresses <u>b</u> ehin	d Gateway based on T	opology information.
	VPN Domaii © All IP Ac • <u>M</u> anuali	n Idresses <u>b</u> ehin v defined	d Gateway based on T 나나 Network_Alic	opology information. .e <u>V</u> ew
	VPN Domaii C All IP Ac I <u>M</u> anuali	n Idresses <u>b</u> ehin y defined	d Gateway based on T 나누 Network_Alic	opology information. :e <u>V</u> <u>New</u>
	VPN Domaii C All IP Ac I Manual≬	n Idresses <u>b</u> ehin y defined	d Gateway based on T	opology information. se <u>v</u> <u>New</u>
	VPN Domai C All IP Ac 준 <u>M</u> anuall	n Idresses <u>b</u> ehin y defined	d Gateway based on T ++ Network_Alic	opology information. :e <u>v</u> <u>New</u>
	VPN Domai C All IP Ac C <u>M</u> anuall	n Idresses <u>b</u> ehin y defined	d Gəteway based on T 내 Network_Alic	opology information. re <u>v</u> <u>N</u> ew

The 'Interoperable Device' window will then appear.

Interoperable Device	- SNWL_Bob	×
Interoperable Device	Name: SNWL_Bob IP Address 00.62 91.20 Bet address Comment: Color:	X
	OK Cancel Help	



In this window, under 'General Properties' enter: Name: SNWL\_Bob IP Address: 80.62.91.20 Next click 'Topology' on the left hand side.

On the 'Topology' page, under the 'VPN Domain' section select 'Manually defined' and select the previously created "Network\_Bob" Network Object with the dropdown menu. Click on 'OK' to finish.

Interoperable Device - SNW	/L_Bob	×
General Properties	Topology	
Topology	Get	
T. ALU	Name IP Address Network Mask IP Addresses behind interface	
	Add Edit <u>R</u> emove	
	VPN Domain	
	C All IP Addresses behind Gateway based on Topology information.	
	Manually defined      Hetwork_Bob     ✓ New	
	OK Cancel Help	

Now all the Network Addresses are created which will be needed to setup the VPN SA on the Checkpoint NGAI unit. Next, define the VPN. From the top menu, select 'Manage' and then 'VPN Communities...'; the 'VPN Communities' window will appear.

🞇 vanherten.com - Check Point Sr	imartDashboard - VPN Manager	_ <u>-</u> – ×
Eile Edit View Manage Rules Po	olicy <u>S</u> earch <u>Wi</u> ndow <u>H</u> elp	
] 🖬 🕹   🎗 🖷 🖷 🗍 🖷 🛍	2 狭 み │ 目 │ 思 目 〒 = 乳 → │ ♥ ▲ 唱 目	
🗱 🔀 🔚   隆 🛅   🕮   🌢	24 💵 🛛 💽 🔍 🔍 🖾 🔀	
\$\$ \$\$ \$\$ \$\$ \$\$	🗱 Security 📴 Address Translation   🏭 SmartDefense 🔞 VPN Manager 🛅 Desktop Security	
Network Objects		
Check Point     Nodec		
Interoperable Devices	HUB-IEST MyIntranet RemoteAccess	
🗉 🖶 Networks		
⊕ 🔛 Groups		
⊡		
	SNIV/L Bob comodule SNIV/L Ali	<u></u>
		×.
For Help, press F1	vanherten.com Read/Write NUM	



From the 'VPN Communities' window, select the 'New' button on the bottom. Then select 'Site To Site' and 'Star...' The 'Star Community Properties' page will appear.



On the 'Star Community Properties' page, enter the VPN name in the 'Name:' field. In this example, the 'Name:' is "HUB-TEST" which needs to be the same as the SNWL Identifier setup in the VPN SA on the Spokes.

Star Community Properti	es - HUB-TEST	×
Star Community Propertia General - Central Gateways - Satelike Gateways - Excluded Services - VPN Properties - Advanced Properties - Shared Secret	s - HUB-TEST	×
	VPN targets	
	Accept all encrypted traffic.	
	Note: The rule applies for all Internally Managed community members. Log Traffic as defined in Global Properties, Logging Tab:	
	, -	
	OK Cancel Help	

For the 'Enable VPN routing for satellites' you need to select the option 'To center, or through the center to other satellites, to internet and other VPN targets.'

At the Community Traffic Security Policy it is necessary to have the checkbox 'Accept all encrypted traffic' ticked. Next, click on 'Central Gateways'.

On the Central Gateways, click on the 'Add...' button under the 'Central Gateways:' section. This will bring up the 'Central Gateways' window. Select here the address object 'cpmodule' and press OK.



Star Community Propertie	2s - HUB-TEST	×	
General Central Galeways Satellic Galeways Excluded Services Advanced Properties Shared Secret	Central Gateways   Add		Add Central Gateways  Add Central Gateways  For comodule  The candidates must be defined as:  VPN-1 installed.  Version NG FP1 and above (Only for Internally managed).  Host, Gateway, Gateway Cluster or Interoperable Device
	OK Cancel Help		OKCancelHelp

Next, click on 'Satellite Gateways'. On the Satellite Gateways, click on the 'Add...' button under the 'Satellite Gateways' section. This will bring up the 'Satellite Gateways' window.

	Star Community Properties - HUB-TEST	
Add Satellite Gateways	General     General     General     General     Ganeral     G	Satellite Gateways       All the connections between the Gateways below and the Central Gateways will be encrypted.       Participant Gateways:       Image: SNML_Alice       Image: SNML_Bob       Image: SNML_Bob       Add       Edit
The candidates must be defined as.		
VPN-1 instelled.     Version NG FP1 and above (Only for Internally managed).     S. Host, Gateway, Cluster or Interoperable Device		
UK Lancel <u>H</u> elp		OK Cancel Help

Select here the address objects 'SNWL\_Alice' and address object 'SNWL\_Bob' after this is done press OK.



Click on 'VPN Properties'.

General	VPN Properties		
- Central Gateways - Satellite Gateways	IKE (Phase 1) Properties		
VPN Properties	Perform key exchange encryption with:	3DES	•
Shared Secret	Perform gata integrity with:	SHA1	•
	IPsec (Phase 2) Properties		
	Perform IPsec data encryption with:	3DES	•
	Perform gata integrity with:	SHA1	-

Enter the 'IKE (Phase 1) Properties' and the 'IPsec (Phase 2) Properties'. In this example, the 'IKE (Phase 1)' section the settings are as follows:

#### IKE (Phase 1) Properties

Perform key exchange encryption with: 3DES Perform data integrity with: SHA1

#### **Ipsec (Phase 2) Properties**

Perform IPsec data encryption with: 3DES Perform data integrity with: SHA1

Next, click on 'Advanced Properties.'

Star Community Propertie	es - HUB-TEST	×
General Central Gateways	Advanced Properties	
Central Gateways     Setelling Gateways     Excluded Services     VPN Properties     Advanced Properties     Shared Secret	IKE (Phase 1)       Group 5 (1536 bit) ▼         Lese Diffie Hellman group:       Group 5 (1536 bit) ▼         Benegotiate IKE security associations every       60 ★         If Use aggressive mode       IPsec (Phase 2)         Lese Diffie Hellman group:       Group 2 (1024 bit) ▼         Lese Diffie Hellman group:       Group 2 (1024 bit) ▼         Benegotiate IPsec security associations every       3500 ★ seconds         If support Site to Site IP compression       Support Site to Site IP compression	
	NAT	
	OK Cancel Help	



In the 'Advanced Properties' section, under IKE (Phase 1), modify the 'Renegotiate IKE security associations every' field to "60" minutes and the 'Use Diffie-Hellman group' should be "Group 5 (1536 bit). Tick the option 'Use aggressive mode' For the 'Ipsec (Phase 2) Proposal' section the settings are as follows: 'Life Time (seconds)' is "3600". Do not enable Perfect Forward Security. At the 'NAT' it is necessary to tick the option 'Disable NAT inside the VPN community'

Click 'Shared Secret'.

General	Shared Secret			
<ul> <li>Central Lateways</li> <li>Satellite Gateways</li> <li>Excluded Services</li> <li>VPN Properties</li> <li>Advanced Properties</li> <li>Shared Secret</li> </ul>	☑ Lise only Shared Secret for all External members Each External member will have the following secret with all internal members in this community.			
	Peer Name	Shared Secret		
	SNWL_Alice	NNN		
	<u> </u>	<u>R</u> emove		

On the 'Shared Secret' section, tick the option 'Use only Shared Secret for all External members'. Highlight "SNWL\_Alice" in the 'Peer Name' table below. Click on the 'Edit..." button to enter the secret. In this example, the shared secret is "HaRd!\_to\_Gue55\_Al1c3" press the OK button. After this Highlight "SNWL\_Bob" in the 'Peer Name' table below. Click on the 'Edit..." button to enter the secret is "HaRd!\_to\_Gue55\_B0b" and press the OK button.

Insert Secret		X
Enter secret:	HaRd!_to_Gu	
OK		Cancel

Click 'OK' to finish the VPN Interoperability Hub Spoke setup between the SonicOS 2.5 Enhanced and Checkpoint NG within the SmartDashboard. Make sure that the Policy has been installed onto the Checkpoint firewall to have it working.

Document Created: 11/16/2004 Last Updated: 06/19/2008 Version 1.1



Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com