

WELCOME TO THE FUTURE OF CYBER SECURITY

Site to Site VPN in R80.x

Author: Danny Drake

Table of Contents

SITE TO SITE VPN IN R80.X	1
INTRODUCTION	2
SITE TO SITE VPN SETTINGS	
VPN WITH A THIRD PARTY	-
COMMON SKS FOR TROUBLESHOOTING S2S VPNS	16

Introduction

This document is a tutorial for beginners. It provides step by step instructions and examples of setting up Site to Site VPN with Check Point R80.x products. It also includes an example of setting up a S2S VPN with a third-party Gateway (Fortinet).

Some experience with R80.x SmartConsole is assumed, as well as basic understanding of IPSec and principles of Site to Site VPNs.

Site to Site VPN Settings

1. First thing you want to do is create the network/host objects you'll need to use on both ends of the VPN tunnel. i.e.

Network				Q 🖗	×
.	Network_1 Enter Object Cor				
General	IPv4				
NAT	Network ad	dress: 10.0	.0.0		
	Net mask:	255.	255.255.0		
	Broadcast a Inclu Not				
	IPv6 ······				
	Prefix:				
	🧳 Add Tag				
		ОК		Cancel	
	/ pc rr Object Comment			୍ ୧	× •
General	Machine				
Network Mana NAT Advanced	gement IPv4 addre: IPv6 addre:		Re	solve from name	
Servers	Add Tag				
	1		ОК	Cancel	

2. Then open the gateway object you are installing the VPN tunnel on and enable the IPSec VPN blade.

Network Security (9)	Management (0)		
Firewall FiPSec VPN Policy Ser Mobile Acces Application Co URL Filtering Data Loss Pre	s ontrol	 ✓ IPS ✓ Anti-Bot ✓ Anti-Virus ✓ Threat Emulation Threat Extraction △ Anti-Spam & Email Security △ Identity Awareness ✓ Content Awareness 	Advanced Networking & Clustering: Dynamic Routing SecureXL QoS Monitoring

3. Select the th to open the Network Management options. Select VPN domain. Unless you want all interfaces to be part of the tunnel you need to manually define the VPN domain. Click the manually define radial and select the internal network you are coming from (created in step 1).

Check Point Gateway - Branc	hOffice	? ×
General Properties Network Management System Backup VPN Domain Proxy 	VPN Domain O All IP Addresses behind Gateway are based on Topology information Manually defined Manually defined	
 Proxy NAT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal UserCheck IPSec VPN Link Selection VPN Advanced VPN Clients Authentication Office Mode Remote Access Clientless VPN Logs Fetch Policy Optimizations Hit Count Other 	Manually defined Access Community Set domain for Remote Access Community	
< >>	OK	el

4. If your GWs external IP is different from the IP on the interface you are using for your tunnel you will need to select the link manually. Open the drop down under IPSec VPN and select Link Selection. Then select the Selected address from topology table radial and select the interface you want to use.

Check Point Gateway - Branc	hOffice	8 ×
General Properties Network Management HTTP/S Inspection HTTP/HTTPS Proxy Platform Portal UserCheck PSec VPN └Ink Selection VPN Advanced Ugs Fetch Policy Optimizations Hit Count Other	IP Selection by Remote Peer Locally managed VPN peers determine this gateway's IP address using the following method:	
< >>	Outgoing link tracking:	Cancel

5. For 3rd party GWs you will need to create it as an interoperable device, and select the link selection within the topology tab. The click the manually defined radial and select the inside network on the other end of the tunnel.

Interoperable Device - Mark	s_Fortinet					? ×
General Properties Topology ⊕ IPSec VPN	Machine Name: IPv4 Address: IPv6 Address: Comment:	Marks_Fortinet 68.104.253.119	Resolve from Name	Color:	Black	· · · ·
	Products:	ers				
				ОК	Ce	ancel

Interoperable Device - Marks_Fortinet								P) x
General Properties		۹ ا	<u>G</u> et 🗈	<u>N</u> ew	<u> </u>	× <u>D</u> elete	1	Actions	
	rk IP Address	Network Mask	Topology						
VPN Domain									-
All IP Address Manually defir	behind Gateway are k d 륨 net 10.200.20		/ information					View	.
(Wandaliy delin	a an net 10.200.2	00.0						view.	
						OK		Cance	1

6. Next you will need to create the VPN community. Click on the security policies tab on the left pane. The select VPN Community at the bottom left.



7. There are two types of communities you could create; a Mesh community, consisting of multiple gateways all being able to connect VPN to each other; or a

Star community, which is one central GW with remote GWs VPN back to it. Select new, and your choice of community.

VPN Communities			*	🔨 🗙 🔍 Sean	ch	3 items
Name 🔺	Topology	Encryption Suite		Star Community		
🔅 demo_VPN	Star	Custom	*	Meshed Community		
🗱 MyIntranet	Meshed	Custom				
RemoteAccess	Remote Access	Custom				

8. Give it a name and select your participating GWs

			Q, 😢 🗙
demo_VPI			
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP Excluded Services Shared Secret Wire Mode Advanced	Center Gateways All the connections between will be encrypted. + × Name firelink_shrine Mesh center gateways Satellite Gateways	n the Gateways below and the Satellite Search Comments n the Gateways below and the Center O Search Comments	e Gateways
		ОК	Cancel

9. You can choose to accept all internal traffic if the participating GWs without the need for an access rule.

_	Q 😧 X
demo_ Enter Objec	
Gateways	Encrypted Traffic
Encrypted Traffic	Accept all encrypted traffic on: Both center and satellite gateways
Encryption	The rule applies for all to internally managed community members.
Tunnel Management	Log Traffic: LOG (Defined in Global Properties, Log and Alert Tab)
VPN Routing	
MEP	
Excluded Services	
Shared Secret	
Wire Mode	
Advanced	
	🖉 Add Tag
	OK Cancel

10. Next, choose the encryption method. This is where most of your troubleshooting with 3rd party GWs will take place. The Encryption methods must be identical on both ends. Use Aggressive mode if you are connecting to a 3rd party that does not support Main mode. Use Perfect Forward Secrecy for extreme security needs as it will affect performance.

		Q. 🧿 🛛 🗙
etter Object		
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP	Encryption Method:	Prefer IKEv2, support IKEv1 Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di *
Excluded Services	IKE Security Associatio	n (Phase 1)
Shared Secret	Encryption Algorithm:	3DES *
Wire Mode	Data Integrity:	SHA1 *
Advanced	Diffie-Hellman group:	Group 5 (1536 bit) *
	IKE Security Associatio	n (Phase 2)
	Encryption Algorithm:	3DES 👻
	Data Integrity:	MD5 ·
	More IKE Security Association (F Use aggressive mode IKE Security Association (F Use Perfect Forward Sec Diffie-Hellman grou Support IP Compression Add Tag	Phase 2) recy p: Group 5 (1536 bit)
		OK Cancel

11. You can choose to create permanent tunnels if you wish.

😍 _ demo V	/DN		Q 0		
Enter Object					
Gateways	Permanent Tunnels				
Encrypted Traffic	Set Permanent Tunne	els:			
Encryption	On all tunnels in	the community			
Tunnel Management	On all tunnels of	specific gateways	Select Gateways		
VPN Routing	 On specific tunne 	els in the community	Select Permanent Tunnels		
MEP	Enable Route Inje	ection Mechanism (RIM)	Settings		
Excluded Services	Tunnel down track:	Log	~		
Shared Secret	Tunnel up track:	Loa	w.		
Wire Mode		3			
Advanced	VPN Tunnel Sharing				
	One VPN tunnel per	each pair of hosts			
	One VPN tunnel per	subnet pair			
	One VPN tunnel per Gateway pair				
	🥑 Add Tag				
			OK Cancel		

12. Decide how the tunnel routes. Whether the satellites can go through the center or just to it only.

	Q, 😧 X
enter Object	
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP Excluded Services Shared Secret Wire Mode Advanced	 VPN Routing Enable VPN routing for satellites To center only To center and to other satellites through center To center or through the center to other satellites, to Internet and other VPN targets
	🖉 Add Tag
	OK Cancel

13.MEP (Multiple Entry Points) is used for load balancing if you are expecting heavy load on your tunnel.

	Q. 🕑 X
enter Object	
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP Excluded Services Shared Secret Wire Mode Advanced	MEP (Multiple Entry Points) Enable center gateways as MEP Entry point selection mechanism Choose the method by which the entry point gateway will be chosen from the gateways in the center: Select the closest gateway to source (first to respond) Select the closest gateway to destination (by VPN domain) Random selection (for load distribution) Manually set priority list Set. Tracking:
	OK Cancel
	OK

14. You can choose certain traffic that will not be encrypted over the tunnel to increase performance.

_				Q 🚯 🛛 🗙
• demo_V Enter Object				
Gateways Encrypted Traffic Encryption	Excluded Services The following service Connections with the and will not match ru	es are excluded fr ese services will no		l community.
Tunnel Management	$+ \mid \times$		🔍 Search	
VPN Routing MEP	Name	*	Comments	
Excluded Services				
Shared Secret Wire Mode Advanced		No item	ns found	
			ОК	Cancel

15. When connecting to a 3rd party you will need a Shared Secret. This password must be identical on both ends of the tunnel.

	୍ ଚ ା ×
enter Obje	VPN ct Comment
Gateways Encrypted Traffic	Shared Secret
Encryption Tunnel Managemer VPN Routing MEP Excluded Services	Cancel with all internal
Shared Secret Wire Mode Advanced	✓ Add Tag
	OK Cancel

16. Wired mode simulates the GWs being connected together via wired connection, bypassing the GW completely.

	Q. 😨 X
• demo_\ Enter Object	
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP Excluded Services Shared Secret Wire Mode Advanced	 Wire Mode Bypass Firewall Allow uninspected encrypted traffic between Wire mode interfaces of this Community members Wire mode routing - Allow members to route uninspected encrypted traffic in VPN routing configurations Add Tag
	OK Cancel

17. In the advanced settings you can configure when IKE phase 1 and 2 are autorenegotiated. You will also want to disable NAT here. NAT can cause issues accessing internal assets if you are connecting by IP.

		Q 😗 🛛 🗙
enter Object		
Gateways Encrypted Traffic Encryption Tunnel Management VPN Routing MEP	IKE (Phase 1) Renegotiate IKE security associations every (minutes): IPsec (Phase 2) Renegotiate IPsec security associations every (seconds): NAT	1440 <u>*</u> 3600 <u>*</u>
Excluded Services Shared Secret Wire Mode Advanced	Disable NAT inside the VPN community Reset Reset All VPN Properties Add Tag	Both center and satellite gateways *
		OK Cancel

18. Next, you will create an Access Rule to allow the VPN traffic. You will add the network/host objects in the destination and source. Choose the VPN community you created, then allow and log the traffic.

vpn	A 10.2.2.0	A 10.2.2.0	🗱 demo_VPN	* Any	🕀 Accep
	🚍 my pc	💭 турс			
	🚣 net 10.200.200.0	Anet 10.200.200.0			
	A 192	4 192			

19. Publish and install policy on participating GWs

VPN with a Third Party

1. An example of configuring on a Fortinet for the 3rd party. The IPSec wizard. Name, select type of VPN, and NAT configuration.

FortiGate 90D FGT9	0D3Z1	3008012			>_ [] 🕐 т Д2 🌅 adm
Dashboard	>	VPN Creation Wizard			
🔆 Security Fabric	>	1 VPN Setup	Authentication 3 Policy & Routing		
KortiView	>	Name	Checkpoint-FW	Site to Site - Cisco	
+ Network	>	Template Type	Site to Site Remote Access Custom	Site to Site - Cisco	
System	>	Remote Device Type	FortiGate		\sim
📕 Policy & Objects	>	Remote Device Type			Internet
Security Profiles	>	NAT Configuration	No NAT between sites	11	
🖵 VPN	~	NAT Configuration	This site is behind NAT	This FortiGate	Cisco
One-Click VPN Settings			The remote site is behind NAT		
IPsec Tunnels					
IPsec Wizard	☆		< Bac	k Next > Cancel	
IPsec Tunnel Templates			- 500		
SSL-VPN Portals					
SSL-VPN Settings					
🛔 User & Device	>				
🗢 WiFi & Switch Controller	>				
네 Log & Report	>				
C Monitor	>				

2. Configure IP, interface, and authentication methods.

FortiGate 90D FGT90	D3Z1	3008012					>_	[] @•	40 🙎
🚯 Dashboard	>	VPN Creation Wizard							
🔆 Security Fabric	>	VPN Setup 2 A	uthentication 3 Policy	& Routing					
FortiView	>	Remote Device	IP Address Dynamic DN			Checkpoint-FW: Site to Site	Ciasa		
+ Network	>	IP Address	1.1.1.1	3			- CISCO		
System	>	Outgoing Interface		-					\sim
📕 Policy & Objects	>	outgoing interface	Detected via routing lookup				Internet		cisco.
Security Profiles	>	Authentication Method	Pre-shared Key Signatur				Internet		N°
므 VPN	~	Pre-shared Key	•••••	۲		This FortiGate			Cisco
One-Click VPN Settings									
IPsec Tunnels									
IPsec Wizard	☆			< Back	Next >	Cancel			
IPsec Tunnel Templates									
SSL-VPN Portals									
SSL-VPN Settings									
User & Device	>								
🗢 WiFi & Switch Controller	>								
네 Log & Report	>								
Monitor	>								

3. Configure the source and destination subnets. Click create.

FortiGate 90D FGTS	90D3Z1	3008012				>_ []	⑦▪ 🗘 🛛 🧕 admin
Dashboard	>	VPN Creation Wiz	ard				
🔆 Security Fabric	>	VPN Setup	Authentication 3 Policy &	Routing			
FortiView	>		→ internal	-	Charles lat DM Charles Cha	C1	
Network	>	Local Interface Local Subnets	10.200.200.0/24	•	Checkpoint-FW: Site to Site	- Cisco	
System	>	Local Subhets	0.200.200.0/24				~
Policy & Objects	>	Remote Subnets	172.2.2.0/24				- Cisco
Security Profiles	>	Keniote Subnets	0			Internet	
🖵 VPN	~	Internet Access	None Share WAN Force to use	remote WAN	This FortiGate		Cisco
One-Click VPN Settings							
IPsec Tunnels							
IPsec Wizard	☆			< Back	Create Cancel		
IPsec Tunnel Templates							
SSL-VPN Portals							
SSL-VPN Settings							
💄 User & Device	>						
🗢 WiFi & Switch Controller	>						
네 Log & Report	>						

Dashboard	>	+ Create New 🖋 Edi	t 🗊 Delete 🔒 Print Instructions			
Security Fabric	>	T Tunnel	T Interface Binding	Template	T Status	T
E FortiView	>	CheckPoint	wan1	Site to Site - Cisco	OUp	4
Network	>					
System	>					
Policy & Objects	>					
Security Profiles	>					
⊒ VPN	~					
One-Click VPN Settings						
IPsec Tunnels	☆					
IPsec Wizard						
IPsec Tunnel Templates						
SSL-VPN Portals						
SSL-VPN Settings						
User & Device	>					
WiFi & Switch Controller	>					
≝ Log & Report	>					
Monitor	\$					

4. Preconfigured templates

Dashboard	>	⊙ View	
🔆 Security Fabric	>	Template	T Description
🛋 FortiView	>	Dialup - FortiClient (Windows, Mac OS, Android)	On-demand tunnel for users using the FortiClient software.
₽ Network	>	🕄 Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
System	>	🕄 Dialup - FortiGate	On-demand tunnel between two FortiGate devices.
Policy & Objects	>	Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec clie
	ĺ.	Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client
Security Profiles	>	Elisten Dialup - Windows (Native L2TP/IPsec)	On-demand tunnel for Windows users using the native L2TP/IPsec clien
⊒ VPN	~	🗯 Dialup - Cisco IPsec Client	On-demand tunnel for users using the Cisco IPsec client.
One-Click VPN Settings		the Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.
IPsec Tunnels		the Dialup - Cisco Firewall	On-demand tunnel between a FortiGate device and a Cisco Firewall.
IPsec Wizard			
IPsec Tunnel Templates	☆		
SSL-VPN Portals			
SSL-VPN Settings			
User & Device	>		
WiFi & Switch Controller	>		
■ Log & Report	>		

5. Configure the encryption method here.

FortiGate 90D FGT90D3Z13008012		
🍪 Dashboard	>	VPN Template Details
🔆 Security Fabric	>	
🛎 FortiView	>	🗱 Site to Site - Cisco
🕂 Network	>	
System	>	Phase 1 Interface
Policy & Objects	>	Proposal: 3des-sha1 3des-md5
Security Profiles	>	Dead Peer Detection: on-demand
	~	DH Group: 5
One-Click VPN Settings		
IPsec Tunnels		Remote Gateway Address
IPsec Wizard		
IPsec Tunnel Templates	☆	Allow this object in routing table: enable
SSL-VPN Portals		
SSL-VPN Settings		Local Address Group
🛔 User & Device	>	Allow this object in routing table: enable
🏶 WiFi & Switch Controller	>	
네 Log & Report	>	Remote Address Group
C Monitor	>	Allow this object in routing table: enable
		Phase 2 Interface
		DH Group: 5
		Perfect Forward Secrecy (PFS): enable
		Source Address Type: name
		Destination Address Type: name
		Proposal: 3des-md5
		Static Pauta

Common SKs for troubleshooting S2S VPNs

<u>sk34467</u> - Debugging Site-to-Site VPN <u>sk60318</u> - How to Troubleshoot VPN Issues in Site to Site <u>sk108600</u> - VPN Site-to-Site with 3rd party