Forcepoint ONE and Palo Alto IPSec Configuration Guide



forcepoint.com

Forcepoint ONE Integrated with Palo Alto IPSec

This guide will provide you with a step-by-step walkthrough for establishing the IPSec tunnel between Forcepoint ONE and the Palo Alto Firewall environment.

The first step in the IPsec VPN tunnel creation is to configure the IKE Crypto profiles, IKE Gateway, IPsec Crypto, IPsec tunnel and security profile.

- 1. Create IKE Crypto Profile
 - Go to Network > Network Profile > IKE crypto > Create a profile, then configure the encryption algorithm, autherntication algorithm and lifetime values according to your requirements.

DH GROUP	ENCRYPTION
group20	aes-256-cbc
Add ODelete 1 Move Up 1 Move Down	
AUTHENTICATION	Timers
sha256	Key Lifetime Hours
	24
	Minimum litetime = 3 mins
Add O Delete ↑ Move Up ↓ Move Down	IKEv2 Authentication 0 Multiple
Add O Delete † Move Up 👃 Move Down	Minimum litetime = 3 mins IKEv2 Authentication Multiple

- 2. Configure IKE Gateway
 - o Peer Address is "Cloud IKE ID"
 - o Location Identification is "Site IKE ID"
 - Peer Identification is "Cloud IKE ID"

General Advance	ed Options		
Name	IKE-GW-ForcePointOne		
Version	IKEv2 only mode		~
Address Type	○ IPv4 ○ IPv6		
Interface	ethernet1/1		~
Local IP Address	None		~
Peer IP Address Type		namic	
Peer Address	us.vp	n.forcepoint.io	~
Authentication	O Pre-Shared Key O Cer	tificate	
Pre-shared Key			
Confirm Pre-shared Key			
Local Identification	FQDN (hostname)	~	com 🗸
Peer Identification	FQDN (hostname)	~	us.vpn.forcepoir 🗸
Comment		1	
	/		

 If NAT is involved, then you will need to enable NAT Traversal. Go to Advance Options > Enable NAT Traversal > click OK.

	?
I Options	
de	
sal	
FarcePointOne	~
] Strict Cookie Validation	
OK Can	icel
OK Can	10

- 3. Configure IPsec tunnel prameters
 - Go to Network > Network Profiles > IPSec Crypto
 - Create a new IPSec Crypto profile.
 - Configure the encryption algorithm, dh-group and lifetime values according to your requirements.

	TWITE .			U
Name	IPSec-Crypto-ForcePointOne			
IPSec Protocol	ESP	 DH Group 	8100019	Ψ.
ENCRYPTION		Lifetting	Hours V 8	
acs-256-gcm		- CEnuble	Minimum Multime + 2 mins	
• Add O Delete	1 Move Op 1 Move Down			
AUTHENTICAT	ION			
			Þ	
🕑 Add : 🕞 Dullum	T More Op 1 More Down			
				Carcel

4. Create a New Tunnel Interface

- Select Tunnel Interface > New Tunnel Interface
- In the Interface Name field, specify a numeric suffix such as 1.
- \circ $\;$ In the Configuration tab, select the Virtual Router and the Security Zone.

O PANORAMA	DASHBOARD	ACC MONITOR	POLICIES OBJE	NETWORK	DEVICE P	ANORAMA	
Panorama 🗸 🗸	Template tmpl_av	vsuseastbroweatfw1 🗸	View b Device	~	Mode Multi V	SYS: Normal Mode; VP	N Enabled
Interfaces	Ethernet VLA	N Loopback Tunn	el SD-WAN				
Zones =							
Co Virtual Wires	Q						
Virtual Routers =	INTERFACE	MANAGEMENT	IP ADDRESS	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	FEAT
PSec Tunnels							
GRE Tunnels							
I DHCP		Tunnel Interface					(?)
DNS Proxy							
GlobalProtect		Interface Name			. 1		
Portais		Comment	ForcePointOne Tunnel				
Gateways		Netflow Profile	None				~
Cientiers Anne							
Clientiess App Groups		Config IPv4 I	Pv6 Advanced				
A Ons		Assign Interface To					
		Virtual Router	- Mr				
Retwork Profiles		Vistaal Castor					
GlobalProtect IPSec Cryptc		virtual system	vsys1				
H IKE Gateways		Security Zone					~
1PSec Crypto *							
B IKE Crypto # 1							
A Monitor						ОК	Cancel
interface Mgmt =							

- 5. Create IPSec Tunnel
 - Go to Network > IPSec Tunnels and click on Add
 - Provide a name for the tunnel and select the tunnel interface created in Step 4.

General Pro	cy IDs	
Name	PointOne	
Tunnel Interface	tunnel.1	~
Туре	Auto Key Manual Key GlobalProtect Satellite	
Address Type	○ IPv4 ○ IPv6	
IKE Gateway	IKE Gateway	
	bintOne	\sim
Sec Crypto Profile	ForcePointOne	~
	Anti Replay Window	~
•	Copy ToS Header	
	Add GRE Encapsulation	
Tunnel Monitor		
Destination IP	None	
Profile	None	
Comment		

- 6. Create a Proxy ID to identify the VPN peers
 - Select the **Proxy IDs** tab.
 - Select the IPv4 tab.
 - Click Add and enter the Proxy ID name.
 - Enter the local IP address or subnet for the VPN gateway.
 - Remote address for the VPN gateway is 0.0.0/0

Virtual Routers				
	IPSec Tunnel			0
GebellProtect Portals A Geteways	General Proxy IDs			
]] MDM ge Climptoss Apps	PROXY ID	LOCAL	REMOTE	PROTOCOL
Sis LDP Lowek Profiles © GobaProtect IPSec Crypte 11 UE Gateways = 11 INE Crypto = 12 INE Crypto = 12 Monitor 13 Interface Mignt = 24 Zone Protection	P	Proxy ID Proxy ID tunnel-inite tocal 0 0 P Adress o Remote 0.0.0.0/0 P Adress o P Adress o Protocol Any	rresting-traffic 1/16 IP/rotorials, only needed when peer requires i IP/rotorials, only needed when peer requires i	
Quố Punhe LLOP Punhe Di BFD Pinhe SD-WAN Interface Punhe	Add Opelete	_	СК	Cancel

- 7. Create a Policy-Based Forwarding (PBF) rule.
 - When creating a PBF rule, you must specify a name for the rule, a source zone or interface and an egress interface. All other components are either optional or have default value.
 - To begin configuration of Destination Interface, go to Objects > Addresses
 - o Note: You can copy Cloud FQDN from the Forcepoint ONE setup information.

Cisco-IPsec-Site4-Azure - IPsec Configuration		C Address	C Incaration	LOCATION.	(144	
SITE IKE ID		Constant Unit Constant		Field	(# Network	
20.228.84.74	G	Apple and a second seco				
CLOUD FQDN		Die Tear Call Devices Er Calebrary				
qac1-qa-acme.com-1.oh.us.vpn.dev.msvokxavdlwatqovcwze.com	ß	CD Harr Chapters Coll 1927 Frankers Control Conserve Lines		Address		
CLOUD IKE ID		Competition		Name FCON	ghoeffaile can's blat Lar an april ArcapaleCla of	
qac1-qa-acme.com.msvokxavdlwatqovcwze.com	G	Statematilite (IR): Compress (IR): Compress (IR): Compress (IR): Compress		Type FQDN Type	~ [pulycopsin
PRE-SHAREDKEY		Annual Annu				
cisco123	G	Carl Financia Carl Financian Carl Statistics Analysis		-		
MONITORING IP		C. Data Principa C. Data Principa C. Contention Principal Company				
116.50.59.230	G	E Aug Formating E Automatication I Destroyation				
		Constanting Prome				
	1005	The Party County Party				
c	LUSE	der Lenne Connection Profile 253 Schematic				

8. To configure security polices:

- Select Palo Alto Networks > Pre Rules > Security Policy Rule
- Click Add to create a new security policy rule.
- Configure **Source** and **Destination** policy rules.

General Source Destinatio	Application Service/URL Category	Actions Target		
Any	Any	any v	any v	
SOURCE ZONE	SOURCE ADDRESS A	SOURCE USER A	SOURCE DEVICE	
Internet	ATFW1-ETH-1-1			
	Þ			
	50			
	⊕ Add ⊖ Delete			
Contraction Contraction	Creat Contra	Orac Occas	Creating Constants	

	Any	
2 P2 internet		
€) Add) Delete	(+) k ^{[h}] ⊖ Delete	◆ Add
	Negate	

• Application should be IPSec.

General Source Destination Application Service/URL Category Action	ns Target
Any APPLICATIONS A	

9. Forwarding

- \circ $\;$ The next hop egress interface will be the tunnel that you created in Step 4.
- Save and commit the changes.

Policy Based Fe	orwarding Rule	1
General Sour	ce Destination/Application/Service Forwarding Active/Active HA Binding Tar	get
Action	Forward	~
Egress Interface	tunnel.1	~
Next Hop	None	~
Monitor —		
Profile		~
	Disable this rule if nexthop/monitor ip is unreachable	
IP Address		
- Enforce Symme	tric Return	
NEXT HOP ADDRE	ISS LIST	
	Ν	
	45	
🕣 Add 💮 Dele		
Schedule	None	~
		Cancel
		_

Troubleshooting PAN

- o Useful CLI commands
- Show vpn ike-sa gateway <name>
- Test vpn ike-sa gateway <name>
- o Debug ike stat
- o Check if the firewalls are negotiating the tunnels and ensure the two unidirectional SPIs exist
- o Show vpn ispec-sa
- Show vpn ipsec-sa tunnel <tunnel.name>

```
tacadmin@awsuseastbroweatfwl> show vpn ike-sa detail gateway IKE-GW-ForcePointOne
IKE Gateway IKE-GW-ForcePointOne, ID 1 10.128.230.253 =>
Current time: Jun.23 15:00:08
IKE SA:
SFI: C163A374A7840CE4:8BEFB4344439F4A8 Init
State: Established
SN: 1
Authentication: PSK, peer PSK
Proposal: AES256-CBC/SHA256/DH20
ID local: fqdn:
    remote: fqdn:
    ID_1: FQDN:
    ID_r: FQDN:
    ID_r: FQDN:
    MAT: ME PE
    Message ID: rx 0, tx 8
Liveness check: sending informational packet after idle 5 seconds
```

Forcepoint

About Forcepoint

forcepoint.com/contact

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. [FP ONE and Palo Alto IPSec Configuration Guide] 10Oct2023