

Creating Site – to – site VPN tunnel in fortigate.
Two phages will be created, Phase-1 and Phase-2

Creating Phase -1. This phase include mapping of public ip of client side.

FortiGate 80E FGT80ETK18004889				
<div>Dashboard ></div> <div>Security Fabric ></div> <div>FortiView ></div> <div>Network ></div> <div>System ></div> <div>Policy & Objects ></div> <div>Security Profiles ></div> <div>VPN ></div> <div>One-Click VPN Settings ></div> <div>IPsec Tunnels ☆</div> <div>IPsec Wizard</div> <div>IPsec Tunnel Templates</div> <div>SSL-VPN Portals</div> <div>SSL-VPN Settings</div> <div>User & Device ></div> <div>WiFi & Switch Controller ></div> <div>Log & Report ></div> <div>Monitor ></div>	<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Print Instructions</div><div>Search</div></div>			
	<div>Tunnel ▾Interface Binding ▾Status ▾R</div>			
	<div>Custom 9</div>			
	Amba	wan1	Up	4
	Batacurki	wan1	Up	4
	Chandgarh	wan1	Up	4
	Chikodi-Karosi	wan1	Inactive	4
	Jaisalmer	wan1	Up	4
	Jath	wan1	Up	4
	Jath-CLP	wan1	Up	4
	Lingasugur	wan1	Up	4
	RON	wan1	Up	4

2. Give name to the site.

FortiGate 80E FGT80ETK18004889	
<div>Dashboard ></div> <div>Security Fabric ></div> <div>FortiView ></div> <div>Network ></div> <div>System ></div> <div>Policy & Objects ></div> <div>Security Profiles ></div> <div>VPN ></div> <div>One-Click VPN Settings</div> <div>IPsec Tunnels</div> <div>IPsec Wizard ☆</div> <div>IPsec Tunnel Templates</div> <div>SSL-VPN Portals</div> <div>SSL-VPN Settings</div> <div>User & Device ></div> <div>WiFi & Switch Controller ></div> <div>Log & Report ></div> <div>Monitor ></div>	<div>VPN Creation Wizard</div> <div><div>1 VPN Setup</div><div>Name</div><div>Template Type</div><div>Site to Site Remote Access Custom</div><div>< Back</div><div>Next ></div><div>Cancel</div></div>

3. Map public IP of remote side.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

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

New VPN Tunnel

Name

Enter site name

Comments

Comments0/255

Network

IP Version

IPv4IPv6

Remote Gateway

Static IP Address

IP Address

0.0.0.0

Interface

Local Gateway

Mode Config

NAT Traversal

EnableDisableForced

Keepalive Frequency

10

Dead Peer Detection

DisableOn IdleOn Demand

Authentication

Method

Pre-shared Key

Pre-shared Key

.....

IKE

Version

12

Mode

AggressiveMain (ID protection)

OK

4. Set Encryption type according to remote configuration.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

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

New VPN Tunnel

Phase 1 Proposal

Add

Encryption

AES128

Authentication

SHA256

Encryption

AES256

Authentication

SHA256

Encryption

AES128

Authentication

SHA1

Encryption

AES256

Authentication

SHA1

Diffie-Hellman Groups

31

30

29

28

27

21

20

19

18

17

16

15

14

5

2

1

Key Lifetime (seconds)

86400

Local ID

XAUTH

Type

Disabled

Phase 2 Selectors

Name

Enter site name

Local Address

0.0.0.0/0.0.0.0

Remote Address

0.0.0.0/0.0.0.0

New Phase 2

Name

Enter site name

Comments

Comments

Local Address

Subnet0.0.0.0/0.0.0.0

OK

5. Phase -2 includes configuration of private ip mapping of both the sides(encryption domain). Also configure the encryption type.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

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

New VPN Tunnel

Phase 2 Selectors

Name	Local Address	Remote Address
Enter site name	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

New Phase 2

Name

Enter site name

Comments

Comments

Local Address

Subnet

0.0.0.0/0.0.0.0

Remote Address

Subnet

0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Add

Encryption	AES128	Authentication	SHA1
Encryption	AES256	Authentication	SHA1
Encryption	AES128	Authentication	SHA256
Encryption	AES256	Authentication	SHA256
Encryption	AES128GCM		
Encryption	AES256GCM		
Encryption	CHACHA20POLY1305		

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

313029282721

OKCancel

6. Configure the static route in the static route field.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

Network

Interfaces

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes

System

Policy & Objects

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Create NewEditCloneDelete

Destination	Gateway	Comment
0.0.0.0/0	205.147.96.1	wan1
192.168.111.1/32		Jath
192.168.111.2/32		Amba
192.168.111.6/32		Batacurki
192.168.111.8/32		Chandgarh
192.168.111.9/32		Jath-CLP
192.168.111.3/32		Lingasugur
192.168.111.4/32		Chikodi-Karosi
192.168.111.5/32		RON
192.168.111.7/32		Jaisalmer

7. Define policy of IN and OUT traffic, Example given in the point 8 and 9.

FortiGate 80E FGT80ETK18004889									
+ Create New Edit Delete Policy Lookup Search									
		Address		all					
		Type		Subnet					
		Subnet		0.0.0.0/0					
		Interface		any					
ID	Name	From	To	Source	Destination	Schedule	Service		
1		lan	wan1	all	all	always	ALL		
2	VPN-in	Jath	wan2	jath-local-subnet	E2E-Local-subnet	always	ALL		
3	VPN-out	wan2	Jath	E2E-Local-subnet	jath-local-subnet	always	ALL		
4	VPN-AMBA-IN	Amba	wan2	Amba-Local-Subnet	E2E-Local-subnet	always	ALL		
5	VPN-AMBA-OUT	wan2	Amba	E2E-Local-subnet	Amba-Local-Subnet	always	ALL		
6	VPN-BATA-IN	Batacurki	wan2	BATACURKI-LOCAL-SUBNET	E2E-Local-subnet	always	ALL		
7	VPN-BATA-OUT	wan2	Batacurki	E2E-Local-subnet	BATACURKI-LOCAL-SUBNET	always	ALL		
8	VPN-CHANDGARH-IN	Chandgarh	wan2	Chandgarh-local-SUB	E2E-Local-subnet	always	ALL		
9	VPN-CHANDGARH-OUT	wan2	Chandgarh	E2E-Local-subnet	Chandgarh-local-SUB	always	ALL		
10	VPN-JATH-CLP-IN	Jath-CLP	wan2	Jath-CLP-local-SUB	E2E-Local-subnet	always	ALL		
11	VPN-JATH-CLP-OUT	wan2	Jath-CLP	E2E-Local-subnet	Jath-CLP-local-SUB	always	ALL		

8. Setting IN traffic.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Traffic Shapers

Traffic Shaping Policy

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Edit Policy

Name

VPN-AMBA-IN

Incoming Interface

Amba

Outgoing Interface

wan2

Source

Amba-Local-Subnet

Destination

E2E-Local-subnet

Schedule

always

Service

ALL

Action

ACCEPT

DENY

Firewall / Network Options

NAT

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

SSL Inspection

OK

Cancel

9. Setting OUT traffic.

The screenshot shows the 'Edit Policy' configuration page for a policy named 'VPN-AMBA-OUT'. The configuration is as follows:

- Name:** VPN-AMBA-OUT
- Incoming Interface:** wan2
- Outgoing Interface:** Amba
- Source:** E2E-Local-subnet
- Destination:** Amba-Local-Subnet
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)

Below the policy configuration, the 'Firewall / Network Options' section shows 'NAT' is disabled. The 'Security Profiles' section shows all options (AntiVirus, Web Filter, DNS Filter, Application Control, and SSL Inspection) are disabled.

At the bottom right, there are 'OK' and 'Cancel' buttons.

10. Start the tunnel by clicking bringing UP, example in point 11.

The screenshot shows the 'Monitor' page with the 'IPsec Monitor' section selected. The table displays the status of various IPsec tunnels. The 'Bring Up' button is highlighted in the top toolbar.

Name	Type	Remote Gateway	User Name	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Amba	Custom	117.240.218.11		9.44 MB	3.41 MB	Amba	Amba
Batacurki	Custom	182.73.180.44		426.00 kB	301.33 kB	Batacurki	Batacurki
Chandgarh	Custom	42.104.88.20		426.04 kB	168.90 kB	Chandgarh	Chandgarh
Chikodi-Karosi	Custom	182.72.141.222		0 B	0 B	Chikodi-Karosi	Chikodi-Karosi
Jaisalmer	Custom	123.63.121.106		294.92 kB	37.08 kB	Jaisalmer	Jaisalmer
Jath	Custom	117.240.219.234		16.55 MB	247.98 MB	Jath	Jath
Jath-CLP	Custom	117.240.219.236		294.95 kB	168.31 kB	Jath-CLP	Jath-CLP
Lingasugur	Custom	182.71.105.21		16.47 kB	16.47 kB	Lingasugur	Lingasugur
RON	Custom	182.74.120.90		1.08 MB	697.12 kB	RON	RON

11. Bringing UP of the tunnel.

FortiGate 80E FGT80ETK18004889

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Routing Monitor

DHCP Monitor

SD-WAN Monitor

IPsec Monitor

SSL-VPN Monitor

Refresh

Reset Statistics

Bring Up

Bring Down

Name	Type	Remote Gateway	User Name	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Amba	Custom	117.240.218.11		9.44 MB	3.41 MB	Amba	Amba
Batacurki	Custom	182.73.180.44		426.00 kB	301.33 kB	Batacurki	Batacurki
Chandgarh	Custom	42.104.88.20		426.04 kB	168.90 kB	Chandgarh	Chandgarh
Chikodi-Karosi	Custom	182.72.141.22		0 B	0 B	Chikodi-Karosi	Chikodi-Karosi
Jaisalmer	Custom	123.63.121.10			37.08 kB	Jaisalmer	Jaisalmer
Jath	Custom	117.240.219.2			247.98 MB	Jath	Jath
Jath-CLP	Custom	117.240.219.236		294.95 kB	168.31 kB	Jath-CLP	Jath-CLP
Lingasugur	Custom	182.71.105.21		16.47 kB	16.47 kB	Lingasugur	Lingasugur
RON	Custom	182.74.120.90		1.08 MB	697.12 kB	RON	RON

Reset Statistics

Bring Up

Bring Down

Phase 2 Selector: Chikodi-Karosi

All Phase 2 Selectors

- * Try to ping the remote side pvt ip. If possible create static route in the local server.
- * `/sbin/route add -net xxx.xxx.xxx.xxx netmask 255.255.240.0 gw xxx.xxx.xx.xxx`
- * or add permanantly in route by adding in `/etc/rc.local` in end of file , before `"exit 0"`.