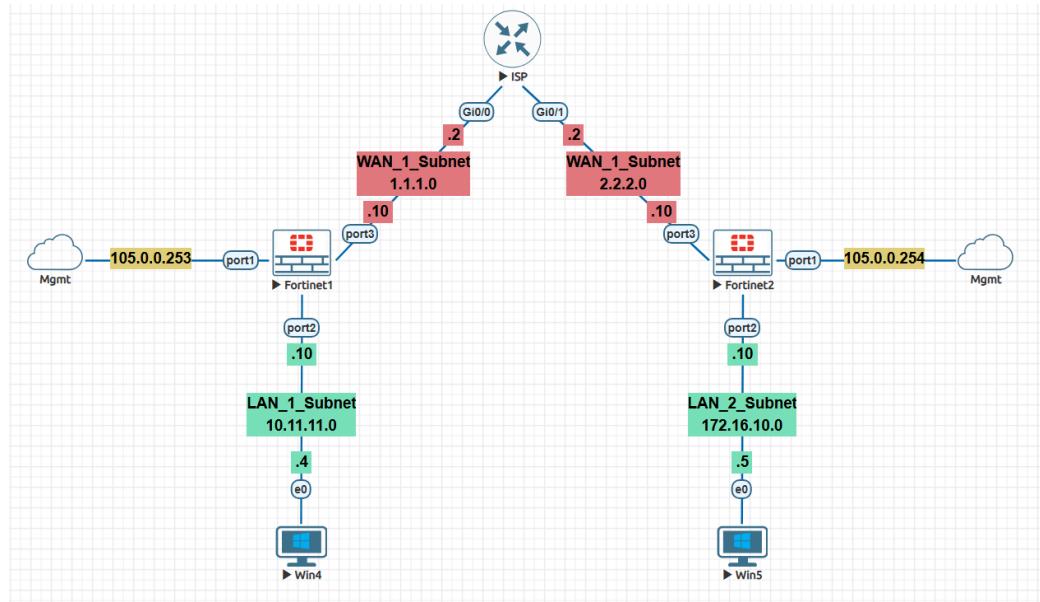


Configuring IPsec Site to Site VPN using different Next Generation Firewalls

Fortigate



Step 1: Configure the basic topology

Step 2: Create the Default route on both the firewalls towards the ISP

Screenshot of the FortiGate VM64-KVM interface showing the configuration of a static route on Forti1. The "Static Routes" tab is selected in the left sidebar.

New Static Route

Destination	Subnet	Internet Service
Gateway Address	0.0.0.0/0.0.0	1.1.1.2
Interface	WAN (port3)	
Administrative Distance	10	
Comments	Write a comment... /255	
Status	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Advanced Options

OK Cancel

Screenshot of the FortiGate VM64-KVM interface showing the configuration of a static route on Forti2. The "Static Routes" tab is selected in the left sidebar.

New Static Route

Destination	Subnet	Internet Service
Gateway Address	0.0.0.0/0.0.0	2.2.2.2
Interface	WAN (port3)	
Administrative Distance	10	
Comments	Write a comment... /255	
Status	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Advanced Options

OK Cancel

Check the basic connectivity before configuring the site to site VPN

```

Forti1 # execute ping 2.2.2.10
PING 2.2.2.10 (2.2.2.10): 56 data bytes
64 bytes from 2.2.2.10: icmp_seq=0 ttl=254 time=5.4 ms
64 bytes from 2.2.2.10: icmp_seq=1 ttl=254 time=4.9 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 2.2.2.10: icmp_seq=2 ttl=254 time=3.9 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=254 time=3.2 ms
Warning: Got ICMP 3 (Destination Unreachable)
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 2.2.2.10: icmp_seq=4 ttl=254 time=3.1 ms
--- 2.2.2.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.1/4.1/5.4 ms

Forti1 #

Forti2 # execute ping 1.1.1.10
Password: *****
Welcome !
PING 1.1.1.10 (1.1.1.10): 56 data bytes
64 bytes from 1.1.1.10: icmp_seq=0 ttl=254 time=2.7 ms
64 bytes from 1.1.1.10: icmp_seq=1 ttl=254 time=7.3 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 1.1.1.10: icmp_seq=2 ttl=254 time=2.1 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 1.1.1.10: icmp_seq=3 ttl=254 time=2.6 ms
64 bytes from 1.1.1.10: icmp_seq=4 ttl=254 time=2.1 ms
--- 1.1.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.1/3.3/7.3 ms

Forti2 #

```

2. Fortinet1 3. Fortinet2

Step 3: Configure Site to Site VPN

Change the NGFW mode setting from policy based to profile based

System> Settings> NGFW Mode

FortiGate VM64-KVM Forti1

System Settings

WiFi CA certificate: Fortinet_CA

>Password Policy: Off Admin IPsec Both

View Settings: Language English, Lines per page 50 (20 - 1000), Theme Green, Date/Time display FortiGate timezone, Browser timezone

NGFW Mode: **Profile-based** (Policy-based)

Central SNAT: Off

Start Up Settings: Auto file system check: On, USB auto-install: Detect configuration fgt_system.conf, Detect firmware image.out

Email Service: Off

Apply

Configure IPsec

Dashboard> VPN> IPsec Wizard>

FortiGate VM64-KVM Forti1

IPsec Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name: Forti1

Template type: **Site to Site** (Hub-and-Spoke, Remote Access, Custom)

NAT configuration: No NAT between sites (This site is behind NAT, The remote site is behind NAT)

Remote device type: FortiGate (Cisco)

Site to Site - FortiGate diagram: This FortiGate (Local) is connected via the Internet to a Remote FortiGate (Remote).

< Back Next > Cancel

FortiGate VM64-KVM Forti1

Dashboard > VPN Creation Wizard > 2 Authentication > 3 Policy & Routing

Remote device IP Address Dynamic DNS
2.2.2.10

Outgoing Interface WAN (port3)

Authentication method Pre-shared Key Signature
Pre-shared key Cisc@0123

Forti1: Site to Site - FortiGate

< Back Next > Cancel

FortiGate VM64-KVM Forti1

Dashboard > VPN Creation Wizard > 2 Authentication > 3 Policy & Routing

Local interface LAN (port2)

Local subnets 10.11.10.0/24

Remote Subnets 172.16.10.0/24

Internet Access None Share Local Use Remote

Forti1: Site to Site - FortiGate

< Back Create Cancel

FortiGate VM64-KVM Forti1

Dashboard > VPN Creation Wizard > 2 Authentication > 3 Policy & Routing

The VPN has been set up

Summary of Created Objects

Phase 1 Interface	Forti1
Local Address Group	Forti1_local
Remote Address Group	Forti1_remote
Phase 2 Interface	Forti1
Static Route	2
Blackhole Route	3
Local to Remote Policy	vpn_Forti1_local (1)
Remote to Local Policy	vpn_Forti1_remote (2)

Add Another Show Tunnel List

Same way configure the Fortigate2

Step 4: Configure the Policy

Dashboard > Policy & Objects > Ipv4 Policy

FortiGate VM64-KVM Forti1

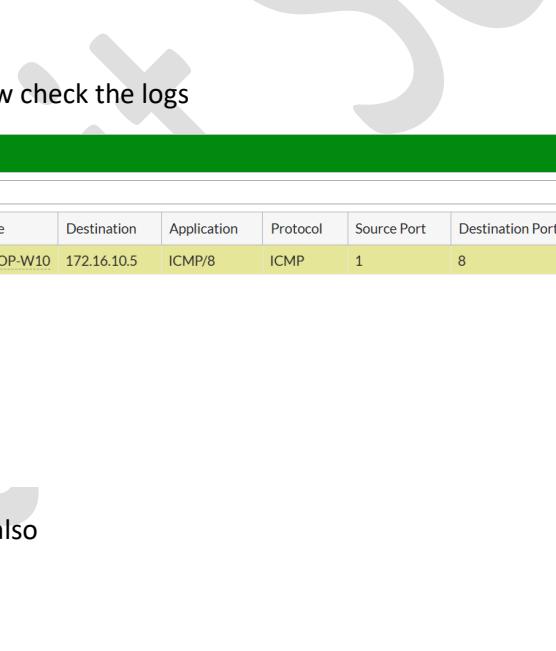
Dashboard		+ Create New	Edit	Delete	Policy Lookup	Search	Interface Pair View	By Sequence		
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Forti1 → LAN (port2)	Forti1_remote	Forti1_local	always	All	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
2	LAN (port2) → Forti1	Forti1_local	Forti1_remote	always	All	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
Implicit	1									
0	Implicit Deny	all	all	always	All	✗ DENY			✗ Disabled	0 B

FortiGate VM64-KVM Forti2

Dashboard		+ Create New	Edit	Delete	Policy Lookup	Search	Interface Pair View	By Sequence		
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Forti2 → LAN (port2)	Forti2_remote	Forti2_local	always	All	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
2	LAN (port2) → Forti2	Forti2_local	Forti2_remote	always	All	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
Implicit	1									
0	Implicit Deny	all	all	always	All	✗ DENY			✗ Disabled	0 B

If you will see, automatically tunnel interfaces are created

If you try communicating from LAN 1 to LAN 2



QEMU (Win4)

Command Prompt

```

ThC:\Users\user>ping 10.11.11.10
Pinging 10.11.11.10 with 32 bytes of data:
Reply from 10.11.11.10: bytes=32 time=430ms TTL=255
Reply from 10.11.11.10: bytes=32 time=1ms TTL=255
Reply from 10.11.11.10: bytes=32 time=2ms TTL=255
Reply from 10.11.11.10: bytes=32 time=2ms TTL=255

Ping statistics for 10.11.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 430ms, Average = 108ms

ContrC:\Users\user>firewall.cpl

C:\Users\user>
C:\Users\user>ping 172.16.10.5

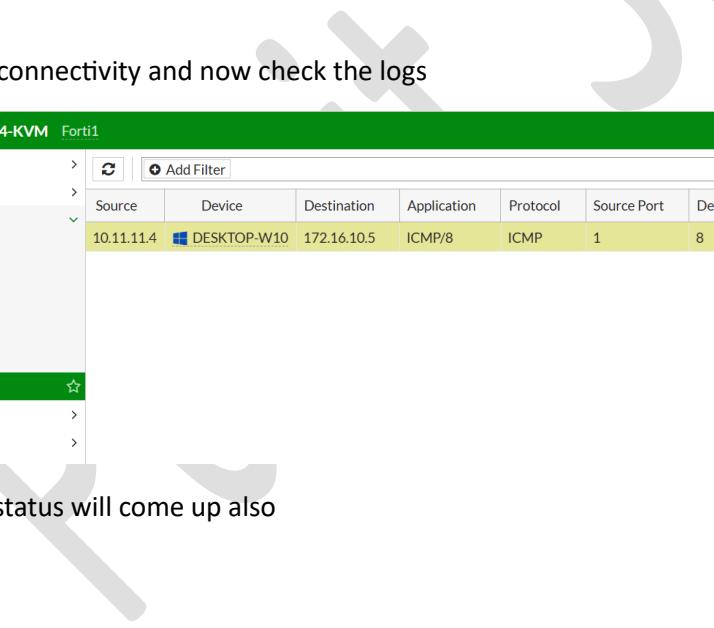
Pinging 172.16.10.5 with 32 bytes of data:
Request timed out.
Reply from 172.16.10.5: bytes=32 time=10ms TTL=126
Reply from 172.16.10.5: bytes=32 time=7ms TTL=126
Reply from 172.16.10.5: bytes=32 time=4ms TTL=126

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 10ms, Average = 7ms

C:\Users\user>
```

5:13 AM

We got the connectivity and now check the logs



FortiGate VM64-KVM FortiView

Dashboard > Add Filter

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	packets	Duration (sec)
10.11.11.4	DESKTOP-W10	172.16.10.5	ICMP/8	ICMP	1	8	480 B	8	6s

FortiView

- Sources
- Destinations
- Applications
- Web Sites
- Policies

All Sessions

- Network
- System

The tunnel status will come up also

The screenshot shows the FortiGate VM64-KVM interface. The left sidebar navigation includes: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN (selected), Overlay Controller VPN, IPsec Tunnels (selected), IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings, VPN Location Map, User & Device, Log & Report, and Monitor.

The main content area displays a table for Site to Site - FortiGate 1. It shows one entry for Forti1, which is connected to WAN (port3). The status is Up, and there are 4 references.

If you will check on the CLI

#show system interface

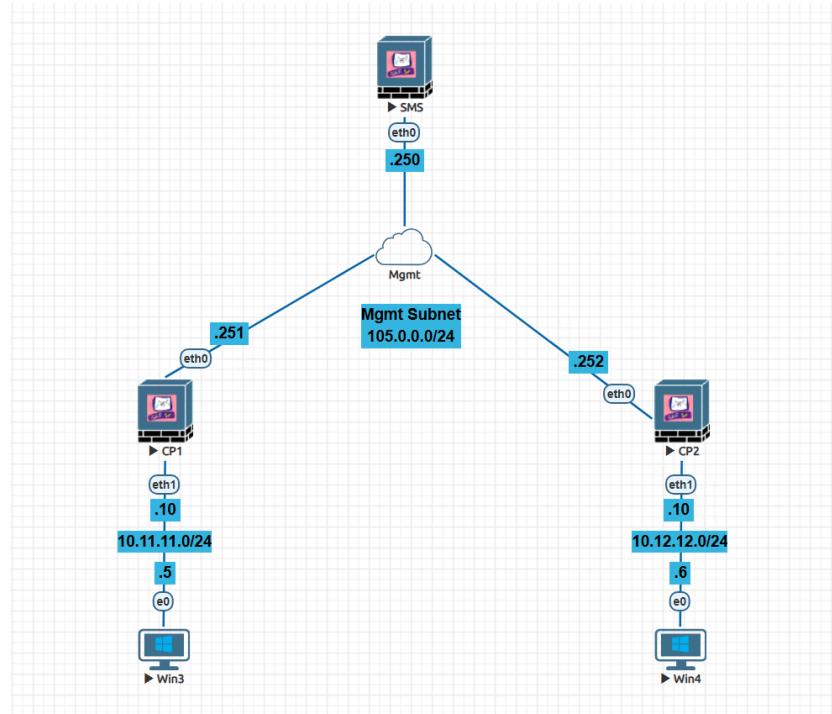
```

edit "port2"
set vdom "root"
set ip 10.11.11.10 255.255.255.0
set allowaccess ping
set type physical
set alias "LAN"
set device-identification enable
set lldp-transmission enable
set role lan
set snmp-index 2
2025/04/20:20:57
edit "port3"
set vdom "root"
set ip 1.1.1.10 255.255.255.0
set allowaccess ping
set type physical
set alias "WAN"
set lldp-reception enable
set role wan
set snmp-index 3
2025/04/20:20:25
edit "port4"
set vdom "root"
set type physical
set snmp-index 4
next
2025/04/20:20:25
edit "$ssl.root"
set vdom "root"
set type tunnel
set alias "SSL VPN interface"
set snmp-index 5
next
edit "Forti1"
set vdom "root"
set type tunnel
set snmp-index 6
set interface "port3"
next
end
Forti1 #
Forti1 # 

```

2. Fortinet1

Checkpoint



Step 1: Configure the basic topology

Step 2: Create the policy for management subnet and LAN interfaces

No.	Name	Source	Destination	VPN	Services & Applications	Time
1	LAN2_CP2	LAN2_Subnet	LAN2_Subnet	* Any	* Any	* Any
2	LAN1_CP1	LAN1_Subnet	LAN1_Subnet	* Any	* Any	* Any
3	Mgmt Rule	Mgmt_Subnet	Mgmt_Subnet	* Any	* Any	* Any
4	Cleanup rule	* Any	* Any	* Any	* Any	* Any

Step 3: Check the connectivity between LAN PCs to respective firewall and CP1 to CP2

```
QEMU (Win3)
This PC

Command Prompt
C:\Users\user>ping 10.11.11.10

Pinging 10.11.11.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 10.11.11.10: bytes=32 time=23ms TTL=64
Ping statistics for 10.11.11.10:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 23ms, Average = 23ms

C:\Users\user>
C:\Users\user>
C:\Users\user>
C:\Users\user>ping 10.11.11.10

Pinging 10.11.11.10 with 32 bytes of data:
Reply from 10.11.11.10: bytes=32 time=2ms TTL=64
Reply from 10.11.11.10: bytes=32 time=1ms TTL=64
Reply from 10.11.11.10: bytes=32 time=2ms TTL=64
Reply from 10.11.11.10: bytes=32 time=2ms TTL=64

Ping statistics for 10.11.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\user>

QEMU (Win4)
This PC

Command Prompt
Request timed out.
Recycling statistics for 10.12.12.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\user>ping 10.12.12.10

Pinging 10.12.12.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.12.12.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\user>ping 10.12.12.10

Pinging 10.12.12.10 with 32 bytes of data:
Reply from 10.12.12.10: bytes=32 time=14ms TTL=64
Reply from 10.12.12.10: bytes=32 time=3ms TTL=64
Reply from 10.12.12.10: bytes=32 time=2ms TTL=64
Reply from 10.12.12.10: bytes=32 time=2ms TTL=64

Ping statistics for 10.12.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\Users\user>
```

```

CP1
This system is for authorized use only.
login: admin
Password:
Last login: Tue Mar 25 13:26:25 on ttys0
CLINFR0771 Config lock is owned by admin. Use the command 'lock database
CP1>
CP1> ping 105.0.0.252
PING 105.0.0.252 (105.0.0.252) 56(84) bytes of data.
64 bytes from 105.0.0.252: icmp_seq=1 ttl=64 time=25.7 ms
64 bytes from 105.0.0.252: icmp_seq=2 ttl=64 time=3.34 ms
64 bytes from 105.0.0.252: icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 105.0.0.252: icmp_seq=4 ttl=64 time=1.81 ms
--- 105.0.0.252 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.277/8.054/25.781/10.262 ms
CP1> 

CP2
This system is for authorized use only.
login: admin
Password:
Last login: Tue Mar 25 13:26:44 on ttys0
CLINFR0771 Config lock is owned by admin. Use the command 'lock database
CP2>
CP2> ping 105.0.0.251
PING 105.0.0.251 (105.0.0.251) 56(84) bytes of data.
64 bytes from 105.0.0.251: icmp_seq=1 ttl=64 time=27.6 ms
64 bytes from 105.0.0.251: icmp_seq=2 ttl=64 time=2.09 ms
64 bytes from 105.0.0.251: icmp_seq=3 ttl=64 time=2.06 ms
64 bytes from 105.0.0.251: icmp_seq=4 ttl=64 time=3.89 ms
--- 105.0.0.251 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 2.066/8.920/27.622/10.823 ms
CP2> 

```

Step 4: Enable IPsec blades on both the firewalls in smart console

Check Point Gateway - CP2

General Properties

- Machine: Name: CP2, Color: Black
- IPv4 Address: 105.0.0.252, Resolve from Name:
- IPv6 Address:
- Comment:
- Secure Internal Communication: Trust established, Communication:

Platform

- Hardware: Open server, Version: R81.10, OS: Gaia, Get

Network Security (2)

- Access Control:**
 - Firewall
 - IPsec VPN
 - Policy Server
 - Mobile Access
 - Application Control
 - URL Filtering
 - Identity Awareness
 - Content Awareness
- Advanced Networking & Clustering:**
 - Dynamic Routing
 - SecureXL
 - QoS
 - Monitoring
 - Other
 - Data Loss Prevention
 - Anti-Spam & Email Security

IPSec VPN

Sophisticated but simple to manage Site-to-Site VPN and flexible Remote Access working seamlessly with a variety of VPN agents.

Comments

Object Categories

- Network Objects: 22
- Services: 521
- Applications/Categories: 8313
- VPN Communities: 2
- Data Types: 62
- Users/identities: 1
- Servers: 1
- Time Objects: 3
- UserCheck Interactions: 13
- Limit: 4

Activate Blades...

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
Green	CP1	105.0.0.251	R81.10		Open server		Up to date	N/A	
Green	CP2	105.0.0.252	R81.10		Open server		Up to date	N/A	
Green	SMS	105.0.0.250	R81.10		Open server		Up to date	N/A	

CP2

IPv4 Address: 105.0.0.252
Access Control Policy: Standard
OS: Gaia
Version: R81.10
License Status:

Access Blades

Firewall | Site to Site VPN

Step 5: Configure the IPsec

Security Policies > VPN Communities > New Widget > Meshed Community

The screenshot shows the FortiManager interface under the 'SECURITY POLICIES' section. In the left sidebar, 'VPN Communities' is selected. The main pane displays a table of 'VPN Communities' with columns: Name, Topology, Encryption Suite, and Comm. Two entries are listed: 'MyIntranet' (Topology: Meshed, Comm: Custom) and 'RemoteAccess' (Topology: Remote Access, Comm: Custom). A new entry, 'Meshed Community', is being added, indicated by a yellow selection bar around its row.

VPN Communities

Name	Topology	Encryption Suite	Comm
MyIntranet	Meshed	Custom	
RemoteAccess	Remote Access	Custom	
Meshed Community			

MyIntranet

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Wiki
- Installation History

Participating Gateways

Encryption

Phase 1:

- Encryption Algorithm: AES-256
- Data Integrity: SHA1

Phase 2:

- Encryption Algorithm: AES-128

Give name > Add the firewalls

The screenshot shows the 'New Meshed Community' configuration dialog. The title is 'Site_To_Site'. The left sidebar lists configuration tabs: Gateways (selected), Encrypted Traffic, Encryption, Tunnel Management, Excluded Services, Shared Secret, Wire Mode, and Advanced. The main pane is titled 'Participating Gateways' and contains a table of selected gateways:

Gateway	Gateway Comments	VPN Domain
CP1	All IP addresses behind gateway based on topo...	
CP2	All IP addresses behind gateway based on topo...	

Buttons at the bottom right include 'OK' and 'Cancel'.

Encryption > Encryption Method > IKEv1 for IPv4 and IKEv2 for IPv6 only

New Meshed Community

Site _To_Site

Enter Object Comment

Gateways
Encrypted Traffic
Encryption
Tunnel Management
Excluded Services
Shared Secret
Wire Mode
Advanced

Encryption Method

Encryption Method: **IKEv1 for IPv4 and IKEv2 for IPv6 only**

Encryption Suite

Use this encryption suite: Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di...
 Custom encryption suite:

IKE Security Association (Phase 1)

Encryption Algorithm: AES-256
Data Integrity: SHA1
Diffie-Hellman group: Group 2 (1024 bit)

IKE Security Association (Phase 2)

Encryption Algorithm: AES-128
Data Integrity: SHA1
 Use Perfect Forward Secrecy
Diffie-Hellman group: Group 2 (1024 bit)

Override Encryption for Externally Managed Gateways

+ | | | Search... No items found

Internal	External	IKE Version	Ciphers

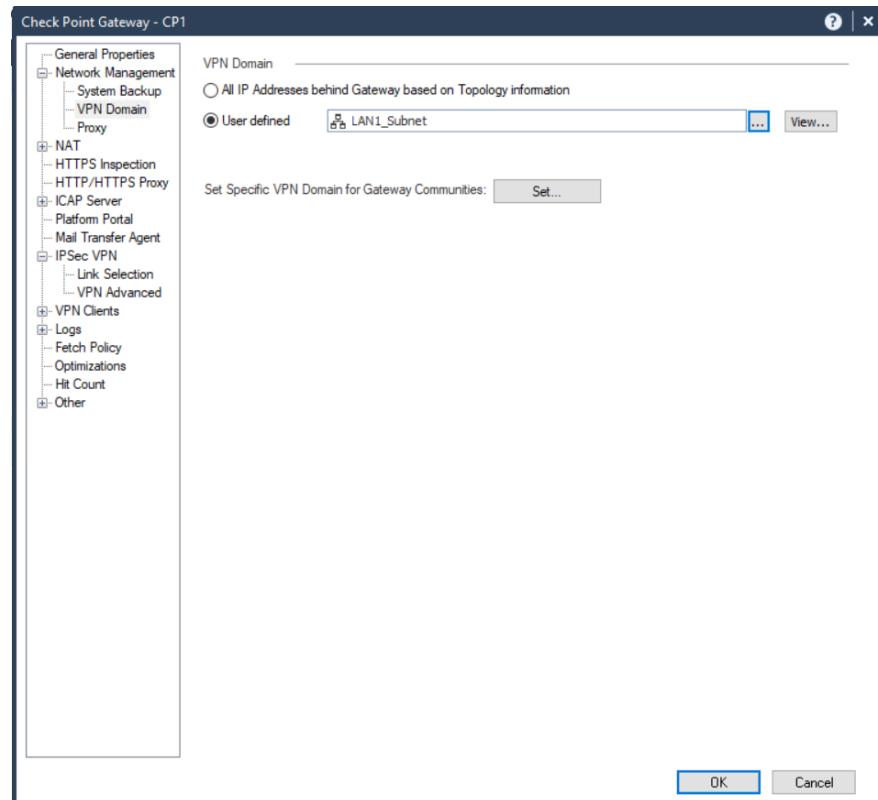
VPN Communities

* | | | Search... 3 items

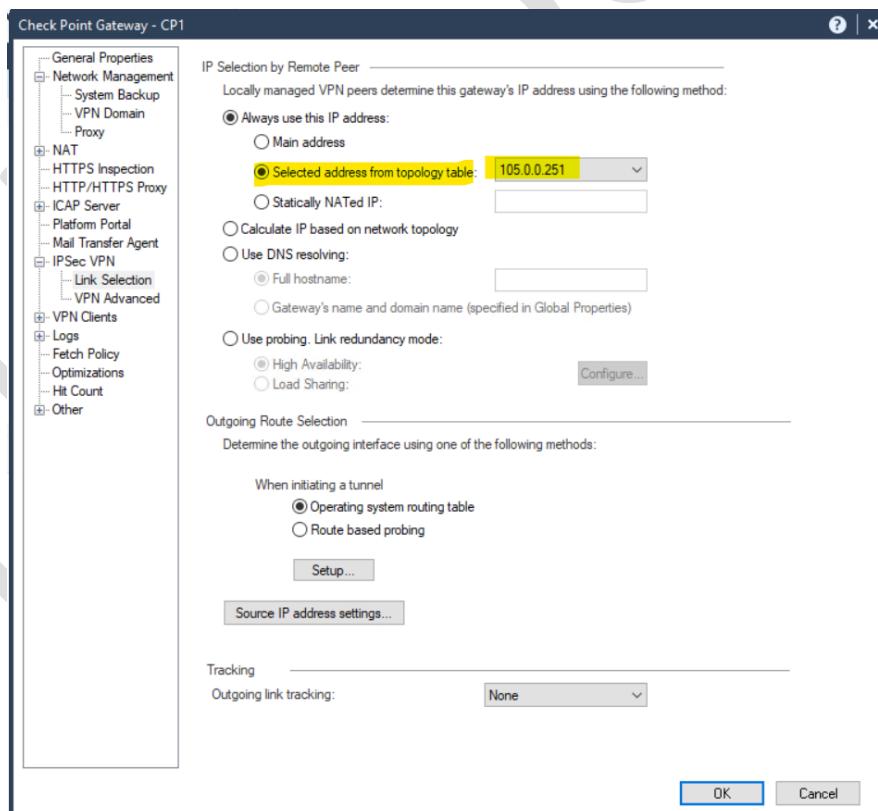
Name	Topology	Encryption Suite	Comments
MyIntranet	Meshed	Custom	
RemoteAccess	Remote Access	Custom	
Site _To_Site	Meshed	Custom	

Step 6: Assign the IPsec under the firewall

Gateways & Servers> CP1> Network Management > VPN Domain>



IPsec VPN> Link Selection



Repeat this on CP2 also

Step 7: Create the Policy

VPN > Right Click > Specific VPN Communities >

No.	Name	Source	Destination	VPN	Services & Applications	Time
1	Site_to_Site_CP1_CP2	LAN1_Subnet LAN2_Subnet	LAN1_Subnet LAN2_Subnet	Site_To_Site	* Any	* Any
2	LAN2_CP2	LAN2_Subnet	LAN2_Subnet	* Any	* Any	* Any
3	LAN1_CP1	LAN1_Subnet	LAN1_Subnet	* Any	* Any	* Any
4	Mgmt Rule	Mgmt_Subnet	Mgmt_Subnet	* Any	* Any	* Any
5	Cleanup rule	* Any	* Any	* Any	* Any	* Any

No.	VPN	Services & Applications	Time	Action	Track	Install On
1	Site_To_Site	* Any	* Any	Accept	Log	CP1 CP2
2	* Any	* Any	* Any	Accept	Log	CP2
3	* Any	* Any	* Any	Accept	Log	CP1
4	* Any	* Any	* Any	Accept	Log	CP1 CP2
5	* Any	* Any	* Any	Drop	None	* Policy...

Install and Publish

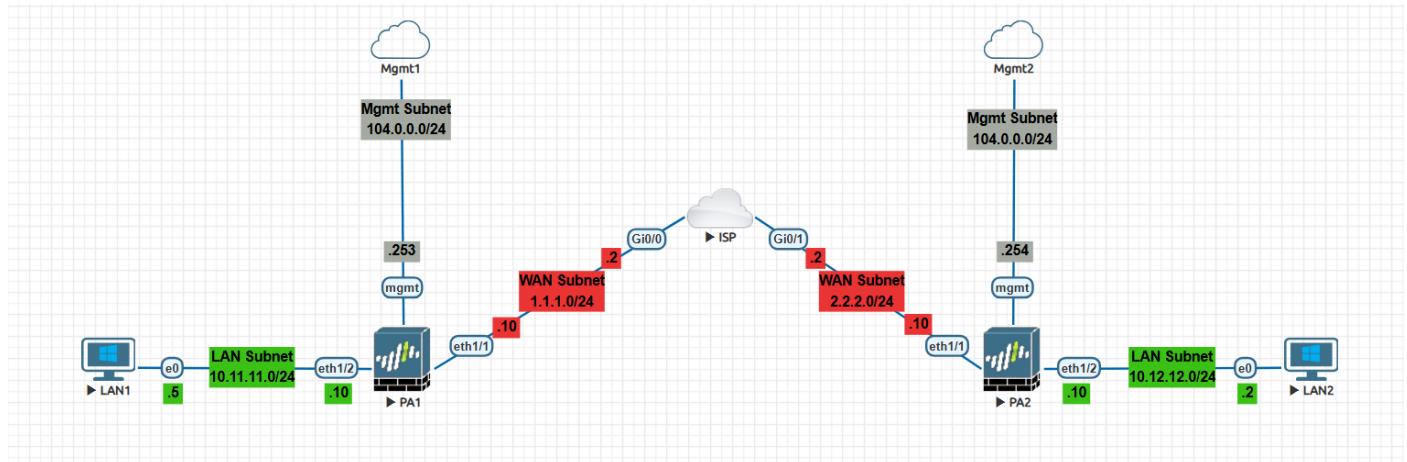
Note: Instead of making so many policies before the site to site policy, you can just change the cleanup rule from deny to allow

No.	Name	Source	Destination	VPN	Services & Applications	Time
1	Site_to_Site_CP1_CP2	LAN1_Subnet LAN2_Subnet	LAN1_Subnet LAN2_Subnet	Site_To_Site	* Any	* Any
2	Cleanup rule	* Any	* Any	* Any	* Any	* Any

No.	VPN	Services & Applications	Time	Action	Track	Install On
1	Site_To_Site	* Any	* Any	Accept	Log	CP1 CP2
2	* Any	* Any	* Any	Accept	None	* Policy...

Step 8: Try to ping from LAN 1 PC to LAN 2 PC and check the logs

Palo Alto



Step 1: Configure the topology

Step 2: Configure the interfaces on Palo Alto

Interface Management Profile

Name: WAN_Profile

Administrative Management Services:

- HTTP
- HTTPS
- Telnet
- SSH

Network Services:

- Ping
- HTTP OCSP
- SNMP
- Response Pages
- User-ID
- User-ID Syslog Listener-SSL
- User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

+ Add - Delete

Ex: IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To:

Virtual Router: default

Security Zone: WAN Zone

OK Cancel

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Link Settings

Link Speed: auto

Link Duplex: auto

Link State: auto

Other Info | ARP Entries | ND Entries | NDP Proxy | LLDP | DDNS

Management Profile: WAN_Profile

MTU: [576 - 1500]

Adjust TCP MSS

IPv4 MSS Adjustment: 40

IPv6 MSS Adjustment: 60

Untagged Subinterface

OK Cancel

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit | Undo | Redo | Search | ?

Interfaces

- Zones
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- GlobalProtect
- Portals

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	FEATURES	COMMENT
ethernet1/1	Layer3	WAN_Profile	Up	WAN_1	default	Untagged	none	WAN Zone			
ethernet1/2	Layer3	LAN_Profile	Up	LAN_IP	default	Untagged	none	LAN Zone			
ethernet1/3			Up	none	none	Untagged	none	none			
ethernet1/4			Up	none	none	Untagged	none	none			

24 items → X

Create a default route towards ISP

Virtual router> Choose the routing table> Static Route>

Virtual Router - default

Router Settings

Static Routes

IPv4 | IPv6

Redistribution Profile

NAME	DESTINA...	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
			TYPE	VALUE				
WAN Router	0.0.0.0/0		ip-address	2.2.2.2	default	10	None	unicast

+ Add | - Delete | Clone

OK | Cancel

Step 3: Check the reachability among PA1 and PA2

QEMU (PA1)

```
admin@PA-VM:~# delete deviceconfig system type dhcp-client
(admin@PA-VM) set deviceconfig system ip
+ ip-address: management address for the management interface
+ ip-address-lookup-url: IP address for the management interface
+ ip-default-gateway: IP default gateway
admin@PA-VM:~# set deviceconfig system ip-address 104.0.0.251 netmask 255.255.255.0
(admin@PA-VM) commit
Commit job 1 is in progress. Use Ctrl-C to return to command prompt
....., 559, 750, 98c....., 100%
Configuration committed successfully

(admin@PA-VM) exit
Exiting configuration mode
```

QEMU (PA2)

```
(edit)
admin@PA-VM:~# set device config system ip
+ ip-address: management address for the management interface
+ ip-address-lookup-url: IP address for the management interface
+ ip-default-gateway: IP default gateway
admin@PA-VM:~# set deviceconfig system ip-address 104.0.0.252 netmask 255.255.255.0
(admin@PA-VM) commit
Commit job 2 is in progress. Use Ctrl-C to return to command prompt
....., 559, 750, 98c....., 100%
Configuration committed successfully

(admin@PA-VM) exit
Exiting configuration mode
```

ping 2.2.2.10 (2.2.2.10) from 1.1.1.10 host 2.2.2.10
64 bytes from 2.2.2.10: icmp_seq=1 ttl=63 time=10.9 ms
64 bytes from 2.2.2.10: icmp_seq=2 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=4 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=5 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=6 ttl=63 time=10.5 ms
TTL=64 bytes from 2.2.2.10 host 1.1.1.10
PING 2.2.2.10 (2.2.2.10) from 1.1.1.10 : 56(64) bytes of data.
64 bytes from 2.2.2.10: icmp_seq=1 ttl=63 time=10.9 ms
64 bytes from 2.2.2.10: icmp_seq=2 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=4 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=5 ttl=63 time=21.6 ms
64 bytes from 2.2.2.10: icmp_seq=6 ttl=63 time=10.5 ms
TTL=64 bytes from 2.2.2.10 host 1.1.1.10
2.2.2.10 ping statistics --
5 packets transmitted, 4 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 2.507/2.590/15.706/5.235 ms
admin@PA-VM:

ping 10.11.11.5 (10.11.11.5) from 10.11.11.10 host 10.11.11.5
PING 10.11.11.5 (10.11.11.5) from 10.11.11.10 : 56(64) bytes of data.
64 bytes from 10.11.11.5: icmp_seq=1 ttl=128 time=2.50 ms
64 bytes from 10.11.11.5: icmp_seq=2 ttl=128 time=2.50 ms
64 bytes from 10.11.11.5: icmp_seq=3 ttl=128 time=2.50 ms
64 bytes from 10.11.11.5: icmp_seq=4 ttl=128 time=2.50 ms
64 bytes from 10.11.11.5: icmp_seq=5 ttl=128 time=2.50 ms
64 bytes from 10.11.11.5: icmp_seq=6 ttl=128 time=2.50 ms
TTL=64 bytes from 10.11.11.5 host 10.11.11.10
10.11.11.5 ping statistics --
5 packets transmitted, 4 received, 0% packet loss, time 401ms
rtt min/avg/max/mdev = 2.507/2.590/15.706/5.235 ms
admin@PA-VM:

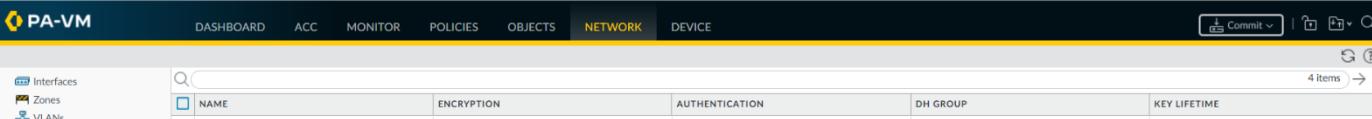
Step 4: Configure IKE phase 1 configuration

Network> Interfaces>Tunnel>Add

Make a tunnel profile enabling PING Service

Network> Network Profile> IKE Crypto> Add new

Note: You can add multiple DH(Defi hymen)group in IKE 1



The screenshot shows the PA-VM network configuration interface. The top navigation bar includes links for Dashboard, ACC, Monitor, Policies, Objects, Network (selected), and Device, along with a Commit button and search/filter icons. The left sidebar contains a tree view of network components: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (expanded to show Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, and Network Profiles (expanded to show GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, and IKE Crypto). The main content area displays a table for Network Profiles, showing columns for Name, Encryption, Authentication, DH Group, and Key Lifetime. The table lists four items: default (aes-128-cbc, 3des, sha1, group2, 8 hours), Suite-B-GCM-128 (aes-128-cbc, sha256, group19, 8 hours), Suite-B-GCM-256 (aes-256-cbc, sha384, group20, 8 hours), and Phase_1 (aes-128-cbc, sha256, group2, 24 hours). A search bar at the top right indicates "4 items" found.

NAME	ENCRYPTION	AUTHENTICATION	DH GROUP	KEY LIFETIME
default	aes-128-cbc, 3des	sha1	group2	8 hours
Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours
Phase_1	aes-128-cbc	sha256	group2	24 hours

Note: You can select multiple algorithms and DH group but any one should match on both the sides

IKE Gateway> Add

IKE Gateway

General | Advanced Options

Name	Phase_1_Gateway
Version	IKEv1 only mode
Address Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Interface	ethernet1/1
Local IP Address	WAN_1
Peer IP Address Type	<input checked="" type="radio"/> IP <input type="radio"/> FQDN <input type="radio"/> Dynamic
Peer Address	2.2.2.10
Authentication	<input checked="" type="radio"/> Pre-Shared Key <input type="radio"/> Certificate
Pre-shared Key	*****
Confirm Pre-shared Key	*****
Local Identification	None
Peer Identification	None
Comment	

You can give any pre shared key

IKE Gateway

General | **Advanced Options**

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1

Exchange Mode: auto

IKE Crypto Profile: Phase_1

Enable Fragmentation

Dead Peer Detection

Interval: 5

Retry: 5

OK **Cancel**

In Palo Alto there is an option for NAT traversal but in CISCO its by default enabled

Step 5: Create IPSEC configuration, phase 2 configuration

Network > Network Profiles > IPsec Crypto > add

IPSec Crypto Profile

Name: Phase_2

IPSec Protocol: ESP

DH Group: group2

Lifetime: Hours 1

Minimum lifetime = 3 mins

Enable

Lifesize: MB [1 - 65535]

Recommended lifesize is 100MB or greater

ENCRYPTION

- aes-128-cbc

AUTHENTICATION

- sha256

OK **Cancel**

Note: In phase 2 we can select the DH group

Step 6: Bind Phase 1 and Phase 2 configuration

LinkedIn: <https://www.linkedin.com/in/itspulkitsehgal/>

Network> IPsec tunnels

IPSec Tunnel

General | Proxy IDs

Name: **IPsec_Tunnel**

Tunnel Interface: **tunnel.1**

Type: Auto Key Manual Key GlobalProtect Satellite

Address Type: IPv4 IPv6

IKE Gateway: **Phase_1_Gateway**

IPSec Crypto Profile: **Phase_2**

Show Advanced Options

Comment:

OK Cancel

Step 7: Check whether tunnel is up or not

IKE Gateway/Satellite												
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	COMMENT
<input checked="" type="checkbox"/>	IPsec_Tunnel	Tunnel Info	Auto Key	ethernet1/1	WAN_1	2.2.2.10	IKE Info	tunnel1	default (Show Routes)	vsys1	Tunnel Zone	

It shows red that means its down, when they are turned green that means tunnel is up

Once you commit and ping the tunnel interfaces then it will be up

```
QEMU (PA1)
Administrator: ~

#0-#0 login: admin
Password:
Last login: Wed Feb 19 04:25:20 on ttys1

Number of failed attempts since last successful login: 0

admin@PA-VM: ping source 1.1.1.10 host 2.2.2.10
PING 2.2.2.10 (2.2.2.10) from 1.1.1.10 : 56(40) bytes of data.
64 bytes from 2.2.2.10: icmp_seq=2 ttl=63 time=39.9 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=63 time=0.32 ms
76
--- 2.2.2.10 ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 200ms
rtt min=0.32ms max=34.66ms avg=33.99ms stdv=15.53ms
admin@PA-VM: ping source 10.11.11.10 host 10.11.11.5
PING 10.11.11.5 (10.11.11.5) from 10.11.11.10 : 56(40) bytes of data.
64 bytes from 10.11.11.5: icmp_seq=1 ttl=120 time=14.5 ms
64 bytes from 10.11.11.5: icmp_seq=2 ttl=120 time=0.99 ms
76
--- 10.11.11.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3000ms
rtt min=0.99ms max=11.341ms avg=14.596ms stdv=3.250ms
admin@PA-VM: ping source 192.168.10.1 host 192.168.10.2
PING 192.168.10.2 (192.168.10.2) from 192.168.10.1 : 56(40) bytes of data.
76
```

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit

Interfaces	IKE Gateway/Satellite							Tunnel Interface				Comment
Zones	Name	Status	Type	Interface	Local IP	Peer Address	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
IPSec Tunnels	IPSEC_TUNNEL	Up Tunnel Info	Auto Key	ethernet1/2	WAN_INT_IP	2.2.2.10	Up IKE Info	tunnel1	default	Show Routes	vsys1	TUNNEL_ZONE

Step 8: Create a policy

Policies > Security > Add

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name	<input type="text" value="Tunnel_Policy"/>
Rule Type	interzone
Description	<input type="text"/>
Tags	<input type="text"/>
Group Rules By Tag	None
Audit Comment	<input type="text"/>
Audit Comment Archive	

OK

Cancel

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	<input type="text" value="any"/>	<input type="text" value="any"/>
<input type="checkbox"/> SOURCE ZONE	<input type="checkbox"/> SOURCE ADDRESS	<input type="checkbox"/> SOURCE USER	<input type="checkbox"/> SOURCE DEVICE
<input type="checkbox"/> LAN Zone			
<input type="checkbox"/> Tunnel Zone			
+ Add Delete			
<input type="checkbox"/> Negate			

OK

Cancel

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select	<input checked="" type="checkbox"/> Any	any
DESTINATION ZONE	DESTINATION ADDRESS	DESTINATION DEVICE
<input type="checkbox"/> LAN Zone		
<input type="checkbox"/> Tunnel Zone		
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="checkbox"/> Negate		
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="checkbox"/> Negate		

OK **Cancel**

Source will be LAN Destination will be tunnel

When source will be Tunnel destination will be LAN

Step 9: Specify the route in the virtual router

At the moment we have a static route towards ISP

But we need to tell that whenever the private IP traffic will come we need to redirect it from tunnel

Network> Virtual router> Select the virtual router> add a static route

Virtual Router - Static Route - IPv4

Name	Tunnel_Route												
Destination	10.12.12.0/24												
Interface	tunnel.1												
Next Hop	IP Address												
	192.168.10.2												
Admin Distance	New <input type="button" value="Address"/>												
Metric	10												
Route Table	Unicast												
BFD Profile	Disable BFD												
<input type="checkbox"/> Path Monitoring Failure Condition <input checked="" type="radio"/> Any <input type="radio"/> All Preemptive Hold Time (min) 2													
<table border="1"> <thead> <tr> <th>NAME</th> <th>ENABLE</th> <th>SOURCE IP</th> <th>DESTINATION IP</th> <th>PING INTERVAL(SEC)</th> <th>PING COUNT</th> </tr> </thead> <tbody> <tr> <td colspan="6"> <input type="button" value="Add"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table>		NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT	<input type="button" value="Add"/> <input type="button" value="Delete"/>					
NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT								
<input type="button" value="Add"/> <input type="button" value="Delete"/>													

OK **Cancel**

Virtual Router - default																																									
Router Settings IPv4 IPv6																																									
Static Routes																																									
Redistribution Profile																																									
RIP OSPF OSPFv3 BGP Multicast																																									
<table border="1"> <thead> <tr> <th rowspan="2"></th> <th rowspan="2">NAME</th> <th rowspan="2">DESTINA...</th> <th rowspan="2">INTERFACE</th> <th colspan="2">Next Hop</th> <th rowspan="2">ADMIN DISTANCE</th> <th rowspan="2">METRIC</th> <th rowspan="2">BFD</th> <th rowspan="2">ROUTE TABLE</th> </tr> <tr> <th>TYPE</th> <th>VALUE</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>WAN Router</td> <td>0.0.0.0/0</td> <td></td> <td>ip-address</td> <td>1.1.1.2</td> <td>default</td> <td>10</td> <td>None</td> <td>unicast</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Tunnel_R...</td> <td>10.12.12....</td> <td>tunnel.1</td> <td>ip-address</td> <td>192.168.1...</td> <td>default</td> <td>10</td> <td>None</td> <td>unicast</td> </tr> </tbody> </table>											NAME	DESTINA...	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE	TYPE	VALUE	<input type="checkbox"/>	WAN Router	0.0.0.0/0		ip-address	1.1.1.2	default	10	None	unicast	<input type="checkbox"/>	Tunnel_R...	10.12.12....	tunnel.1	ip-address	192.168.1...	default	10	None	unicast
	NAME	DESTINA...	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE																																
				TYPE	VALUE																																				
<input type="checkbox"/>	WAN Router	0.0.0.0/0		ip-address	1.1.1.2	default	10	None	unicast																																
<input type="checkbox"/>	Tunnel_R...	10.12.12....	tunnel.1	ip-address	192.168.1...	default	10	None	unicast																																

Ping from LAN1 PC to LAN2 PC

```

Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\user>ping 10.12.12.6

Pinging 10.12.12.6 with 32 bytes of data:
Reply from 10.12.12.6: bytes=32 time=51ms TTL=126
Reply from 10.12.12.6: bytes=32 time=15ms TTL=126
Reply from 10.12.12.6: bytes=32 time=11ms TTL=126
Reply from 10.12.12.6: bytes=32 time=10ms TTL=126

Ping statistics for 10.12.12.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 51ms, Average = 21ms

C:\Users\user>

```

Check the sessions

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CLEAR
02/20 04:09:12	WAN_ZONE	WAN_ZONE	1.1.1.10	2.2.2.10	500	500	17	ike	intrazone-default	ethernet1/2	ethernet1/2	2102	vsys1	<input checked="" type="checkbox"/>	
02/20 04:09:12	TUNNEL_ZO...	WAN_ZONE	1.1.1.10	2.2.2.10	39302	42753	50	ipsec-esp		ethernet1/2		0	vsys1	<input checked="" type="checkbox"/>	
02/20 04:16:15	LAN_ZONE	LAN_ZONE	10.11.11.5	10.11.11.255	138	138	17	undecided	intrazone-default	ethernet1/1	ethernet1/1	254	vsys1	<input checked="" type="checkbox"/>	

It will not show you the private IPs as then there is no point of tunnel

It shows port number 500, that means IKE tunnel

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM	CLEAR
02/20 04:29:02	LAN_ZONE	TUNNEL_ZO...	10.11.11.5	10.12.12.6	1	173	1	ping		TUNNEL_ZO...	ethernet1/1	tunnel.1	148	vsys1	<input checked="" type="checkbox"/>
Detail															
Session ID: 208															
Timeout: 6															
Virtual System: vsys1															
Application: ping															
Protocol: 1															
Security Rule: TUNNEL_POLICY															
QoS Rule: N/A															
QoS Class: 4															
Created By Syn Cookie: False															
To Host Session: False															
Traverse Tunnel: True															
Captive Portal: False															
Session End Log: True															
Session In Ager: False															
Session From HA: False															
End Reason: aged-out															
Tracker Stage Firewall: Aged out															
02/20 04:29:00	LAN_ZONE	TUNNEL_ZO...	10.11.11.5	10.12.12.6	1	171	1	ping		TUNNEL_ZO...	ethernet1/1	tunnel.1	148	vsys1	<input checked="" type="checkbox"/>
02/20 04:28:59	LAN_ZONE	TUNNEL_ZO...	10.11.11.5	10.12.12.6	1	170	1	ping		TUNNEL_ZO...	ethernet1/1	tunnel.1	148	vsys1	<input checked="" type="checkbox"/>
02/20 04:09:12	TUNNEL_ZO...	WAN_ZONE	1.1.1.10	2.2.2.10	39302	42753	50	ipsec-esp			ethernet1/2		0	vsys1	<input checked="" type="checkbox"/>

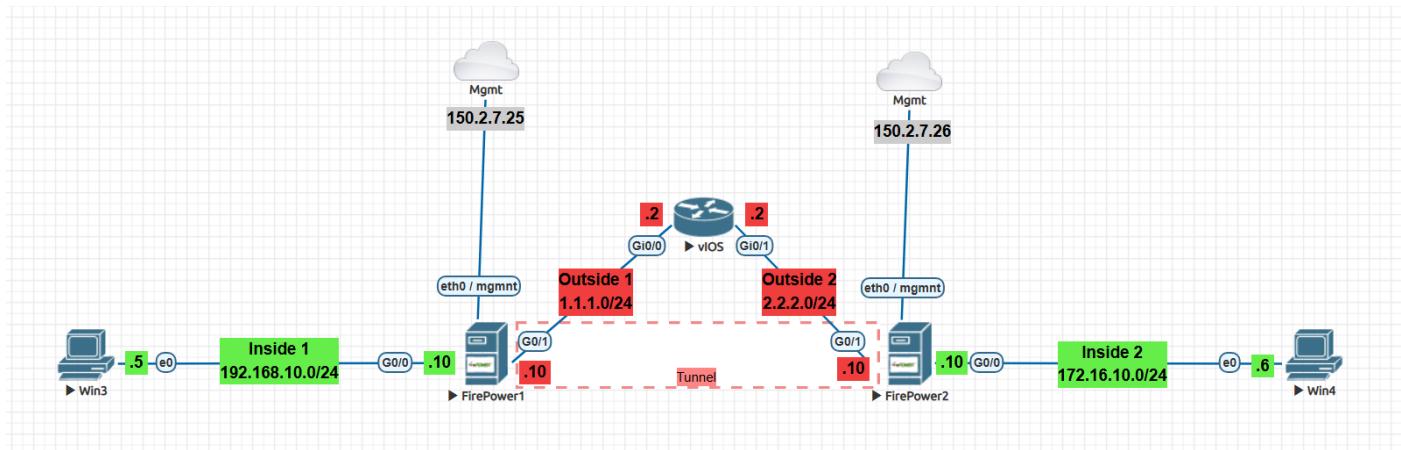
The traffic is generated from LAN1 PC and LAN2 PC is responding

The tunnel starts from WAN interface and ending at other WAN interface

If you will see the log, you will notice that source is LAN1 PC and responder is LAN2 PC

It will not show you the public IP and

CISCO FTD



Step 1: Configure the topology

Step 2: Configure the FMC and add don't add any device or policy

```
FMC_STUDENTS
- At least 1 special character such as @#*-_+!
- No more than 2 sequentially repeated characters
- Not based on a simple character sequence or a string in password cracking dictionary
Enter new password:
Confirm new password:
Enter a hostname or fully qualified domain name for this system [firepower]: FMC
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the Management interface [192.168.45.45]: 150.2.7.50
Enter an IPv4 netmask for the Management interface [255.255.255.0]:
Enter the IPv4 default gateway for the Management interface []: 150.2.7.1
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]: none
Enter a comma-separated list of NTP servers [0.sourceforge.pool.ntp.org, 1.sourceforge.pool.ntp.org]: 150.2.7.231

Hostname: FMC
IPv4 configured via: Manual configuration
Management interface IPv4 address: 150.2.7.50
Management interface IPv4 netmask: 255.255.255.0
Management interface IPv4 gateway: 150.2.7.1
DNS servers: none
NTP servers: 150.2.7.231

Are these settings correct? (y/n) y
```

Step 3: Create a policy and then add the individual FTD under that policy

Firepower Management Center
Policies / Access Control / Access Control

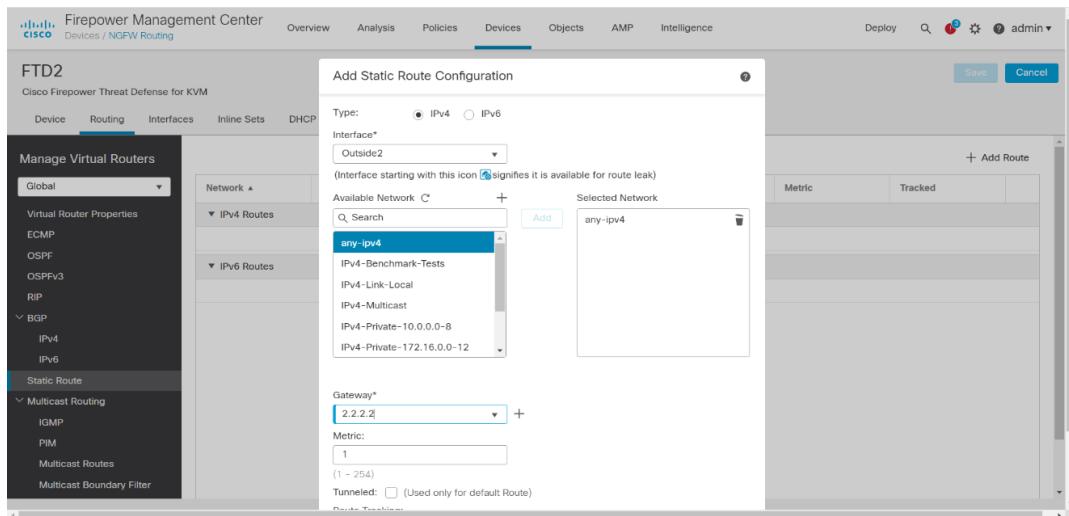
Access Control Policy	Domain	Status	Last Modified	Actions
FTD-Site-1	Global	Targeting 0 devices	2025-02-19 01:15:32 Modified by "admin"	
FTD-Site-2	Global	Targeting 0 devices	2025-02-19 01:16:08 Modified by "admin"	

Note: You cannot configure two devices(FTD) in one single policy

LinkedIn: <https://www.linkedin.com/in/itspulkitsehgal/>

Step 7: Give a static route towards the ISP (WAN router)

Device> Device management> Select the FTD> Edit> Routing> Static Routing> Add route> Interface> Allow any IP> Give Gateway> ok



Save and deploy

Step 8: Check the connectivity from the FTD

FTD to PC

```
QEMU (FirePower1)
05 <48> 3d 00 f0 ff ff 0f 87 cb 00 00 00 41 89 c5 85 c0 0f 85 d8 00 00
[ 878.702748] RSP: 002b:00007ffcf004e140 EFLAGS: 00000246 ORIG_RAX: 000000000000
00038
[ 878.705929] RAX: ffffffff000000000000 RBX: 00007f4264679b000 RCX: 00007f4264672f81
[ 878.708508] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000120001
[ 878.711199] RBP: 0000000000000000 R08: 0000000000000000 R09: 00007f426476d586
[ 878.713663] R10: 00007f426476d850 R11: 0000000000000246 R12: 0000000000000000
[ 878.716472] R13: 00007ffcf004e290 R14: 00005634b34643e8 R15: 0000000000000000
[ 997.244390] hrtimer: interrupt took 5812842 ns

>
>
> ping 192.168.10.5
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/30 ms
>
> ping 1.1.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/40 ms
>
```

FTD to FTD

```
QEMU (FirePower1)
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/40 ms
> ping 2.2.2.10
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 2.2.2.10, timeout is 2 seconds:
!!!!!
Success rate is 0 percent (0/5)
> ping 2.2.2.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/40 ms
>
> ping 2.2.2.10
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 2.2.2.10, timeout is 2 seconds:
!!!!!
Success rate is 0 percent (0/5)
> ping 2.2.2.10
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 2.2.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/20 ms

QEMU (FirePower2)
> ping 2.2.2.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/40 ms
> ping 1.1.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/20 ms
-> ping 172.16.10.6
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 172.16.10.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/30 ms
-> ping 1.1.1.10
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 1.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/30 ms
>
```

Step 9: Configure the Site to Site VPN

Device > VPN > Site to Site > Firepower threat defence device

Policy based (Crypto MAP) > Point to Point > IKEv1

Create New VPN Topology

Topology Name: * FTD_1FTD_2

Policy Based (Crypto Map) Route Based (VTI)

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: * IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Endpoints > Add node 1 > Choose Device > Choose interface > Choose IP address

New Network Object

Name LAN_Subnet

Description

Network Host Range Network FQDN 192.168.10.0/24

Allow Overrides

Cancel Save OK

Network Objects

Available Networks	+
<input type="text"/> Search	
LAN_Subnet	Add
any	
any-ipv4	
any-ipv6	
IPv4-Benchmark-Tests	
IPv4-Link-Local	

Selected Networks

LAN_Subnet	
------------	--

Cancel OK

Add Endpoint

Device:*****
FTD1

Interface:*****
Outside1

IP Address:*****
1.1.1.10

This IP is Private

Connection Type:
Bidirectional

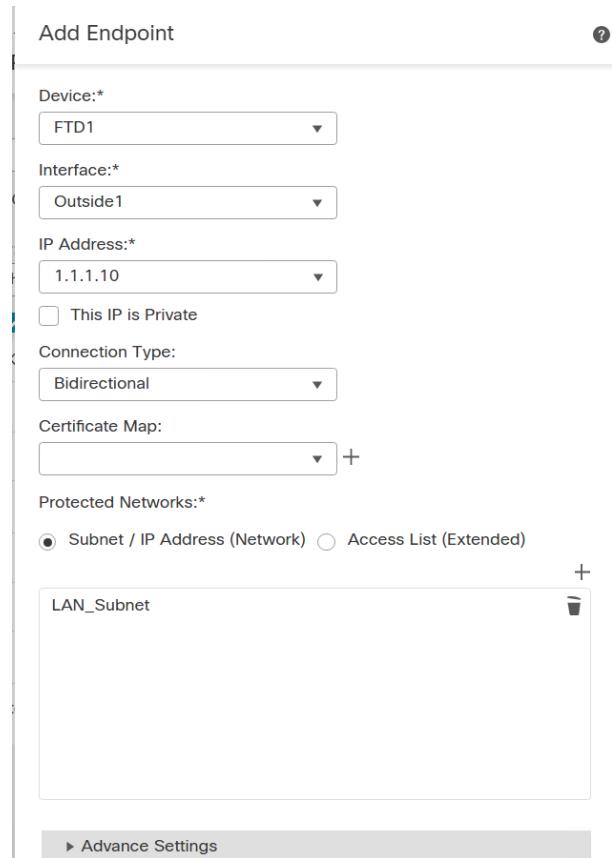
Certificate Map:
+

Protected Networks:*****

Subnet / IP Address (Network) Access List (Extended)

LAN_Subnet
+

▶ Advance Settings



Endpoints> Add node 2> Choose Device> Choose interface> Choose IP address

Add Endpoint

Device:*****
FTD2

Interface:*****
Outside2

IP Address:*****
2.2.2.10

This IP is Private

Connection Type:
Bidirectional

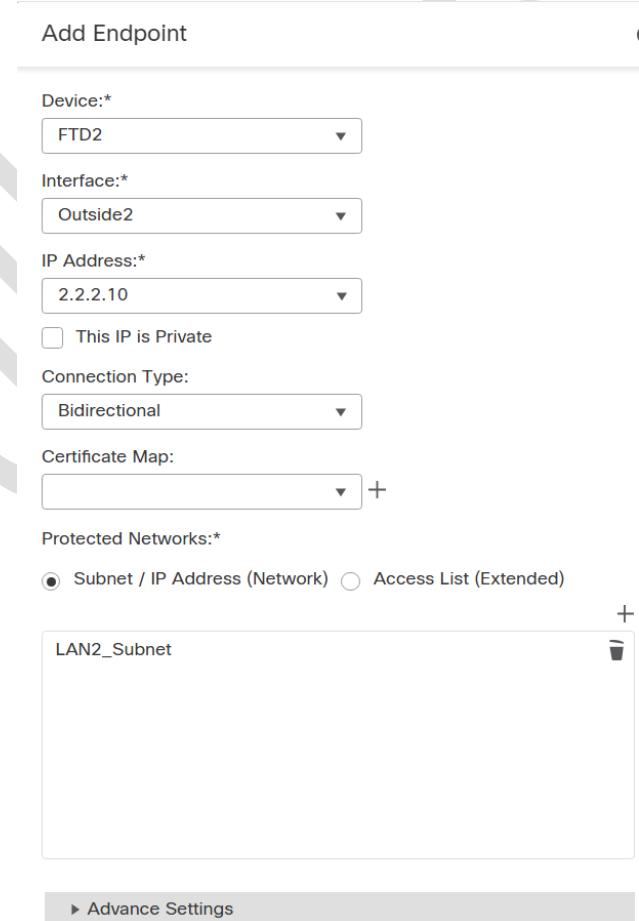
Certificate Map:
+

Protected Networks:*****

Subnet / IP Address (Network) Access List (Extended)

LAN2_Subnet
+

▶ Advance Settings



IKE> preshared_sha_des_dh14_4> Pre-shared Manual Key> Cisc0123

The screenshot shows the IKE configuration page. The top navigation bar has tabs for Endpoints, IKE, IPsec, and Advanced. The IKE tab is selected. Under IKEv1 Settings, the Policies dropdown is set to "preshared_sha_des_dh14_4". The Authentication Type is "Pre-shared Manual Key", and the Key and Confirm Key fields both contain ".....". Under IKEv2 Settings, the Policies dropdown is set to "DES-SHA-SHA-LATEST". At the bottom right are "Cancel" and "Save" buttons.

IPsec> Static

The screenshot shows the IPsec configuration page. The top navigation bar has tabs for Endpoints, IKE, IPsec, and Advanced. The IPsec tab is selected. Under Crypto Map Type, the "Static" radio button is selected. The IKEv2 Mode is set to "Tunnel". Under Transform Sets, there are two entries: "tunnel_des_sha" and "DES_SHA-1". Below these are three checkboxes: "Enable Security Association (SA) Strength Enforcement" (unchecked), "Enable Reverse Route Injection" (checked), and "Enable Perfect Forward Secrecy" (unchecked). The Modulus Group dropdown is set to "14".

IKEv1 and IKEv2 are the option to choose what do we want to configure as a policy

Note: Without License, FMC will not allow us to work with the default policy

The screenshot shows the "Create New VPN Topology" dialog. The Topology Name is "FTD_1FTD_2". The Policy Based (Crypto Map) radio button is selected. The Network Topology is "Point to Point". The IKE Version is set to "IKEv1" (checked) and "IKEv2" (unchecked). The top navigation bar has tabs for Endpoints, IKE, IPsec, and Advanced. Under Node A, there is a table with one row: Device Name "FTD1", VPN Interface "Outside1/1.1.1.10", and Protected Networks "LAN_Subnet". Under Node B, there is a table with one row: Device Name "FTD2", VPN Interface "Outside2/2.2.2.10", and Protected Networks "LAN2_Subnet". A note at the bottom says "Ensure the protected networks are allowed by access control policy of each device." At the bottom right are "Cancel" and "Save" buttons.

Save and deploy

LinkedIn: <https://www.linkedin.com/in/itspulkitsehgal/>

Step 10: Create a policy

Policies > Access control > Choose FTD > Add rule > Zones

Add Rule

Name: FTD1_Tunnel Enabled: Insert: into Mandatory

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Zones: Inside, outside

Source Zones (2): Inside, outside

Destination Zones (2): outside, Inside

Cancel Add

Networks >

Add Rule

Name: FTD1_Tunnel Enabled: Insert: into Mandatory

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Networks: LAN, LAN2_Subnet

Source Networks (2): LAN_Subnet, LAN2_Subnet

Destination Networks (2): LAN2_Subnet, LAN_Subnet

Enter an IP address Add

Cancel Add

Logging >

Add Rule

Name: FTD1_Tunnel Insert: into Mandatory

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Firepower Management Center
 Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)
 SNMP Trap Select an SNMP Alert Configuration +

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts [Add Category](#) [Add Rule](#)

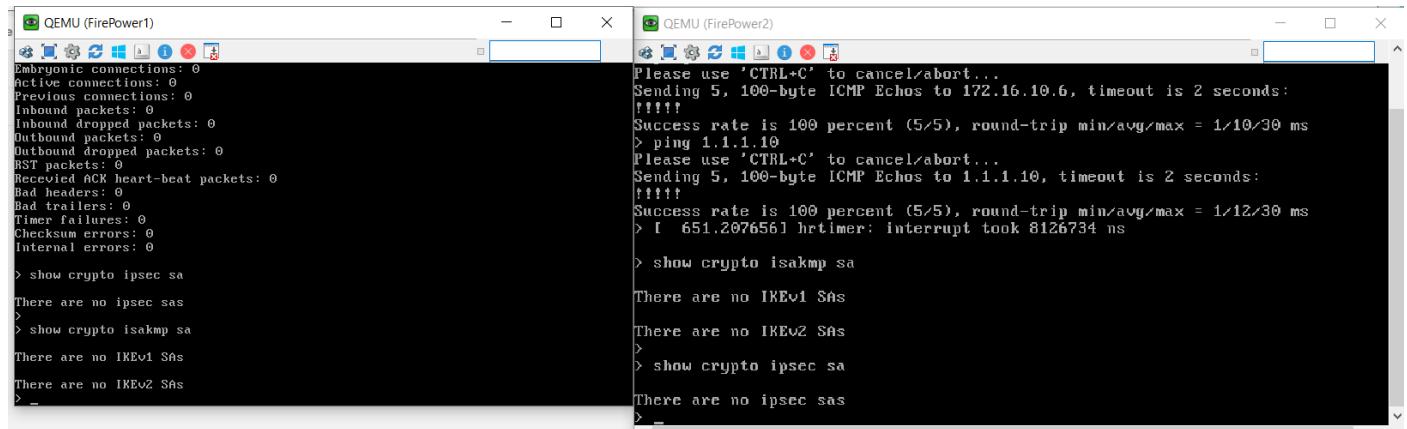
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat...	Action								
1	FTD1_Tunnel	Inside	outside	LAN_Subnet	LAN2_Subnet	LAN_Subnet	Any	Any	Any	Any	Any	Any	Any	Any	Allow							

There are no rules in this section. [Add Rule](#) or [Add Category](#)

Same apply the policy on FTD 2 also

Step 11: Verify the tunnel and communication

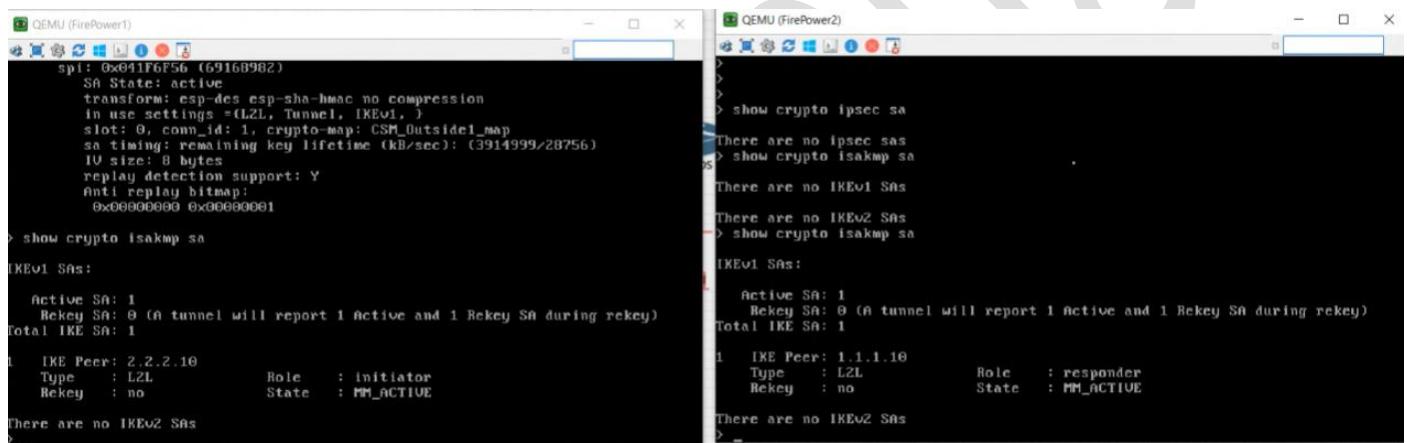
Check on FTD



```
QEMU (FirePower1)
Embryonic connections: 0
active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Received ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
> show crypto ipsec sa
There are no ipsec sas
> show crypto isakmp sa
There are no IKEv1 SAs
There are no IKEv2 SAs
There are no ipsec sas
> =
```

```
QEMU (FirePower2)
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 172.16.10.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/30 ms
> ping 1.1.1.10
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 1.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/30 ms
> [ 651.207656] hrtimer: interrupt took 8126734 ns
> show crypto isakmp sa
There are no IKEv1 SAs
There are no IKEv2 SAs
> show crypto ipsec sa
There are no ipsec sas
> =
```

> show crypto ipsec sa	To display the IPsec
> show crypto isakmp sa	To display the isakmp



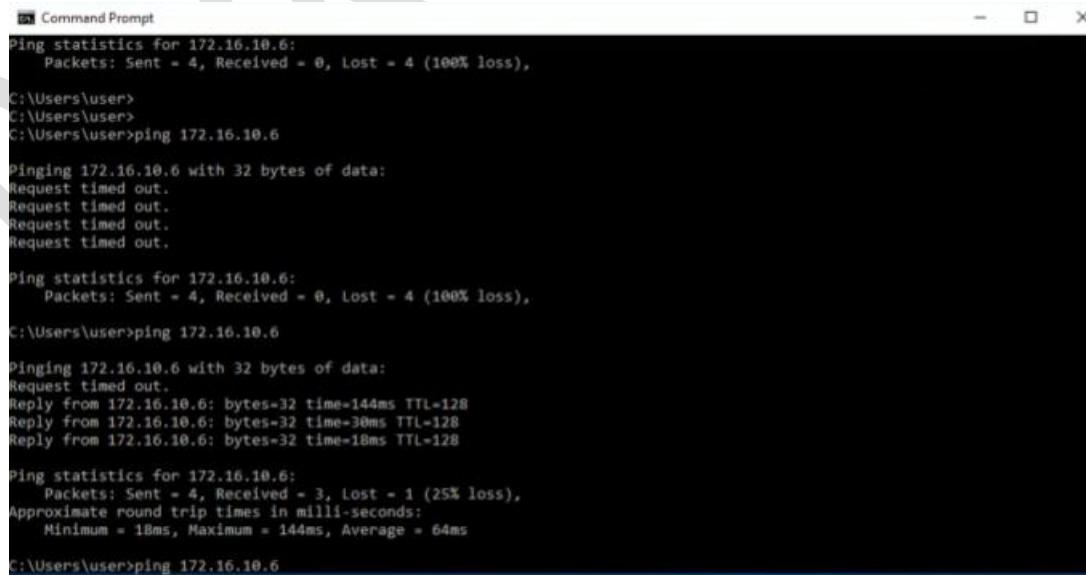
```
QEMU (FirePower1)
spi: 0x041F6F56 (6916B9BZ)
SA State: active
transform: esp-des esp-sha-hmac no compression
in use settings =(L2L, Tunnel, IKEv1, )
slot: 0, conn_id: 1, crypto-map: CSM_Outside1_map
sa timing: remaining key lifetime (kB/sec): (3914999/28756)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

> show crypto isakmp sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 2.2.2.10
Type : L2L          Role : initiator
Rekey : no          State : MM_ACTIVE

There are no IKEv2 SAs
> =
```

```
QEMU (FirePower2)
>
>
> show crypto ipsec sa
There are no ipsec sas
> show crypto isakmp sa
There are no IKEv1 SAs
There are no IKEv2 SAs
> show crypto isakmp sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1 IKE Peer: 1.1.1.10
Type : L2L          Role : responder
Rekey : no          State : MM_ACTIVE

There are no IKEv2 SAs
> =
```



```
Command Prompt
Ping statistics for 172.16.10.6:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\user>
C:\Users\user>
C:\Users\user>ping 172.16.10.6

Pinging 172.16.10.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.10.6:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\user>ping 172.16.10.6

Pinging 172.16.10.6 with 32 bytes of data:
Request timed out.
Reply from 172.16.10.6: bytes=32 time=144ms TTL=128
Reply from 172.16.10.6: bytes=32 time=30ms TTL=128
Reply from 172.16.10.6: bytes=32 time=18ms TTL=128

Ping statistics for 172.16.10.6:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
  Minimum = 18ms, Maximum = 144ms, Average = 64ms
C:\Users\user>ping 172.16.10.6
```