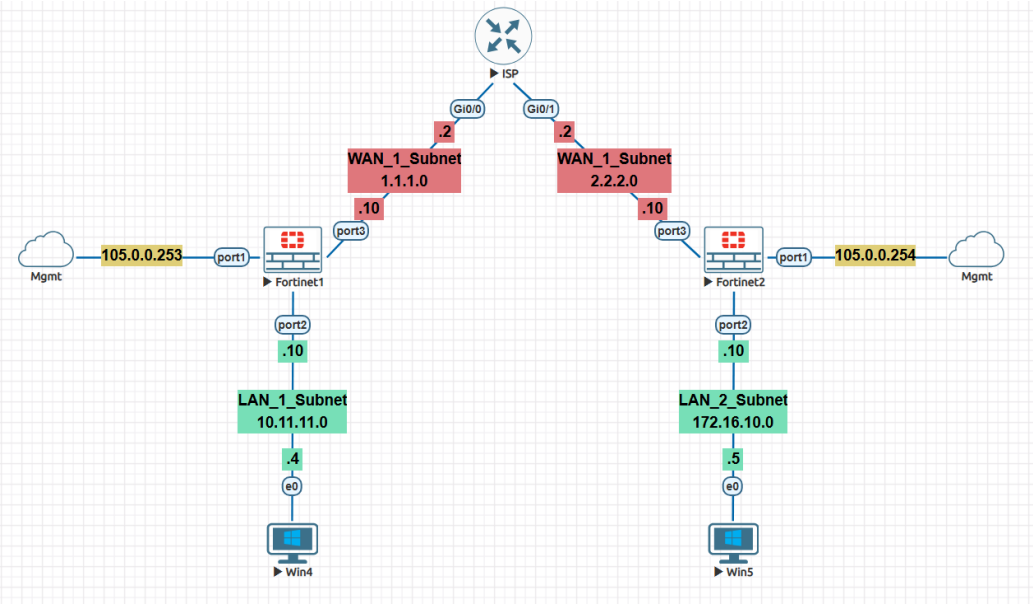
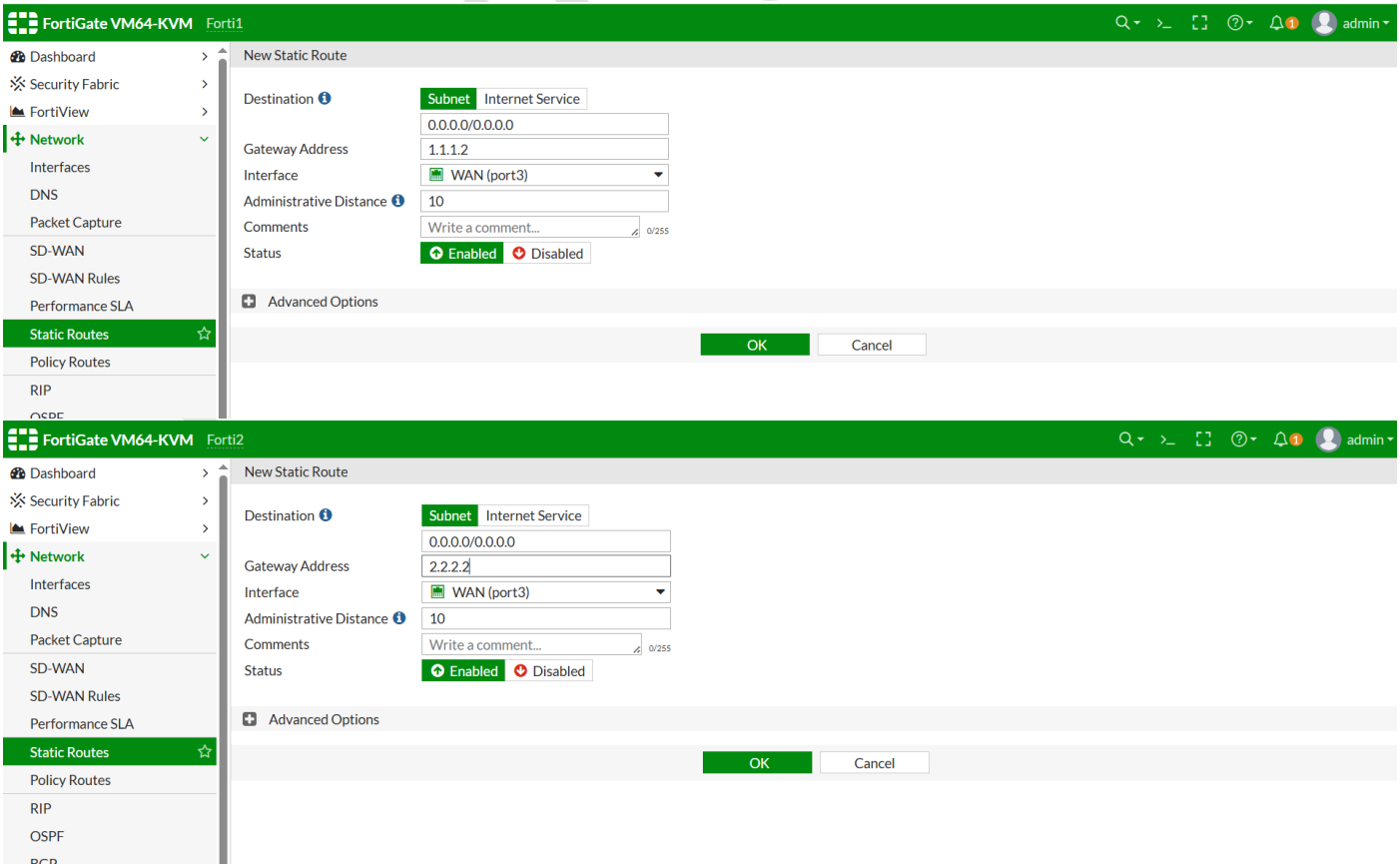
Configuring IPsec Site to Site VPN using different Next Generation Firewalls

Fortigate



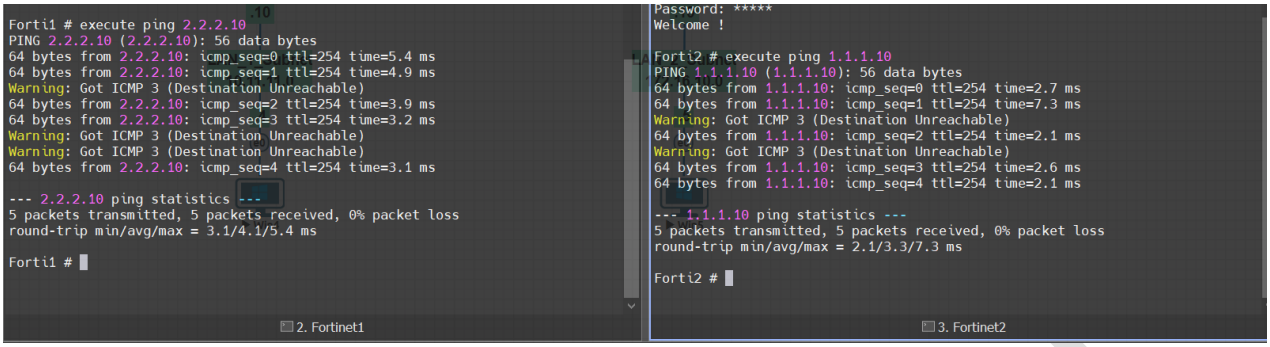
Step 1: Configure the basic topology

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



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

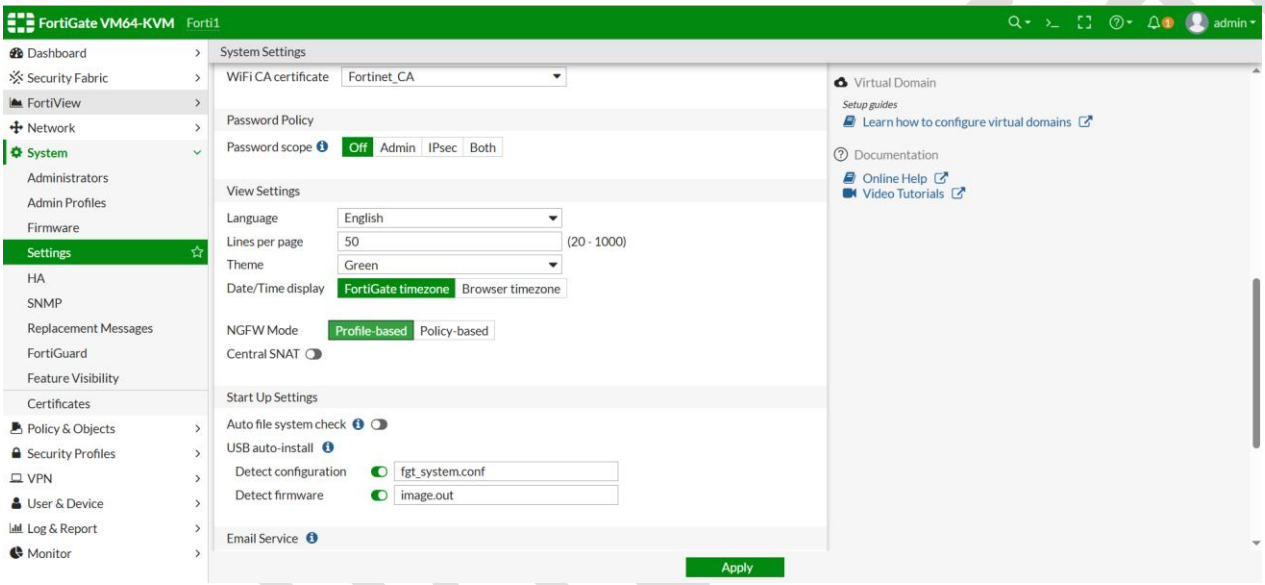
Check the basic connectivity before configuring the site to site VPN



Step 3: Configure Site to Site VPN

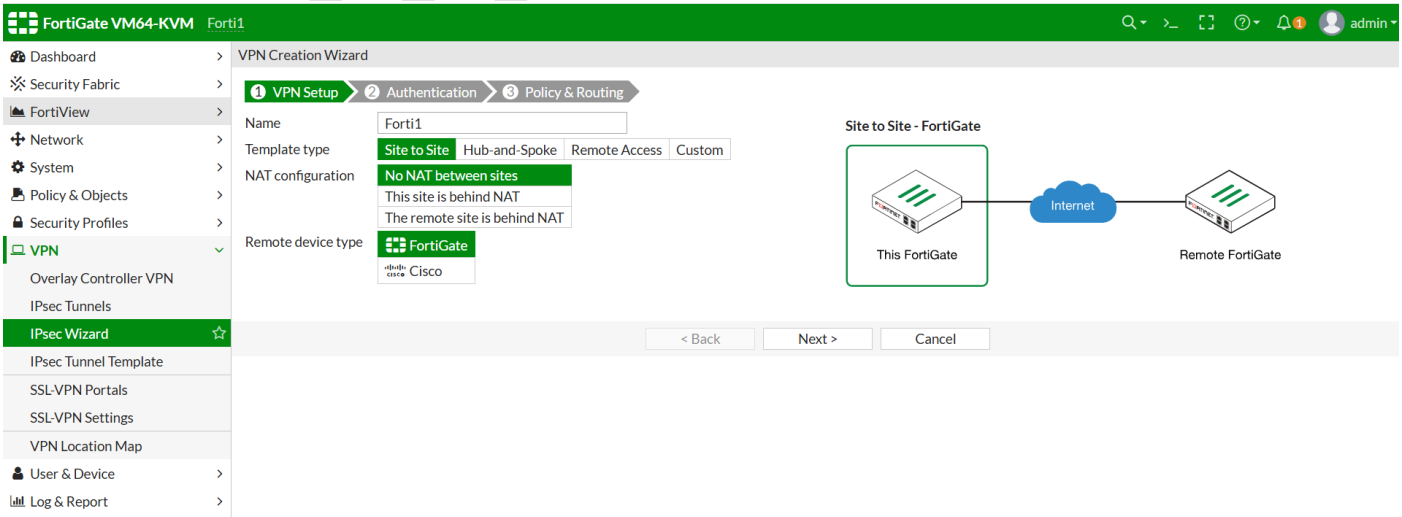
Change the NGFW mode setting from policy based to profile based

System> Settings> NGFW Mode

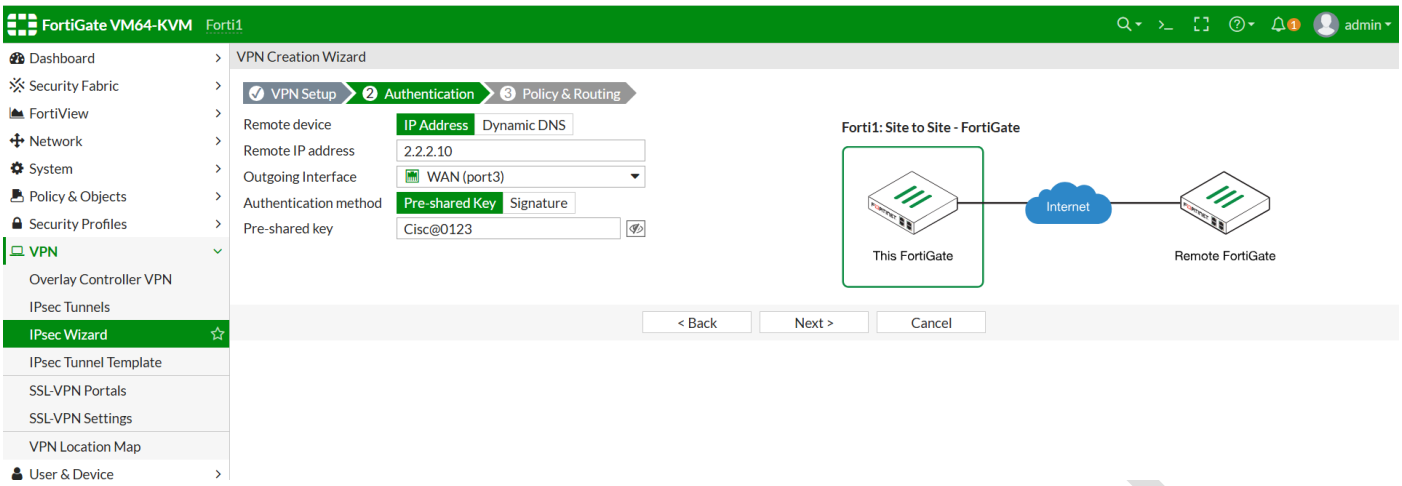


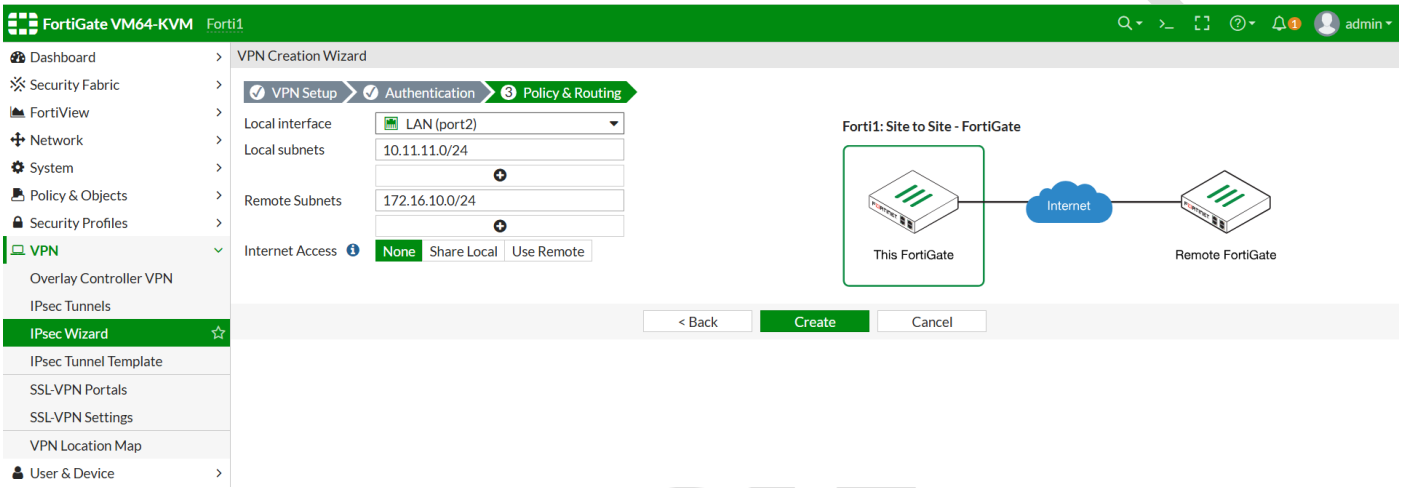
Configure IPsec

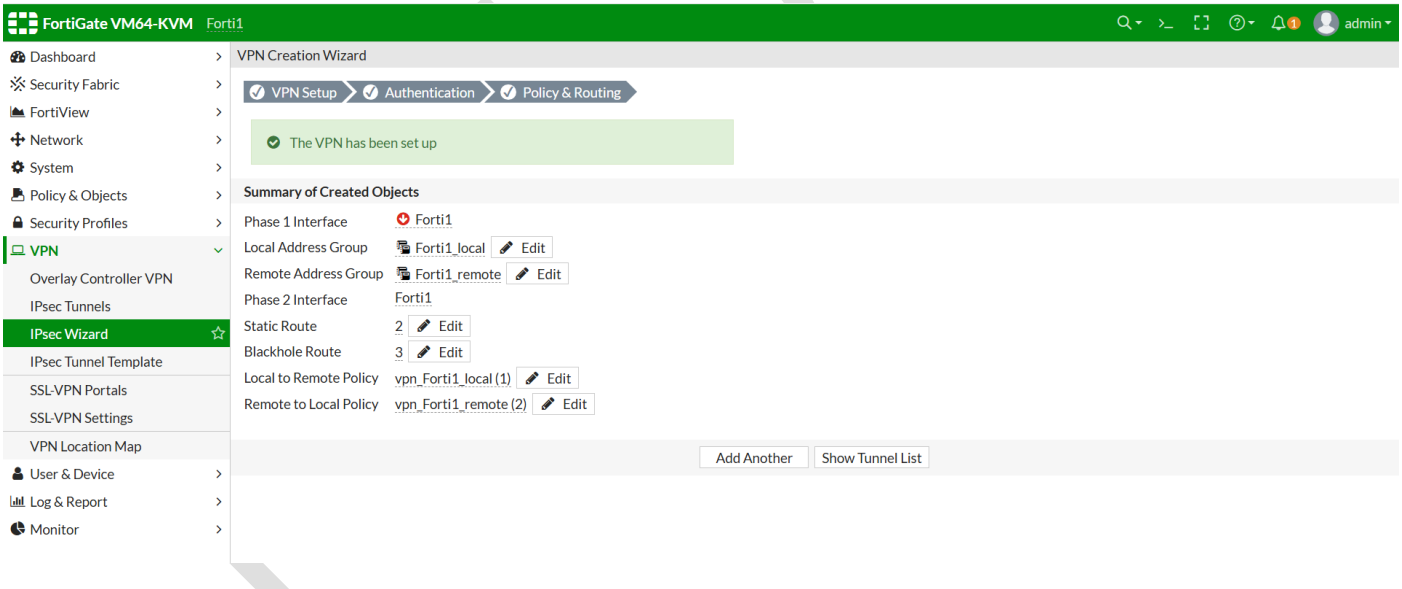
Dashboard> VPN> IPsec Wizard>



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





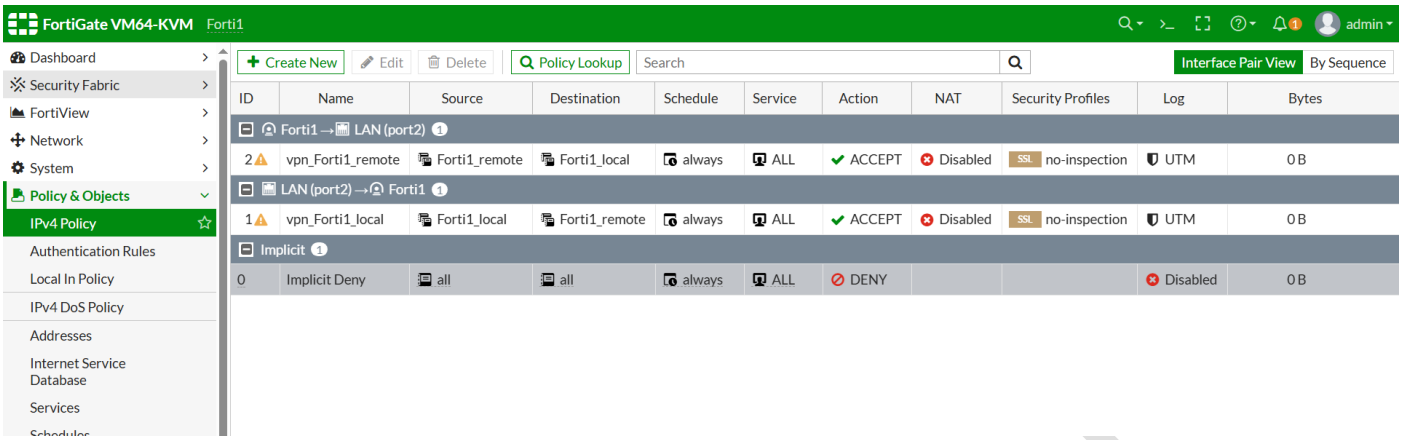


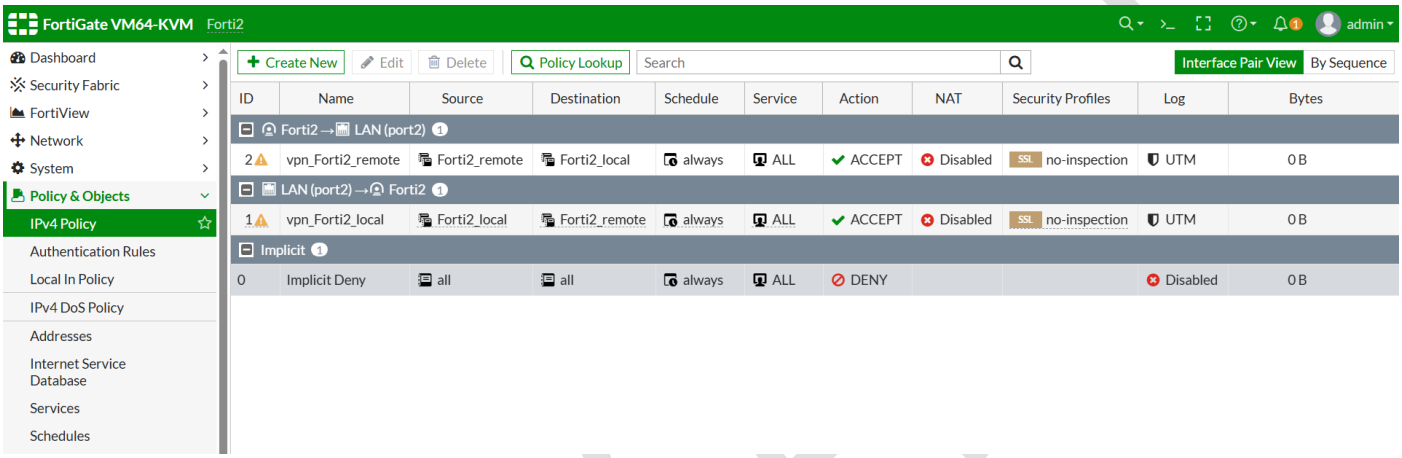
Same way configure the Fortigate2

Step 4: Configure the Policy

Dashboard> Policy & Objects> Ipv4 Policy

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

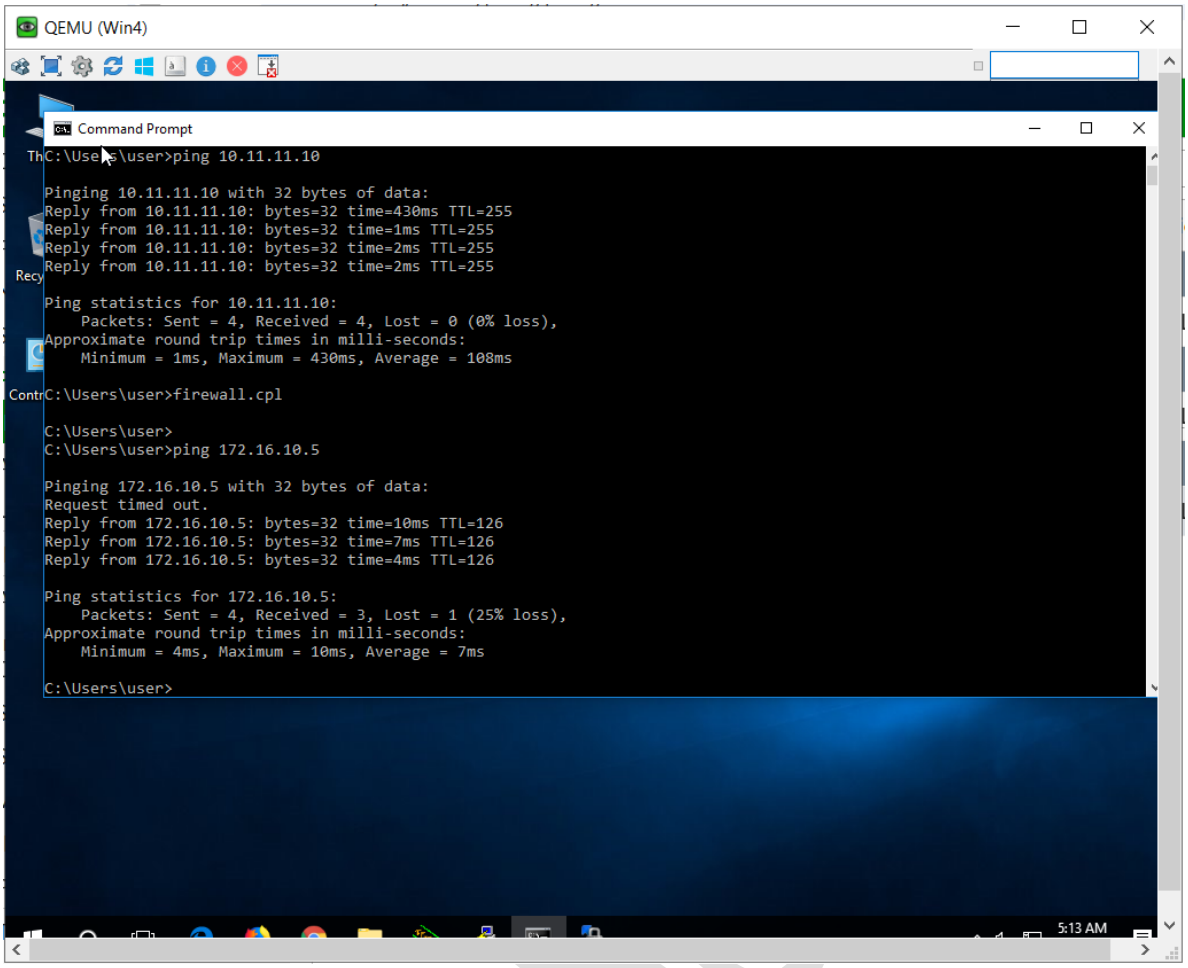




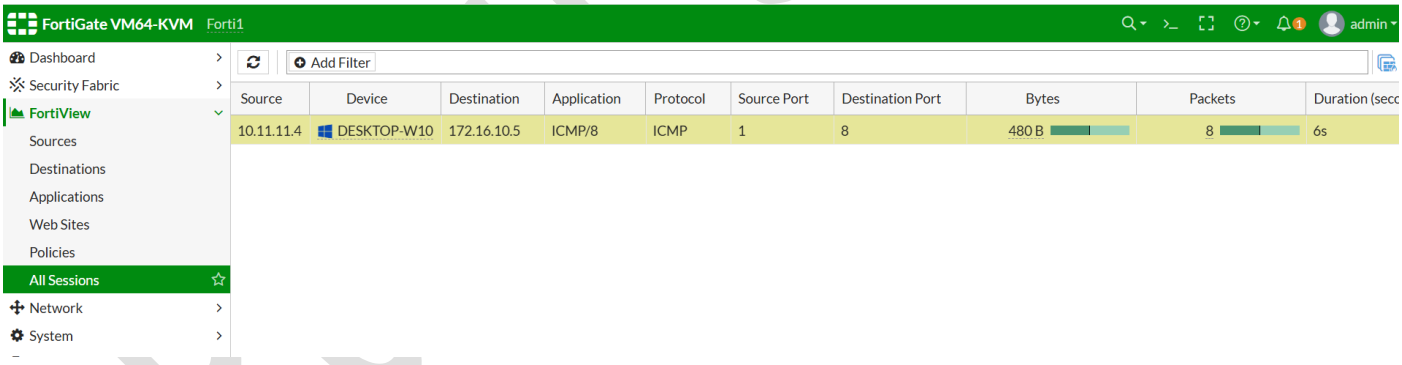
If you will see, automatically tunnel interfaces are created

If you try communicating from LAN 1 to LAN 2

Pulkit Se

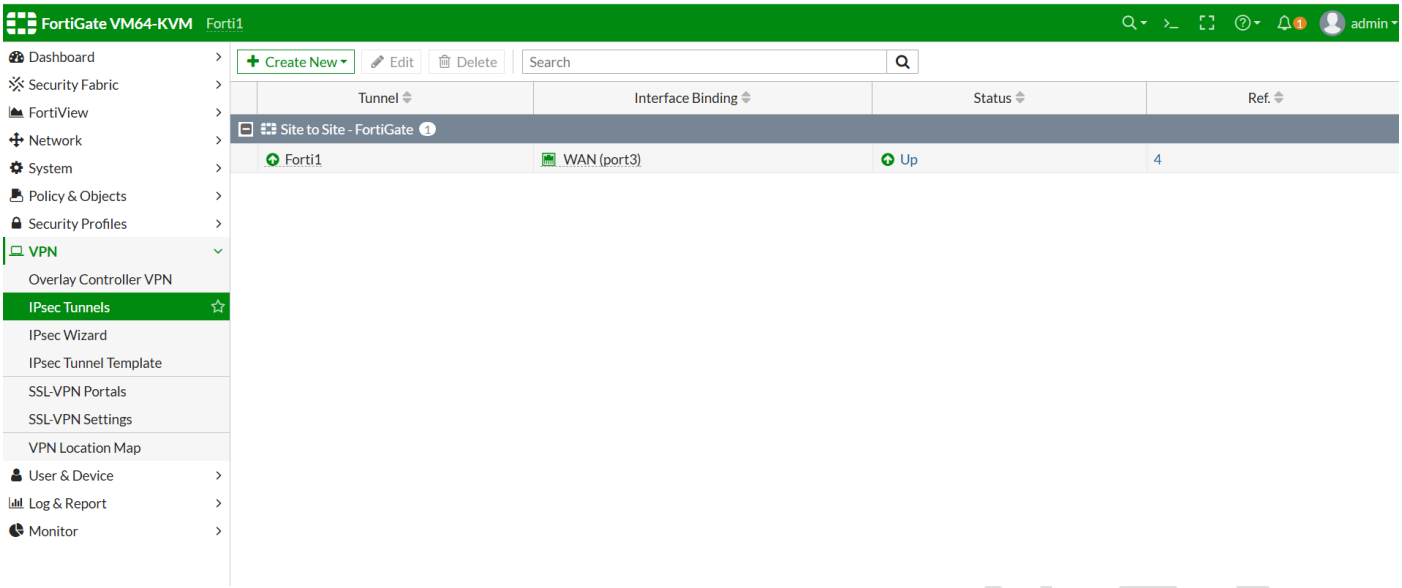


We got the connectivity and now check the logs



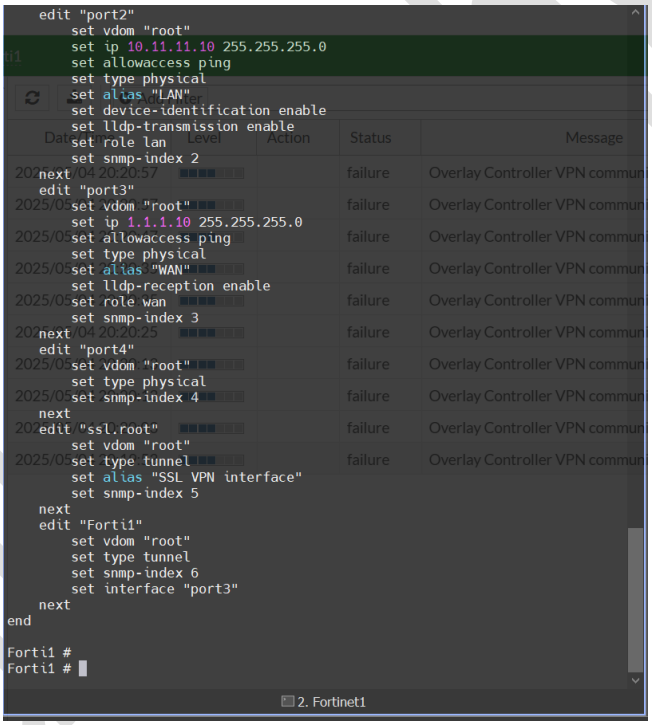
The tunnel status will come up also

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



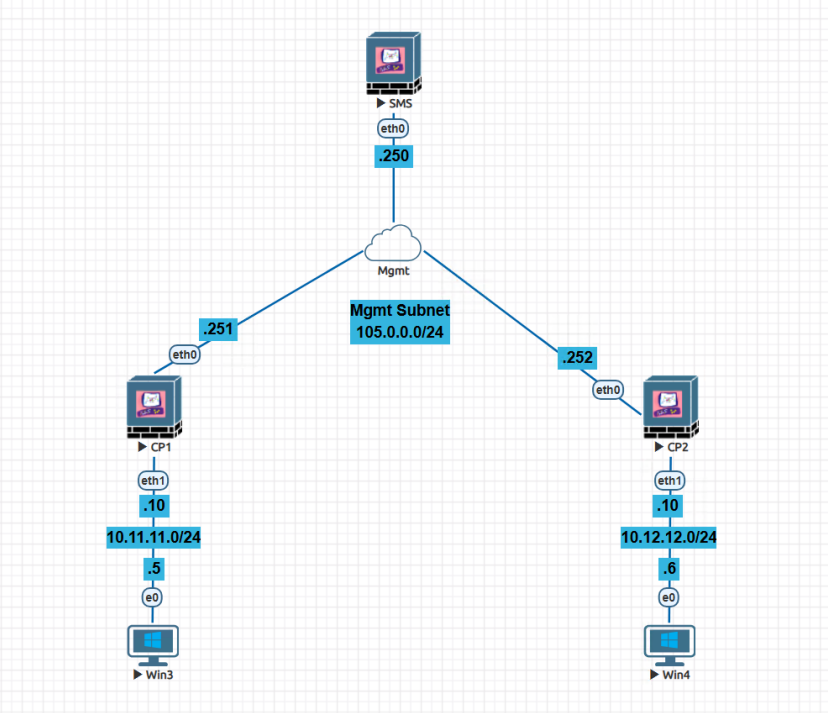
If you will check on the CLI

#show system interface



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

Checkpoint

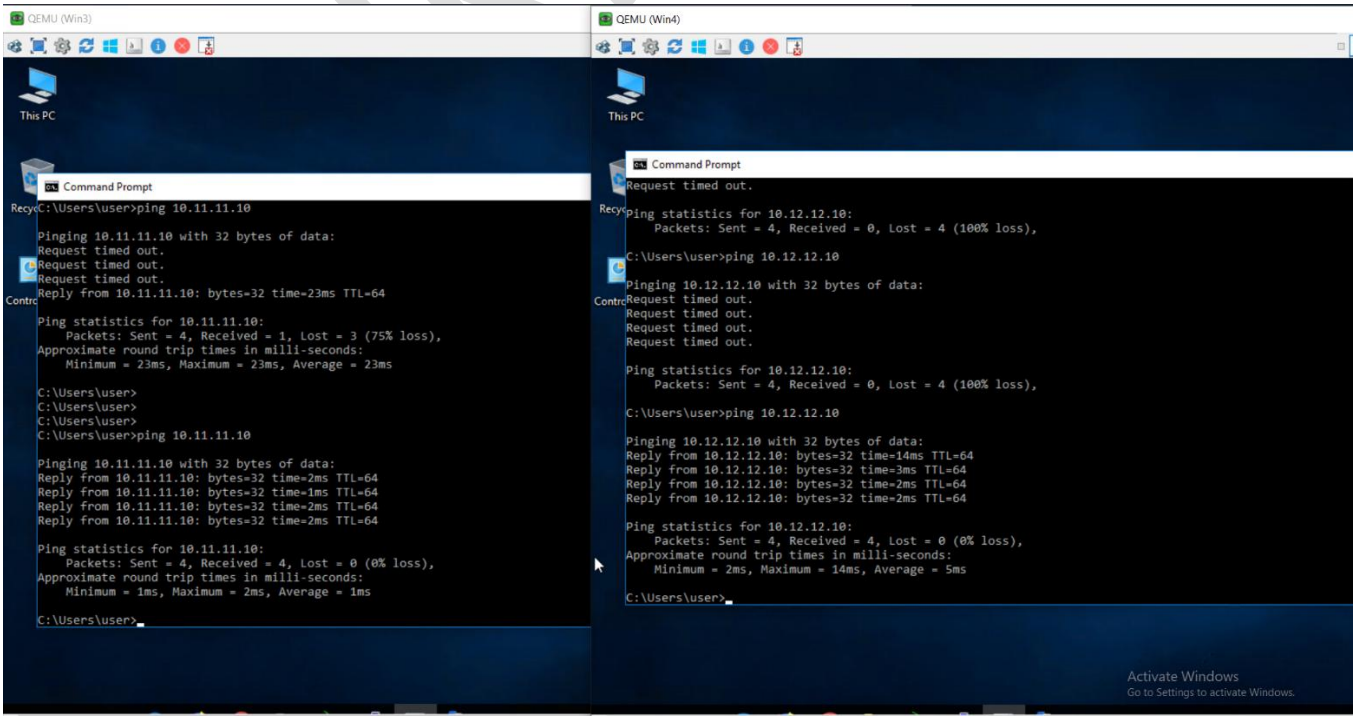


Step 1: Configure the basic topology

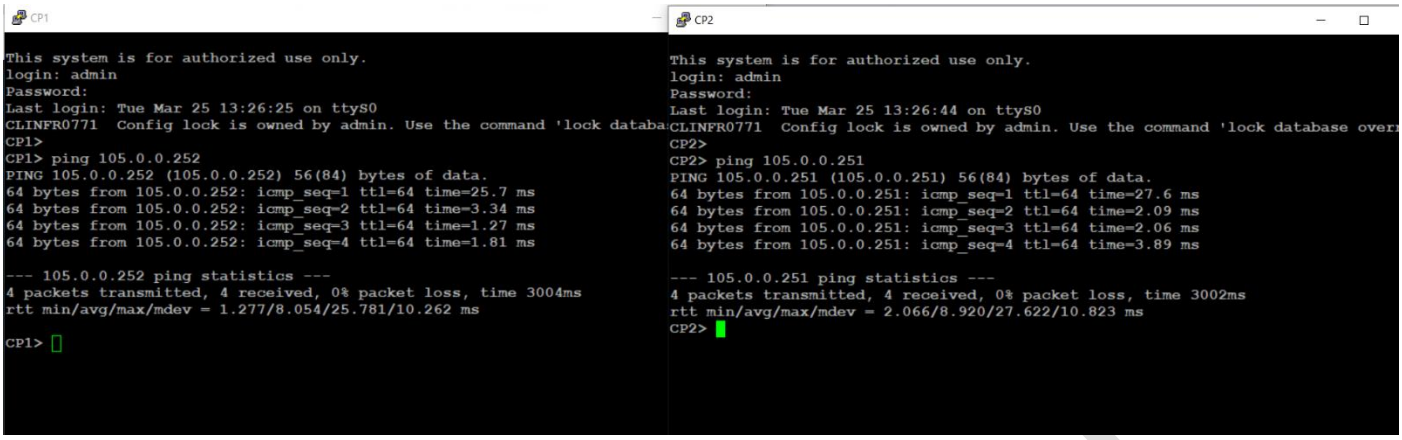
Step 2: Create the policy for management subnet and LAN interfaces

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

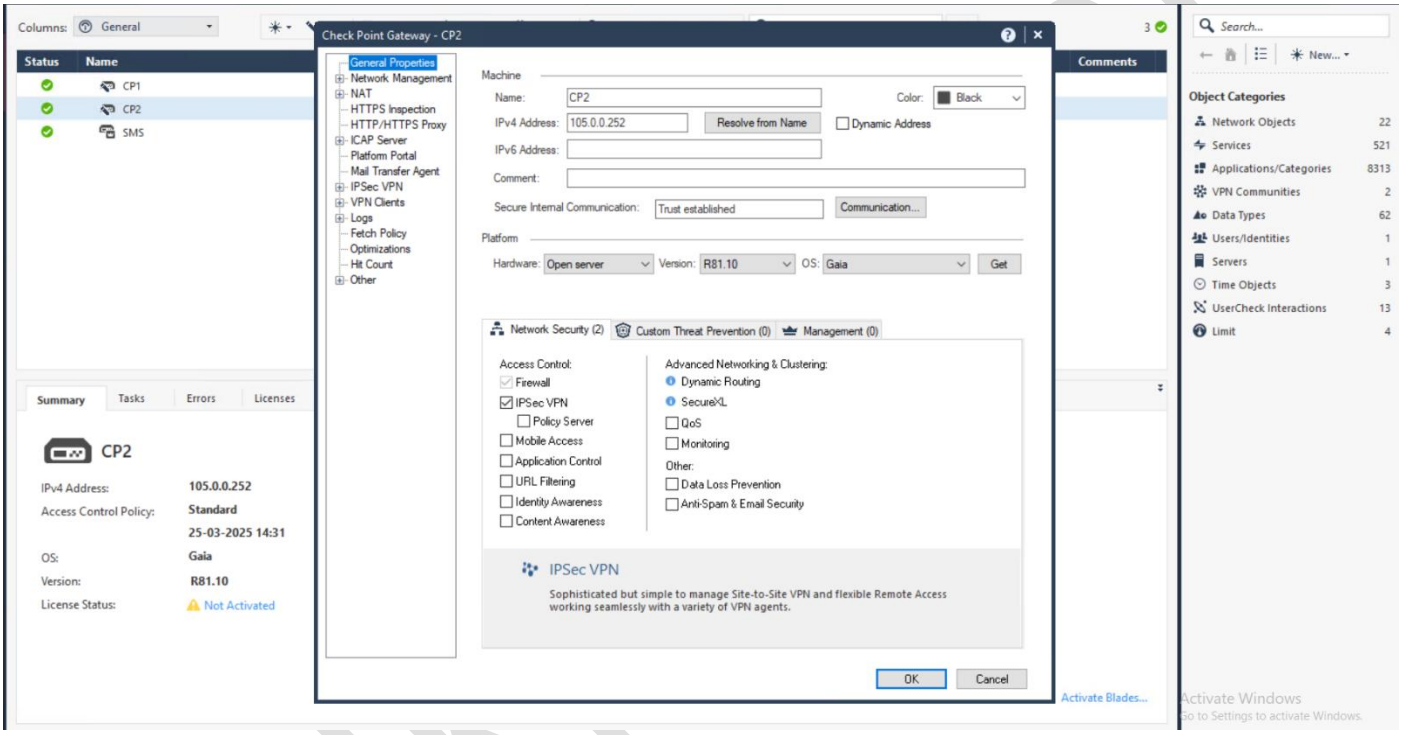
Step 3: Check the connectivity between LAN PCs to respective firewall and CP1 to CP2

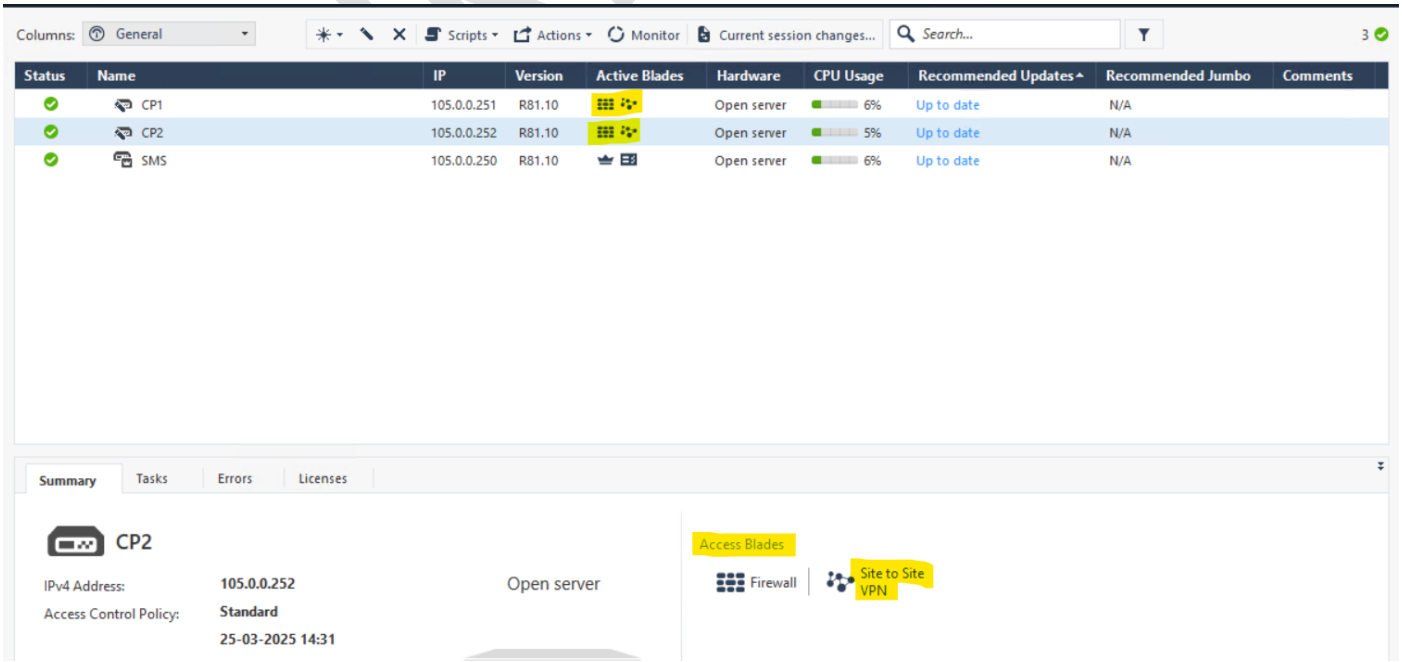


LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/



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

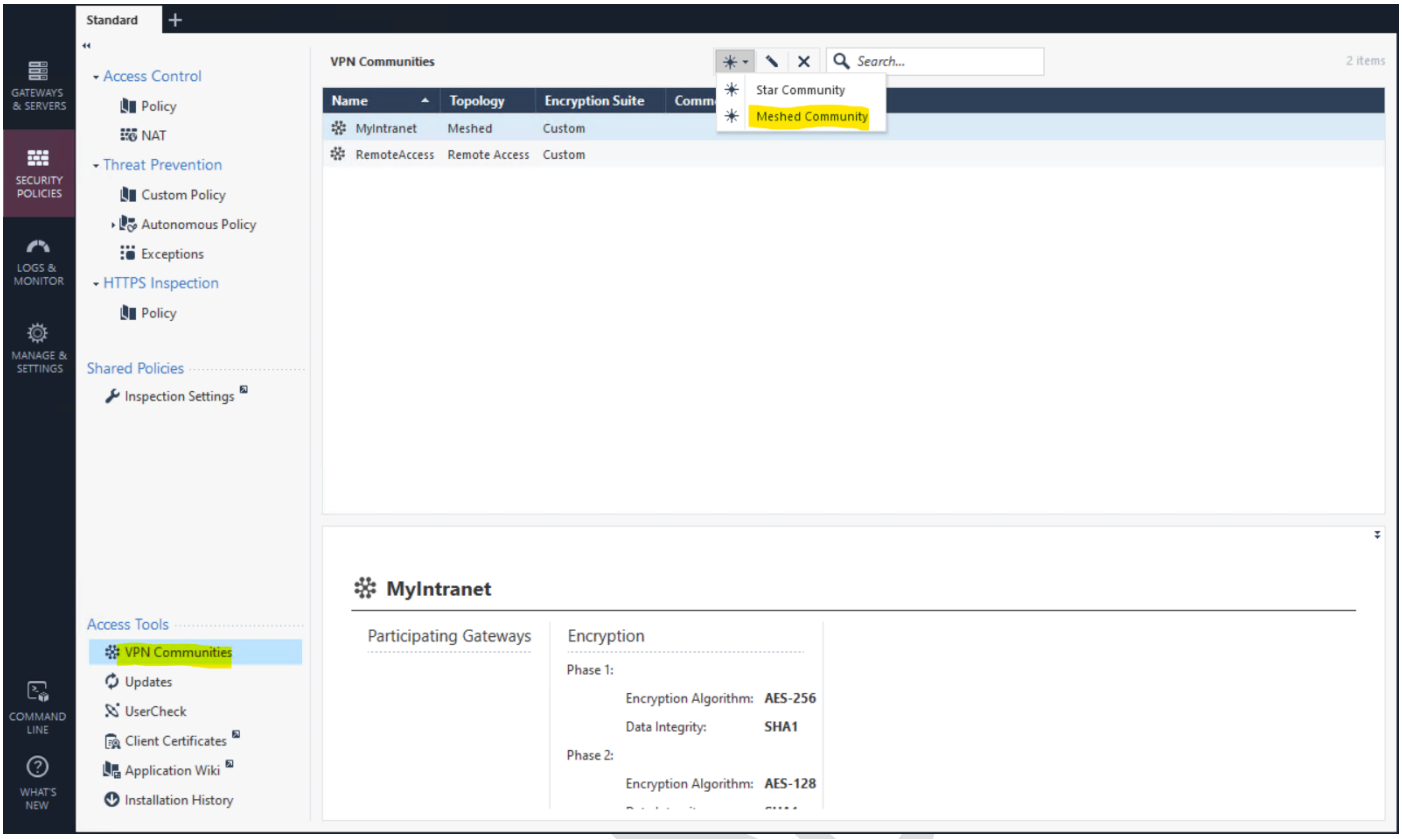




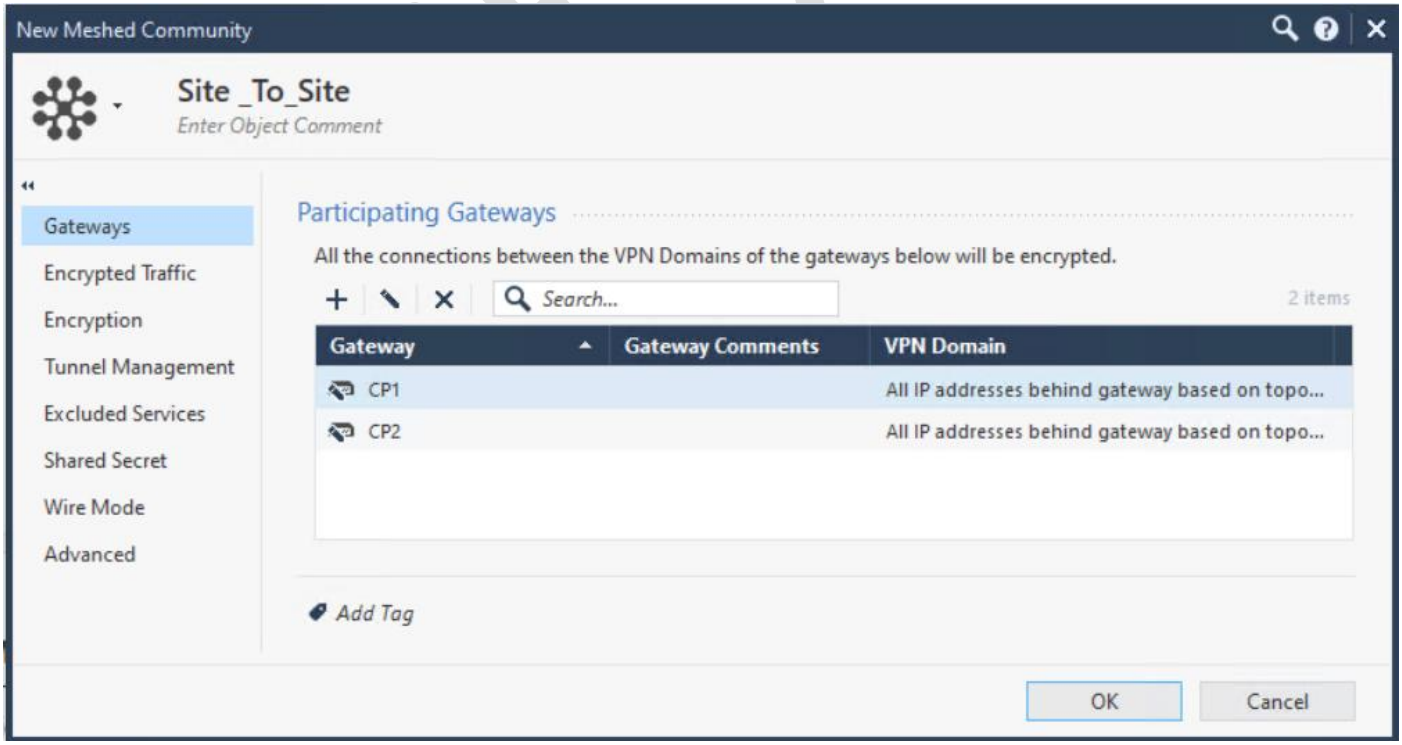
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

Step 5: Configure the IPsec

Security Policies> VPN Communities> New Widget> Meshed Community

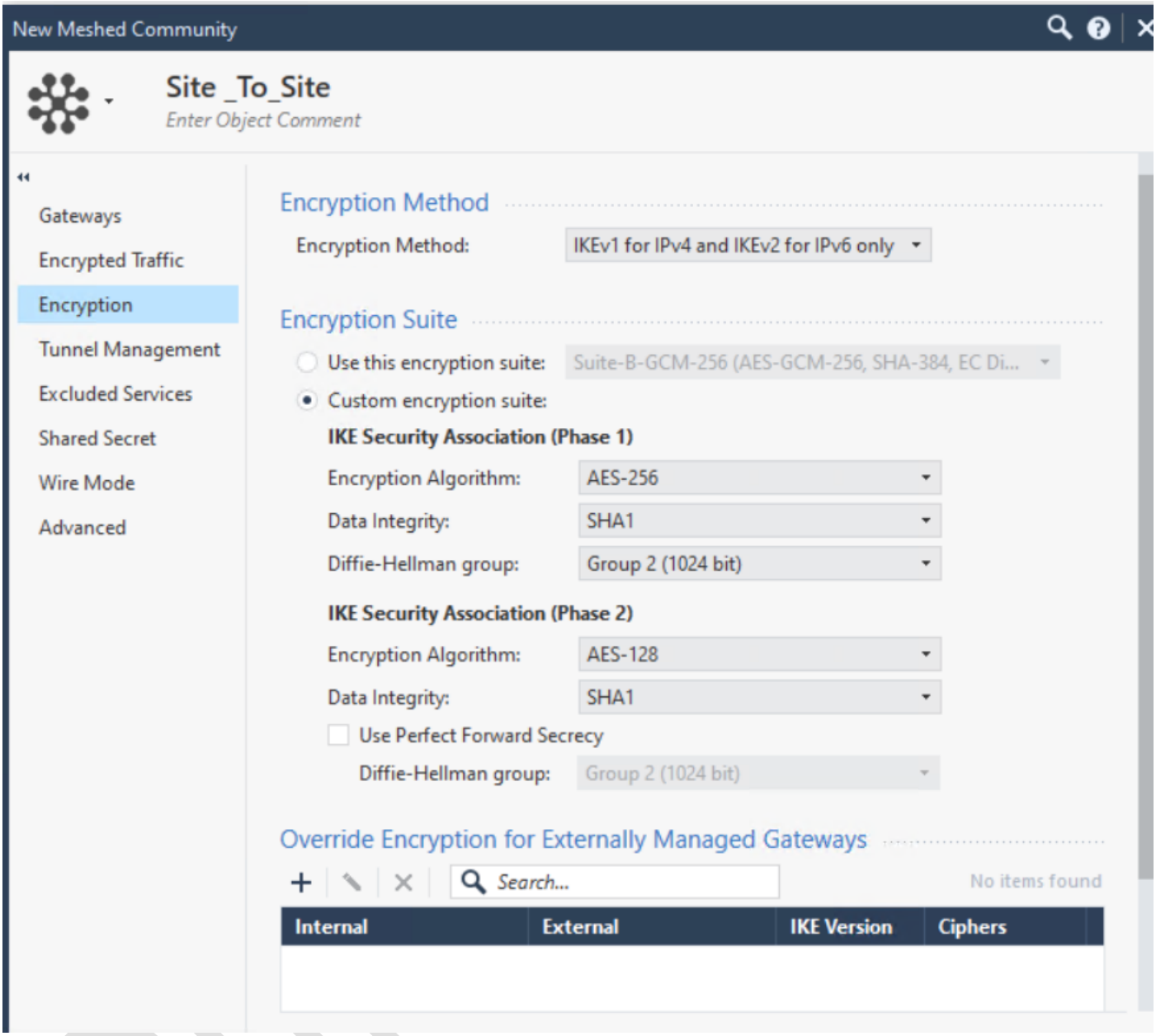


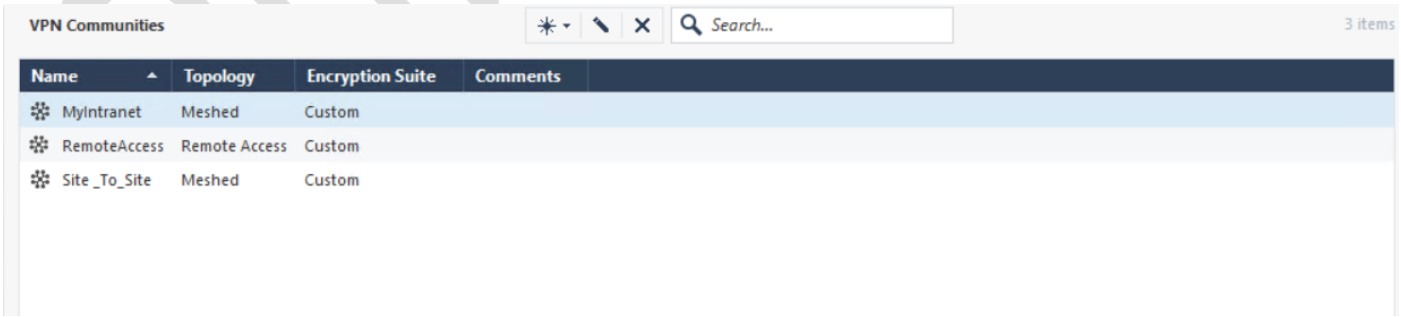
Give name> Add the firewalls



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

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

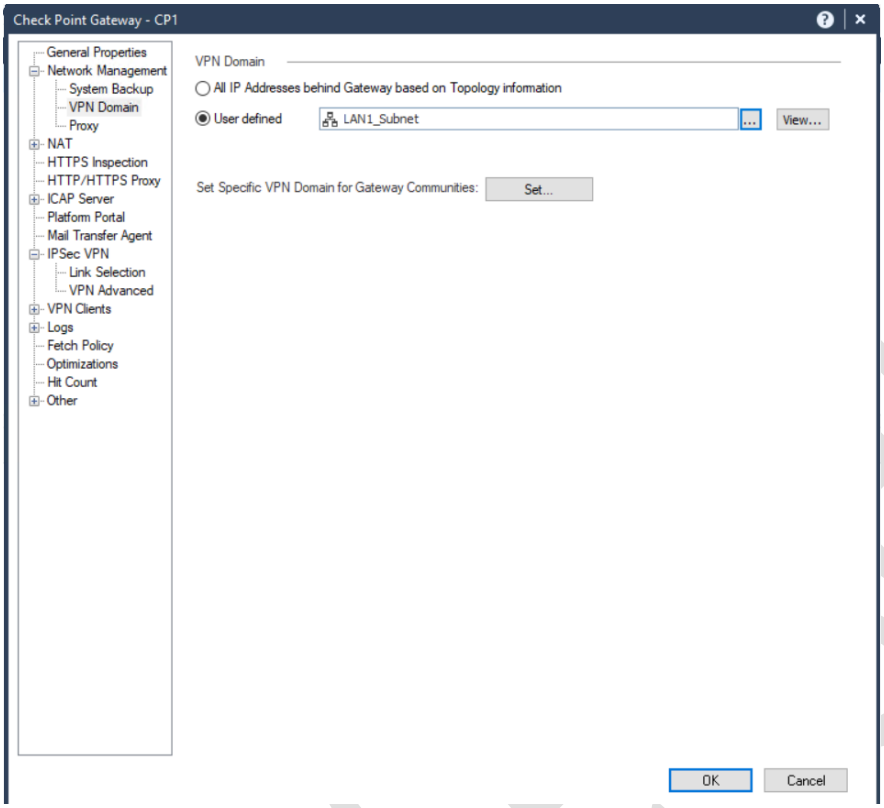




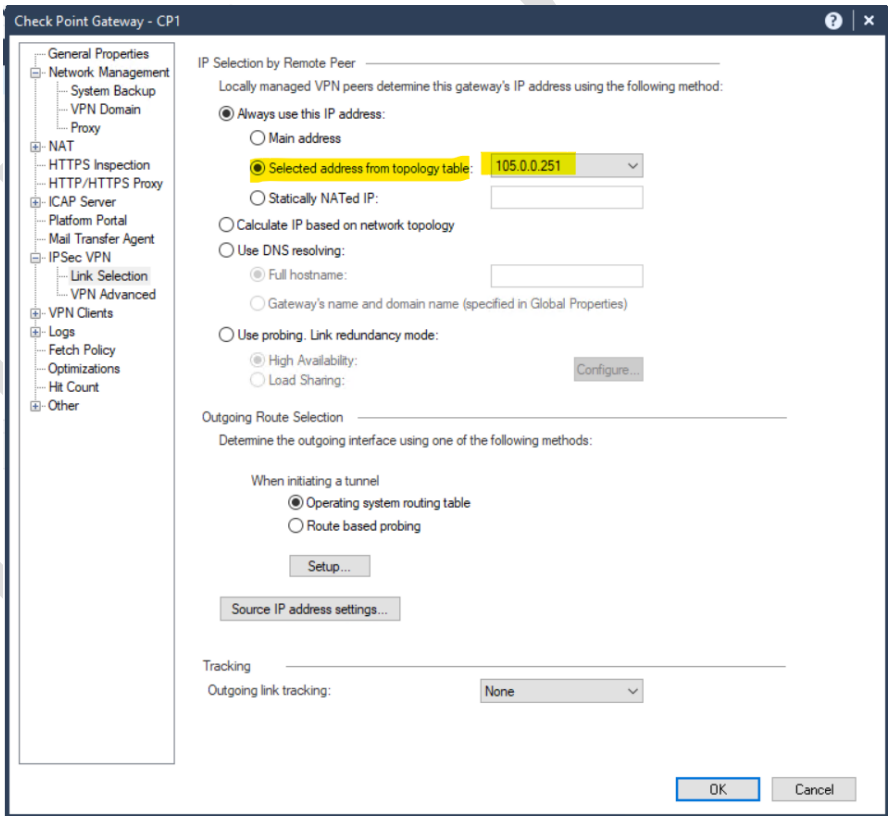
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

Step 6: Assign the IPsec under the firewall

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



IPsec VPN> Link Selection



Repeat this on CP2 also

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

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

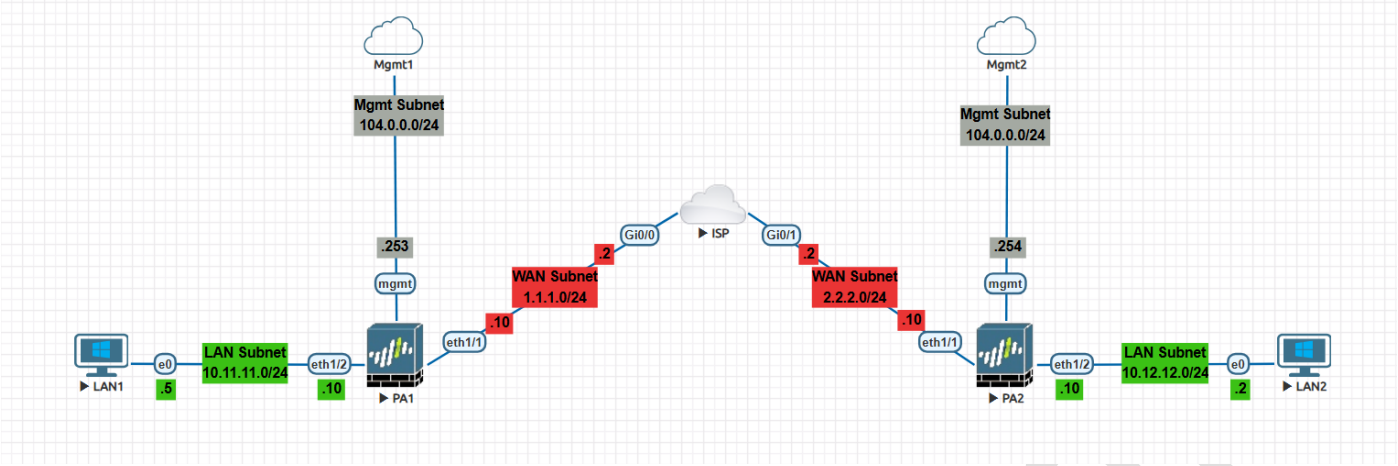
No.	Name	Source	Destination	VPN	Services & Applications	Time
1	Site_to_Site_CP1_CP2	LAN1_Subnet LAN2_Subnet	LAN1_Subnet LAN2_Subnet	Site _To_Site	Any	Any
2	Cleanup rule	Any	Any	Any	Any	Any

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

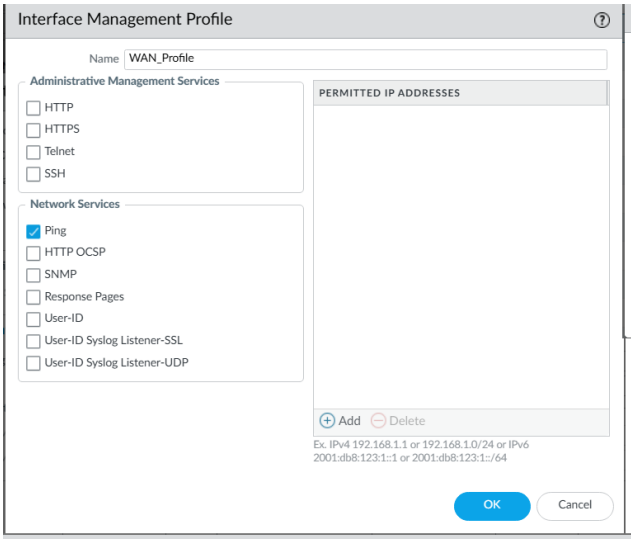
Pulkit Sehgal

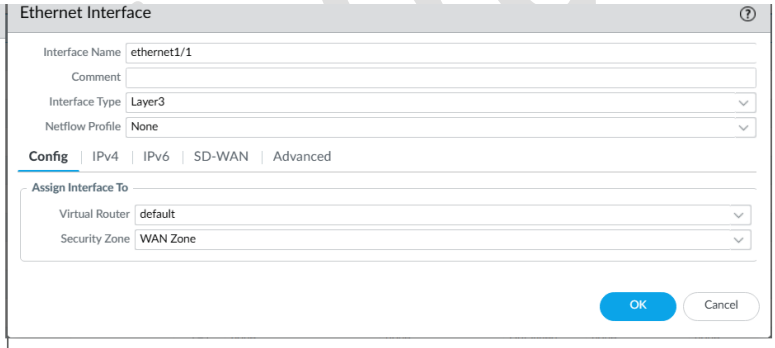
Palo Alto

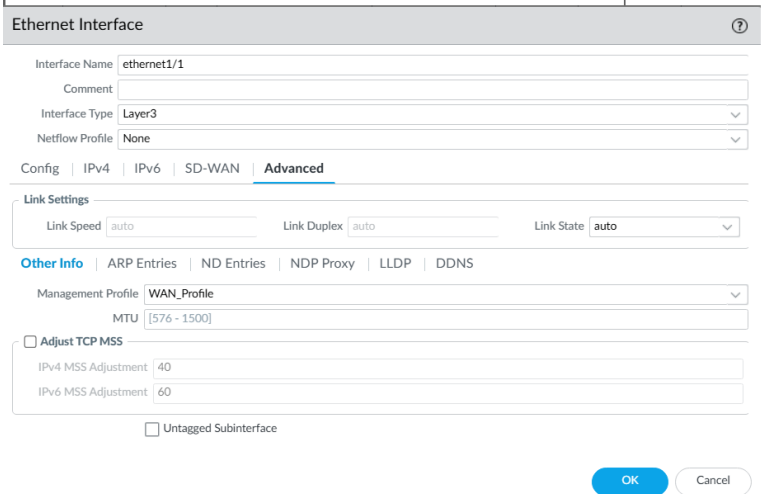


Step 1: Configure the topology

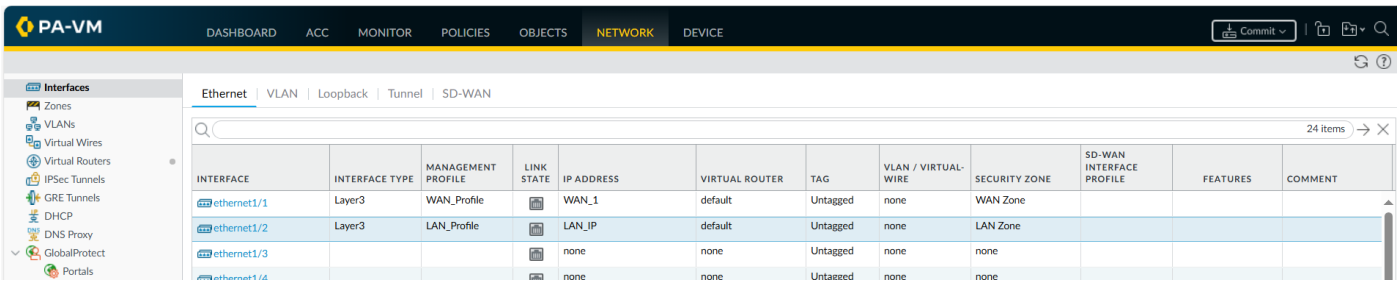
Step 2: Configure the interfaces on Palo Alto





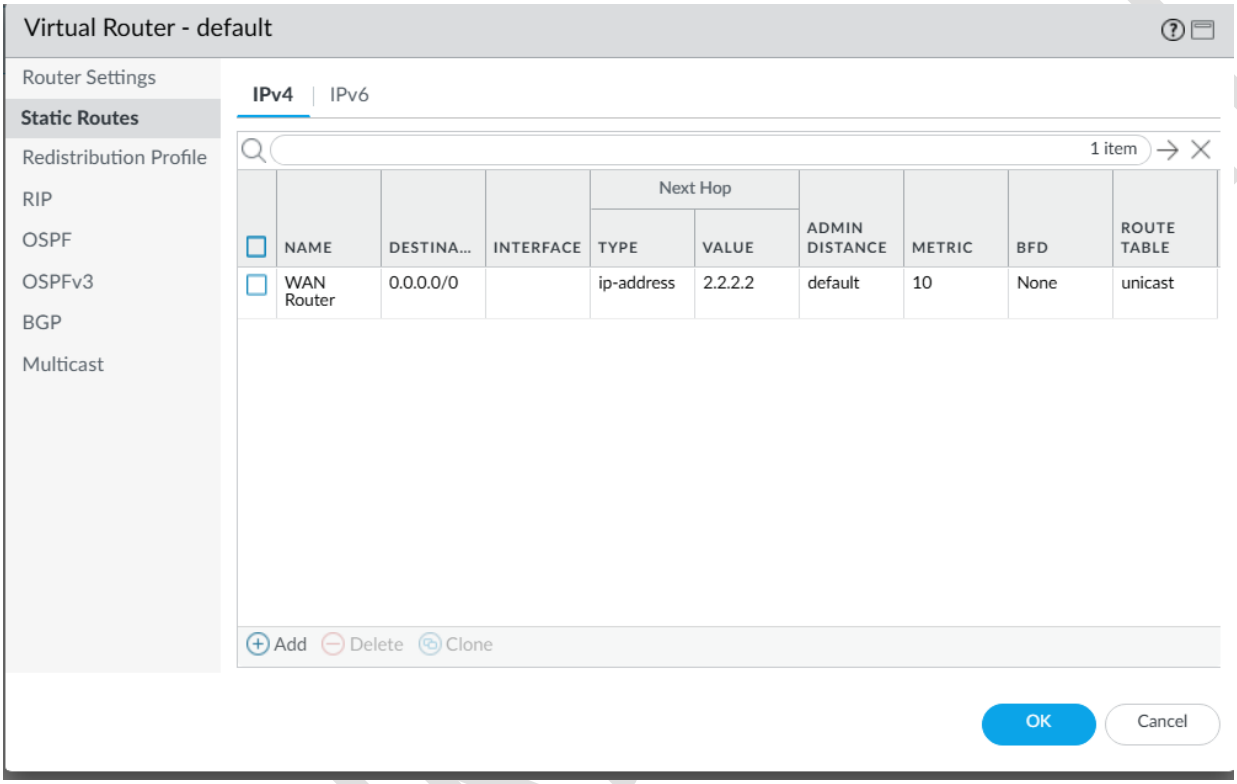


LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

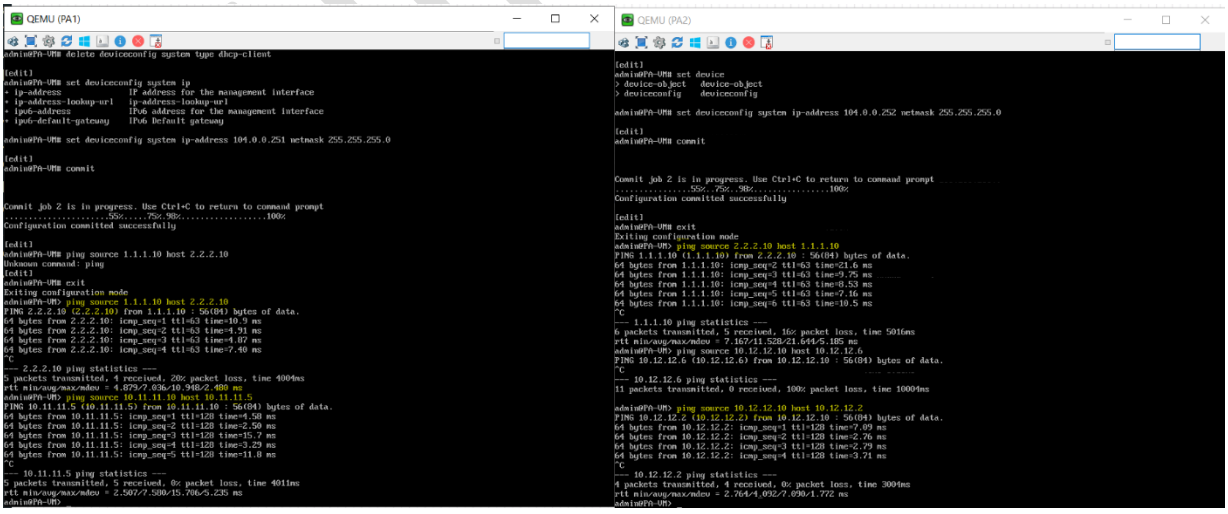


Create a default route towards ISP

Virtual router> Choose the routing table> Static Route>



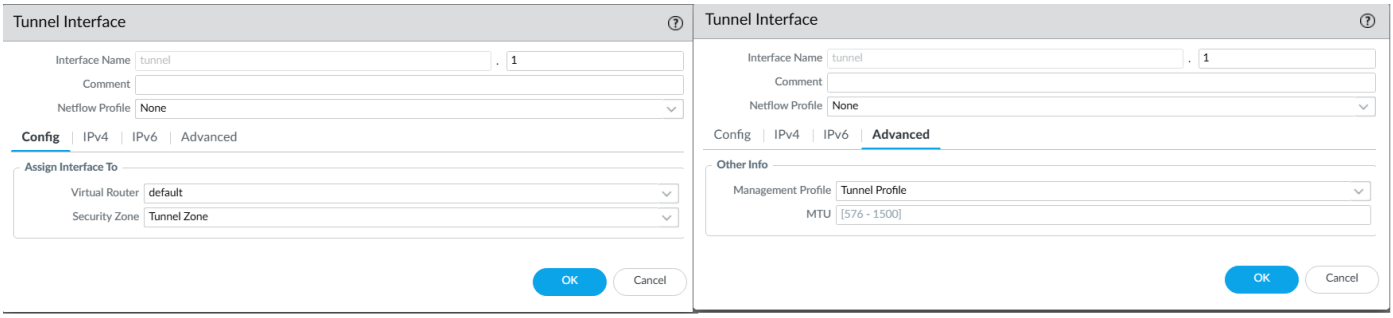
Step 3: Check the reachability among PA1 and PA2



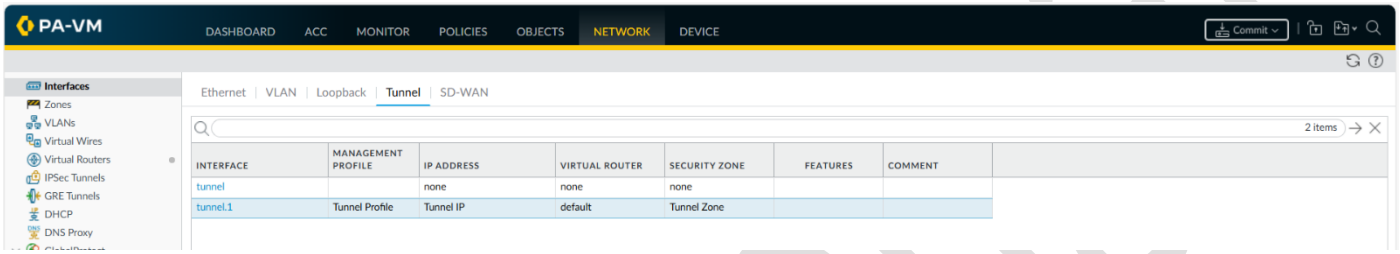
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

Step 4: Configure IKE phase 1 configuration

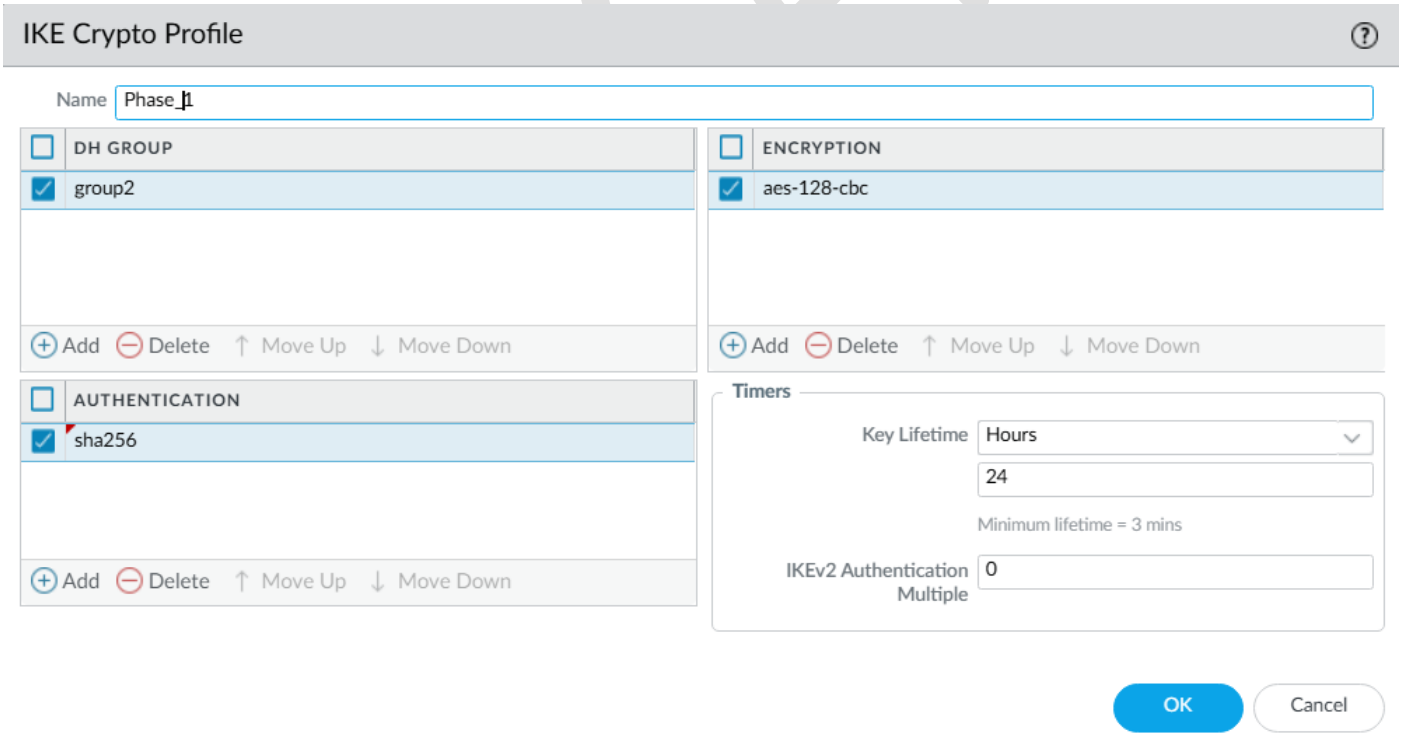
Network> Interfaces>Tunnel>Add



Make a tunnel profile enabling PING Service

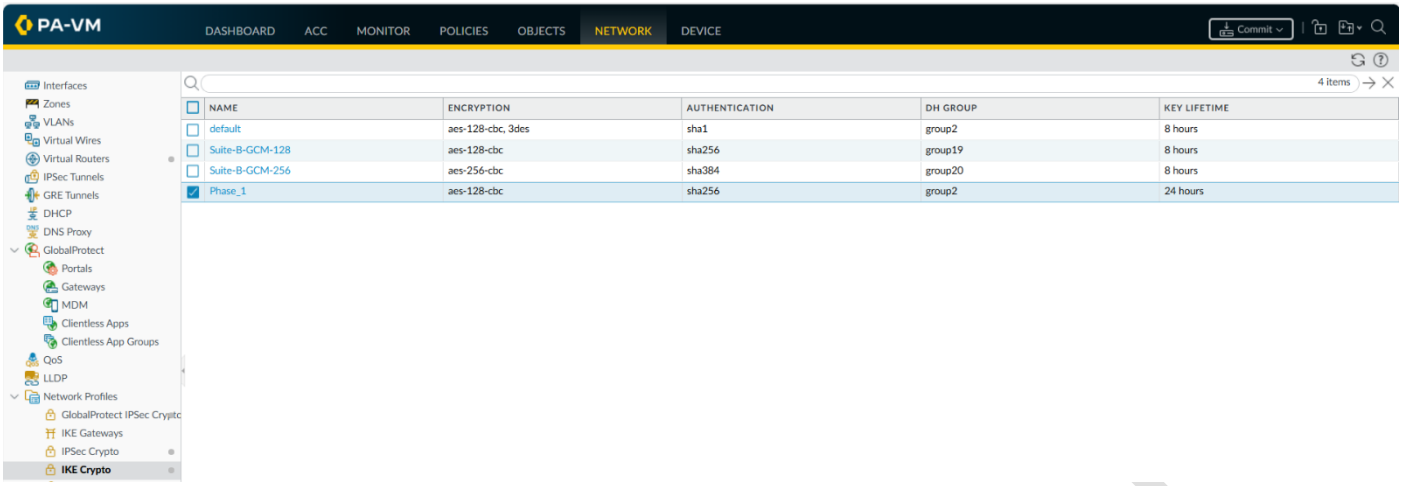


Network> Network Profile> IKE Crypto> Add new



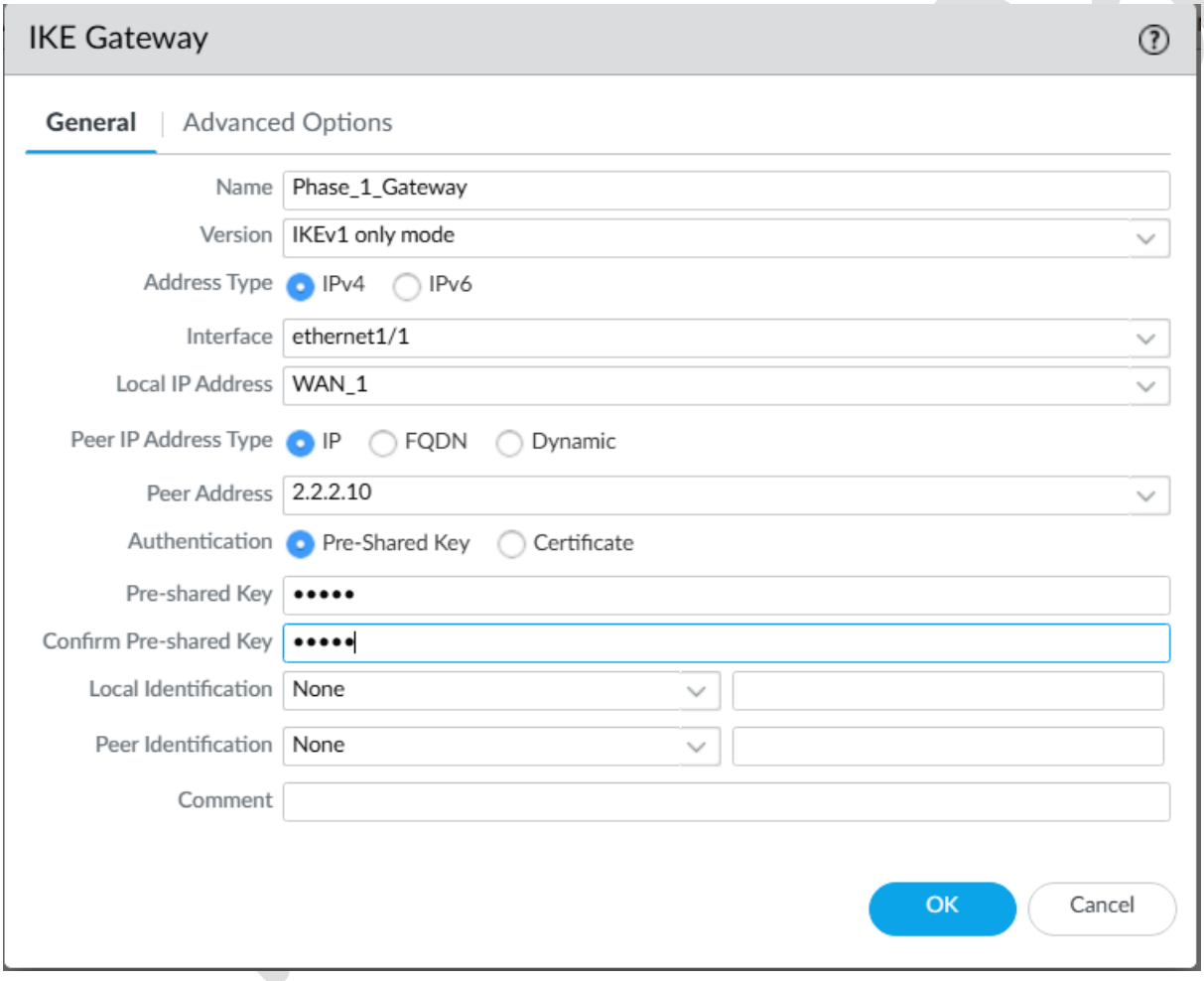
Note: You can add multiple DH(Defi hymen)group in IKE 1

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



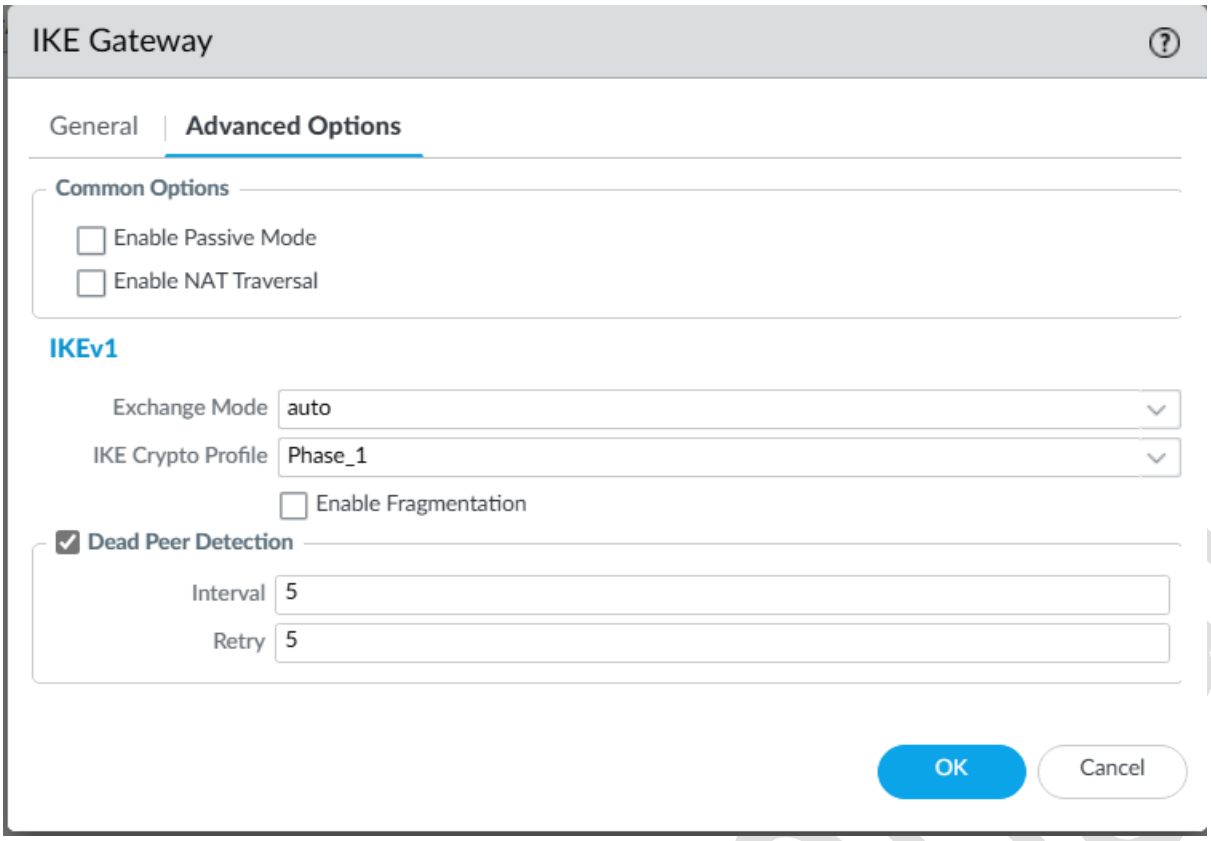
Note: You can select multiple algorithms and DH group but any one should match on both the sides

IKE Gateway> Add



You can give any pre shared key

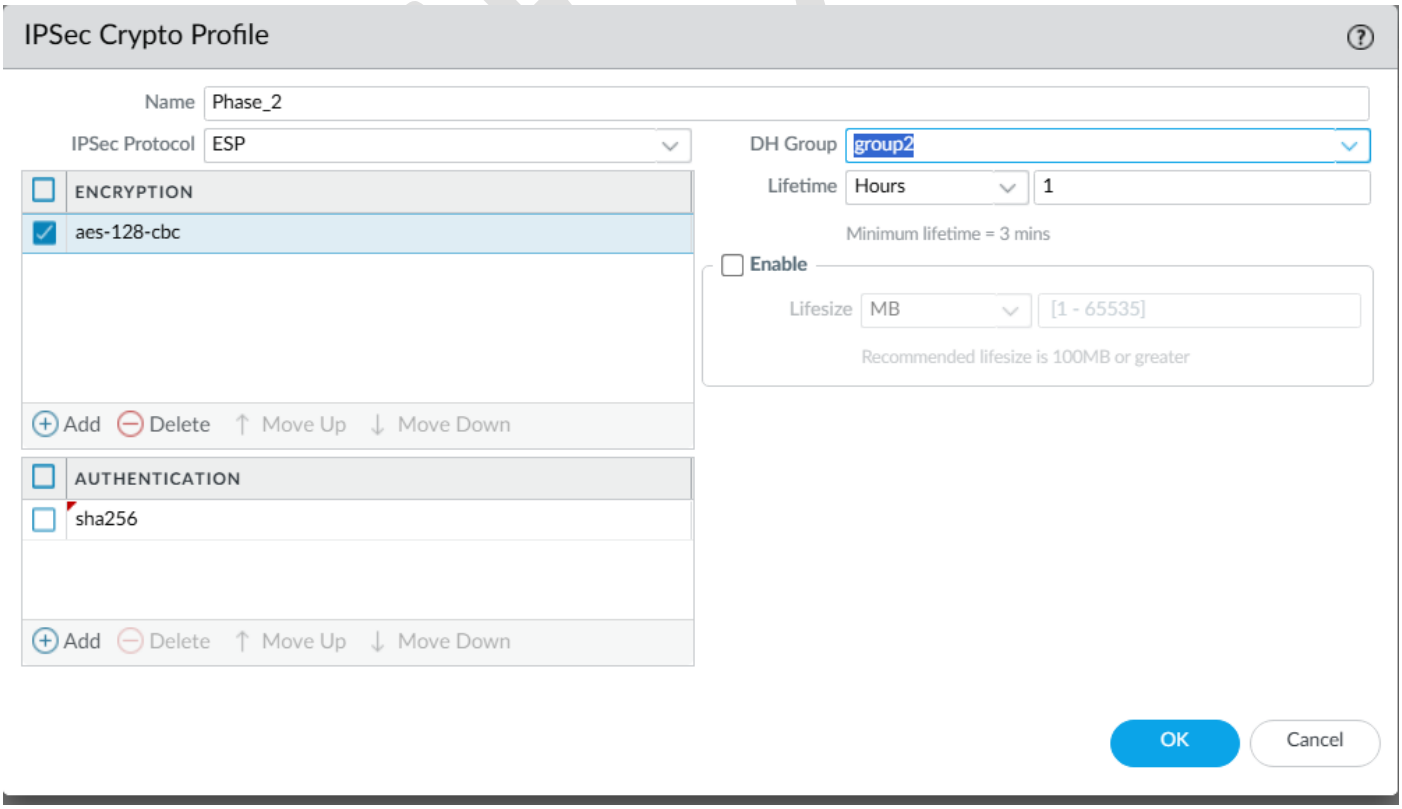
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/



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

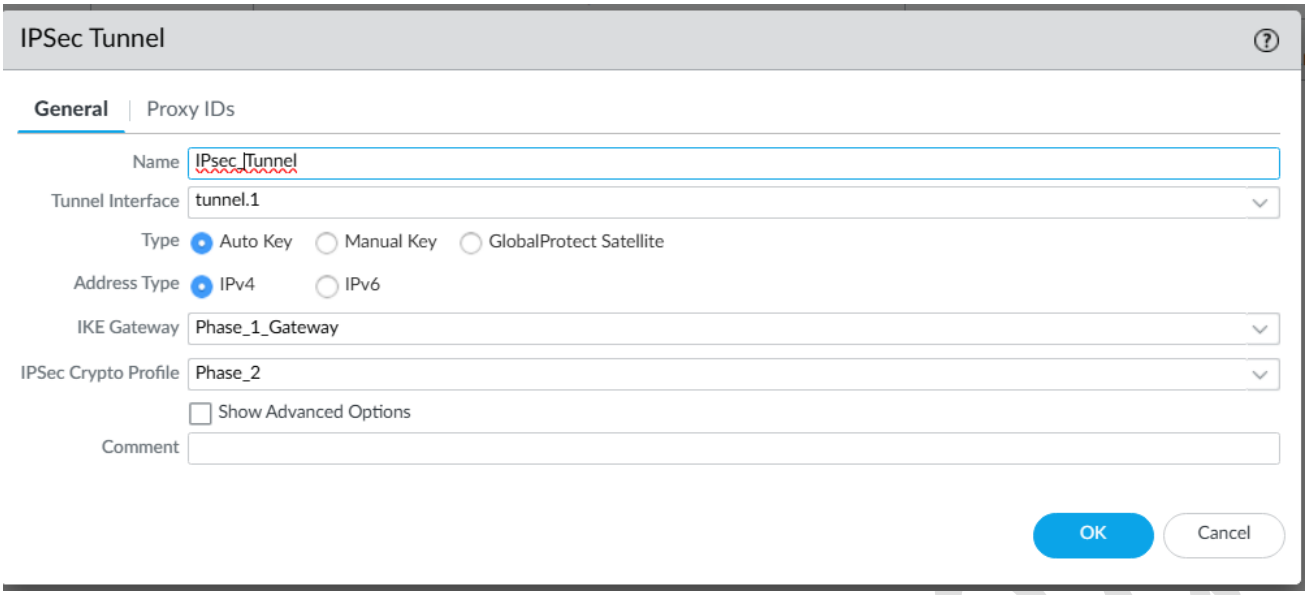


Note: In phase 2 we can select the DH group

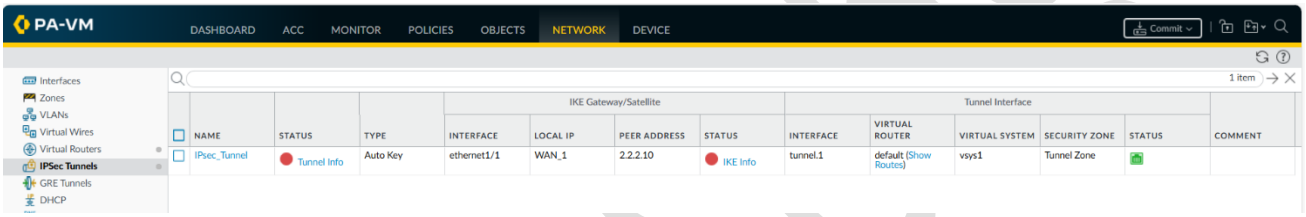
Step 6: Bind Phase 1 and Phase 2 configuration

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

Network> IPsec tunnels

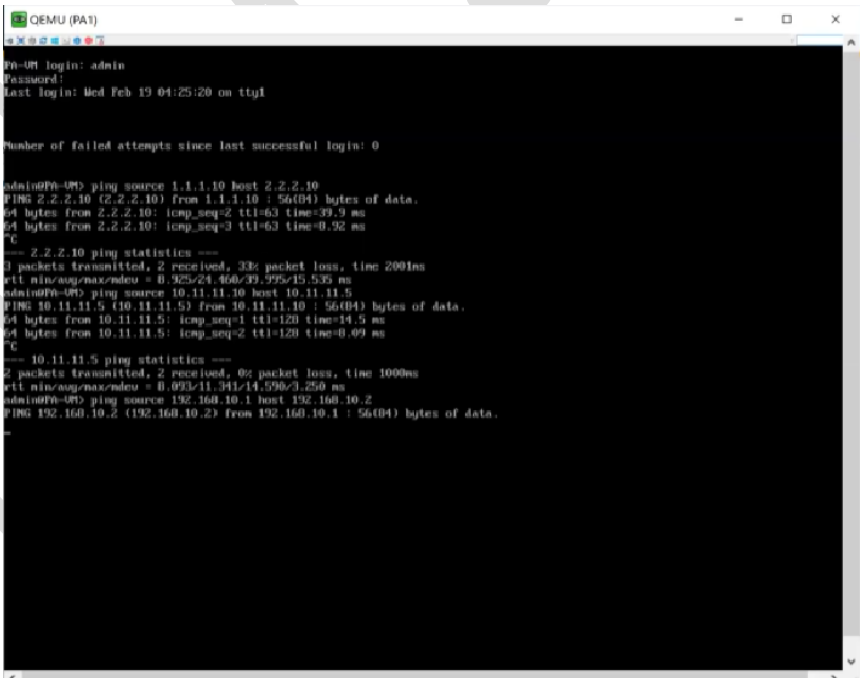


Step 7: Check whether tunnel is up or not



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

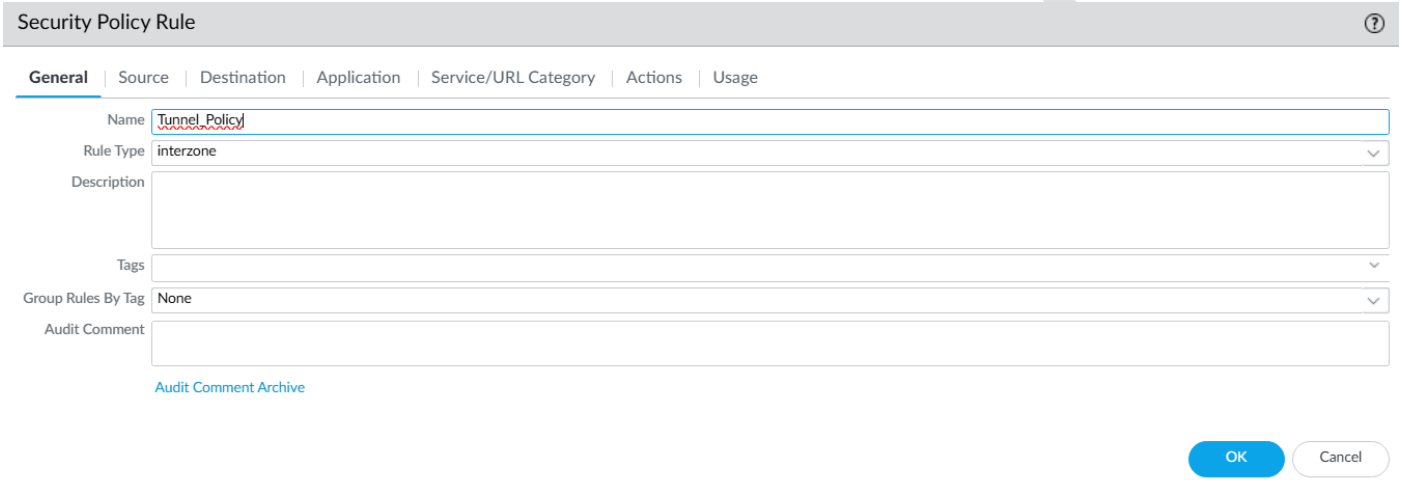
Once you commit and ping the tunnel interfaces then it will be up

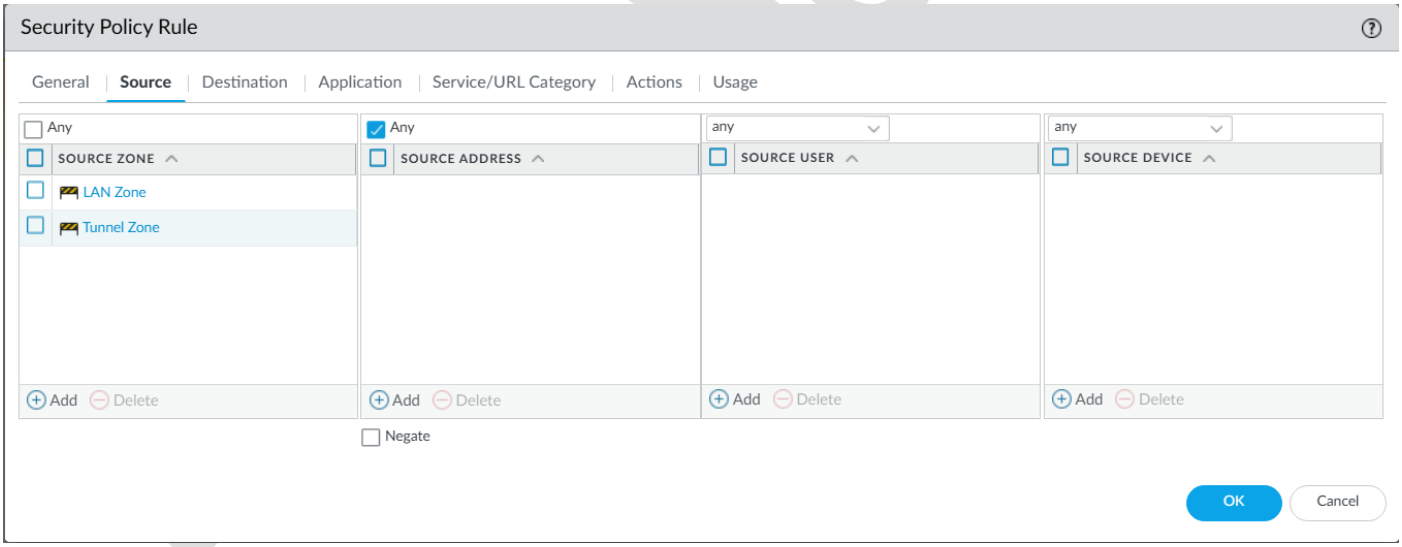


LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

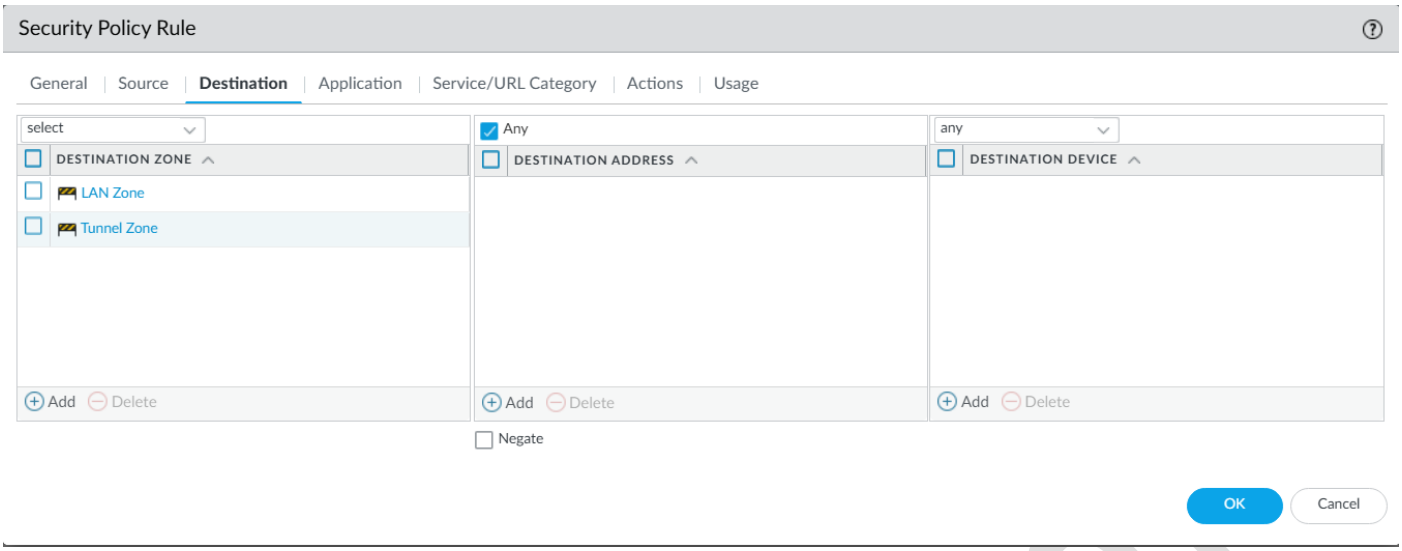
Step 8: Create a policy

Policies> Security> Add





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



Source will be LAN Destination will be tunnel

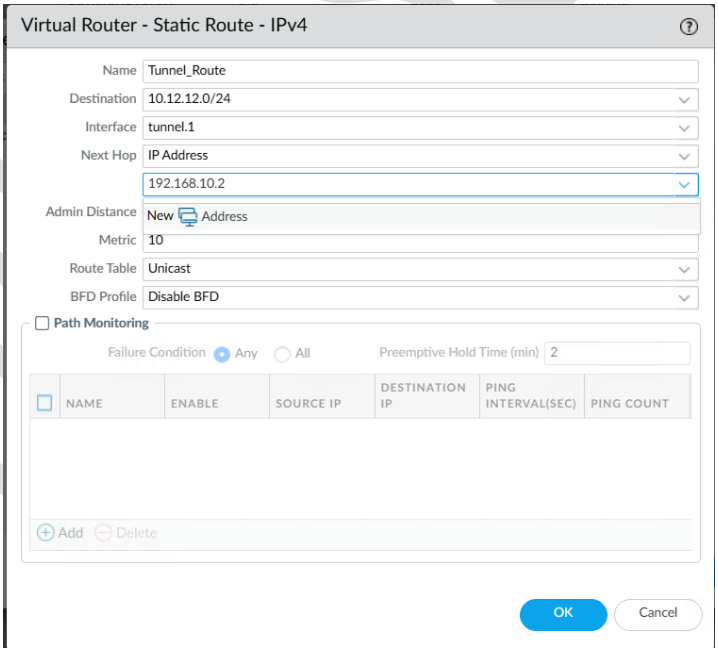
When source will be Tunnel destination will be LAN

Step 9: Specify the route in the virtual router

At the moment we have a static route towards ISP

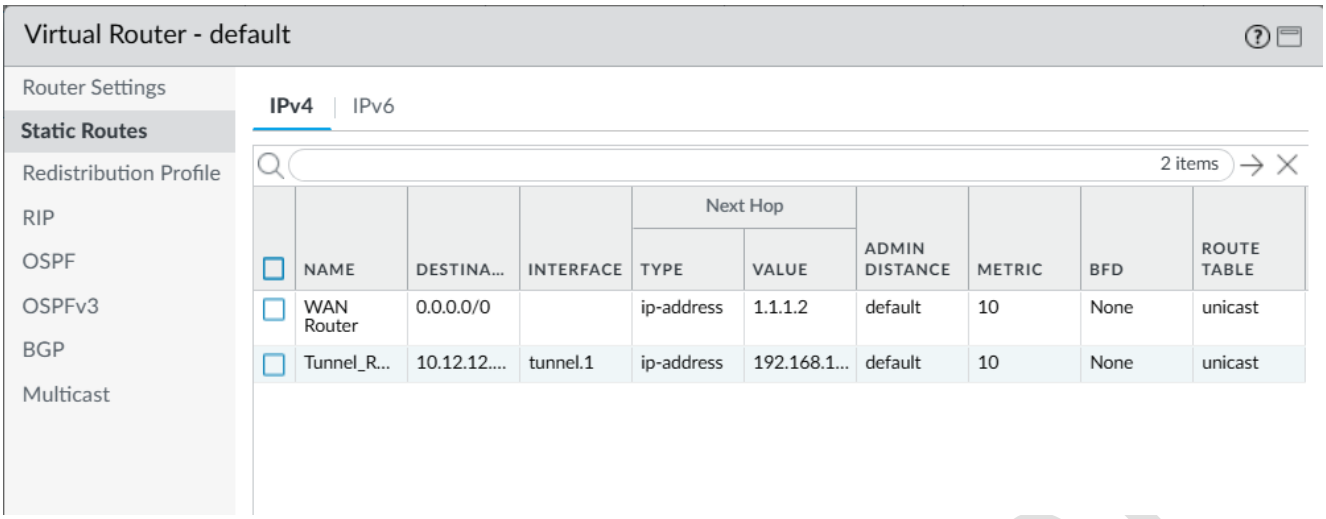
But we need to tell that whenever the private IP traffic will come we need to redirect it from tunnel

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

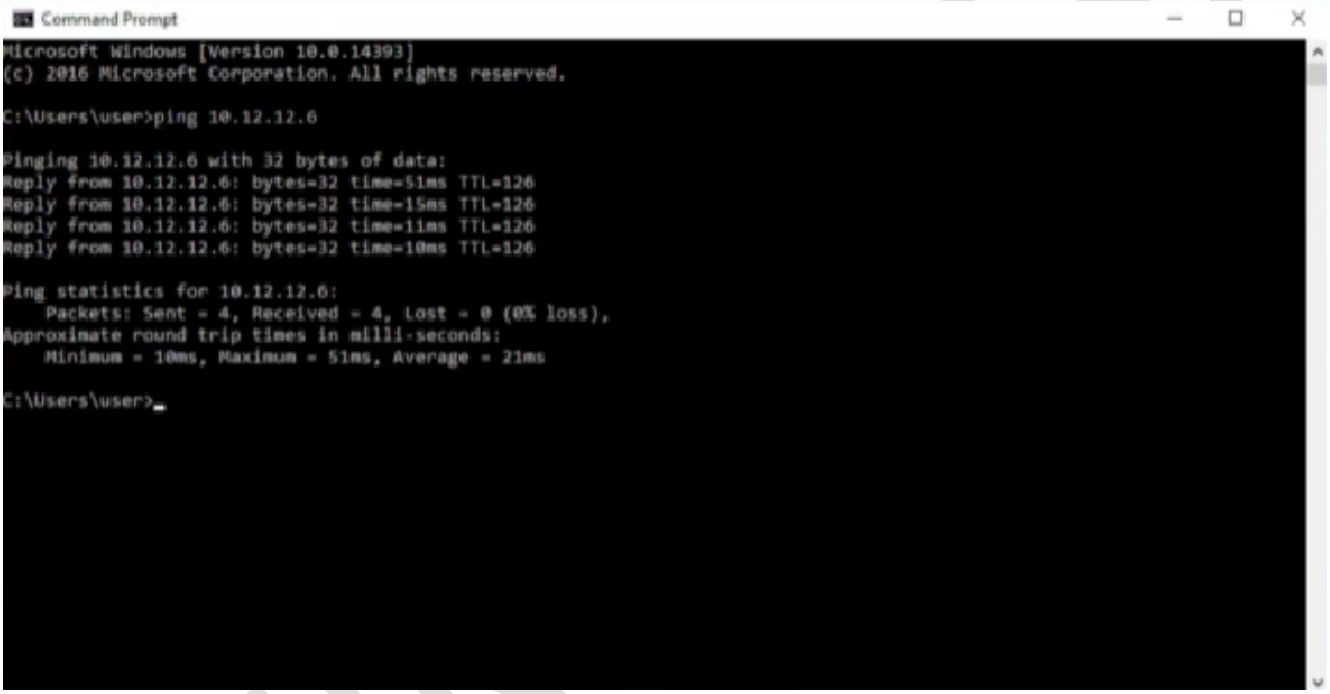


Pulkit Sehgal

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



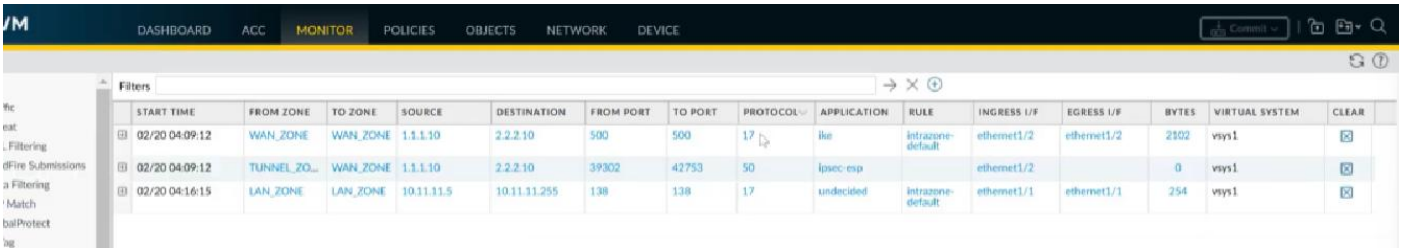
Ping from LAN1 PC to LAN2 PC



Pulkit

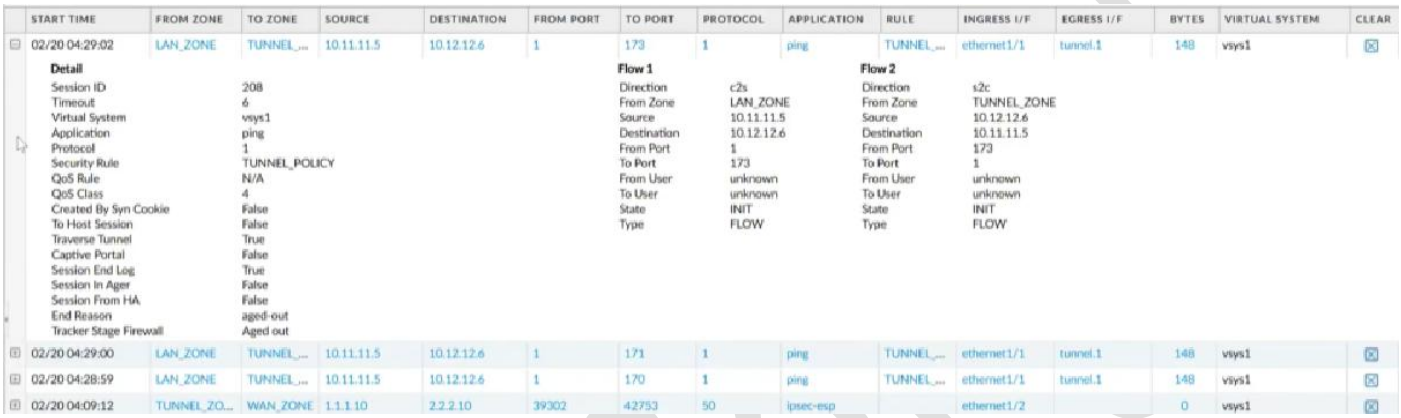
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

Check the sessions



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



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

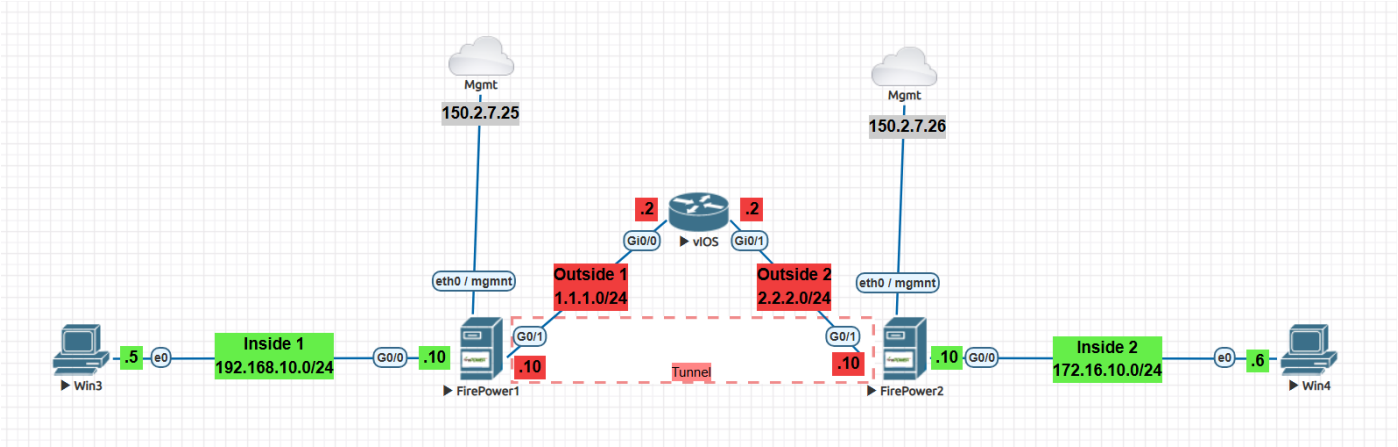
The tunnel starts from WAN interface and ending at other WAN interface

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

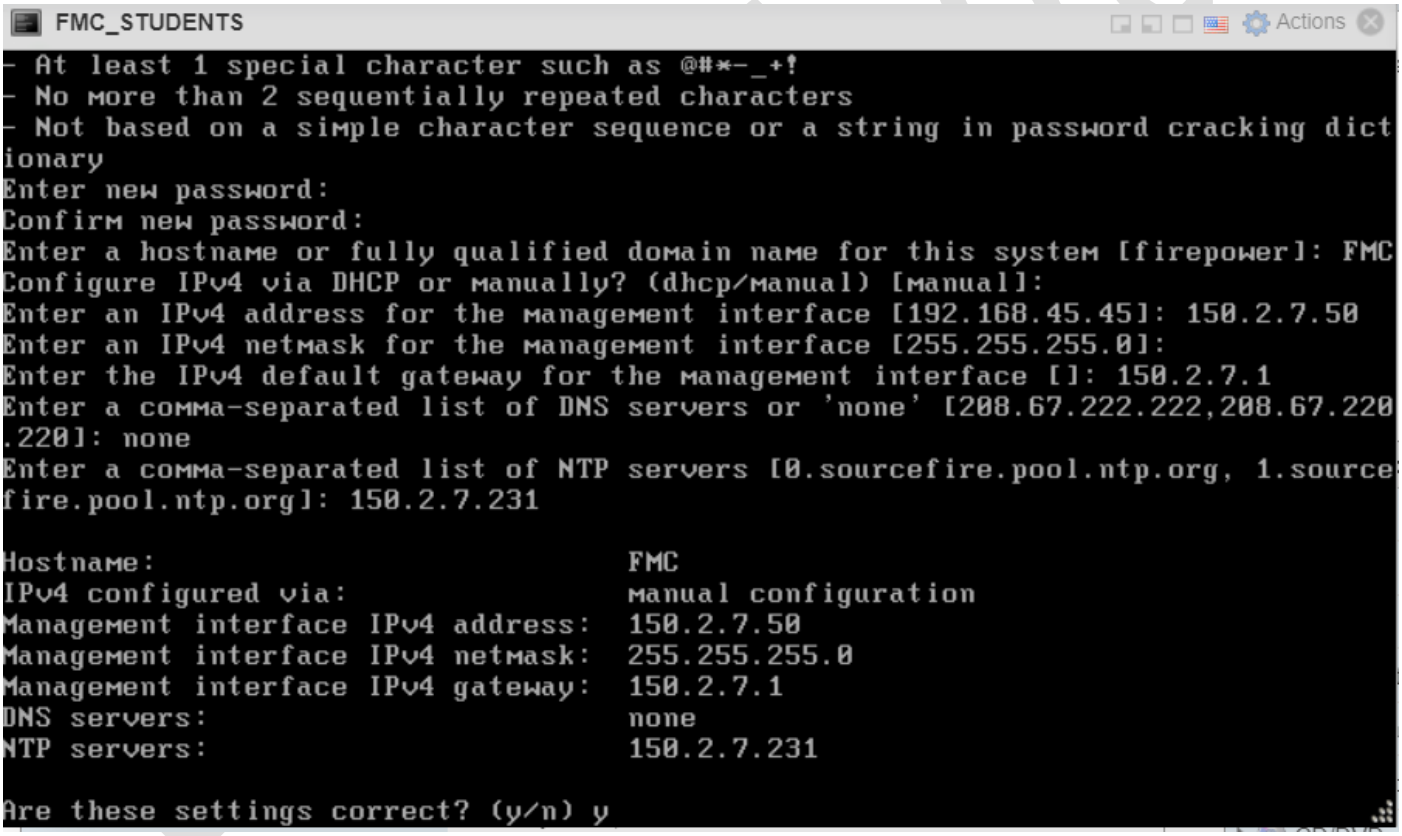
Pulkit Sehgal

CISCO FTD

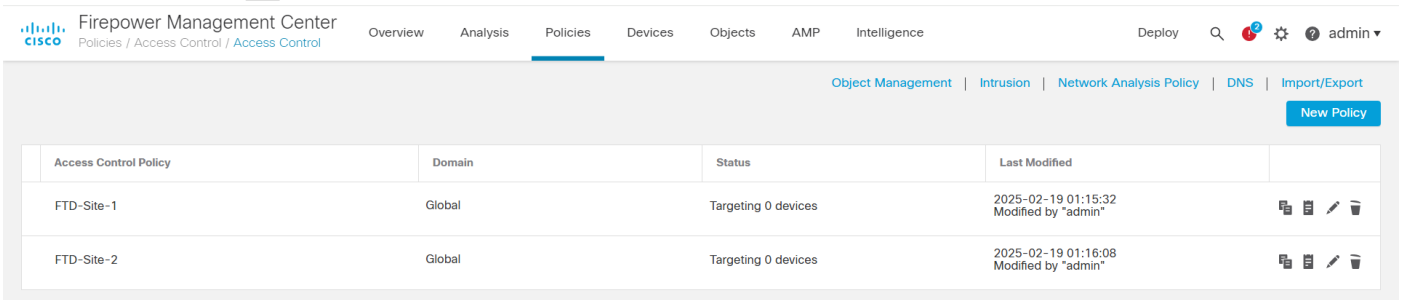


Step 1: Configure the topology

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



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

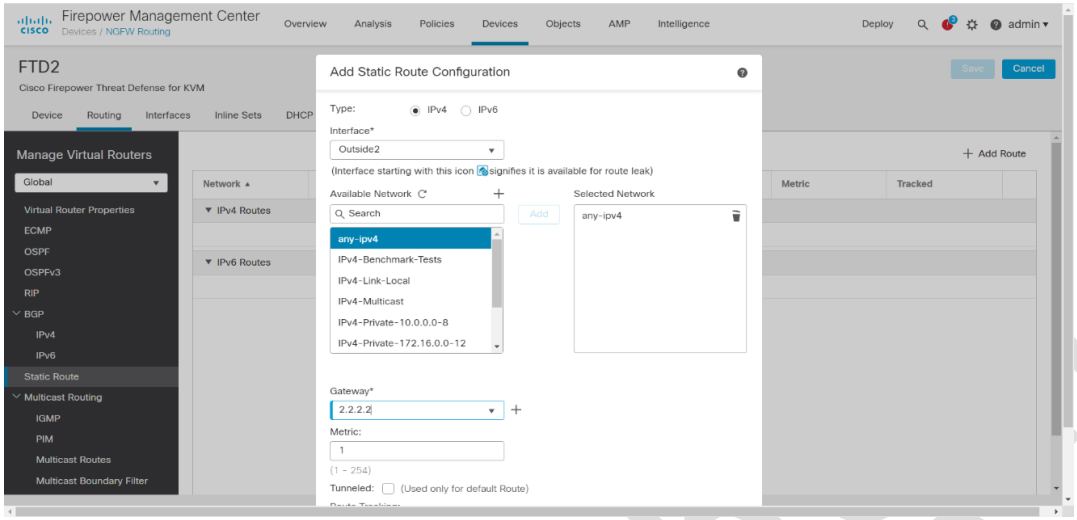


Note: You cannot configure two devices(FTD) in one single policy

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

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

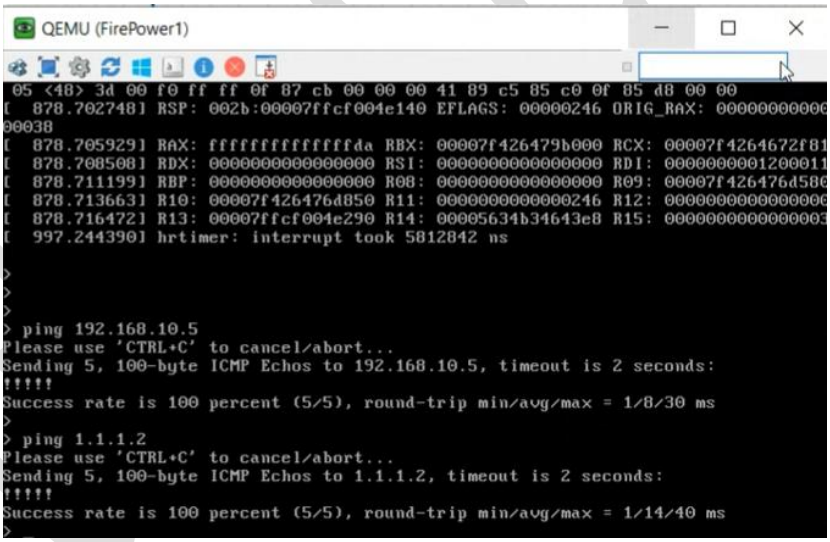
Device> Device management> Select the FTD> Edit> Routing> Static Routing> Add route> Interface> Allow any IP> Give Gateway> ok



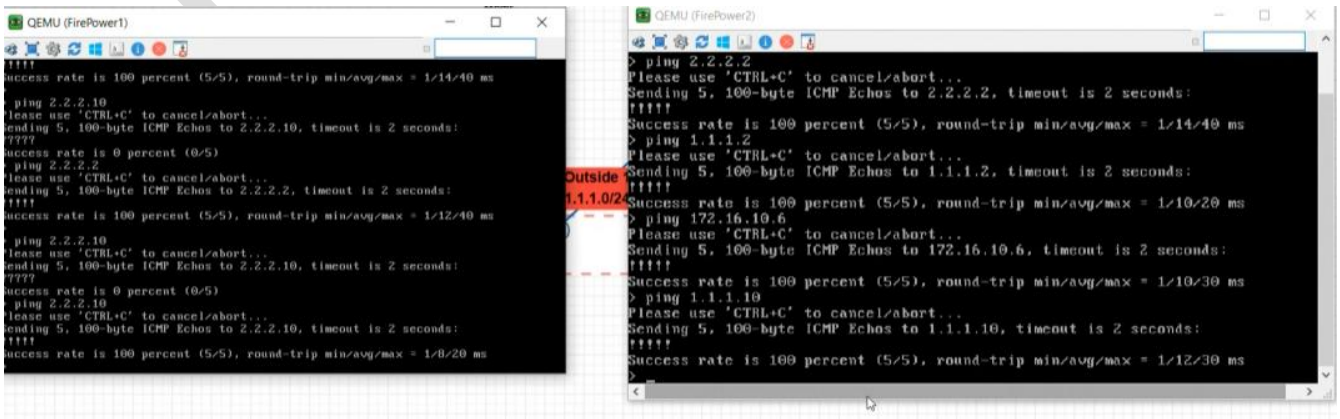
Save and deploy

Step 8: Check the connectivity from the FTD

FTD to PC



FTD to FTD

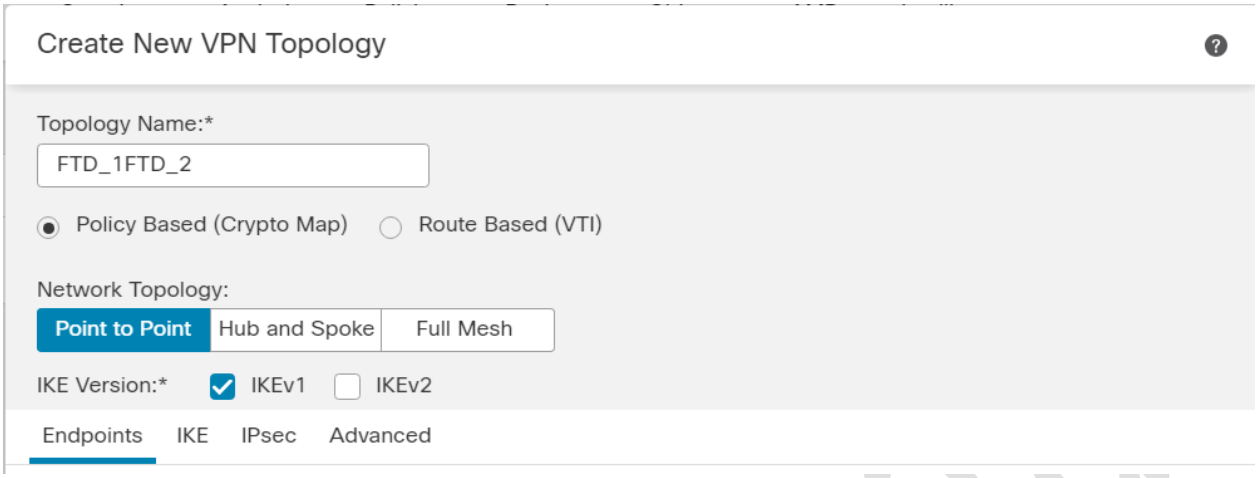


LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

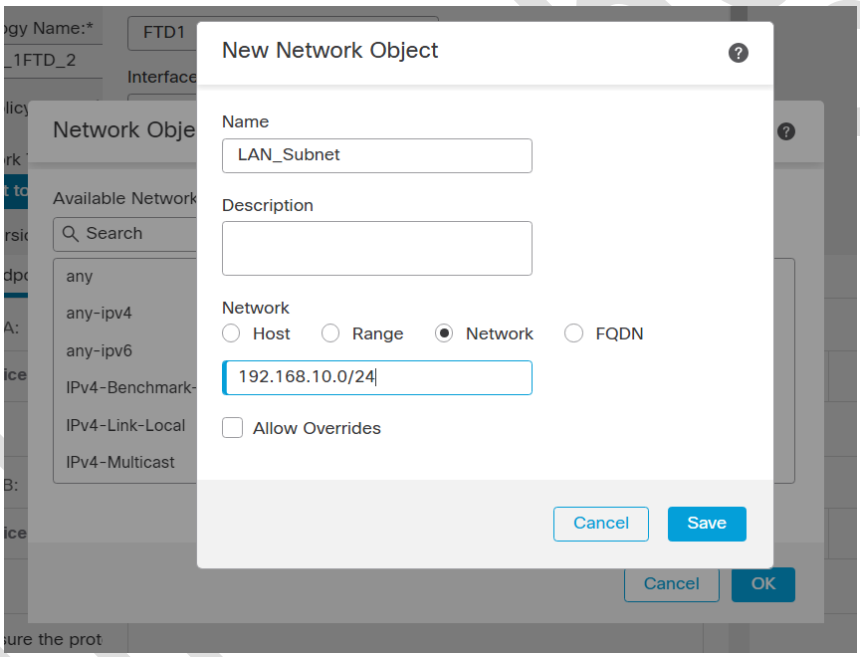
Step 9: Configure the Site to Site VPN

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

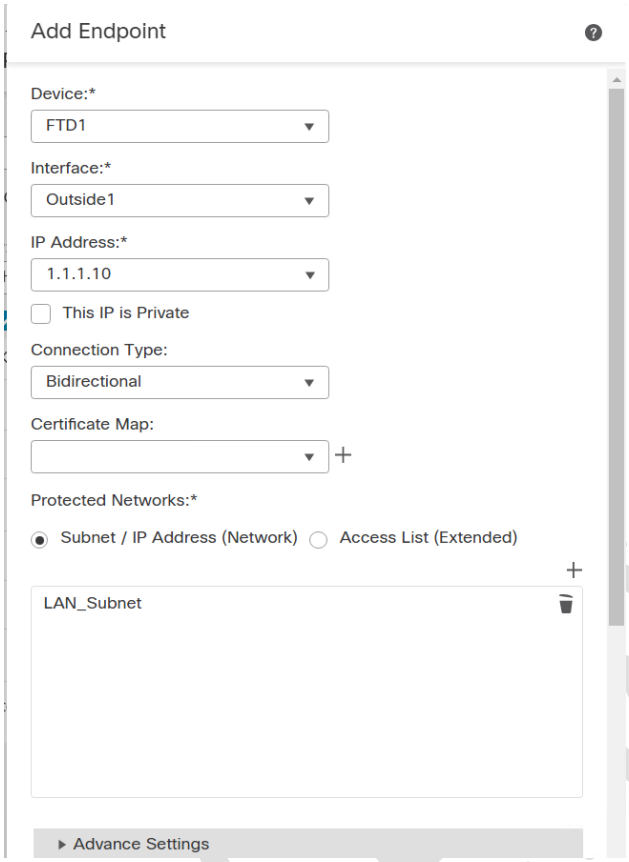
Policy based (Crypto MAP)> Point to Point> IKEv1



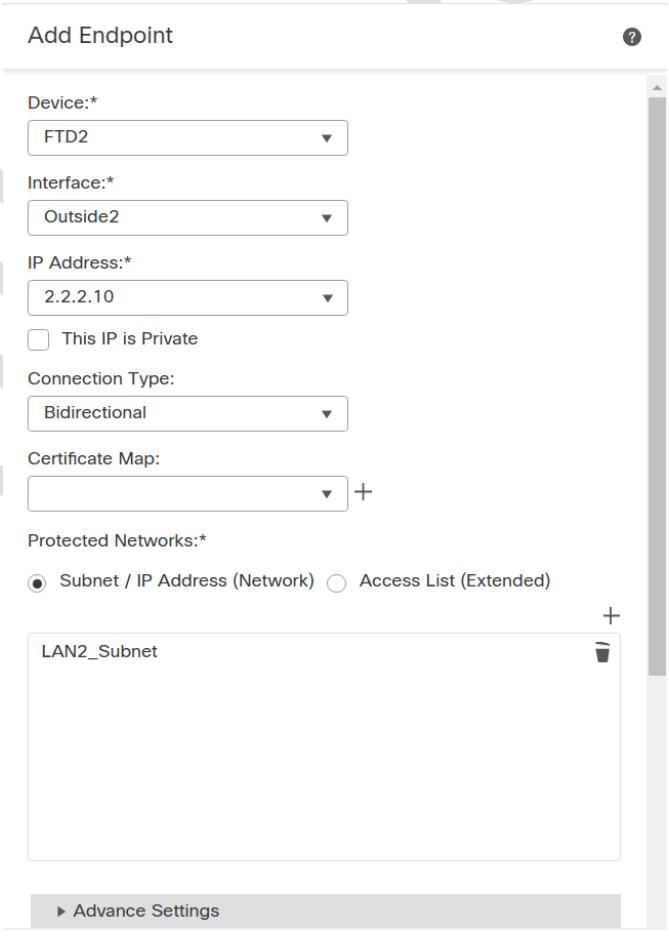
Endpoints> Add node 1> Choose Device> Choose interface> Choose IP address



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

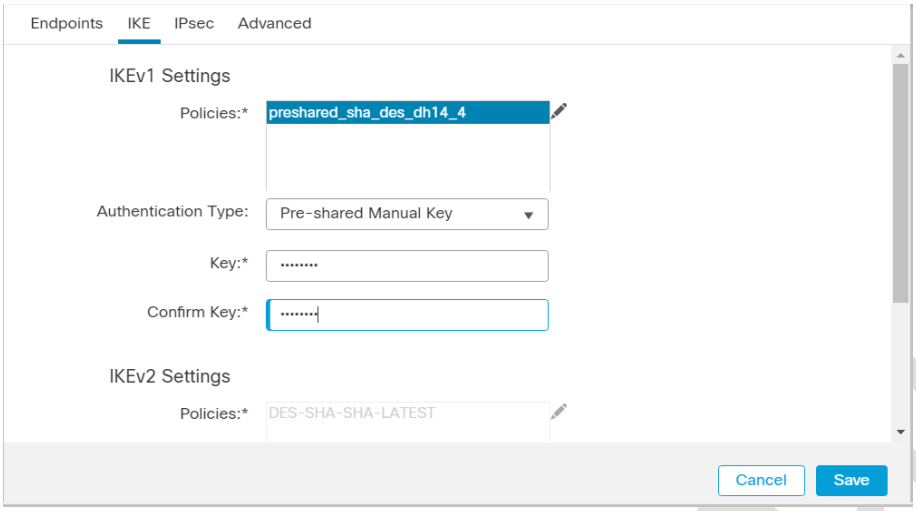


Endpoints> Add node 2> Choose Device> Choose interface> Choose IP address

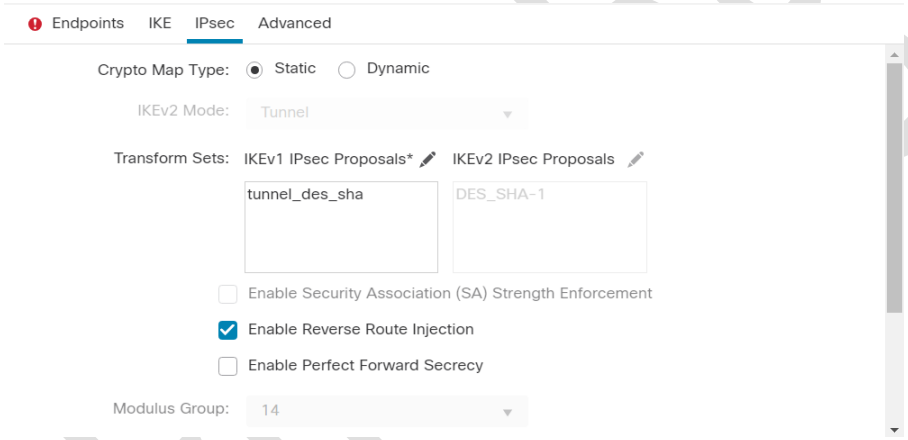


LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

IKE> preshared_sha_des_dh14_4> Pre-shared Manual Key> Cisc0123

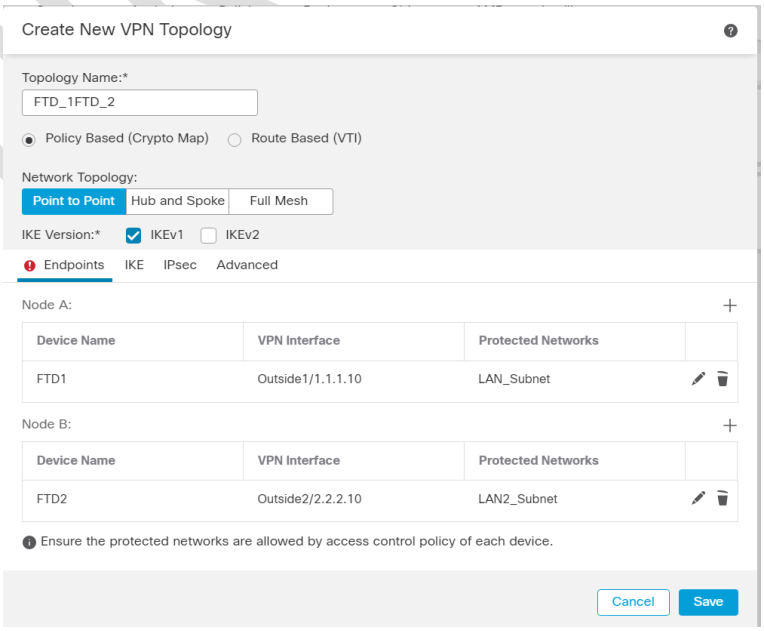


IPsec> Static



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

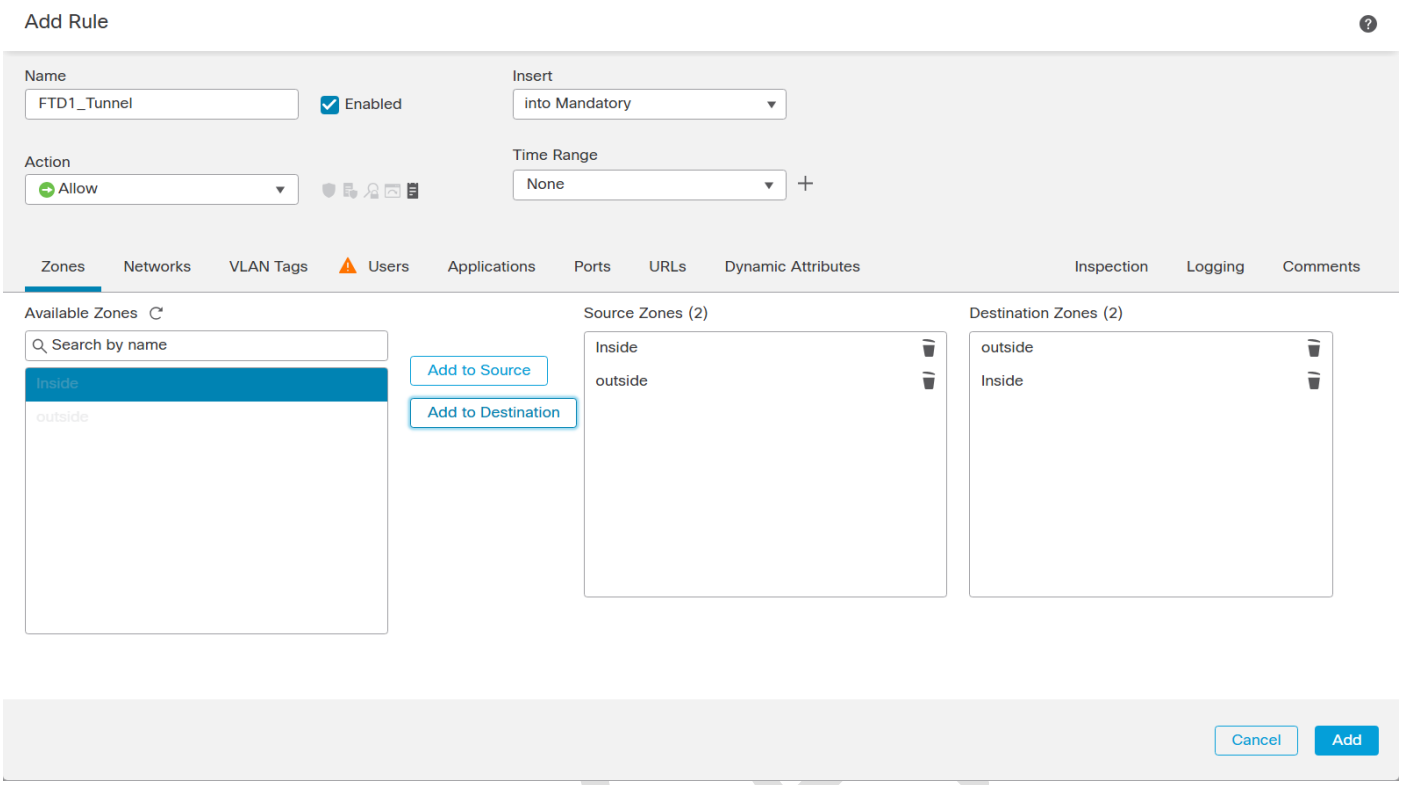


Save and deploy

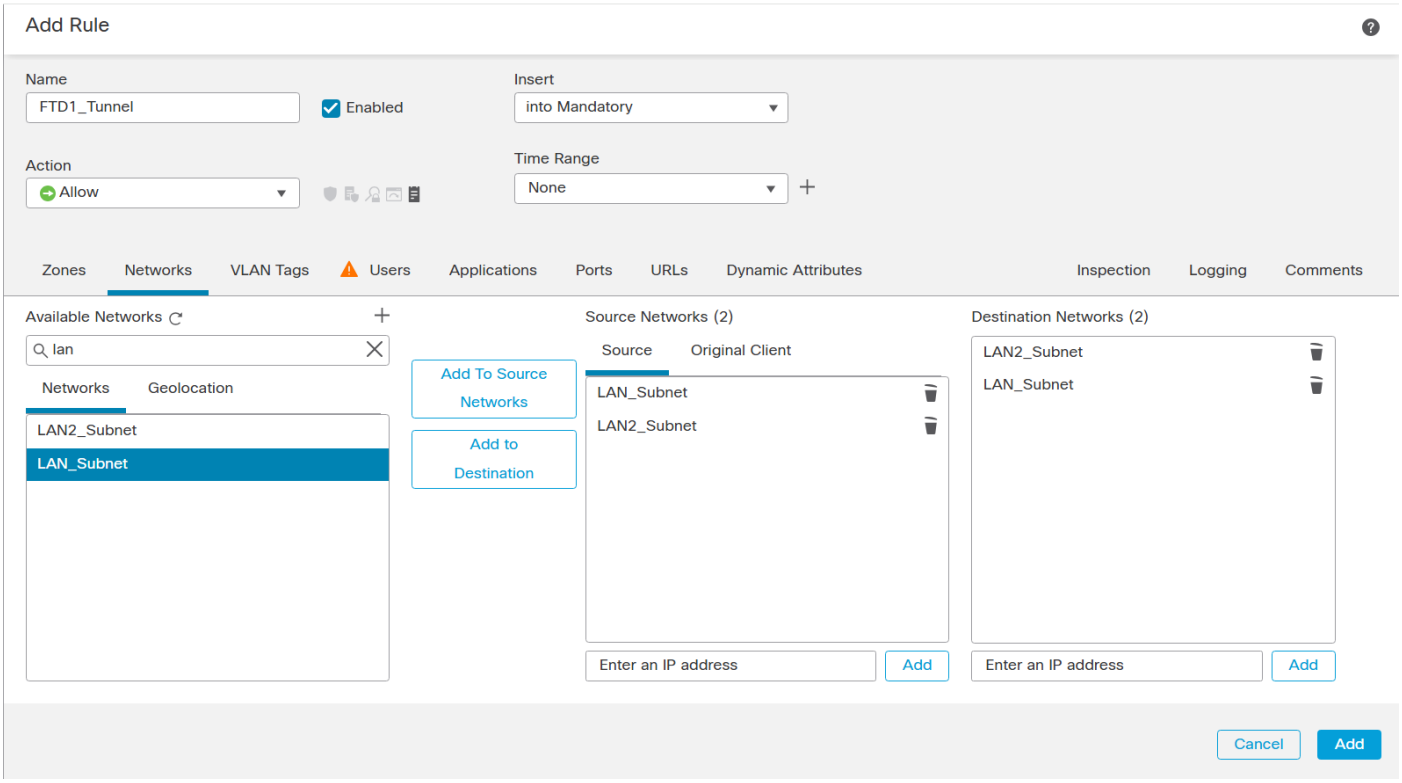
LinkedIn: https://www.linkedin.com/in/itspulkitsehgal/

Step 10: Create a policy

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

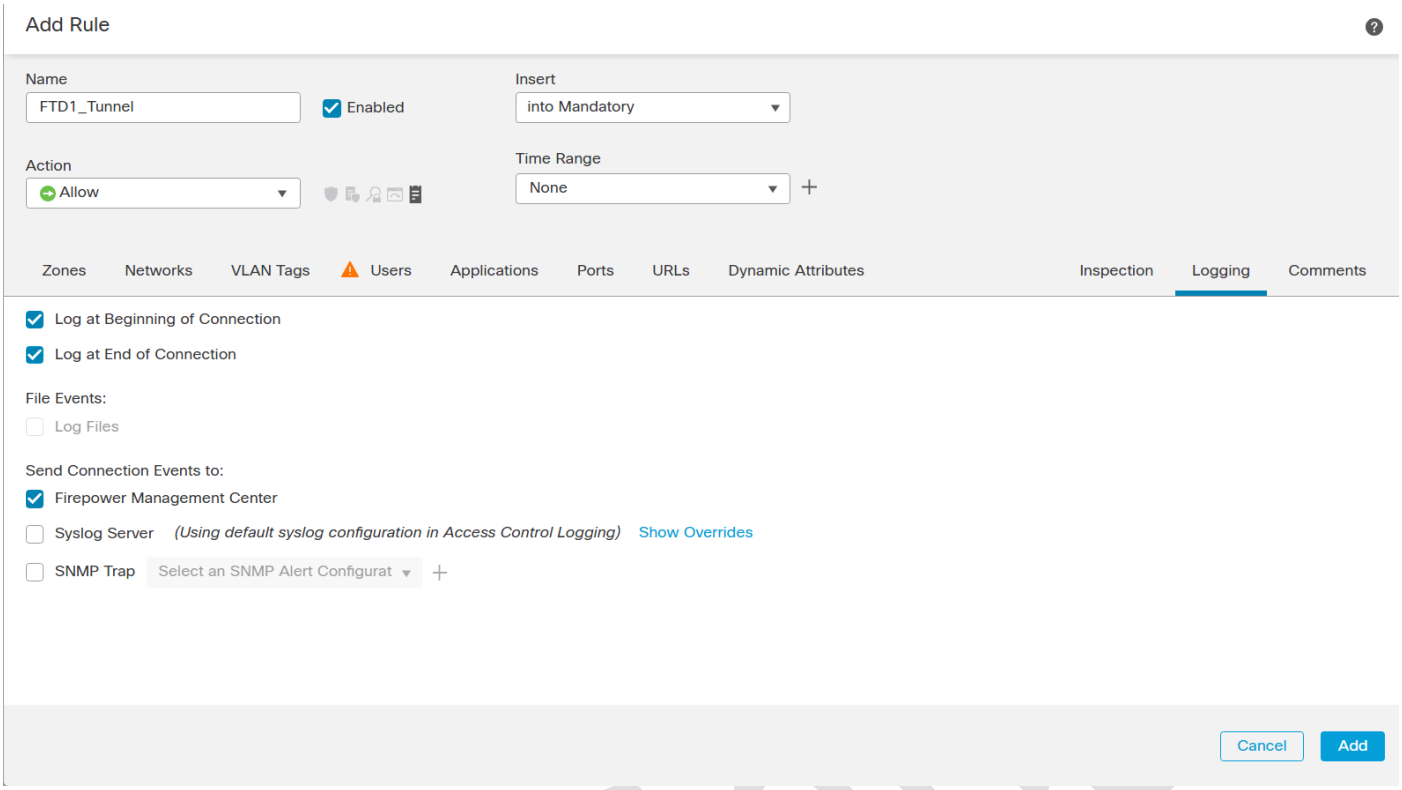


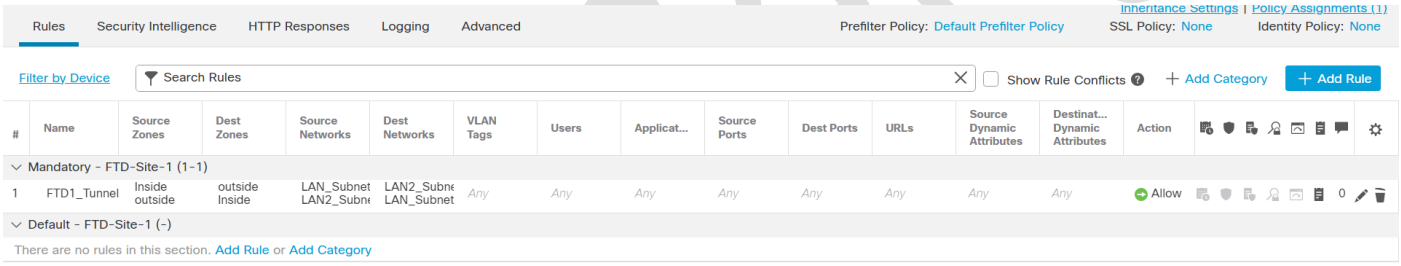
Networks>



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

Logging>





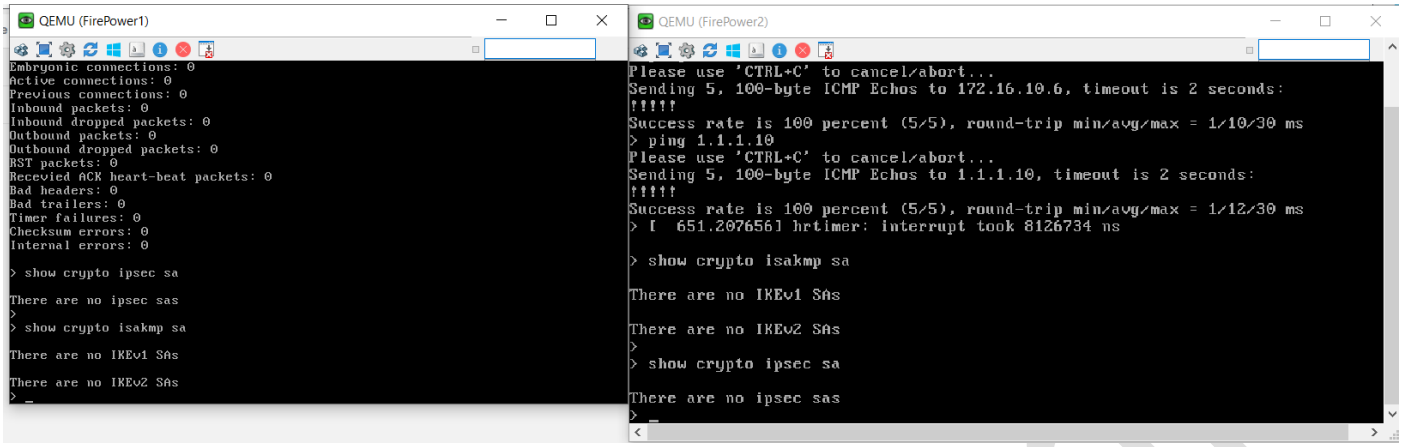
Same apply the policy on FTD 2 also

Pulkit

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

Step 11: Verify the tunnel and communication

Check on FTD



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