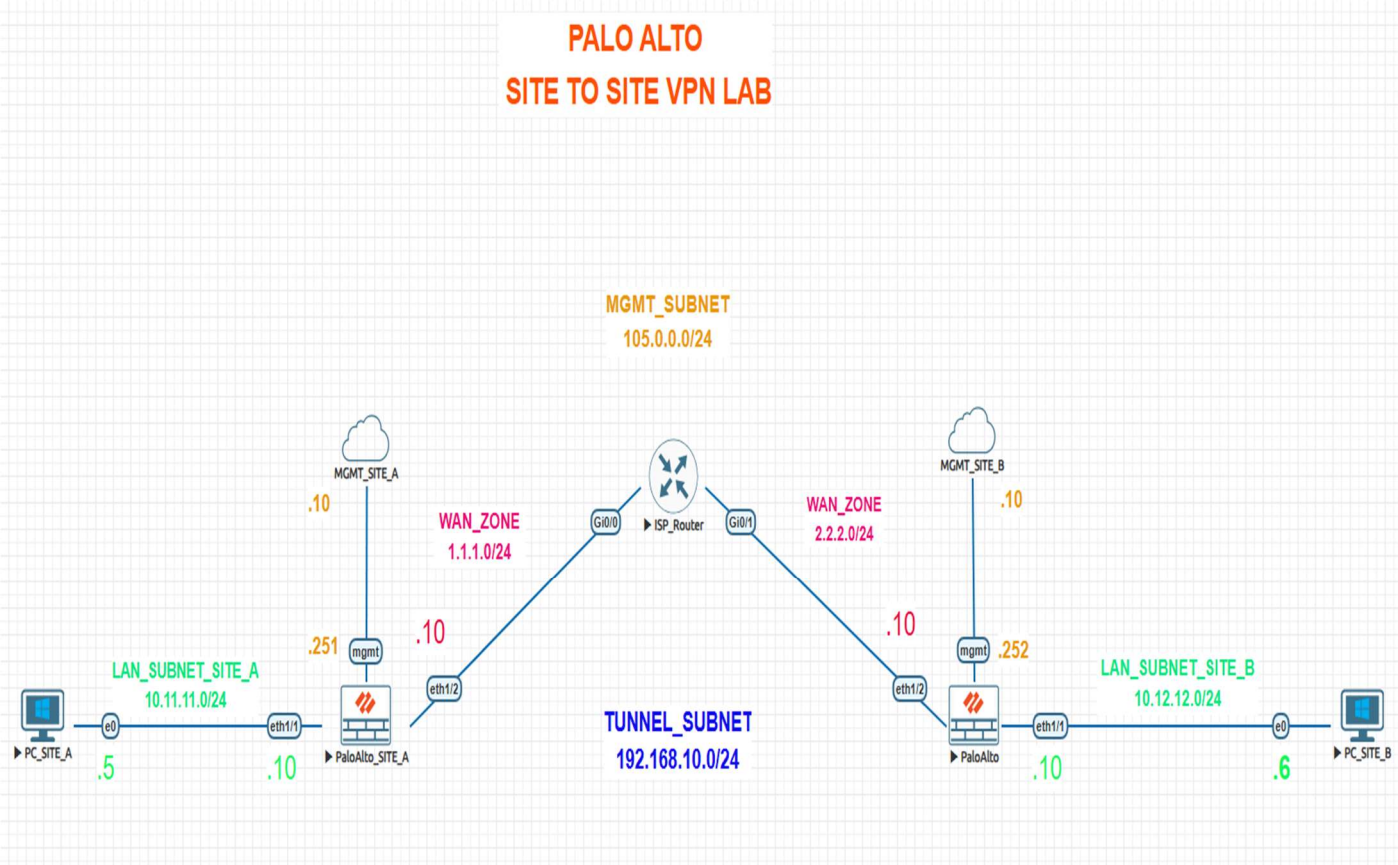
PALO ALTO FIREWALL SITE TO SITE VPN LAB

FOLLOW ME ON LINKEDIN FOR MORE SUCH CONTENTS

linkedin.com/in/imkumarabhishek

TOPOLOGY



Network topology of Site-to-Site VPN between Palo Alto Firewalls

Detailed Description (for documentation):

This diagram should display two Palo Alto Firewalls (Site A and Site B) connected through the Internet (Public Network). Each firewall should connect to a LAN network with one PC.

- Site A Firewall WAN IP: **105.0.0.251**
- Site B Firewall WAN IP: **105.0.0.252**
- Site A LAN: **192.168.1.0/24**
- Site B LAN: **192.168.2.0/24**
- Label tunnel interface tunnel.1 between both sites.
  Optionally, show “IKE Phase 1” and “IPSec Phase 2” across the WAN link.

INITIAL CONFIGURATIONS

==========

PaloAlto_SITE_A - Setup Guide

==========

STEP 1: Login with Default Credentials

---

login: admin (Default username)

password: admin (Default password)

STEP 2: Change Admin Password

Enter old password: admin (Current password)

Enter new password: Ab@12345 (New strong password)

Confirm password: Ab@12345 (Confirm new password)

STEP 3: Enter Configuration Mode

> configure (Enter configuration mode)

STEP 4: Remove DHCP Client Mode

---

delete deviceconfig system type dhcp-client (Remove DHCP if previously enabled)

STEP 5: Set Static IP Address

---

set deviceconfig system ip-address 105.0.0.251 netmask 255.255.255.0 (Assign static IP and subnet mask)

STEP 6: Commit Changes

---

commit (Apply and save config)

STEP 7: Exit Configuration Mode

---

exit (Return to operational prompt)

STEP 8: Verify Interface Settings

> show interface management (View current IP, MAC, status, etc.)

==========

After setup, access GUI at:

https://105.0.0.251

==========

==========

PaloAlto_SITE_B - Setup Guide

==========

STEP 1: Login with Default Credentials

---

login: admin (Default username)

password: admin (Default password)

STEP 2: Change Admin Password

Enter old password: admin (Current password)

Enter new password: Ab@12345 (New strong password)

Confirm password: Ab@12345 (Confirm new password)

STEP 3: Enter Configuration Mode

> configure (Enter configuration mode)

STEP 4: Remove DHCP Client Mode

---

delete deviceconfig system type dhcp-client (Remove DHCP if previously enabled)

STEP 5: Set Static IP Address

---

set deviceconfig system ip-address 105.0.0.252 netmask 255.255.255.0 (Assign static IP and subnet mask)

STEP 6: Commit Changes

---

commit (Apply and save config)

STEP 7: Exit Configuration Mode

---

exit (Return to operational prompt)

STEP 8: Verify Interface Settings

> show interface management

(View current IP, MAC, status, etc.)

==========

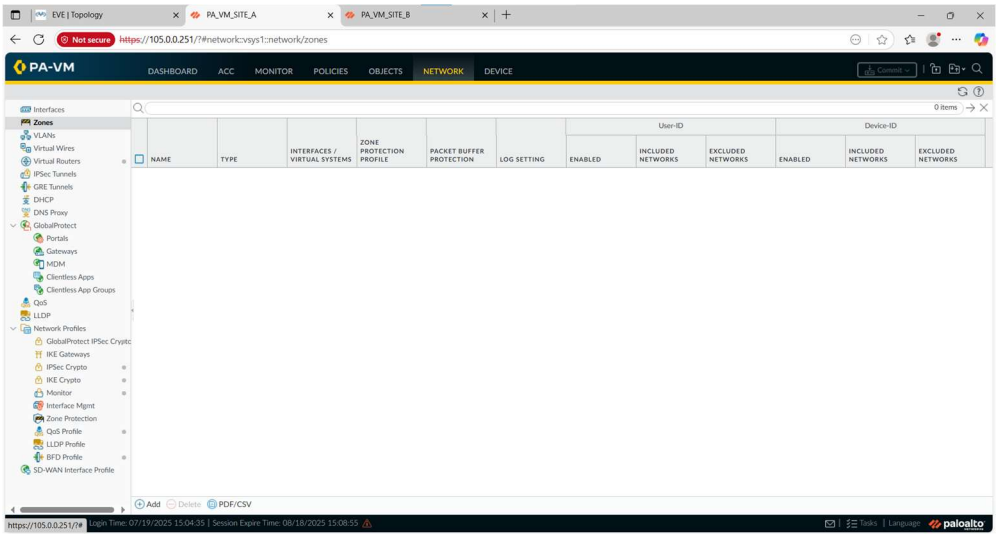
After setup, access GUI at:

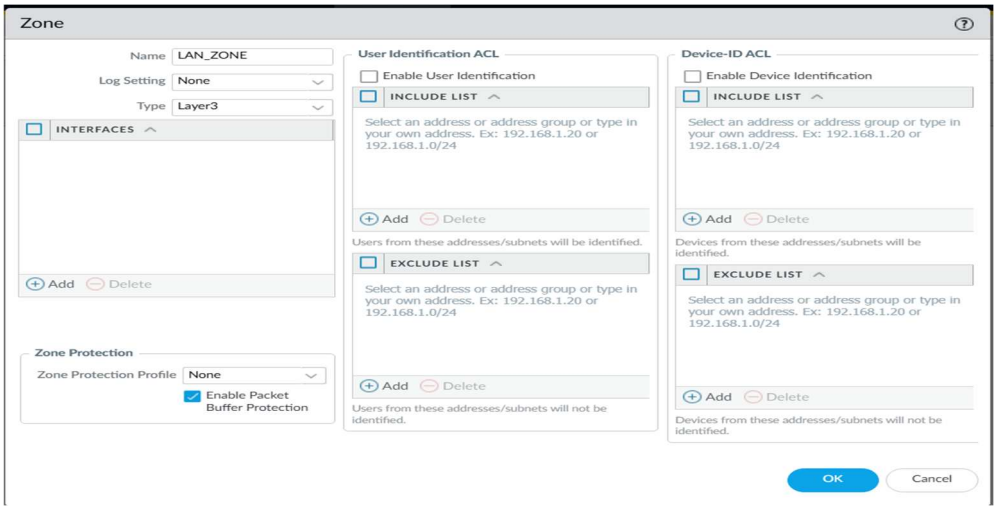
https://105.0.0.252

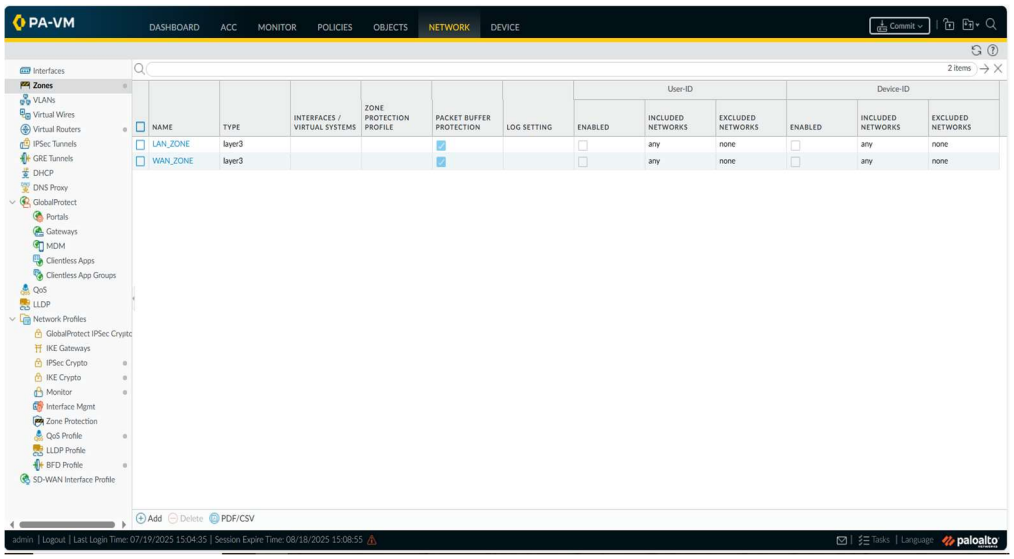
==========

1. To Create Zone

Go to network >zone>add

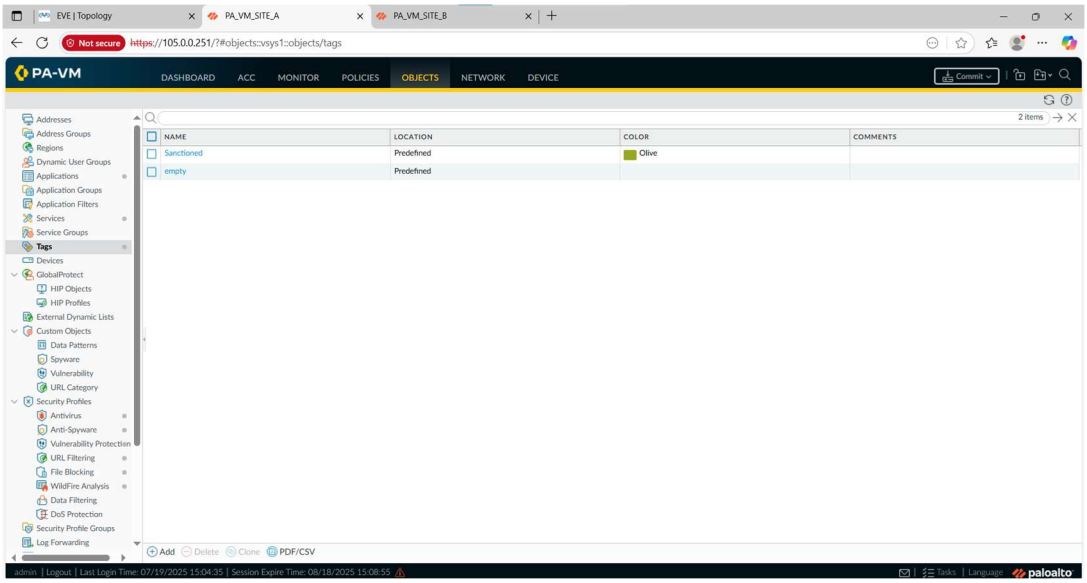


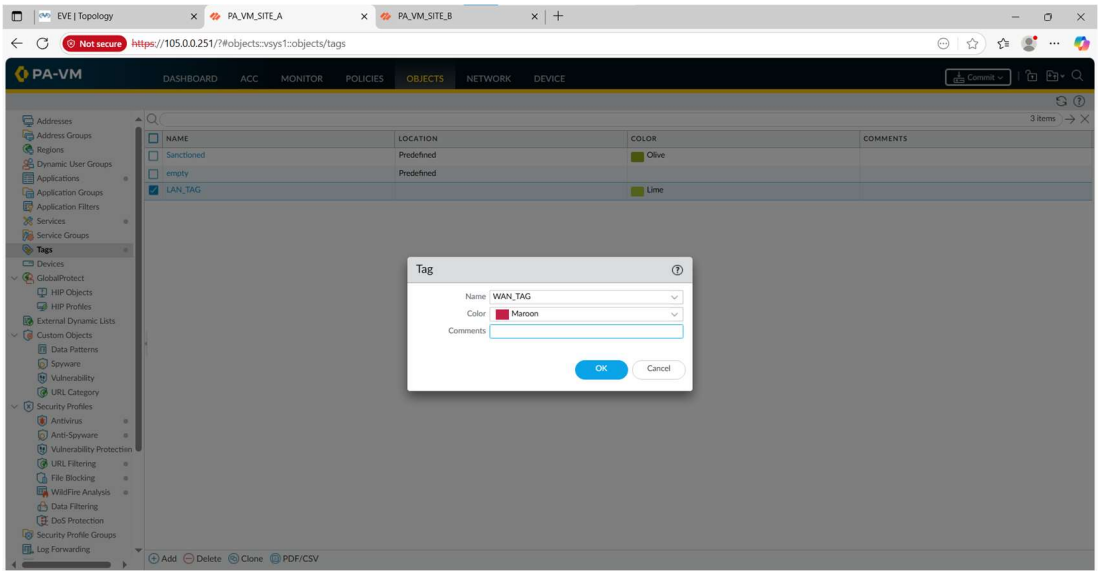


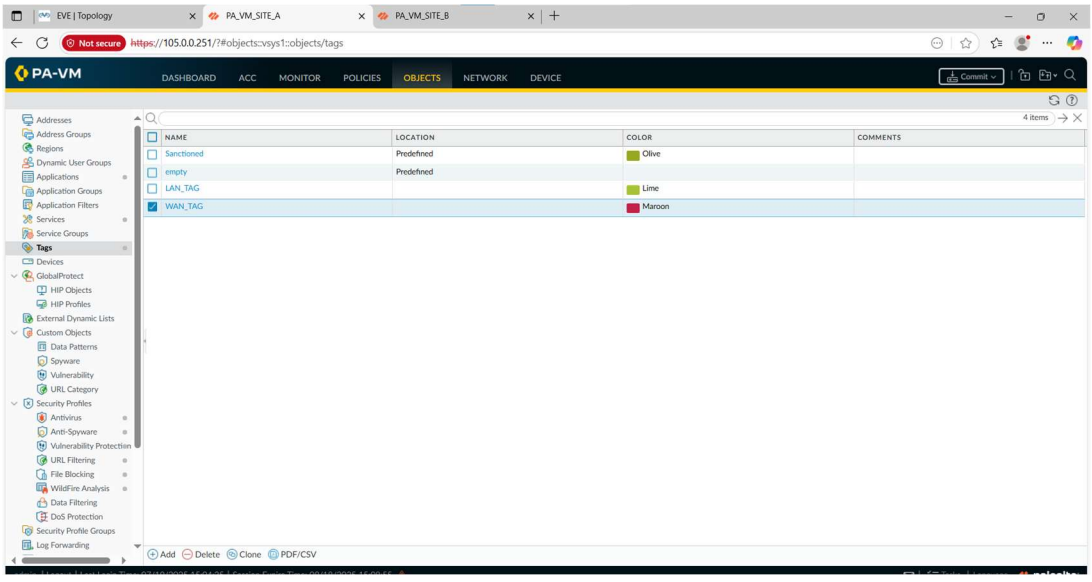


2. To Create Tags

Go to objects>tag>add

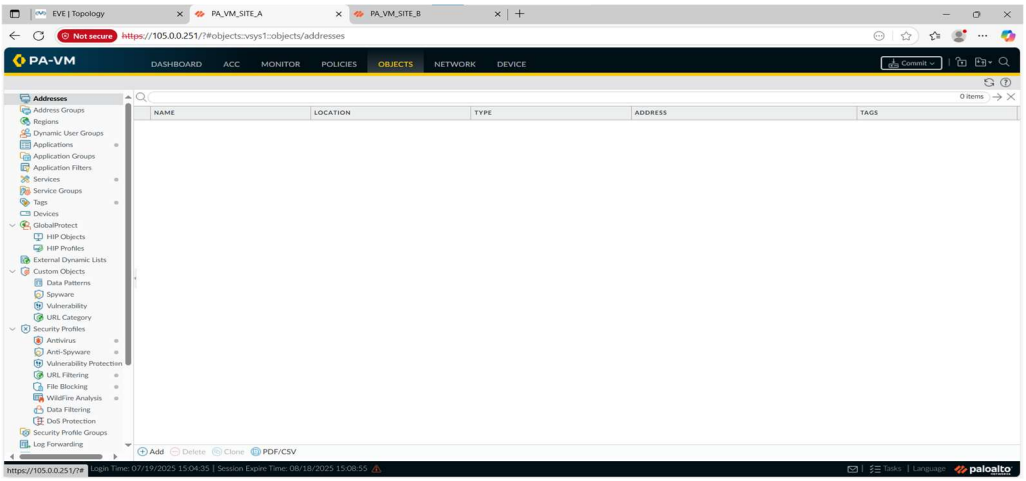


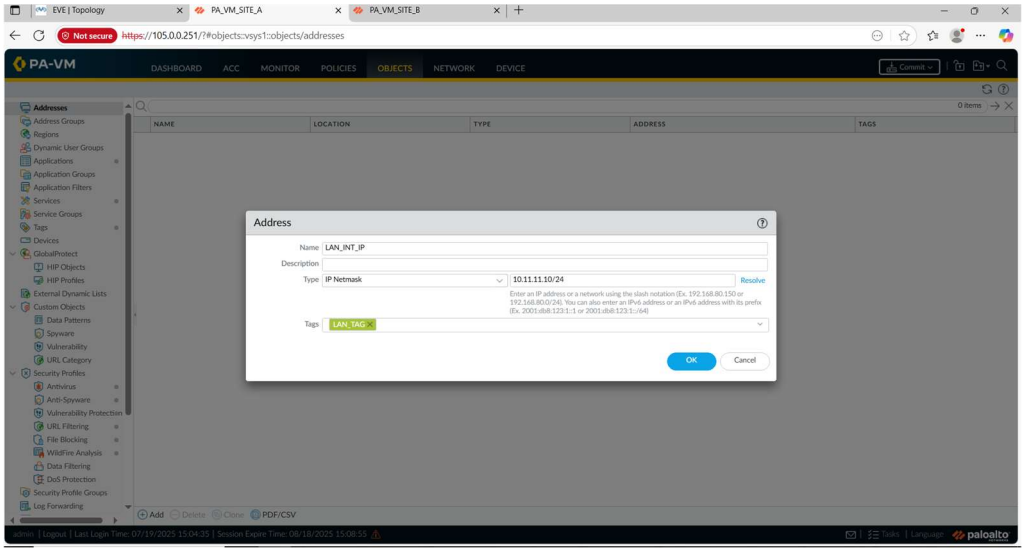


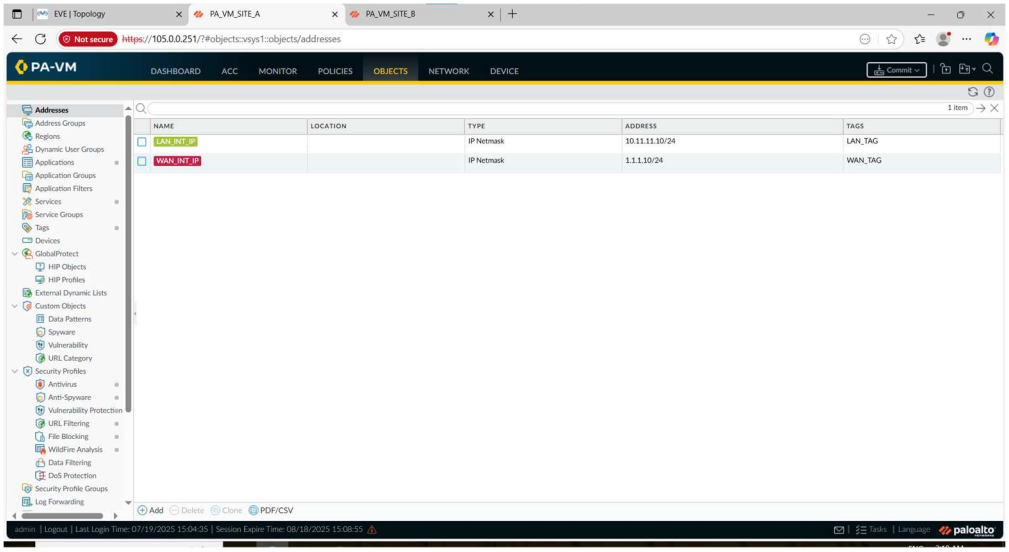


3. To create objects for ip address

Objects >Addresses>Add

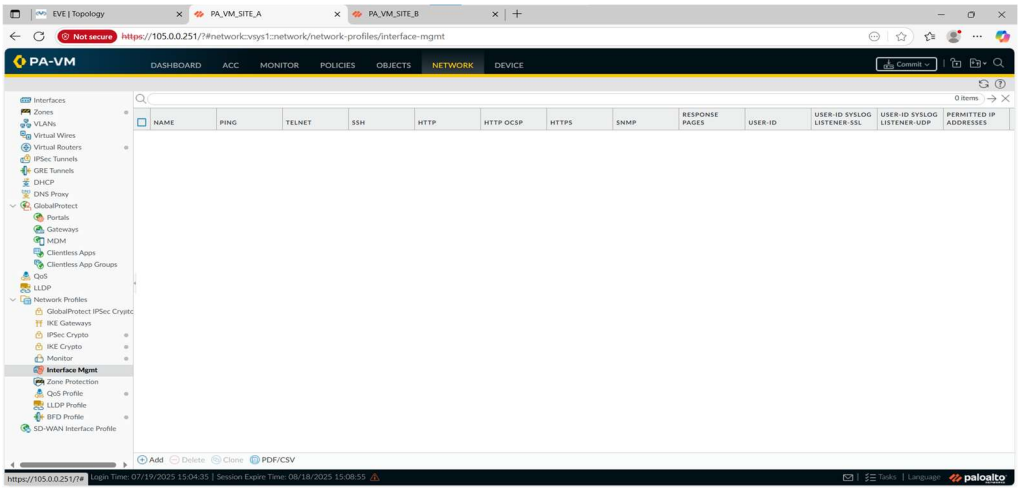


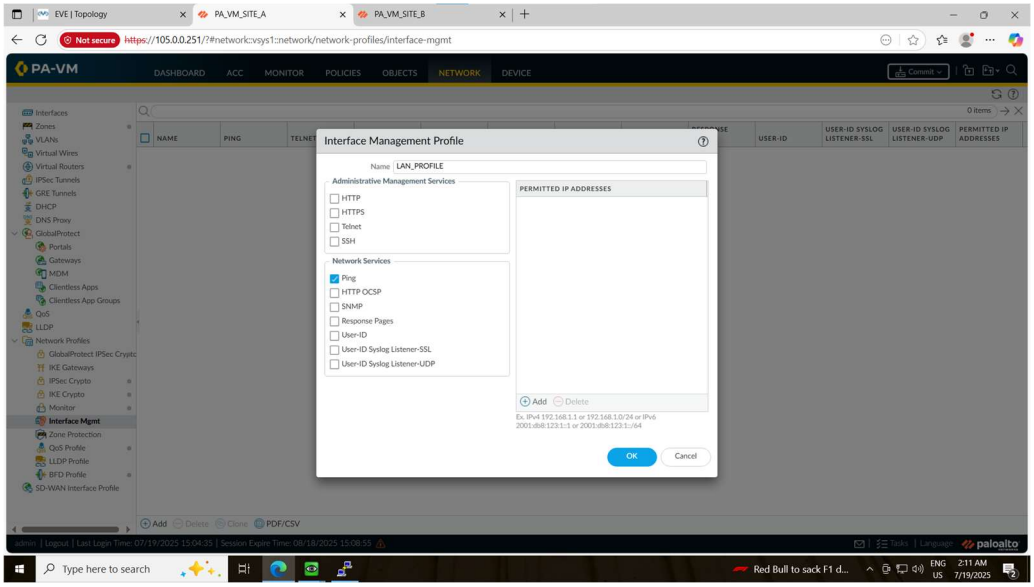


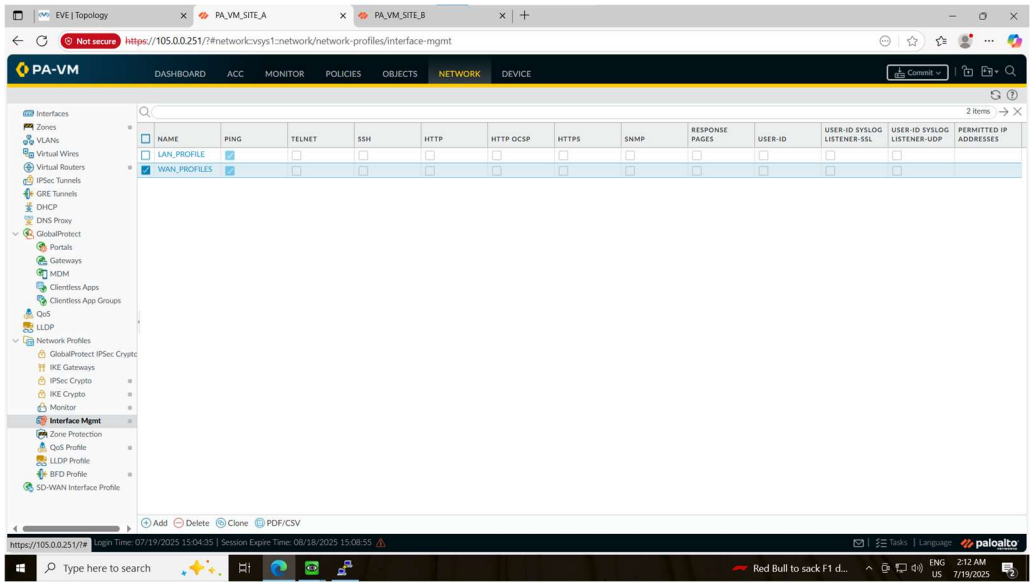


4. To create interface management profile (to enable particular services for given interface)

Network >network profile >interface Mgmt

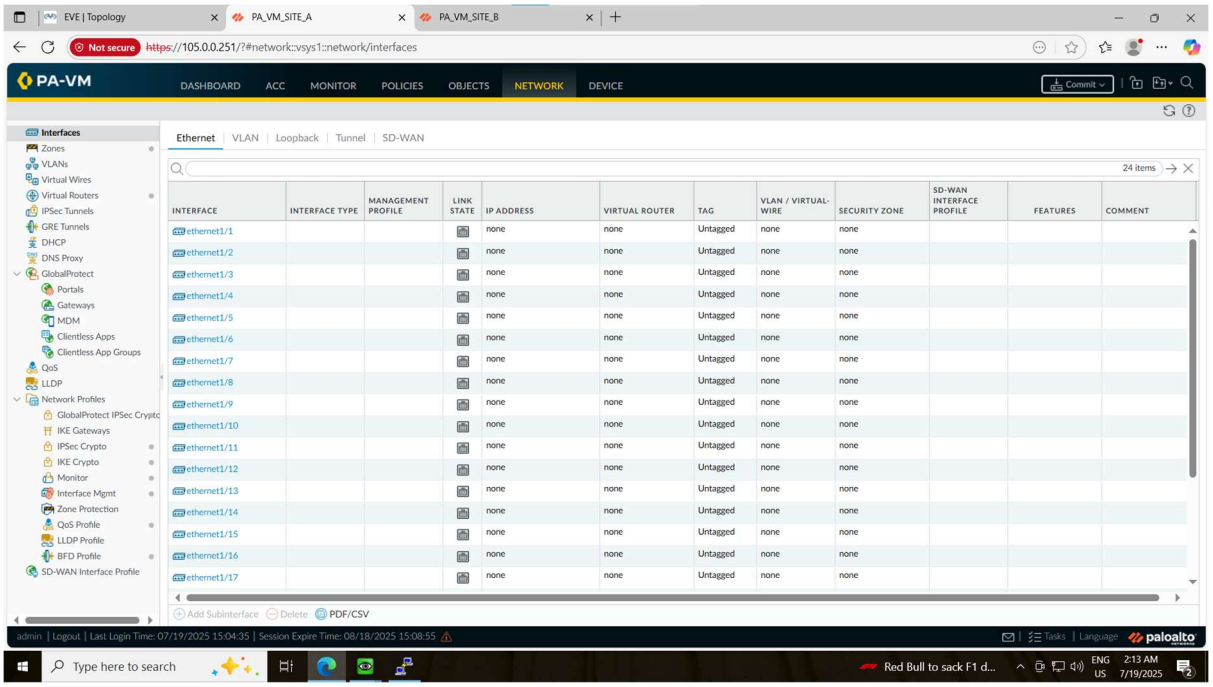


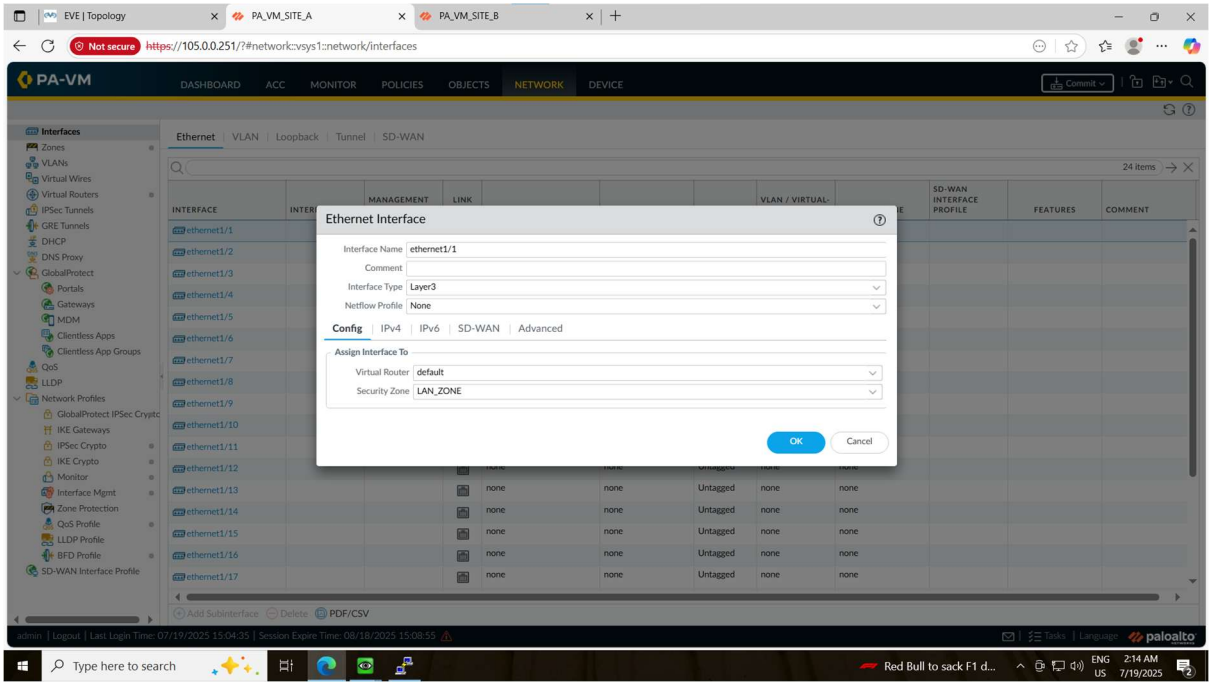


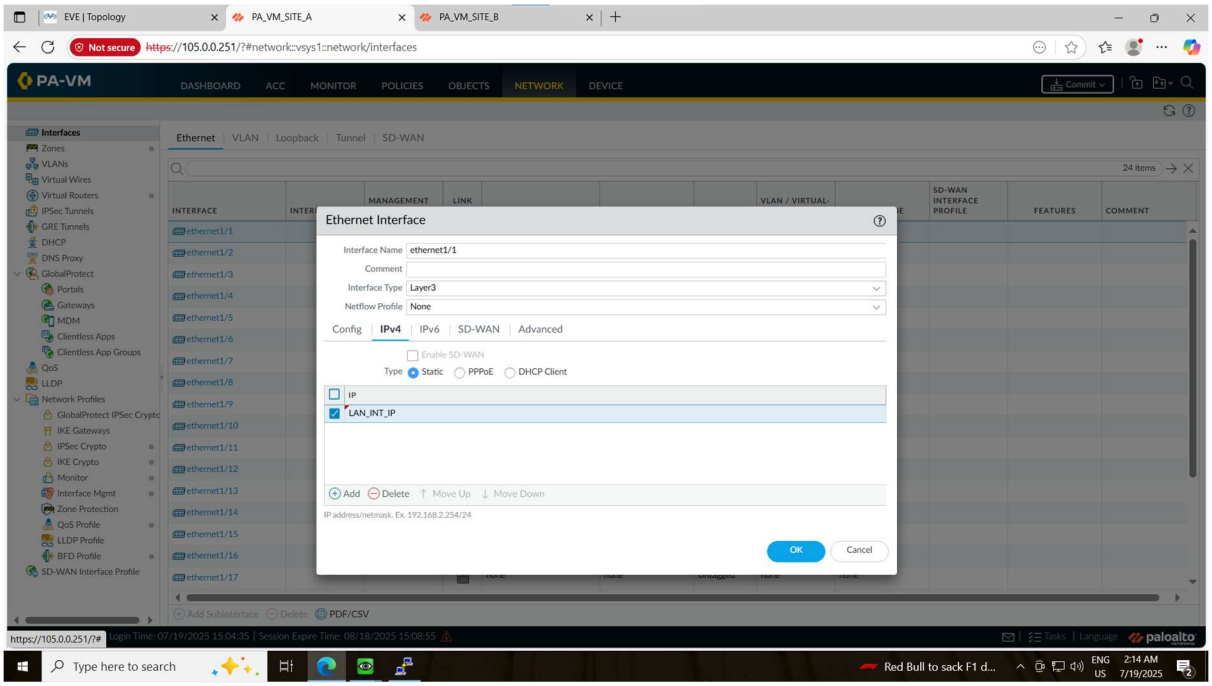


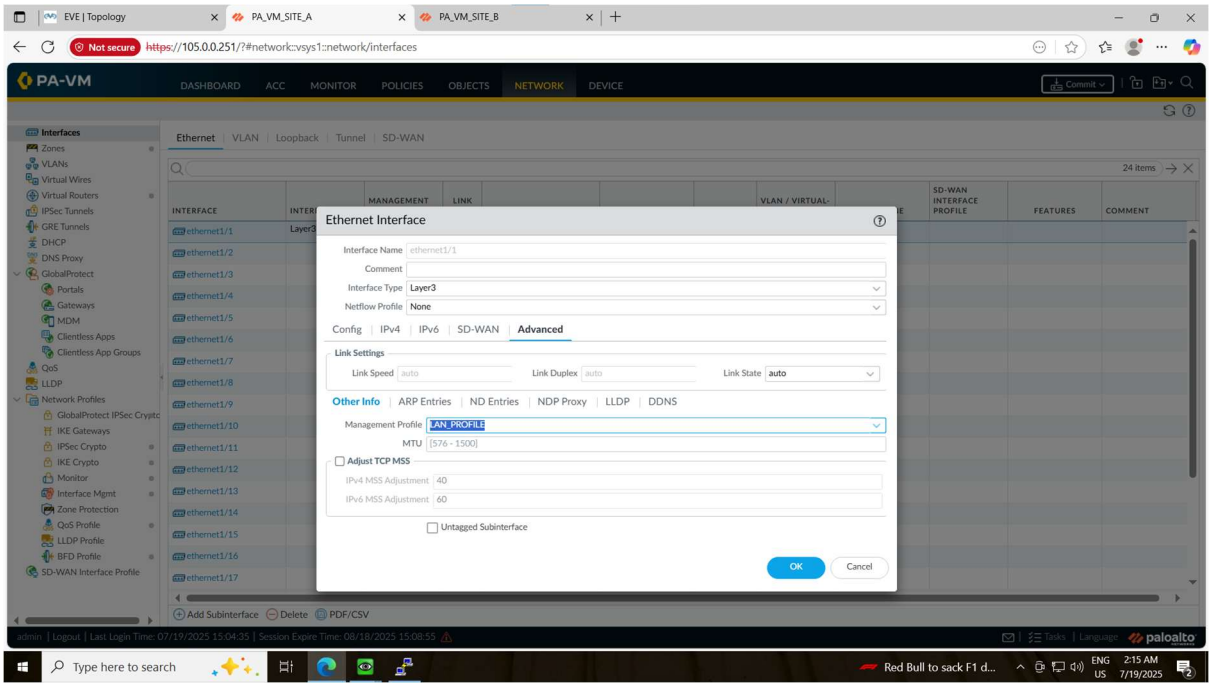
5. Assigning all above configuration to interface

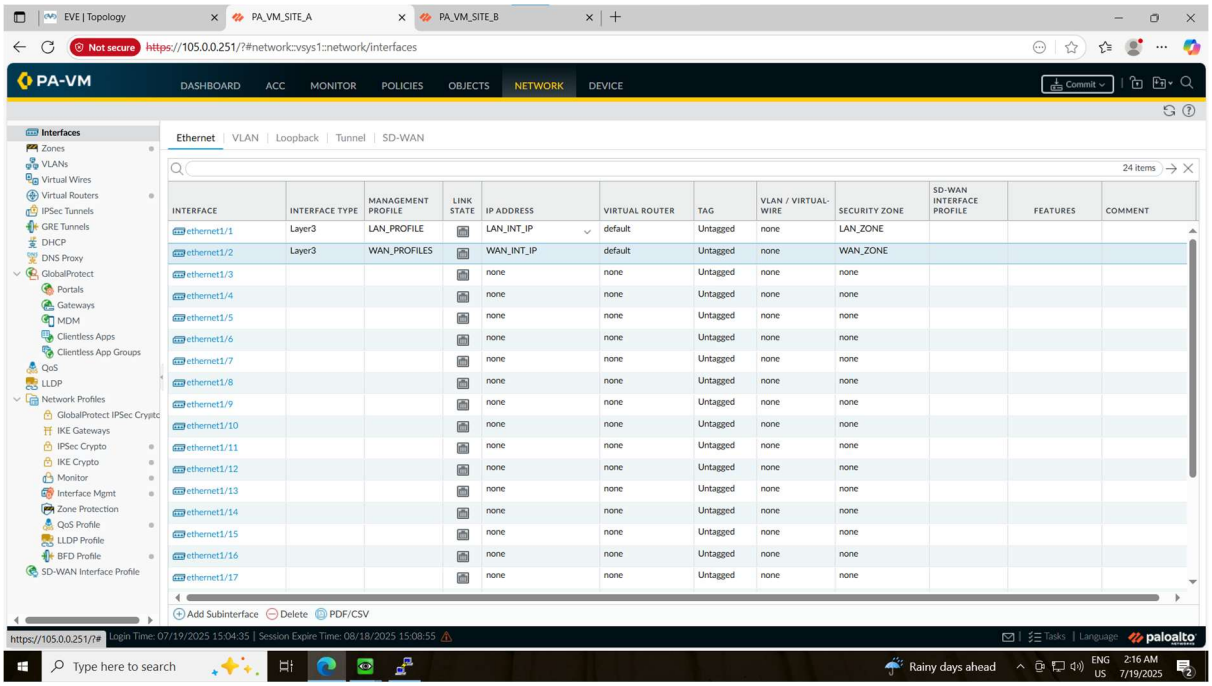
Network>interfaces>select interface





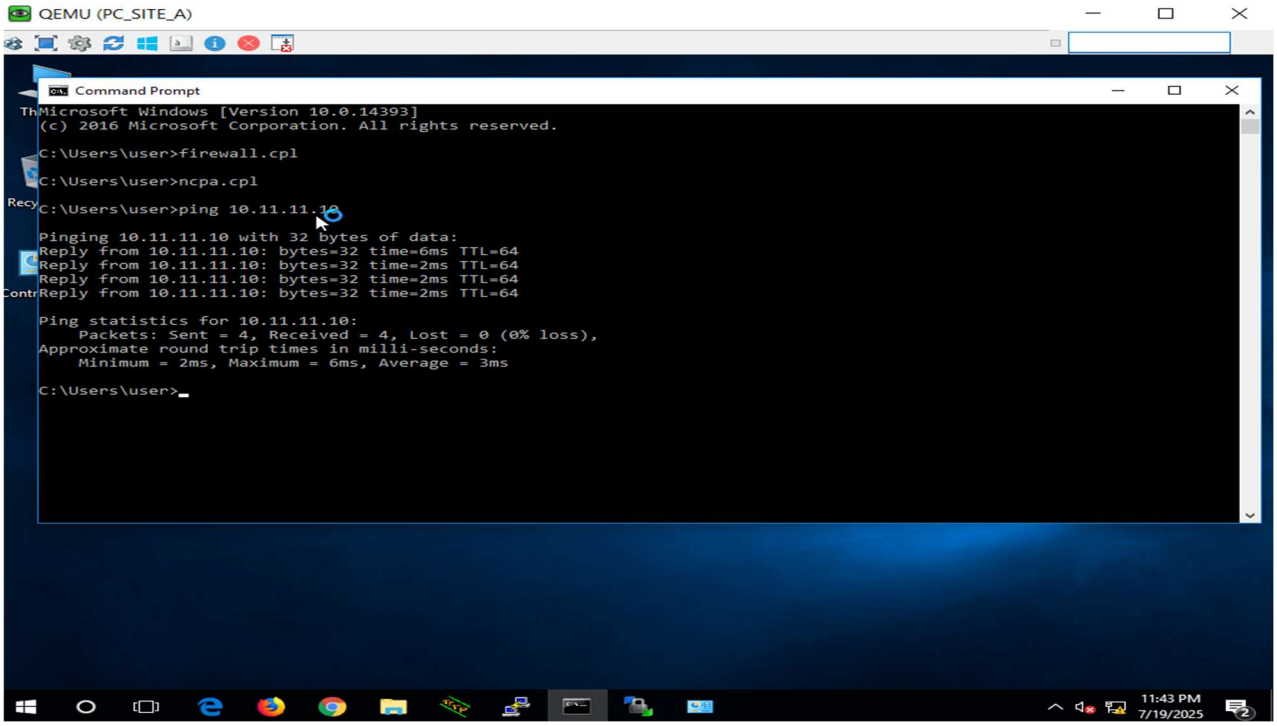

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/interfaces
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
24 items
INTERFACE
MANAGEMENT
LINK
VLAN / VIRTUAL-
SD-WAN INTERFACE PROFILE
FEATURES
COMMENT
ethernet1/1
ethernet1/2
ethernet1/3
ethernet1/4
ethernet1/5
ethernet1/6
ethernet1/7
ethernet1/8
ethernet1/9
ethernet1/10
ethernet1/11
ethernet1/12
ethernet1/13
ethernet1/14
ethernet1/15
ethernet1/16
ethernet1/17
Ethernet Interface
Interface Name ethernet1/1
Comment
Interface Type Layer3
Netflow Profile None
Config
IPv4
IPv6
SD-WAN
Advanced
Enable SD-WAN
Type Static PPPoE DHCP Client
IP
LAN_INT_IP
Add
Delete
Move Up
Move Down
IP address/netmask. Ex. 192.168.2.254/24
OK
Cancel
Add Subinterface
Delete
PDF/CSV
paloalto
Type here to search
Red Bull to sack F1 d...
ENG
US
2:14 AM
7/19/2025


EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/interfaces
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
24 items
INTERFACE
MANAGEMENT
LINK
VLAN / VIRTUAL-
SD-WAN INTERFACE PROFILE
FEATURES
COMMENT
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 LAN_PROFILE
MTU [576 - 1500]
Adjust TCP MSS
IPv4 MSS Adjustment 40
IPv6 MSS Adjustment 60
Untagged Subinterface
OK
Cancel
Add Subinterface
Delete
PDF/CSV
paloalto
Type here to search
Red Bull to sack F1 d...
ENG
US
2:15 AM
7/19/2025



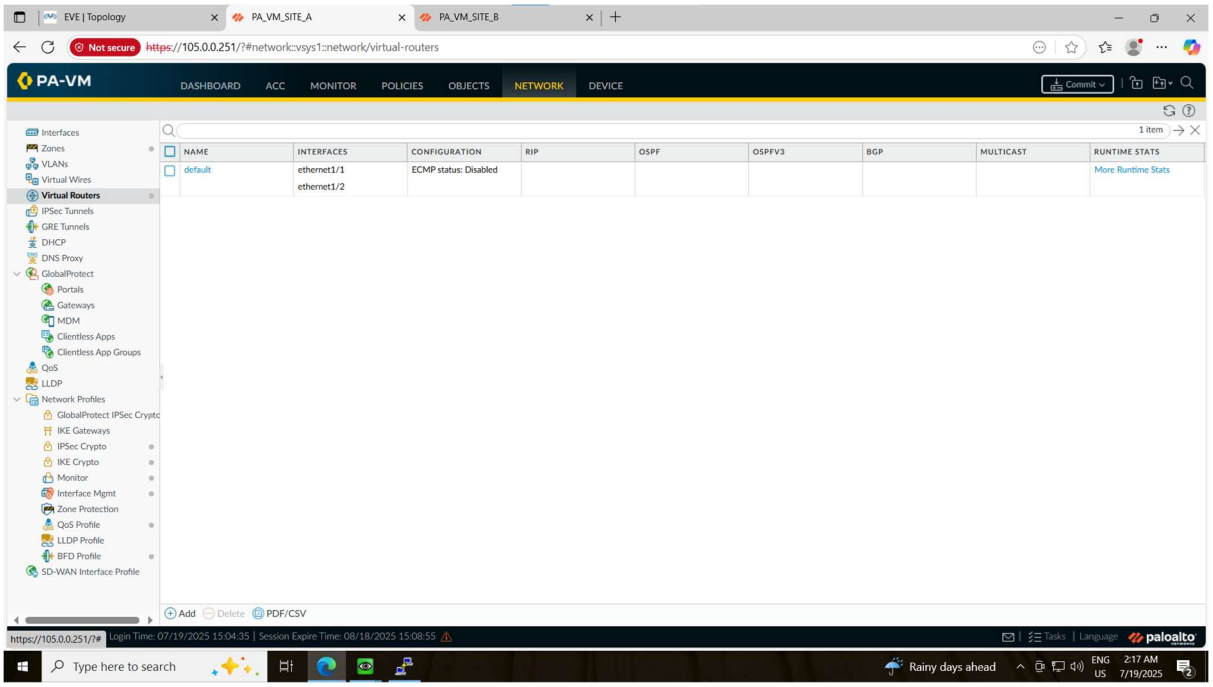
Apply commit for saving all changes

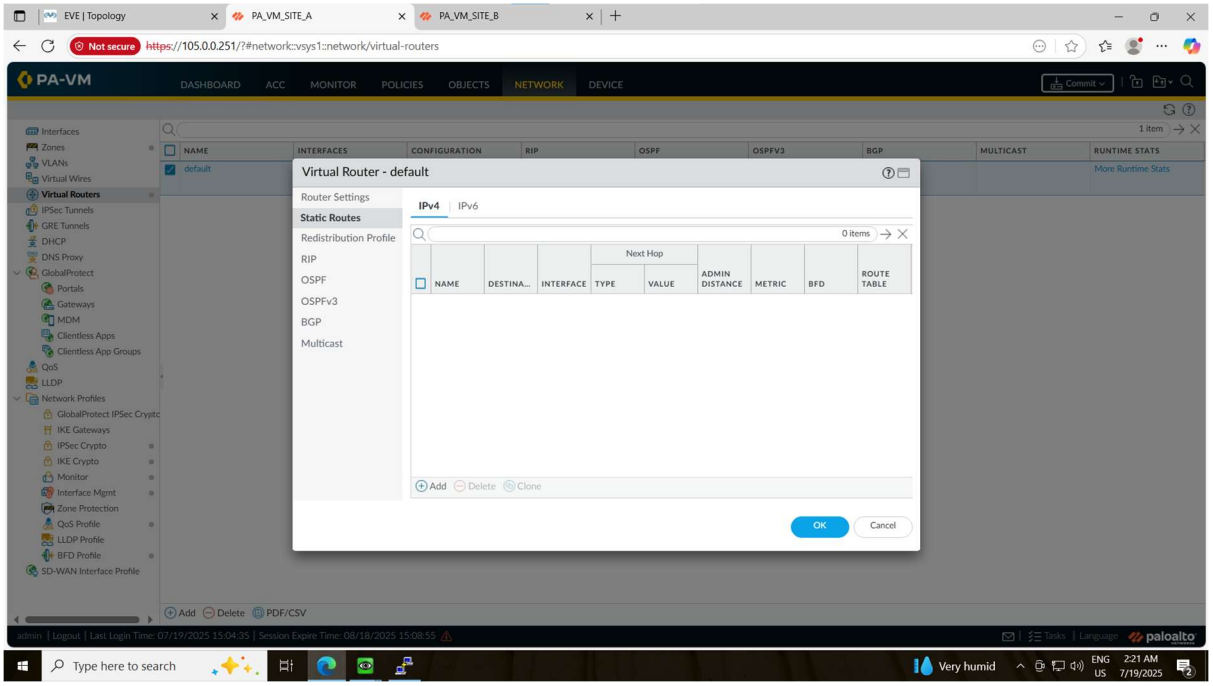
Check reachability from pc to firewall interface in same subnet

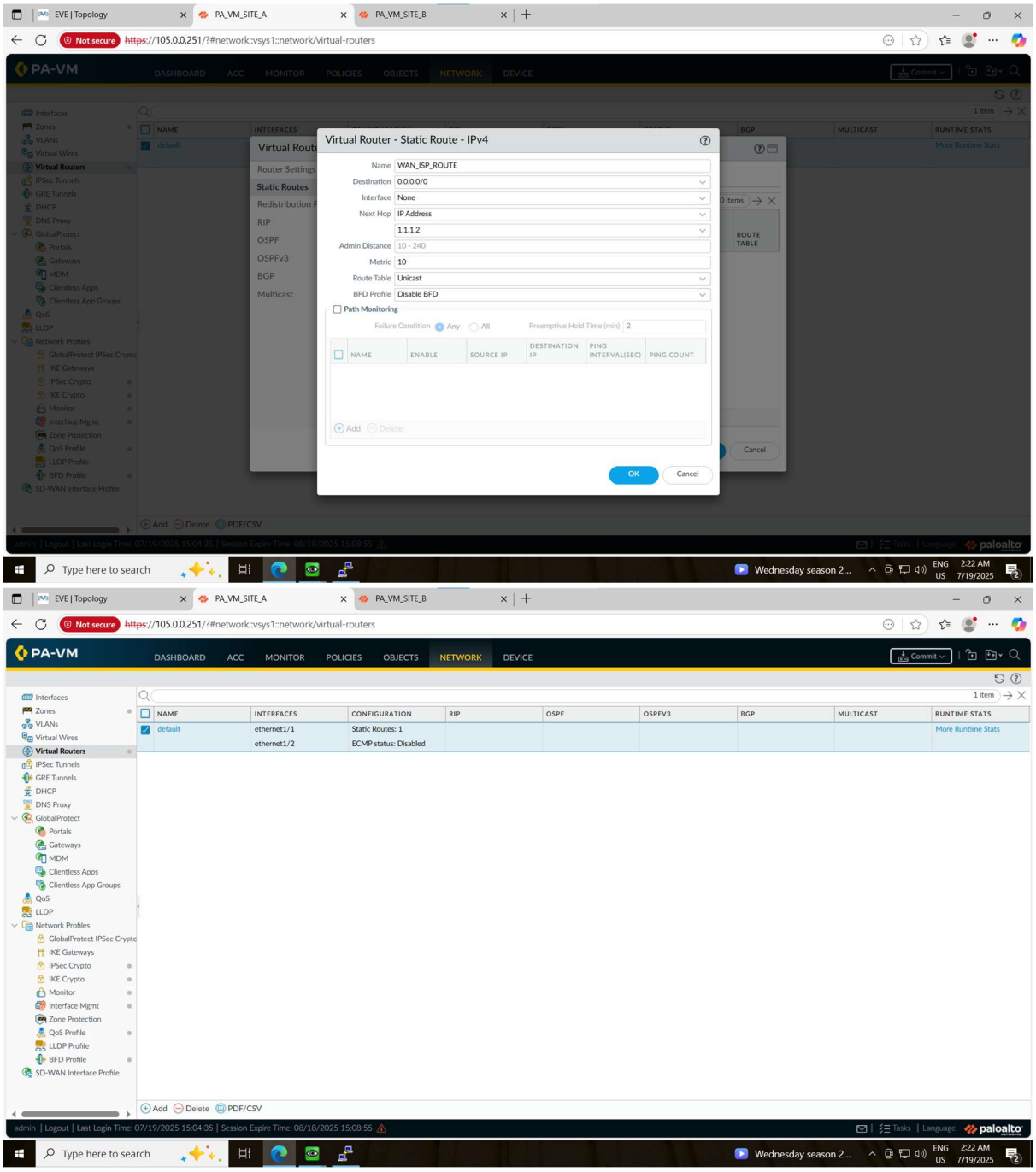


6. For public reachability from site a to b create default routing

Network>virtual routers>add







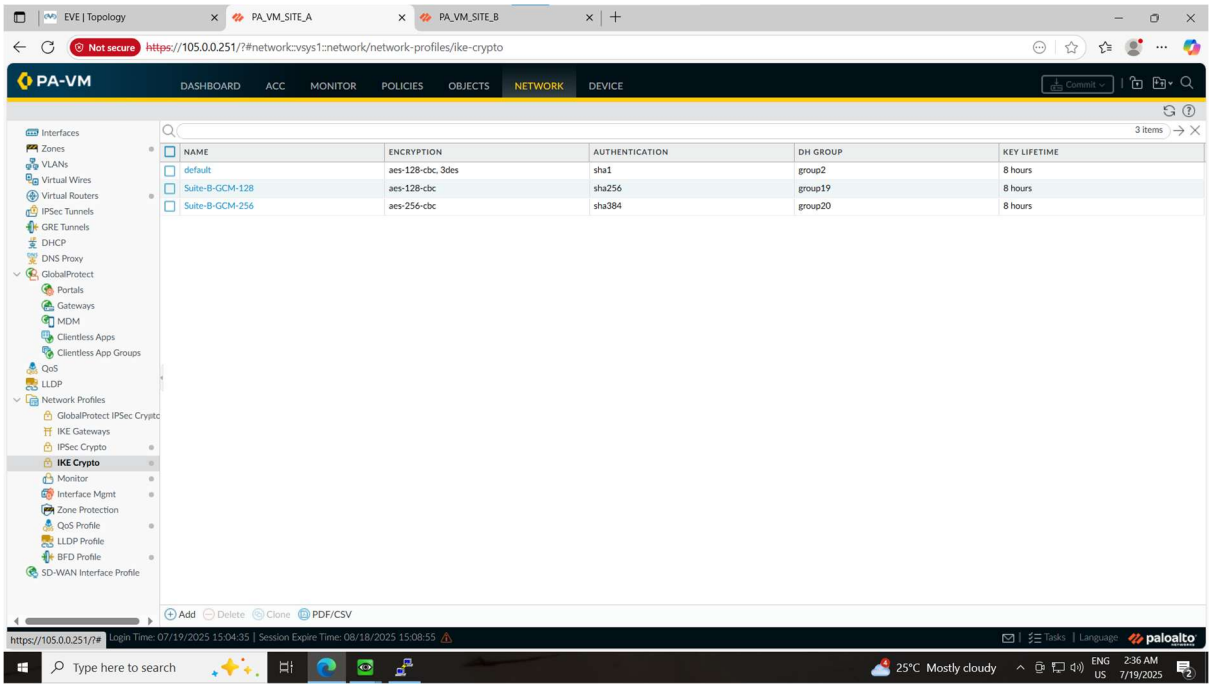
Check reachablity from site A to site b

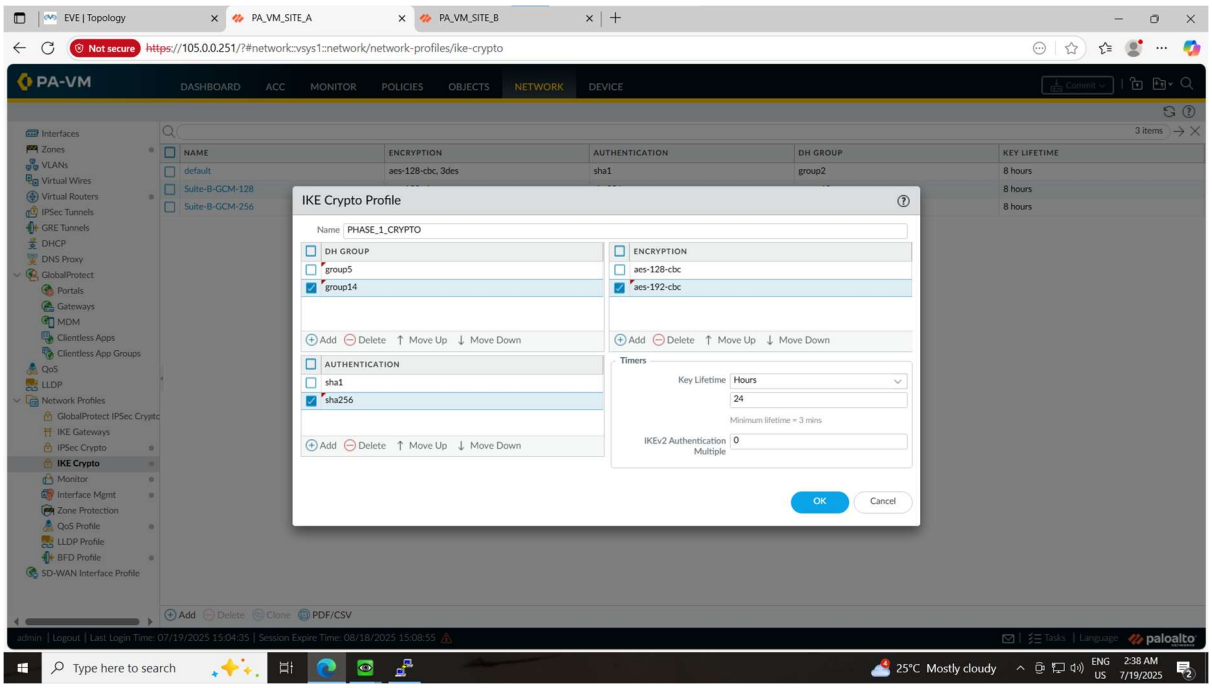
```
admin@PA_VM_SITE_A# run ping source 1.1.1.10 host 2.2.2.10
PING 2.2.2.10 (2.2.2.10) from 1.1.1.10 : 56(84) bytes of data.
64 bytes from 2.2.2.10: icmp_seq=1 ttl=63 time=31.9 ms
64 bytes from 2.2.2.10: icmp_seq=2 ttl=63 time=5.83 ms
64 bytes from 2.2.2.10: icmp_seq=3 ttl=63 time=7.28 ms
64 bytes from 2.2.2.10: icmp_seq=4 ttl=63 time=4.87 ms
64 bytes from 2.2.2.10: icmp_seq=5 ttl=63 time=4.95 ms
64 bytes from 2.2.2.10: icmp_seq=6 ttl=63 time=5.67 ms
^C
--- 2.2.2.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 4.872/10.092/31.933/9.799 ms
[edit]
admin@PA_VM_SITE_A#
```

7. VPN Configurations (Phase 1)

Step 1:

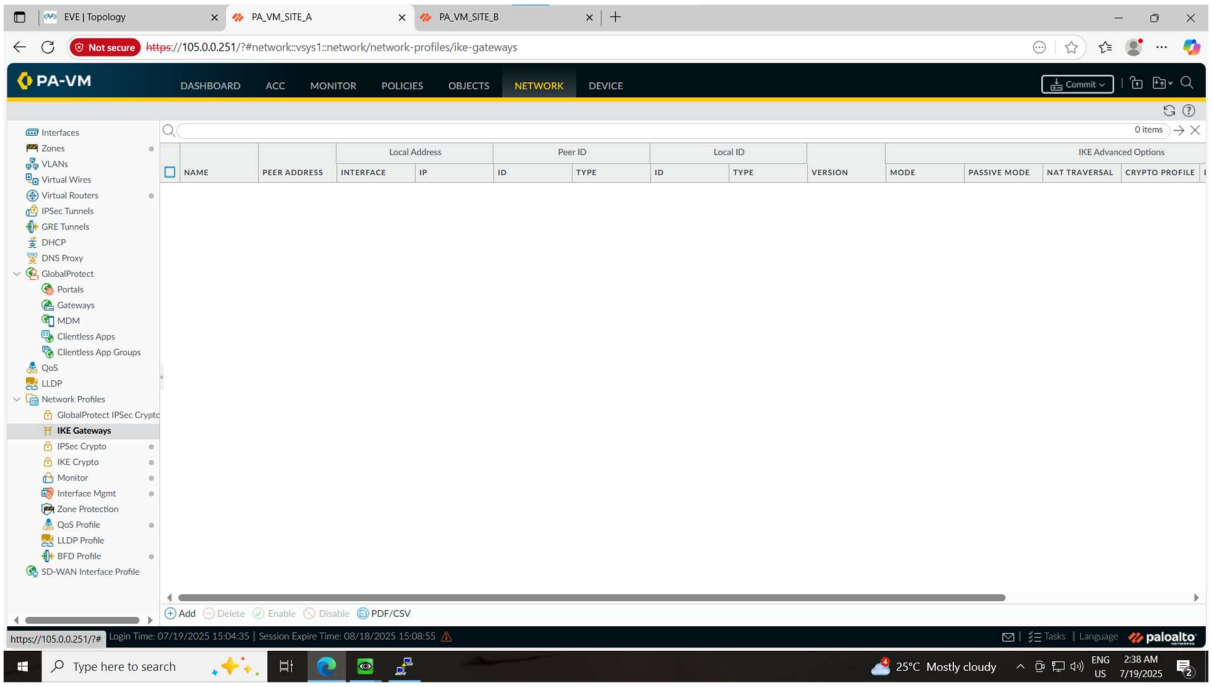
Network>network profile>IKE Crypto>

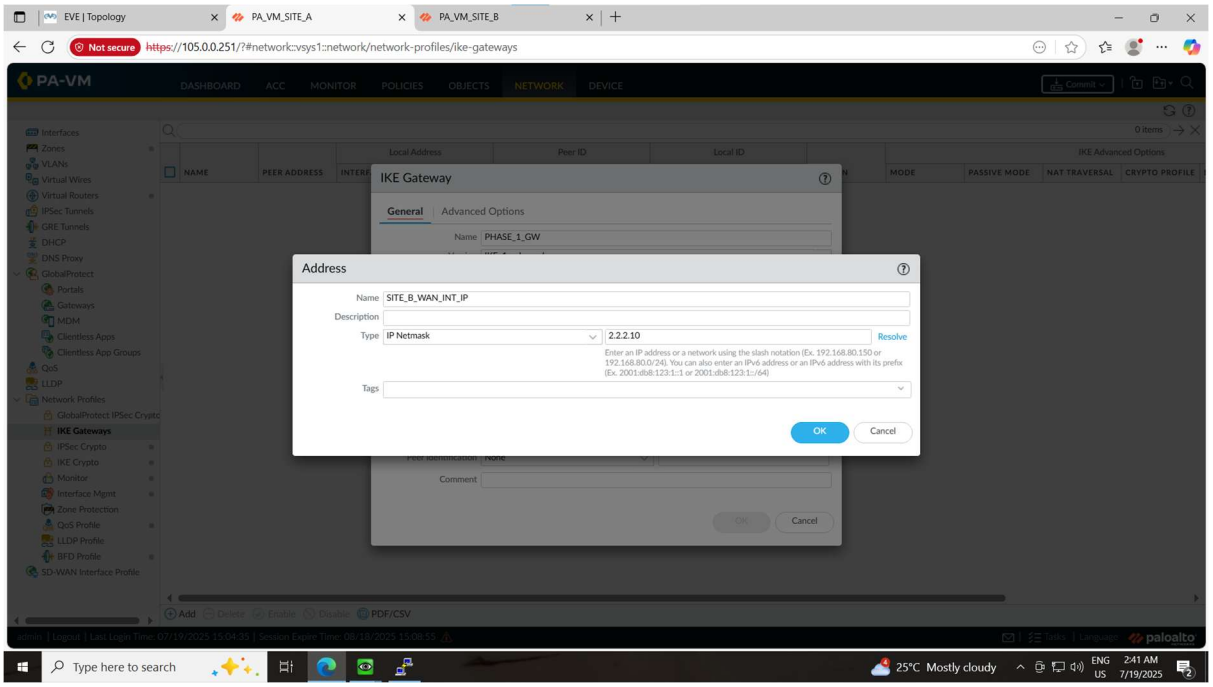


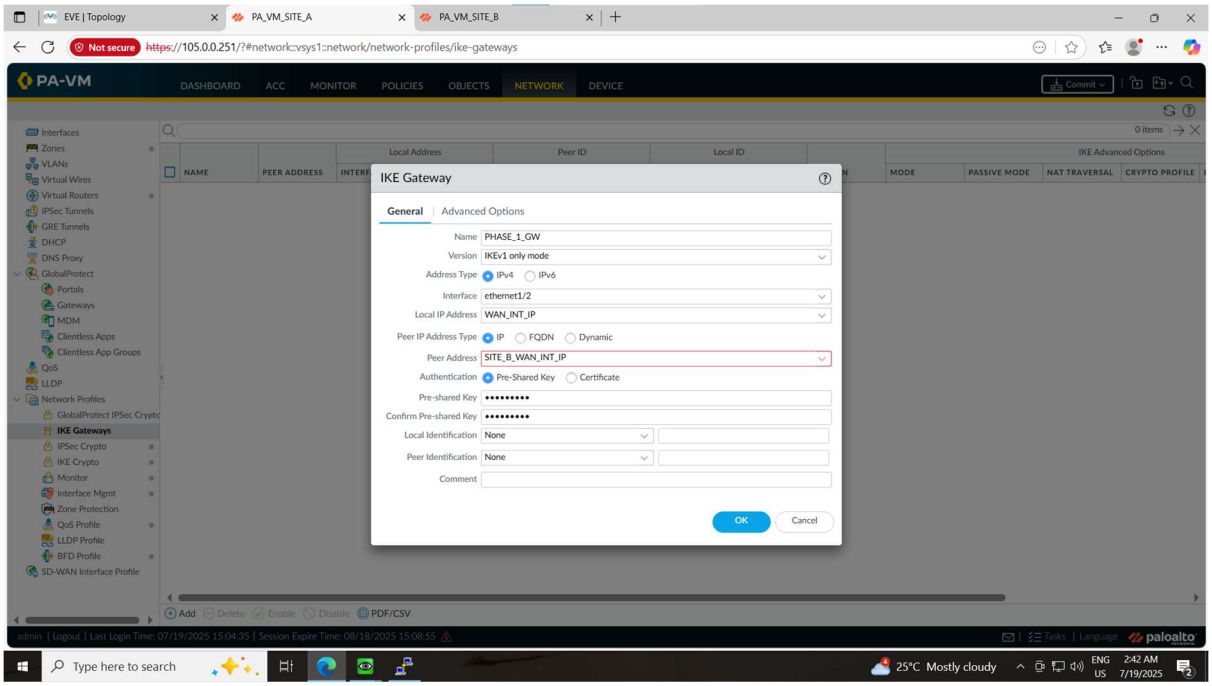


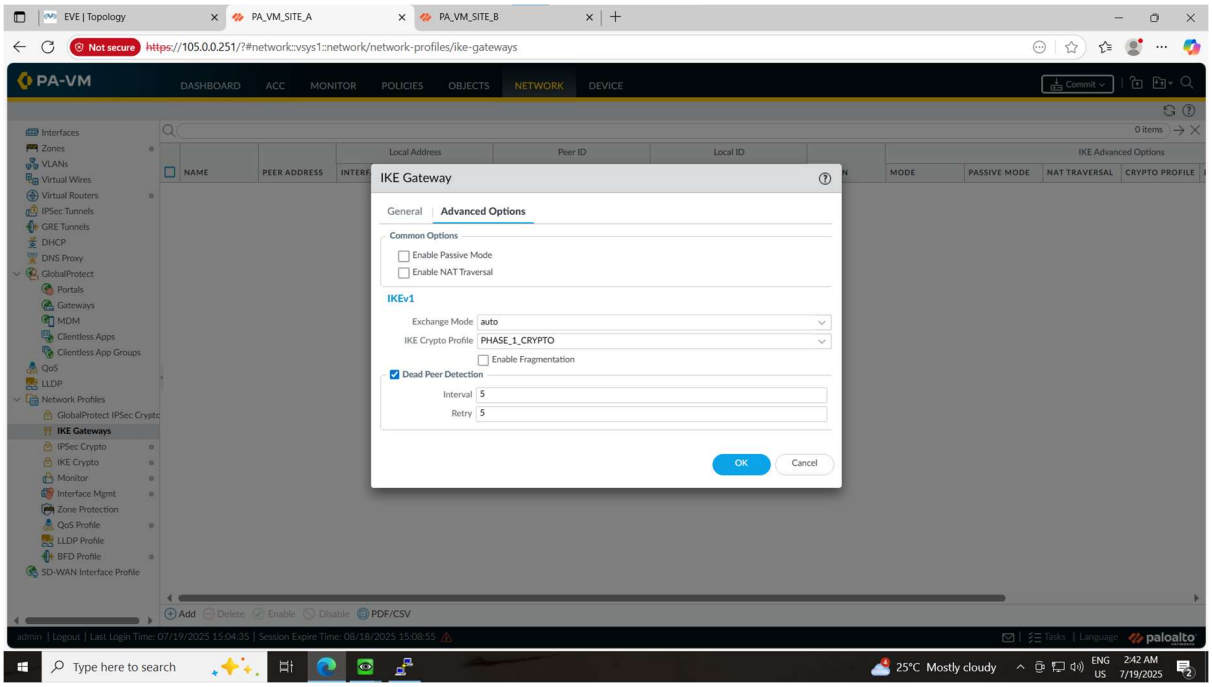
Step 2:

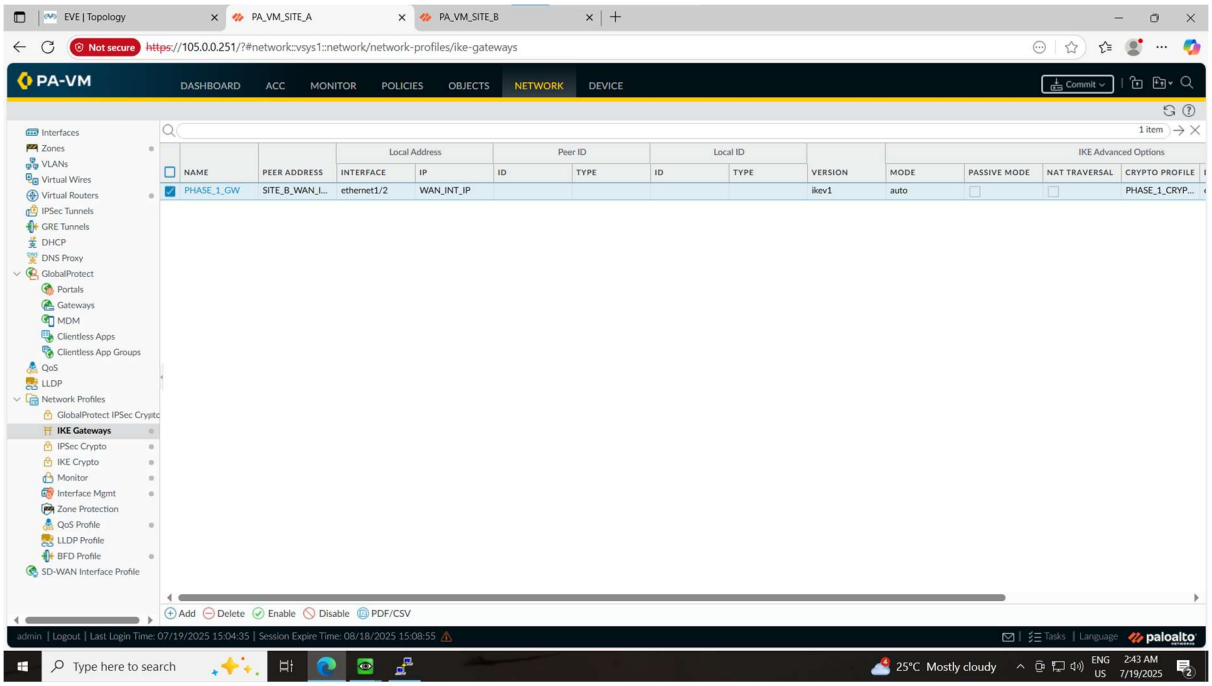
Network>network profile>IKE Gateways






EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/network-profiles/ike-gateways
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
IKE Gateway
General
Advanced Options
Name PHASE_1_GW
Version IKEv1 only mode
Address Type IPv4 IPv6
Interface ethernet1/2
Local IP Address WAN_INT_IP
Peer IP Address Type IP FQDN Dynamic
Peer Address SITE_B_WAN_INT_IP
Authentication Pre-Shared Key Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification None
Peer Identification None
Comment
OK
Cancel
Type here to search
25°C Mostly cloudy
ENG US
2:42 AM 7/19/2025

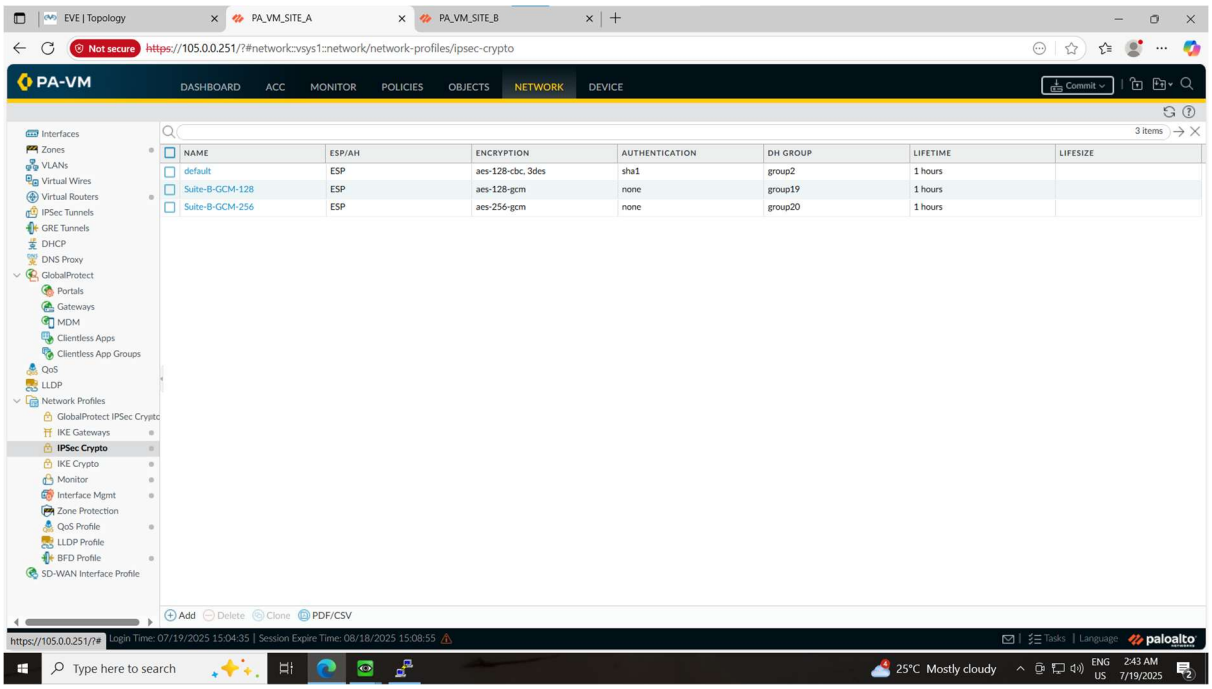

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/network-profiles/ike-gateways
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
IKE Gateway
General
Advanced Options
Common Options
Enable Passive Mode
Enable NAT Traversal
IKEv1
Exchange Mode auto
IKE Crypto Profile PHASE_1_CRYPTO
Enable Fragmentation
Dead Peer Detection
Interval 5
Retry 5
OK
Cancel
Type here to search
25°C Mostly cloudy
ENG US
2:42 AM 7/19/2025

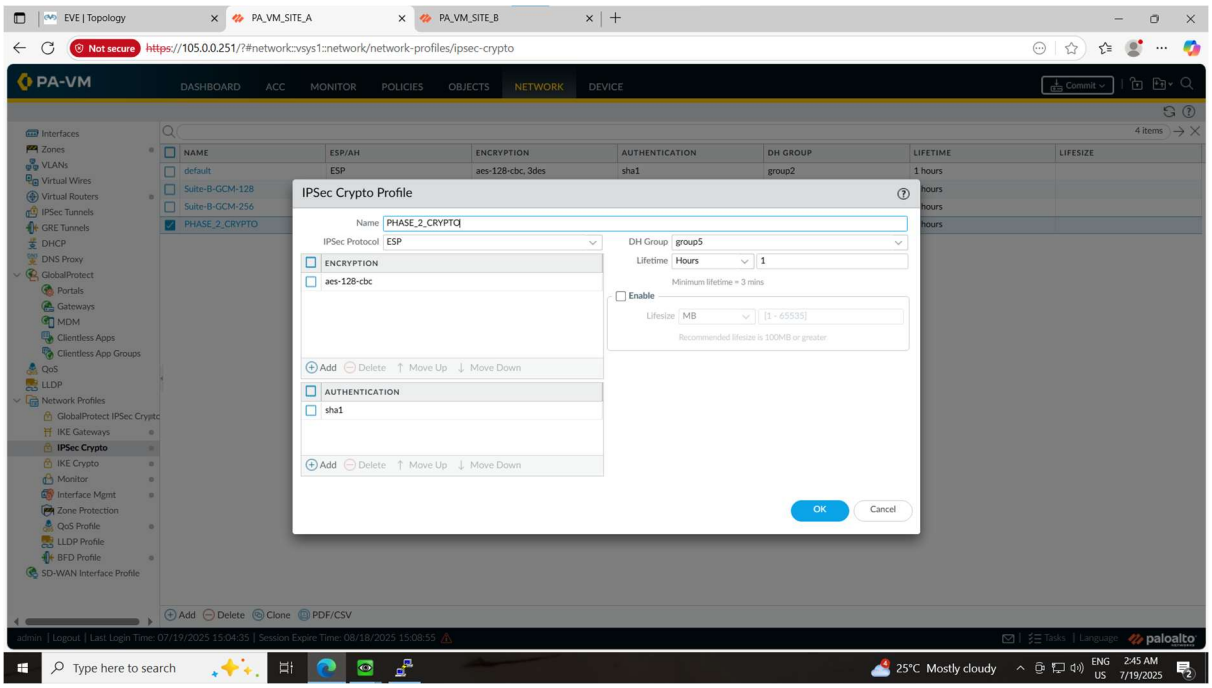

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/network-profiles/ike-gateways
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
1 item
Local Address
Peer ID
Local ID
IKE Advanced Options
NAME
PEER ADDRESS
INTERFACE
IP
ID
TYPE
ID
TYPE
VERSION
MODE
PASSIVE MODE
NAT TRAVERSAL
CRYPTO PROFILE
PHASE_1_GW
SITE_B_WAN_I...
ethernet1/2
WAN_INT_IP
ikev1
auto
PHASE_1_CRYP...
Add
Delete
Enable
Disable
PDF/CSV
admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55
Tasks
Language
paloalto
Type here to search
25°C Mostly cloudy
ENG
US
2:43 AM
7/19/2025

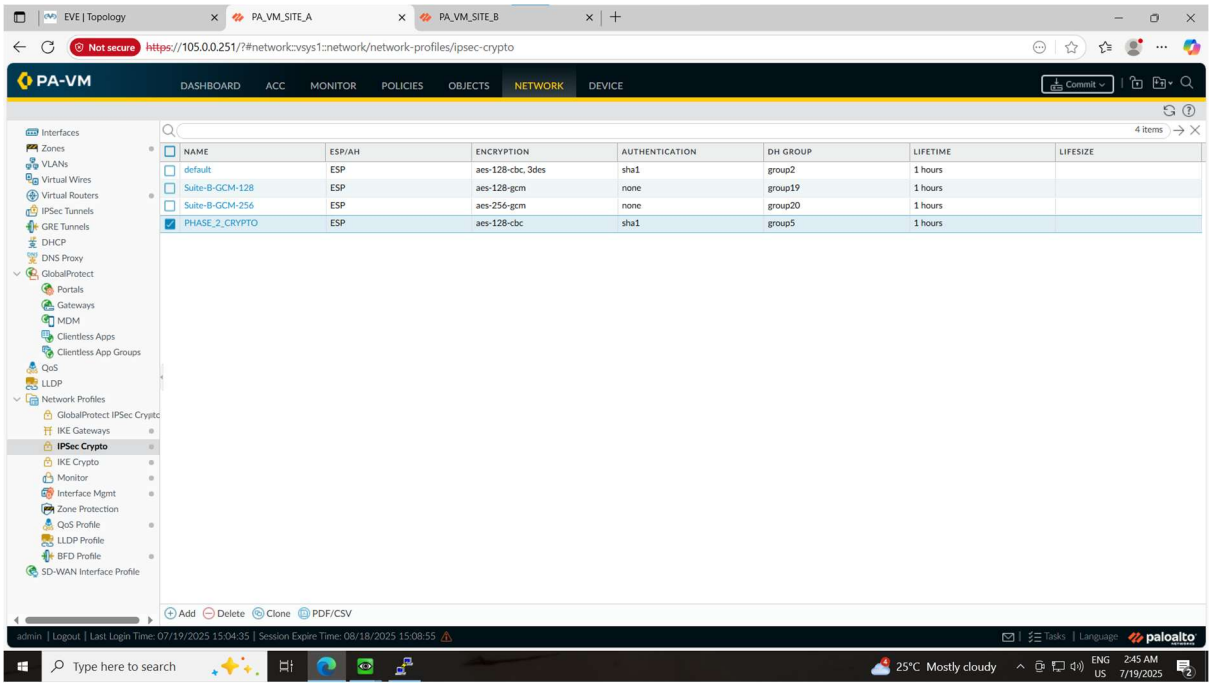
8. VPN Configurations (Phase 2)

Step 1:

Network>network>profile>IPsec Crypto



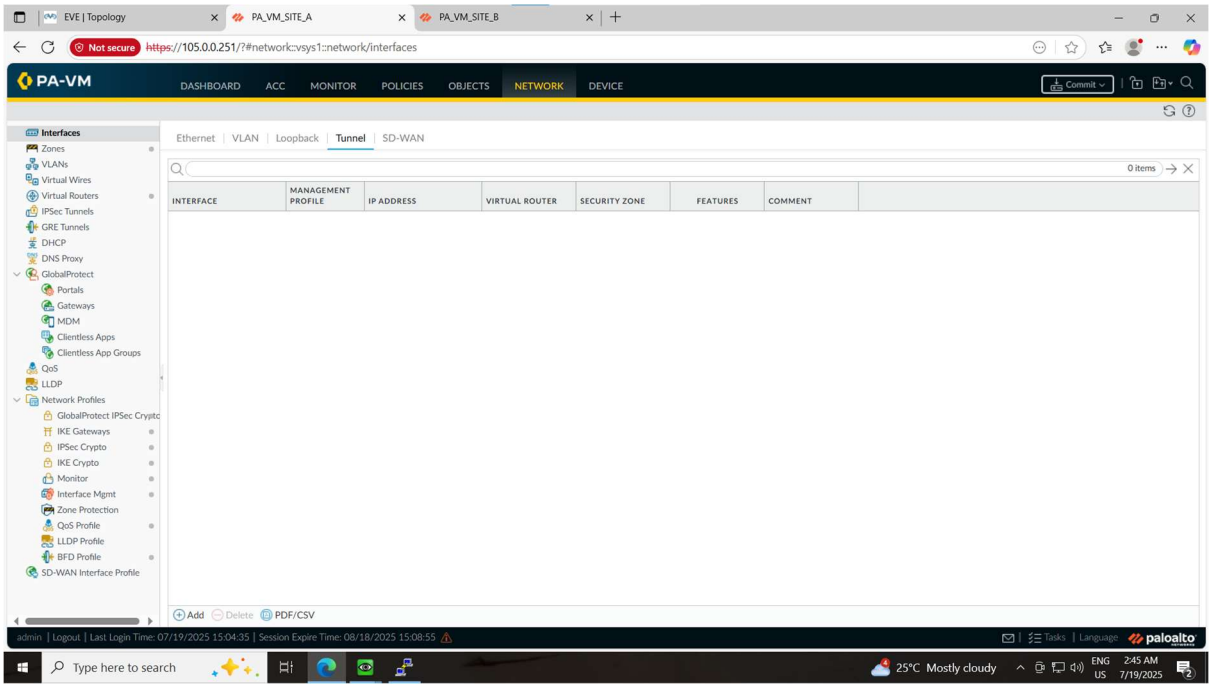


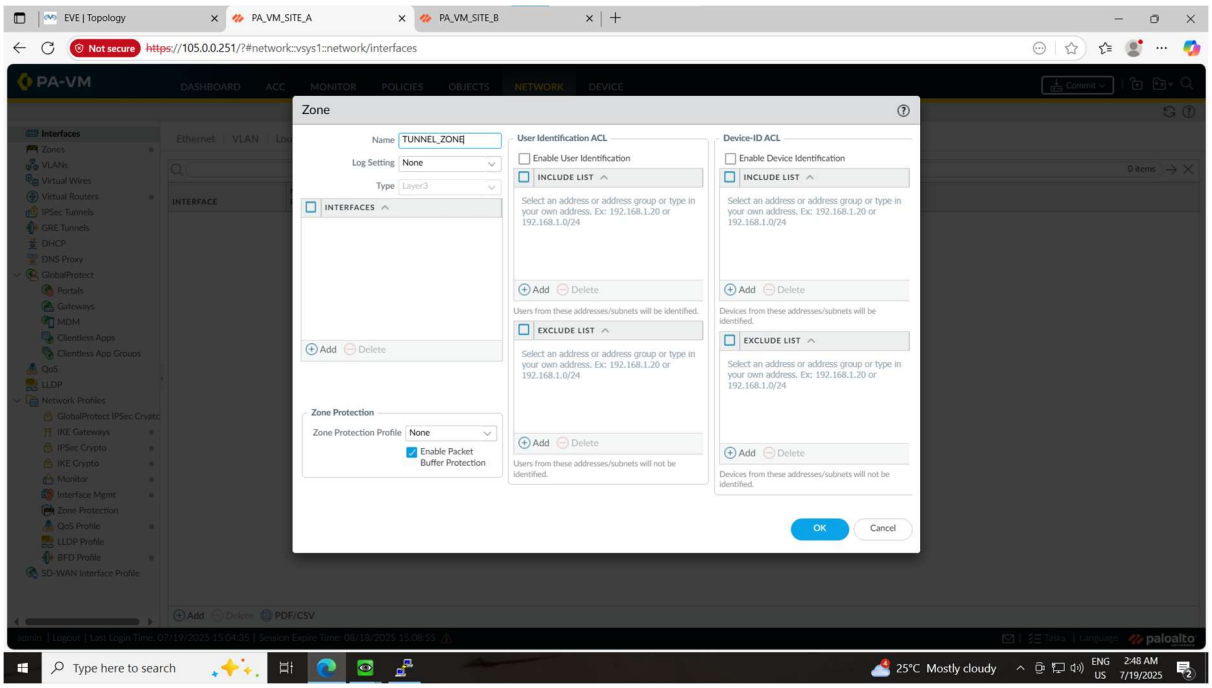

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/network-profiles/ipsec-crypto
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
4 items
NAME
ESP/AH
ENCRYPTION
AUTHENTICATION
DH GROUP
LIFETIME
LIFESIZE
default
ESP
aes-128-cbc, 3des
sha1
group2
1 hours
Suite-B-GCM-128
ESP
aes-128-gcm
none
group19
1 hours
Suite-B-GCM-256
ESP
aes-256-gcm
none
group20
1 hours
PHASE_2_CRYPTO
ESP
aes-128-cbc
sha1
group5
1 hours
Add
Delete
Clone
PDF/CSV
admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55
Tasks
Language
paloalto
Type here to search
25°C Mostly cloudy
ENG
US
2:45 AM
7/19/2025

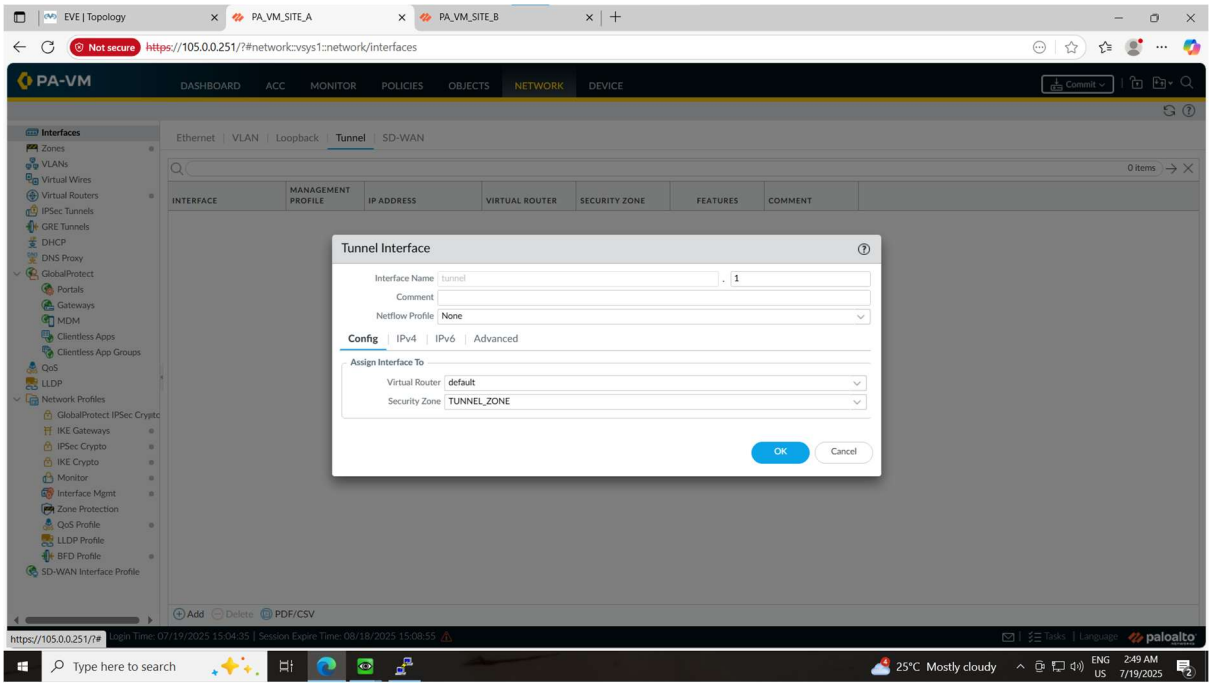
Step:2

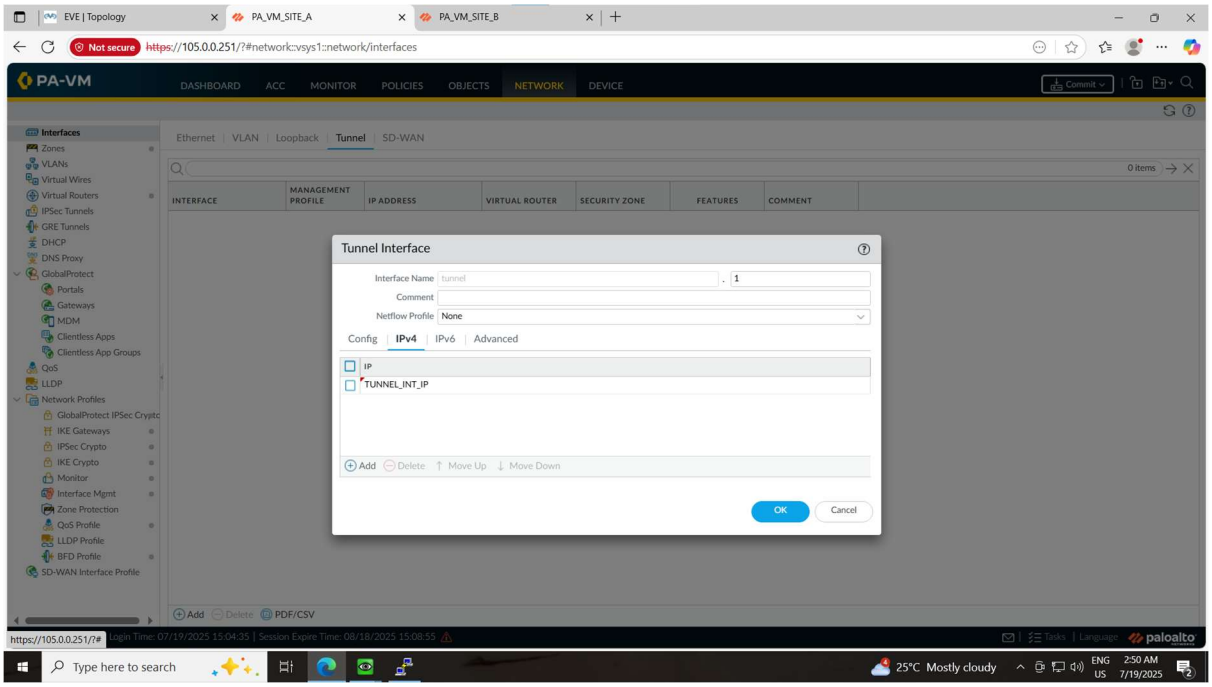
To create tunnel

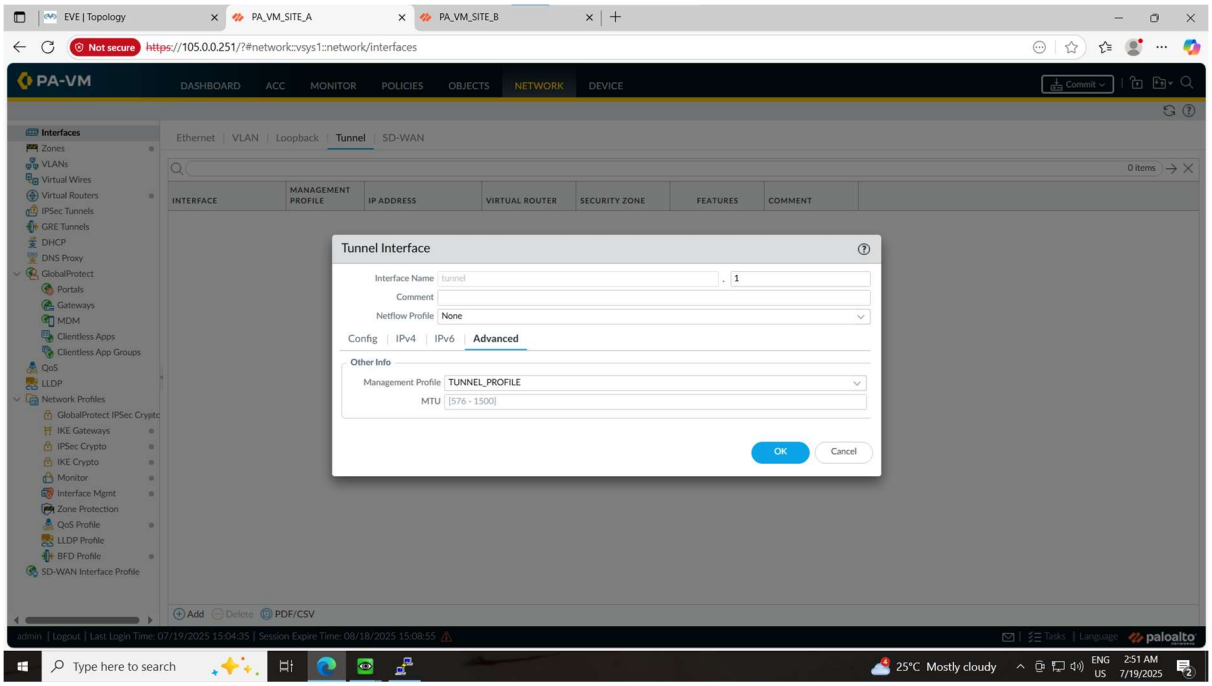
Network>interfaces>tunnel>add





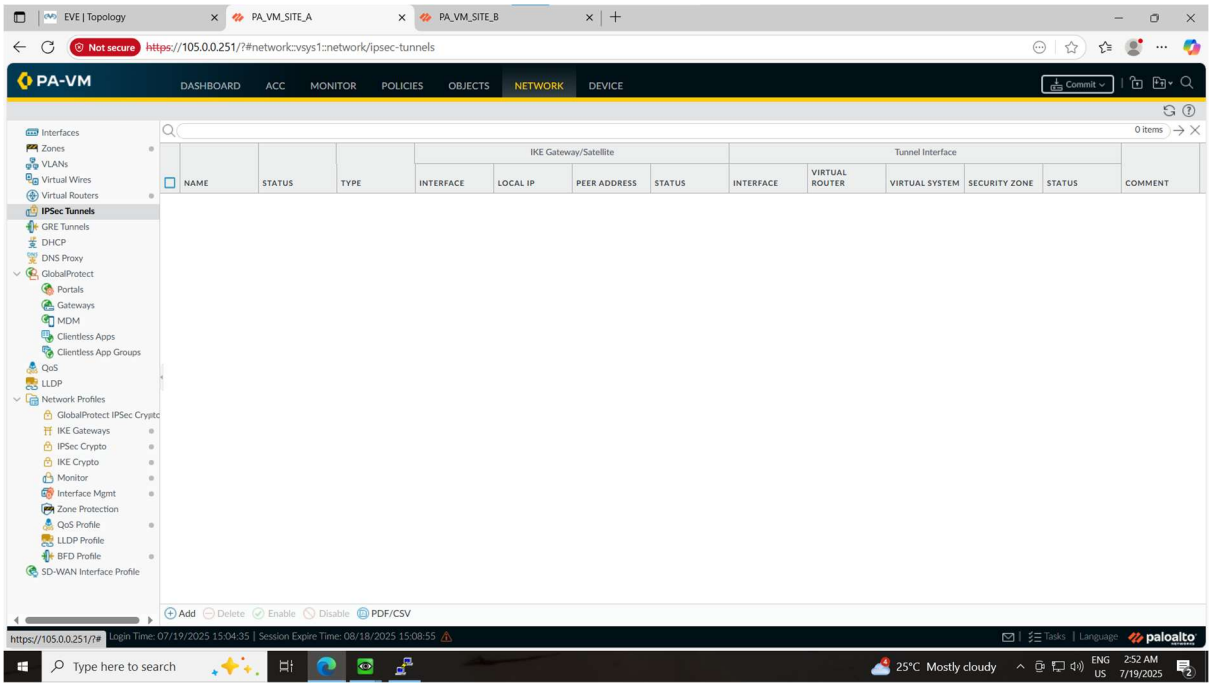

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/interfaces
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
0 items
INTERFACE
MANAGEMENT PROFILE
IP ADDRESS
VIRTUAL ROUTER
SECURITY ZONE
FEATURES
COMMENT
Tunnel Interface
Interface Name
tunnel
1
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router
default
Security Zone
TUNNEL_ZONE
OK
Cancel
Add
Delete
PDF/CSV
https://105.0.0.251/#
Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55
Tasks
Language
paloalto
Type here to search
25°C Mostly cloudy
ENG
US
2:49 AM
7/19/2025

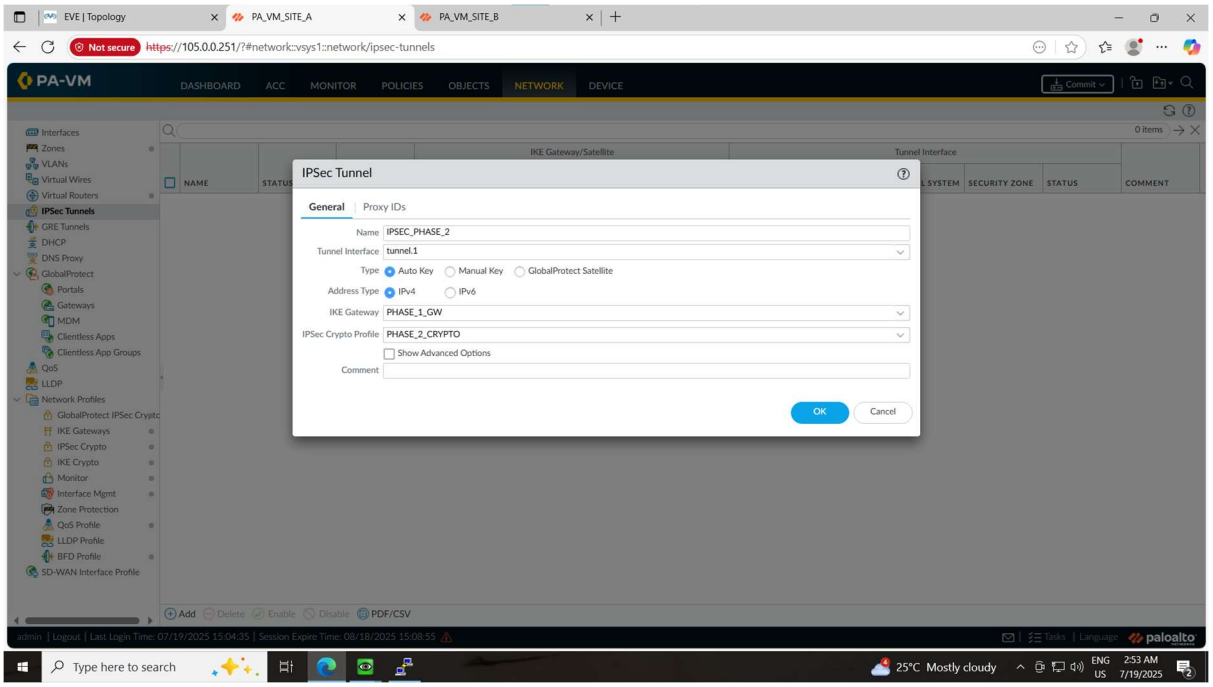

EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/interfaces
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
0 items
INTERFACE
MANAGEMENT PROFILE
IP ADDRESS
VIRTUAL ROUTER
SECURITY ZONE
FEATURES
COMMENT
Tunnel Interface
Interface Name
tunnel
1
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
IP
TUNNEL_INT_IP
Add
Delete
Move Up
Move Down
OK
Cancel
Add
Delete
PDF/CSV
https://105.0.0.251/#
Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55
Tasks
Language
paloalto
Type here to search
25°C Mostly cloudy
ENG
US
2:50 AM
7/19/2025


EVE | Topology
PA_VM_SITE_A
PA_VM_SITE_B
Not secure
https://105.0.0.251/?#network::vsys1::network/interfaces
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
SD-WAN Interface Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
0 items
INTERFACE
MANAGEMENT PROFILE
IP ADDRESS
VIRTUAL ROUTER
SECURITY ZONE
FEATURES
COMMENT
Tunnel Interface
Interface Name
tunnel
1
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Other Info
Management Profile
TUNNEL_PROFILE
MTU
[576 - 1500]
OK
Cancel
Add
Delete
PDF/CSV
admin | Logout | Last Login Time: 07/19/2025 15:04:35 | Session Expire Time: 08/18/2025 15:08:55
Tasks
Language
paloalto
Type here to search
25°C Mostly cloudy
ENG
US
2:51 AM
7/19/2025

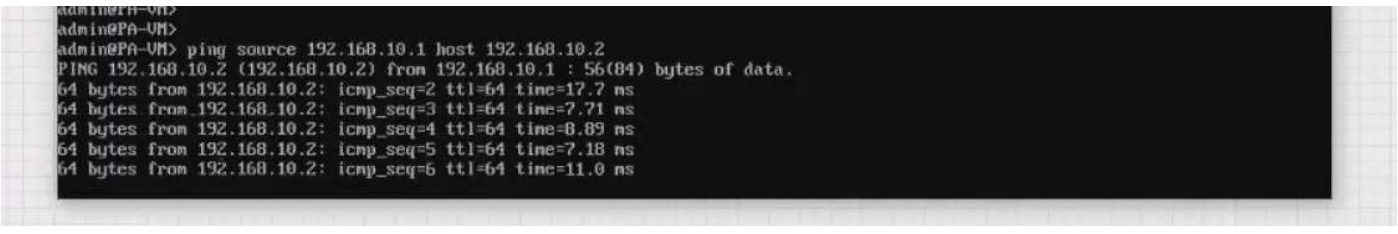
Step 3:

Network>IPsec Tunnels> Add



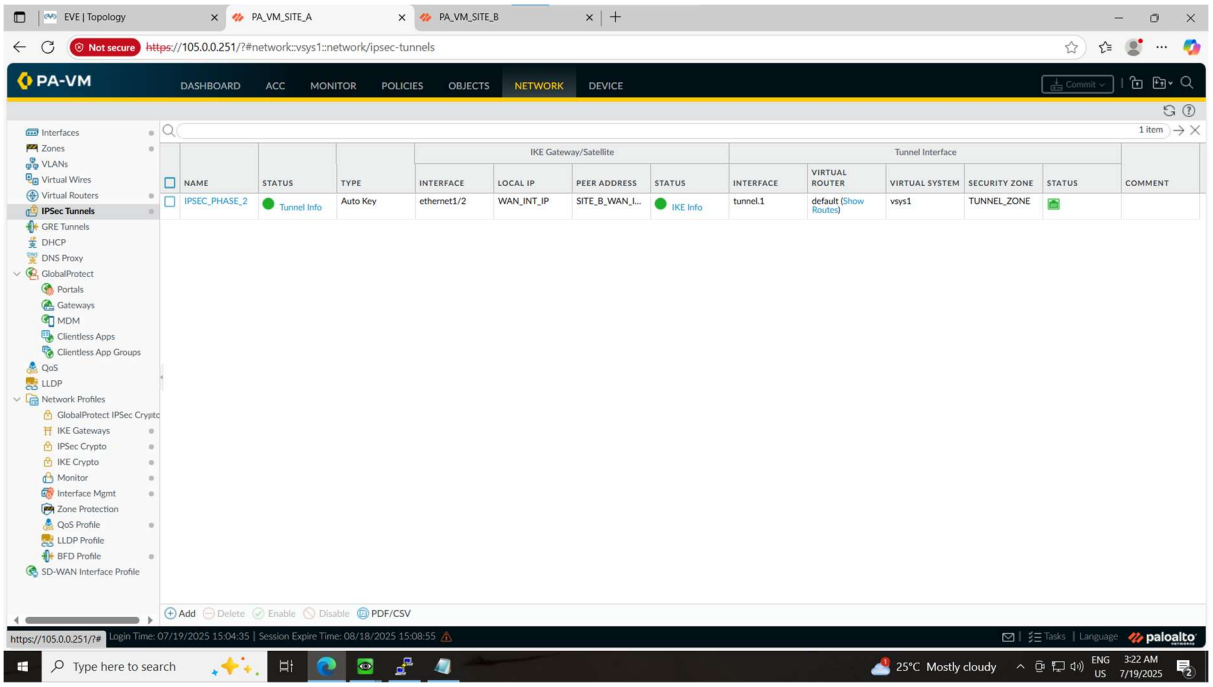


Commit changes and try to ping



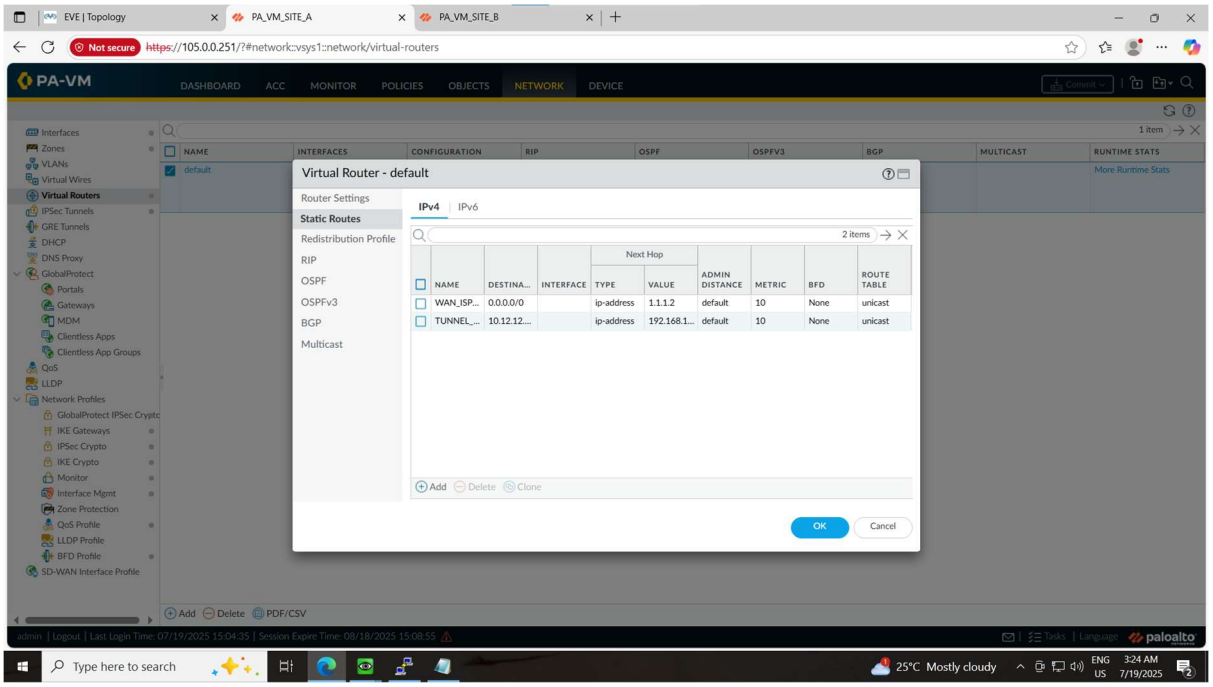
If it can ping, then your tunnel status will turn from red to green

As follows:

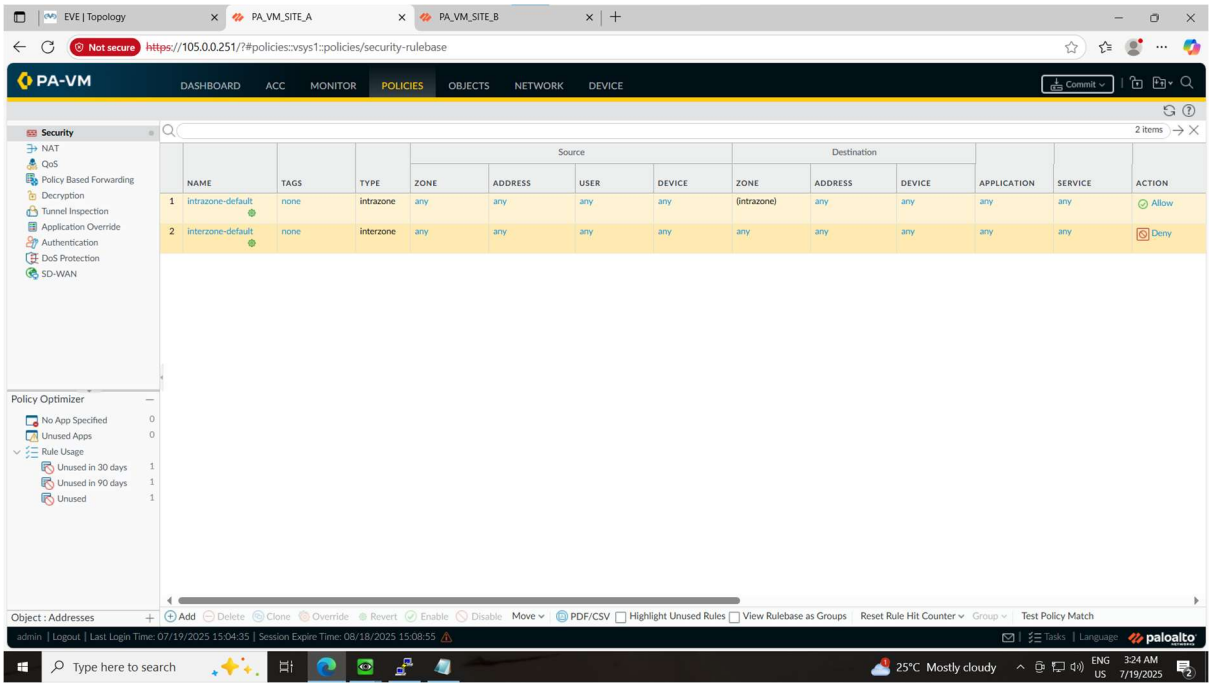


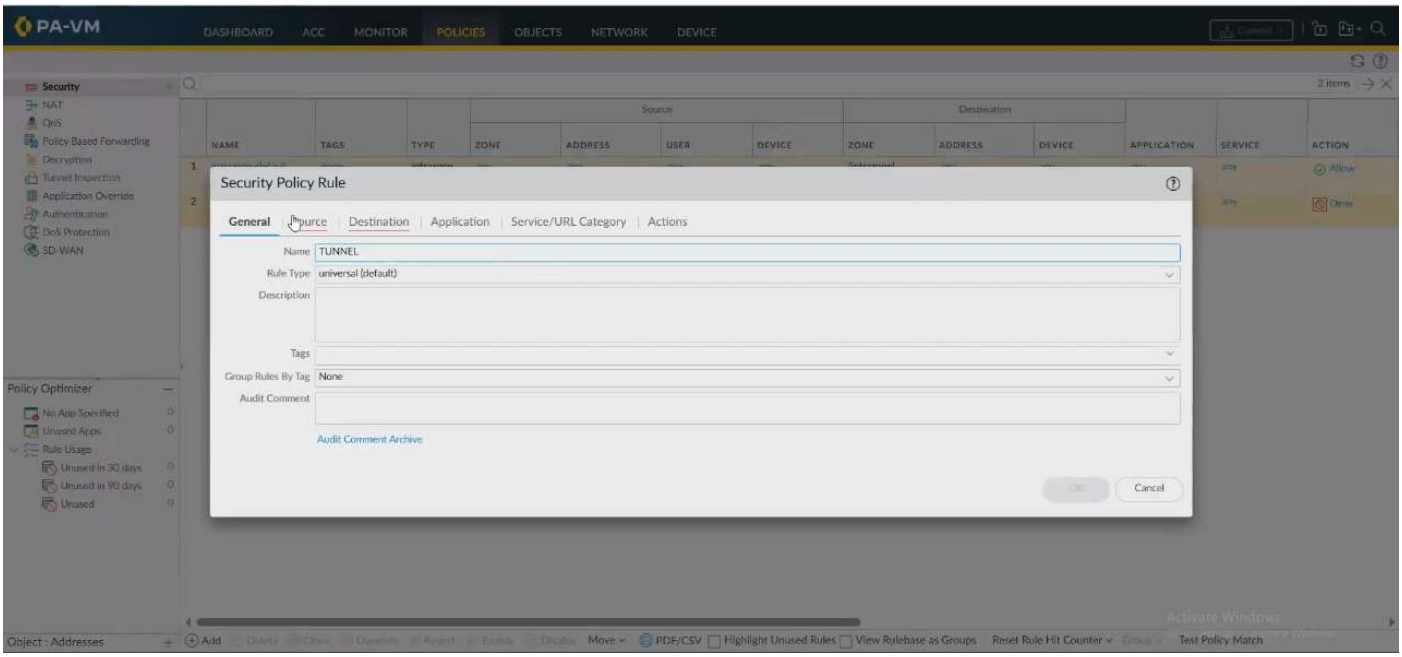
9. Create static routing for site A Lan to site b Lan communication

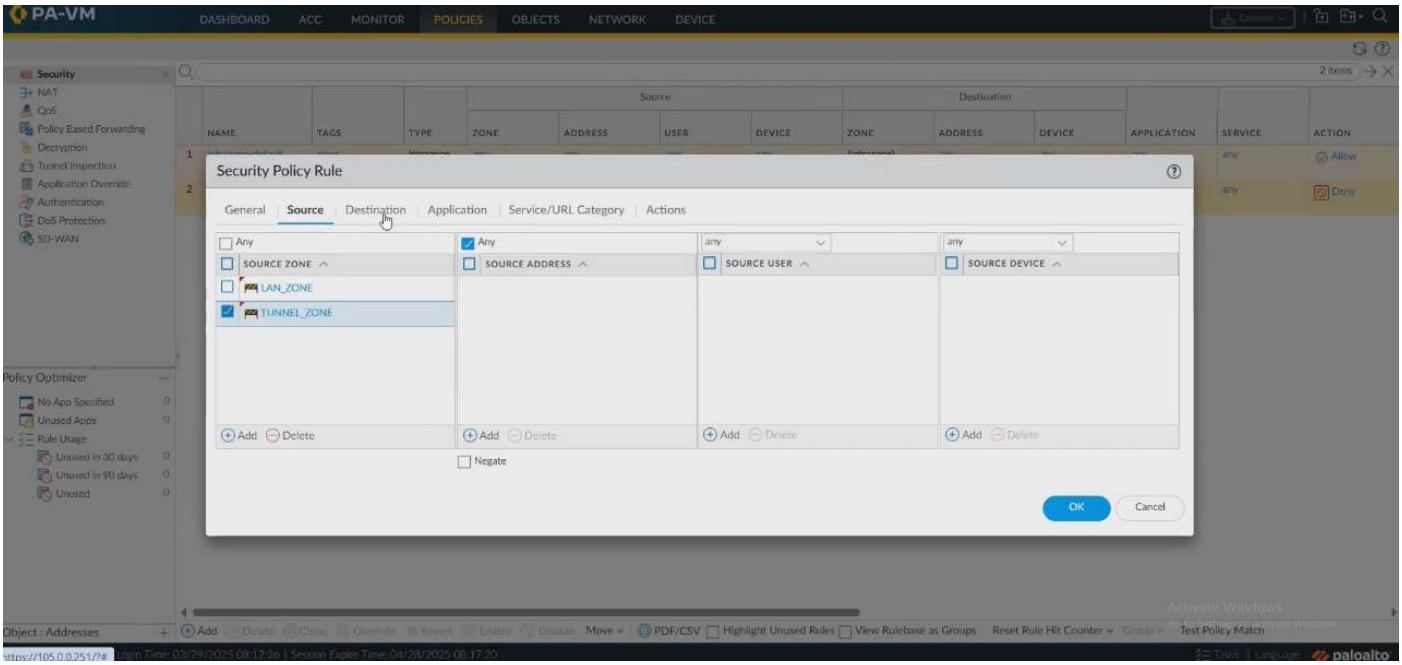
Network> virtual router>default>Static routes> add

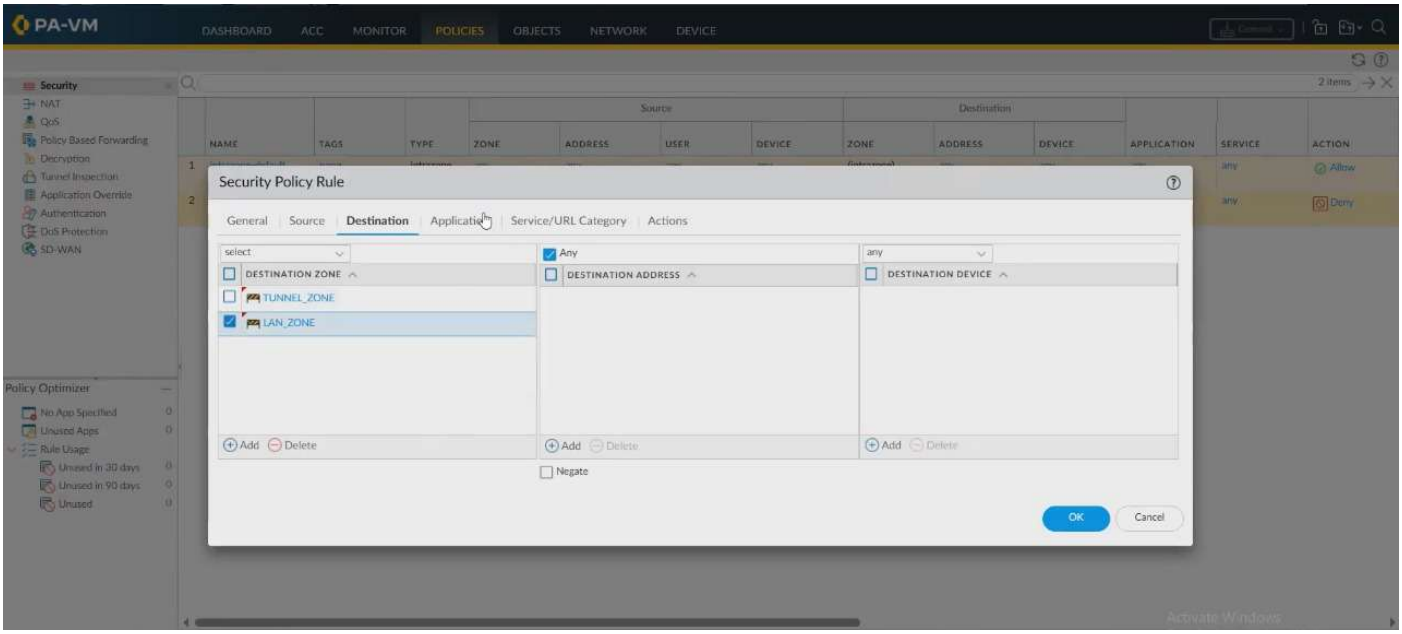


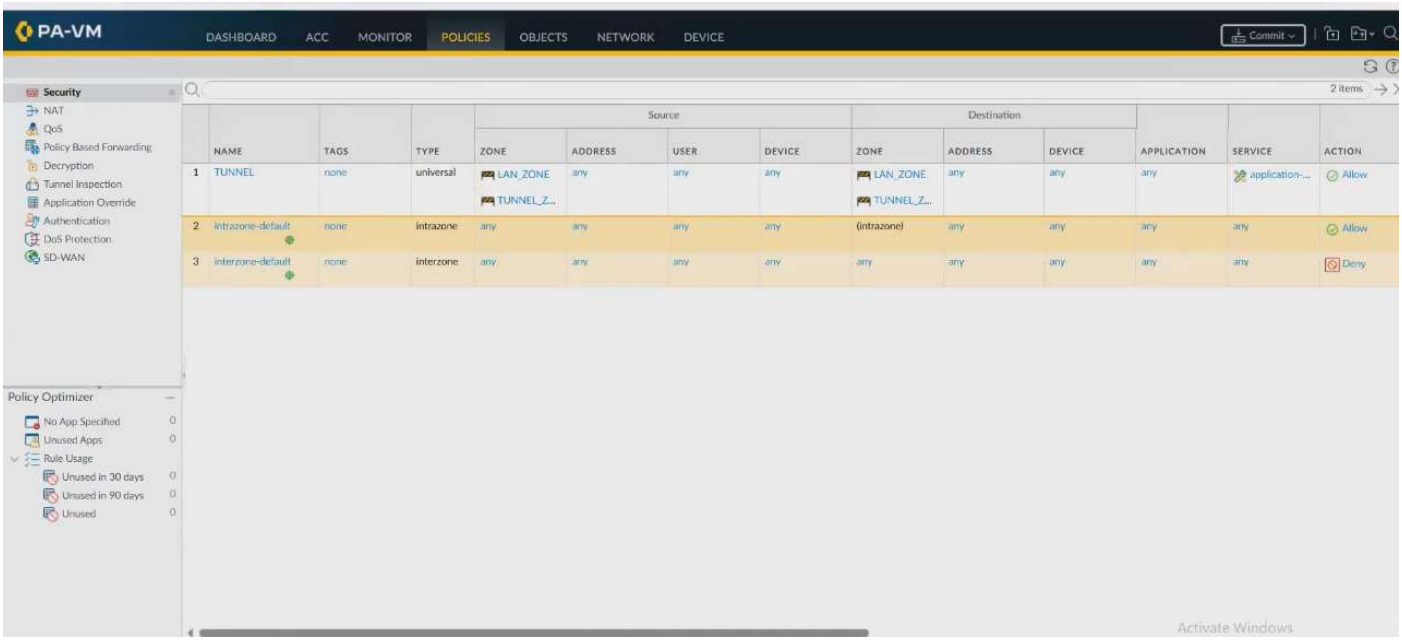
10. Create policy for communication




PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Name
TUNNEL
Rule Type
universal (default)
Description
Tags
Group Rules By Tag
None
Audit Comment
Audit Comment Archive
Cancel


PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
SOURCE ZONE
LAN_ZONE
TUNNEL_ZONE
SOURCE ADDRESS
SOURCE USER
SOURCE DEVICE
Add
Delete
Negate
OK
Cancel





Now commit all changes

REPEAT THE SAME STEPS FROM 1-10 ON PALOALTO VM SITE_B DEVICE

Now you will be able to ping from site A pc to site B pc