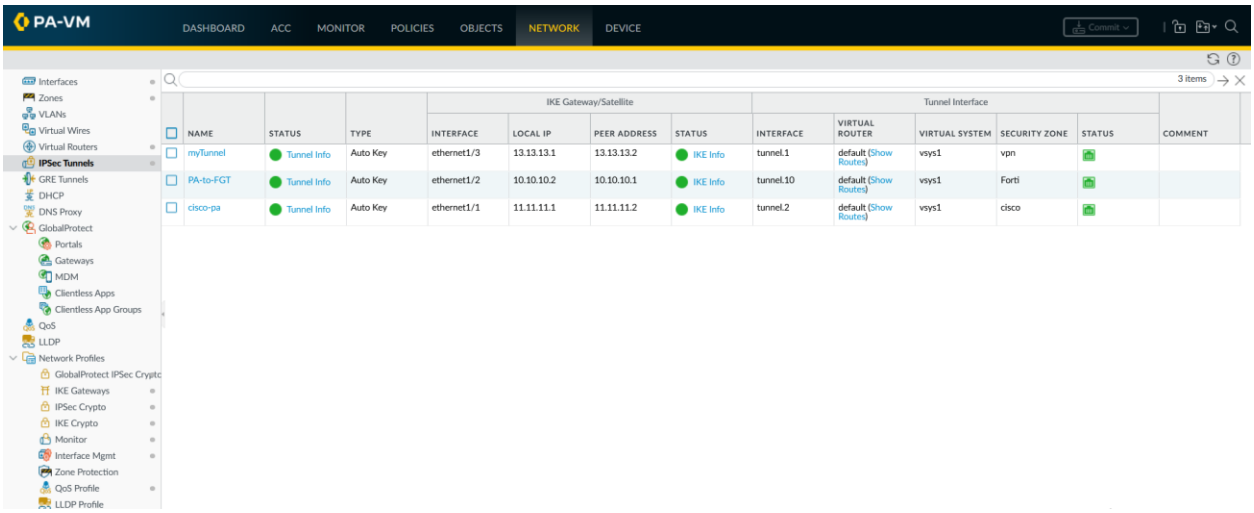
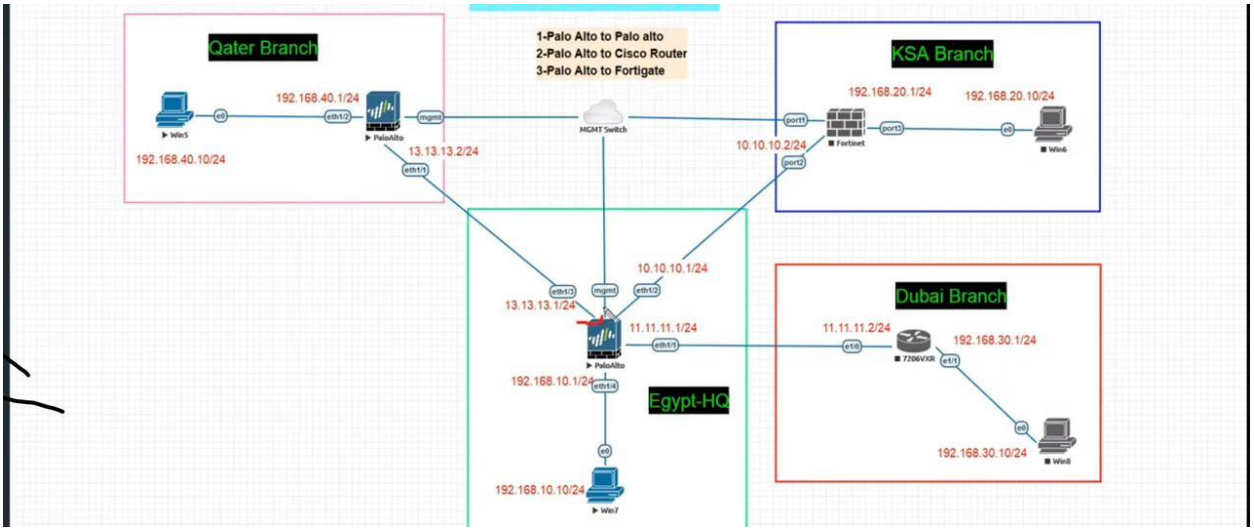
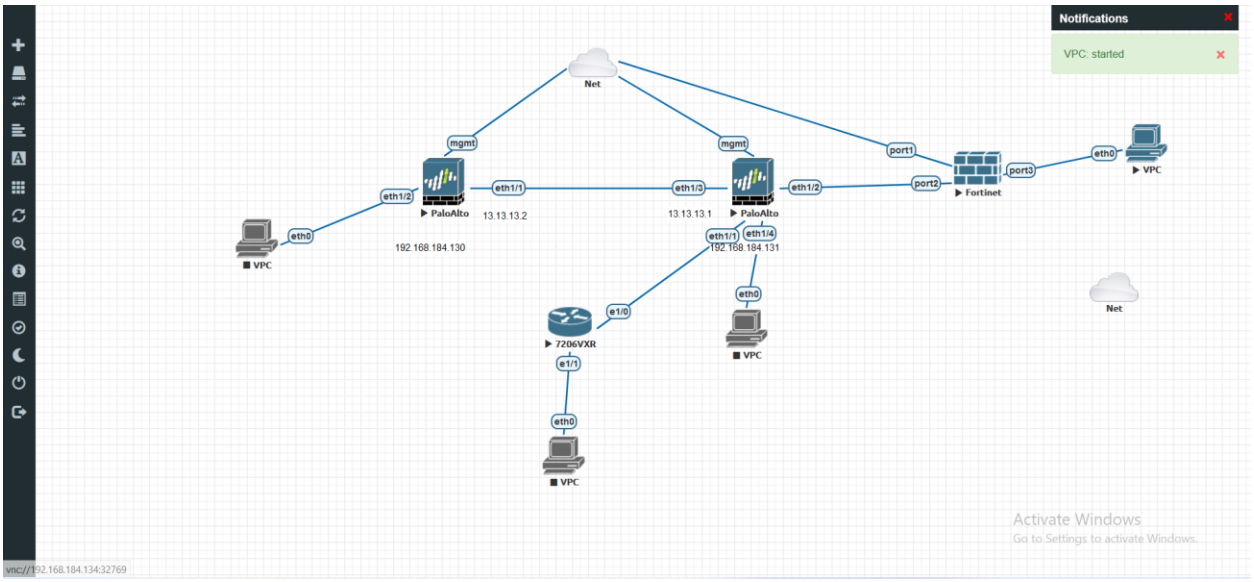
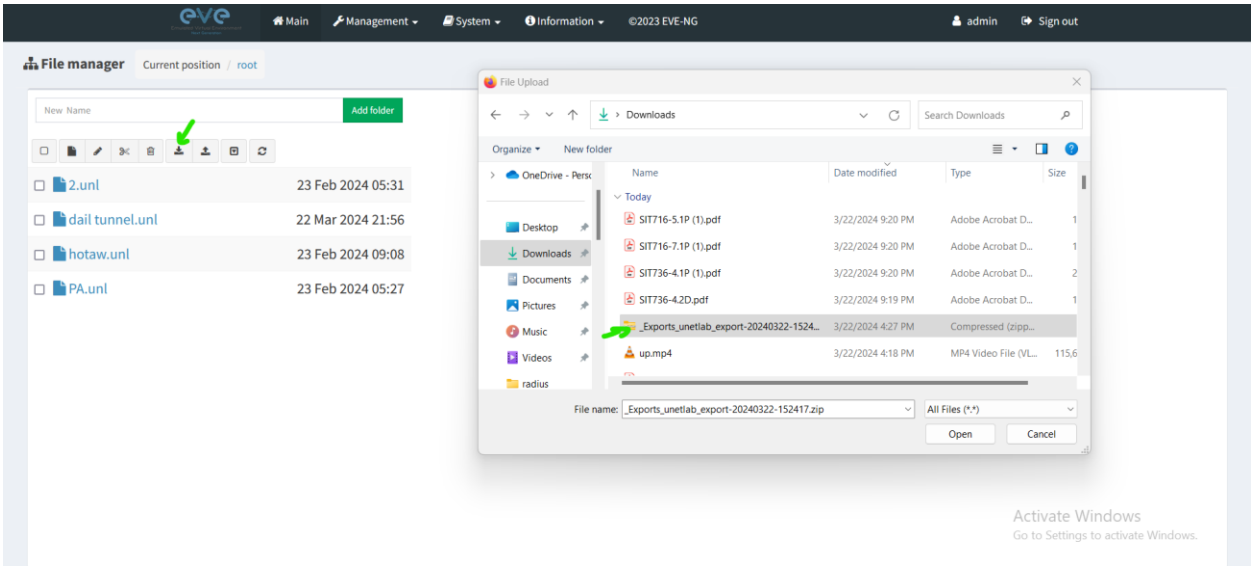

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
3 items
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/3
13.13.13.1
13.13.13.2
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn
PA-to-FGT
Tunnel Info
Auto Key
ethernet1/2
10.10.10.2
10.10.10.1
IKE Info
tunnel.10
default (Show Routes)
vsys1
Forti
cisco-pa
Tunnel Info
Auto Key
ethernet1/1
11.11.11.1
11.11.11.2
IKE Info
tunnel.2
default (Show Routes)
vsys1
cisco

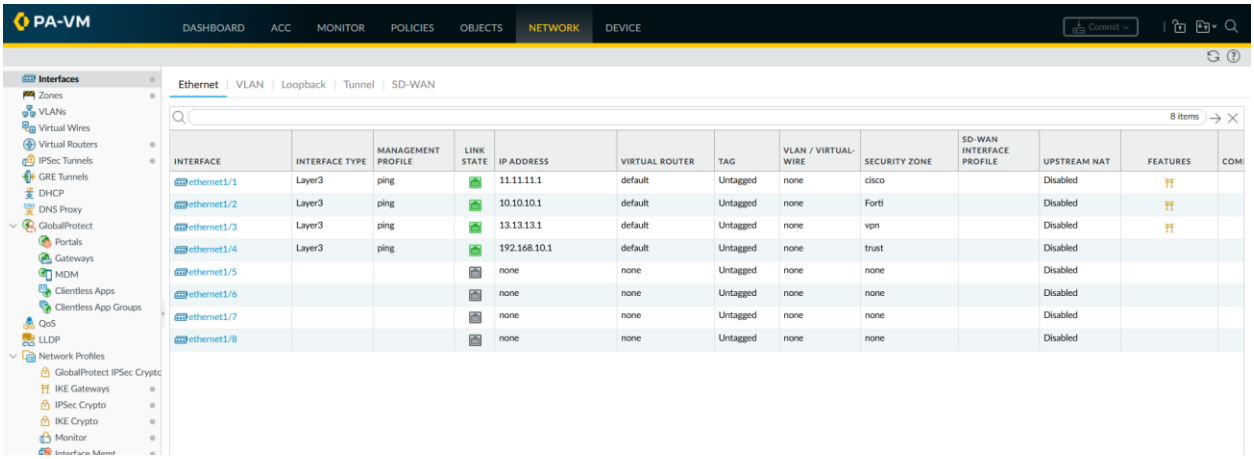

Qater Branch
1-Palo Alto to Palo alto
2-Palo Alto to Cisco Router
3-Palo Alto to Fortigate
KSA Branch
Dubai Branch
Egypt-HQ
192.168.40.1/24
192.168.40.10/24
13.13.13.2/24
MGMT Switch
192.168.20.1/24
192.168.20.10/24
10.10.2/24
10.10.10.1/24
13.13.13.1/24
11.11.11.1/24
192.168.10.1/24
11.11.11.2/24
192.168.30.1/24
192.168.30.10/24
192.168.10.10/24
Win5
PaloAlto
Fortinet
Win6
7206VXR
Win8
Win7

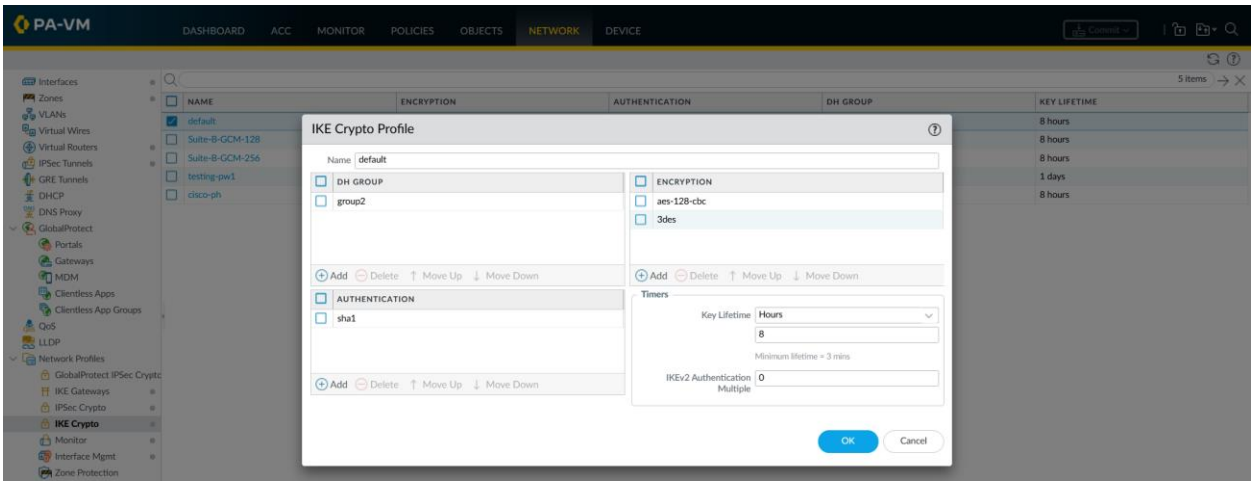

Notifications
VPC: started
Net
mgmt
eth1/2
eth1/1
eth1/3
eth1/2
port1
port2
port3
eth0
PaloAlto
13.13.13.2
13.13.13.1
192.168.184.130
192.168.184.131
Fortinet
VPC
7206VXR
e1/0
e1/1
eth1/4
Activate Windows
Go to Settings to activate Windows.
vnc://192.168.184.134:32769

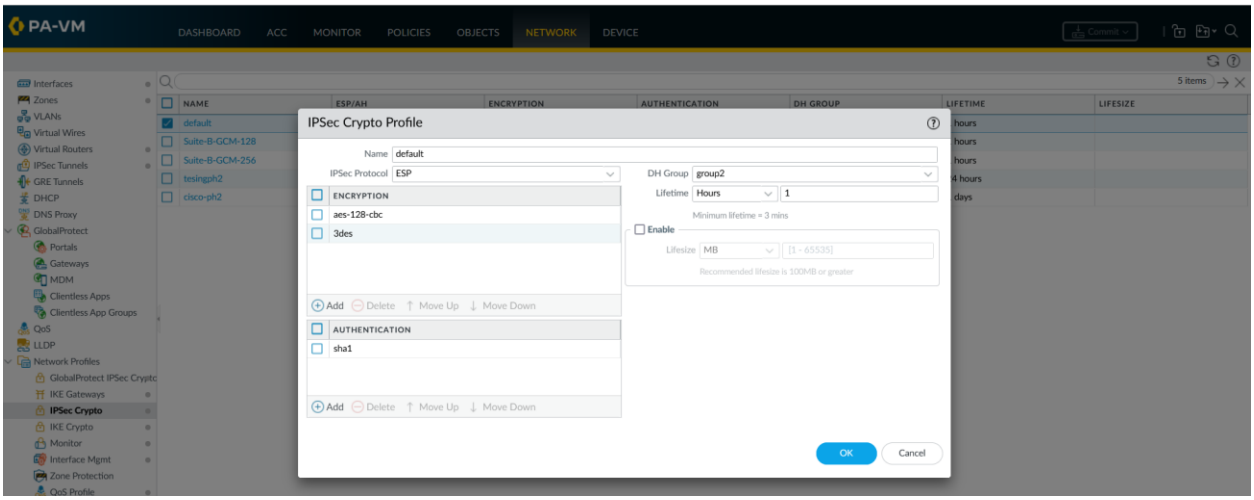

Main
Management
System
Information
©2023 EVE-NG
admin
Sign out
File manager
Current position / root
New Name
Add folder
2.unl
23 Feb 2024 05:31
dail tunnel.unl
22 Mar 2024 21:56
hotaw.unl
23 Feb 2024 09:08
PA.unl
23 Feb 2024 05:27
File Upload
Downloads
Search Downloads
Organize
New folder
Name
Date modified
Type
Size
Today
SIT716-5.1P (1).pdf
SIT716-7.1P (1).pdf
SIT736-4.1P (1).pdf
SIT736-4.2D.pdf
_Exports_unetlab_export-20240322-1524...
up.mp4
Desktop
Downloads
Documents
Pictures
Music
Videos
radius
File name: _Exports_unetlab_export-20240322-152417.zip
All Files (*.*)
Open
Cancel
Activate Windows
Go to Settings to activate Windows.

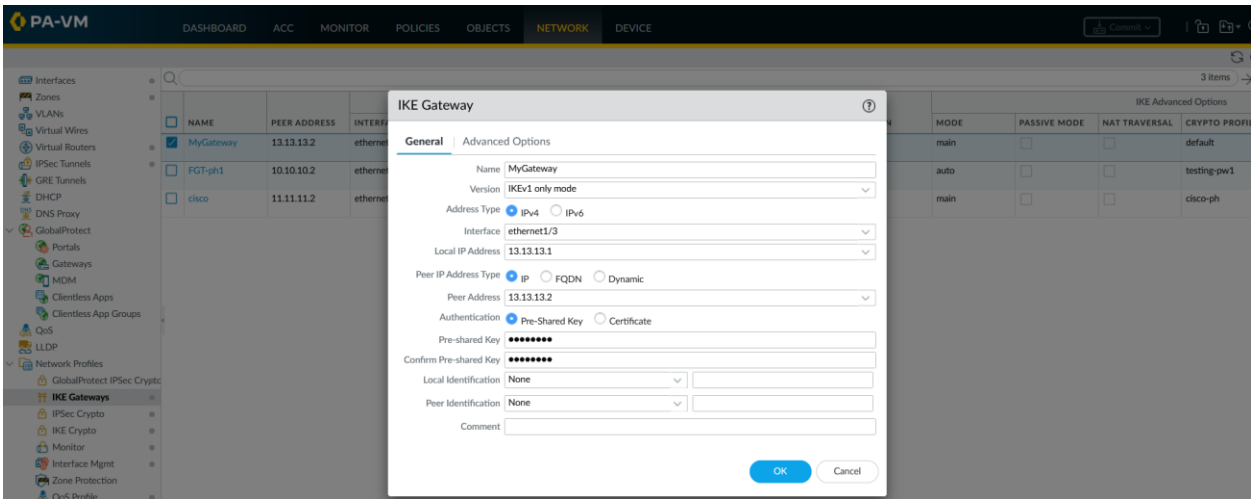
PA-to-PA

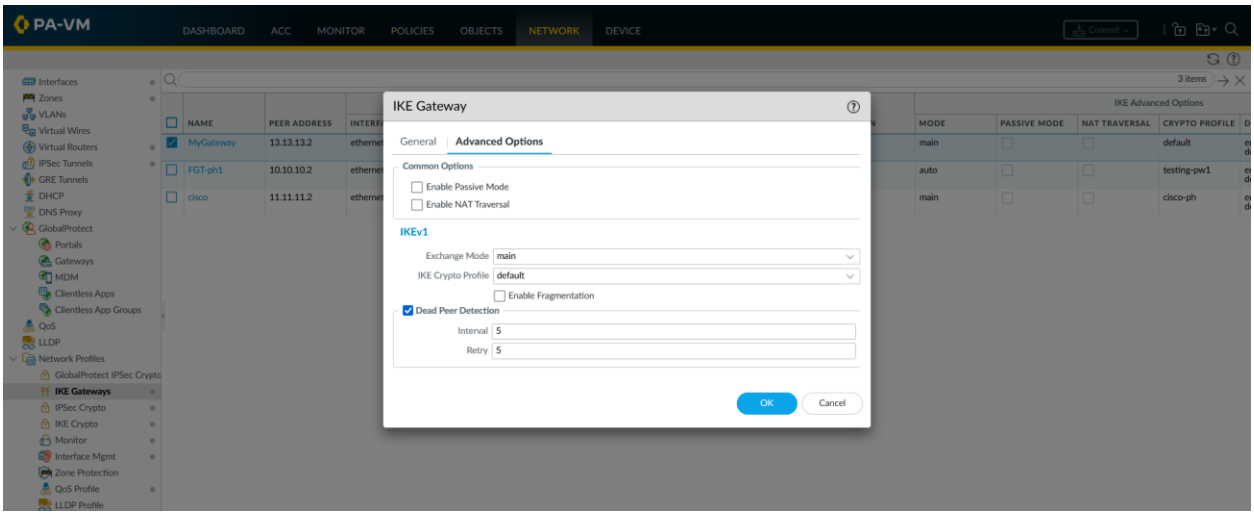
PA1

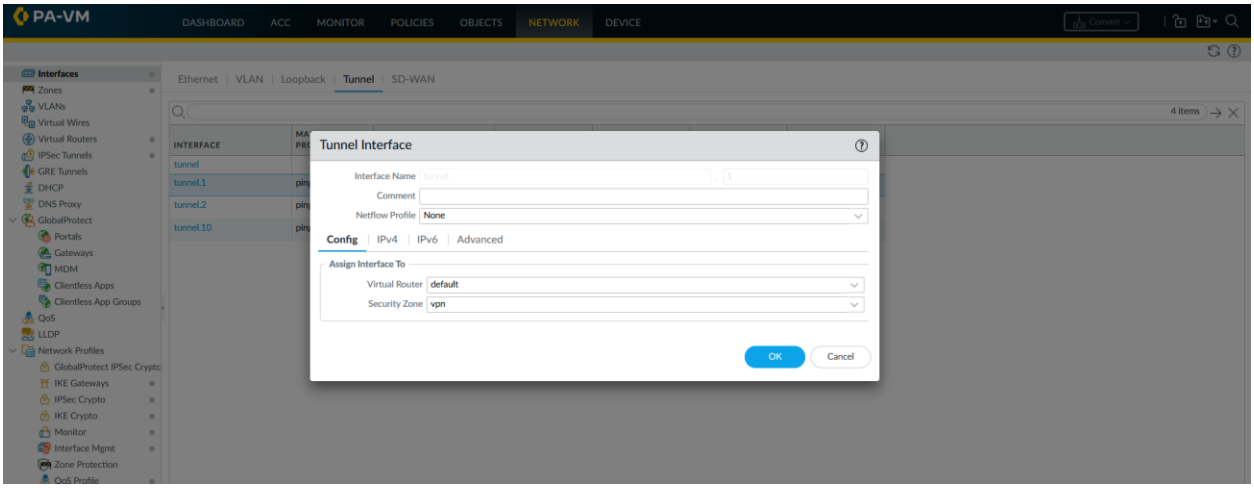

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
8 items
INTERFACE
INTERFACE TYPE
MANAGEMENT PROFILE
LINK STATE
IP ADDRESS
VIRTUAL ROUTER
TAG
VLAN / VIRTUAL-WIRE
SECURITY ZONE
SD-WAN INTERFACE PROFILE
UPSTREAM NAT
FEATURES
ethernet1/1 Layer3 ping 11.11.11.1 default Untagged none cisco Disabled
ethernet1/2 Layer3 ping 10.10.10.1 default Untagged none Forti Disabled
ethernet1/3 Layer3 ping 13.13.13.1 default Untagged none vpn Disabled
ethernet1/4 Layer3 ping 192.168.10.1 default Untagged none trust Disabled
ethernet1/5 none none Untagged none none Disabled
ethernet1/6 none none Untagged none none Disabled
ethernet1/7 none none Untagged none none Disabled
ethernet1/8 none none Untagged none none Disabled

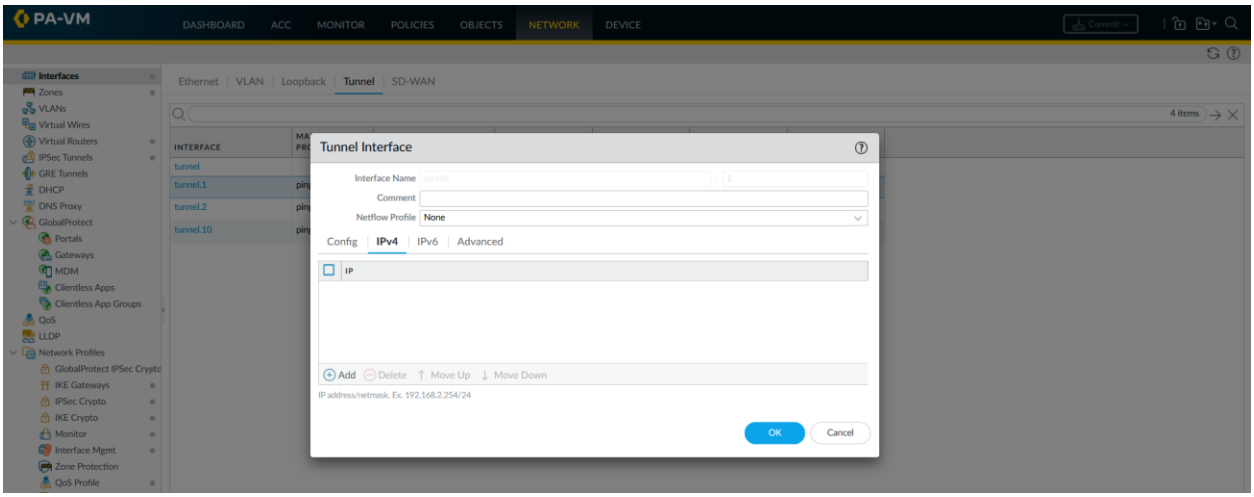

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Crypto Profile
Name default
DH GROUP
group2
ENCRYPTION
aes-128-cbc
3des
AUTHENTICATION
sha1
Add Delete Move Up Move Down
Timers
Key Lifetime Hours
8
Minimum lifetime = 3 mins
IKEv2 Authentication Multiple 0
OK Cancel

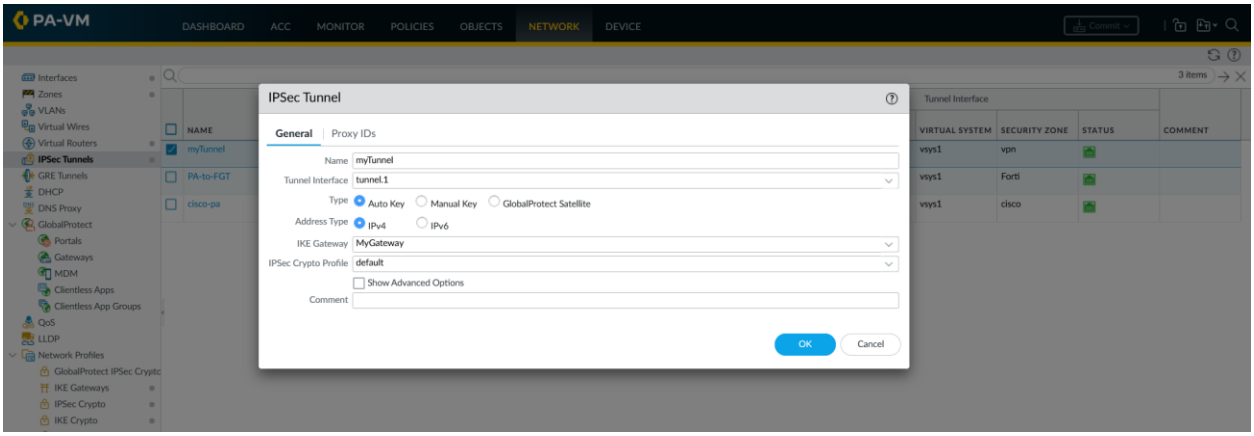

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IPSec Crypto Profile
Name default
IPSec Protocol ESP
DH Group group2
Lifetime Hours 1
Minimum lifetime = 3 mins
Enable
Lifesize MB [1 - 65535]
Recommended lifesize is 100MB or greater
ENCRYPTION
aes-128-cbc
3des
AUTHENTICATION
sha1
Add Delete Move Up Move Down
OK Cancel

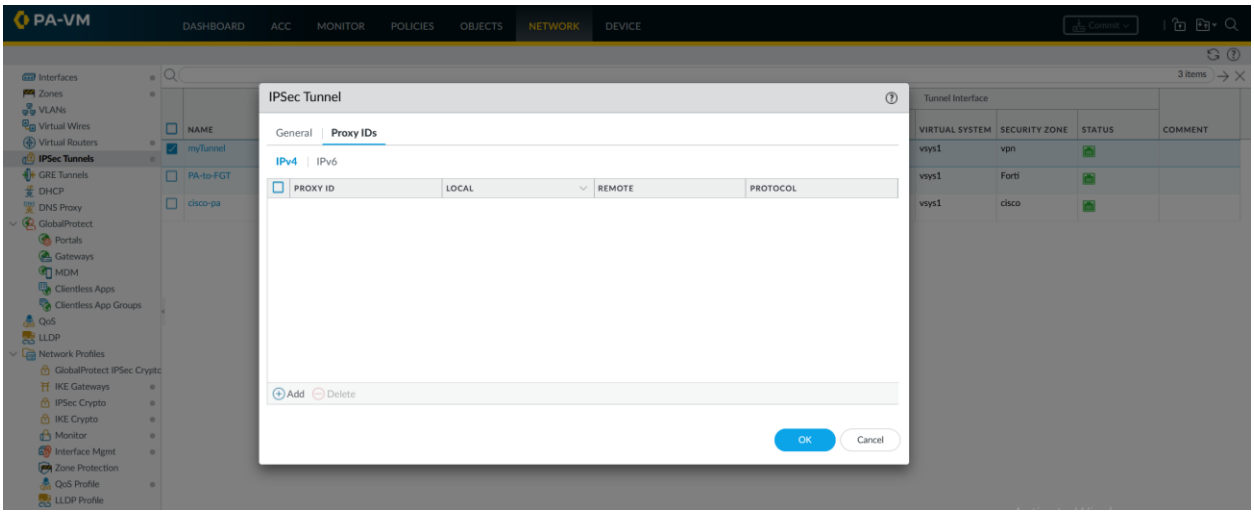

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Gateway
General Advanced Options
Name MyGateway
Version IKEv1 only mode
Address Type IPv4 IPv6
Interface ethernet1/3
Local IP Address 13.13.13.1
Peer IP Address Type IP FQDN Dynamic
Peer Address 13.13.13.2
Authentication Pre-Shared Key Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification None
Peer Identification None
Comment
OK Cancel

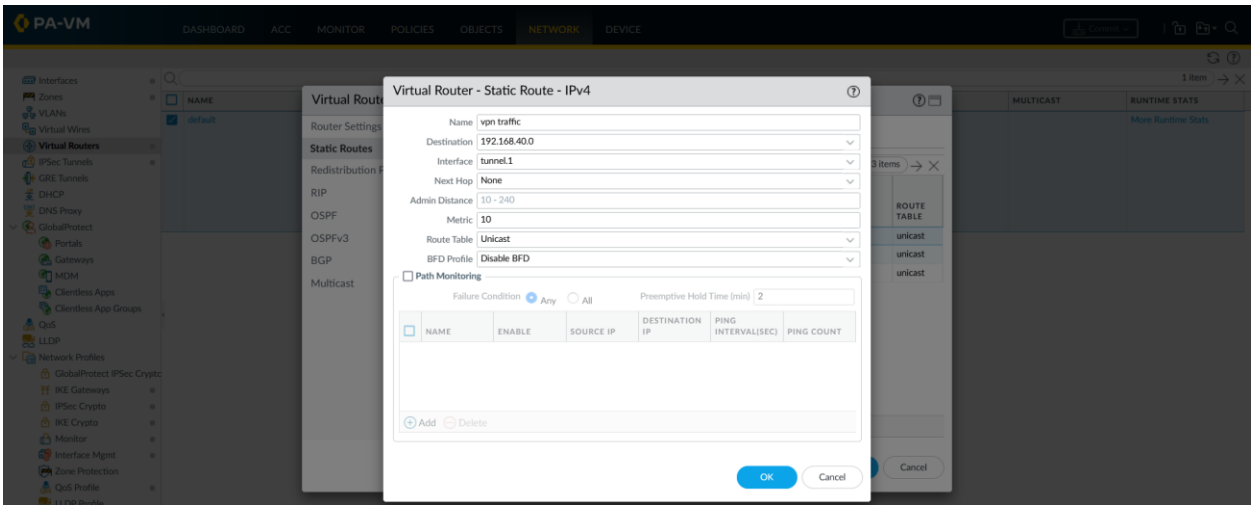

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IKE Gateway
General
Advanced Options
Common Options
Enable Passive Mode
Enable NAT Traversal
IKEv1
Exchange Mode
main
IKE Crypto Profile
default
Enable Fragmentation
Dead Peer Detection
Interval
5
Retry
5
OK
Cancel

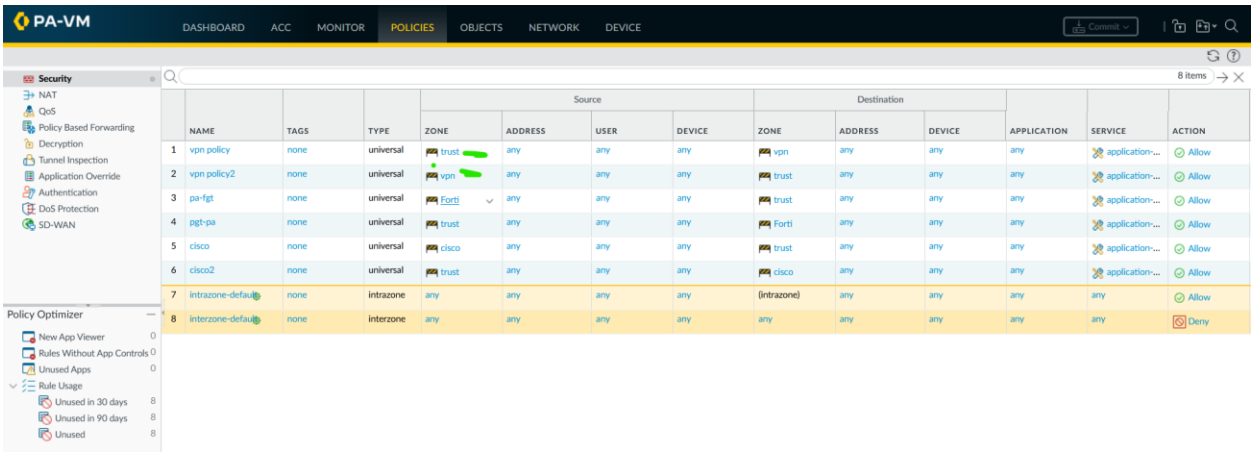

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router
default
Security Zone
vpn
OK
Cancel

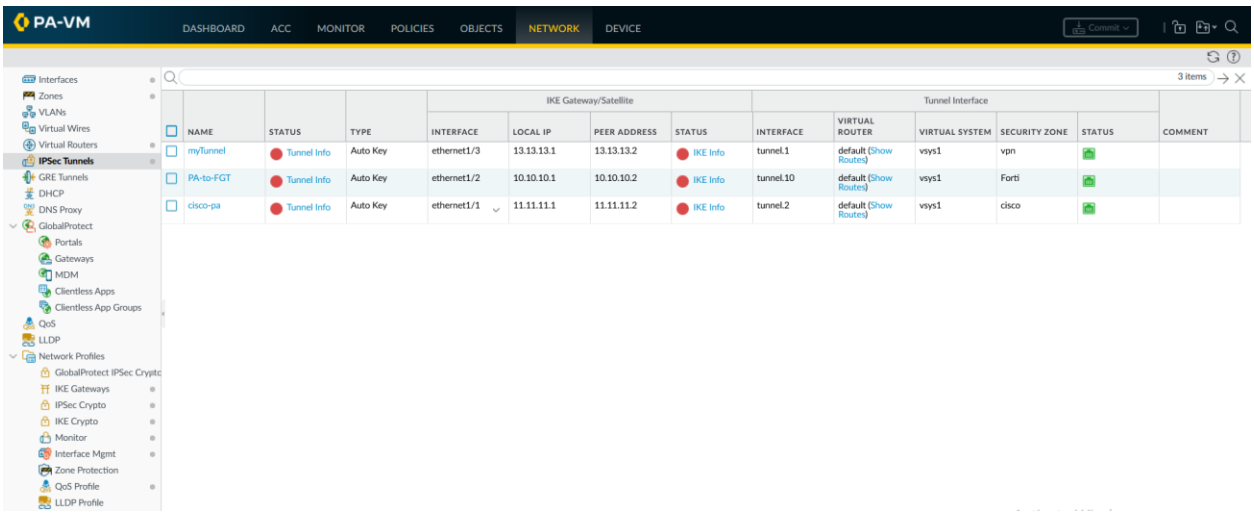

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
IP
Add
Delete
Move Up
Move Down
IP address/netmask. Ex. 192.168.2.254/24
OK
Cancel


PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IPSec Tunnel
General
Proxy IDs
Name
myTunnel
Tunnel Interface
tunnel.1
Type
Auto Key
Manual Key
GlobalProtect Satellite
Address Type
IPv4
IPv6
IKE Gateway
MyGateway
IPSec Crypto Profile
default
Show Advanced Options
Comment
OK
Cancel

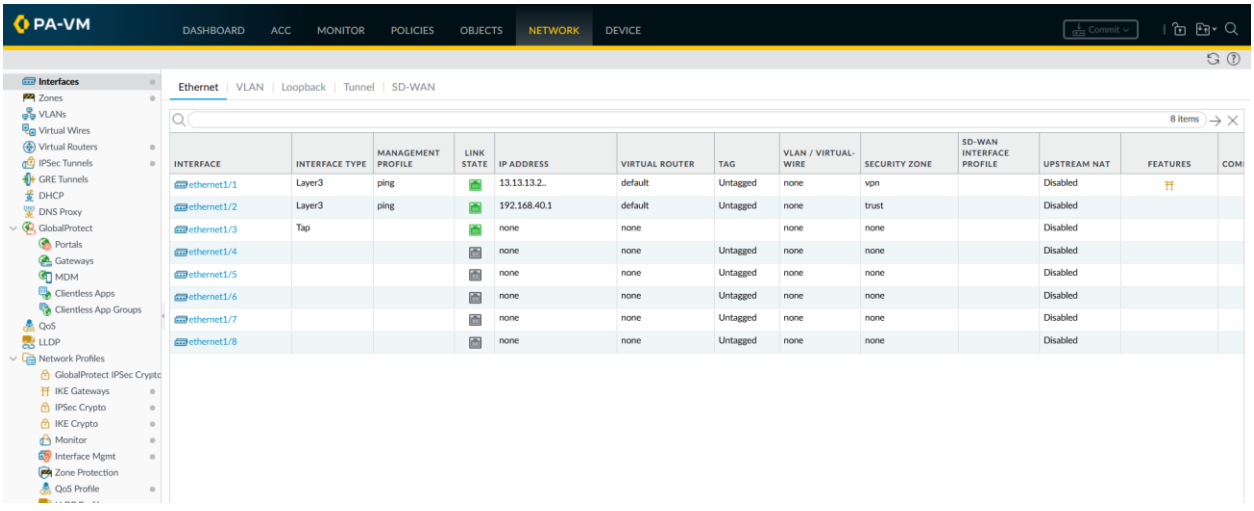

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IPSec Tunnel
General
Proxy IDs
IPv4
IPv6
PROXY ID
LOCAL
REMOTE
PROTOCOL
Add
Delete
OK
Cancel

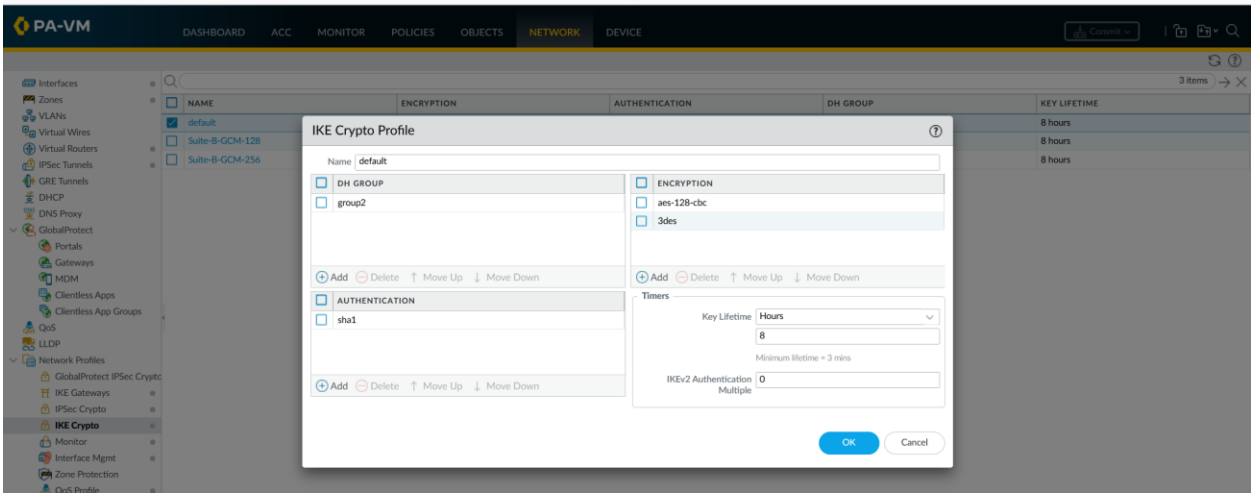

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Virtual Router - Static Route - IPv4
Name
vpn traffic
Destination
192.168.40.0
Interface
tunnel.1
Next Hop
None
Admin Distance
10 - 240
Metric
10
Route Table
Unicast
BFD Profile
Disable BFD
Path Monitoring
Failure Condition
Any
All
Preemptive Hold Time (min)
2
NAME
ENABLE
SOURCE IP
DESTINATION IP
PING INTERVAL(SEC)
PING COUNT
Add
Delete
OK
Cancel

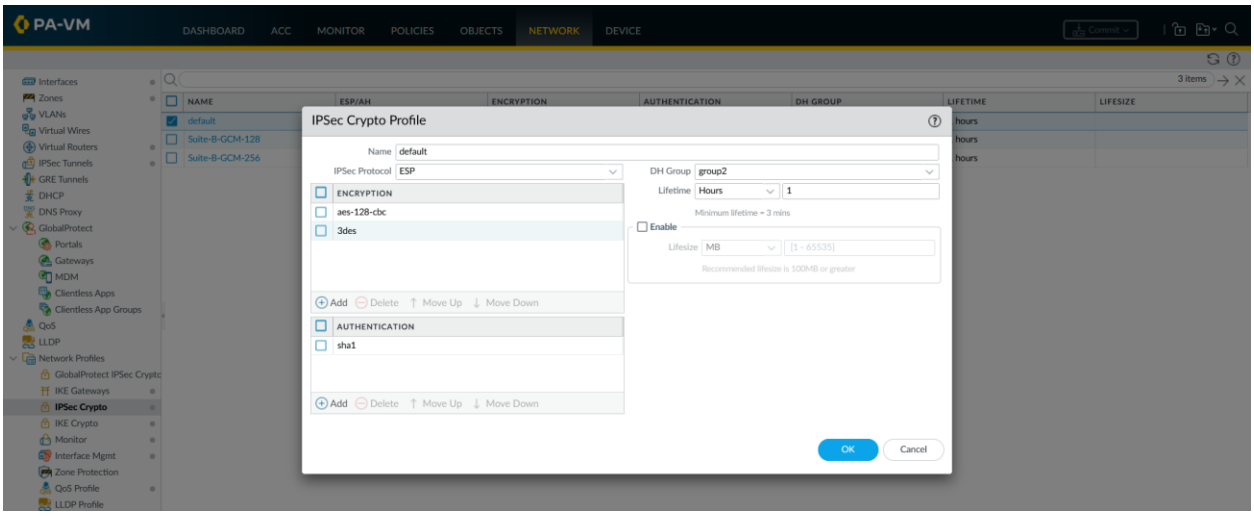

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App Viewer
Rules Without App Controls
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
8 items
Source
Destination
NAME
TAGS
TYPE
ZONE
ADDRESS
USER
DEVICE
APPLICATION
SERVICE
ACTION
1 vpn policy none universal trust any any any vpn any any any application-... Allow
2 vpn policy2 none universal vpn any any any trust any any any application-... Allow
3 pa-fgt none universal Forti any any any trust any any any application-... Allow
4 pgt-pa none universal trust any any any Forti any any any application-... Allow
5 cisco none universal cisco any any any trust any any any application-... Allow
6 cisco2 none universal trust any any any cisco any any any application-... Allow
7 intrazone-default none intrazone any any any any (intrazone) any any any any Allow
8 interzone-default none interzone any any any any any any any any any Deny

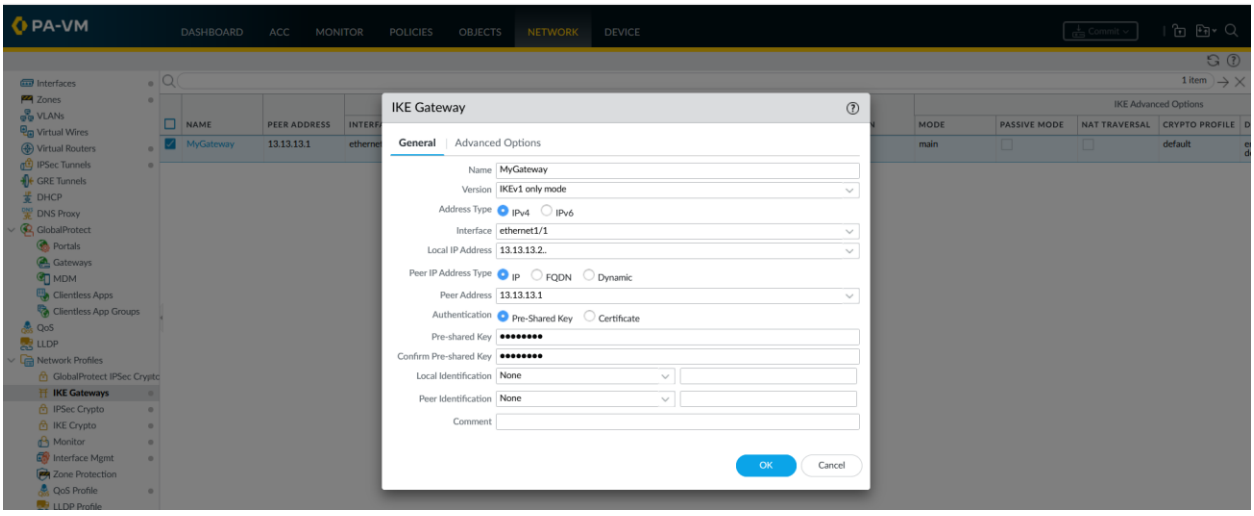

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
3 items
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel Tunnel Info Auto Key ethernet1/3 13.13.13.1 13.13.13.2 IKE Info tunnel.1 default (Show Routes) vsys1 vpn
PA-to-FGT Tunnel Info Auto Key ethernet1/2 10.10.10.1 10.10.10.2 IKE Info tunnel.10 default (Show Routes) vsys1 Forti
cisco-pa Tunnel Info Auto Key ethernet1/1 11.11.11.1 11.11.11.2 IKE Info tunnel.2 default (Show Routes) vsys1 cisco

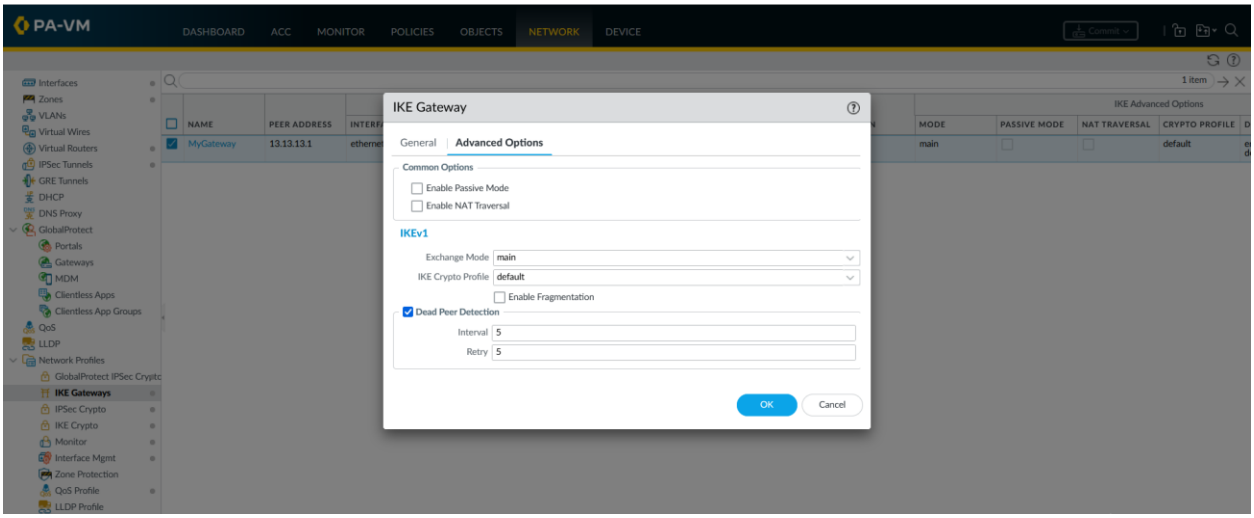
PA2

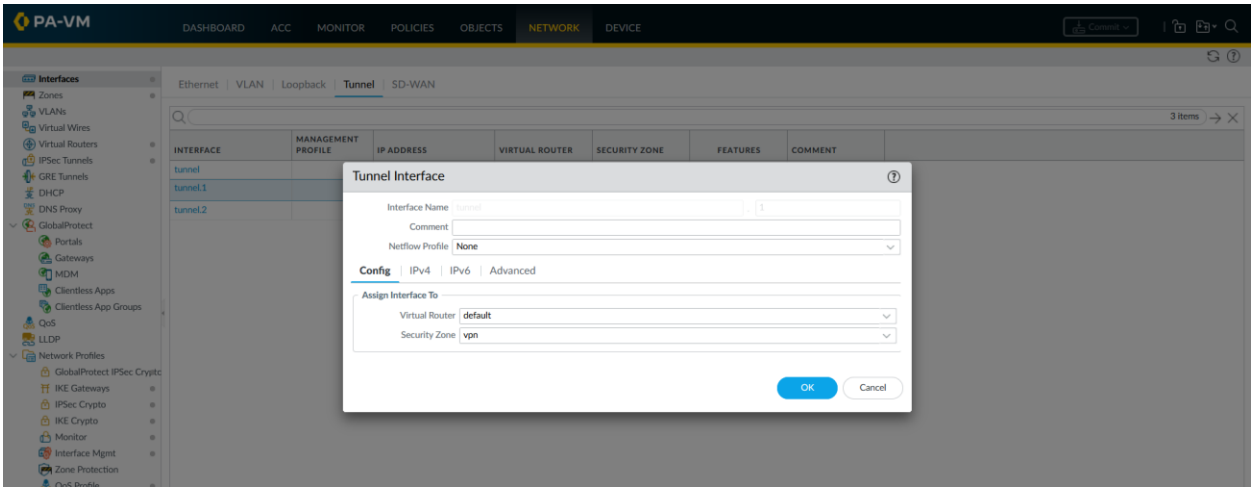

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
8 items
INTERFACE
INTERFACE TYPE
MANAGEMENT PROFILE
LINK STATE
IP ADDRESS
VIRTUAL ROUTER
TAG
VLAN / VIRTUAL-WIRE
SECURITY ZONE
SD-WAN INTERFACE PROFILE
UPSTREAM NAT
FEATURES
ethernet1/1 Layer3 ping 13.13.13.2.. default Untagged none vpn Disabled
ethernet1/2 Layer3 ping 192.168.40.1 default Untagged none trust Disabled
ethernet1/3 Tap none none none none Disabled
ethernet1/4 none none Untagged none none Disabled
ethernet1/5 none none Untagged none none Disabled
ethernet1/6 none none Untagged none none Disabled
ethernet1/7 none none Untagged none none Disabled
ethernet1/8 none none Untagged none none Disabled

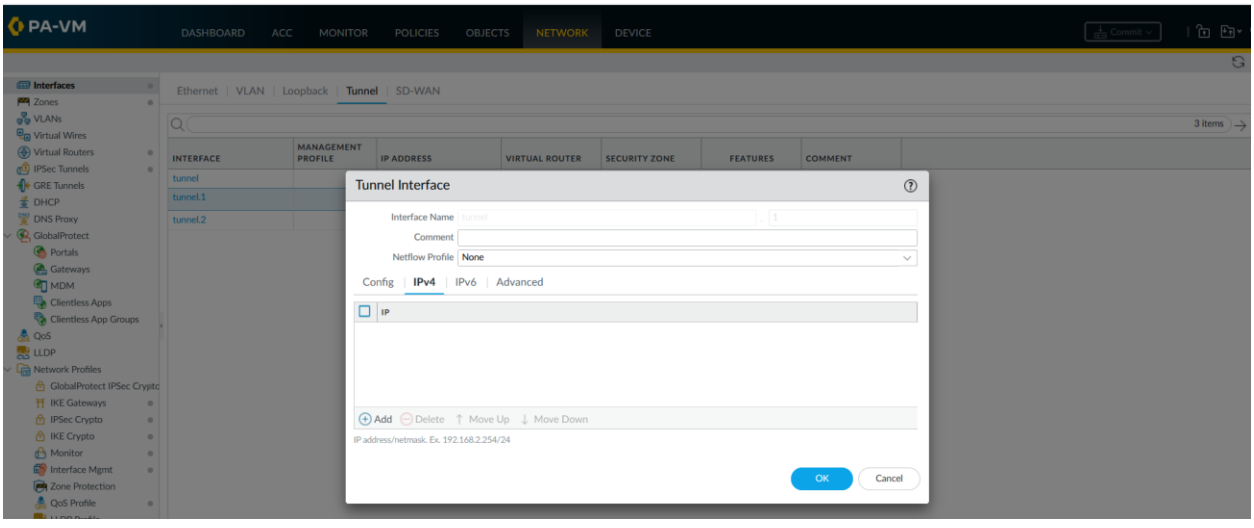

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Crypto Profile
Name default
DH GROUP
group2
ENCRYPTION
aes-128-cbc
3des
AUTHENTICATION
sha1
Timers
Key Lifetime Hours
8
Minimum lifetime = 3 mins
IKEv2 Authentication Multiple 0
OK
Cancel

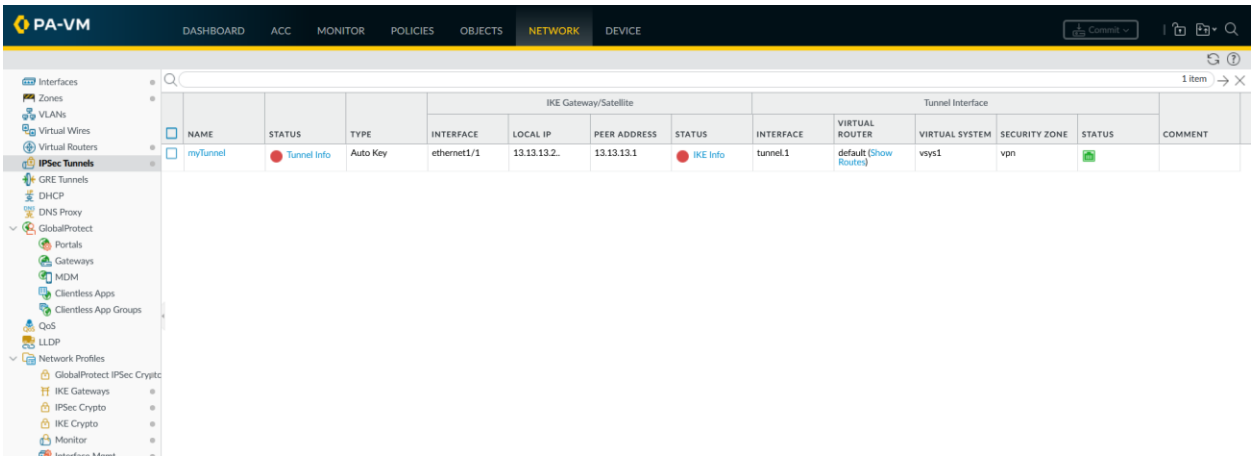

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IPSec Crypto Profile
Name default
IPSec Protocol ESP
DH Group group2
Lifetime Hours 1
Minimum lifetime = 3 mins
Enable
Lifesize MB
Recommended lifesize is 100MB or greater
ENCRYPTION
aes-128-cbc
3des
AUTHENTICATION
sha1
OK
Cancel

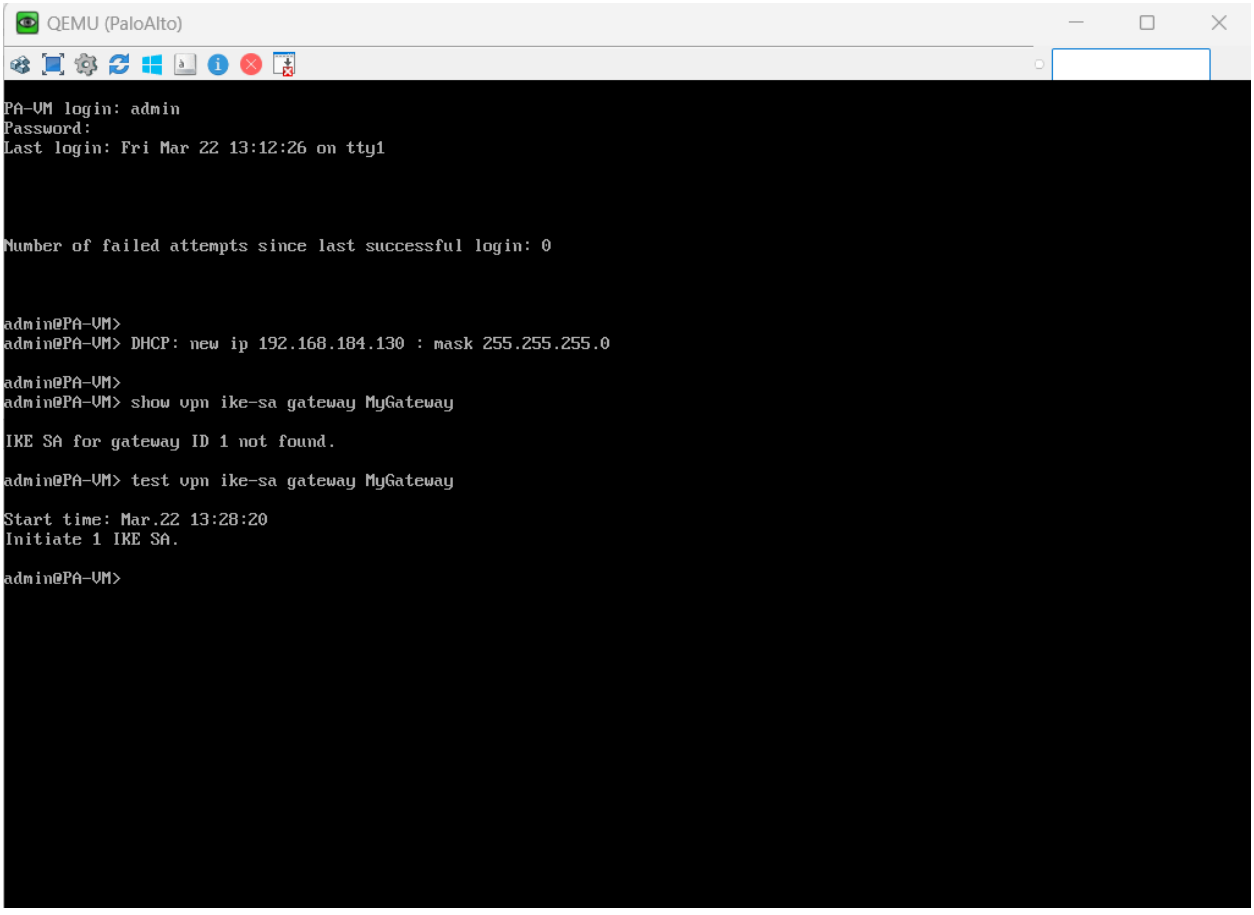

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Gateway
General
Advanced Options
Name MyGateway
Version IKEv1 only mode
Address Type IPv4 IPv6
Interface ethernet1/1
Local IP Address 13.13.13.2..
Peer IP Address Type IP FQDN Dynamic
Peer Address 13.13.13.1
Authentication Pre-Shared Key Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification None
Peer Identification None
Comment
OK
Cancel

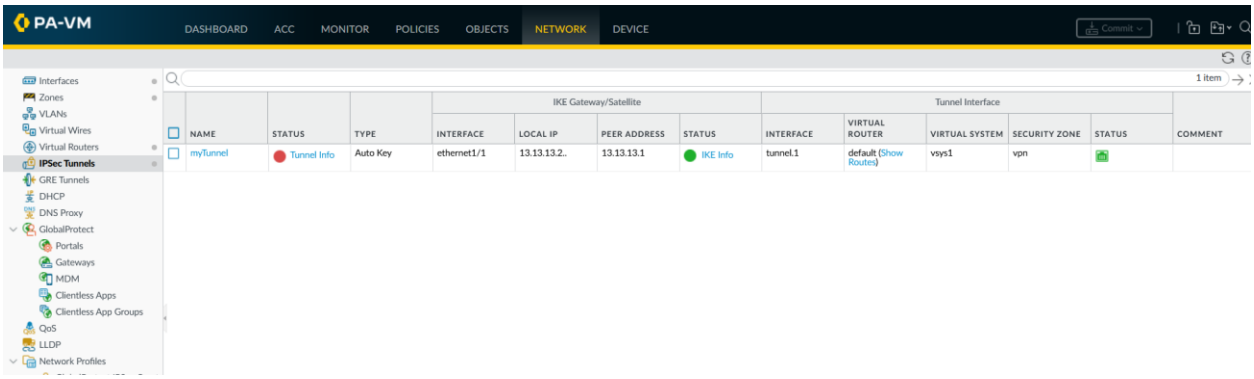

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IKE Gateway
General
Advanced Options
Common Options
Enable Passive Mode
Enable NAT Traversal
IKEv1
Exchange Mode
main
IKE Crypto Profile
default
Enable Fragmentation
Dead Peer Detection
Interval
5
Retry
5
OK
Cancel

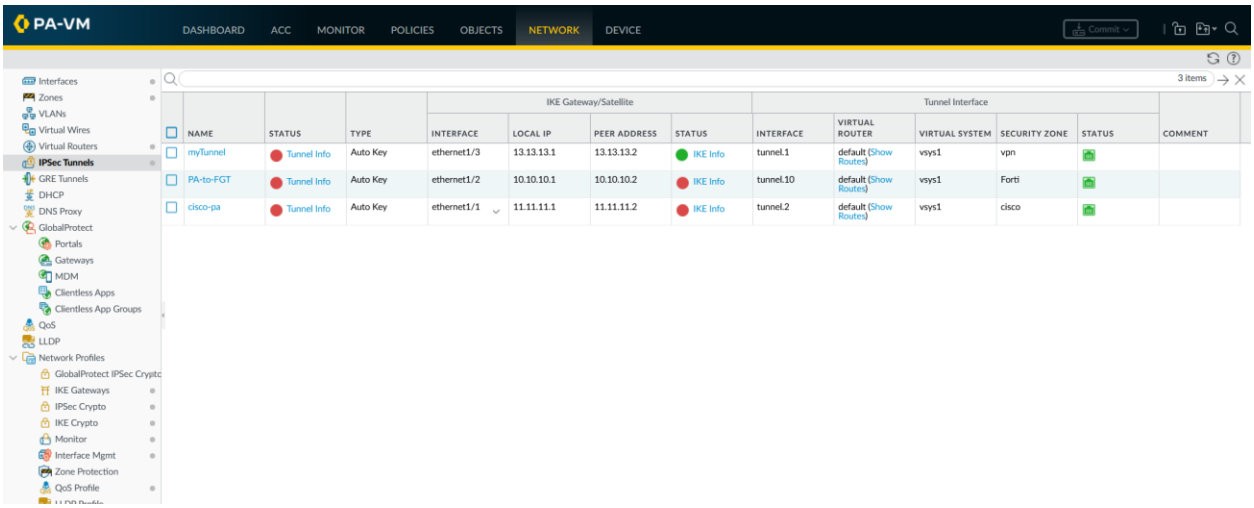

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router
default
Security Zone
vpn
OK
Cancel

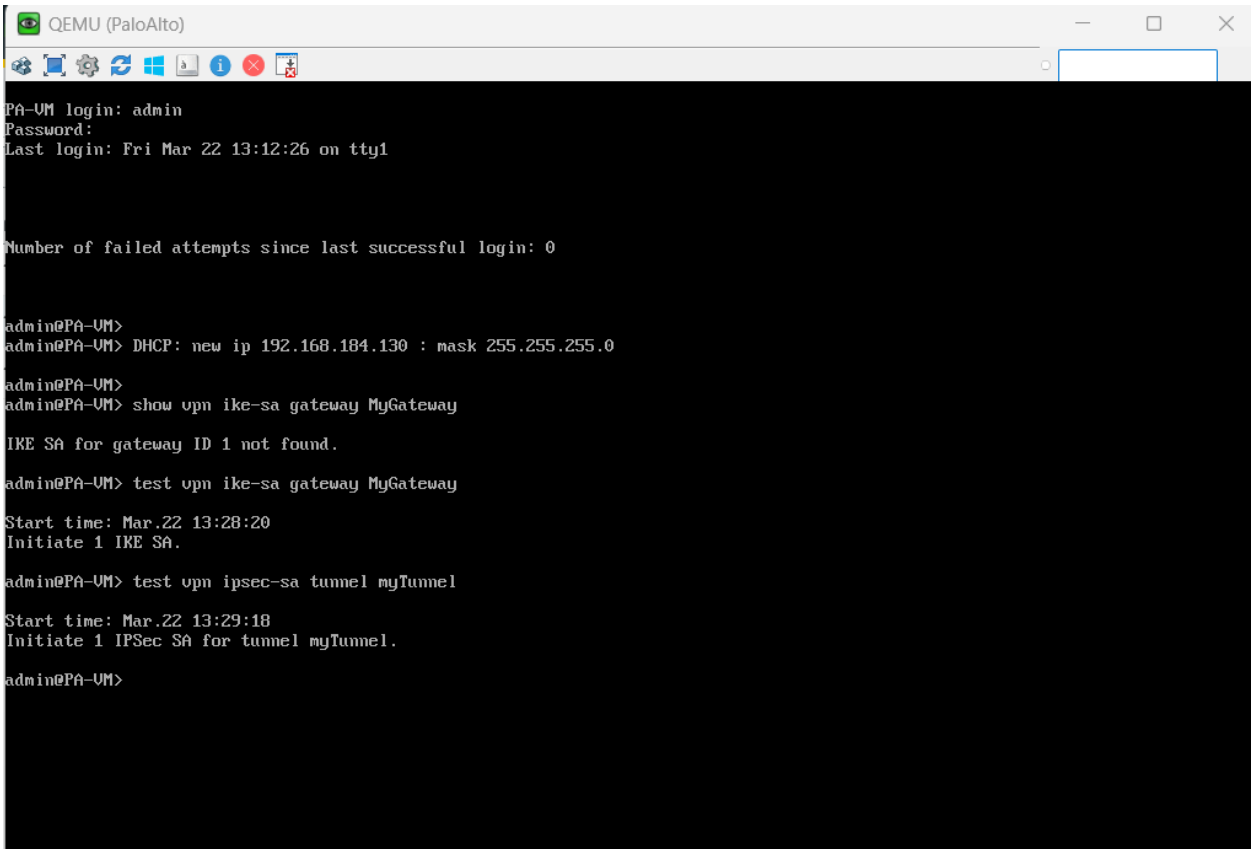

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
IP
Add
Delete
Move Up
Move Down
IP address/netmask. Ex. 192.168.2.254/24
OK
Cancel

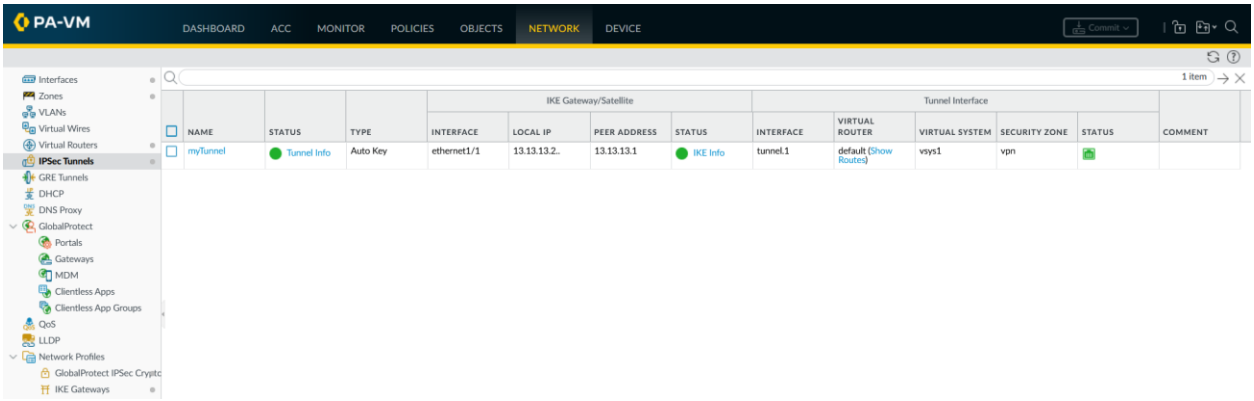

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
1 item
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/1
13.13.13.2..
13.13.13.1
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn

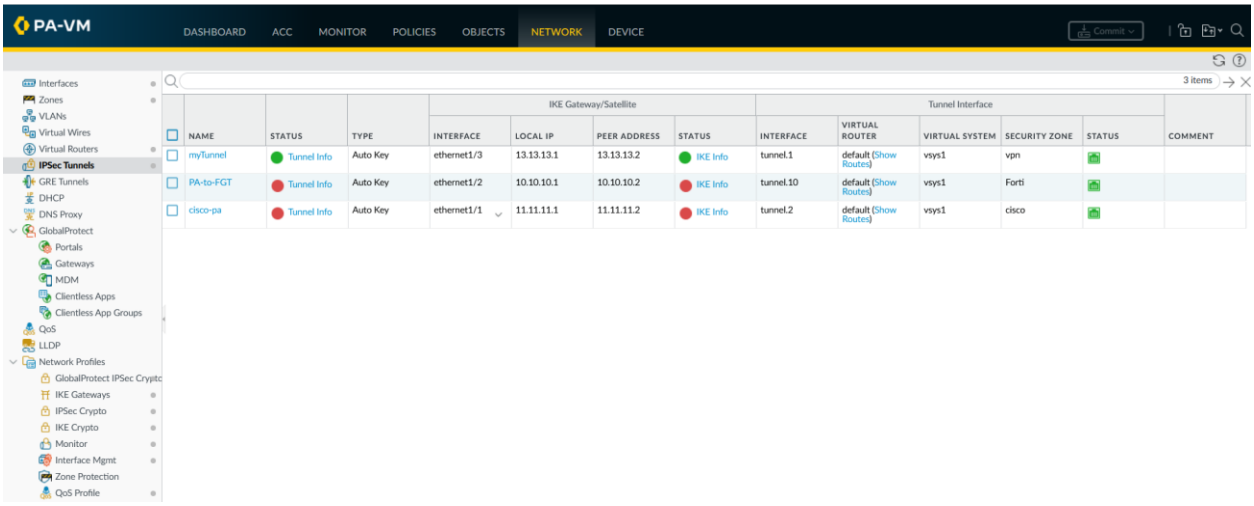

QEMU (PaloAlto)
PA-VM login: admin
Password:
Last login: Fri Mar 22 13:12:26 on tty1
Number of failed attempts since last successful login: 0
admin@PA-VM>
admin@PA-VM> DHCP: new ip 192.168.184.130 : mask 255.255.255.0
admin@PA-VM>
admin@PA-VM> show vpn ike-sa gateway MyGateway
IKE SA for gateway ID 1 not found.
admin@PA-VM> test vpn ike-sa gateway MyGateway
Start time: Mar.22 13:28:20
Initiate 1 IKE SA.
admin@PA-VM>


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
1 item
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/1
13.13.13.2..
13.13.13.1
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn


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
3 items
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/3
13.13.13.1
13.13.13.2
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn
PA-to-FGT
Tunnel Info
Auto Key
ethernet1/2
10.10.10.1
10.10.10.2
IKE Info
tunnel.10
default (Show Routes)
vsys1
Forti
cisco-pa
Tunnel Info
Auto Key
ethernet1/1
11.11.11.1
11.11.11.2
IKE Info
tunnel.2
default (Show Routes)
vsys1
cisco

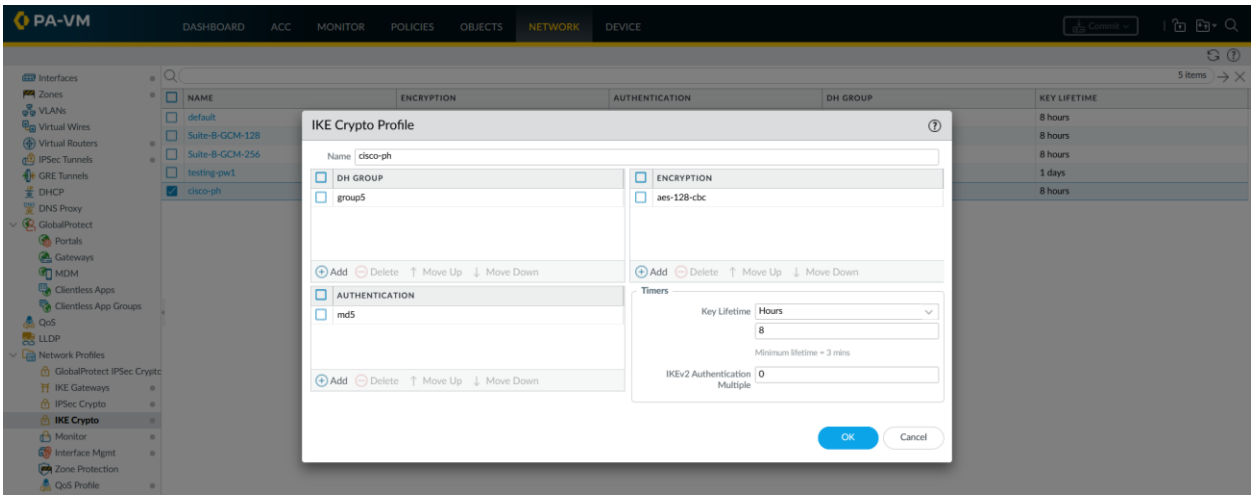

QEMU (PaloAlto)
PA-VM login: admin
Password:
Last login: Fri Mar 22 13:12:26 on tty1
Number of failed attempts since last successful login: 0
admin@PA-VM>
admin@PA-VM> DHCP: new ip 192.168.184.130 : mask 255.255.255.0
admin@PA-VM>
admin@PA-VM> show vpn ike-sa gateway MyGateway
IKE SA for gateway ID 1 not found.
admin@PA-VM> test vpn ike-sa gateway MyGateway
Start time: Mar.22 13:28:20
Initiate 1 IKE SA.
admin@PA-VM> test vpn ipsec-sa tunnel myTunnel
Start time: Mar.22 13:29:18
Initiate 1 IPSec SA for tunnel myTunnel.
admin@PA-VM>

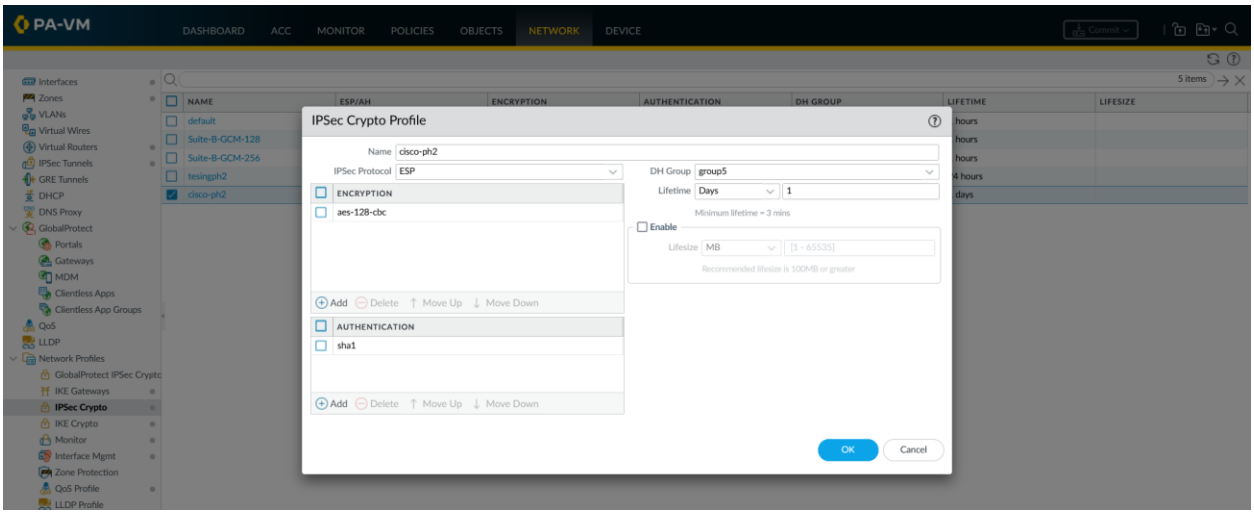

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
1 item
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/1
13.13.13.2..
13.13.13.1
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn

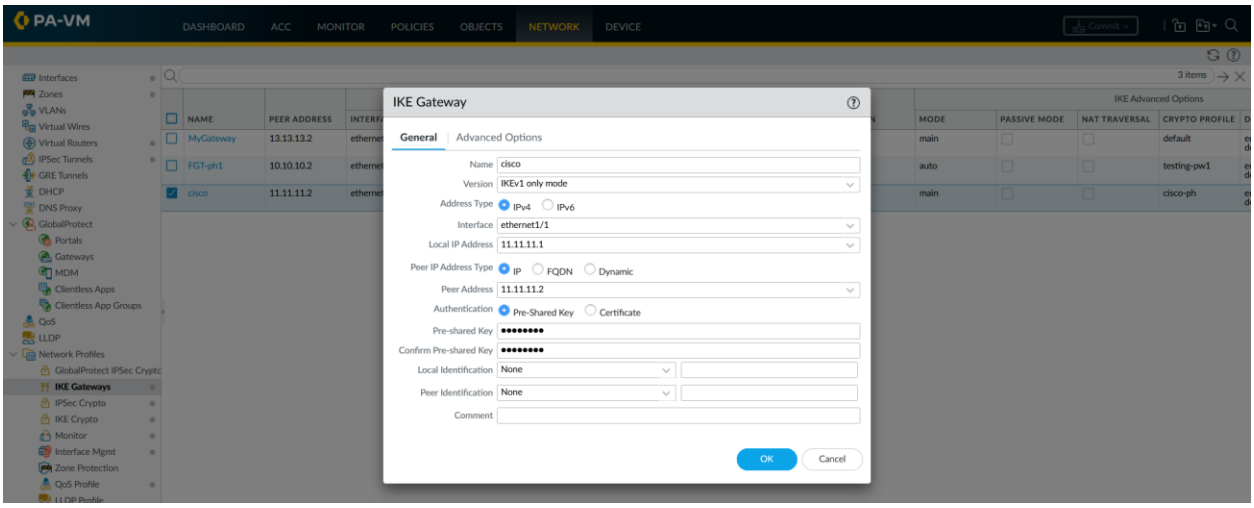


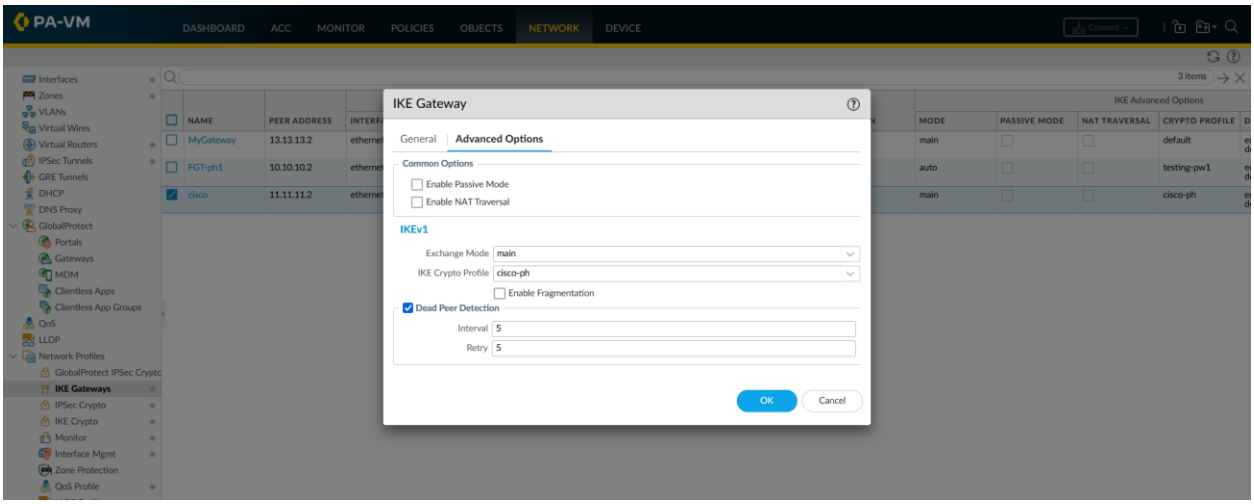
PA-cisco Tunnel

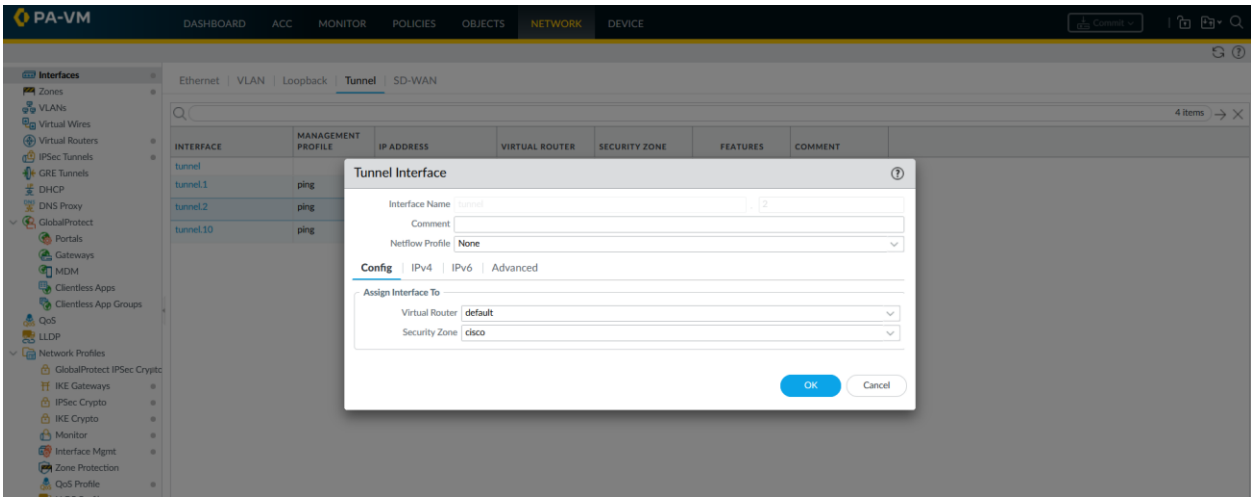
PA

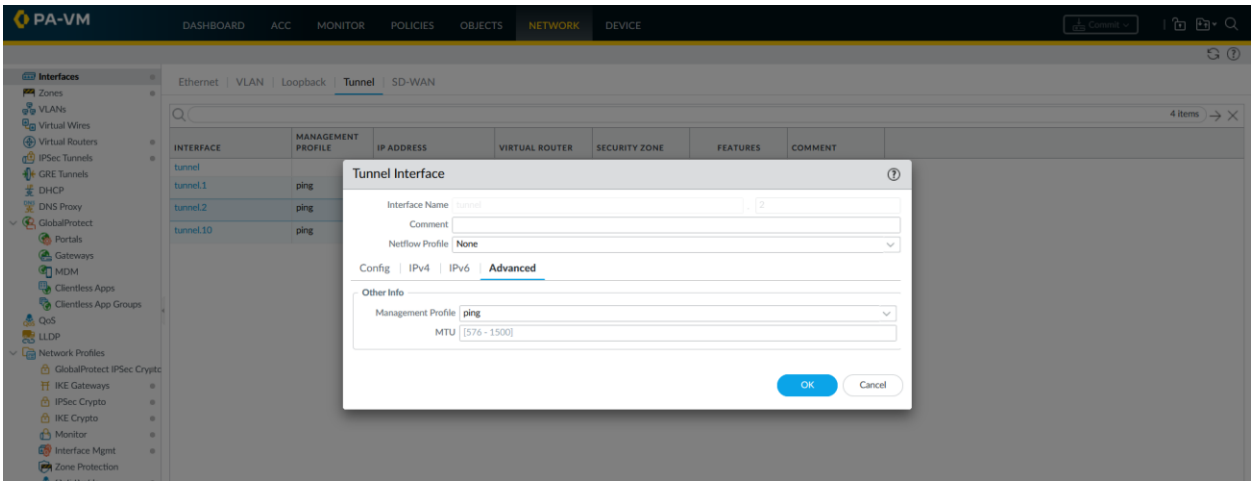


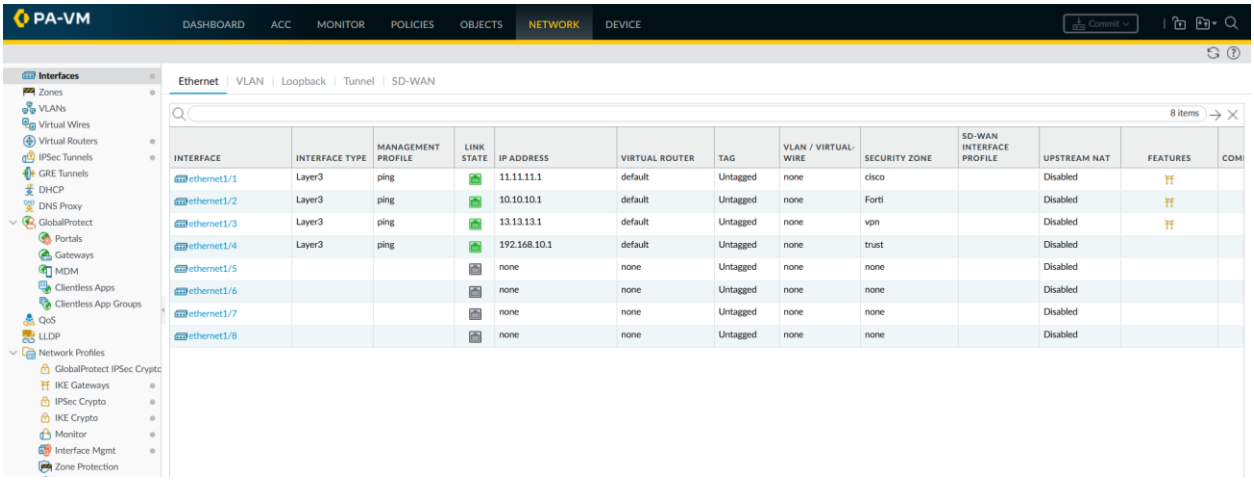


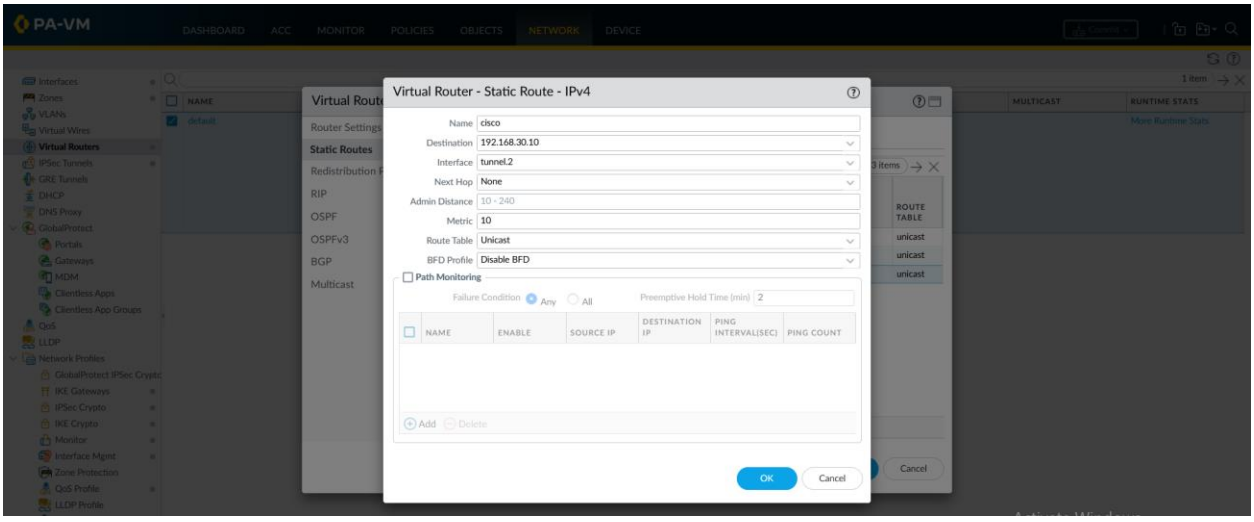

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IKE Gateway
General
Advanced Options
Name cisco
Version IKEv1 only mode
Address Type IPv4 IPv6
Interface ethernet1/1
Local IP Address 11.11.11.1
Peer IP Address Type IP FQDN Dynamic
Peer Address 11.11.11.2
Authentication Pre-Shared Key Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification None
Peer Identification None
Comment
OK
Cancel

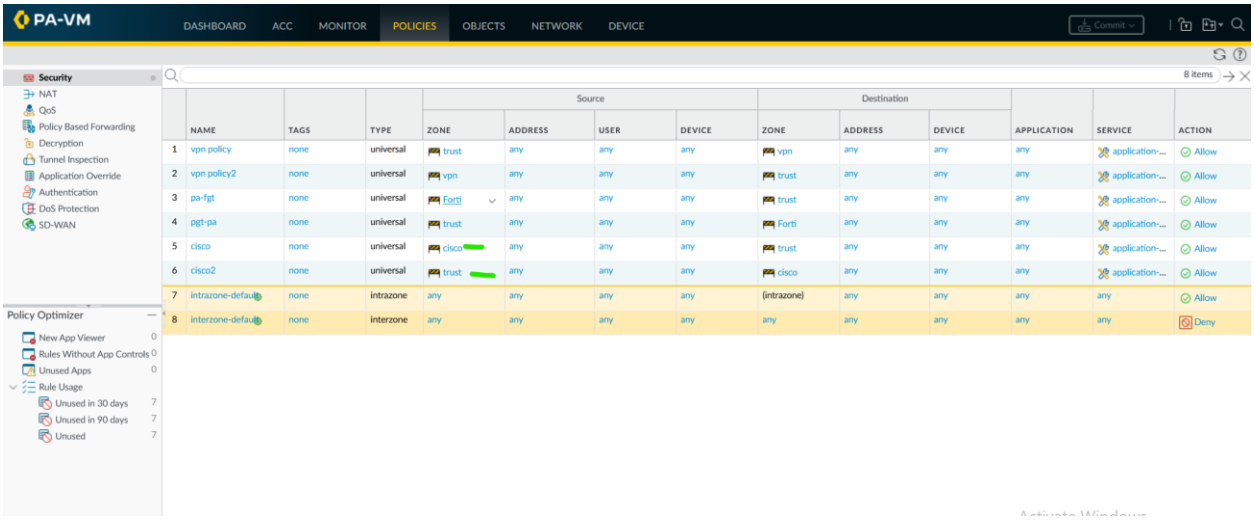

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IKE Gateway
General
Advanced Options
Common Options
Enable Passive Mode
Enable NAT Traversal
IKEv1
Exchange Mode main
IKE Crypto Profile cisco-ph
Enable Fragmentation
Dead Peer Detection
Interval 5
Retry 5
OK
Cancel

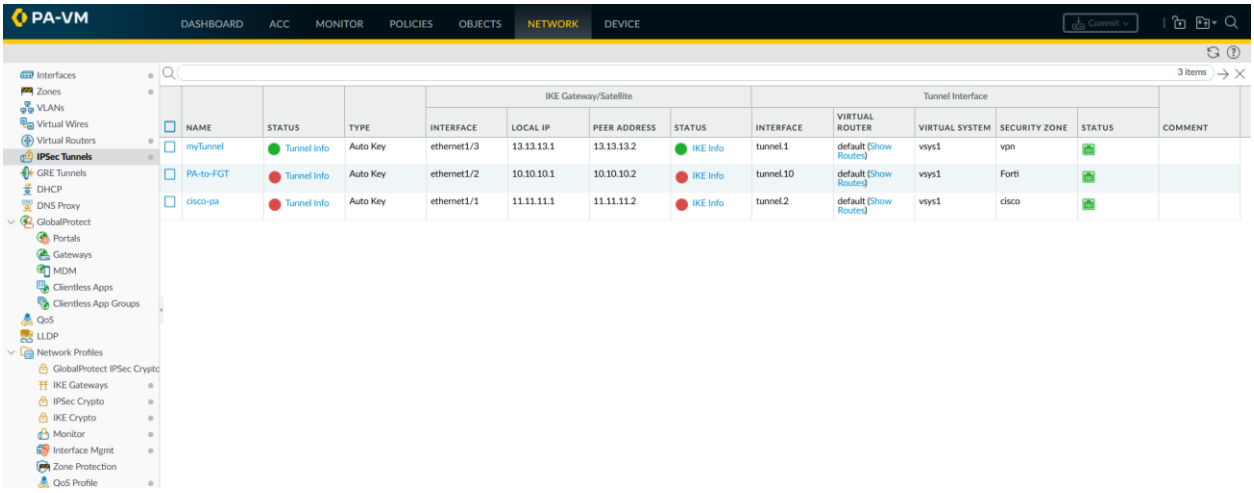

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name tunnel 2
Comment
Netflow Profile None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router default
Security Zone cisco
OK
Cancel


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
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
4 items
INTERFACE
MANAGEMENT PROFILE
IP ADDRESS
VIRTUAL ROUTER
SECURITY ZONE
FEATURES
COMMENT
tunnel
tunnel.1
ping
tunnel.2
ping
tunnel.10
ping
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Other Info
Management Profile
ping
MTU
[576 - 1500]
OK
Cancel


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
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
8 items
INTERFACE
INTERFACE TYPE
MANAGEMENT PROFILE
LINK STATE
IP ADDRESS
VIRTUAL ROUTER
TAG
VLAN / VIRTUAL-WIRE
SECURITY ZONE
SD-WAN INTERFACE PROFILE
UPSTREAM NAT
FEATURES
ethernet1/1 Layer3 ping 11.11.11.1 default Untagged none cisco Disabled
ethernet1/2 Layer3 ping 10.10.10.1 default Untagged none Forti Disabled
ethernet1/3 Layer3 ping 13.13.13.1 default Untagged none vpn Disabled
ethernet1/4 Layer3 ping 192.168.10.1 default Untagged none trust Disabled
ethernet1/5 none none Untagged none none Disabled
ethernet1/6 none none Untagged none none Disabled
ethernet1/7 none none Untagged none none Disabled
ethernet1/8 none none Untagged none none Disabled


PA-VM
Virtual Router - Static Route - IPv4
Name
cisco
Destination
192.168.30.10
Interface
tunnel.2
Next Hop
None
Admin Distance
10 - 240
Metric
10
Route Table
Unicast
BFD Profile
Disable BFD
Path Monitoring
Failure Condition
Any
All
Preemptive Hold Time (min)
2
NAME
ENABLE
SOURCE IP
DESTINATION IP
PING INTERVAL(SEC)
PING COUNT
Add
Delete
OK
Cancel
Router Settings
Static Routes
Redistribution
RIP
OSPF
OSPFv3
BGP
Multicast
ROUTE TABLE
unicast
unicast
unicast

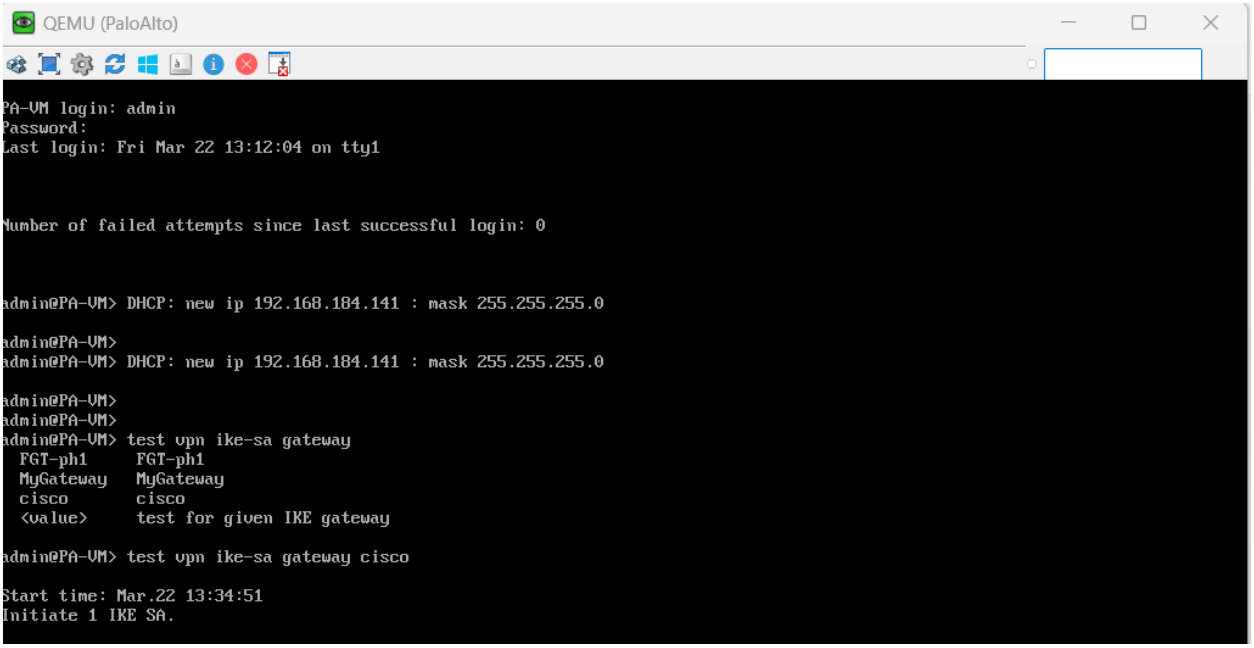

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App Viewer 0
Rules Without App Controls 0
Unused Apps 0
Rule Usage
Unused in 30 days 7
Unused in 90 days 7
Unused 7
8 items
Source
Destination
NAME
TAGS
TYPE
ZONE
ADDRESS
USER
DEVICE
ZONE
ADDRESS
DEVICE
APPLICATION
SERVICE
ACTION
1 vpn policy none universal trust any any any vpn any any any application-... Allow
2 vpn policy2 none universal vpn any any any trust any any any application-... Allow
3 pa-fgt none universal Forti any any any trust any any any application-... Allow
4 pgt-pa none universal trust any any any Forti any any any application-... Allow
5 cisco none universal cisco any any any trust any any any application-... Allow
6 cisco2 none universal trust any any any cisco any any any application-... Allow
7 intrazone-default none intrazone any any any any (intrazone) any any any any Allow
8 interzone-default none interzone any any any any any any any any any Deny

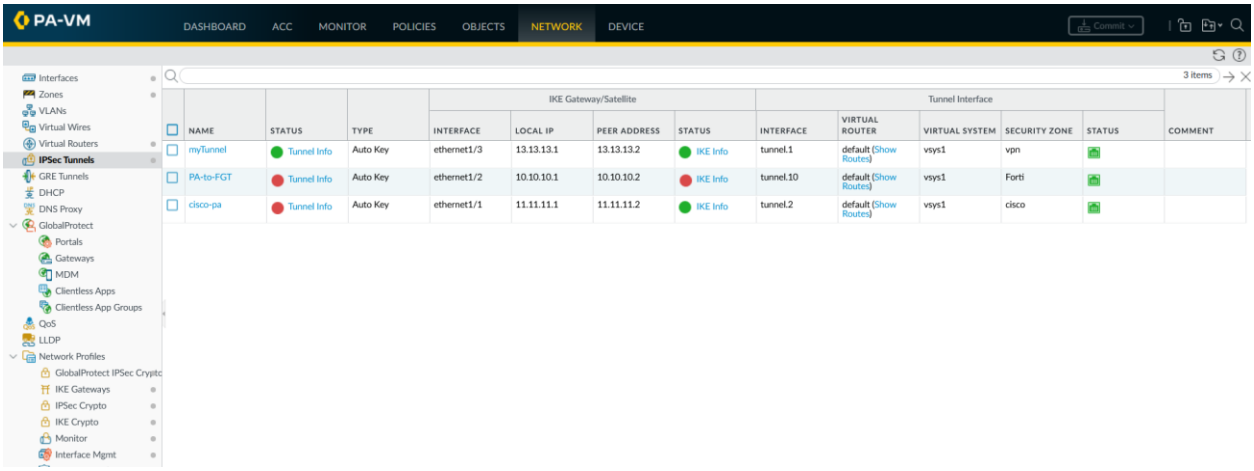

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
3 items
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel Tunnel Info Auto Key ethernet1/3 13.13.13.1 13.13.13.2 IKE Info tunnel.1 default (Show Routes) vsys1 vpn
PA-to-FGT Tunnel Info Auto Key ethernet1/2 10.10.10.1 10.10.10.2 IKE Info tunnel.10 default (Show Routes) vsys1 Forti
cisco-pa Tunnel Info Auto Key ethernet1/1 11.11.11.1 11.11.11.2 IKE Info tunnel.2 default (Show Routes) vsys1 cisco

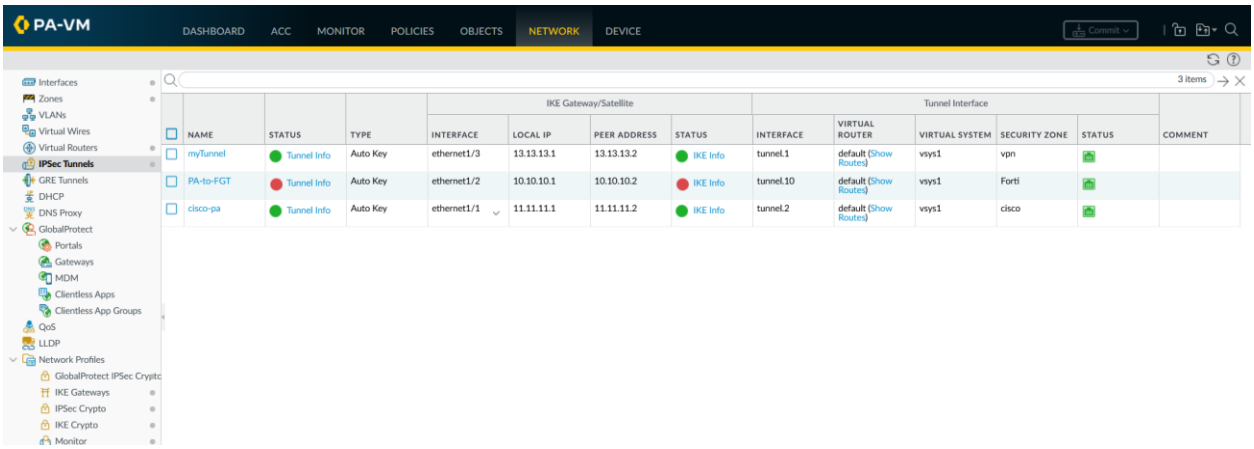
```
!
!
crypto isakmp policy 16
 encr aes
 hash md5
 authentication pre-share
 group 5
!
crypto isakmp policy 20
 encr aes
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key comp123 address 11.11.11.1
crypto isakmp key comp123 address 0.0.0.0
!
!
crypto ipsec transform-set PA-TS esp-aes 256 esp-sha-hmac
 mode transport
crypto ipsec transform-set Test esp-aes esp-sha-hmac
 mode transport
crypto ipsec transform-set TEST esp-aes esp-sha-hmac
 mode tunnel
!
!
!
crypto map CMAP 10 ipsec-isakmp
 set peer 11.11.11.1
 set transform-set TEST
 match address crypto_acl
!
```

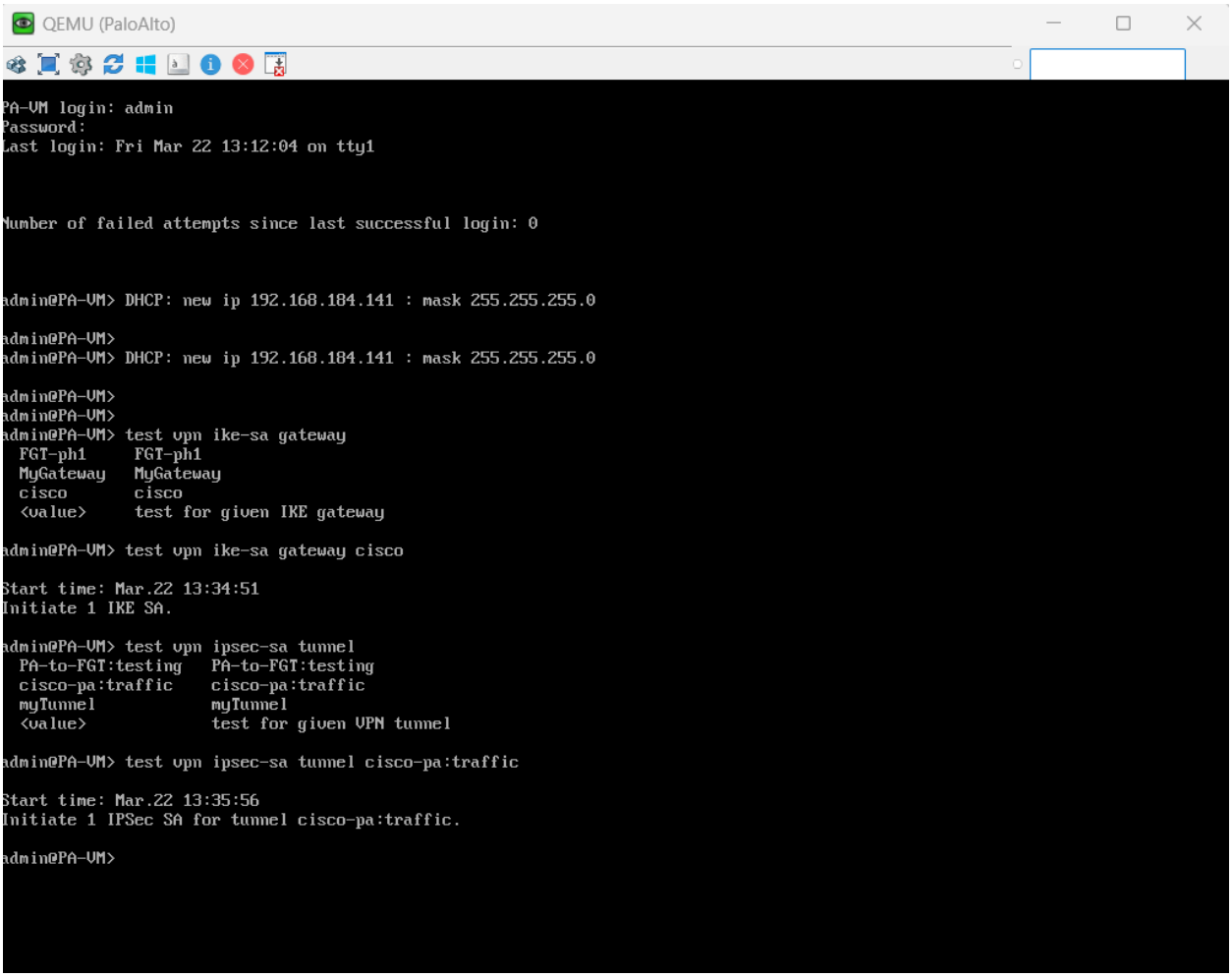
```
!
crypto map PA 20 ipsec-isakmp
 ! Incomplete
 match address crypto-cisco
!
crypto map pa 20 ipsec-isakmp
 set peer 11.11.11.1
 set transform-set Test
 set pfs group5
 match address 101
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
!
interface Ethernet1/0
 ip address 11.11.11.2 255.255.255.0
 duplex full
 crypto map CMAP
!
interface Ethernet1/1
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex full
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
```

```
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended crypto-cisco
 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
ip access-list extended crypto_acl
 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
!
access-list 101 permit ip host 192.168.30.10 any
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
```







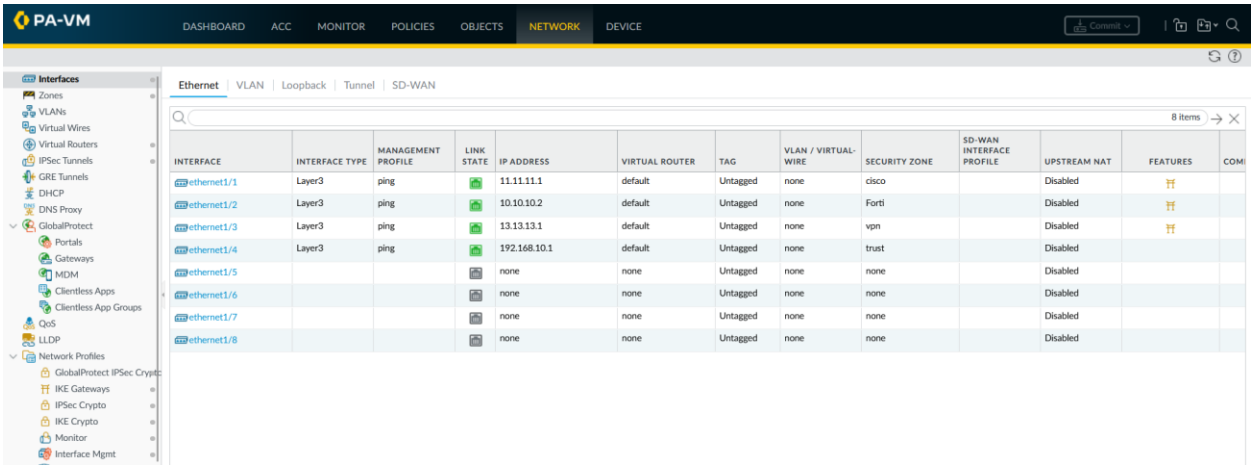


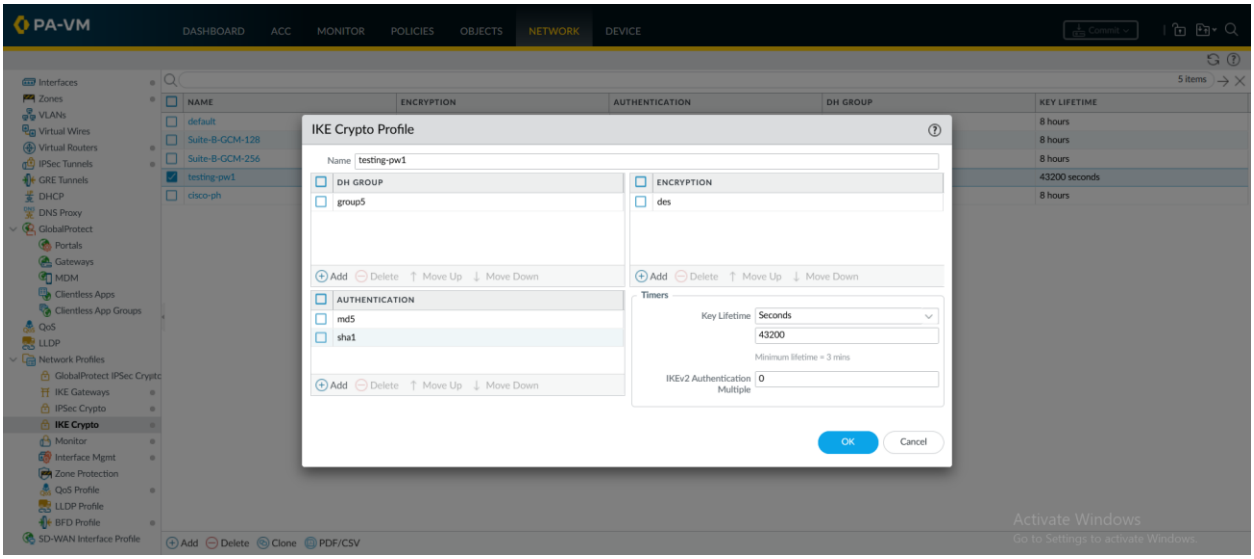
Configuring Cisco

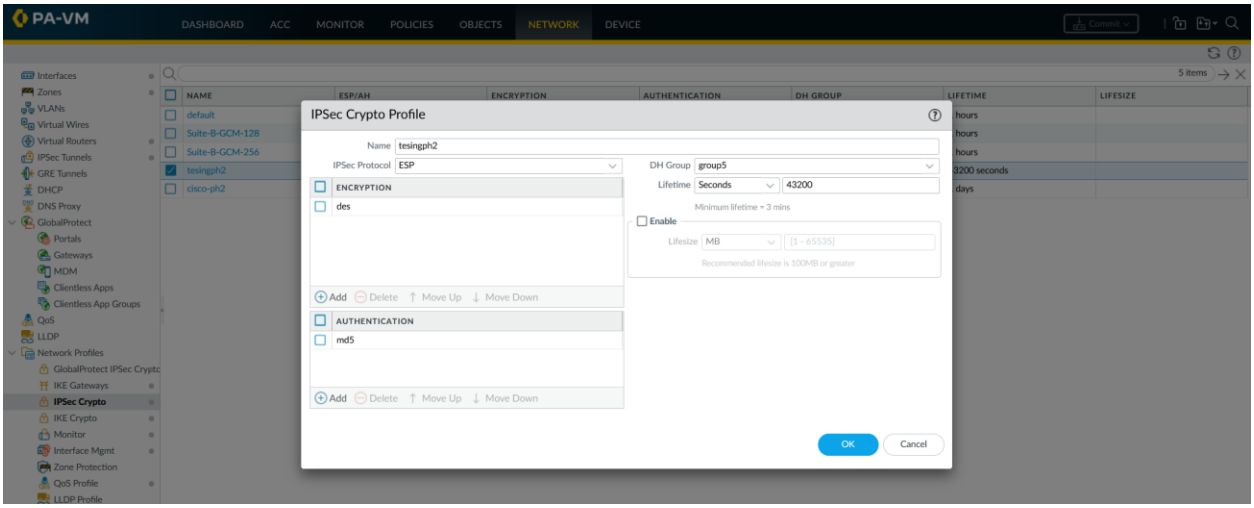
```
ip access-list extended Crypto_Acl
permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
```

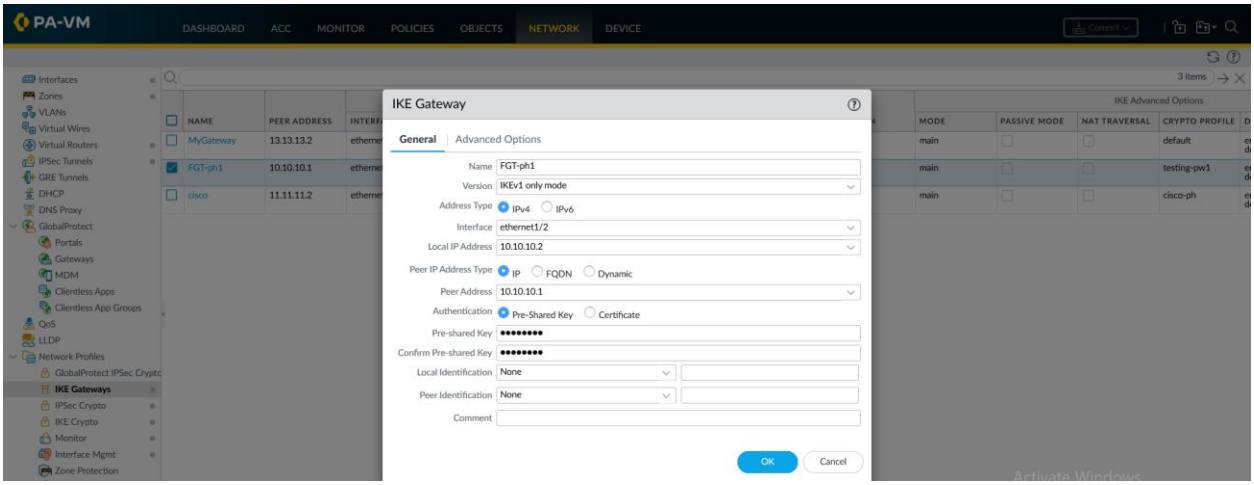
```
crypto isakmp policy 16
encr aes
hash md5
authentication pre-share
group 5

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto map CMAP 10 ipsec-isakmp
set peer 11.11.11.1

set transform-set TSET
match address Crypto_Acl

interface FastEthernet1/0
crypto map CMAP
```

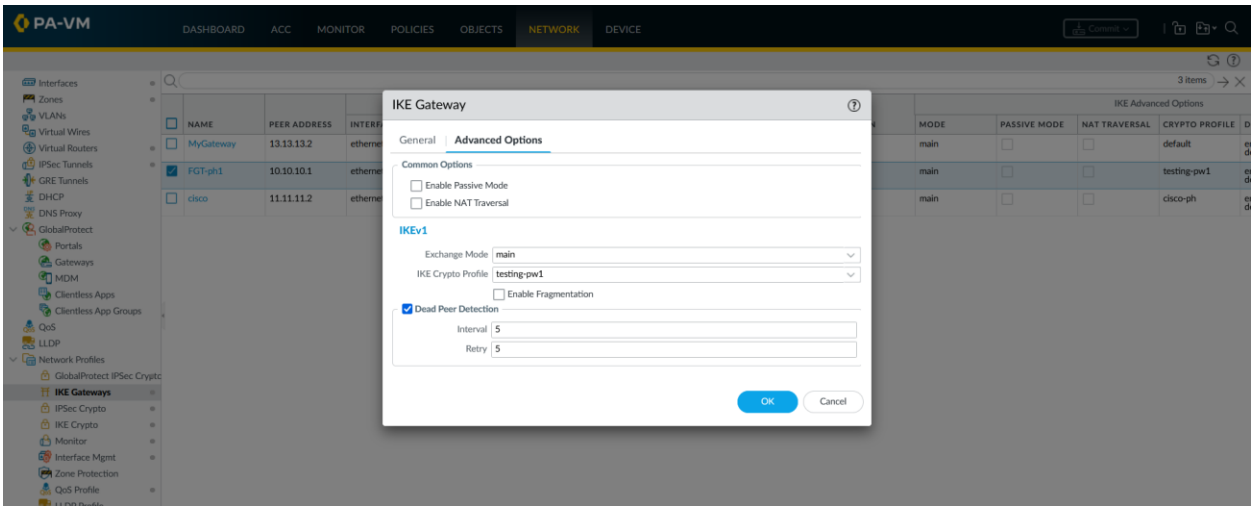
PA-FGT

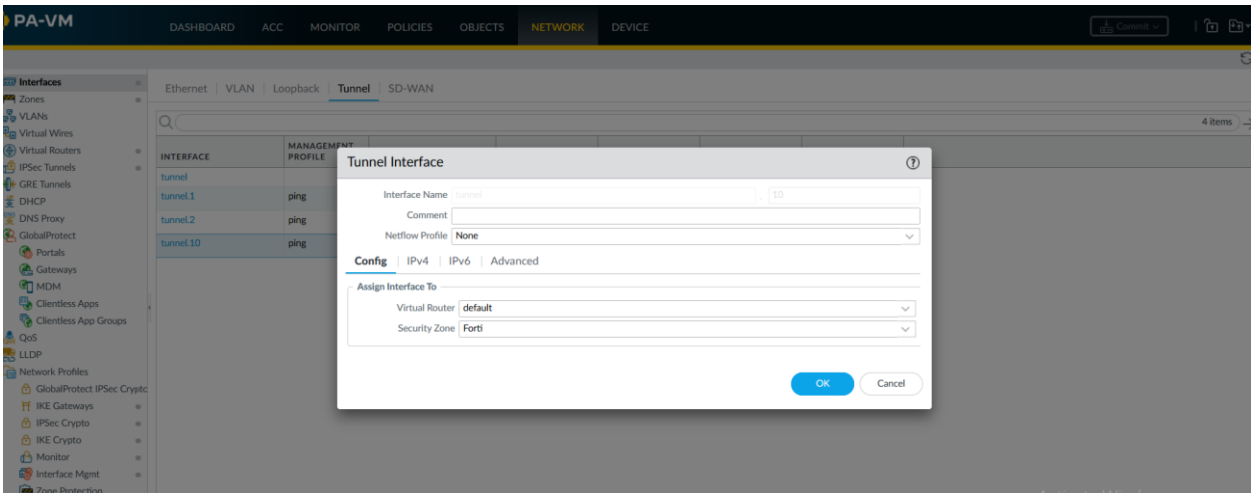


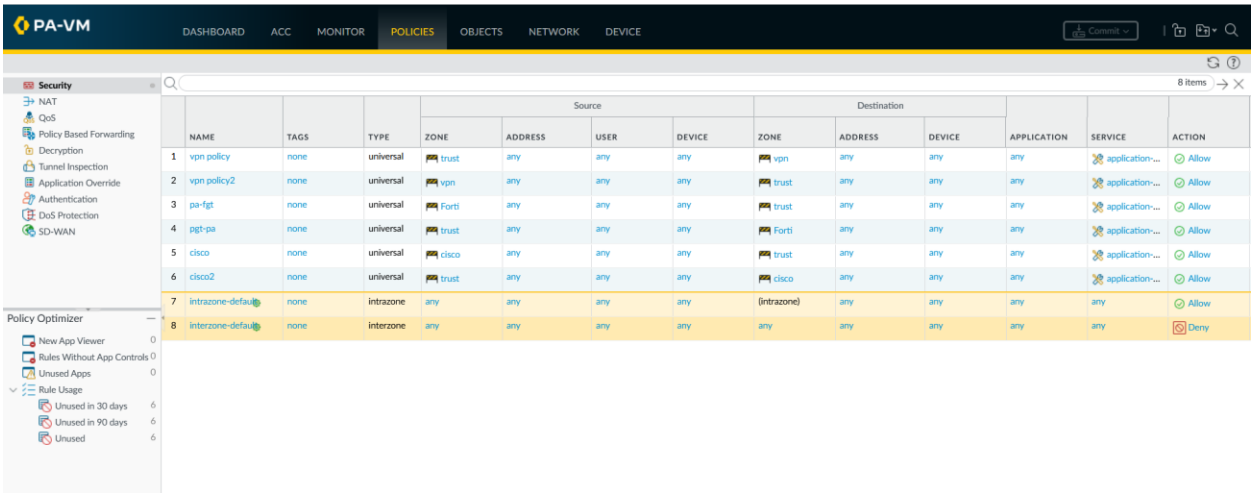

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Crypto Profile
Name testing-pw1
DH GROUP
group5
ENCRYPTION
des
AUTHENTICATION
md5
sha1
Timers
Key Lifetime Seconds
43200
Minimum lifetime = 3 mins
IKEv2 Authentication Multiple 0
OK Cancel

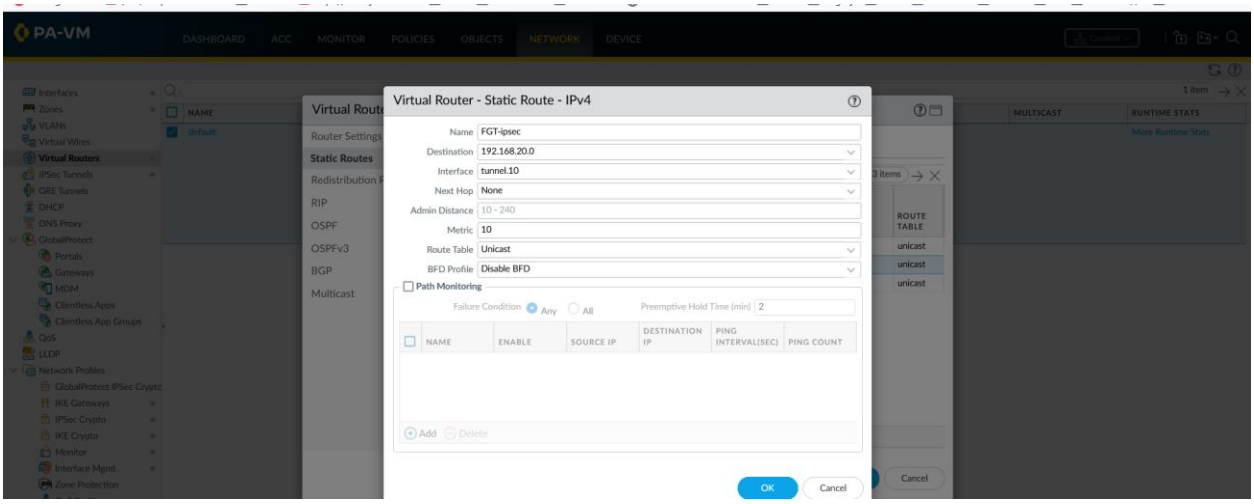

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IPSec Crypto Profile
Name tesingph2
IPSec Protocol ESP
DH Group group5
Lifetime Seconds 43200
Minimum lifetime = 3 mins
Enable
Lifesize MB
ENCRYPTION
des
AUTHENTICATION
md5
OK Cancel

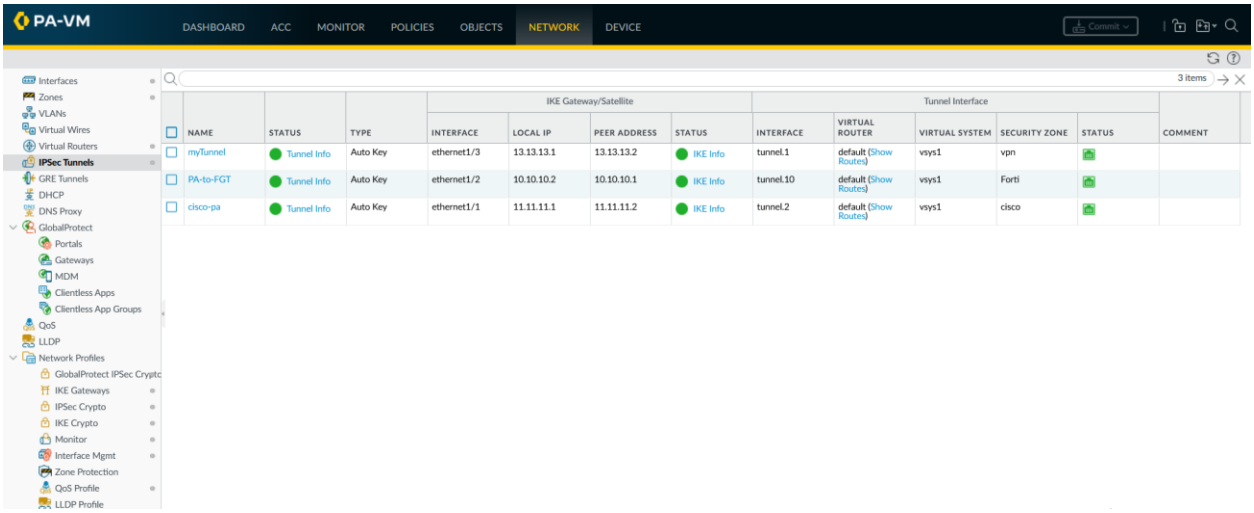

PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
IKE Gateway
General Advanced Options
Name FGT-ph1
Version IKEv1 only mode
Address Type IPv4 IPv6
Interface ethernet1/2
Local IP Address 10.10.10.2
Peer IP Address Type IP FQDN Dynamic
Peer Address 10.10.10.1
Authentication Pre-Shared Key Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification None
Peer Identification None
Comment
OK Cancel


PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
IKE Gateway
General
Advanced Options
Common Options
Enable Passive Mode
Enable NAT Traversal
IKEv1
Exchange Mode
main
IKE Crypto Profile
testing-pw1
Enable Fragmentation
Dead Peer Detection
Interval
5
Retry
5
OK
Cancel

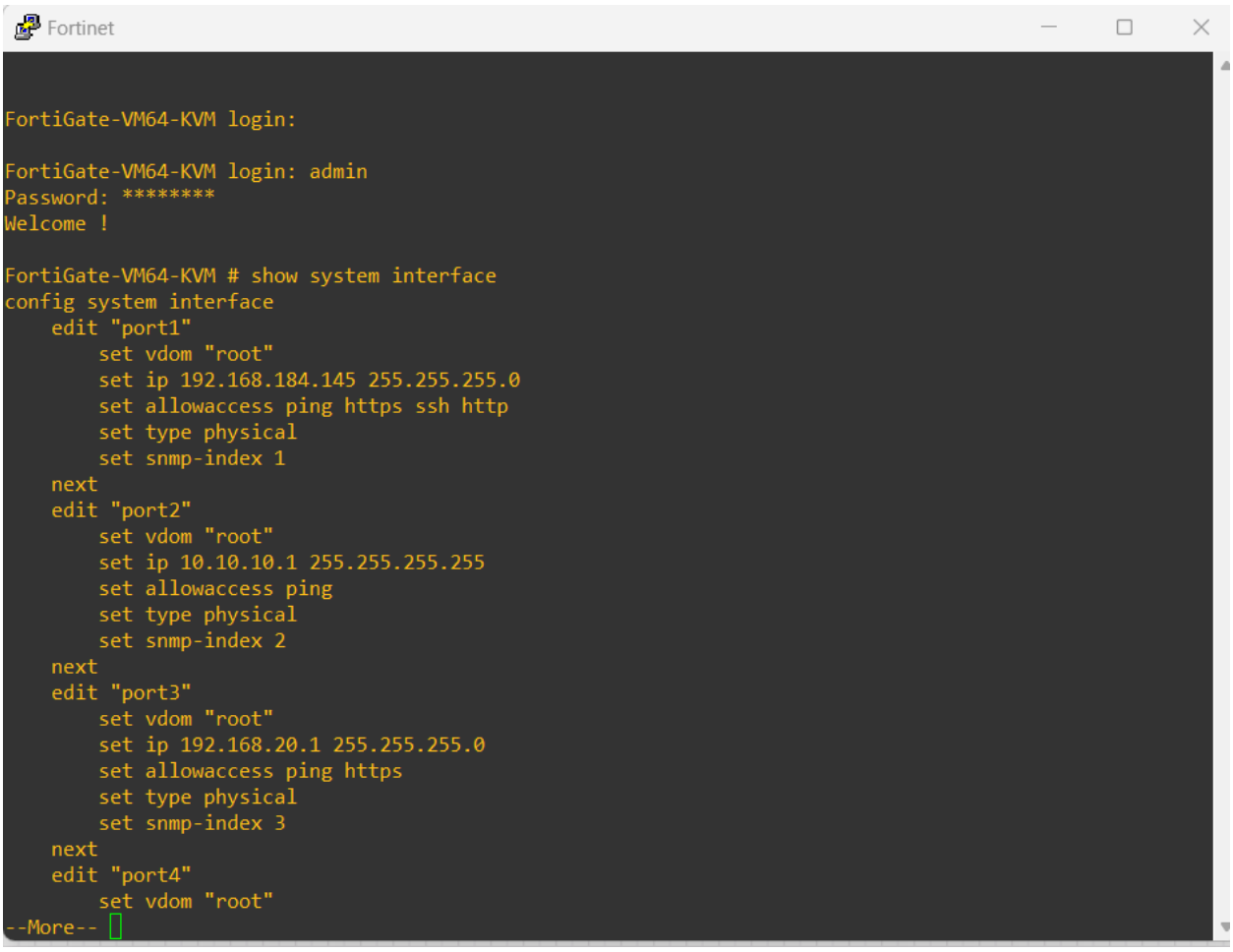

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Ethernet
VLAN
Loopback
Tunnel
SD-WAN
Tunnel Interface
Interface Name
Comment
Netflow Profile
None
Config
IPv4
IPv6
Advanced
Assign Interface To
Virtual Router
default
Security Zone
Forti
OK
Cancel

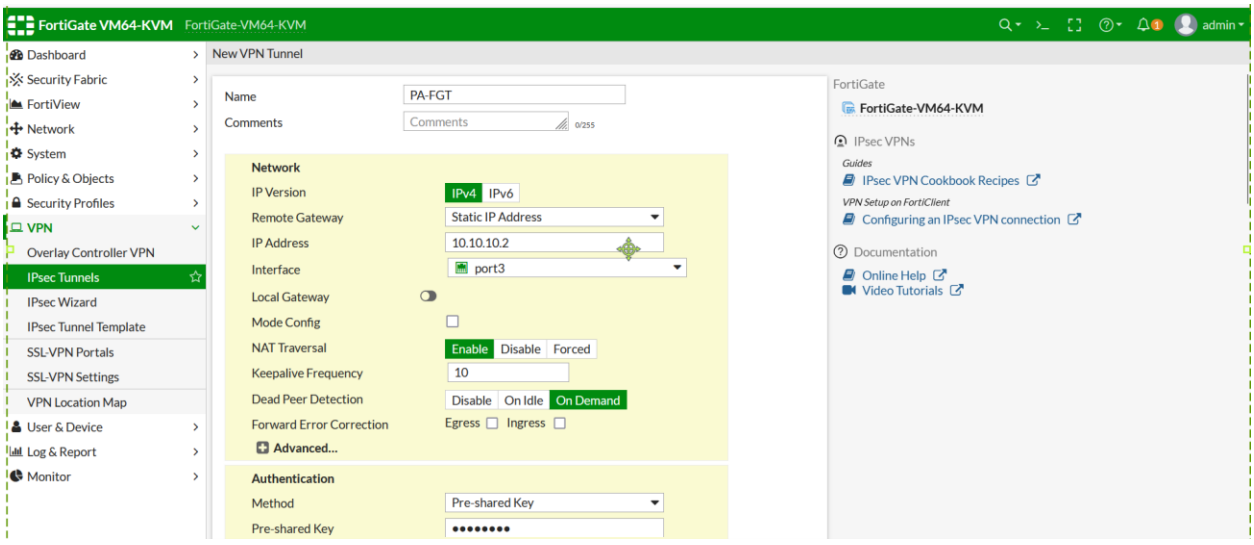

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App Viewer
Rules Without App Controls
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
Source
Destination
NAME
TAGS
TYPE
ZONE
ADDRESS
USER
DEVICE
APPLICATION
SERVICE
ACTION
1 vpn policy none universal trust any any any vpn any any any application-... Allow
2 vpn policy2 none universal vpn any any any trust any any any application-... Allow
3 pa-fgt none universal Forti any any any trust any any any application-... Allow
4 pgt-pa none universal trust any any any Forti any any any application-... Allow
5 cisco none universal cisco any any any trust any any any application-... Allow
6 cisco2 none universal trust any any any cisco any any any application-... Allow
7 intrazone-default none intrazone any any any any (intrazone) any any any any Allow
8 interzone-default none interzone any any any any any any any any any Deny

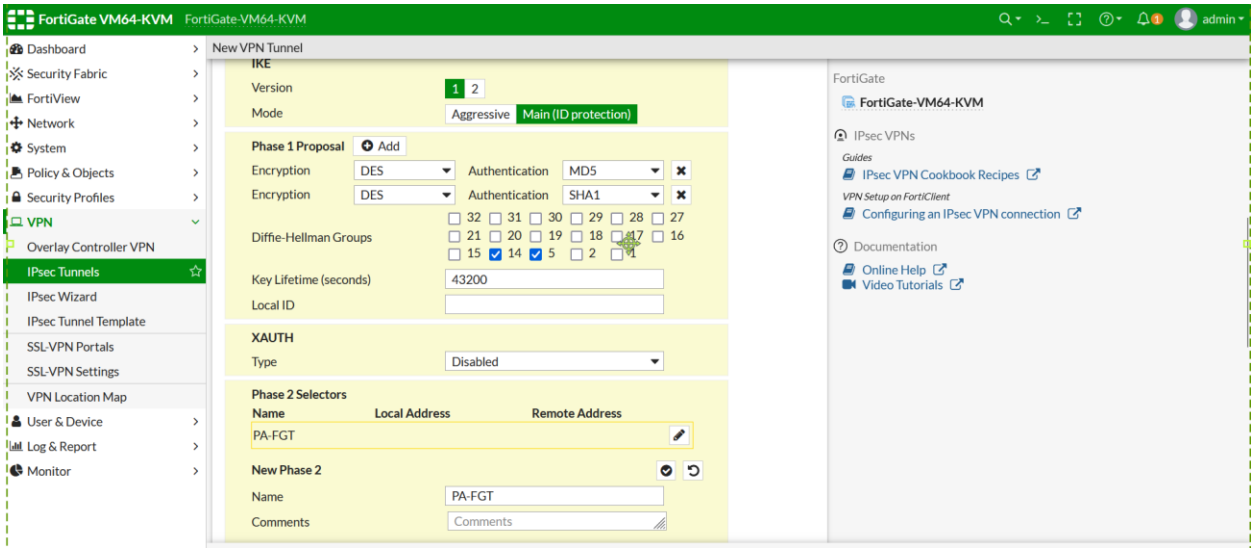

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Virtual Router - Static Route - IPv4
Name FGT-ipsec
Destination 192.168.20.0
Interface tunnel.10
Next Hop None
Admin Distance 10 - 240
Metric 10
Route Table Unicast
BFD Profile Disable BFD
Path Monitoring
Failure Condition Any All
Preemptive Hold Time (min) 2
NAME
ENABLE
SOURCE IP
DESTINATION IP
PING INTERVAL(SEC)
PING COUNT
Add
Delete
OK
Cancel
Router Settings
Static Routes
Redistribution
RIP
OSPF
OSPFv3
BGP
Multicast
MULTICAST
RUNTIME STATS
ROUTE TABLE
unicast

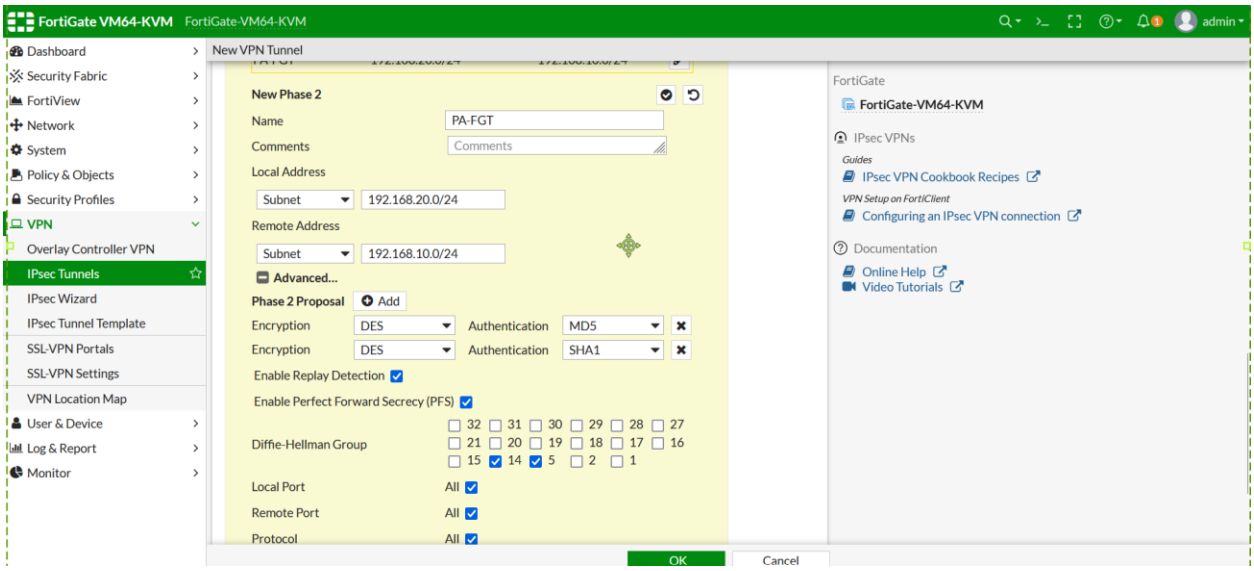

PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
3 items
IKE Gateway/Satellite
Tunnel Interface
NAME
STATUS
TYPE
INTERFACE
LOCAL IP
PEER ADDRESS
STATUS
INTERFACE
VIRTUAL ROUTER
VIRTUAL SYSTEM
SECURITY ZONE
STATUS
COMMENT
myTunnel
Tunnel Info
Auto Key
ethernet1/3
13.13.13.1
13.13.13.2
IKE Info
tunnel.1
default (Show Routes)
vsys1
vpn
PA-to-FGT
Tunnel Info
Auto Key
ethernet1/2
10.10.10.2
10.10.10.1
IKE Info
tunnel.10
default (Show Routes)
vsys1
Forti
cisco-pa
Tunnel Info
Auto Key
ethernet1/1
11.11.11.1
11.11.11.2
IKE Info
tunnel.2
default (Show Routes)
vsys1
cisco
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

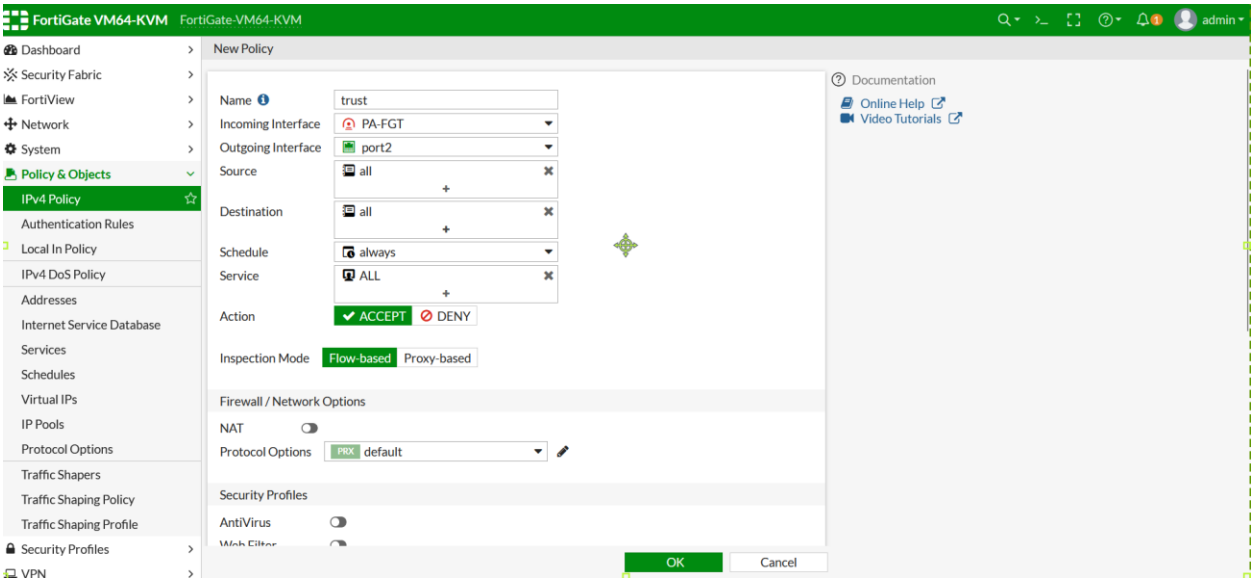
FGT

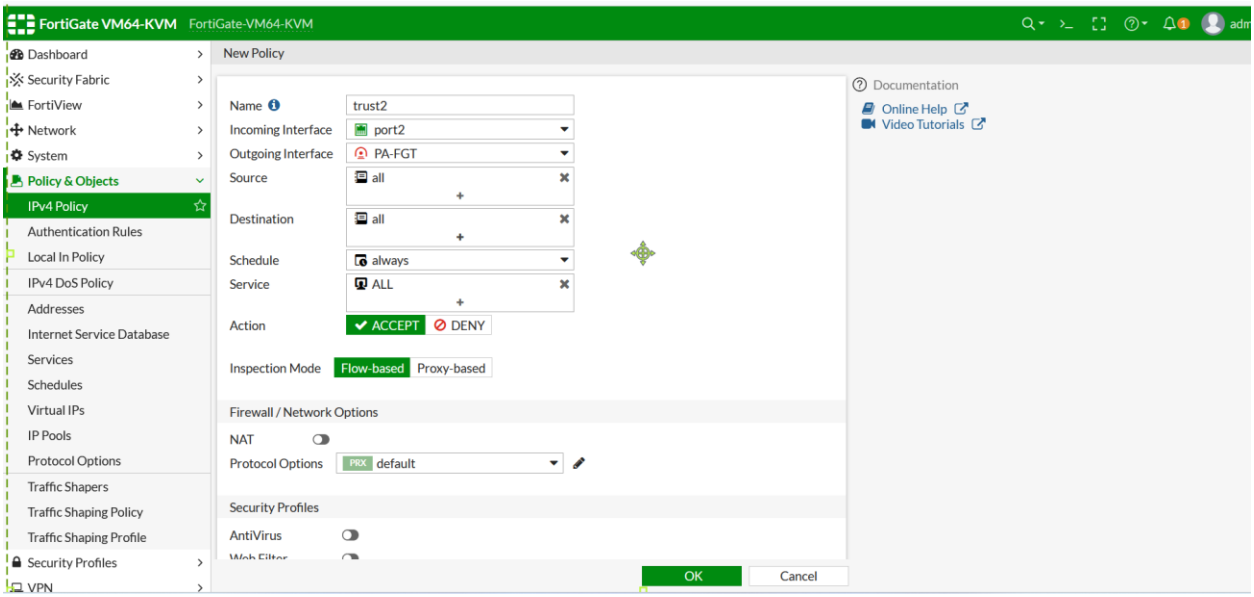

Fortinet
FortiGate-VM64-KVM login:
FortiGate-VM64-KVM login: admin
Password: ********
Welcome !
FortiGate-VM64-KVM # show system interface
config system interface
edit "port1"
set vdom "root"
set ip 192.168.184.145 255.255.255.0
set allowaccess ping https ssh http
set type physical
set snmp-index 1
next
edit "port2"
set vdom "root"
set ip 10.10.10.1 255.255.255.255
set allowaccess ping
set type physical
set snmp-index 2
next
edit "port3"
set vdom "root"
set ip 192.168.20.1 255.255.255.0
set allowaccess ping https
set type physical
set snmp-index 3
next
edit "port4"
set vdom "root"
--More--

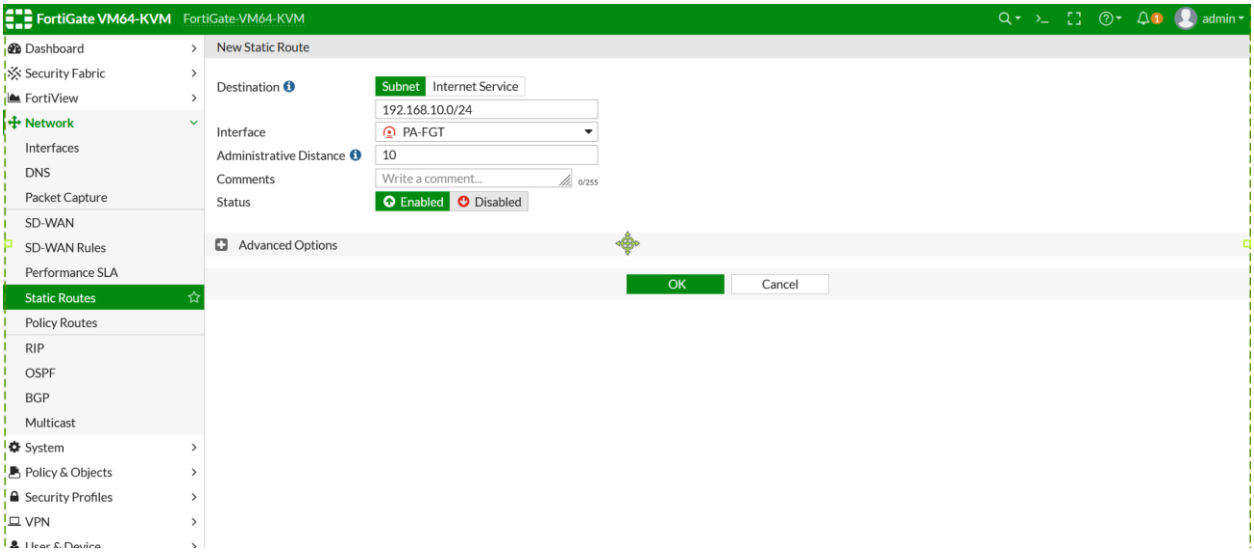

FortiGate VM64-KVM
FortiGate-VM64-KVM
admin
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Device
Log & Report
Monitor
New VPN Tunnel
Name
PA-FGT
Comments
Comments
0/255
Network
IP Version
IPv4
IPv6
Remote Gateway
Static IP Address
IP Address
10.10.10.2
Interface
port3
Local Gateway
Mode Config
NAT Traversal
Enable
Disable
Forced
Keepalive Frequency
10
Dead Peer Detection
Disable
On Idle
On Demand
Forward Error Correction
Egress
Ingress
Advanced...
Authentication
Method
Pre-shared Key
Pre-shared Key
FortiGate
FortiGate-VM64-KVM
IPsec VPNs
Guides
IPsec VPN Cookbook Recipes
VPN Setup on FortiClient
Configuring an IPsec VPN connection
Documentation
Online Help
Video Tutorials

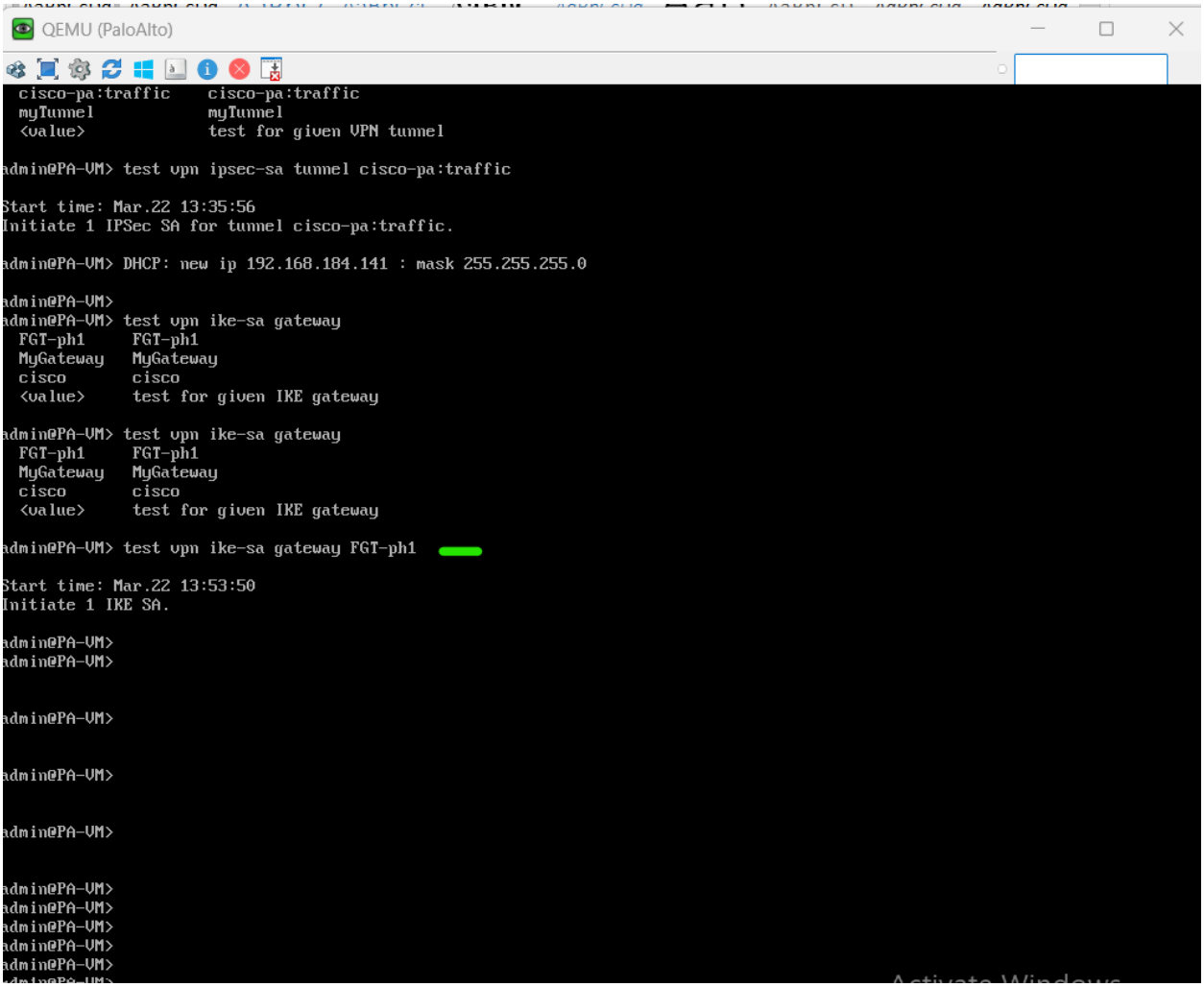

FortiGate VM64-KVM
FortiGate-VM64-KVM
admin
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Device
Log & Report
Monitor
New VPN Tunnel
IKE
Version
1 2
Mode
Aggressive Main (ID protection)
Phase 1 Proposal
Add
Encryption
DES
Authentication
MD5
Encryption
DES
Authentication
SHA1
Diffie-Hellman Groups
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Key Lifetime (seconds)
43200
Local ID
XAUTH
Type
Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
PA-FGT
New Phase 2
Name
PA-FGT
Comments
Comments
FortiGate
FortiGate-VM64-KVM
IPsec VPNs
Guides
IPsec VPN Cookbook Recipes
VPN Setup on FortiClient
Configuring an IPsec VPN connection
Documentation
Online Help
Video Tutorials

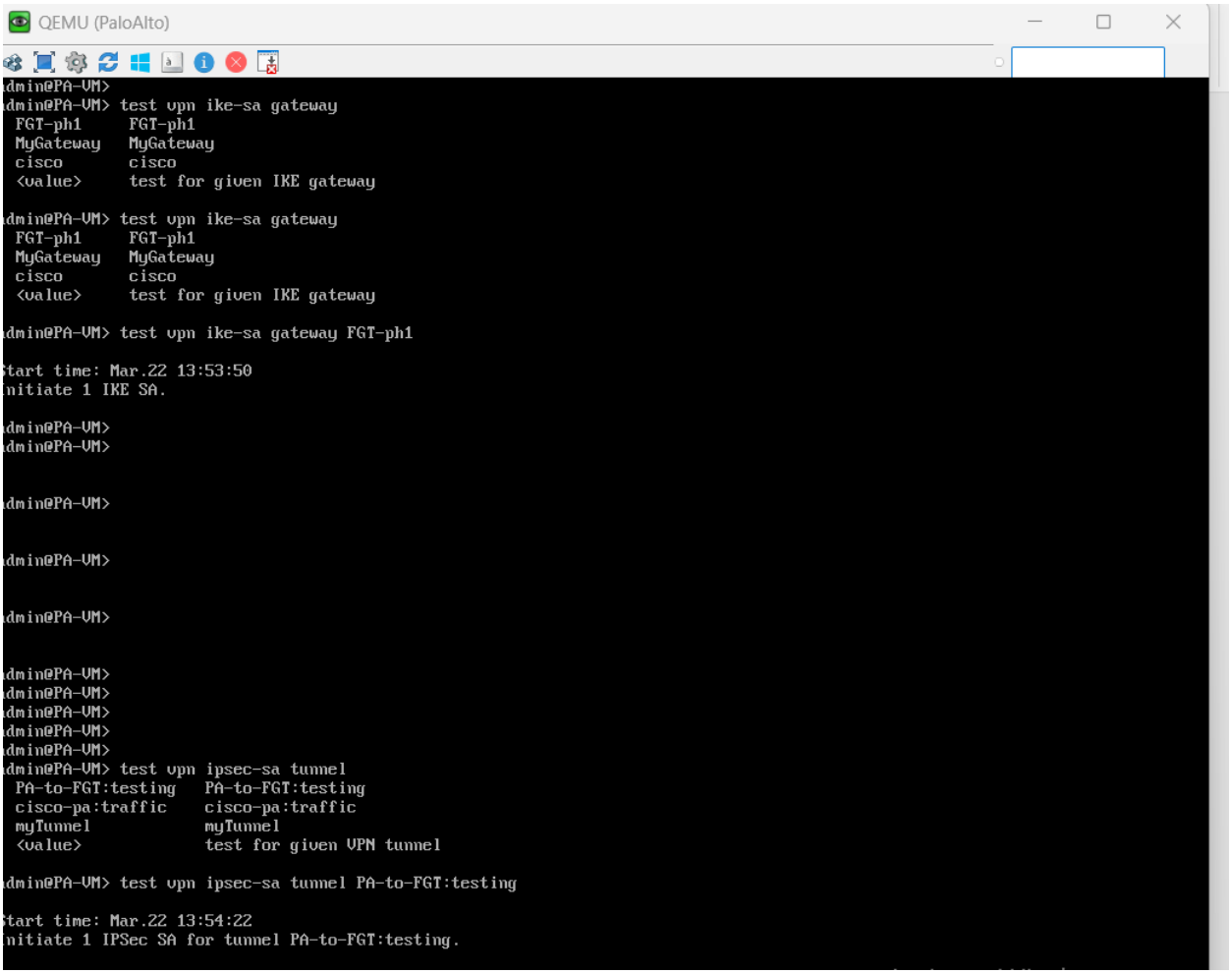

FortiGate VM64-KVM
FortiGate-VM64-KVM
admin
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
VPN Location Map
User & Device
Log & Report
Monitor
New VPN Tunnel
New Phase 2
Name
PA-FGT
Comments
Comments
Local Address
Subnet
192.168.20.0/24
Remote Address
Subnet
192.168.10.0/24
Advanced...
Phase 2 Proposal
Add
Encryption
DES
Authentication
MD5
Encryption
DES
Authentication
SHA1
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
Diffie-Hellman Group
32 31 30 29 28 27
21 20 19 18 17 16
15 14 5 2 1
Local Port
All
Remote Port
All
Protocol
All
OK
Cancel
FortiGate
FortiGate-VM64-KVM
IPsec VPNs
Guides
IPsec VPN Cookbook Recipes
VPN Setup on FortiClient
Configuring an IPsec VPN connection
Documentation
Online Help
Video Tutorials


FortiGate VM64-KVM
FortiGate-VM64-KVM
admin
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Authentication Rules
Local In Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Security Profiles
VPN
New Policy
Name
trust
Incoming Interface
PA-FGT
Outgoing Interface
port2
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
Protocol Options
PRX
default
Security Profiles
AntiVirus
OK
Cancel
Documentation
Online Help
Video Tutorials


FortiGate VM64-KVM
FortiGate-VM64-KVM
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Authentication Rules
Local In Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Security Profiles
VPN
New Policy
Name
trust2
Incoming Interface
port2
Outgoing Interface
PA-FGT
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
Protocol Options
PRX
default
Security Profiles
AntiVirus
OK
Cancel
Documentation
Online Help
Video Tutorials

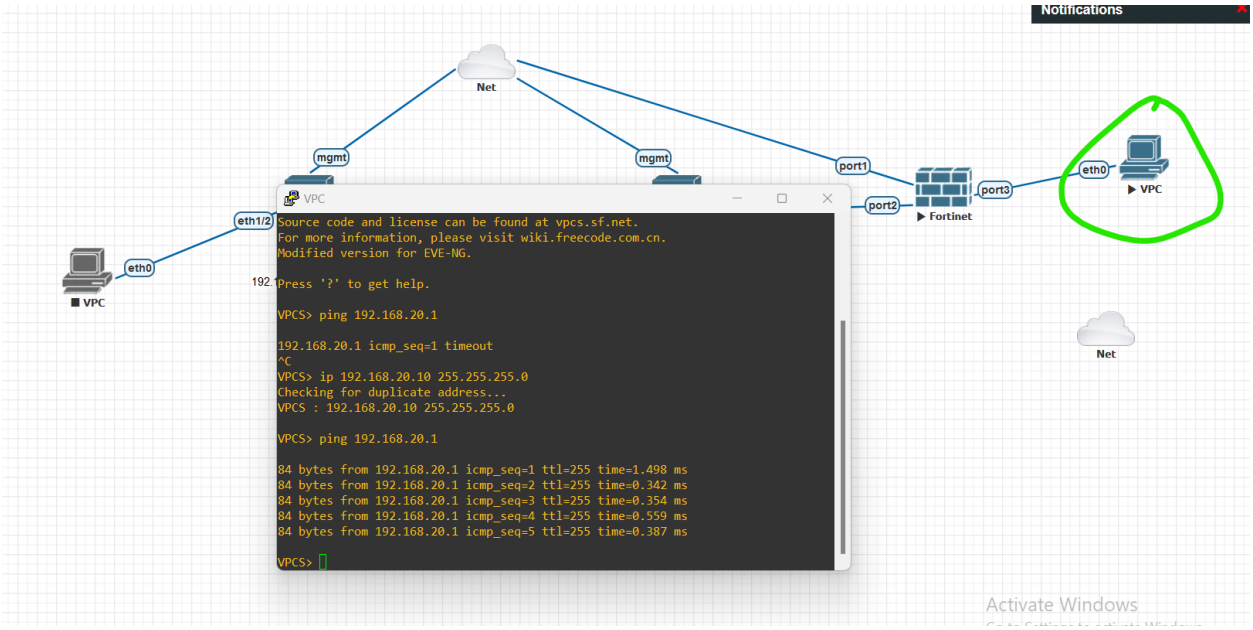

FortiGate VM64-KVM
FortiGate-VM64-KVM
admin
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
New Static Route
Destination
Subnet
Internet Service
192.168.10.0/24
Interface
PA-FGT
Administrative Distance
10
Comments
Write a comment...
0/255
Status
Enabled
Disabled
Advanced Options
OK
Cancel

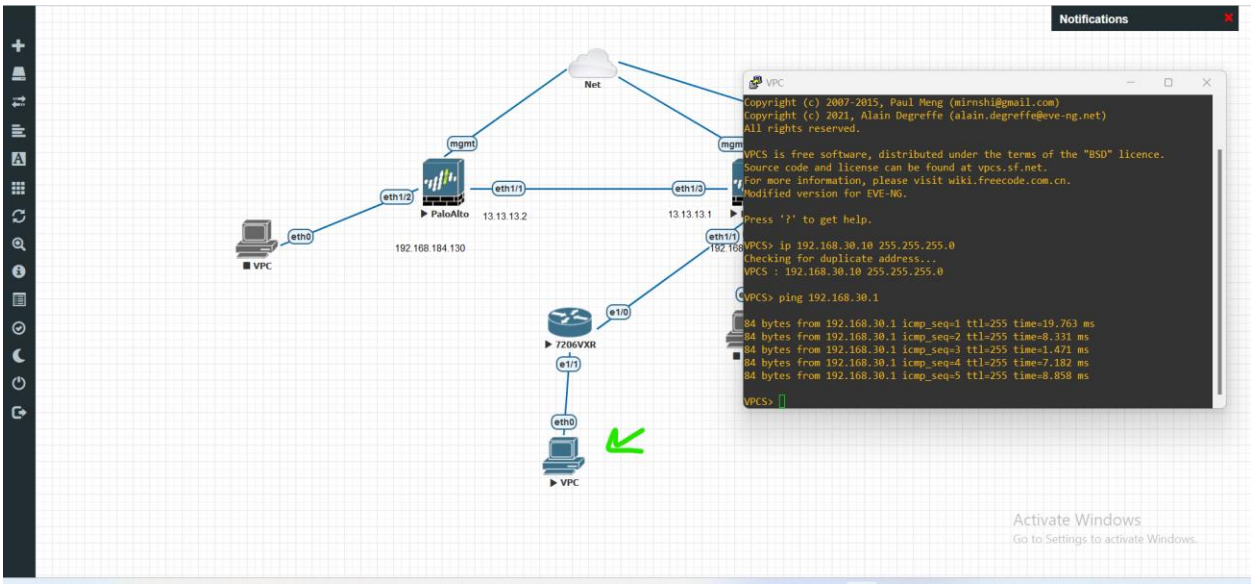

QEMU (PaloAlto)
cisco-pa:traffic cisco-pa:traffic
myTunnel myTunnel
<value> test for given VPN tunnel
admin@PA-VM> test vpn ipsec-sa tunnel cisco-pa:traffic
Start time: Mar.22 13:35:56
Initiate 1 IPSec SA for tunnel cisco-pa:traffic.
admin@PA-VM> DHCP: new ip 192.168.184.141 : mask 255.255.255.0
admin@PA-VM>
admin@PA-VM> test vpn ike-sa gateway
FGT-ph1 FGT-ph1
MyGateway MyGateway
cisco cisco
<value> test for given IKE gateway
admin@PA-VM> test vpn ike-sa gateway
FGT-ph1 FGT-ph1
MyGateway MyGateway
cisco cisco
<value> test for given IKE gateway
admin@PA-VM> test vpn ike-sa gateway FGT-ph1
Start time: Mar.22 13:53:50
Initiate 1 IKE SA.
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>
admin@PA-VM>

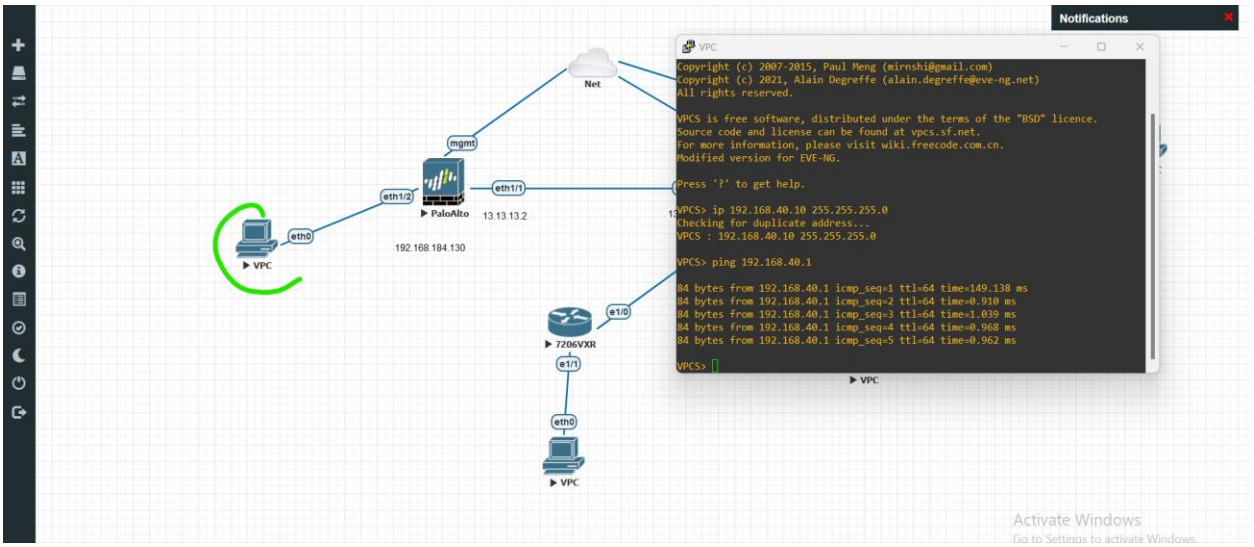

QEMU (PaloAlto)
dmin@PA-VM>
dmin@PA-VM> test vpn ike-sa gateway
FGT-ph1 FGT-ph1
MyGateway MyGateway
cisco cisco
<value> test for given IKE gateway
dmin@PA-VM> test vpn ike-sa gateway
FGT-ph1 FGT-ph1
MyGateway MyGateway
cisco cisco
<value> test for given IKE gateway
dmin@PA-VM> test vpn ike-sa gateway FGT-ph1
tart time: Mar.22 13:53:50
nitiate 1 IKE SA.
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM>
dmin@PA-VM> test vpn ipsec-sa tunnel
PA-to-FGT:testing PA-to-FGT:testing
cisco-pa:traffic cisco-pa:traffic
myTunnel myTunnel
<value> test for given VPN tunnel
dmin@PA-VM> test vpn ipsec-sa tunnel PA-to-FGT:testing
tart time: Mar.22 13:54:22
nitiate 1 IPSec SA for tunnel PA-to-FGT:testing.

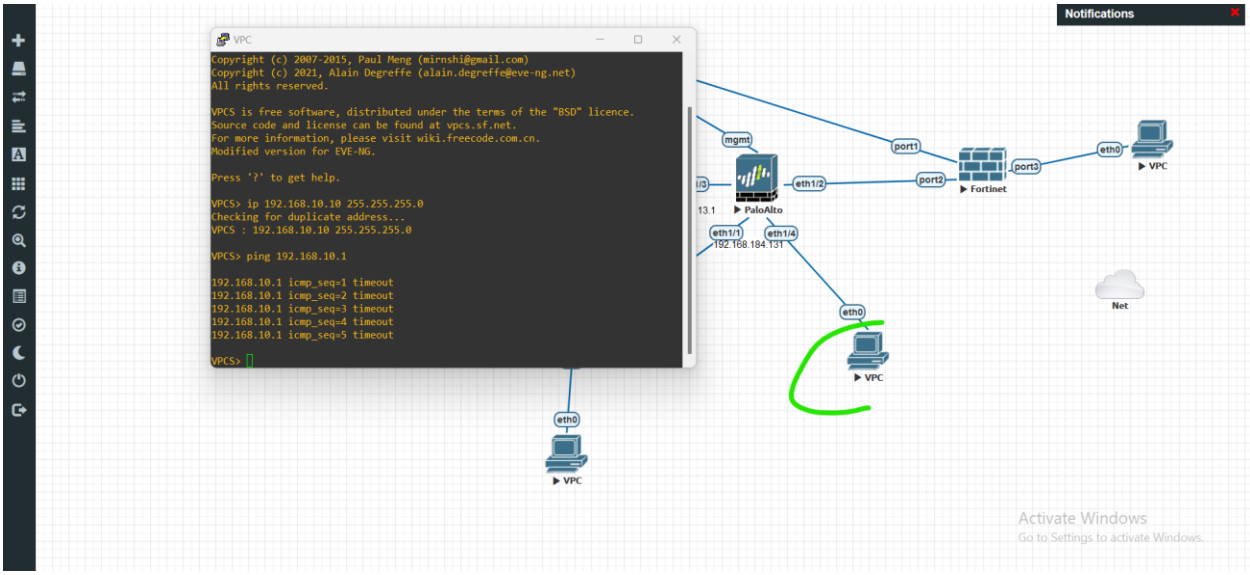
Fortinet

```
        set allowaccess ping https
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical

FortiGate-VM64-KVM # Timeout


FortiGate-VM64-KVM login:

FortiGate-VM64-KVM login:

FortiGate-VM64-KVM login:

FortiGate-VM64-KVM login: admin
Password: ********
Welcome !

FortiGate-VM64-KVM # execute ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms

FortiGate-VM64-KVM #
```




Notifications
Net
mgmt
eth1/2
eth1/1
eth1/3
PaloAlto
13.13.13.2
13.13.13.1
192.168.184.130
eth0
VPC
e1/0
7206VXR
e1/1
eth0
VPC
VPC
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.
Press '?' to get help.
VPCS> ip 192.168.30.10 255.255.255.0
Checking for duplicate address...
VPCS : 192.168.30.10 255.255.255.0
VPCS> ping 192.168.30.1
84 bytes from 192.168.30.1 icmp_seq=1 ttl=255 time=19.763 ms
84 bytes from 192.168.30.1 icmp_seq=2 ttl=255 time=8.331 ms
84 bytes from 192.168.30.1 icmp_seq=3 ttl=255 time=1.471 ms
84 bytes from 192.168.30.1 icmp_seq=4 ttl=255 time=7.182 ms
84 bytes from 192.168.30.1 icmp_seq=5 ttl=255 time=8.858 ms
VPCS>
Activate Windows
Go to Settings to activate Windows.


Notifications
Net
mgmt
eth1/2
eth1/1
PaloAlto
13.13.13.2
192.168.184.130
eth0
VPC
e1/0
7206VXR
e1/1
eth0
VPC
VPC
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.
Press '?' to get help.
VPCS> ip 192.168.40.10 255.255.255.0
Checking for duplicate address...
VPCS : 192.168.40.10 255.255.255.0
VPCS> ping 192.168.40.1
84 bytes from 192.168.40.1 icmp_seq=1 ttl=64 time=149.138 ms
84 bytes from 192.168.40.1 icmp_seq=2 ttl=64 time=0.910 ms
84 bytes from 192.168.40.1 icmp_seq=3 ttl=64 time=1.039 ms
84 bytes from 192.168.40.1 icmp_seq=4 ttl=64 time=0.968 ms
84 bytes from 192.168.40.1 icmp_seq=5 ttl=64 time=0.962 ms
VPCS>
Activate Windows
Go to Settings to activate Windows.


VPC
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.
Press '?' to get help.
VPCS> ip 192.168.10.10 255.255.255.0
Checking for duplicate address...
VPCS : 192.168.10.10 255.255.255.0
VPCS> ping 192.168.10.1
192.168.10.1 icmp_seq=1 timeout
192.168.10.1 icmp_seq=2 timeout
192.168.10.1 icmp_seq=3 timeout
192.168.10.1 icmp_seq=4 timeout
192.168.10.1 icmp_seq=5 timeout
VPCS>
Notifications
mgmt
port1
port2
port3
eth1/2
eth1/1
eth1/4
192.168.184.131
PaloAlto
Fortinet
eth0
VPC
Net
Activate Windows
Go to Settings to activate Windows.