NAME: Ikem Mercy Ogechi

STUDENT ID: 8859960

COURSE CODE: INFO-8501-23S

PROFESSOR NAME: Tariq Mahmood .

DUE DATE: 9th August 2023

Table of Contents

DESCRIPTION

This project will involve me designing and implementing a site-to-site Virtual Private Network (VPN) solution to meet some specific needs and policy requirements. The aim of this is to provide secure access to servers and the internet for staff and guests at both the Headquarter and Branch site while following to the naming conventions and subnet allocations.

HEADQUARTER SITE

REQUIREMENT

In the headquarters site, I followed the required or provided policy that must be met for the site-to-site VPN solution:

✓ STAFF ACCESS TO SERVERS:

- All staff members at the headquarters site should have access to the servers located at the headquarters.

✓ INTERNET ACCESS FOR STAFF:

- All staff members at the headquarters site should have access to the Internet.

✓ Guest Internet Access:

- Guests visiting the headquarters site should have access to the Internet only.

✓ INTERNET ACCESS SOURCE:

- Internet access for all hosts located at the headquarters site must originate from within the headquarters site.

✓ ACCESS TO INTERNET VIA NAT:

- All access to the Internet from the headquarters site should go through Network Address Translation (NAT).

All this requirement is going to be implemented in my design and I will implement the site-to-site vpn for the headquarters site.

DESIGN

✓ NETWORK TOPOLOGY

Router 1:

- eth0/0 is connected to BR router (**172.16.20.1/30** in the **172.16.20.0/30** subnet)
- eth0/1 is connected to my Palo Alto Firewall (**172.16.20.6/30** in the **172.16.20.4/30** subnet)

Palo Alto Firewall:

- eth1/1 **(172.16.20.6/30)** in the **MI9960-internet zone.**
- eth1/2 **(172.16.30.1/24**) in the **MI9960-inside zone**.
- eth1/3 **(172.16.40.1/24)** in the **MI9960-guest zone**.
- eth1/4 **(172.16.50.1/24)** in the **MI9960-dmz zone.**
- **Staff VM1** (**172.16.20.6/30)** in the **172.16.30.0/24** network.
- **Guest VM2 (172.16.40.6/24)** in the **172.16.40.0/24** network.
- **Server VM3 (172.16.50.3/24)** in the **172.16.50.0/4** network.

✓ IP ADDRESSING:

- I utilize VLSM (variable length subnet mask) to assign my IP addresses to all my devices in my HQ site, including my routers, firewalls, and VM.

✓ INTERNET ACCESS

- I established an internet connection through my Palo Alto firewall with IP address of **10.173.254.58 (kit 64)**
- I also set up a **NAT (Network Address Translation)** on the Palo Alto Firewall to allow all internal devices to access the internet using a shared IP address.

✓ SERVER ACCESS

- I configured my ACLs on the Palo Alto Firewall to permit my staff access to the server VM 3(**172.16.50.3)** in the **MI9960-dmz zone.**

✓ VPN IMPLEMENTATION

- I Implemented a site-to-site VPN tunnel between Router 1 and Router 2 for secure communication between the HQ site and the branch site.

✓ FIREWALL AND SECURITY

- I configured firewall rules on the Palo Alto firewall to allow necessary incoming and outgoing traffic for each zone while blocking unauthorized or unwanted traffic.

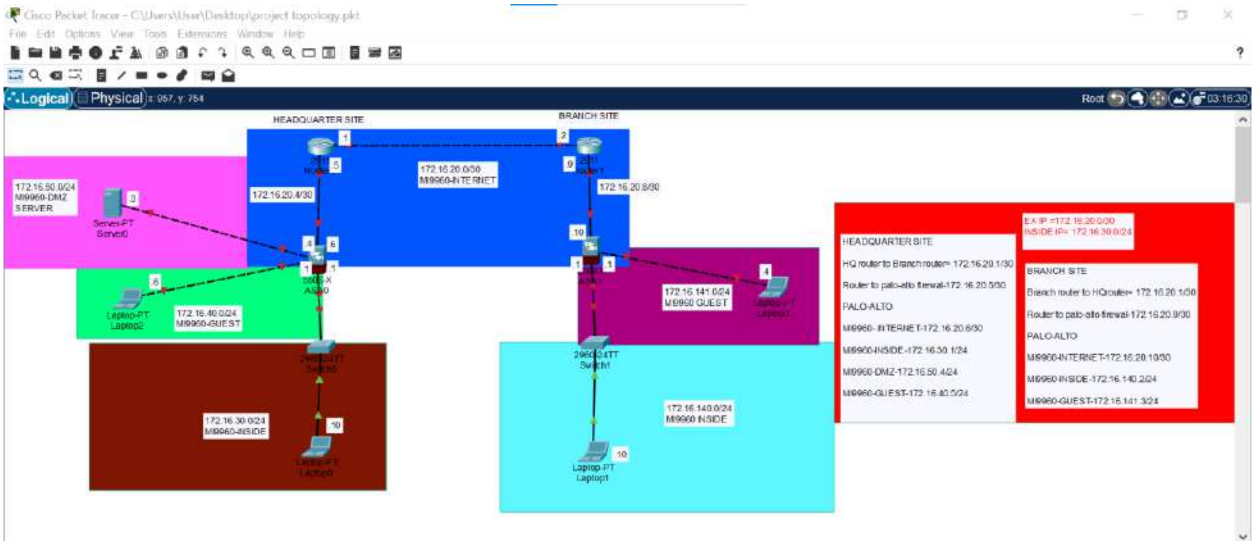
✓ NAME CONVENTION

- I updated the design document to include the new devices, IP addressing, interface connections, and ACL configured related to the Palo Alto Firewall and the additional subnets for staff, guest, and server networks.

✓ CONCLUSION

By offering secure access to internal resources, Internet connectivity for employees and visitors, and a strong site-to-site VPN for communication with the branch site, this design seeks to comply with the policy requirements for the headquarters site. A scalable and secure network environment will be produced by using virtual machines, Cisco routers, and a Palo Alto Firewall. The successful implementation of the VPN solution will be ensured by routine testing and verification.

SCREENSHOT



EX IP =172.16.20.0/30
INSIDE IP= 172.16.30.0/24

HEADQUARTER SITE

HQ router to Branch router= 172.16.20.1/30

Router to palo-alto firewall-172.16.20.5/30

PALO-ALTO

MI9960- INTERNET-172.16.20.6/30

MI9960-INSIDE-172.16.30.1/24

MI9960-DMZ-172.16.50.4/24

MI9960-GUEST-172.16.40.5/24

BRANCH SITE

Branch router to HQrouter= 172.16.20.1/30

Router to palo-alto firewal-172.16.20.9/30

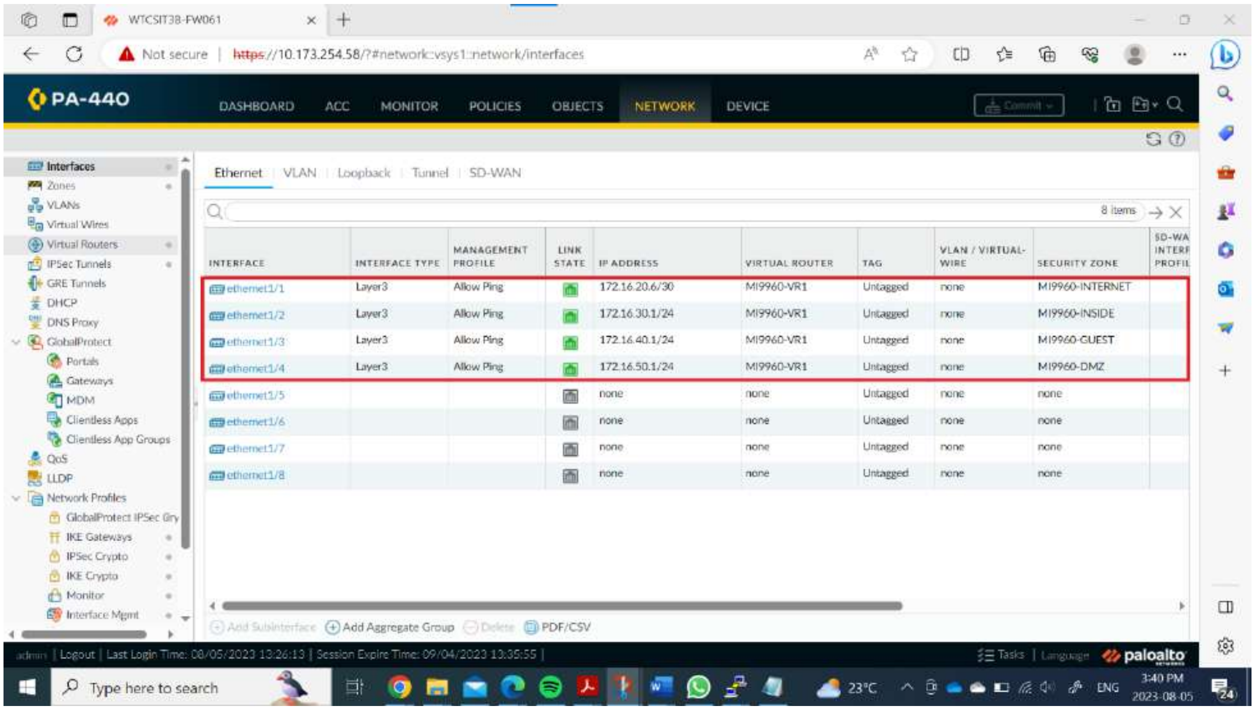
PALO-ALTO

MI9960-INTERNET-172.16.20.10/30

MI9960-INSIDE-172.16.140.2/24

MI9960-GUEST-172.16.141.3/24

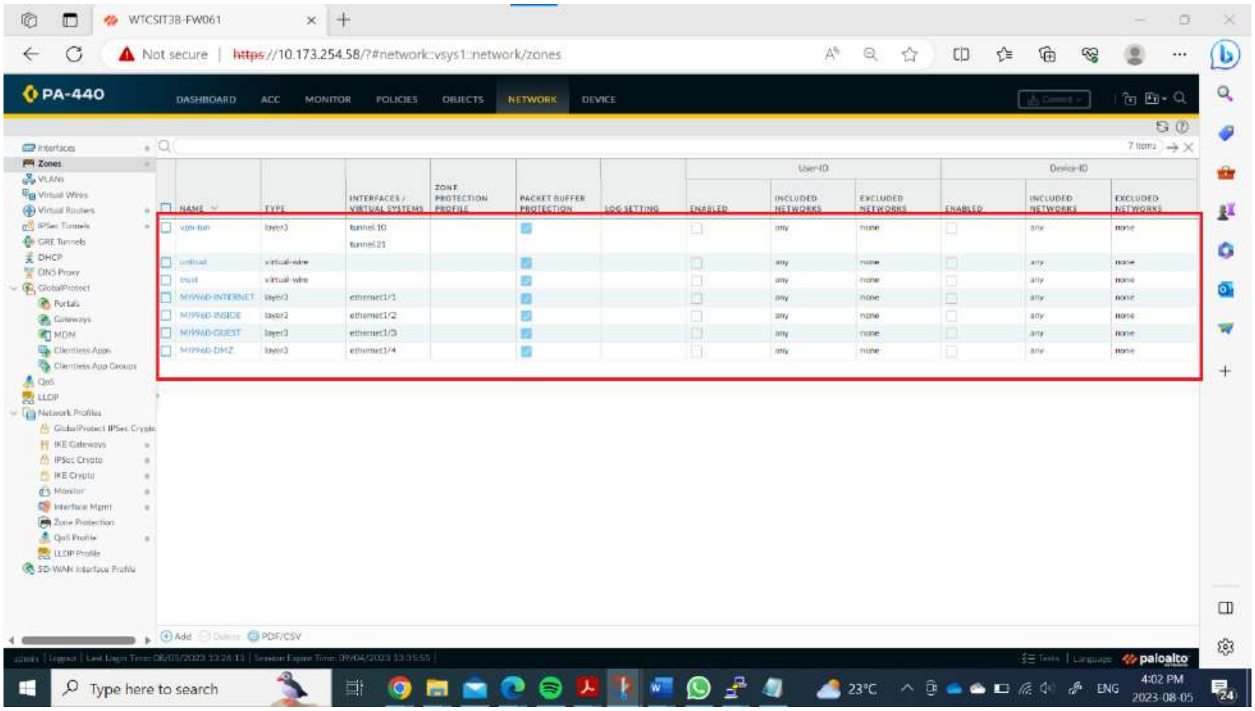
Figure 1 shows my topology.



https://10.173.254.58/?#network::vsys1::network/interfaces

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE
ethernet1/1	Layer3	Allow Ping	🟩	172.16.20.6/30	MI9960-VR1	Untagged	none	MI9960-INTERNET	
ethernet1/2	Layer3	Allow Ping	🟩	172.16.30.1/24	MI9960-VR1	Untagged	none	MI9960-INSIDE	
ethernet1/3	Layer3	Allow Ping	🟩	172.16.40.1/24	MI9960-VR1	Untagged	none	MI9960-GUEST	
ethernet1/4	Layer3	Allow Ping	🟩	172.16.50.1/24	MI9960-VR1	Untagged	none	MI9960-DMZ	
ethernet1/5			▨	none	none	Untagged	none	none	
ethernet1/6			▨	none	none	Untagged	none	none	
ethernet1/7			▨	none	none	Untagged	none	none	
ethernet1/8			▨	none	none	Untagged	none	none	

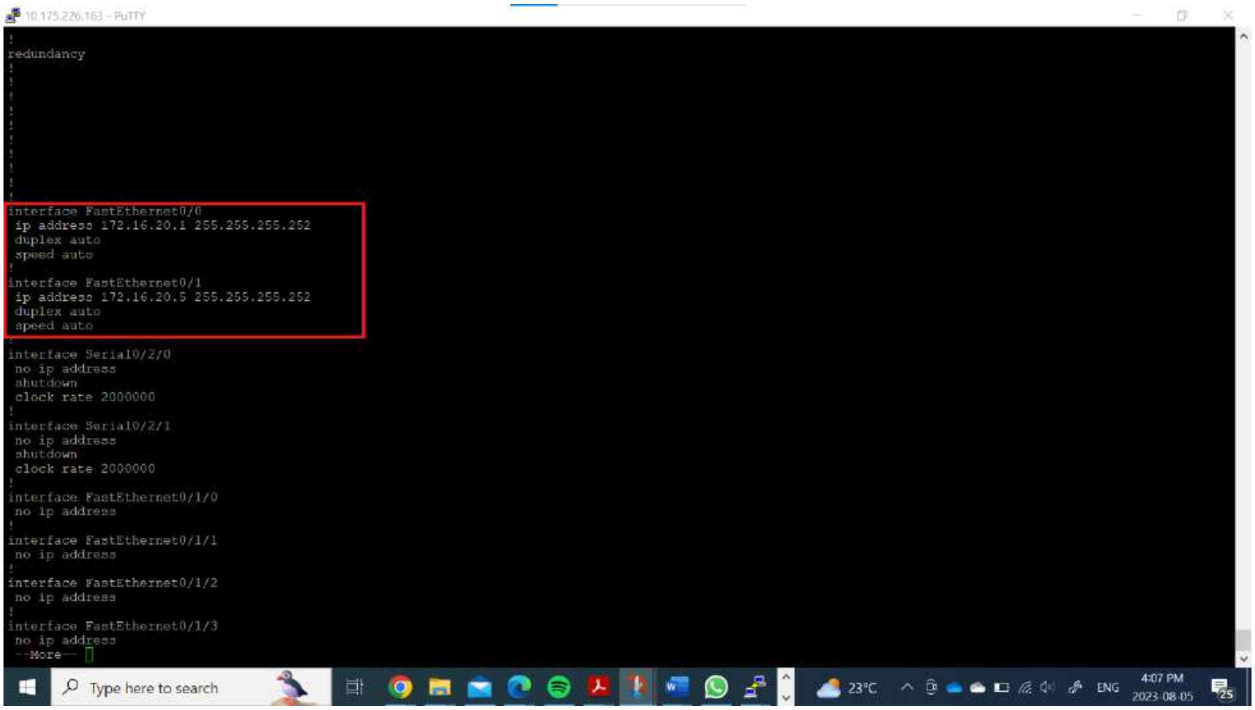
Figure 2 shows my ethernet interface in my Palo-Alto.



https://10.173.254.58/?#network::vsys1::network/zones

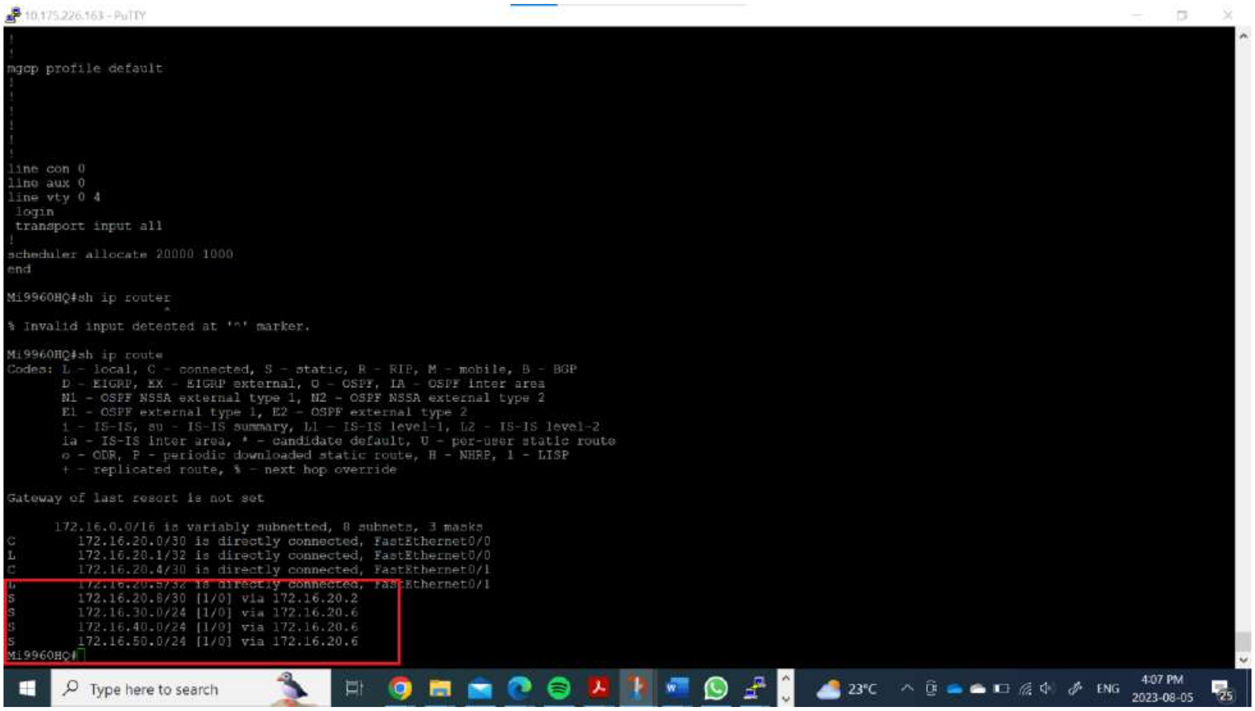
NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID ENABLED	User-ID INCLUDED NETWORKS	User-ID EXCLUDED NETWORKS	Device-ID ENABLED	Device-ID INCLUDED NETWORKS	Device-ID EXCLUDED NETWORKS
vpn-tun	layer3	tunnel.10 tunnel.21		☑		□	any	none	□	any	none
untrust	virtual-wire			☑		□	any	none	□	any	none
trust	virtual-wire			☑		□	any	none	□	any	none
MI9960-INTERNET	layer3	ethernet1/1		☑		□	any	none	□	any	none
MI9960-INSIDE	layer3	ethernet1/2		☑		□	any	none	□	any	none
MI9960-GUEST	layer3	ethernet1/3		☑		□	any	none	□	any	none
MI9960-DMZ	layer3	ethernet1/4		☑		□	any	none	□	any	none

Figure 3 shows the zones i created.



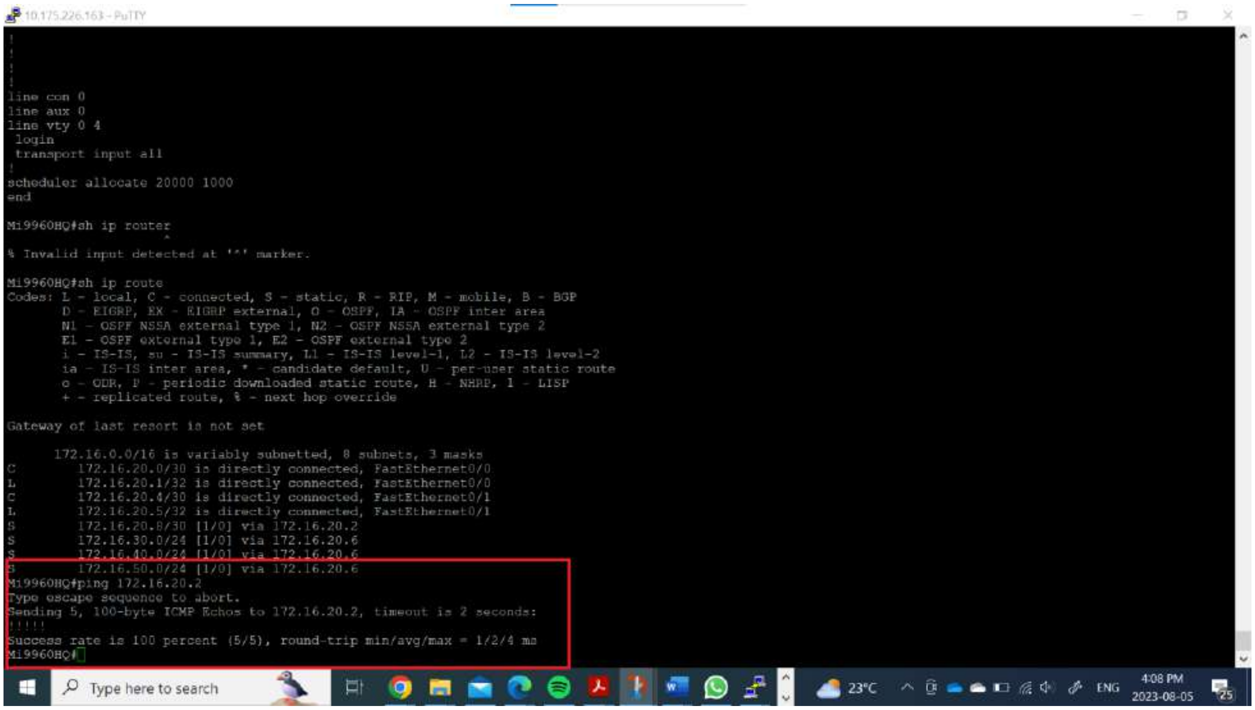
```
!
redundancy
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.20.5 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1/0
 no ip address
!
interface FastEthernet0/1/1
 no ip address
!
interface FastEthernet0/1/2
 no ip address
!
interface FastEthernet0/1/3
 no ip address
 --More--
```

Figure 4 shows my router IP address for each interface.



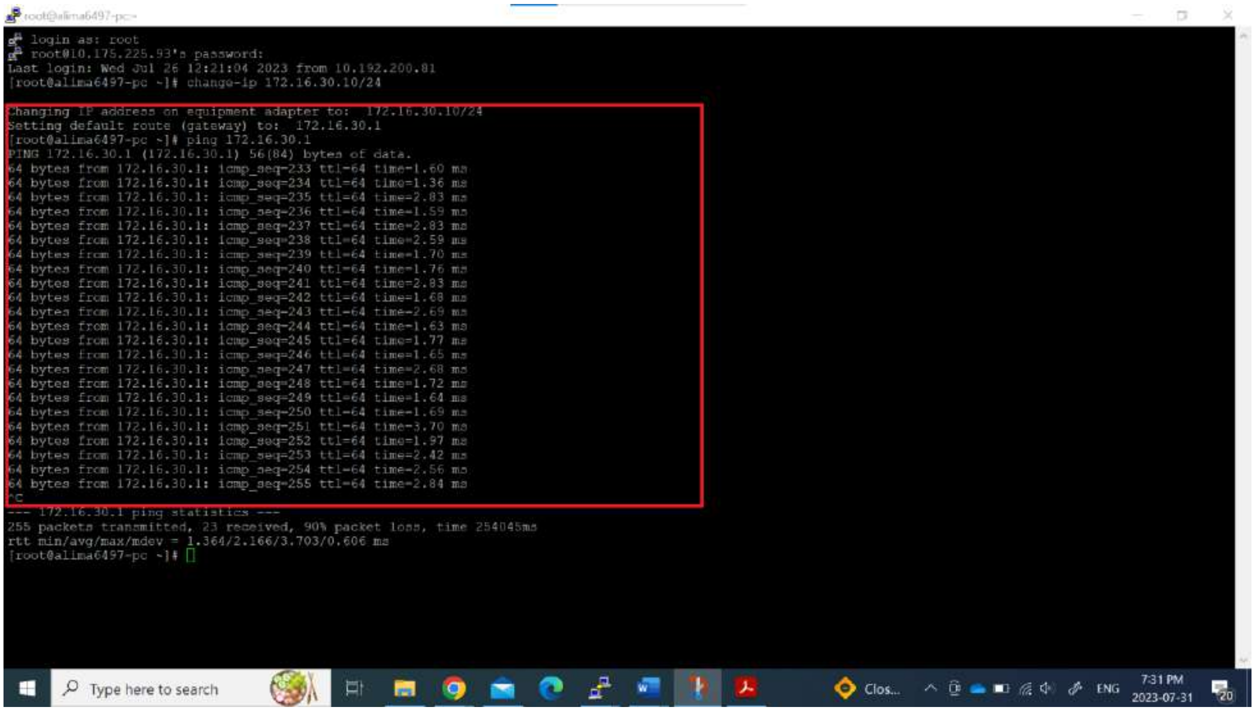
```
!
!
mgcp profile default
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end

Mi9960HQ#sh ip router
                   ^
% Invalid input detected at '^' marker.

Mi9960HQ#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.20.0/30 is directly connected, FastEthernet0/0
L        172.16.20.1/32 is directly connected, FastEthernet0/0
C        172.16.20.4/30 is directly connected, FastEthernet0/1
L        172.16.20.5/32 is directly connected, FastEthernet0/1
S        172.16.20.8/30 [1/0] via 172.16.20.2
S        172.16.30.0/24 [1/0] via 172.16.20.6
S        172.16.40.0/24 [1/0] via 172.16.20.6
S        172.16.50.0/24 [1/0] via 172.16.20.6
Mi9960HQ#
```

Figure 5 shows the static route on my HQ interface.



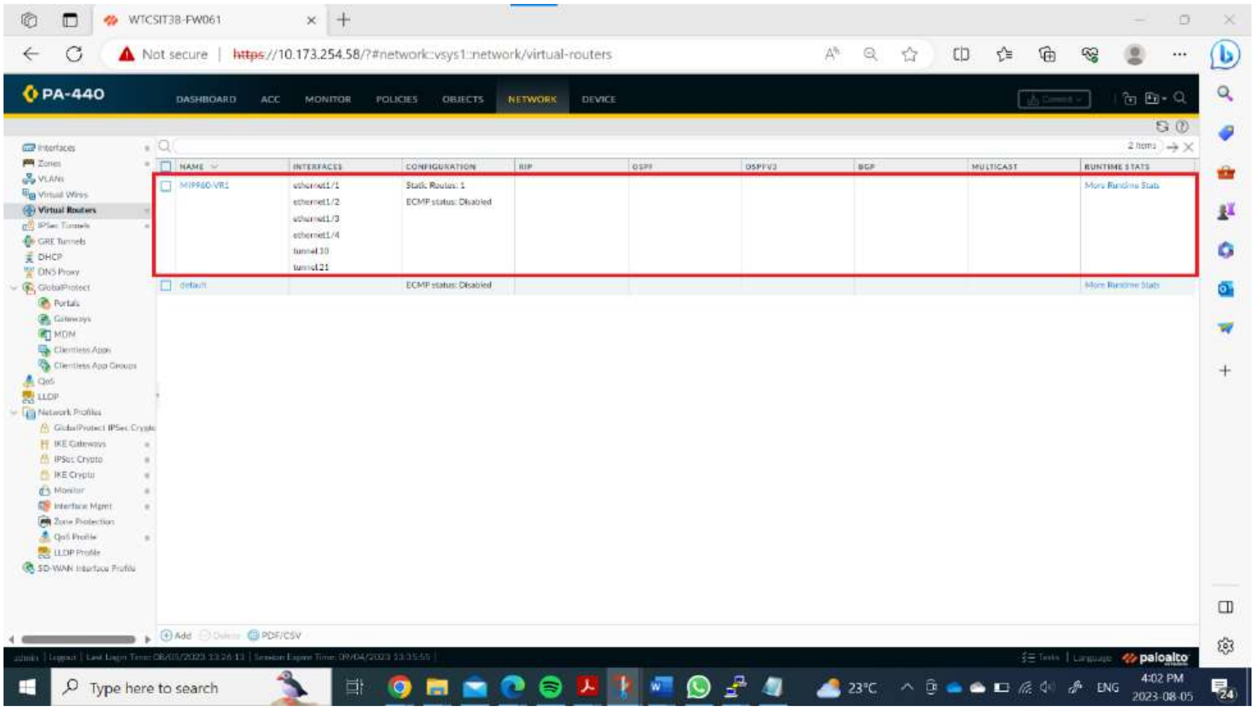
```
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end

Mi9960HQ#sh ip router
                   ^
% Invalid input detected at '^' marker.

Mi9960HQ#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
C        172.16.20.0/30 is directly connected, FastEthernet0/0
L        172.16.20.1/32 is directly connected, FastEthernet0/0
C        172.16.20.4/30 is directly connected, FastEthernet0/1
L        172.16.20.5/32 is directly connected, FastEthernet0/1
S        172.16.20.8/30 [1/0] via 172.16.20.2
S        172.16.30.0/24 [1/0] via 172.16.20.6
S        172.16.40.0/24 [1/0] via 172.16.20.6
S        172.16.50.0/24 [1/0] via 172.16.20.6
Mi9960HQ#ping 172.16.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Mi9960HQ#
```

Figure 6 shows i can ping my branch router.



```
login as: root
root@10.175.225.93's password:
Last login: Wed Jul 26 12:21:04 2023 from 10.192.200.81
[root@alima6497-pc ~]# change-ip 172.16.30.10/24

Changing IP address on equipment adapter to:  172.16.30.10/24
Setting default route (gateway) to:  172.16.30.1
[root@alima6497-pc ~]# ping 172.16.30.1
PING 172.16.30.1 (172.16.30.1) 56(84) bytes of data.
64 bytes from 172.16.30.1: icmp_seq=233 ttl=64 time=1.60 ms
64 bytes from 172.16.30.1: icmp_seq=234 ttl=64 time=1.36 ms
64 bytes from 172.16.30.1: icmp_seq=235 ttl=64 time=2.83 ms
64 bytes from 172.16.30.1: icmp_seq=236 ttl=64 time=1.59 ms
64 bytes from 172.16.30.1: icmp_seq=237 ttl=64 time=2.83 ms
64 bytes from 172.16.30.1: icmp_seq=238 ttl=64 time=2.59 ms
64 bytes from 172.16.30.1: icmp_seq=239 ttl=64 time=1.70 ms
64 bytes from 172.16.30.1: icmp_seq=240 ttl=64 time=1.76 ms
64 bytes from 172.16.30.1: icmp_seq=241 ttl=64 time=2.83 ms
64 bytes from 172.16.30.1: icmp_seq=242 ttl=64 time=1.68 ms
64 bytes from 172.16.30.1: icmp_seq=243 ttl=64 time=2.69 ms
64 bytes from 172.16.30.1: icmp_seq=244 ttl=64 time=1.63 ms
64 bytes from 172.16.30.1: icmp_seq=245 ttl=64 time=1.77 ms
64 bytes from 172.16.30.1: icmp_seq=246 ttl=64 time=1.65 ms
64 bytes from 172.16.30.1: icmp_seq=247 ttl=64 time=2.68 ms
64 bytes from 172.16.30.1: icmp_seq=248 ttl=64 time=1.72 ms
64 bytes from 172.16.30.1: icmp_seq=249 ttl=64 time=1.64 ms
64 bytes from 172.16.30.1: icmp_seq=250 ttl=64 time=1.69 ms
64 bytes from 172.16.30.1: icmp_seq=251 ttl=64 time=3.70 ms
64 bytes from 172.16.30.1: icmp_seq=252 ttl=64 time=1.97 ms
64 bytes from 172.16.30.1: icmp_seq=253 ttl=64 time=2.42 ms
64 bytes from 172.16.30.1: icmp_seq=254 ttl=64 time=2.56 ms
64 bytes from 172.16.30.1: icmp_seq=255 ttl=64 time=2.84 ms
^C
--- 172.16.30.1 ping statistics ---
255 packets transmitted, 23 received, 90% packet loss, time 254045ms
rtt min/avg/max/mdev = 1.364/2.166/3.703/0.606 ms
[root@alima6497-pc ~]# 
```

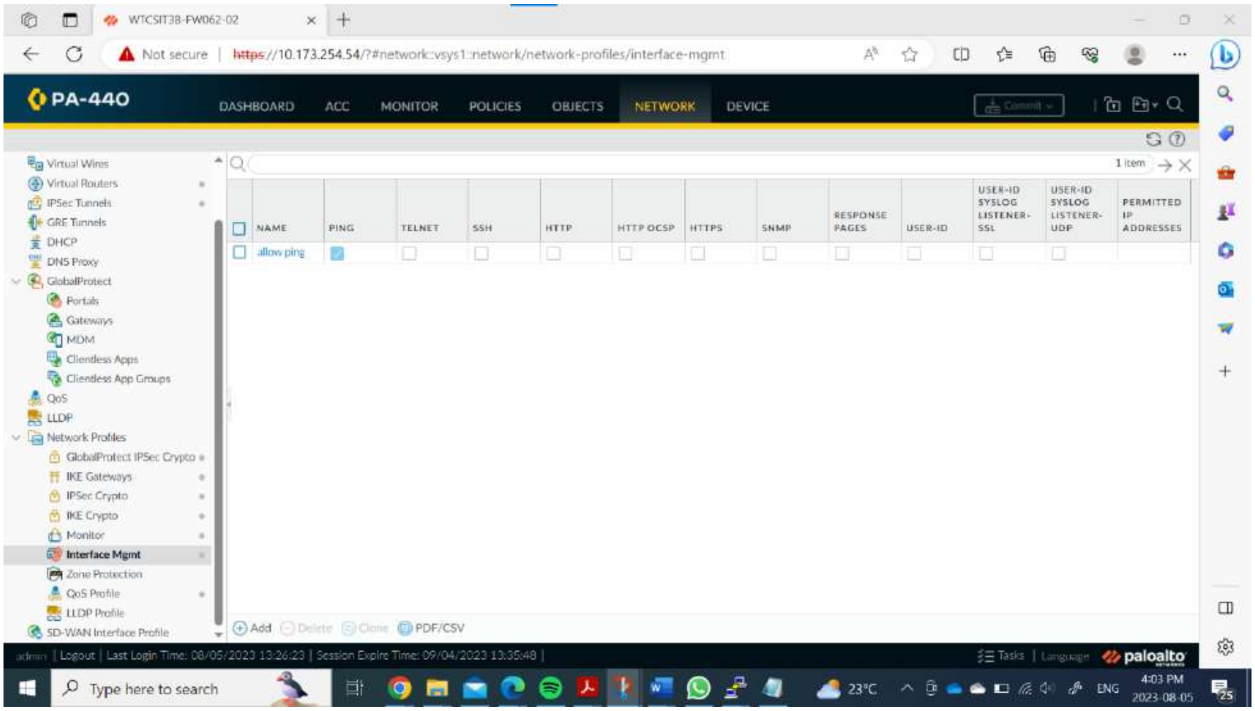
Figure 7 pinging my palo-alto.



https://10.173.254.58/?#network::vsys1::network/virtual-routers

NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
MI9960-VR1	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 tunnel.10 tunnel.21	Static Routes: 1 ECMP status: Disabled						More Runtime Stats
default		ECMP status: Disabled						More Runtime Stats

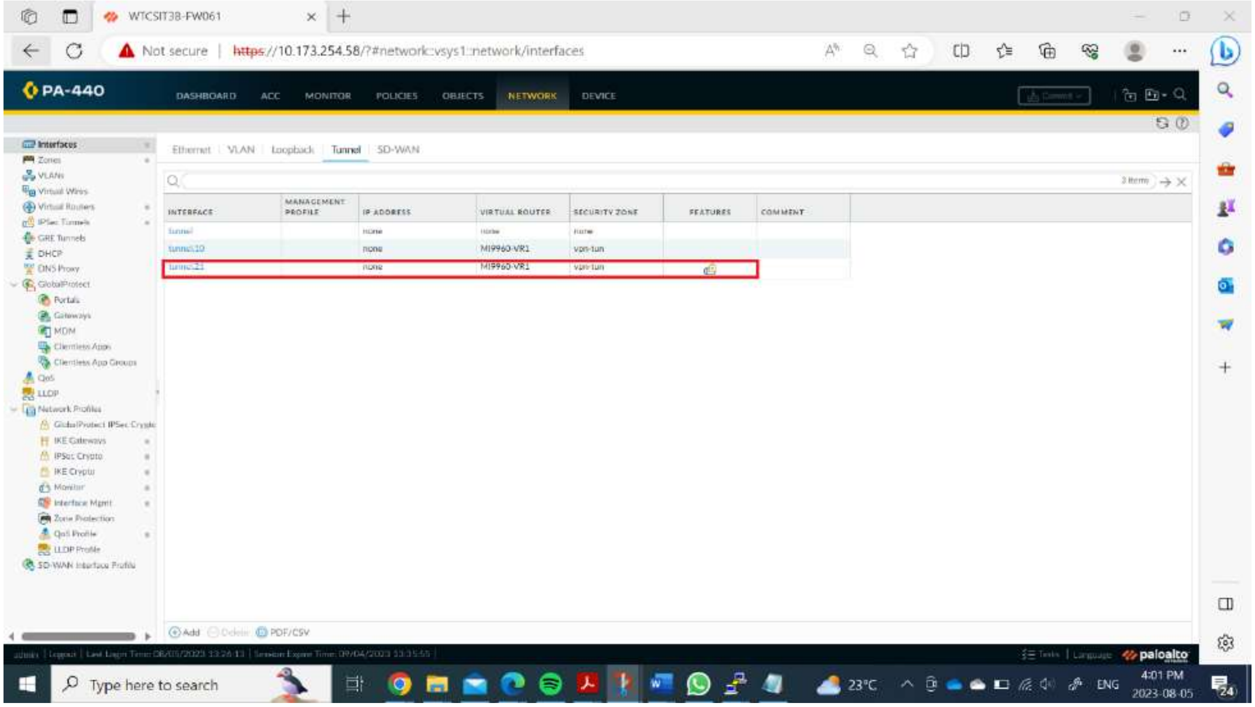
Figure 8 shows my virtual routing i created.



https://10.173.254.54/?#network::vsys1::network/network-profiles/interface-mgmt

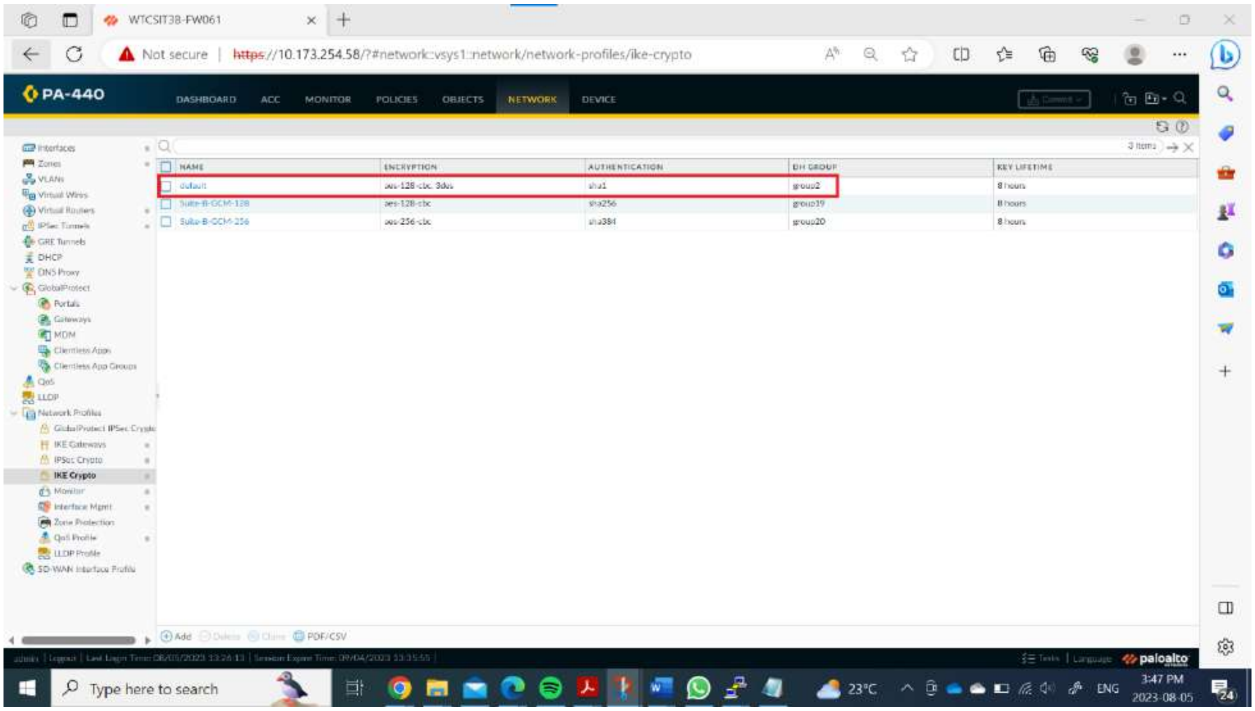
NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	USER-ID SYSLOG LISTENER-SSL	USER-ID SYSLOG LISTENER-UDP	PERMITTED IP ADDRESSES
allow ping	☑	□	□	□	□	□	□	□	□	□	□	

Figure 9 shows i allowed ping in the interface mgt.



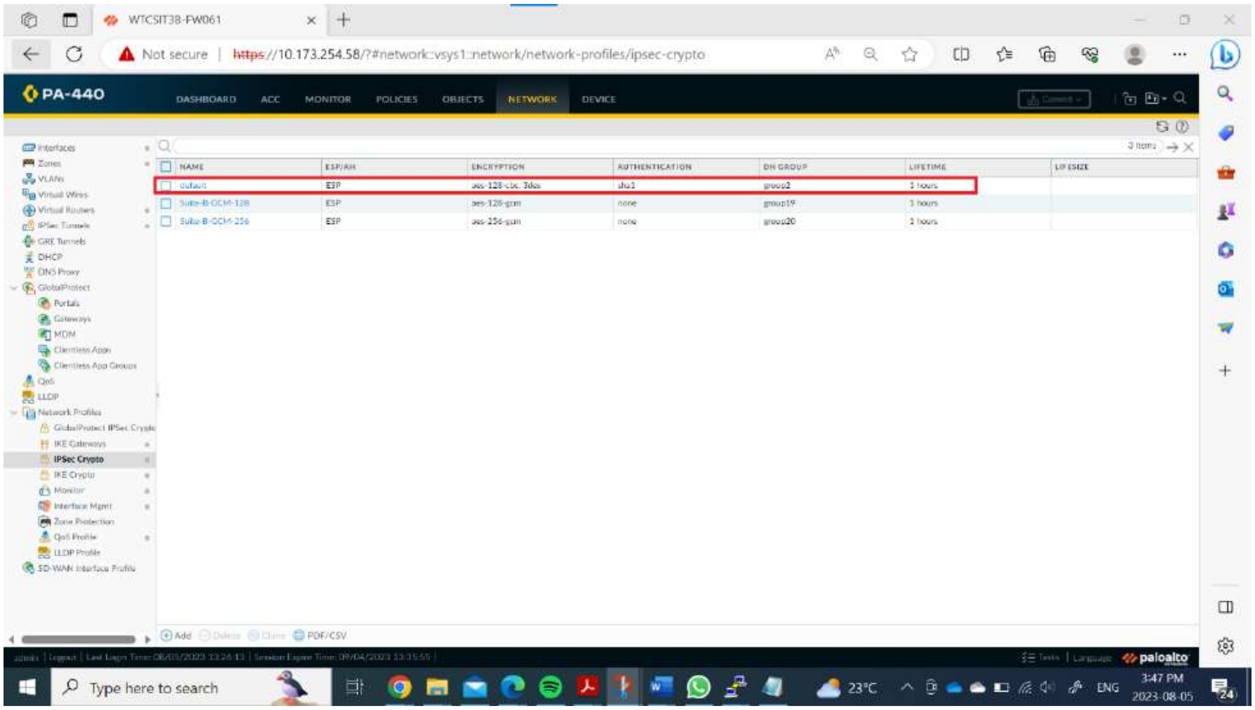
INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
tunnel		none	none	none		
tunnel.10		none	MI9960-VR1	vpn-tun		
tunnel.21		none	MI9960-VR1	vpn-tun		

Figure 10 shows my HQ tunnel i created.



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

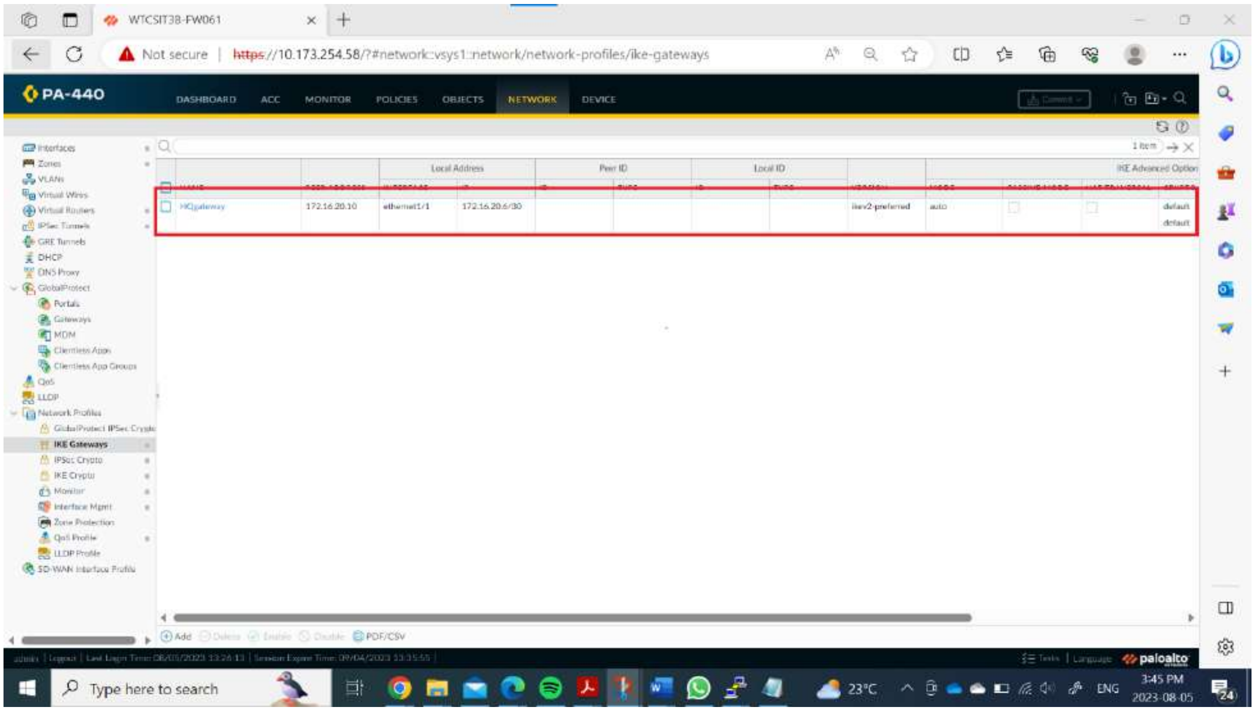
Figure 11 shows my IKE Crypto.



https://10.173.254.58/?#network::vsys1::network/network-profiles/ipsec-crypto

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	

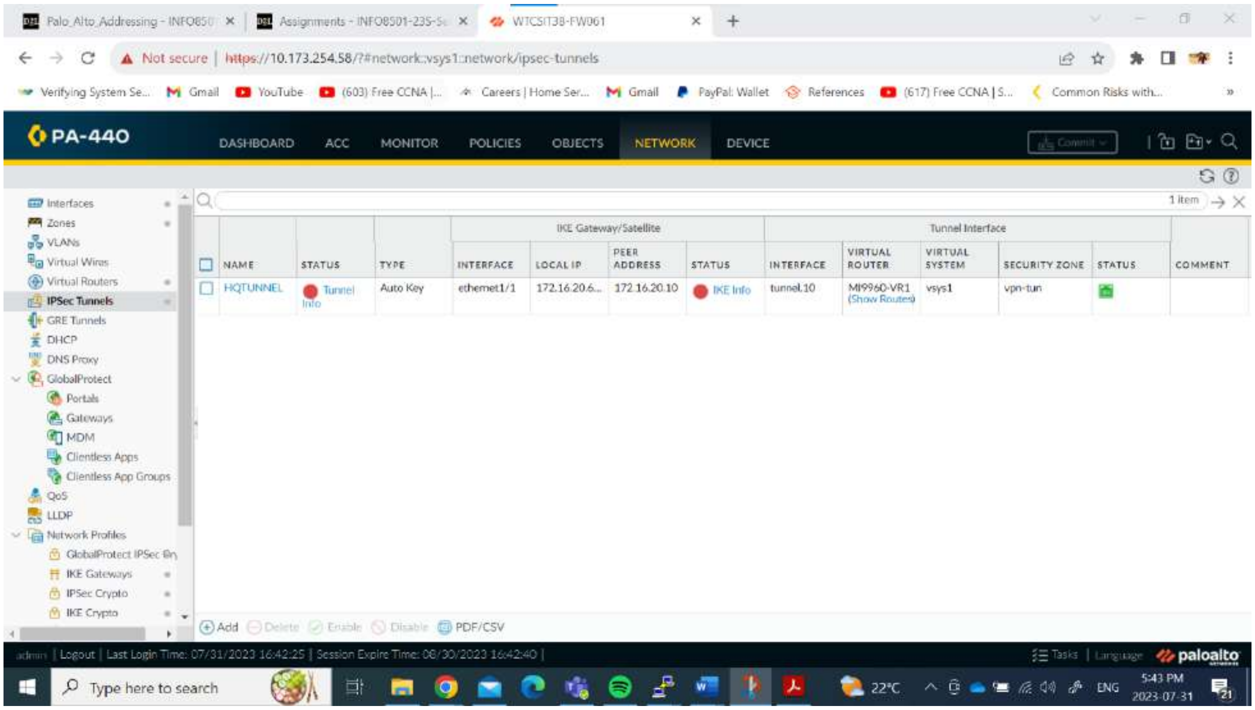
Figure 12 shows my ipsec crypto.



https://10.173.254.58/?#network::vsys1::network/network-profiles/ike-gateways

		Local Address		Peer ID		Local ID			IKE Advanced Option			
HQgateway	172.16.20.10	ethernet1/1	172.16.20.6/30					ikev2-preferred	auto	□	□	default default

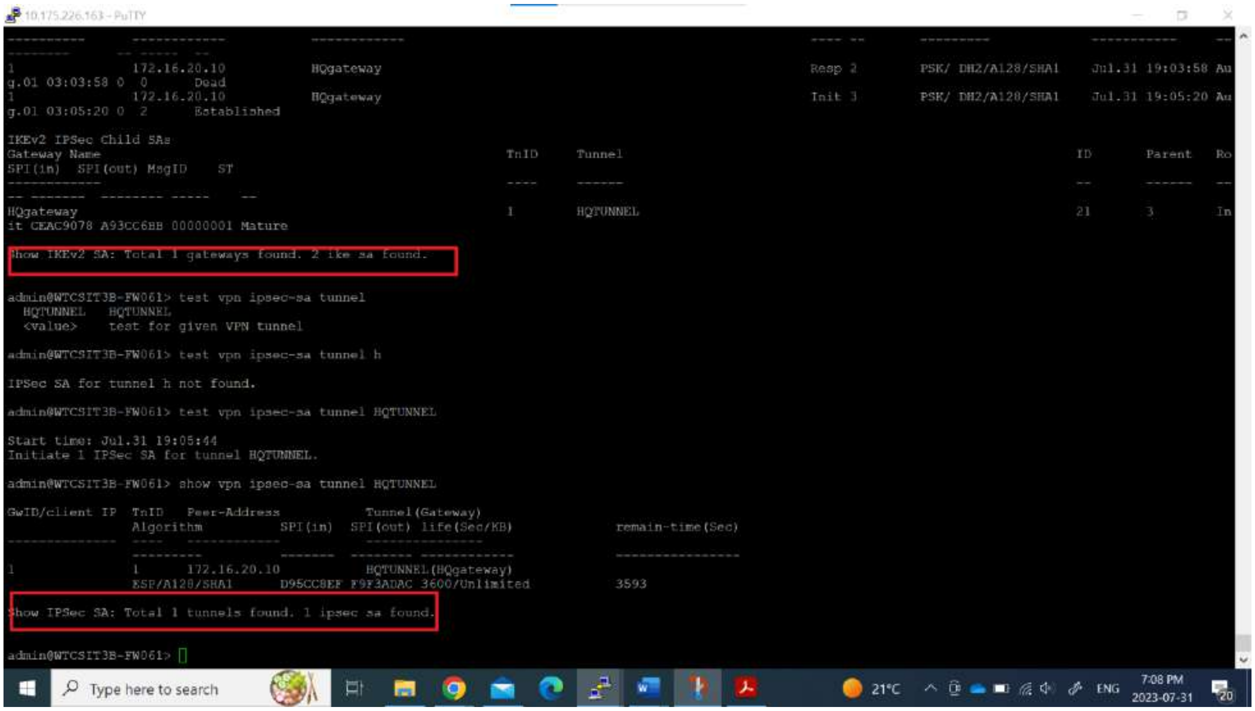
Figure 13 shows my IKE gateway.



			IKE Gateway/Satellite				Tunnel Interface					
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	COMMENT
HQTUNNEL	● Tunnel Info	Auto Key	ethernet1/1	172.16.20.6...	172.16.20.10	● IKE Info	tunnel.10	MI9960-VR1 (Show Routes)	vsys1	vpn-tun	🟩	

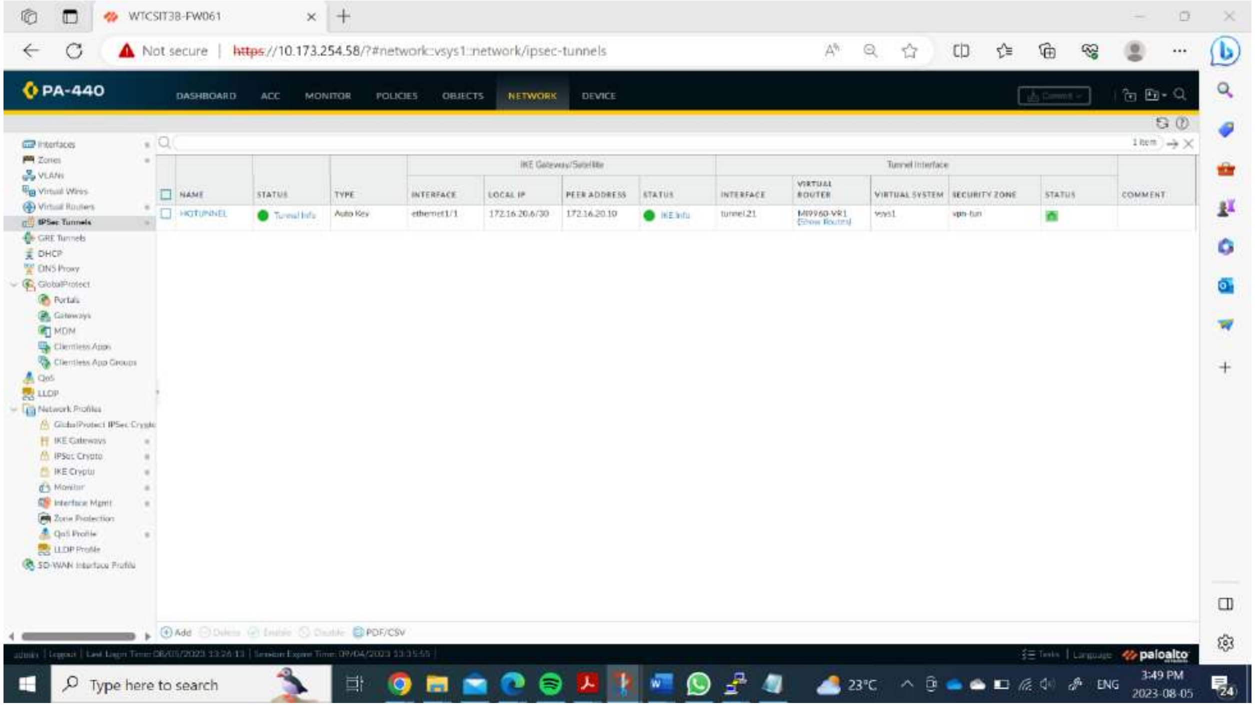
admin | Logout | Last Login Time: 07/31/2023 16:42:25 | Session Expire Time: 08/30/2023 16:42:40 |

Figure 14 shows my Ipsec tunnel before initializing it.



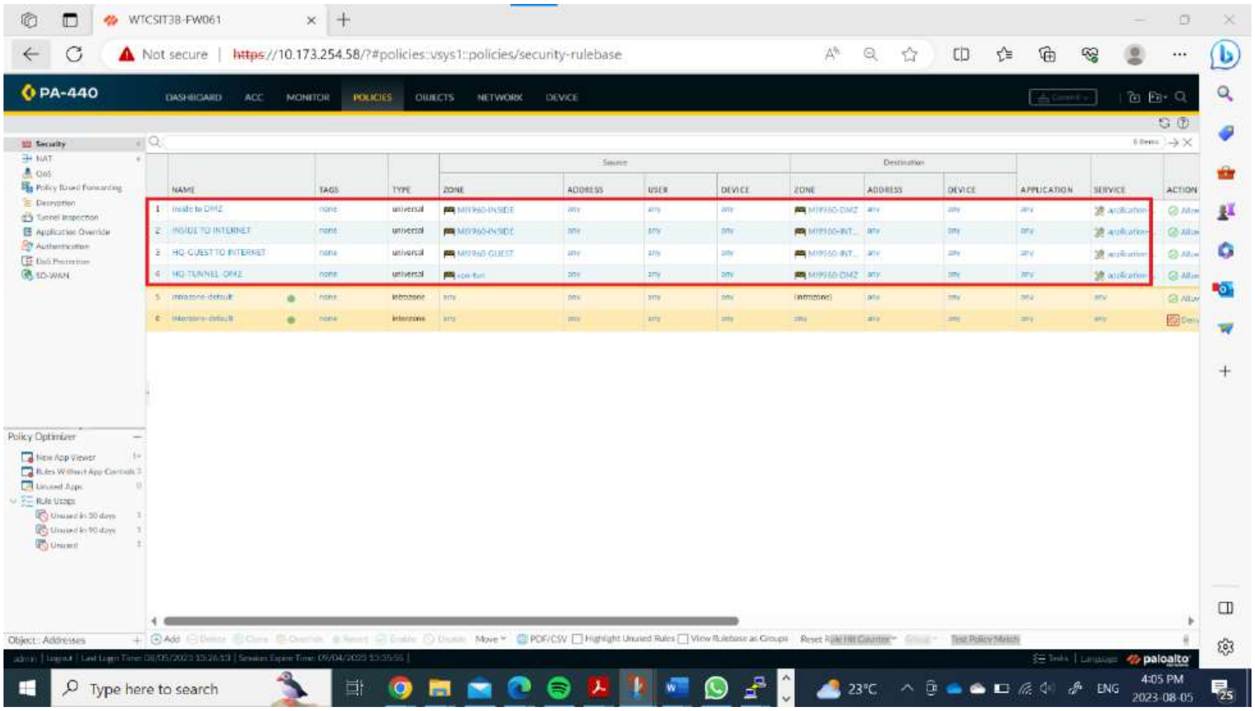
```
1              172.16.20.10          HQgateway                                  Resp 2      PSK/ DH2/A128/SHA1    Jul.31 19:03:58 Au
g.01 03:03:58 0  0      Dead
1              172.16.20.10          HQgateway                                  Init 3      PSK/ DH2/A128/SHA1    Jul.31 19:05:20 Au
g.01 03:05:20 0  2      Established

IKEv2 IPSec Child SAs
Gateway Name                                             TnID    Tunnel                                              ID      Parent   Ro
SPI(in)  SPI(out) MsgID    ST
-------------                                            ----    -------                                             --      ------   --
-- -------- -------- -----    --
HQgateway                                                1       HQTUNNEL                                            21      3        In
it CEAC9078 A93CC6BB 00000001 Mature

Show IKEv2 SA: Total 1 gateways found. 2 ike sa found.

admin@WTCSIT3B-FW061> test vpn ipsec-sa tunnel
  HQTUNNEL   HQTUNNEL
  <value>    test for given VPN tunnel

admin@WTCSIT3B-FW061> test vpn ipsec-sa tunnel h

IPSec SA for tunnel h not found.

admin@WTCSIT3B-FW061> test vpn ipsec-sa tunnel HQTUNNEL

Start time: Jul.31 19:05:44
Initiate 1 IPSec SA for tunnel HQTUNNEL.

admin@WTCSIT3B-FW061> show vpn ipsec-sa tunnel HQTUNNEL

GwID/client IP  TnID   Peer-Address          Tunnel(Gateway)
                Algorithm          SPI(in)   SPI(out) life(Sec/KB)          remain-time(Sec)
--------------  ----   ------------          ----------------
                ---------          -------   -------- ------------          ----------------
1               1      172.16.20.10          HQTUNNEL(HQgateway)
                ESP/A128/SHA1      D95CC8EF  F9F3ADAC 3600/Unlimited        3593

Show IPSec SA: Total 1 tunnels found. 1 ipsec sa found.

admin@WTCSIT3B-FW061> 
```

Figure 15 shows that it found my gateway and tunnel.



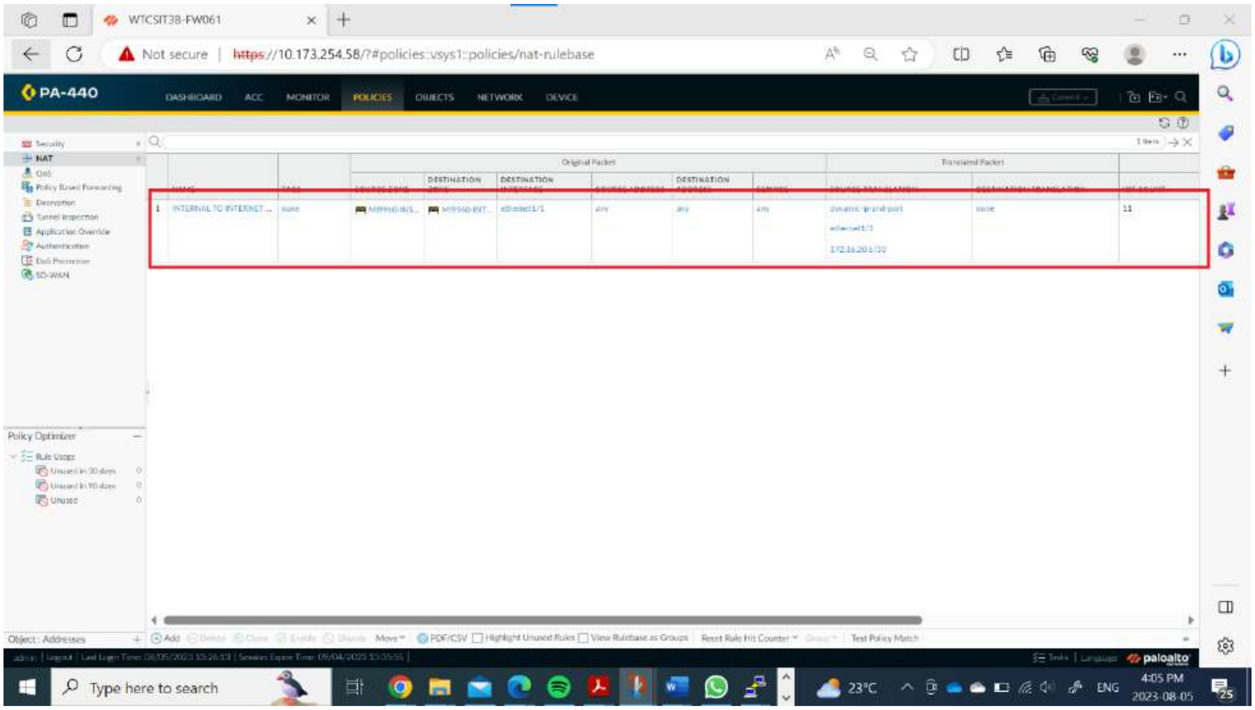
			IKE Gateway/Satellite				Tunnel Interface					
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	COMMENT
HQTUNNEL	● Tunnel Info	Auto Key	ethernet1/1	172.16.20.6/30	172.16.20.10	● IKE Info	tunnel.21	MI9960-VR1 (Show Routes)	vsys1	vpn-tun	🟩	

Figure 16 shows the IPsec tunnel has been established.



				Source				Destination				
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
1	inside to DMZ	none	universal	MI9960-INSIDE	any	any	any	MI9960-DMZ	any	any	any	application-	Allow
2	INSIDE TO INTERNET	none	universal	MI9960-INSIDE	any	any	any	MI9960-INT...	any	any	any	application-	Allow
3	HQ-GUEST TO INTERNET	none	universal	MI9960-GUEST	any	any	any	MI9960-INT...	any	any	any	application-	Allow
4	HQ-TUNNEL-DMZ	none	universal	vpn-tun	any	any	any	MI9960-DMZ	any	any	any	application-	Allow
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

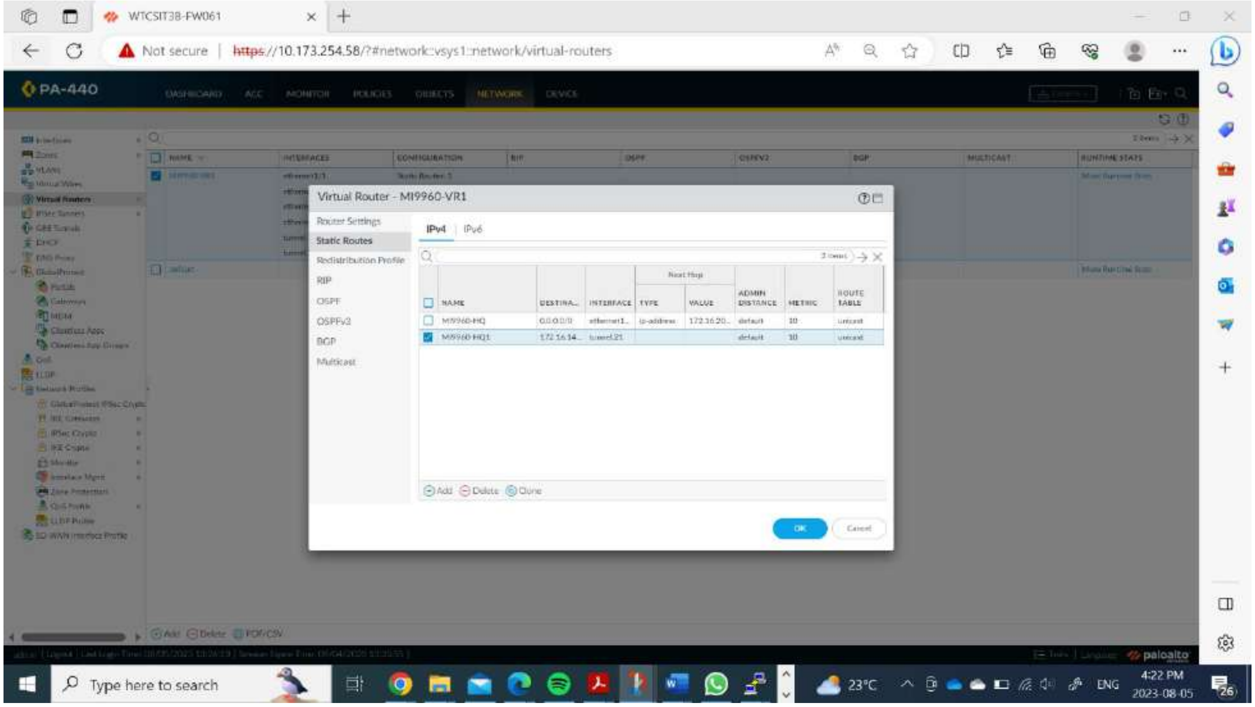
Figure 17 shows the policy I implemented.



https://10.173.254.58/?#policies::vsys1::policies/nat-rulebase

			Original Packet						Translated Packet		
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT
1	INTERNAL TO INTERNET...	none	MI9960-INS...	MI9960-INT...	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 172.16.20.1/30	none	11

Figure 18 shows my NAT policy i created.



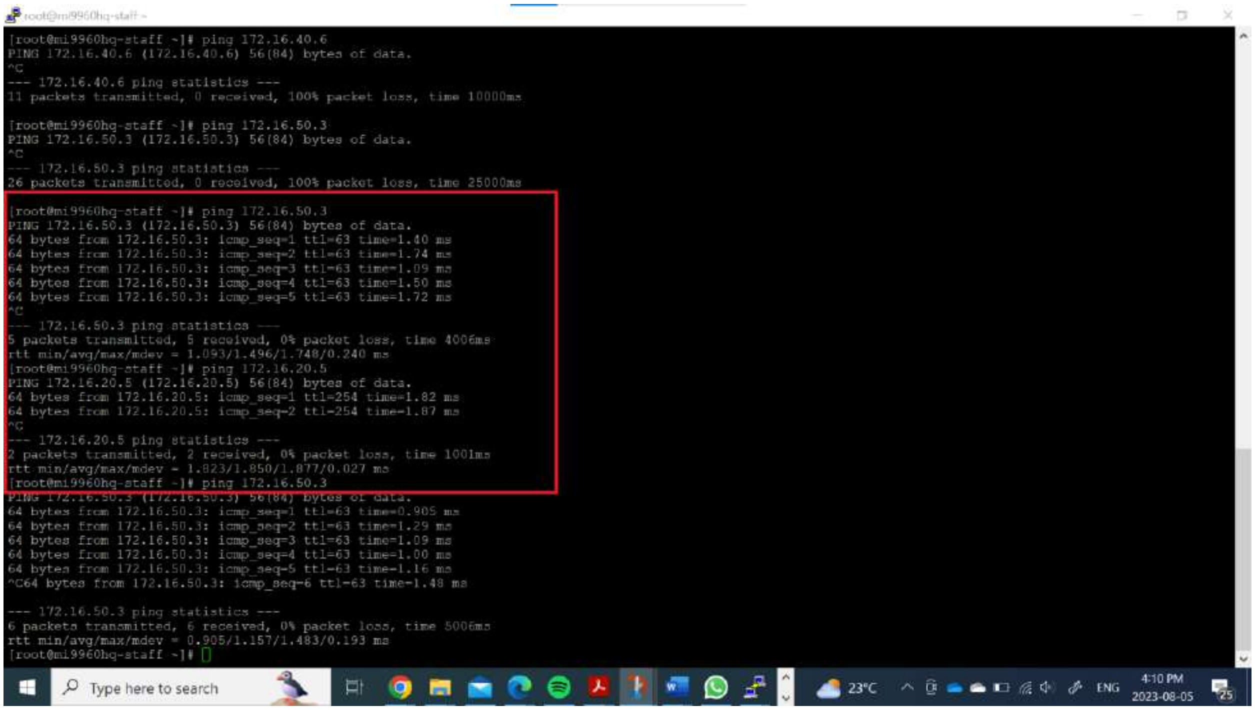
https://10.173.254.58/?#network::vsys1::network/virtual-routers

Virtual Router - MI9960-VR1

Static Routes — IPv4

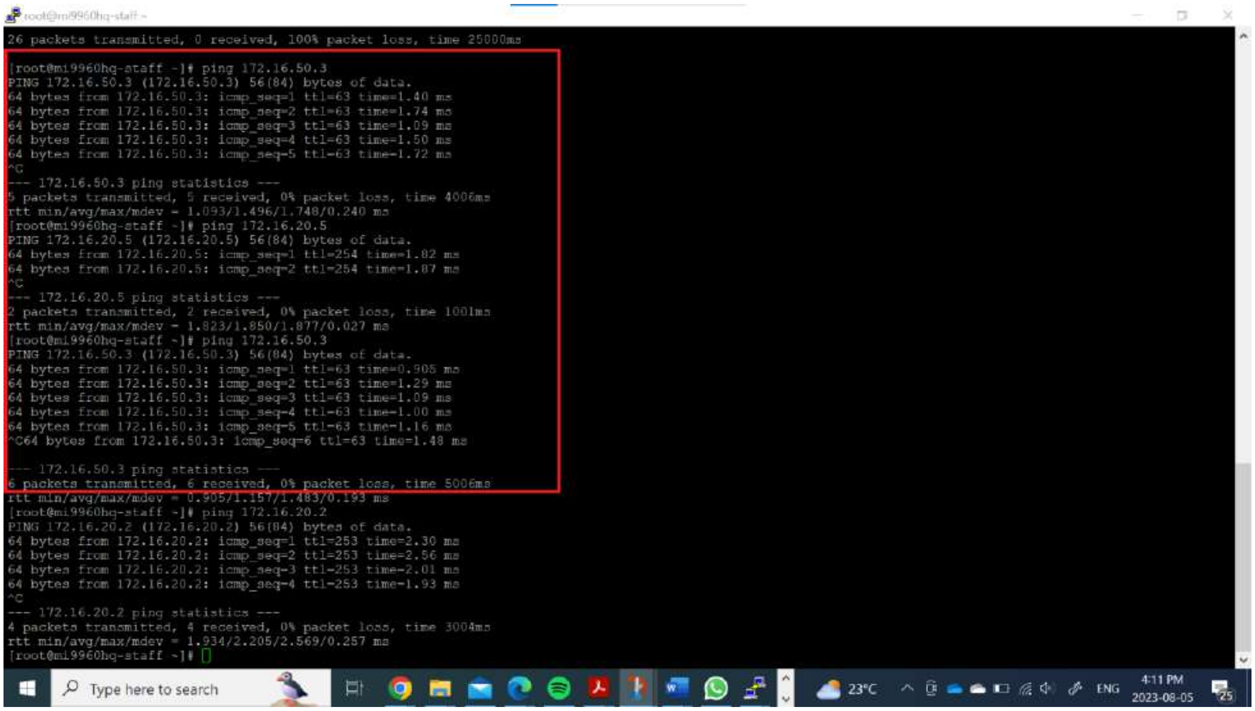
				Next Hop				
□	NAME	DESTINA...	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	METRIC	ROUTE TABLE
□	MI9960-HQ	0.0.0.0/0	ethernet1...	ip-address	172.16.20...	default	10	unicast
☑	MI9960-HQ1	172.16.14...	tunnel.21			default	10	unicast

Figure 19 shows the static route i created to allow ping and communication.



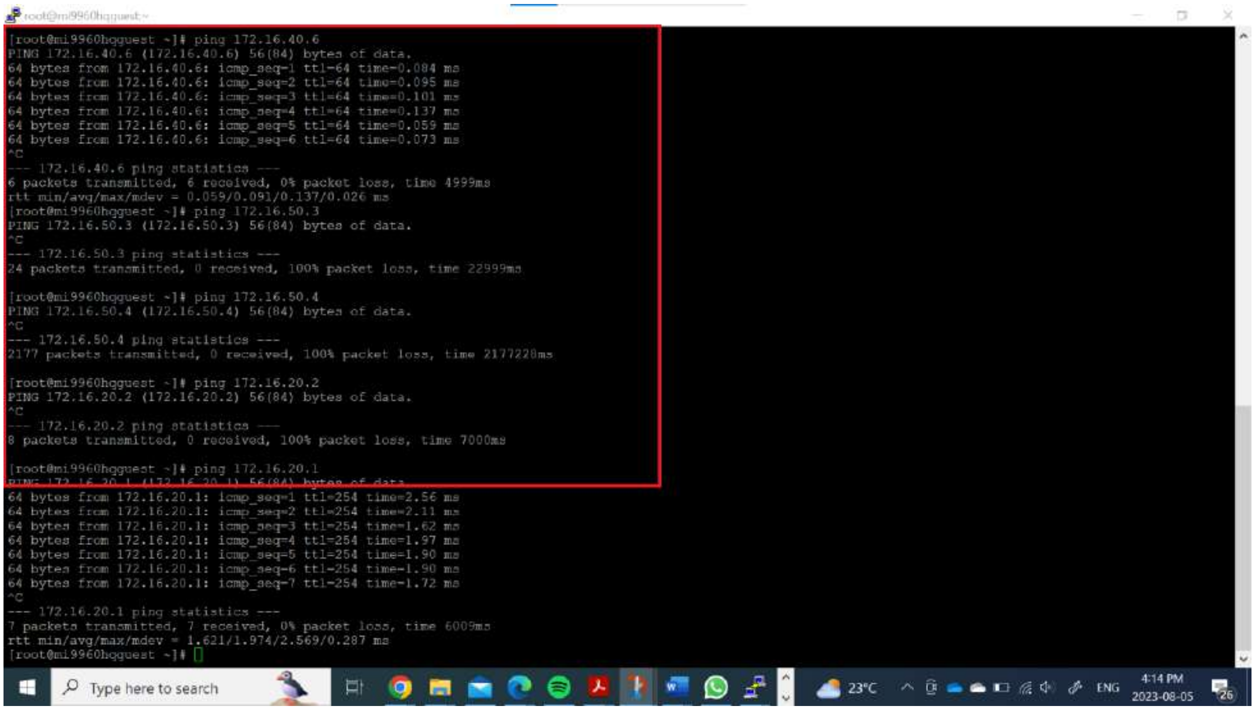
```
[root@mi9960hq-staff ~]# ping 172.16.40.6
PING 172.16.40.6 (172.16.40.6) 56(84) bytes of data.
^C
--- 172.16.40.6 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10000ms

[root@mi9960hq-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
^C
--- 172.16.50.3 ping statistics ---
26 packets transmitted, 0 received, 100% packet loss, time 25000ms

[root@mi9960hq-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=63 time=1.50 ms
64 bytes from 172.16.50.3: icmp_seq=5 ttl=63 time=1.72 ms
^C
--- 172.16.50.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.093/1.496/1.748/0.240 ms
[root@mi9960hq-staff ~]# ping 172.16.20.5
PING 172.16.20.5 (172.16.20.5) 56(84) bytes of data.
64 bytes from 172.16.20.5: icmp_seq=1 ttl=254 time=1.82 ms
64 bytes from 172.16.20.5: icmp_seq=2 ttl=254 time=1.87 ms
^C
--- 172.16.20.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.823/1.850/1.877/0.027 ms
[root@mi9960hq-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=63 time=0.905 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=63 time=1.00 ms
64 bytes from 172.16.50.3: icmp_seq=5 ttl=63 time=1.16 ms
^C64 bytes from 172.16.50.3: icmp_seq=6 ttl=63 time=1.48 ms

--- 172.16.50.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 0.905/1.157/1.483/0.193 ms
[root@mi9960hq-staff ~]# 
```

Figure 20 shows i can ping my inside network to my server in my dmz.



```
26 packets transmitted, 0 received, 100% packet loss, time 25000ms

[root@mi9960hq-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=63 time=1.50 ms
64 bytes from 172.16.50.3: icmp_seq=5 ttl=63 time=1.72 ms
^C
--- 172.16.50.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.093/1.496/1.748/0.240 ms
[root@mi9960hq-staff ~]# ping 172.16.20.5
PING 172.16.20.5 (172.16.20.5) 56(84) bytes of data.
64 bytes from 172.16.20.5: icmp_seq=1 ttl=254 time=1.82 ms
64 bytes from 172.16.20.5: icmp_seq=2 ttl=254 time=1.87 ms
^C
--- 172.16.20.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.823/1.850/1.877/0.027 ms
[root@mi9960hq-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=63 time=0.905 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=63 time=1.00 ms
64 bytes from 172.16.50.3: icmp_seq=5 ttl=63 time=1.16 ms
^C64 bytes from 172.16.50.3: icmp_seq=6 ttl=63 time=1.48 ms

--- 172.16.50.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 0.905/1.157/1.483/0.193 ms
[root@mi9960hq-staff ~]# ping 172.16.20.2
PING 172.16.20.2 (172.16.20.2) 56(84) bytes of data.
64 bytes from 172.16.20.2: icmp_seq=1 ttl=253 time=2.30 ms
64 bytes from 172.16.20.2: icmp_seq=2 ttl=253 time=2.56 ms
64 bytes from 172.16.20.2: icmp_seq=3 ttl=253 time=2.01 ms
64 bytes from 172.16.20.2: icmp_seq=4 ttl=253 time=1.93 ms
^C
--- 172.16.20.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.934/2.205/2.569/0.257 ms
[root@mi9960hq-staff ~]# 
```

Figure 21 shows i can ping my inside network to the internet.



```
[root@mi9960hqguest ~]# ping 172.16.40.6
PING 172.16.40.6 (172.16.40.6) 56(84) bytes of data.
64 bytes from 172.16.40.6: icmp_seq=1 ttl=64 time=0.084 ms
64 bytes from 172.16.40.6: icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from 172.16.40.6: icmp_seq=3 ttl=64 time=0.101 ms
64 bytes from 172.16.40.6: icmp_seq=4 ttl=64 time=0.137 ms
64 bytes from 172.16.40.6: icmp_seq=5 ttl=64 time=0.059 ms
64 bytes from 172.16.40.6: icmp_seq=6 ttl=64 time=0.073 ms
^C
--- 172.16.40.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.059/0.091/0.137/0.026 ms
[root@mi9960hqguest ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
^C
--- 172.16.50.3 ping statistics ---
24 packets transmitted, 0 received, 100% packet loss, time 22999ms

[root@mi9960hqguest ~]# ping 172.16.50.4
PING 172.16.50.4 (172.16.50.4) 56(84) bytes of data.
^C
--- 172.16.50.4 ping statistics ---
2177 packets transmitted, 0 received, 100% packet loss, time 2177228ms

[root@mi9960hqguest ~]# ping 172.16.20.2
PING 172.16.20.2 (172.16.20.2) 56(84) bytes of data.
^C
--- 172.16.20.2 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7000ms

[root@mi9960hqguest ~]# ping 172.16.20.1
PING 172.16.20.1 (172.16.20.1) 56(84) bytes of data.
64 bytes from 172.16.20.1: icmp_seq=1 ttl=254 time=2.56 ms
64 bytes from 172.16.20.1: icmp_seq=2 ttl=254 time=2.11 ms
64 bytes from 172.16.20.1: icmp_seq=3 ttl=254 time=1.62 ms
64 bytes from 172.16.20.1: icmp_seq=4 ttl=254 time=1.97 ms
64 bytes from 172.16.20.1: icmp_seq=5 ttl=254 time=1.90 ms
64 bytes from 172.16.20.1: icmp_seq=6 ttl=254 time=1.90 ms
64 bytes from 172.16.20.1: icmp_seq=7 ttl=254 time=1.72 ms
^C
--- 172.16.20.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 1.621/1.974/2.569/0.287 ms
[root@mi9960hqguest ~]# 
```

Figure 22 shows i can my guest network can pick the internet network.

BRANCH SITE

REQUIREMENT

✓ ACCESS TO HQ SERVERS via VPN:

- All staff at the branch site must have secure access to the servers located at the HQ site.
- I made sure there is communication between the branch site and the HQ servers should be encrypted through the site-to site VPN over the internet.

✓ INTERNET ACCESS FOR BRANCH STAFF:

- I made sure all staff should have access to the internet.
- I made sure my internet access provided through the branch site's network connection.

✓ GUEST INTERNET ACCESS:

- All guests at the branch site must have access to the internet only.
- These guests should be able to connect to the internet without accessing internal resources.

✓ INTERNAL NETWORK FOR BRANCH:

- At the branch location, an internal network should be set up to facilitate device communication.
- The branch network should have access to internal resources like printers or local servers.

✓ INTERNET ACCESS FOR BRANCH GUESTS:

- Internet access should be available to visitors to the branch location.
- The guest access network should be separate from the internal network, much like the main staff network is.

✓ NAT for INTERNET ACCESS:

- Set up network Address Translation (NAT) for each host accessing the internet from the branch site.
- This adds an extra layer of security and helps preserve public IP addresses.

✓ ADHERENCE TO ACCESS POLICIES:

- The guidelines outlined in the project requirements should be followed for all access to resources, whether internal or external.
- unauthorized use of any resources not specifically mentioned should be prohibited.

✓ SECURITY AND CONFIDENTIALITY:

- The branch site's communication with the cooperate office and with the internet should be kept private and secure.
- Implementing encryption techniques is a good idea for data privacy.

✓ COMPLIANCE WITH NAMING CONVENTIONS:

- I used my initials and the final four digits of my student ID **MI9960** was included in the names of all gadgets, things, and configurations.

DESIGN

✓ NETWORK TOPOLGY:

Router 2: (Branch Router):

- Interface eth0/0: connected to Router 1 **(172.16.20.2/30** in the **172.16.20.0/30** subnet).
- Interface eth0/1: connected to Palo Alto Firewall (**172.16.20.9/30** in the **172.16.20.8/30** subnet).

Palo Alto Firewall:

- eth0/0: connected to the internet (**172.16.20.10/30** in the **MI9960-internet zone**).
- eth1/1 connected to the inside zone (**172.16.20.10/30** in the **MI9960-inside zone)**
- eth1/2 connected to the guest zone (**172.16.141.1/24** in the **MI9960-guest zone)**

Branch Staff Devices:

- Staff VM1 **172.16.140.10/24** in the **172.16.140.0/24** network.

Branch Guest Devices:

- Guest VM2 **172.16.141.4/24** in the **172.161.141.0/24** network.

✓ IP ADDRESSING SCHEME:

- Router 2 eth0/0: **172.16.20.2/30**
- Router 2 eth0/1: **172.16.20.9/30**
- Palo Alto eth1/1: **172.16.20/10/30 (internet)**
- Palo Alto eth1/2: **172.16.140.1/24 (inside)**
- Palo Alto eth1/3: **172.16.141.1/24 (guest)**
- Branch staff Devices: Staff VM1: **172.16.140.10/24**
- Branch Guest Devices: VM2: **1722.16.141.4/24**

✓ VPN CONNECTIVITY:

- I will establish a site-to-site VPN tunnel will be established between Router 2 and Router 1 to ensure secure communication between the branch site and the HQ site.

✓ ACCESS CONTROL AND SECURITY:

- I will configure Router 2 and the Palo Alto firewall to regulate traffic flow between the internal network and the VPN.

✓ INTERNET ACCESS:

- NAT will be configured on the Palo Alto Firewall to allow branch devices to access the internet using a shared public IP address.

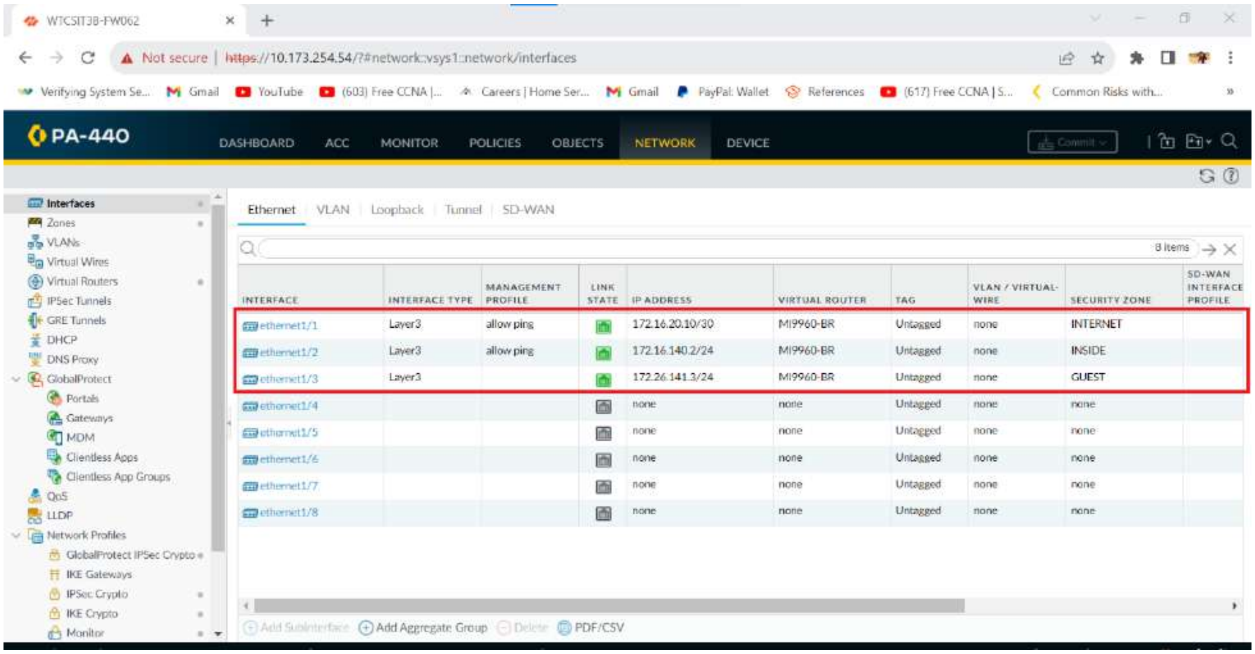
✓ NAMING CONVENTIONS AND COMPLIANCE:

- I used my initials and the final four digits of my student ID **MI9960** was included in the names of all gadgets, things, and configurations.

✓ CONCLUSION:

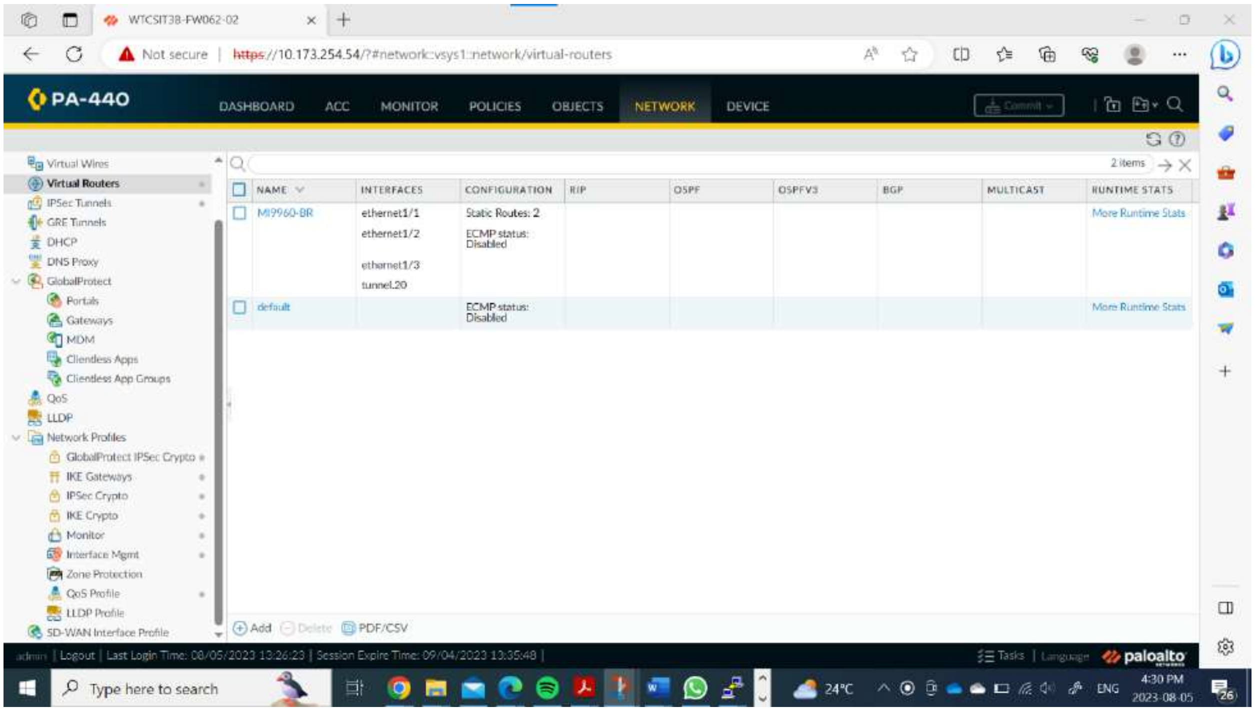
By giving staff secure access to headquarters servers, guest Internet access, and internal network communication, this design makes sure the branch site satisfies its unique requirements. A secure and useful network environment can be built with the help of virtual machines, routers, and a Palo Alto Firewall. The proper deployment of the VPN solution at the branch site will be confirmed after extensive testing and verification.

SCREENSHOT



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE
ethernet1/1	Layer3	allow ping	🟩	172.16.20.10/30	MI9960-BR	Untagged	none	INTERNET	
ethernet1/2	Layer3	allow ping	🟩	172.16.140.2/24	MI9960-BR	Untagged	none	INSIDE	
ethernet1/3	Layer3		🟩	172.26.141.3/24	MI9960-BR	Untagged	none	GUEST	
ethernet1/4			▨	none	none	Untagged	none	none	
ethernet1/5			▨	none	none	Untagged	none	none	
ethernet1/6			▨	none	none	Untagged	none	none	
ethernet1/7			▨	none	none	Untagged	none	none	
ethernet1/8			▨	none	none	Untagged	none	none	

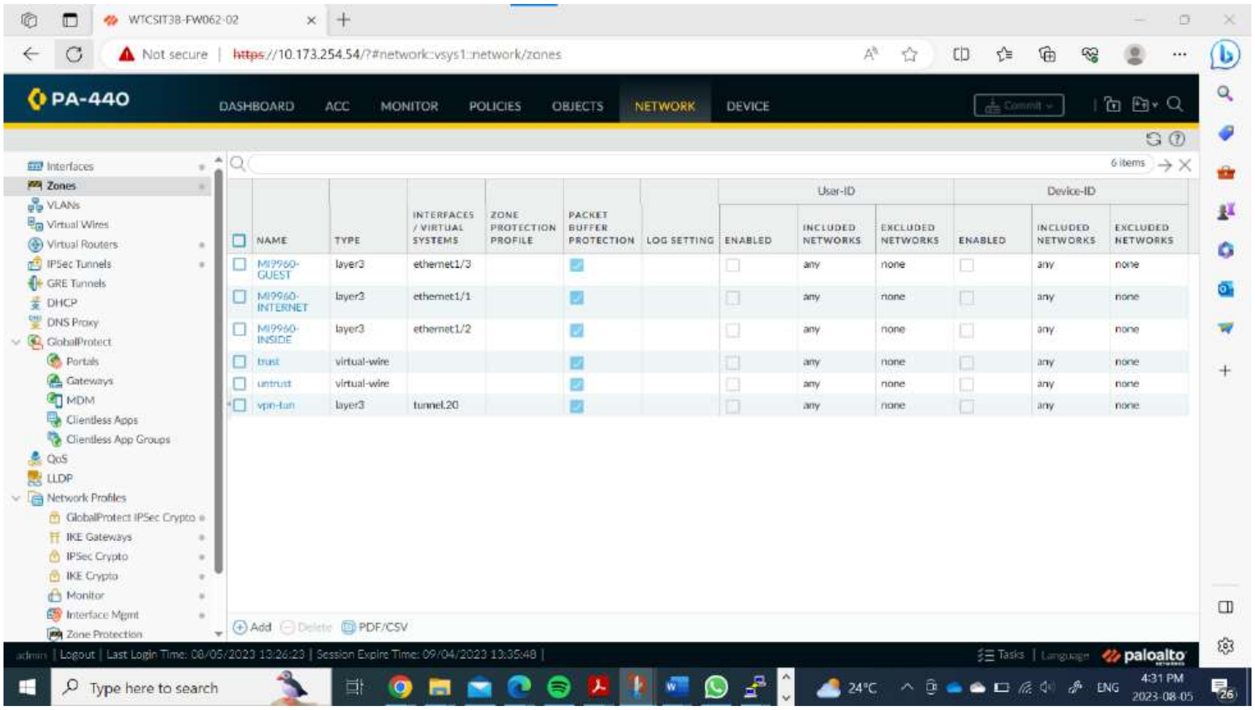
Figure 23 shows my branch interface on my palo -alto.



□	NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
□	MI9960-BR	ethernet1/1 ethernet1/2 ethernet1/3 tunnel.20	Static Routes: 2 ECMP status: Disabled						More Runtime Stats
□	default		ECMP status: Disabled						More Runtime Stats

admin | Logout | Last Login Time: 08/05/2023 13:26:23 | Session Expire Time: 09/04/2023 13:35:48 |

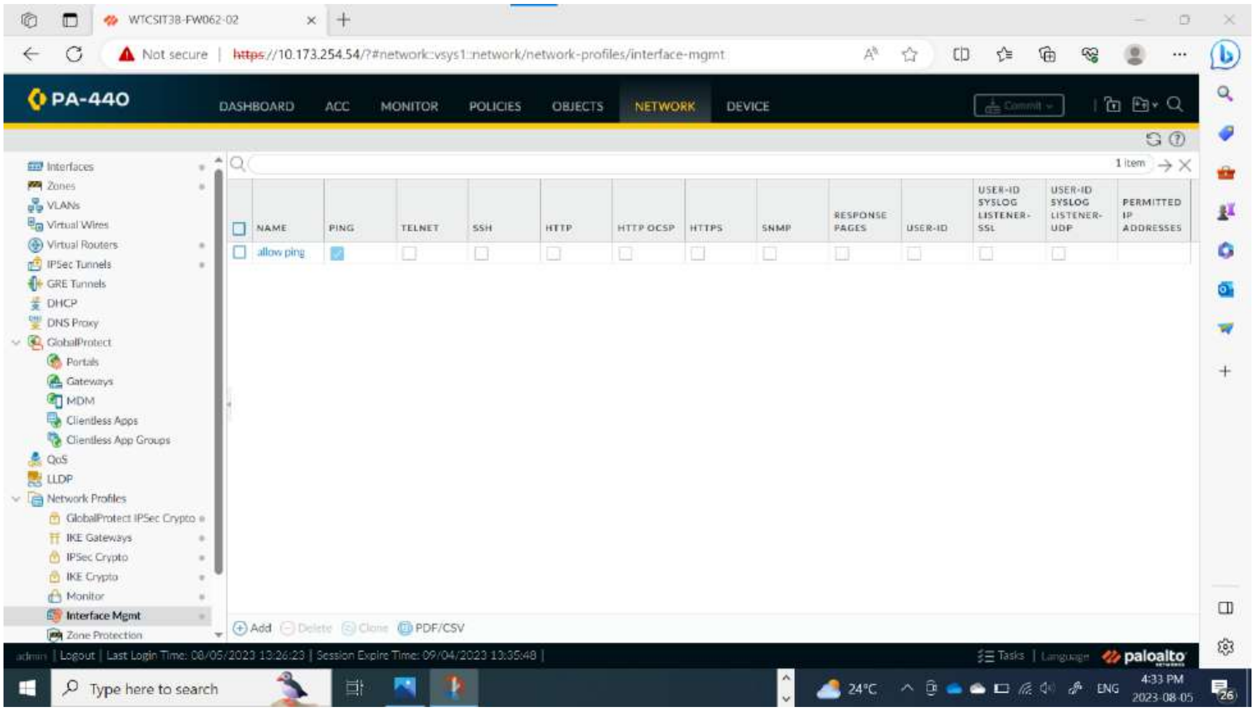
Figure 24 shows my virtual router created.



https://10.173.254.54/?#network::vsys1::network/zones

☐	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID ENABLED	User-ID INCLUDED NETWORKS	User-ID EXCLUDED NETWORKS	Device-ID ENABLED	Device-ID INCLUDED NETWORKS	Device-ID EXCLUDED NETWORKS
☐	MI9960-GUEST	layer3	ethernet1/3		☑		☐	any	none	☐	any	none
☐	MI9960-INTERNET	layer3	ethernet1/1		☑		☐	any	none	☐	any	none
☐	MI9960-INSIDE	layer3	ethernet1/2		☑		☐	any	none	☐	any	none
☐	trust	virtual-wire			☑		☐	any	none	☐	any	none
☐	untrust	virtual-wire			☑		☐	any	none	☐	any	none
☐	vpn-tun	layer3	tunnel.20		☑		☐	any	none	☐	any	none

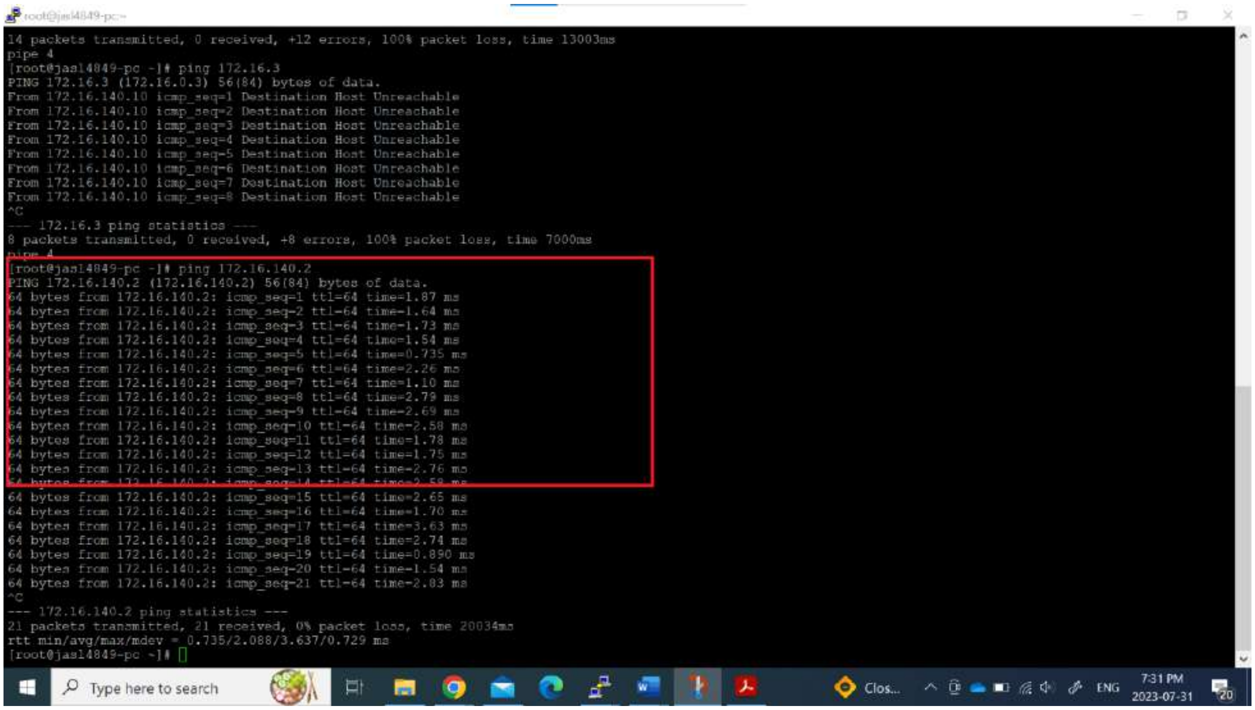
Figure 25 shows the zone i created.



https://10.173.254.54/?#network::vsys1::network/network-profiles/interface-mgmt

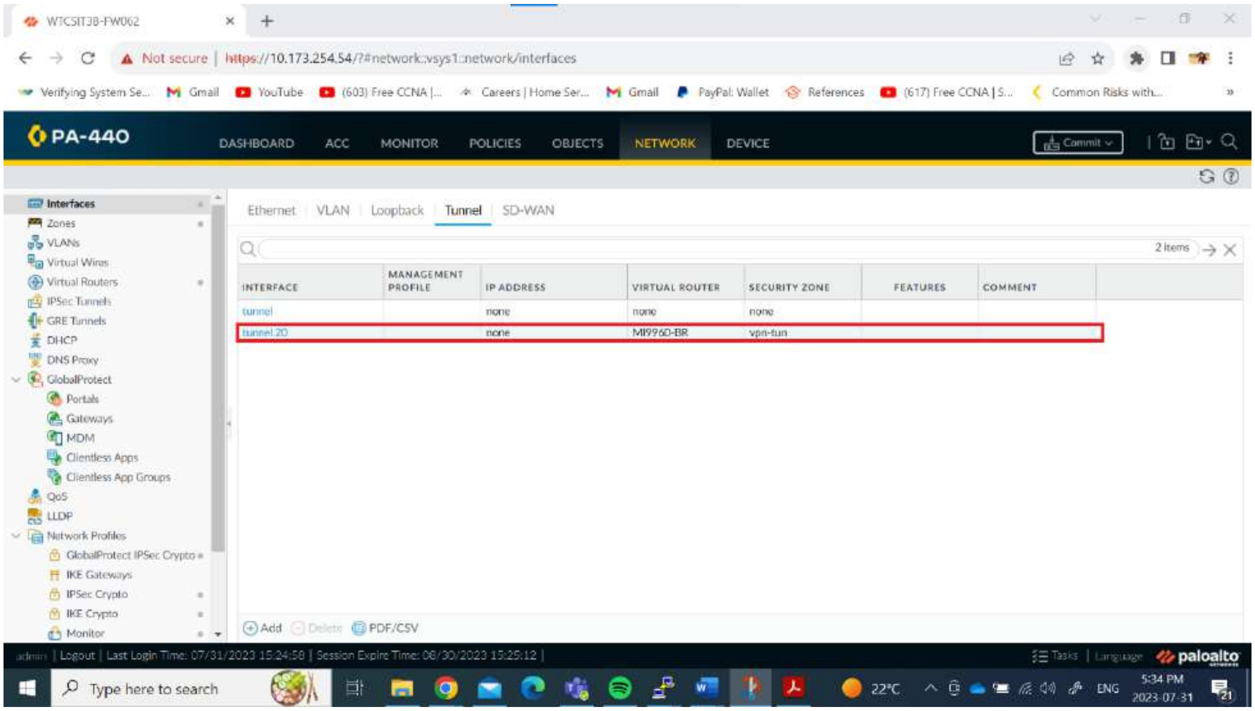
☐	NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	USER-ID SYSLOG LISTENER-SSL	USER-ID SYSLOG LISTENER-UDP	PERMITTED IP ADDRESSES
☐	allow ping	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Figure 26 shows i allowed ping.



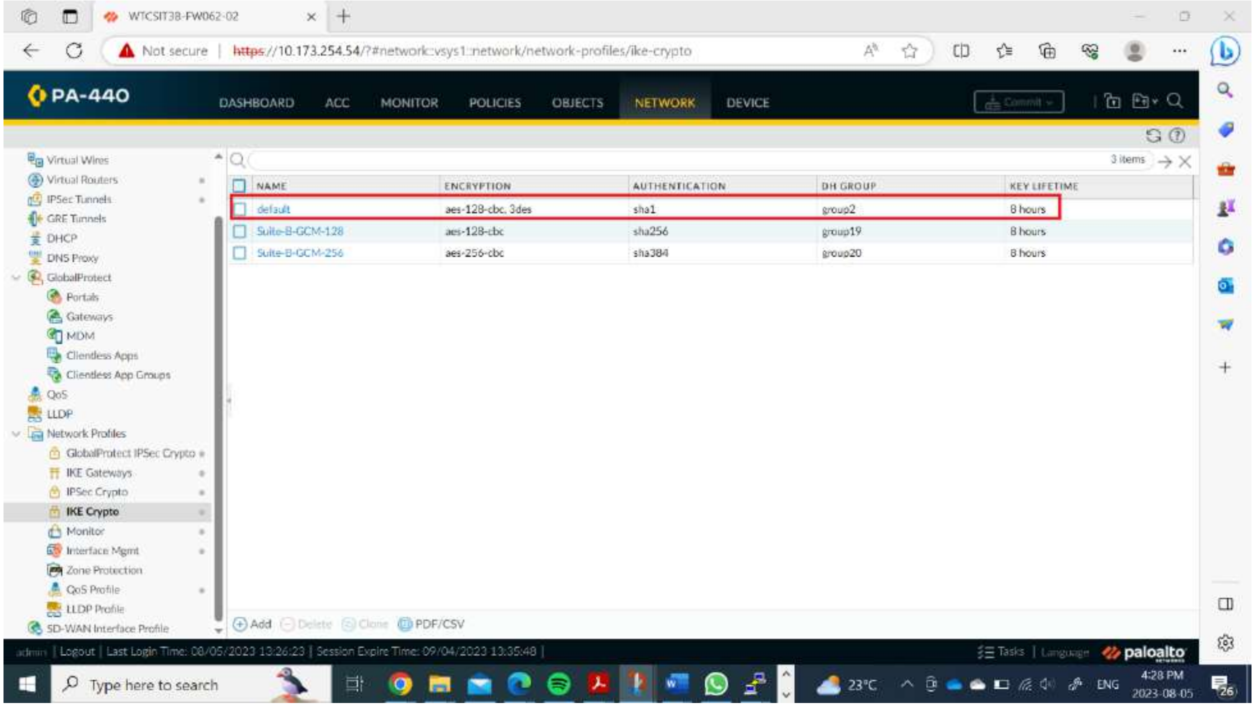
```
14 packets transmitted, 0 received, +12 errors, 100% packet loss, time 13003ms
pipe 4
[root@jasl4849-pc ~]# ping 172.16.3
PING 172.16.3 (172.16.0.3) 56(84) bytes of data.
From 172.16.140.10 icmp_seq=1 Destination Host Unreachable
From 172.16.140.10 icmp_seq=2 Destination Host Unreachable
From 172.16.140.10 icmp_seq=3 Destination Host Unreachable
From 172.16.140.10 icmp_seq=4 Destination Host Unreachable
From 172.16.140.10 icmp_seq=5 Destination Host Unreachable
From 172.16.140.10 icmp_seq=6 Destination Host Unreachable
From 172.16.140.10 icmp_seq=7 Destination Host Unreachable
From 172.16.140.10 icmp_seq=8 Destination Host Unreachable
^C
--- 172.16.3 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 7000ms
pipe 4
[root@jasl4849-pc ~]# ping 172.16.140.2
PING 172.16.140.2 (172.16.140.2) 56(84) bytes of data.
64 bytes from 172.16.140.2: icmp_seq=1 ttl=64 time=1.87 ms
64 bytes from 172.16.140.2: icmp_seq=2 ttl=64 time=1.64 ms
64 bytes from 172.16.140.2: icmp_seq=3 ttl=64 time=1.73 ms
64 bytes from 172.16.140.2: icmp_seq=4 ttl=64 time=1.54 ms
64 bytes from 172.16.140.2: icmp_seq=5 ttl=64 time=0.735 ms
64 bytes from 172.16.140.2: icmp_seq=6 ttl=64 time=2.26 ms
64 bytes from 172.16.140.2: icmp_seq=7 ttl=64 time=1.10 ms
64 bytes from 172.16.140.2: icmp_seq=8 ttl=64 time=2.79 ms
64 bytes from 172.16.140.2: icmp_seq=9 ttl=64 time=2.69 ms
64 bytes from 172.16.140.2: icmp_seq=10 ttl=64 time=2.58 ms
64 bytes from 172.16.140.2: icmp_seq=11 ttl=64 time=1.78 ms
64 bytes from 172.16.140.2: icmp_seq=12 ttl=64 time=1.75 ms
64 bytes from 172.16.140.2: icmp_seq=13 ttl=64 time=2.76 ms
64 bytes from 172.16.140.2: icmp_seq=14 ttl=64 time=2.58 ms
64 bytes from 172.16.140.2: icmp_seq=15 ttl=64 time=2.65 ms
64 bytes from 172.16.140.2: icmp_seq=16 ttl=64 time=1.70 ms
64 bytes from 172.16.140.2: icmp_seq=17 ttl=64 time=3.63 ms
64 bytes from 172.16.140.2: icmp_seq=18 ttl=64 time=2.74 ms
64 bytes from 172.16.140.2: icmp_seq=19 ttl=64 time=0.890 ms
64 bytes from 172.16.140.2: icmp_seq=20 ttl=64 time=1.54 ms
64 bytes from 172.16.140.2: icmp_seq=21 ttl=64 time=2.83 ms
^C
--- 172.16.140.2 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20034ms
rtt min/avg/max/mdev = 0.735/2.088/3.637/0.729 ms
[root@jasl4849-pc ~]# 
```

Figure 27 pinging my palo-alto.



INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
tunnel		none	none	none		
tunnel.20		none	MI9960-BR	vpn-tun		

Figure 28 shows the interface i created.

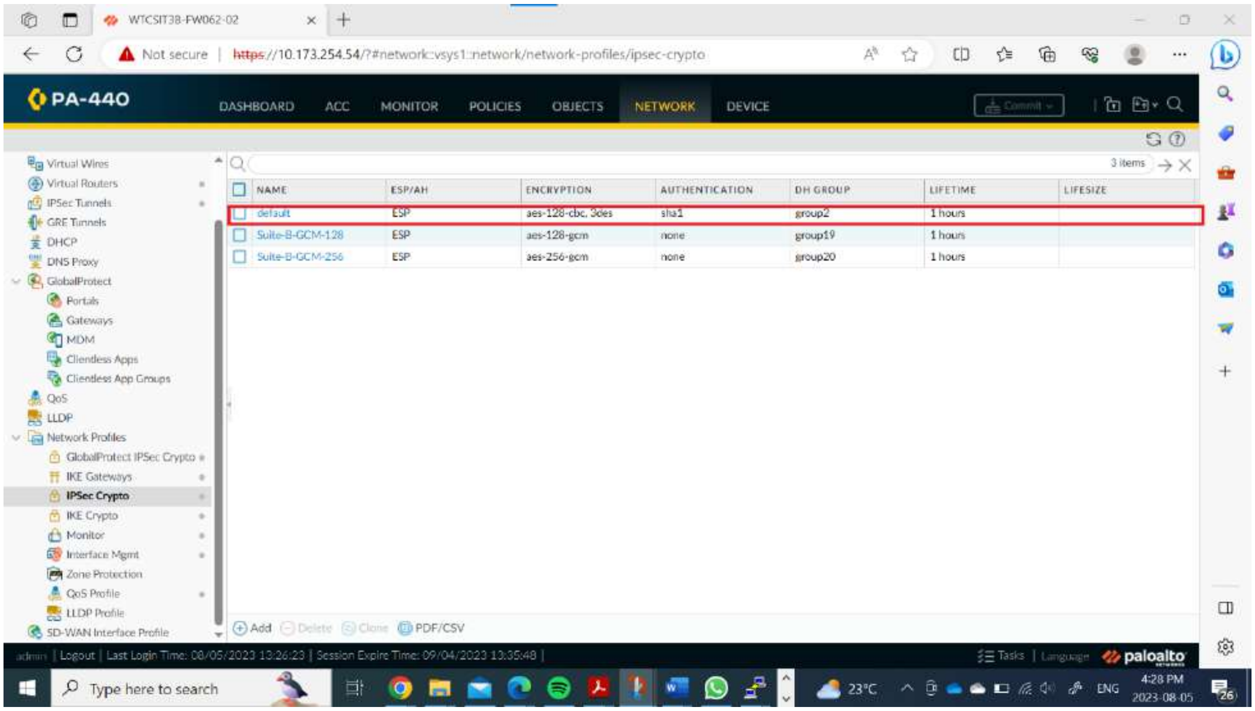


https://10.173.254.54/?#network::vsys1::network/network-profiles/ike-crypto

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

admin | Logout | Last Login Time: 08/05/2023 13:26:23 | Session Expire Time: 09/04/2023 13:35:48 |

Figure 29 shows the IKE crypto.

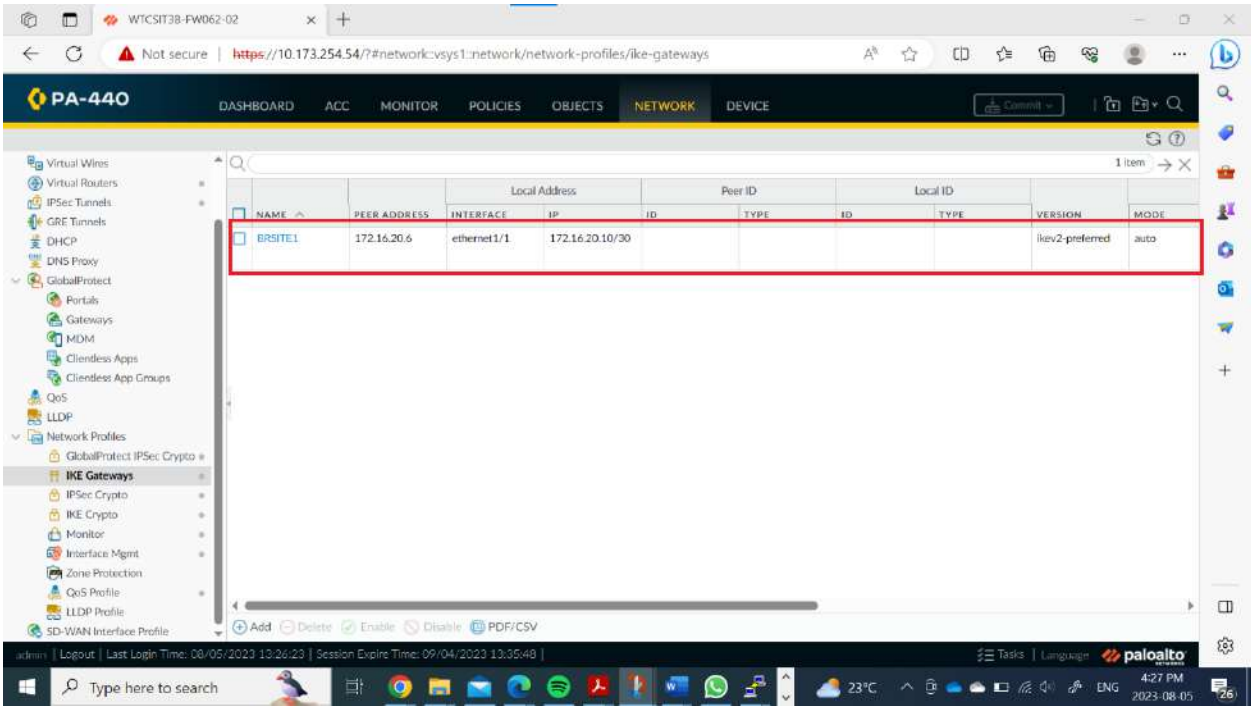


https://10.173.254.54/?#network::vsys1::network/network-profiles/ipsec-crypto

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	

admin | Logout | Last Login Time: 08/05/2023 13:26:23 | Session Expire Time: 09/04/2023 13:35:48 |

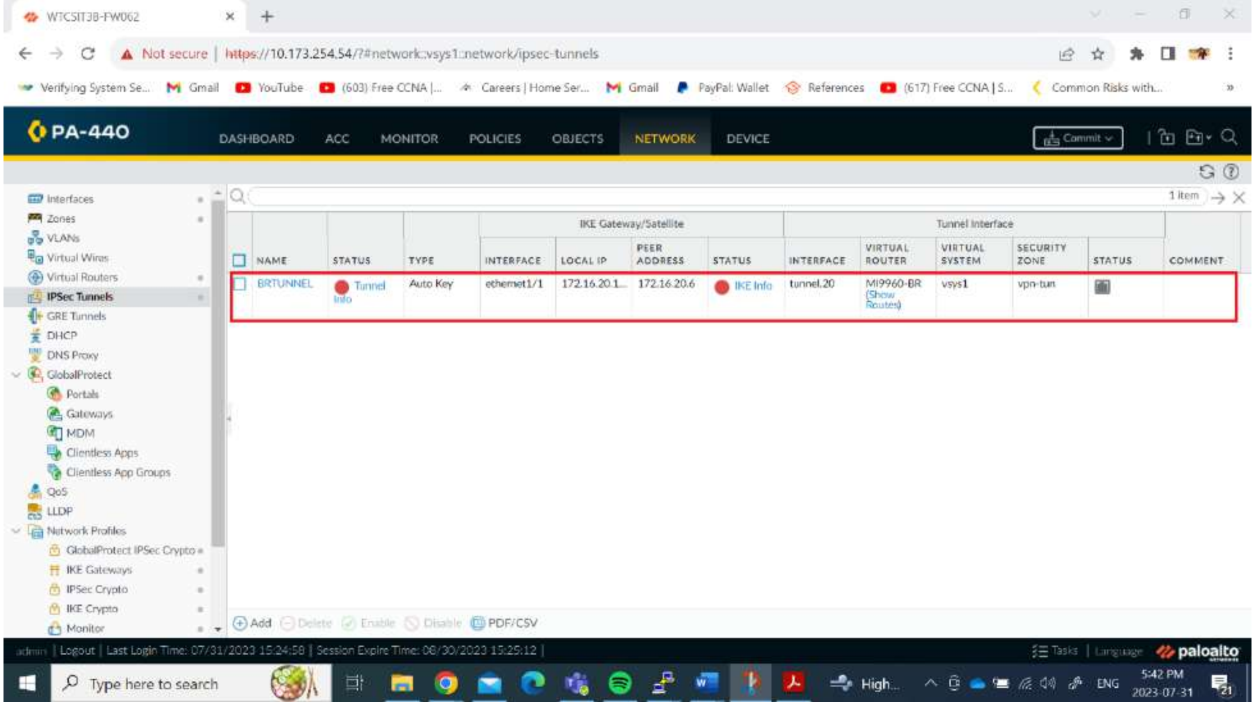
Figure 30 shows the IPSec Crypto.



https://10.173.254.54/?#network::vsys1::network/network-profiles/ike-gateways

		Local Address		Peer ID		Local ID			
NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION	MODE
BRSITE1	172.16.20.6	ethernet1/1	172.16.20.10/30					ikev2-preferred	auto

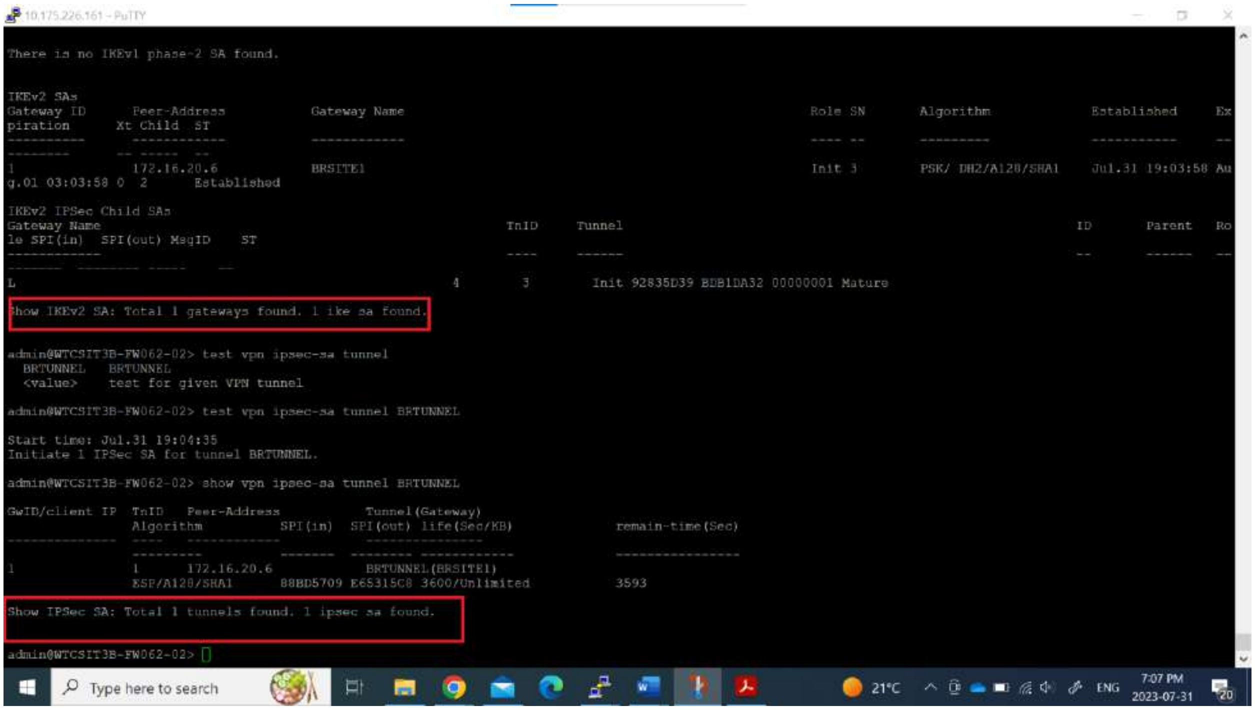
Figure 31 shows my IKE gateway created.



https://10.173.254.54/?#network::vsys1::network/ipsec-tunnels

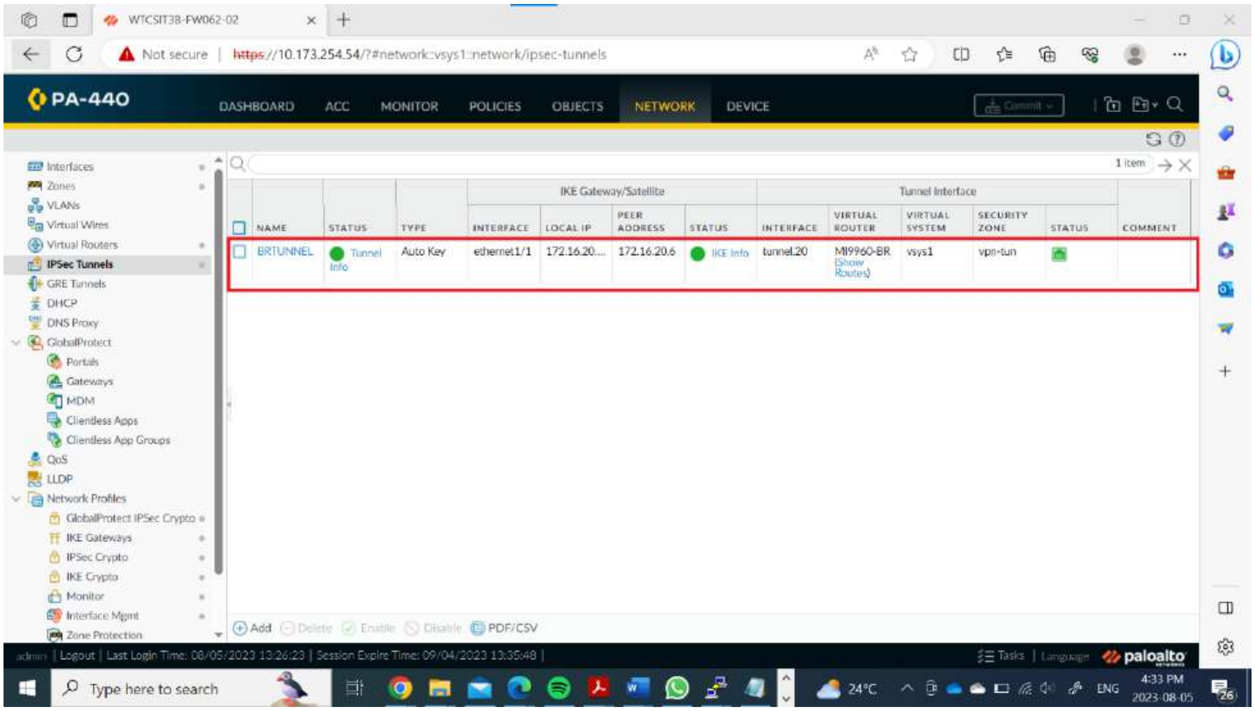
			IKE Gateway/Satellite				Tunnel Interface					
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	COMMENT
BRTUNNEL	● Tunnel Info	Auto Key	ethernet1/1	172.16.20.1...	172.16.20.6	● IKE Info	tunnel.20	MI9960-BR (Show Routes)	vsys1	vpn-tun		

Figure 32 shows the IPsec tunnel i created.



```
There is no IKEv1 phase-2 SA found.


IKEv2 SAs
Gateway ID      Peer-Address           Gateway Name                                                         Role SN      Algorithm             Established     Ex
piration      Xt Child  ST
----------      ------------           ------------                                                         ---- --      ---------             -----------     --
--------      -- -----  --
1               172.16.20.6            BRSITE1                                                              Init 3       PSK/ DH2/A128/SHA1    Jul.31 19:03:58 Au
g.01 03:03:58 0  2      Established

IKEv2 IPSec Child SAs
Gateway Name                                                      TnID     Tunnel                                                   ID       Parent   Ro
le SPI(in)  SPI(out) MsgID    ST
------------                                                      ----     ------                                                   --       ------   --
-------- -------- -----    --
L                                                         4         3        Init 92835D39 BDB1DA32 00000001 Mature

Show IKEv2 SA: Total 1 gateways found. 1 ike sa found.

admin@WTCSIT3B-FW062-02> test vpn ipsec-sa tunnel
  BRTUNNEL   BRTUNNEL
  <value>    test for given VPN tunnel

admin@WTCSIT3B-FW062-02> test vpn ipsec-sa tunnel BRTUNNEL

Start time: Jul.31 19:04:35
Initiate 1 IPSec SA for tunnel BRTUNNEL.

admin@WTCSIT3B-FW062-02> show vpn ipsec-sa tunnel BRTUNNEL

GwID/client IP  TnID   Peer-Address          Tunnel(Gateway)
                Algorithm          SPI(in)   SPI(out) life(Sec/KB)              remain-time(Sec)
--------------  ----   ------------          ----------------
                ---------          -------   -------- ------------              ----------------
1               1      172.16.20.6           BRTUNNEL(BRSITE1)
                ESP/A128/SHA1      88BD5709 E65315C8 3600/Unlimited             3593

Show IPSec SA: Total 1 tunnels found. 1 ipsec sa found.

admin@WTCSIT3B-FW062-02>
```

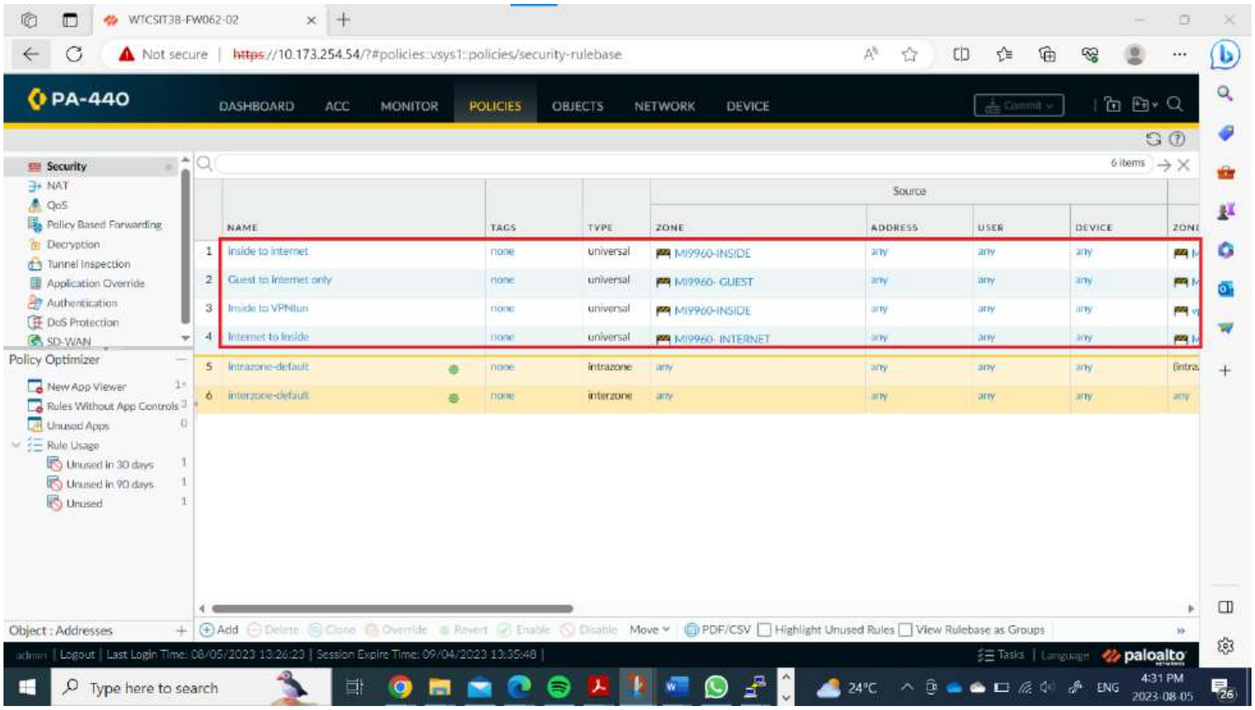
Figure 33 shows my initialization of my branch tunnel.



			IKE Gateway/Satellite				Tunnel Interface					
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS	COMMENT
BRTUNNEL	● Tunnel Info	Auto Key	ethernet1/1	172.16.20....	172.16.20.6	● IKE Info	tunnel.20	MI9960-BR (Show Routes)	vsys1	vpn-tun	🟩	

admin | Logout | Last Login Time: 08/05/2023 13:26:23 | Session Expire Time: 09/04/2023 13:35:48 |

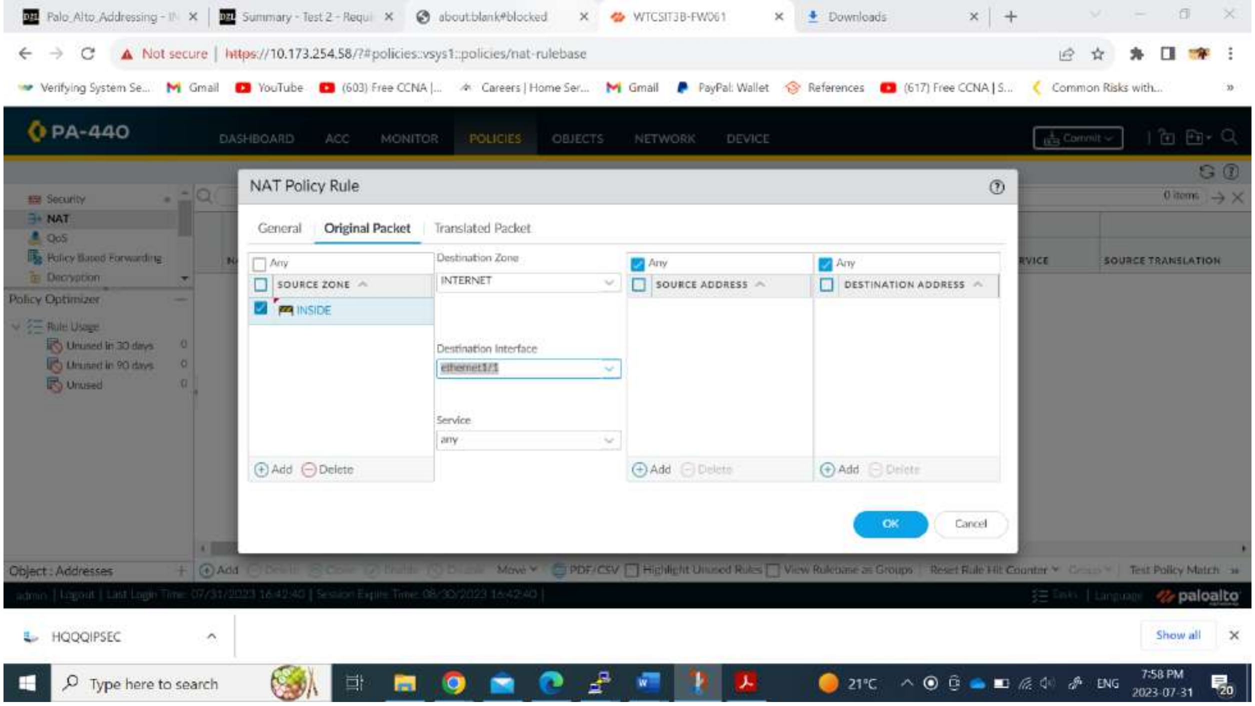
Figure 34 shows my tunnel connection has been established.



admin | Logout | Last Login Time: 08/05/2023 13:26:23 | Session Expire Time: 09/04/2023 13:35:48 |

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE
1	Inside to internet	none	universal	MI9960-INSIDE	any	any	any
2	Guest to Internet only	none	universal	MI9960- GUEST	any	any	any
3	Inside to VPNtun	none	universal	MI9960-INSIDE	any	any	any
4	Internet to Inside	none	universal	MI9960- INTERNET	any	any	any
5	intrazone-default	none	intrazone	any	any	any	any
6	interzone-default	none	interzone	any	any	any	any

Figure 35 shows my policy i established.



NAT Policy Rule

General | **Original Packet** | Translated Packet

□ Any
□ SOURCE ZONE
☑ INSIDE

Destination Zone: INTERNET

Destination Interface: ethernet1/1

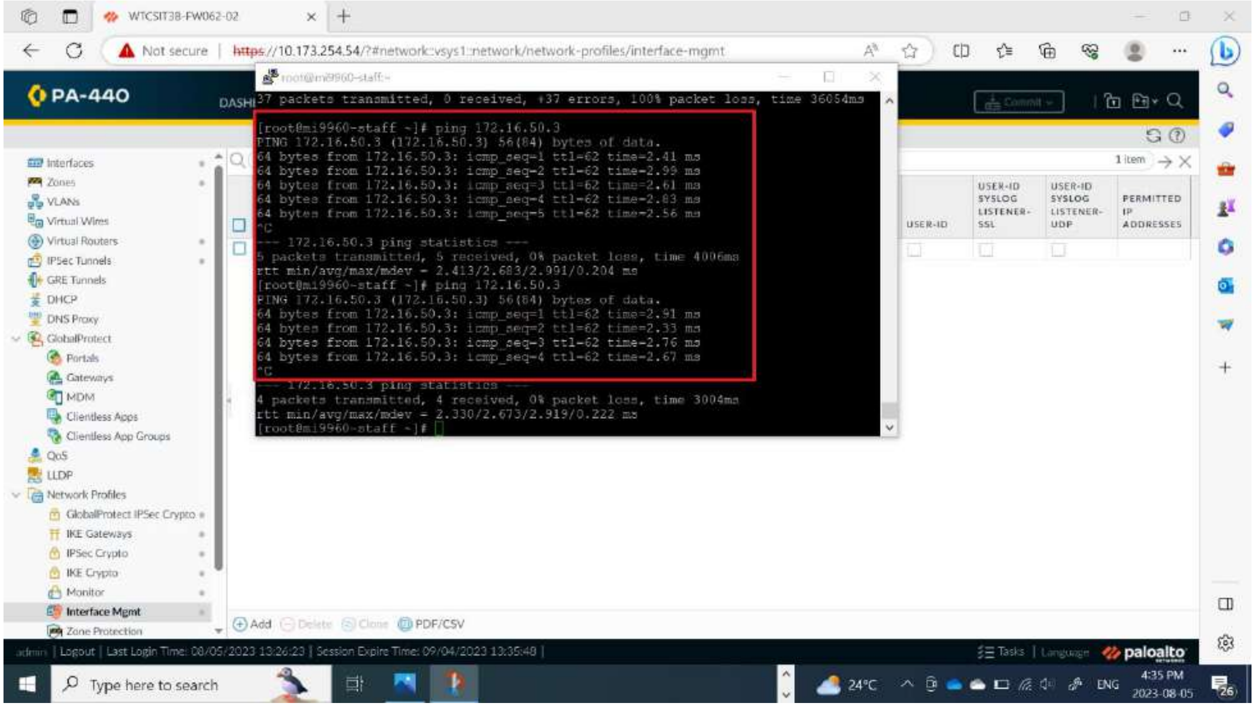
Service: any

☑ Any
□ SOURCE ADDRESS

☑ Any
□ DESTINATION ADDRESS

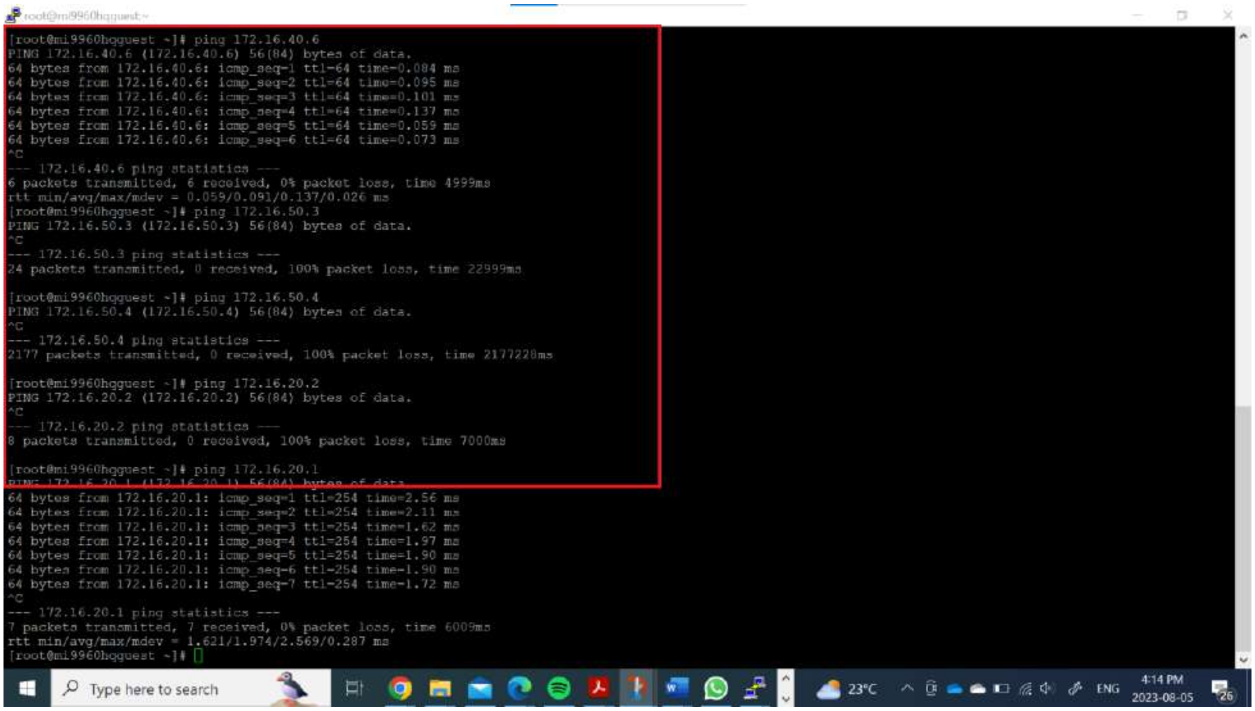
OK | Cancel

Figure 36 shows the NAT policy i created.



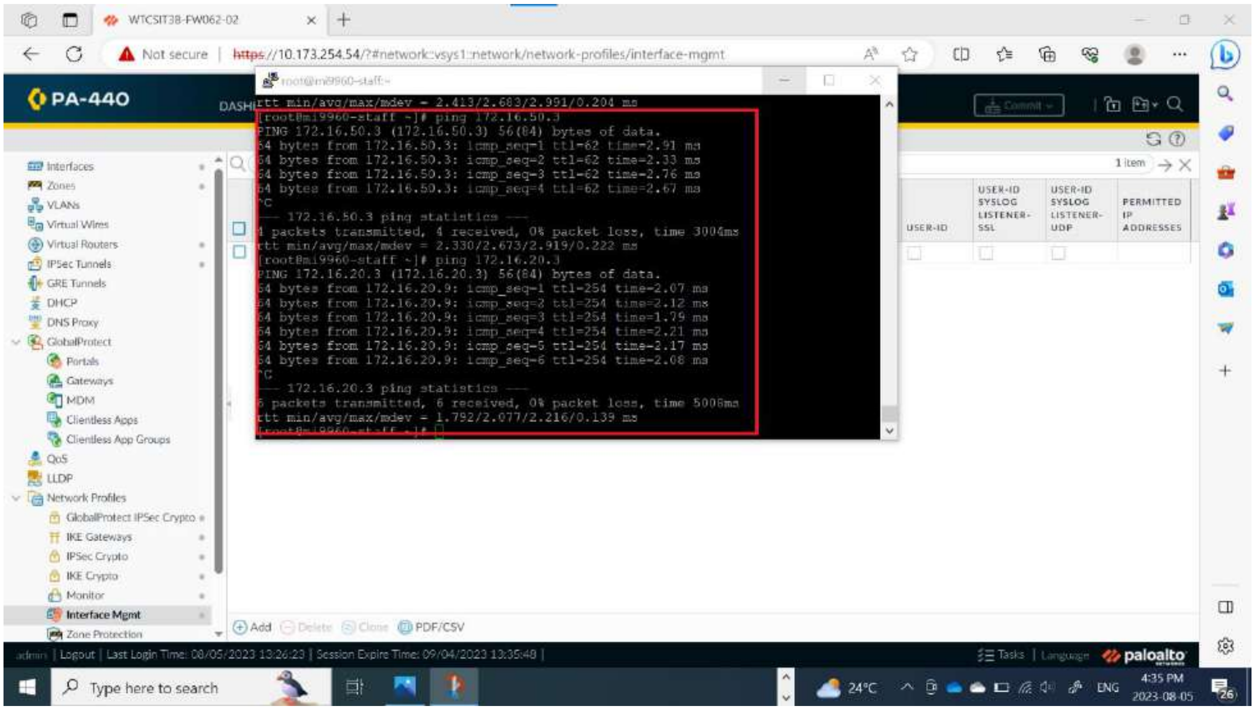
```
37 packets transmitted, 0 received, +37 errors, 100% packet loss, time 36054ms

[root@mi9960-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=62 time=2.41 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=62 time=2.99 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=62 time=2.61 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=62 time=2.83 ms
64 bytes from 172.16.50.3: icmp_seq=5 ttl=62 time=2.56 ms
^C
--- 172.16.50.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.413/2.683/2.991/0.204 ms
[root@mi9960-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=62 time=2.91 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=62 time=2.33 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=62 time=2.76 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=62 time=2.67 ms
^C
--- 172.16.50.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.330/2.673/2.919/0.222 ms
[root@mi9960-staff ~]#
```

Figure 37 shows my ping from my inside to my server in HQ.



```
[root@mi9960hqguest ~]# ping 172.16.40.6
PING 172.16.40.6 (172.16.40.6) 56(84) bytes of data.
64 bytes from 172.16.40.6: icmp_seq=1 ttl=64 time=0.084 ms
64 bytes from 172.16.40.6: icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from 172.16.40.6: icmp_seq=3 ttl=64 time=0.101 ms
64 bytes from 172.16.40.6: icmp_seq=4 ttl=64 time=0.137 ms
64 bytes from 172.16.40.6: icmp_seq=5 ttl=64 time=0.059 ms
64 bytes from 172.16.40.6: icmp_seq=6 ttl=64 time=0.073 ms
^C
--- 172.16.40.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.059/0.091/0.137/0.026 ms
[root@mi9960hqguest ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
^C
--- 172.16.50.3 ping statistics ---
24 packets transmitted, 0 received, 100% packet loss, time 22999ms

[root@mi9960hqguest ~]# ping 172.16.50.4
PING 172.16.50.4 (172.16.50.4) 56(84) bytes of data.
^C
--- 172.16.50.4 ping statistics ---
2177 packets transmitted, 0 received, 100% packet loss, time 2177228ms

[root@mi9960hqguest ~]# ping 172.16.20.2
PING 172.16.20.2 (172.16.20.2) 56(84) bytes of data.
^C
--- 172.16.20.2 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7000ms

[root@mi9960hqguest ~]# ping 172.16.20.1
PING 172.16.20.1 (172.16.20.1) 56(84) bytes of data.
64 bytes from 172.16.20.1: icmp_seq=1 ttl=254 time=2.56 ms
64 bytes from 172.16.20.1: icmp_seq=2 ttl=254 time=2.11 ms
64 bytes from 172.16.20.1: icmp_seq=3 ttl=254 time=1.62 ms
64 bytes from 172.16.20.1: icmp_seq=4 ttl=254 time=1.97 ms
64 bytes from 172.16.20.1: icmp_seq=5 ttl=254 time=1.90 ms
64 bytes from 172.16.20.1: icmp_seq=6 ttl=254 time=1.90 ms
64 bytes from 172.16.20.1: icmp_seq=7 ttl=254 time=1.72 ms
^C
--- 172.16.20.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 1.621/1.974/2.569/0.287 ms
[root@mi9960hqguest ~]#
```

Figure 38 my guest can ping the internet.



```
rtt min/avg/max/mdev = 2.413/2.683/2.991/0.204 ms
[root@mi9960-staff ~]# ping 172.16.50.3
PING 172.16.50.3 (172.16.50.3) 56(84) bytes of data.
64 bytes from 172.16.50.3: icmp_seq=1 ttl=62 time=2.91 ms
64 bytes from 172.16.50.3: icmp_seq=2 ttl=62 time=2.33 ms
64 bytes from 172.16.50.3: icmp_seq=3 ttl=62 time=2.76 ms
64 bytes from 172.16.50.3: icmp_seq=4 ttl=62 time=2.67 ms
^C
--- 172.16.50.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.330/2.673/2.919/0.222 ms
[root@mi9960-staff ~]# ping 172.16.20.3
PING 172.16.20.3 (172.16.20.3) 56(84) bytes of data.
64 bytes from 172.16.20.9: icmp_seq=1 ttl=254 time=2.07 ms
64 bytes from 172.16.20.9: icmp_seq=2 ttl=254 time=2.12 ms
64 bytes from 172.16.20.9: icmp_seq=3 ttl=254 time=1.79 ms
64 bytes from 172.16.20.9: icmp_seq=4 ttl=254 time=2.21 ms
64 bytes from 172.16.20.9: icmp_seq=5 ttl=254 time=2.17 ms
64 bytes from 172.16.20.9: icmp_seq=6 ttl=254 time=2.08 ms
^C
--- 172.16.20.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.792/2.077/2.216/0.139 ms
[root@mi9960-staff ~]#
```

Figure 39 shows inside can ping internet network.