Introduction:

After updating the operating system and configuring SOHO on our Palo Alto PA-220s, this is what I would consider our first non-initial configuration lab. This lab requires 2 firewalls to establish a tunnel across the network, so we are working in groups of 4 (2 pairs). We will establish a site-to-site VPN using Internet Protocol Security (IPSec) which is widely used within the industry to establish secure connections over Internet Protocol (IP) networks. Because of the wide use of site-to-site VPN using IPSec and IPSec in general, this lab is meant to build a foundational understanding of this protocol and how to set up and implement it.

Background Information:

-Site-to-site VPNs provides a secure IPSec connection between two or more different networks. IPsec works by encrypting traffic before the packets are transferred over the network and decrypts them when they arrive at the destination. This encryption is done by the use of Internet Key Exchange (IKE) protocol which allows for the establishment of a secure authenticated connection which can also negotiate parameters. IKE gateways are used to encrypt and decrypt traffic that travels across the VPN tunnel acting to essentially get traffic on and off the network. IKE gateways also initiate the IKE negotiations process when establishing a VPN.

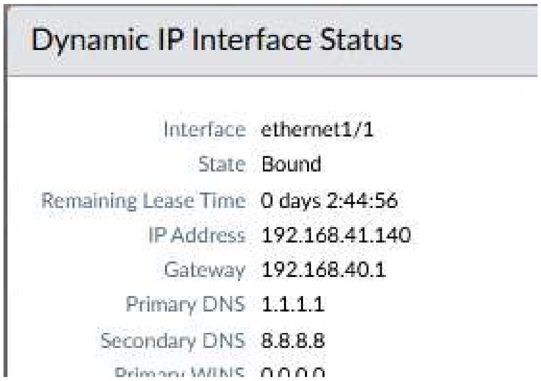
Site-to-site VPNs differ from point-to-point VPNs as they have different uses. Site-to-site is a more "grand” VPN as it sends traffic between two networks whereas point-to-point is meant for just specific devices or remote access. This narrows the scope for point-to-point’s scalability whereas site-to-site was designed to be scalable due to it’s use to establish connections between entire networks instead of devices.

Site-to-Site VPNs with IPSec have many benefits to it, but the most important one is how cost-effective and scalable it is opposed to other secure connectivity methods. In terms of scalability, the lack of dedicated infrastructure for site-to-site results in it being easy to deploy over already existing networks without having to build new infrastructure. Site-to-site is also highly cloud compatible enabling for more users to be able to implement easily with cloud infrastructure. In terms of cost effectiveness, due to running off existing infrastructure, site-to-site doesn't require things like dedicated lease lines which cost much more to build, maintain, and manage. Site-to-site also has scalable pricing, much like AWS' pay as you go model, you only pay for what you use over set time period reducing costs for consumers. Site-to-site's easy could implementation means that consumers can easily take advantage of the cheaper costs of cloud services over on site servers, which allows site-to-site to indirectly cut costs.

Lab Summary:

This lab establishes a site-to-site VPN connection between two PA-220s, in order to do this, we first need to set static IPs for our firewalls so DHCP doesn't mess up our configurations. Then we create the VPN zone for the traffic to travel through and IKE gateways for traffic encryption and decryption. We also create an IPSec crpyto profile. We then create the tunnel and tunnel interface before modifying the security policy in order for the traffic to be able to be sent though the tunnel. We are now able to remote desktop though the VPN from one machine on one network to another in the opposite network.

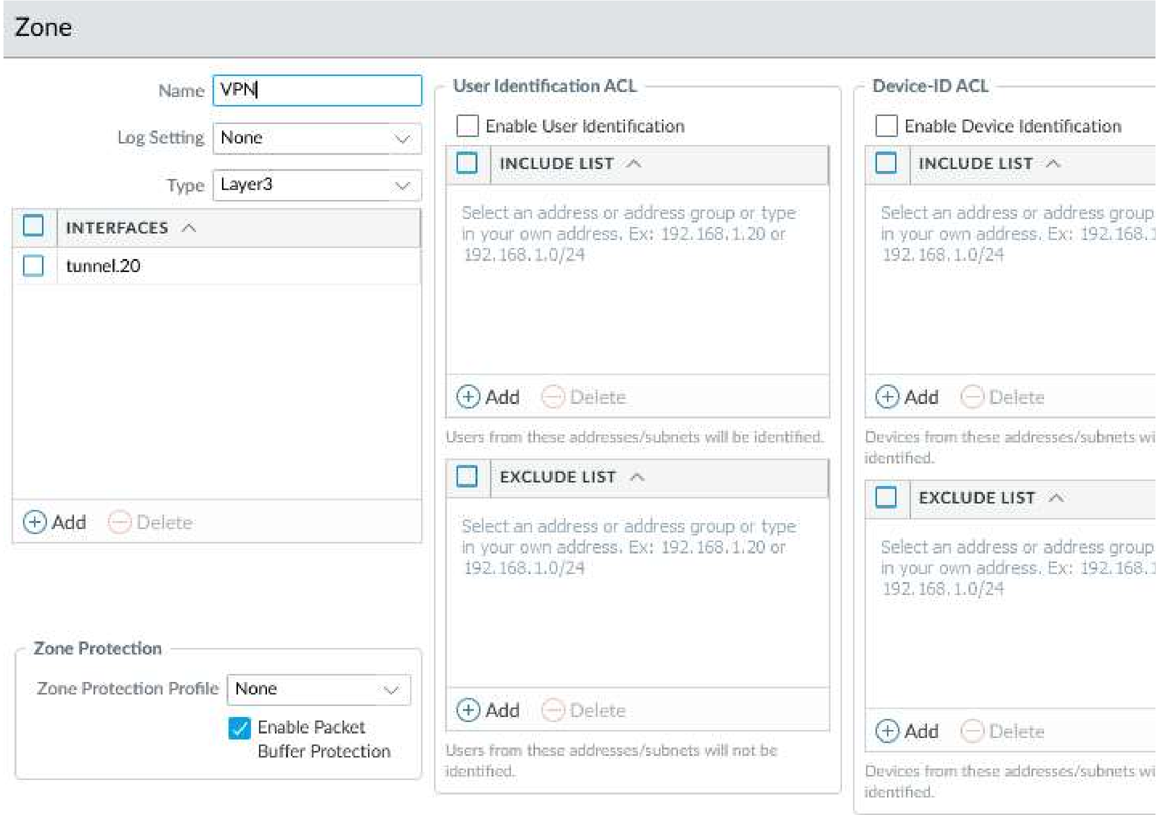
Lab:



Dynamic IP Interface Status

Interface ethernet1/1
State Bound
Remaining Lease Time 0 days 2:44:56
IP Address 192.168.41.140
Gateway 192.168.40.1
Primary DNS 1.1.1.1
Secondary DNS 8.8.8.8
Primary WINS 0.0.0.0

1: Check your DHCP IP address on both firewalls. To ensure that the gateway address does not change between restarts of the firewall, set dedicated addresses to the firewalls.



Zone

Name VPN
Log Setting None
Type Layer3

□ INTERFACES
□ tunnel.20

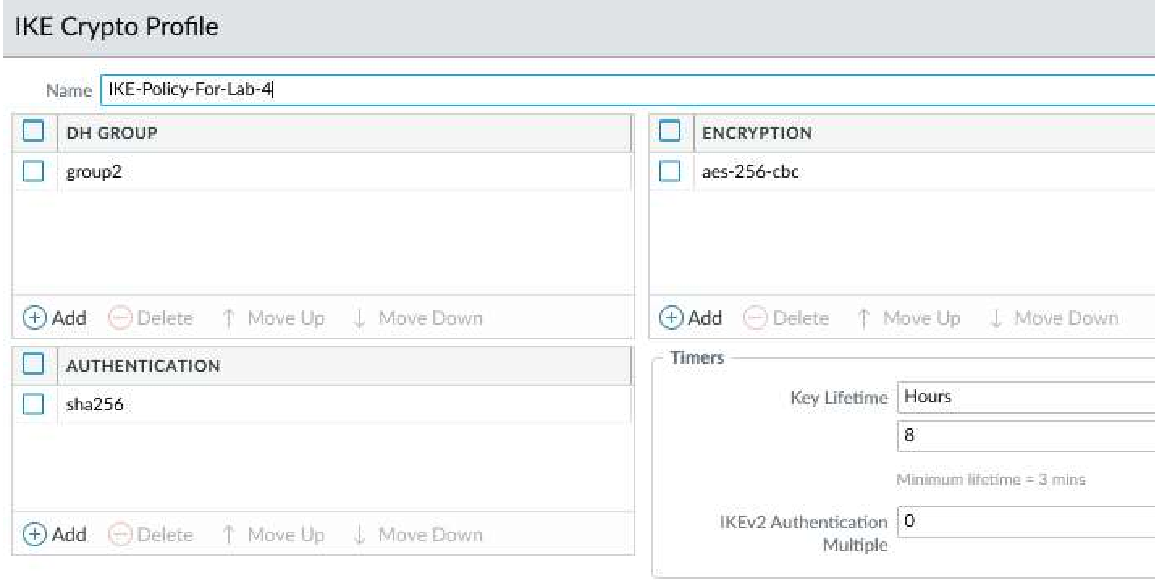
⊕ Add ⊖ Delete

Zone Protection
Zone Protection Profile None
☑ Enable Packet Buffer Protection

User Identification ACL
□ Enable User Identification
□ INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Users from these addresses/subnets will be identified.
□ EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
⊕ Add ⊖ Delete
Users from these addresses/subnets will not be identified.

Device-ID ACL
□ Enable Device Identification
□ INCLUDE LIST
Select an address or address group in your own address. Ex: 192.168.1 192.168.1.0/24
⊕ Add ⊖ Delete
Devices from these addresses/subnets wi identified.
□ EXCLUDE LIST
Select an address or address group in your own address. Ex: 192.168.1 192.168.1.0/24
⊕ Add ⊖ Delete
Devices from these addresses/subnets wi identified.

2: On both firewalls under Zones > add, create a new zone with the configuration shown above.


IKE Crypto Profile

Name IKE-Policy-For-Lab-4

□	DH GROUP
□	group2

□	ENCRYPTION
□	aes-256-cbc

□	AUTHENTICATION
□	sha256

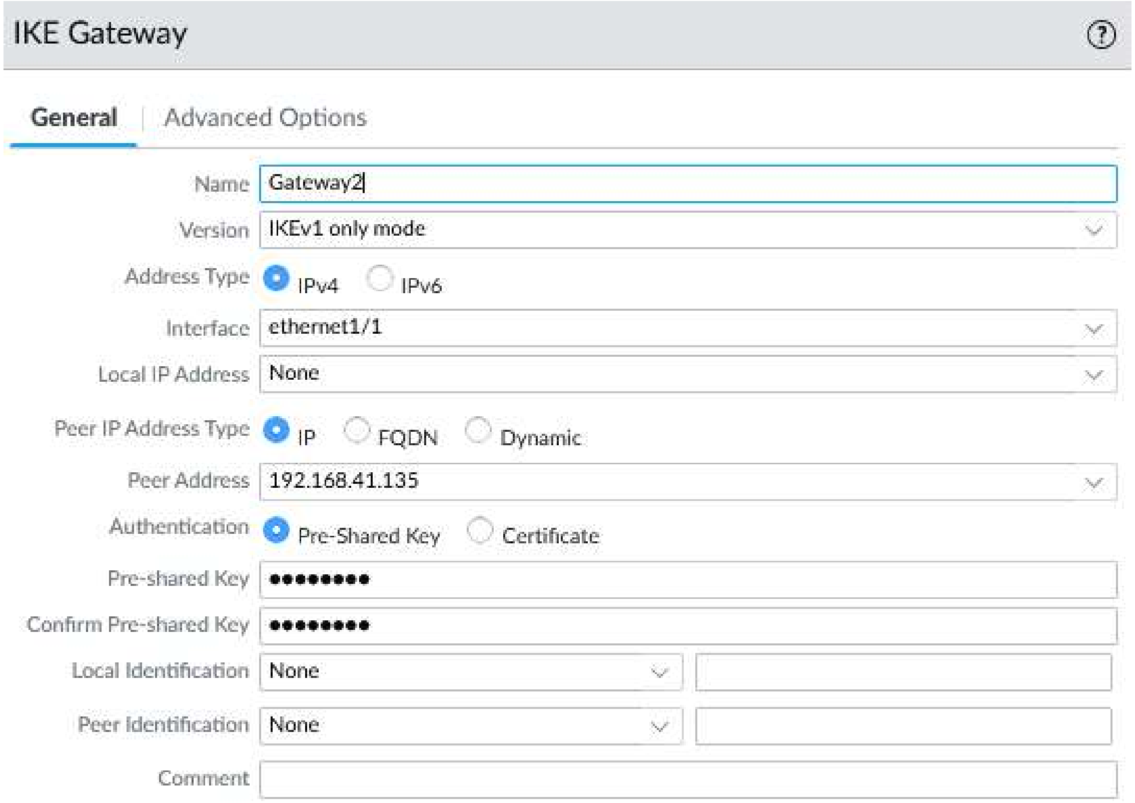
Timers

Key Lifetime: Hours, 8

Minimum lifetime = 3 mins

IKEv2 Authentication Multiple: 0

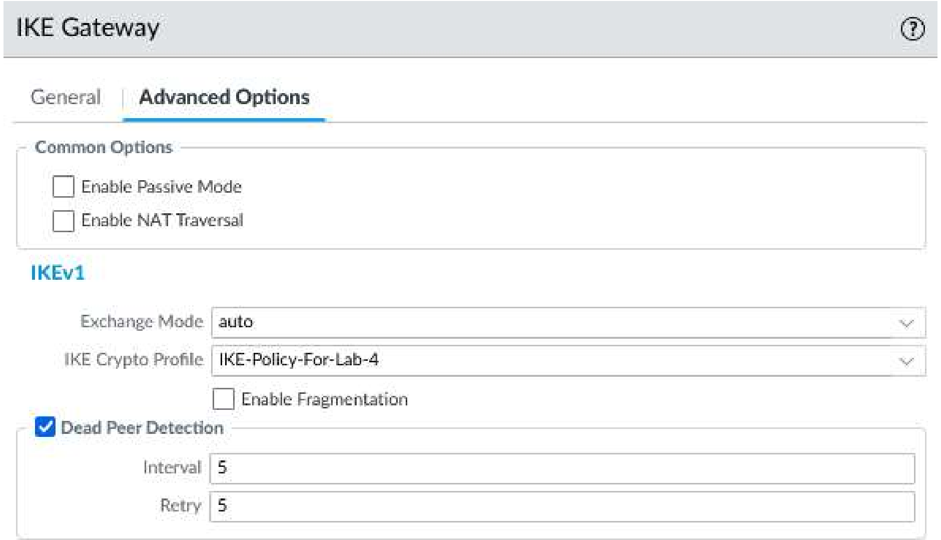
3: On BOTH firewalls, create an IKE Crypto profile under Network > IKE Crypto and select a group number and encryption/authentication method.



IKE Gateway

Name	Gateway2
Version	IKEv1 only mode
Address Type	● IPv4 ○ IPv6
Interface	ethernet1/1
Local IP Address	None
Peer IP Address Type	● IP ○ FQDN ○ Dynamic
Peer Address	192.168.41.135
Authentication	● Pre-Shared Key ○ Certificate
Pre-shared Key	••••••••
Confirm Pre-shared Key	••••••••
Local Identification	None
Peer Identification	None
Comment	

4: Create an IKE Gateways under Network > IKE Gateway. Enter a name and choose IKEv1 only mode as your Version. Configure the interface as your outbound interface then enter then Peer Address as the outbound interface of your opposing firewall. Enter the same preshared key on both firewalls.



IKE Gateway

General | Advanced Options

Common Options

☐ Enable Passive Mode

☐ Enable NAT Traversal

IKEv1

Exchange Mode: auto

IKE Crypto Profile: IKE-Policy-For-Lab-4

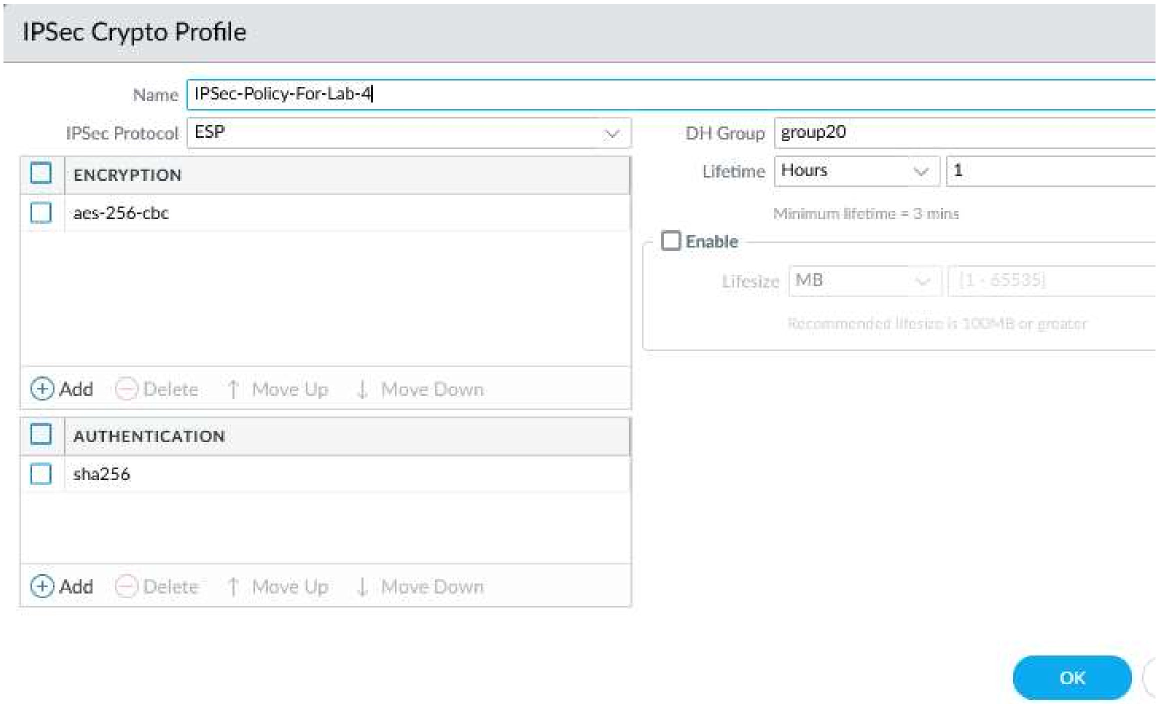
☐ Enable Fragmentation

☑ Dead Peer Detection

Interval: 5

Retry: 5

5: Under Advanced options, set your IKE Crypto Profile to the profile you created. Both firewalls should have the profile.



IPSec Crypto Profile

Name: IPSec-Policy-For-Lab-4

IPSec Protocol: ESP

DH Group: group20

Lifetime: Hours 1

Minimum lifetime = 3 mins

☐ Enable

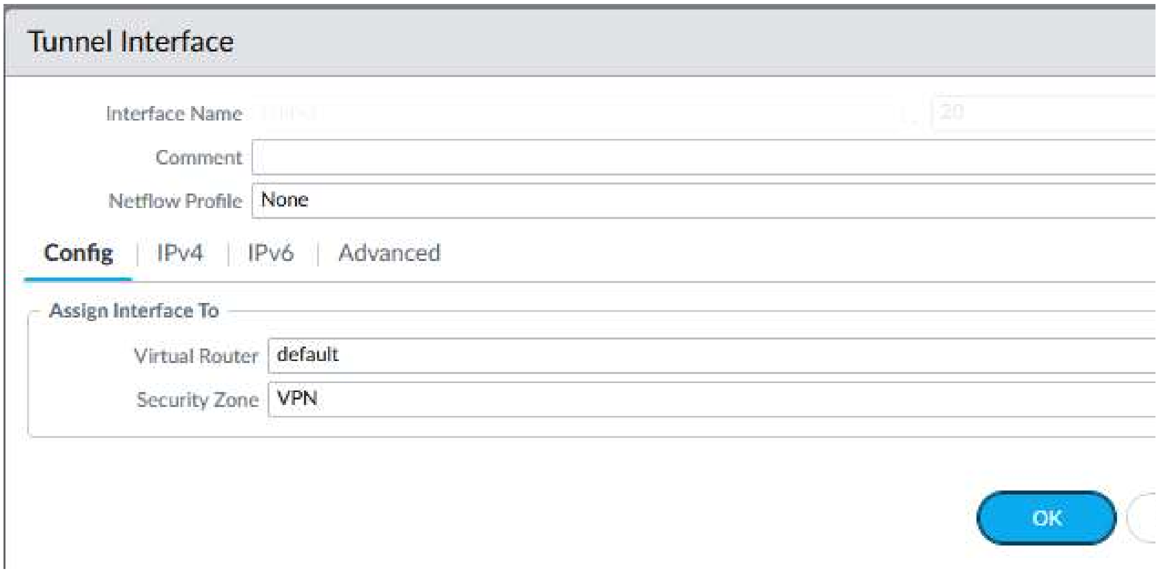
Lifesize: MB [1 - 65535]

Recommended lifesize is 100MB or greater

☐	ENCRYPTION
☐	aes-256-cbc

☐	AUTHENTICATION
☐	sha256

6: Create an IPSec Crypto Profile under Network > IPSec Crypto. Enter a name and select the IPSec Protocol to be ESP


Tunnel Interface

Interface Name

Comment

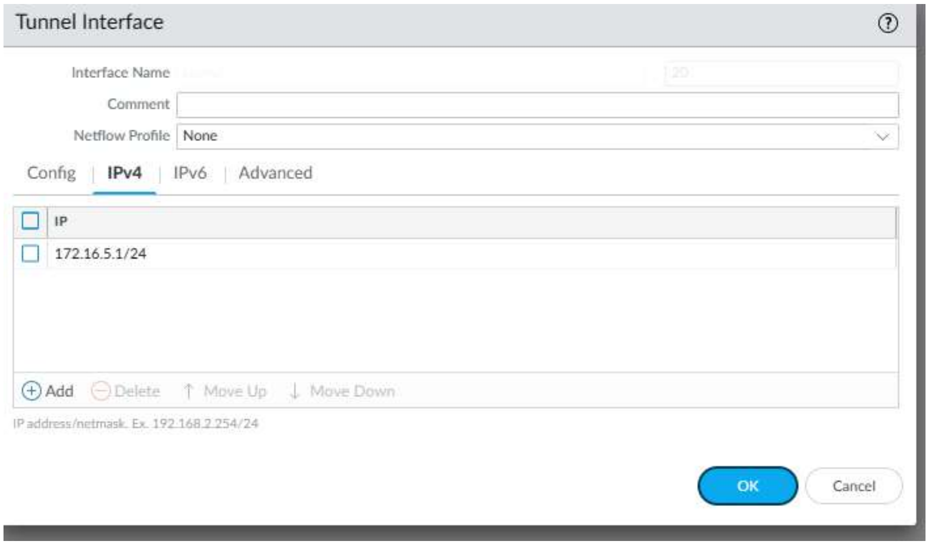
Netflow Profile: None

Assign Interface To

Virtual Router: default

Security Zone: VPN

7: Create a new Tunnel interface and set the virtual router and security zone as shown above.


Tunnel Interface

Interface Name

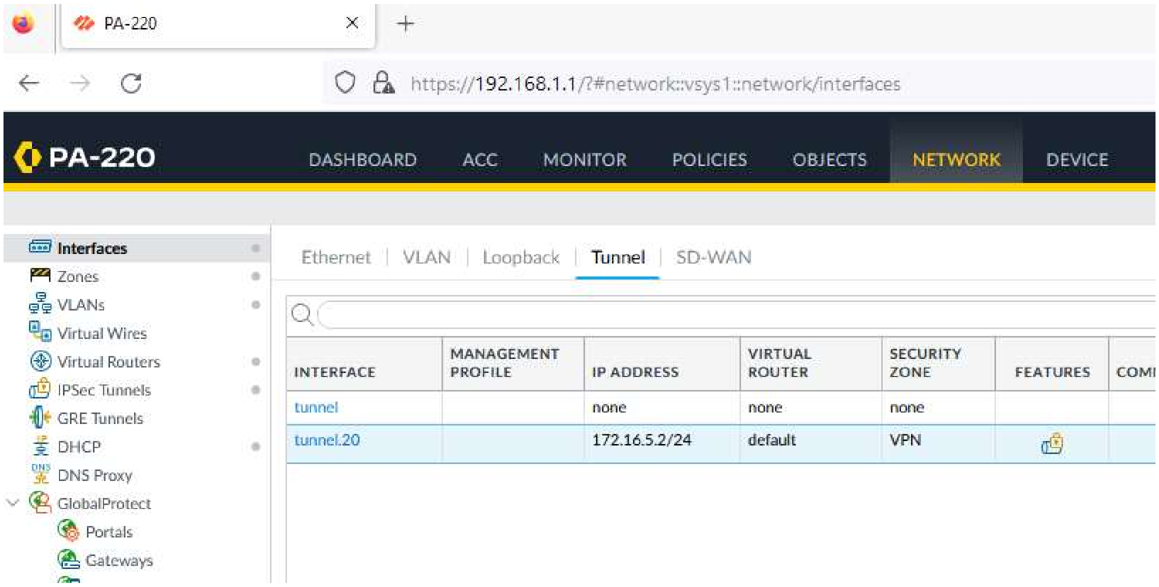
Comment

Netflow Profile: None

□	IP
□	172.16.5.1/24

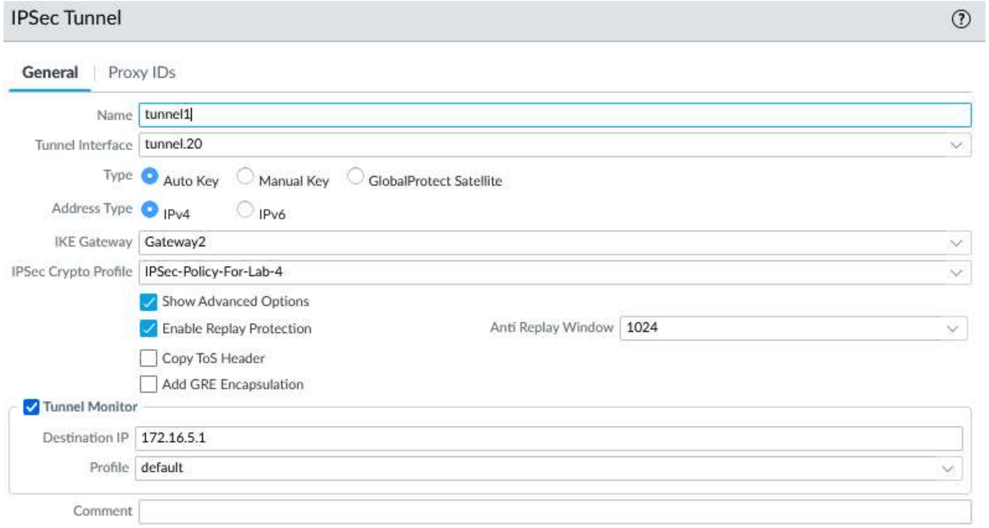
IP address/netmask. Ex. 192.168.2.254/24

8: Create a private IP address for the tunnel. This should not be a public IP nor the IP address of your current network.



INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMI
tunnel		none	none	none		
tunnel.20		172.16.5.2/24	default	VPN		

9: You now have a tunnel.20 interface



Name: tunnel1|

Tunnel Interface: tunnel.20

Type: ● Auto Key ○ Manual Key ○ GlobalProtect Satellite

Address Type: ● IPv4 ○ IPv6

IKE Gateway: Gateway2

IPSec Crypto Profile: IPSec-Policy-For-Lab-4

☑ Show Advanced Options

☑ Enable Replay Protection   Anti Replay Window: 1024

□ Copy ToS Header

□ Add GRE Encapsulation

☑ Tunnel Monitor

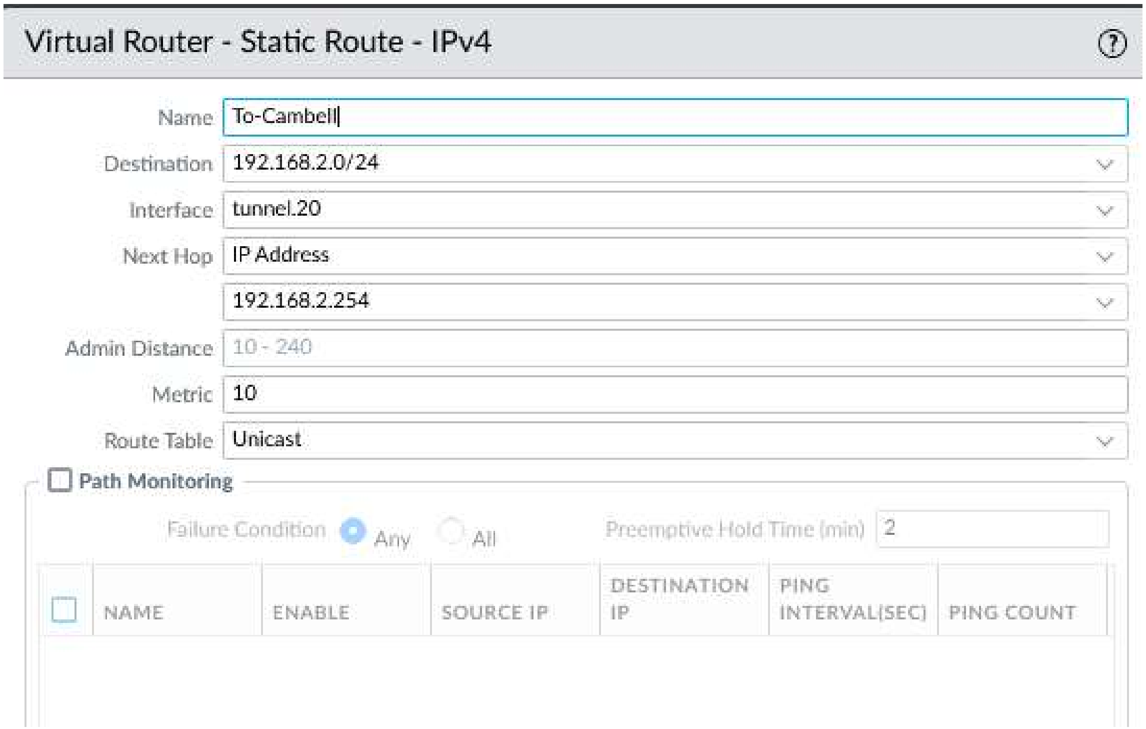
Destination IP: 172.16.5.1

Profile: default

Comment:

10: Under Network > interfaces > IPsec Tunnel, create a new tunnel and name it.

Select your Tunnel interface to the interface you just created
Set the Address type to IPv4
Select your IKE Gateway to the one previously created
Select your IPSec Crypto profile
Enable replay protection
Enable Tunnel Monitoring and set the destination IP as an address in your VPN network



Virtual Router - Static Route - IPv4

Name: To-Cambell
Destination: 192.168.2.0/24
Interface: tunnel.20
Next Hop: IP Address
192.168.2.254
Admin Distance: 10 - 240
Metric: 10
Route Table: Unicast

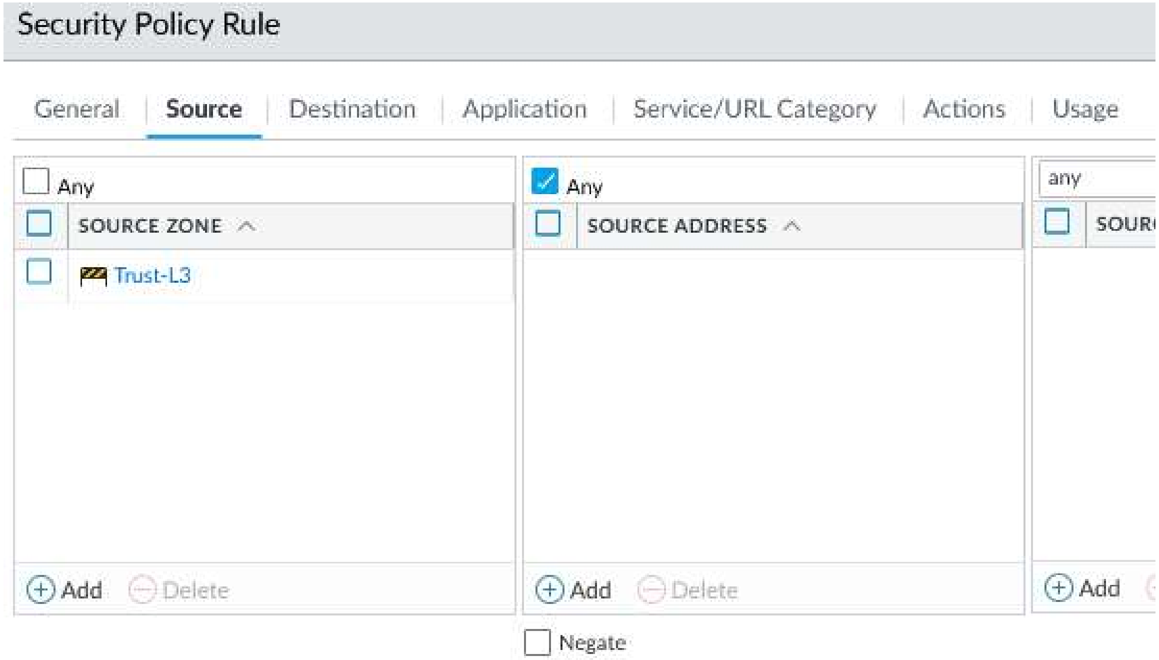
□ Path Monitoring

Failure Condition ● Any ○ All
Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

11: Enter Network > Virtual Router and add your tunnel interface into the Virtual router. Enter static routes and add a static route to the destination private network and select the next hop address.

12: Enter Policies > Security, these are all your current policies, create new policies by clicking Add.



Security Policy Rule

□ Any

□	SOURCE ZONE
□	Trust-L3

☑ Any

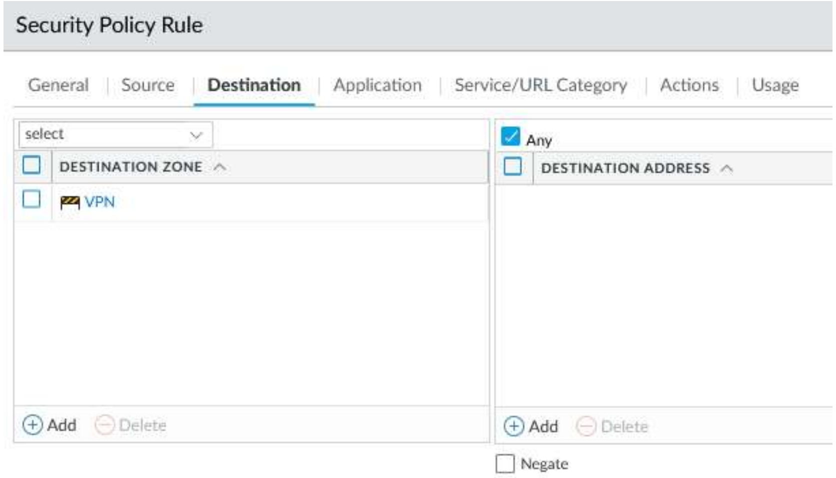
□	SOURCE ADDRESS

□ Negate

any

□	SOUR

13: Name the the policy “ToTunnel” with the source of Trust-L3



Security Policy Rule

select

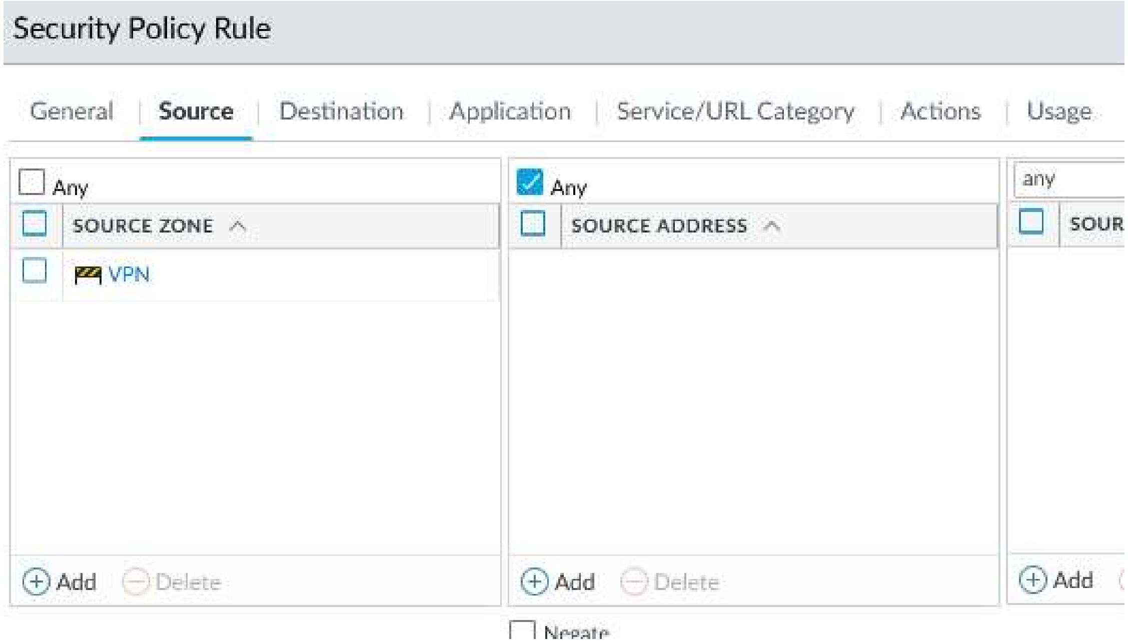
□	DESTINATION ZONE
□	VPN

☑ Any

□	DESTINATION ADDRESS

□ Negate

14: In the destination tab, select your VPN zone.



Security Policy Rule

☐ Any

☐	SOURCE ZONE
☐	VPN

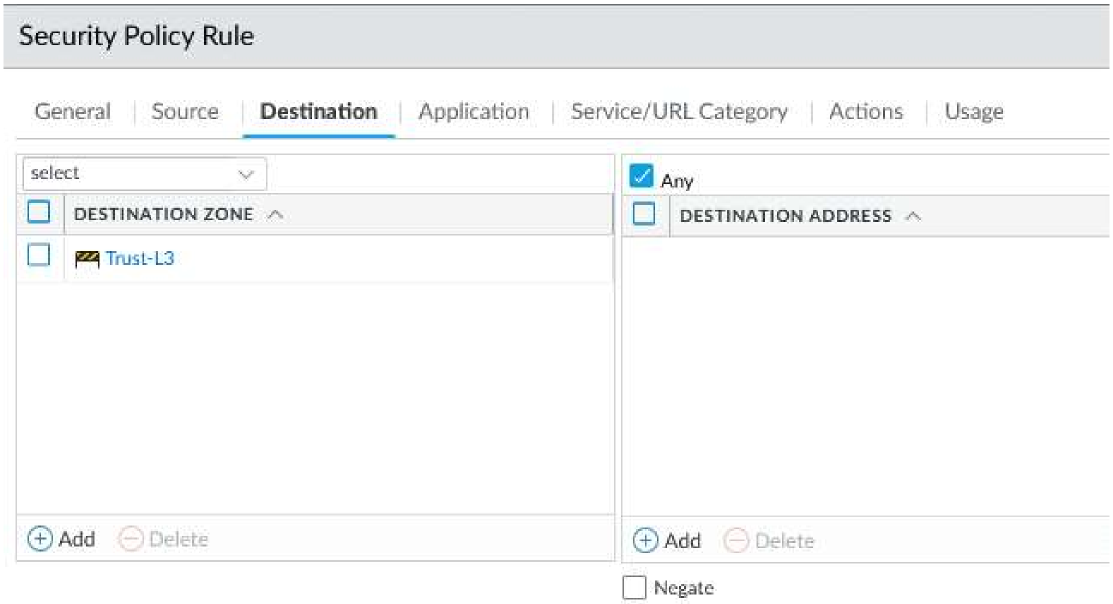
☑ Any

☐	SOURCE ADDRESS

any

☐	SOUR

15: Create a “FromTunnel” policy with a source set as your VPN zone



Security Policy Rule

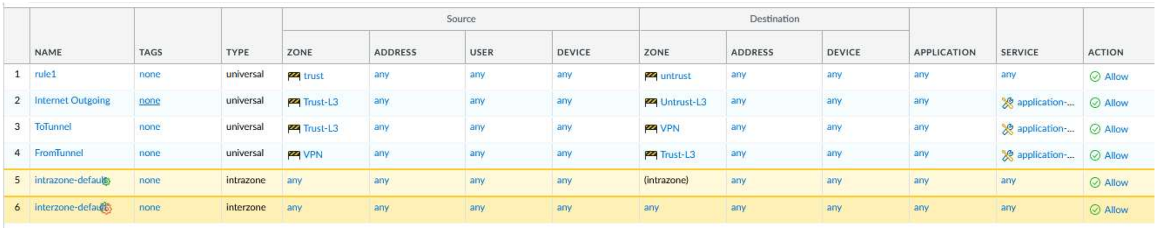
select

☐	DESTINATION ZONE
☐	Trust-L3

☑ Any

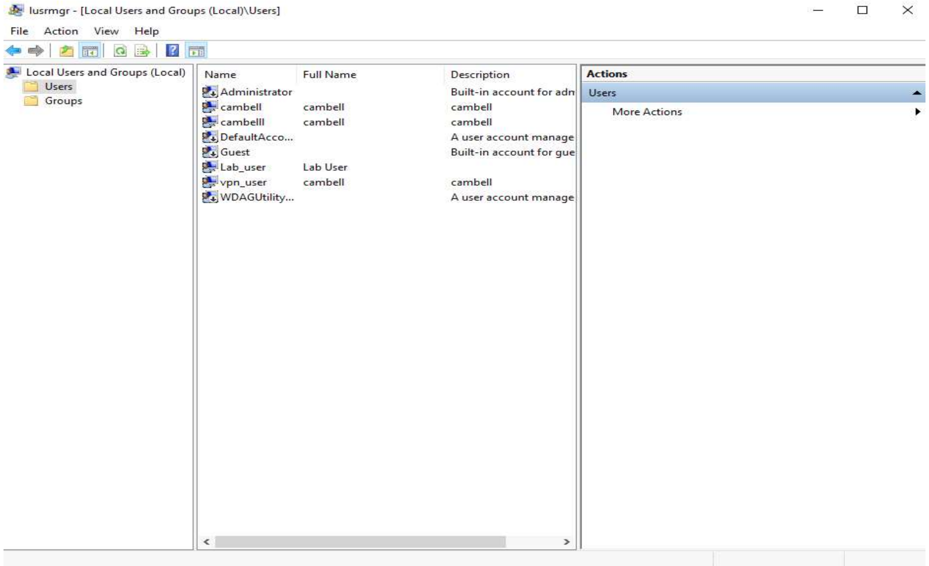
☐	DESTINATION ADDRESS

16: Set your Destination to Trust-L3



				Source				Destination					
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
1	rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow
2	Internet Outgoing	none	universal	Trust-L3	any	any	any	Untrust-L3	any	any	any	application-...	Allow
3	ToTunnel	none	universal	Trust-L3	any	any	any	VPN	any	any	any	application-...	Allow
4	FromTunnel	none	universal	VPN	any	any	any	Trust-L3	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	Allow

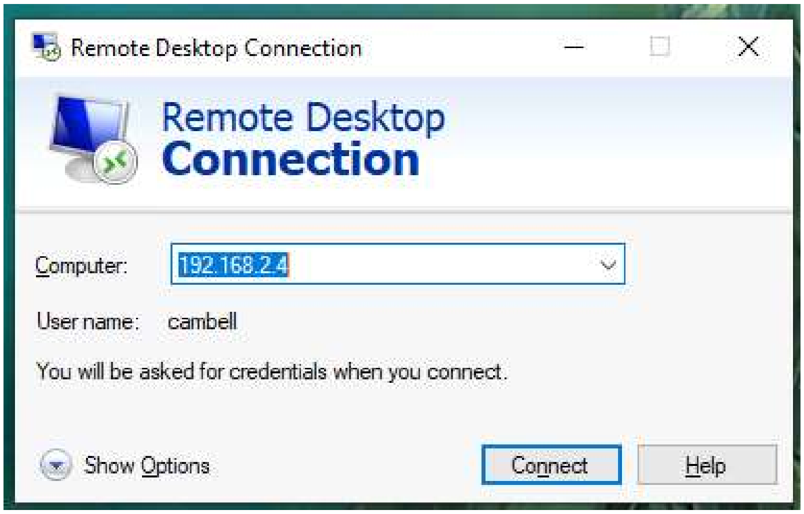
17: Your Security Polices should now looks something like this.



lusrmgr - [Local Users and Groups (Local)\Users]

Name	Full Name	Description
Administrator		Built-in account for adn
cambell	cambell	cambell
cambelll	cambell	cambell
DefaultAcco...		A user account manage
Guest		Built-in account for gue
Lab_user	Lab User	
vpn_user	cambell	cambell
WDAGUtility...		A user account manage

18. On both PCs, Enter lusrmgr.msc and set a username and password for your Remote Desktop Connection.

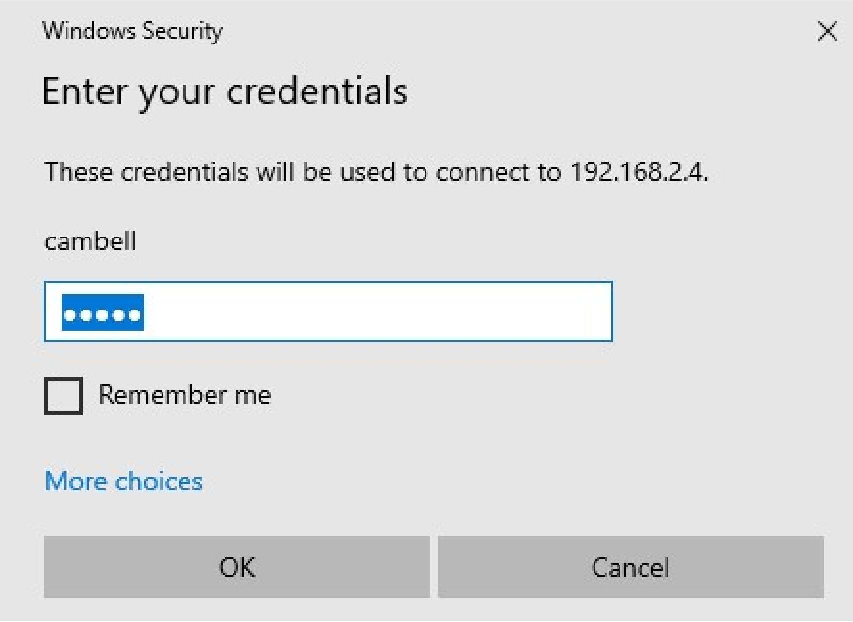


Computer: 192.168.2.4

User name: cambell

You will be asked for credentials when you connect.

19: From one endpoint device (PC), open remote desktop manager and enter the private IP address of the other endpoint device (PC).



Enter your credentials

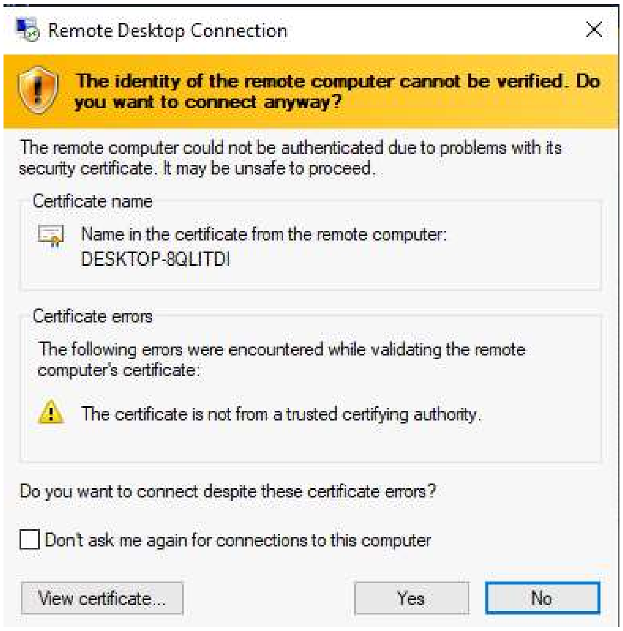
These credentials will be used to connect to 192.168.2.4.

cambell

●●●●●

□ Remember me

20: Enter your password.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
DESKTOP-8QLITDI

Certificate errors

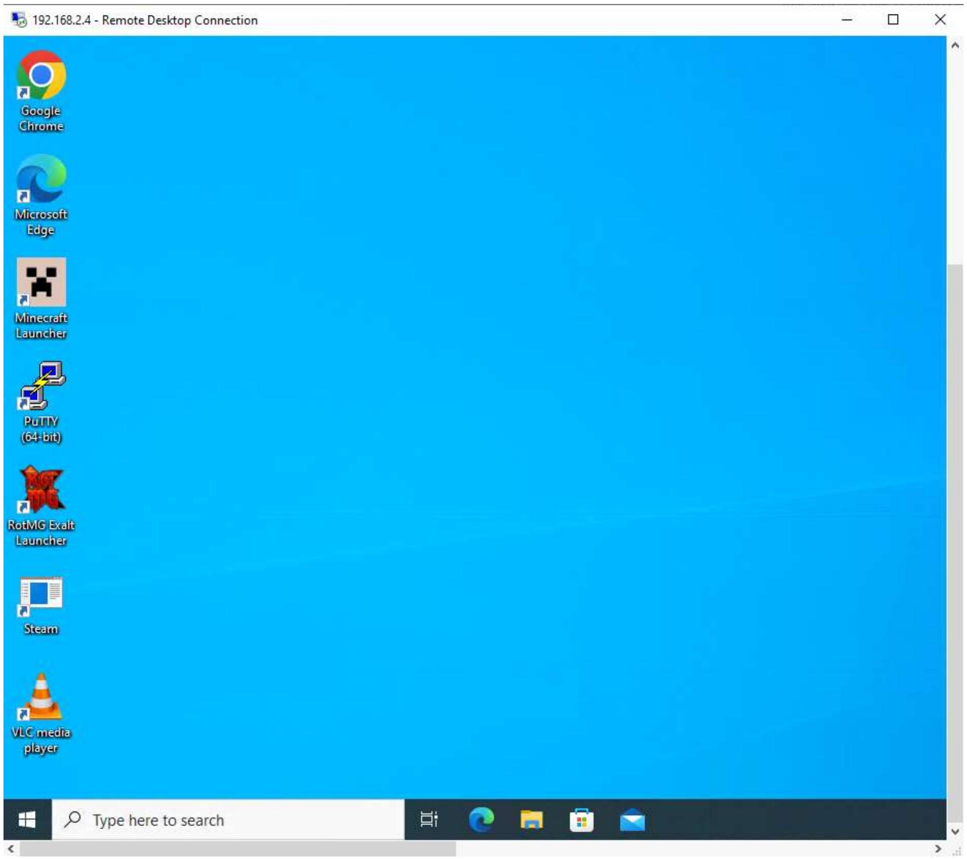
The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

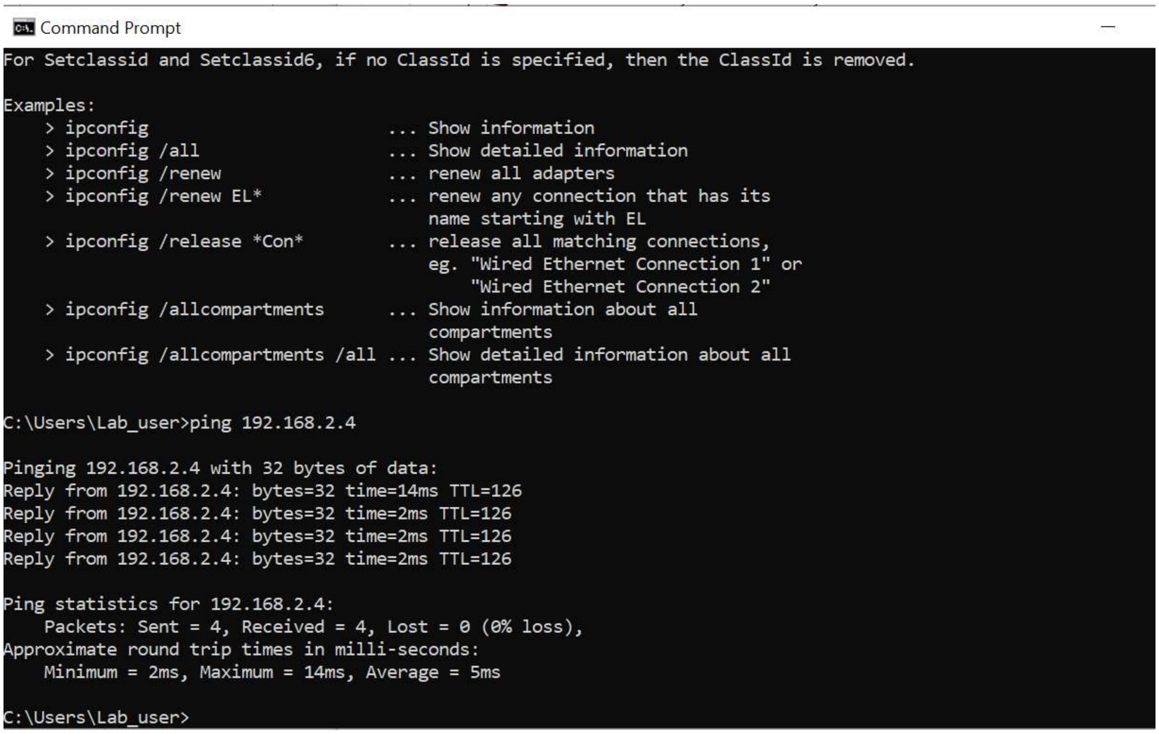
Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

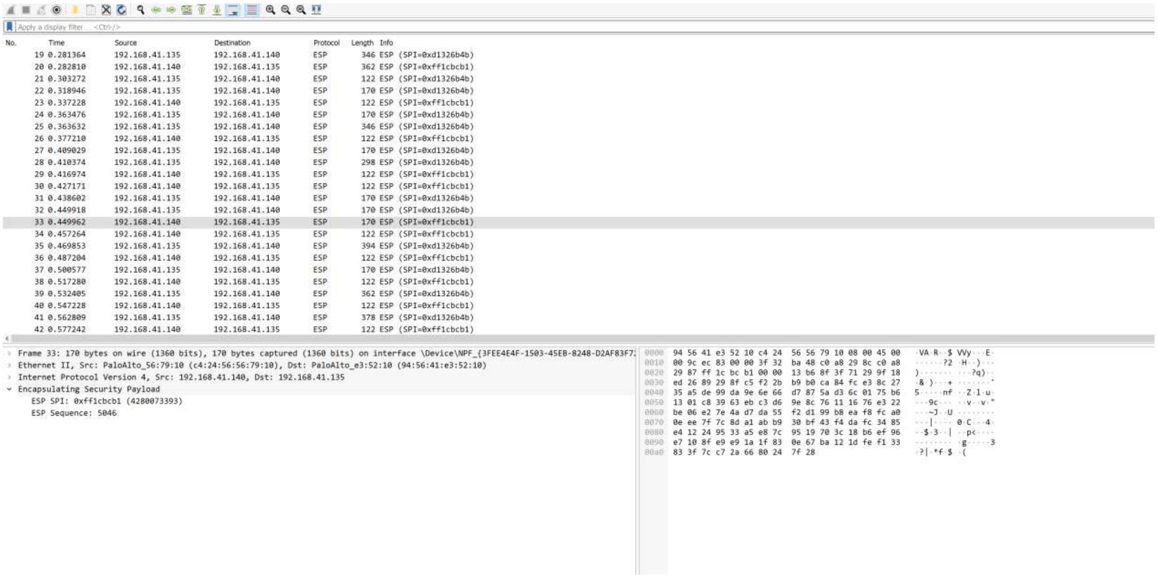
19: A prompt will appear on the computer that is being remote connected to. Click Yes.



You now are remotely connected to the other PC though your VPN.



```
For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                       ... Show information
    > ipconfig /all                  ... Show detailed information
    > ipconfig /renew                ... renew all adapters
    > ipconfig /renew EL*            ... renew any connection that has its
                                         name starting with EL
    > ipconfig /release *Con*        ... release all matching connections,
                                         eg. "Wired Ethernet Connection 1" or
                                             "Wired Ethernet Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                         compartments

C:\Users\Lab_user>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time=14ms TTL=126
Reply from 192.168.2.4: bytes=32 time=2ms TTL=126
Reply from 192.168.2.4: bytes=32 time=2ms TTL=126
Reply from 192.168.2.4: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\Users\Lab_user>
```



```
No.    Time        Source           Destination      Protocol  Length Info
    19 0.281364    192.168.41.135   192.168.41.140   ESP       346 ESP (SPI=0xd1326b4b)
    20 0.282810    192.168.41.140   192.168.41.135   ESP       362 ESP (SPI=0xff1cbcb1)
    21 0.303272    192.168.41.135   192.168.41.140   ESP       122 ESP (SPI=0xd1326b4b)
    22 0.318946    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    23 0.337228    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    24 0.363476    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    25 0.363632    192.168.41.135   192.168.41.140   ESP       346 ESP (SPI=0xd1326b4b)
    26 0.377210    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    27 0.409029    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    28 0.410374    192.168.41.135   192.168.41.140   ESP       298 ESP (SPI=0xd1326b4b)
    29 0.416974    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    30 0.427171    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    31 0.438602    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    32 0.449918    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    33 0.449962    192.168.41.140   192.168.41.135   ESP       170 ESP (SPI=0xff1cbcb1)
    34 0.457264    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    35 0.469853    192.168.41.135   192.168.41.140   ESP       394 ESP (SPI=0xd1326b4b)
    36 0.487204    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    37 0.500577    192.168.41.135   192.168.41.140   ESP       170 ESP (SPI=0xd1326b4b)
    38 0.517280    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    39 0.532405    192.168.41.135   192.168.41.140   ESP       362 ESP (SPI=0xd1326b4b)
    40 0.547228    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
    41 0.562809    192.168.41.135   192.168.41.140   ESP       378 ESP (SPI=0xd1326b4b)
    42 0.577242    192.168.41.140   192.168.41.135   ESP       122 ESP (SPI=0xff1cbcb1)
```

```
> Frame 33: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface \Device\NPF_{3FEE4E4F-1503-45EB-8248-D2AF83F7
> Ethernet II, Src: PaloAlto_56:79:10 (c4:24:56:56:79:10), Dst: PaloAlto_e3:52:10 (94:56:41:e3:52:10)
> Internet Protocol Version 4, Src: 192.168.41.140, Dst: 192.168.41.135
v Encapsulating Security Payload
     ESP SPI: 0xff1cbcb1 (4280073393)
     ESP Sequence: 5046
```

```
0000  94 56 41 e3 52 10 c4 24  56 56 79 10 08 00 45 00   ·VA·R··$ VVy···E·
0010  00 9c ec 83 00 00 3f 32  ba 48 c0 a8 29 8c c0 a8   ······?2 ·H··)···
0020  29 87 ff 1c bc b1 00 00  13 b6 8f 3f 71 29 9f 18   )······· ···?q)··
0030  ed 26 89 29 8f c5 f2 2b  b9 b0 ca 84 fc e3 8c 27   ·&·)···+ ·······'
0040  35 a5 de 99 da 9e 6e 66  d7 87 5a d3 6c 01 75 b6   5·····nf ··Z·l·u·
0050  13 01 c8 39 63 eb c3 d6  9e 8c 76 11 16 76 e3 22   ···9c··· ··v··v·"
0060  be 06 e2 7e 4a d7 da 55  f2 d1 99 b8 ea f8 fc a0   ···~J··U ········
0070  0e ee 7f 7c 8d a1 ab b9  30 bf 43 f4 da fc 34 85   ···|···· 0·C···4·
0080  e4 12 24 95 33 a5 e8 7c  95 19 70 3c 18 b6 ef 96   ··$·3··| ··p<····
0090  e7 10 8f e9 e9 1a 1f 83  0e 67 ba 12 1d fe f1 33   ········ ·g·····3
00a0  83 3f 7c c7 2a 66 80 24  7f 28                     ·?|·*f·$ ·(
```

Issues:

We faced problems getting our VPN tunnel working in order to remote desktop over the tunnel. But these mainly boiled down to two main issues, inexperience with site-to-site IPSec and miscommunication between our groups.

The first issue we had was that both firewalls were not configured in the same way leading to the inability to establish a tunnel. I would consider this problem under miscommunication because since many of the configurations have to be the same in order for the VPN to work, us not communicating properly the configurations set on our firewalls lead to weeks of confusion of what we did wrong.

The second issue we faced was that we didn't create a VPN zone on the firewalls. The VPN zone is vital because it where traffic routed across the VPN travels and is used to isolate the traffic in VPN tunnel from other traffic within the network. This issue was due to inexperience with firewalls and VPNs leading us to have to use online guides that aren't always the most reliable or are hard to understand. We were able to identify this issue eventually and fix it after a mix of online research and talking to peers.

Conclusion:

While you can make site-to-site VPNs on my types of devices, we used PA-220s because Palo Alto firewalls are widely used within the networks of large corporations. This lab then not only emphasizes the use of site-to-site VPNs, IPSec, and IKE but also familiarizes us with the use firewalls from Palo Alto. Our next lab will be about Fortinet firewalls which are more popular among medium and small businesses.