===;

Brit Stevens 11/27/23

IPsec Tunneling

Site to Site

**Purpose:**

The purpose of this lab was to better understand the uses of the PA-220 and how to configure IPsec tunnels, a type of tunnel to protect your data from being viewed my packet sniffer. We also learned the different configurations of the tunnel either pushing all information through the tunnel or said information meant for the other firewall.

**Background Information on lab concepts:**

There is a feature called IPsec tunneling on the PA-220 that encrypts data to make it secure over public networks through a virtual tunnel using IP addresses. IPsec tunneling is one of the modes of another protocol called IPsec VPN. IPsec differs from IPsec Transport with an encapsulated IP header. To set up this tunnel you need to establish a tunnel that is encrypted and secured with your other firewall or network then negotiate keys and parameters for the IPsec tunnel. A key is a password or code that is known by both end devices connected to the tunnel that is used to decrypt the data once received. This key can only be used by those firewalls to decrypt the data and not anyone else on the internet who may be snooping to receive packets. The negotiations have a phase one and phase two. Phase one’s purpose is to establish the tunnel connection. Once complete phase two begins to negotiate the keys and parameters to make sure everything matches between the firewalls. The tunnel will be up after phase two completes but you may need to configure a policy rule that allows traffic from the other firewall enter the destination zone (range of IPs on the internal network of the firewall) and vice versa. IPsec Protocol has five main procedures: Interesting Traffic or On-Demand, IKE Phase 1, IKE Phase 2, IPsec Data Transfer, and IPsec Tunnel Session Termination.

**Interesting Traffic or On-Demand:**

The traffic that the policy rules deem as interesting are IPs allowed through the tunnel. When that policy sees an IP trying to go out in that specified range it will go through the tunnel towards the end of the tunnel. The tunnel only goes up when there is interesting traffic is destined for the tunnel.

It also adds authentication to the data with a stamp telling the receiver who sent the data. This ensures it is not a fraudulent packet and is from a trusted source.

**IKE Phase one:**

IKE stands for Internet Key Exchange and is the key management protocol standard with IPsec. IKE authenticates each peer in an IPsec session and exchanges their keys if authentication is successful.

**IKE Phase two:**

IKE negotiates the stricter IPsec SA (security associations) parameters between the peers.

**IPsec Data Transfer:**

The interesting or on-demand data is transferred to the IPsec peer. The interesting packets and encrypted on one end of the tunnel then decrypted by the peer using what parameters specified in IKE phase 2.

**IPsec Tunnel Sessions Termination:**

Once the traffic ends or the timeout listed in the PA parameters the IPsec tunnel is terminated and the keys are discarded. The timeout can either be a set number of bytes or number of seconds. Once this happens IKE phase two will need to occur again and possibly phase one. If you need to the PA parameters can be changed while the tunnel is up without interruption to data.

An example of an IPsec site to site VPN could be a host on the internal network on one firewall sends a packet out. Once the packet reaches the end of its internal network and the packet matches the IP address range specified IPsec in the PA parameters then it is recognized as an interesting IP. This causes the tunnel to come up and after the tunnel connection is secured the packet is encrypted and sent through the tunnel. Once it is received by the other end of the tunnel, it is decrypted and sent to its internal network.

Some elements that need configuration to bring an IPsec tunnel up are IKE gateway, IKE crypto and IPsec crypto.

**IKE gateway:**

The parameters configured here enable the Site-to-Site connection between the firewalls. These parameters are what establish the phase one connection of the IKE. You must enter the IP address of the port facing the internet of the firewall you are trying to tunnel with. You also enter the interface your tunnel will be covering and the PSK (pre-shared key, kind of like a password between the tunnel endpoints). You must select the version of IKE as well. All these parameters must match to begin IKE negotiation.

**IKE crypto:**

IKE crypto is a profile that is used to set up the encryption and authentication algorithms used for the key exchange process in Phase one of the IKE process. You attach this profile to the IKE gateway and is a part of the parameters that must match. The parameters in the IKE crypto are the encryption and authentication algorithms and the DH groups (Diffie-Hellman groups, they determine the strength of the key used in the key exchange process. They are split into two different group types: MODP which are non-random bits and ECP which are random bits. Within a group type the higher group number is more secure).

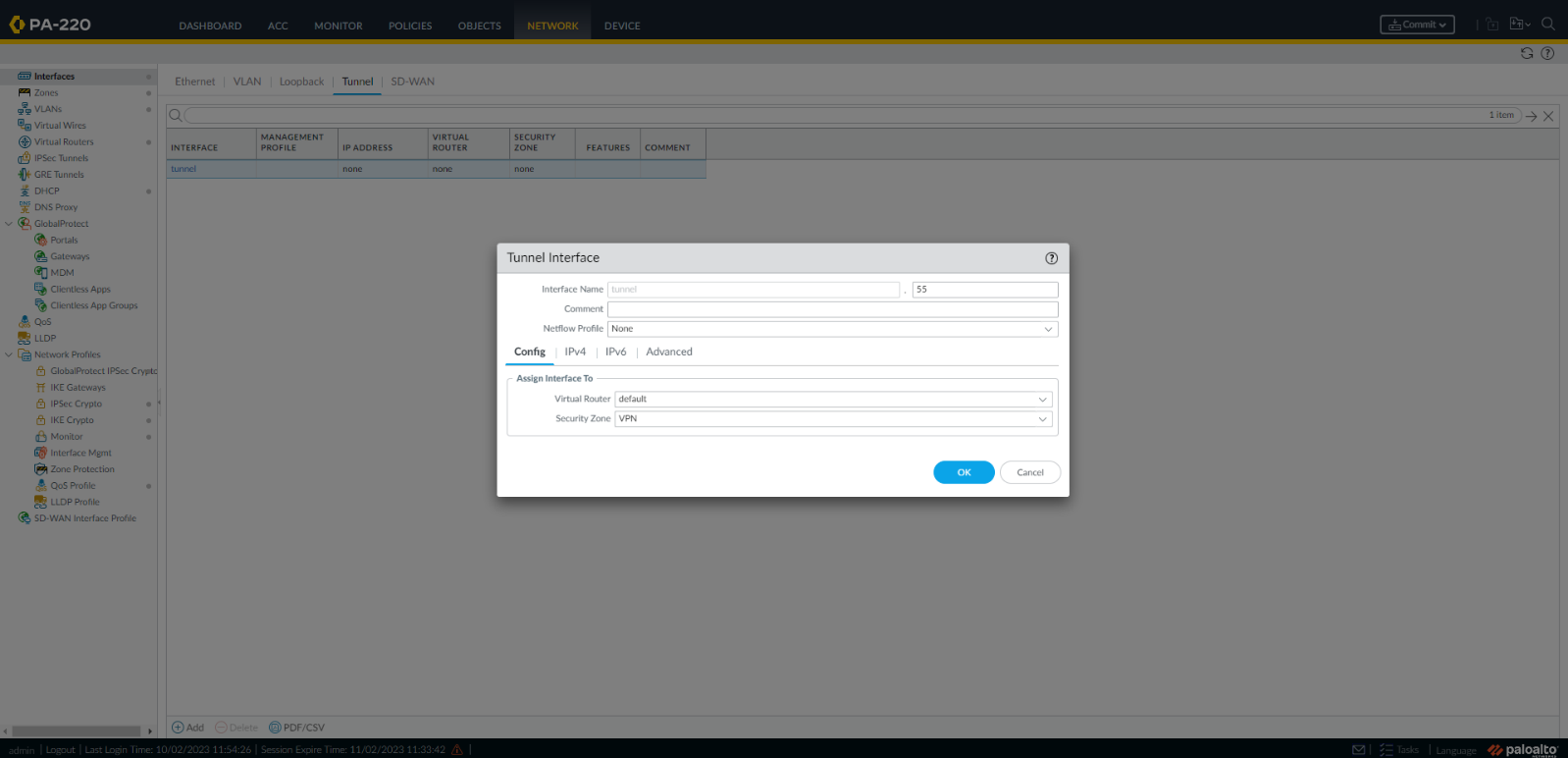
Authentication Algorithms: there are many different authentication algorithms like sha512 and md5. Sha functions by transforming data into hashes that cannot be undone to get the plain text without the PSK between the end devices. Hackers do have methods to decrypt the hashing which is why having a greater encryption is important. Sha has different versions with each higher number having more bits per word in the hashing process making the data harder to decrypt. Md5 works similar to sha but is limited at 128-bit hashing. It is recommended to use sha over md5 because it more secure and harder to break the encryption although md5 is faster, so it is used in safe environments occasionally. These are authentication because the only device that can decrypt the data easily is the device that has the other PSK.

Encryption Algorithms: Some encryption algorithms for the PA-220 are different versions of AES and DES. AES, Advanced Encryption Standard, is a symmetric block cipher meaning that it encrypts data in blocks of 128 bits at a time. It does this by transferring the plain text data into different values like turning a ‘u’ into e4 (not a real example) based off the cryptographic key that is shared between devices in the IKE connection. The length of the key is determined by the version of AES used with the higher version being more bits than previous versions. This new text is called ciphertext. After rewriting the data like this it is then shuffled around many different rounds depending on the version of AES to make the data essentially impossible to decrypt without the key. There are two different types of AES with AES-CDC and AES-GCM. GCM is has greater data confidentiality and data integrity making it more secure and optimal over CDC. DES is the first version of AES and is now outdated and very unsecure. It uses the same key to decrypt and encrypt messages making it vulnerable to brute force attacks guessing at the key.

**IPsec crypto:**

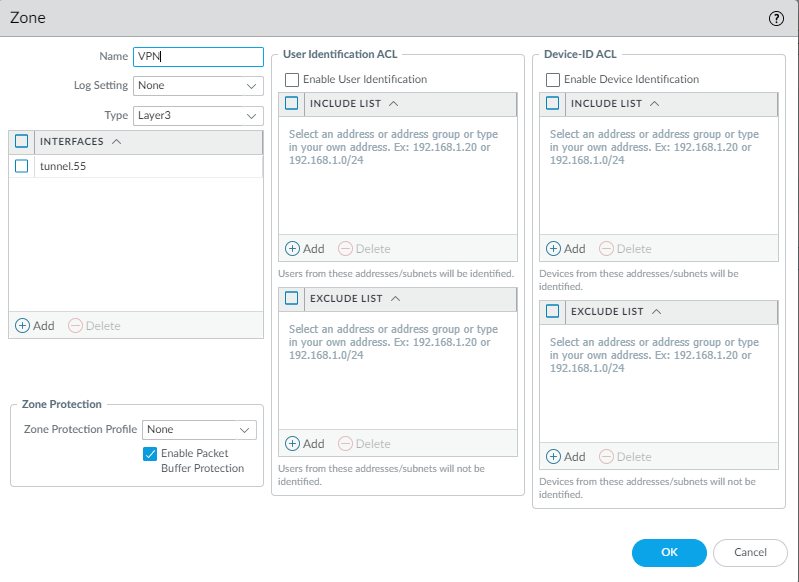
The IPsec crypto profile is invoked in IKE Phase 2 and specifies how data is secured within the IPsec tunnel. Just like IKE crypto all the parameters must match between both ends of the tunnels. You attach IPsec profile to the IPsec tunnel while configuring it. The parameters are IPsec protocol and the previous parameters explained in the IKE Crypto. IPsec protocol has two different modes, ESP and AH. IPsec ESP (Encapsulating Security Payload) provides data confidentiality (encryption), and authentication (data integrity, Data origin authentication, and Replay protection). ESP provides the data confidentiality using a PSK and the encryption algorithms mentioned previously. ESP provides authentication using the respective algorithms listed previously on the IP datagram (just the data not the header telling the packet where it needs to go). IPsec AH (Authentication Header) is authentication only and cannot provide encryption algorithms. It uses the same authentication algorithms as ESP except it authenticates the entire IP packet including the payload and outer IP header.

**Lab Summary:**



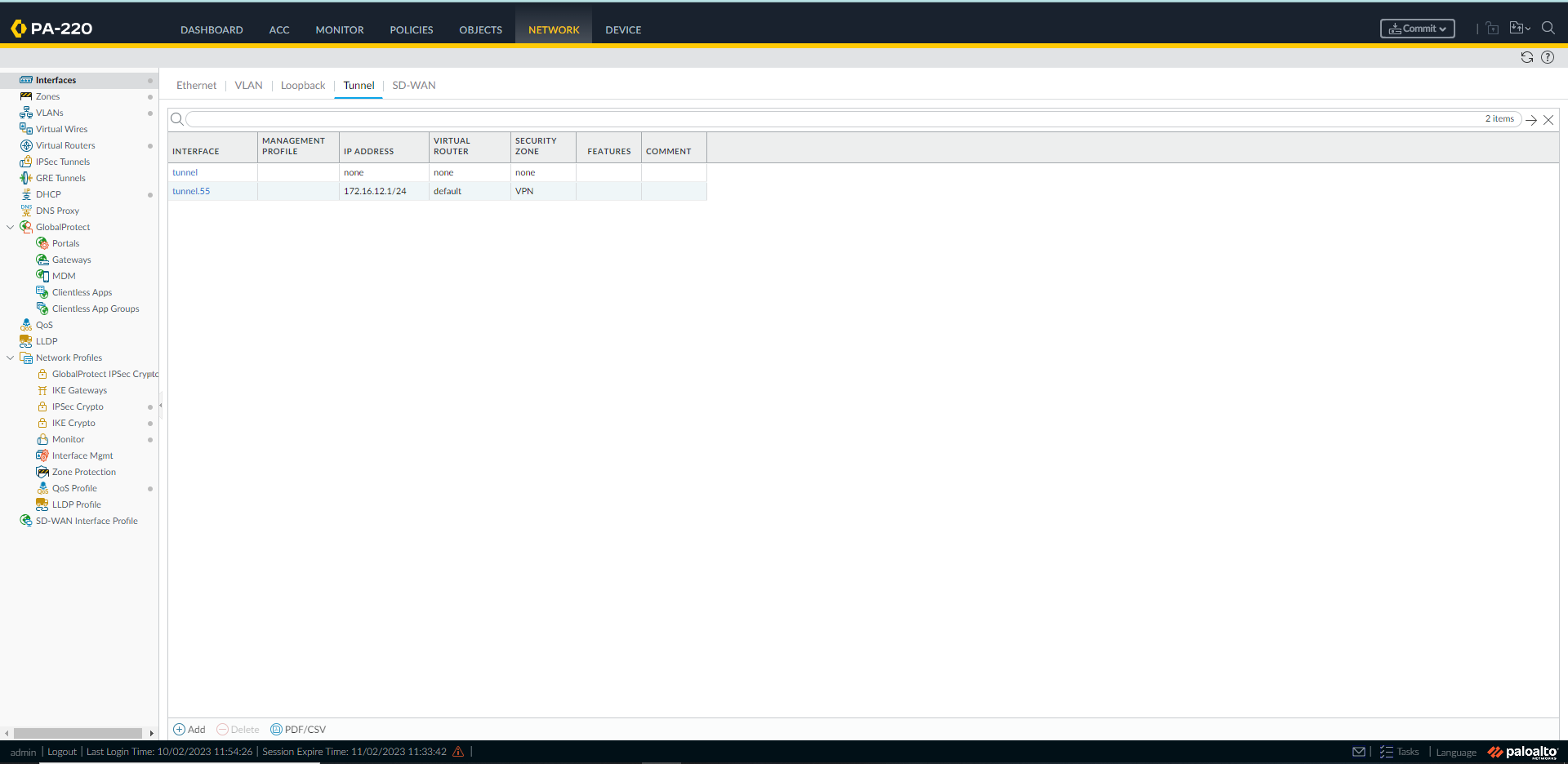
On FW-A under the networks tab go to interface. Once in interfaces go to tunnel and select add at the bottom of the page. For now, leave the security zone as none and select default for Virtual Router. Under IPv4 configured your desired IP, we used 172.17.12.1/24. This will be important later as you will need it to connect the other firewall tunnel interface.

Repeat this in FW-B with the address of 172.17.12.1/24.

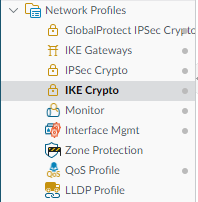
****

Under the networks tab click onto Zones. Once under zones select add to see a config box like above. Name the zone VPN with the type of Layer3. Add your previously configured tunnel interface to this zone. Go back to your tunnel interface now and apply the new security zone to the tunnel interfaces.

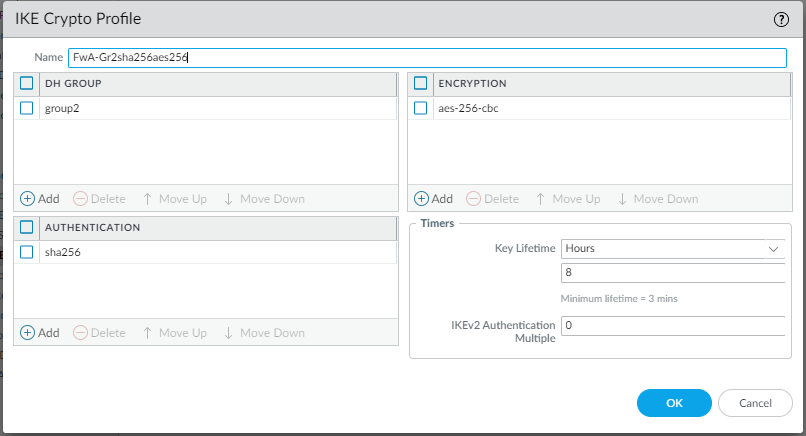
Repeat for FW-B.

****

Your interfaces should now look like this.

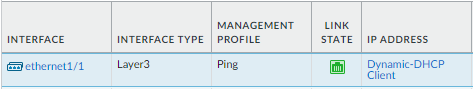


Still under network expand the network profiles and select IKE Crypto select add at the bottom.

****

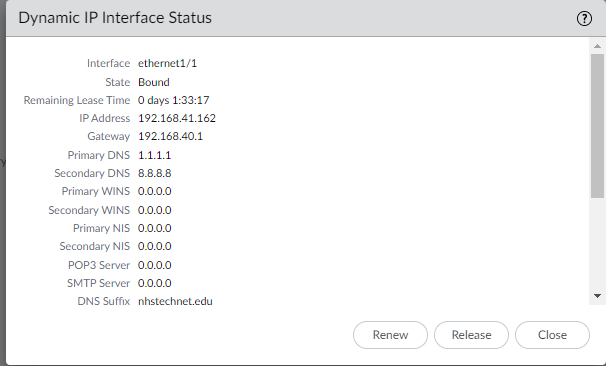
Now in the config box type in any name that you can remember. Select add DH GROUP and click group2. Select add ENCRYPTION and choose aes-256-cbc or other encryption methods. Select add AUTHENTIFICATION and select sha256. You can leave the timer as default.

Repeat for FW-B

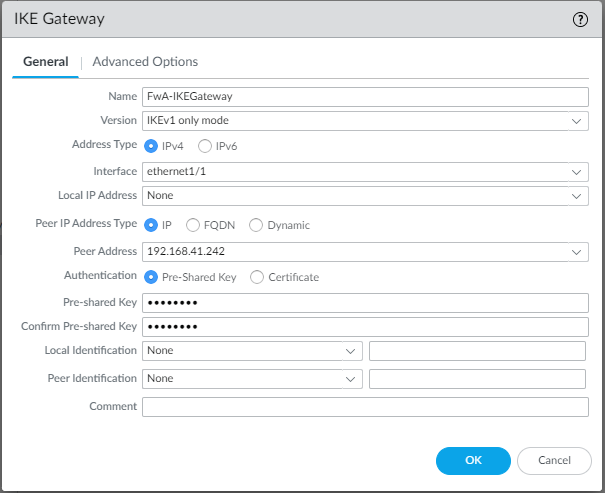
****

Go to interfaces and set ethernet 1/1 to DHCP client. This allows the interface to receive an ipv4 address from the DHCP server of the wan.

Repeat for FW-B

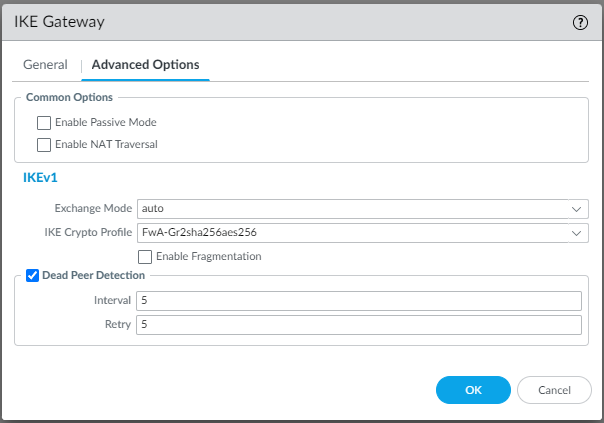
****

You should see this when you click on dynamic-DHCP Client.

****

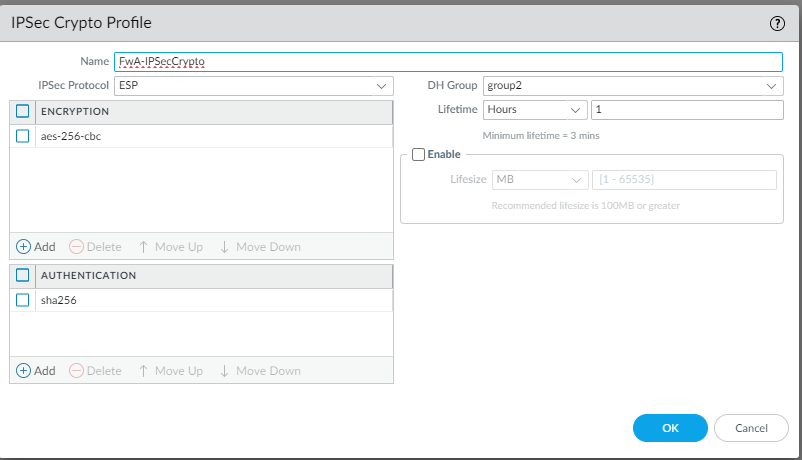
Now go to IKE Gateway under network and create new. Select IKEv1 only mode or any other option just make sure the Firewalls match. Select the interface connecting to the internet (ethernet1/1 for us). The local IP will be none because it given by the DHCP server. Set the peer IP to the IP address given by the DHCP server to the external interface on FW-B. Enter a Pre-shared key that will be the same on both firewalls.

Repeat on FW-B with the Peer address the address given to the external interface on FW-A.

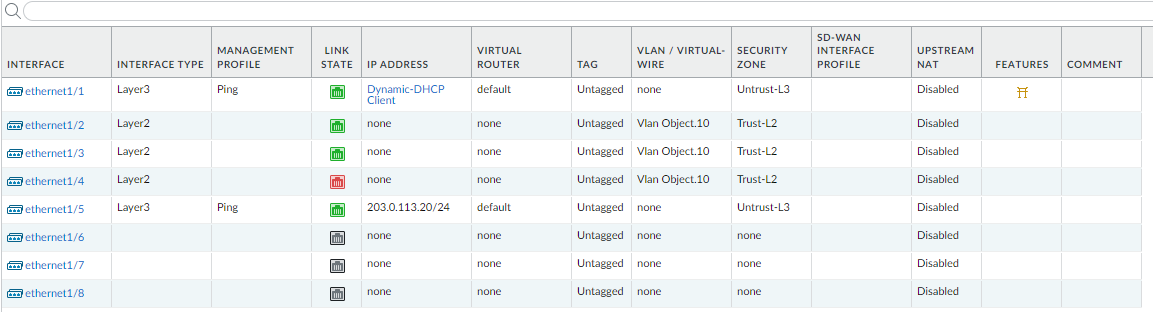
****

Under advanced options set the IKE Crypto Profile to the profile we configured in previous steps.

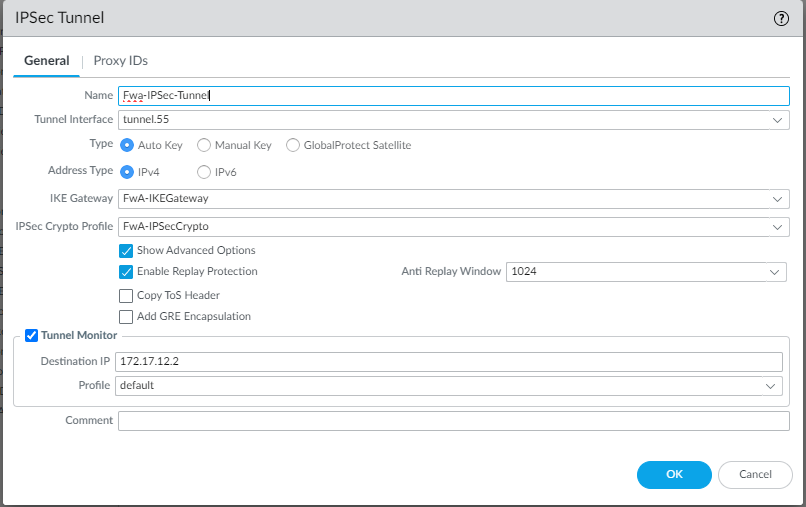
Repeat on FW-B

****

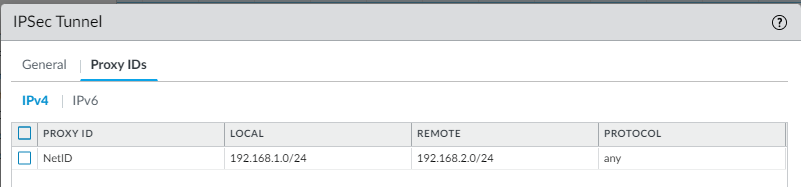
Go to IPsec Crypto and create a new profile. Select aes-256-cbc as encryption and sha256 as encryption. Put this profile in the DH group of group2. Repeat for FW-B

****

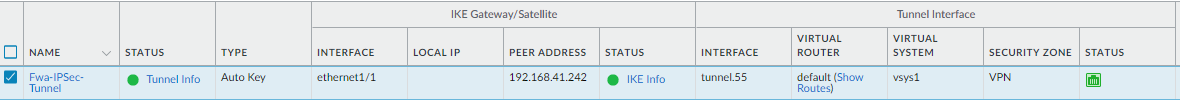
That symbol now shows that the IKE gateway is up.

****

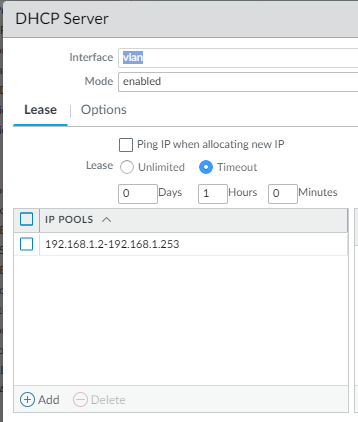
We can now configure the IPsec Tunnel. Set the tunnel interface as well as the IKE Gateway and IPsec Crypto Profile to the ones configured previously. Set the tunnel monitor to the IP of the tunnel on the other firewall.

****

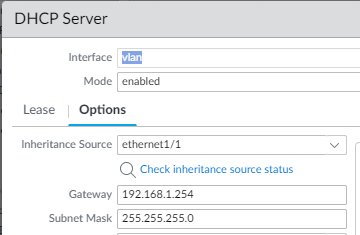
Set the local IP to the subnet of the local network in the firewall (IP on the internal DHCP pool).

****

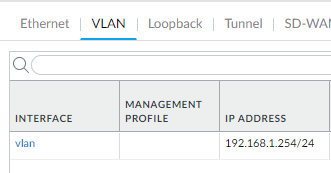
If the tunnel shows green that means it is now up and functional. If you cannot send data through it check your DHCP pool is configured correctly.

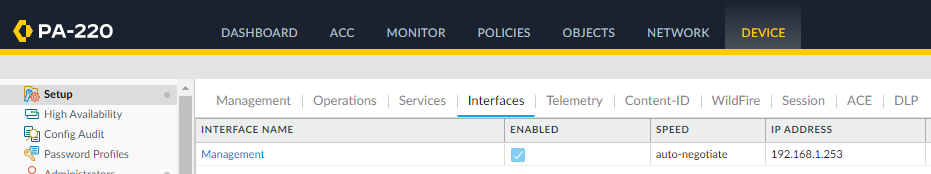
****

The range of the IPs should be in the range of the Vlan interface we configured during the soho configuration lab or vice versa.

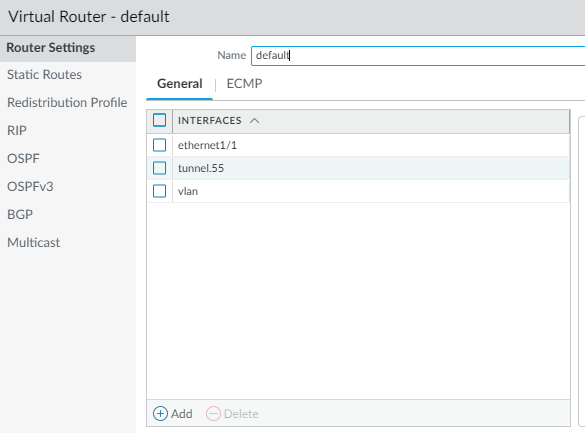
****

Configure the gateway of the DHCP server to be the Vlan interface IP address.

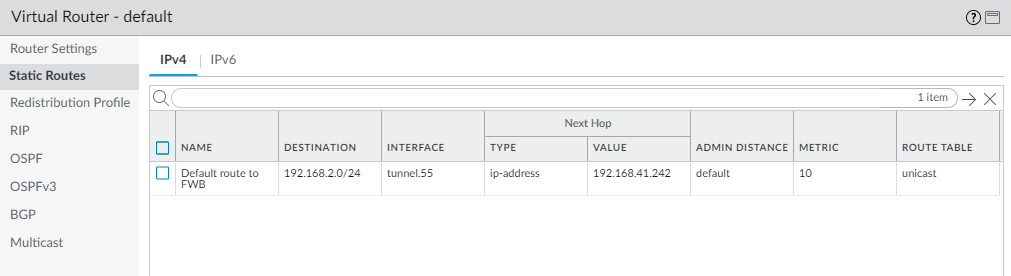
****

****

Once you have set up the DHCP pool and Vlan interface to be in the same subnet, click onto device and setup. In setup go to interfaces and select management. You must have the management interface in the same subnet as the dhcp pool so you can access the management port on your web browser. Once all subnets match commit changes.

****

As committing finishes go to network and virtual router. You should see settings like this.

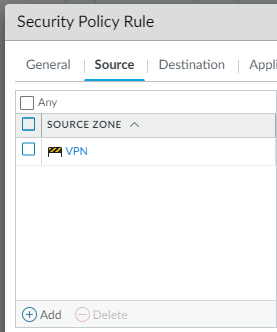
****

Click onto the static routes and add new. Set the destination to the address of the internal network of your other firewall and use your tunnel as the interface. Set the next hop address to the address of the external port of the other firewall. You can leave the AD, metric, and route table as default. This will tell your firewall to send any traffic destined for that internal network to go to the external port of the other firewall.

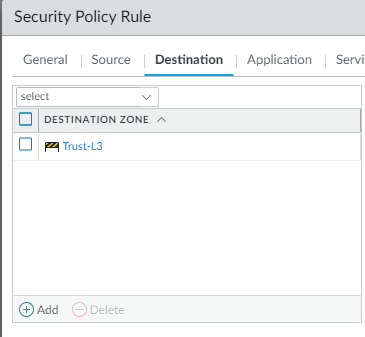
Repeat on Firewall B with the inside network of 192.168.1.0/24 and the next hop of the external port of FW-A

****

Under policies select security and add a new security policy.

****

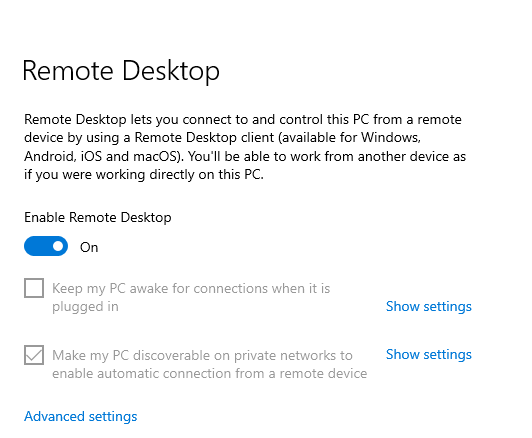
Select the source zone of VPN and destination as Trust-L3. This will let data going to from VPN go to your inside network. Create the policy with a name like VPN to TL3.

****

Do the inverse of that with data from Trust-L3 going to the VPN.

Repeat on FW-B

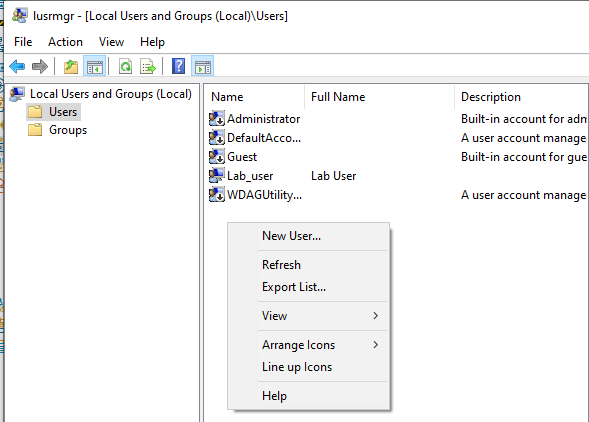
Your tunnel should now be up and functional.

****

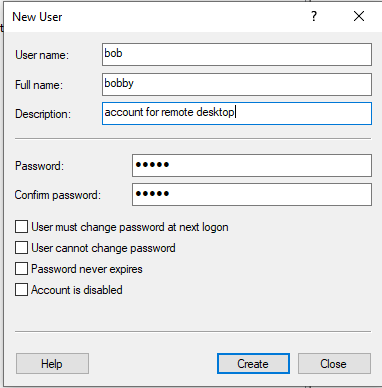
To test this search for remote desktop on your desktop and ensure it is enabled. If you are on a company or school computer, you may need to add a user to remote desktop with the following steps.

****

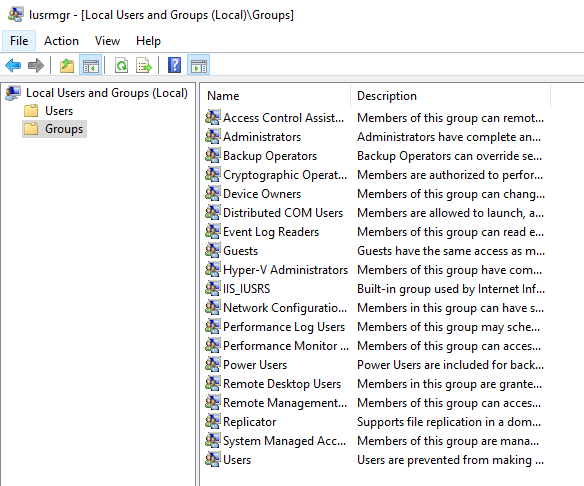
Search lusrmgr.msc and click enter

****

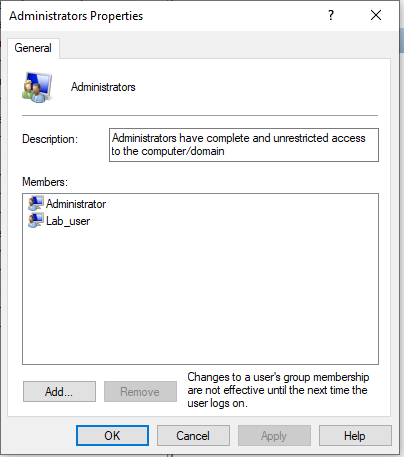
This will bring you to the Local users and groups page where you can make an administrator user. Click onto the users folder and right click the blank space to select new user.

****

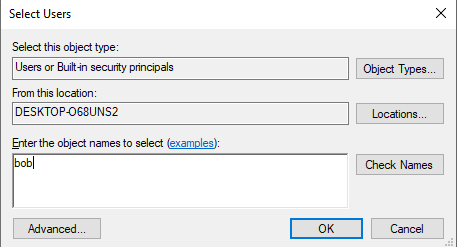
The user can be any name or password just remember what you choose. Do the same thing on a desktop in the other inside network with a different username.

****

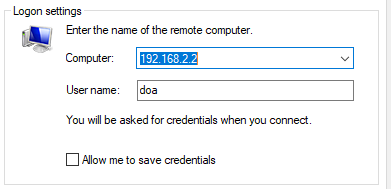
Now that you have made the user, you have to admin it. Select groups and find administrators. Double click on it to open a config box.

****

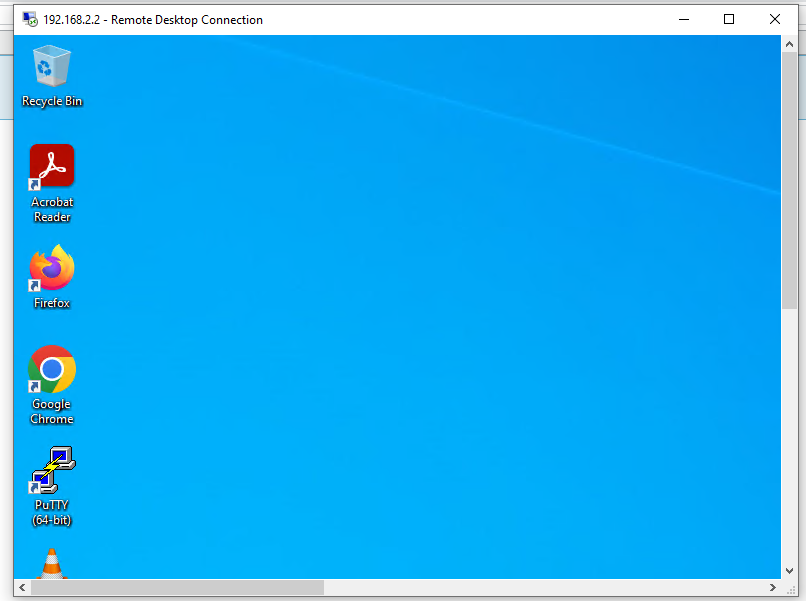
Select add and type in the name of your user you create.

****

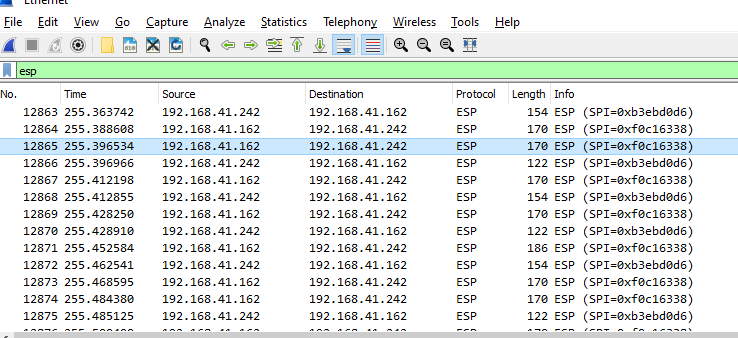
Click OK and your user is now an admin. Repeat steps on the device at the other inside network.

****

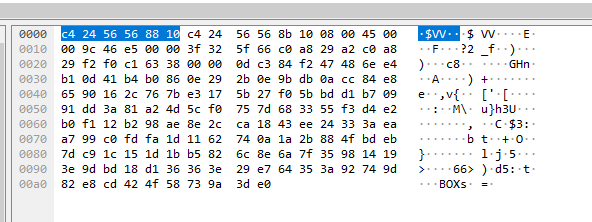
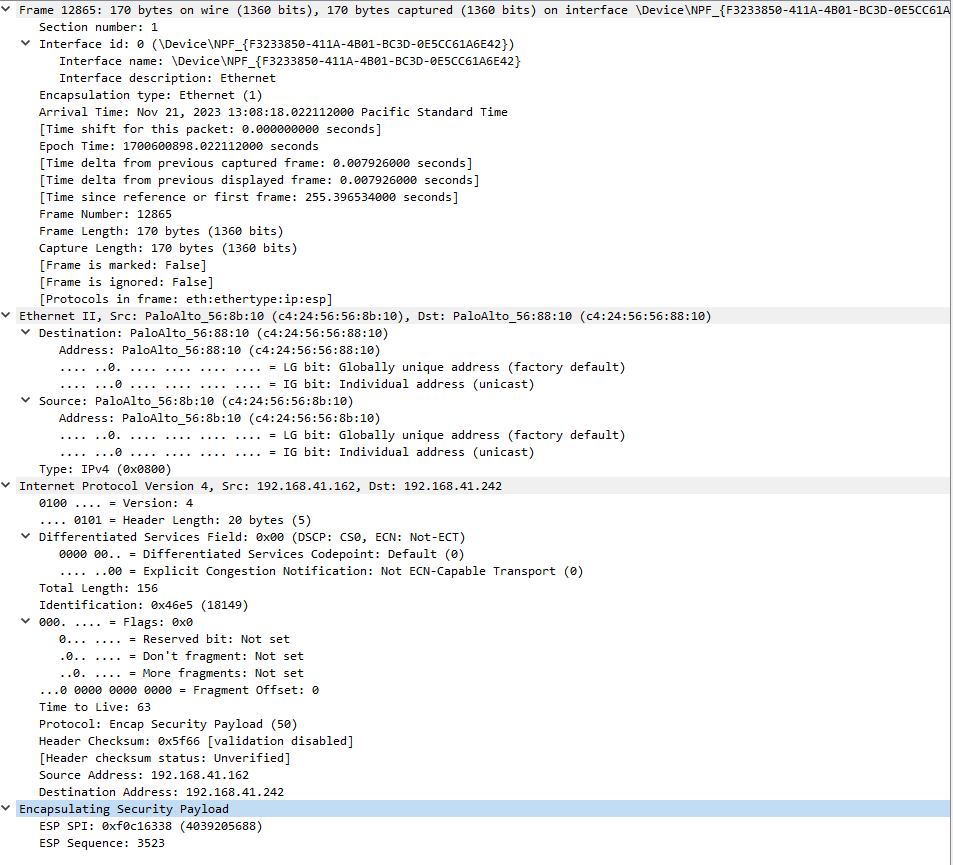
Open remote desktop and type in the Ip of the desktop on the other inside network and the user you created on it. To log in use the password you set for the user and click connect.

****

If successful, you should see a window like this of the remote desktop connection controlling the other pc.

****

Using a packet sniffer, you can view the data being sent and received through the firewalls to confirm it is encrypted.

****

You can see that this data is encrypted because it is now Cyphertext, and not clear text and it is an ESP file type which is an encrypted type of file.

**Problems:**

* soho was not functional
  + when changing Vlan IP we forgot to change dhcp default gateway disabling soho and access to the internet
* limited access to rack
  + share a period with another class so could not access Firewall B 50% of the time
* internal ip's could not be pinged across
  + tried changing IPs
    - Did not allow pings across, realized it wasn't necessary to ping
* IPsec tunnel was up but we could not communicate between firewalls
  + took many different solutions to fix
  + rechecked all dhcp default gateway and Vlan interface
  + tried many different IP addresses, only one combination worked
    - we don't know why only 192.168.1.0/24 and 192.168.2.0/24 worked but
* Conflicting information between articles
  + Crosschecked and experimented through trial and error until connection was functional
    - Used information between each article to create a functional IPsec Tunnel
* Guides had different preconfigured firewalls
  + Had to adjust our configurations of the firewalls to match more closely to the guides when applicable
    - Fixed many small issues and assisted in sections not covered in the guides

**Conclusion:**

Overall, this lab was very beneficial to our learning as it took many weeks of troubleshooting and collaboration with other groups to figure out solutions and collaboration with our small team to coordinate IPsec settings. Learning these skills is essential for future career in Cybersecurity and any career in general as you will need to collaborate and troubleshoot efficiently to meet deadlines. That is likely the most important takeaway from this lab but not the only one. Learning the different types of authentication and encryption protocols gives us a greater understanding of how they function and which protocols to choose in certain scenarios. My partner and I believed this would be a relatively easy lab when we found a video guiding us through the process of setting up the IPsec site to site tunnel but learned that it was more complex than shown in the guide. We had to find many different guides, some full text and some videos explaining the process and concepts, to cross check information and to allow the firewalls to transmit data between themselves through the tunnels. This taught us to find reliable sources and even though a source may be reliable, it may skip steps as they had a different configuration before starting the guide than our firewalls did.

