Kk;

David Singam 11/27/23

IPsec Tunneling Site to Site

## Purpose:

The purpose of this lab was to better understand the uses of the PA-220 firewall and how to configure IPSec tunnels between two firewalls to allow secure communication between networks.

## Background Information on lab concepts:

### IPSec VPN:

There is a feature called IPSec tunneling, which is used to encrypt data transferred between two points. IPSec VPN (Virtual private network) uses IPSec tunneling and provides a private and secure IP communication over a public network infrastructure (for example, the internet). With this technology, different sites or users in different geographical areas can communicate over a network and thus safely use their resources. IPSec provides data confidentiality and integrity, including authentication, integrity check, and encryption.

### IPsec Data Transfer:

IKE is a key management protocol standard used with IPSec. IKE authenticates each peer in an IPSec session, automatically negotiates two levels of SAs (Security Associations) and handles the exchange of session keys accomplished in two phases: phase 1 and phase 2. An SA is a set of mutually agreed-upon keys and algorithms that are used by both VPN peers to allow the flow of data across the VPN tunnel. The main purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers.

### IPsec Tunnel Sessions Termination:

The IPSec session can be terminated because the traffic ended and the IPSec SA was deleted or the SA can timeout based on either SA lifetime setting. The SA timeout can be after a specified number of seconds or a specified number of bytes passed through the connection. The keys are discarded when SAs terminate, requiring IKE to perform a new phase two and, possibly, a new phase one negotiation. New SAs can be established before the current ones expire, maintaining uninterrupted data flows.

### IKE Phase one:

The main purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers. In this phase, the firewalls use the parameters defined in the IKE Gateway configuration and the IKE Crypto profile to authenticate each other and set up a secure control channel. IKE Phase supports the use of pre-shared keys or digital certificates (which use public key infrastructure, PKI) for mutual authentication of the VPN peers. Pre-shared keys are a simple solution for securing smaller networks because they don’t require the support of a PKI infrastructure. Digital certificates can be more convenient for larger networks or implementations that require stronger authentication security.

### IKE Phase two:

IKE negotiates the stricter IPSec Security Associations (SA) parameters between the peers. After the tunnel is secured and authenticated, in Phase 2 the channel is further secured for the transfer of data between the networks. IKE Phase 2 uses the keys that were established in Phase 1 of the process and the IPSec Crypto profile, which defines the IPSec protocols and keys used for the SA in IKE Phase 2. Encapsulating Security Payload (ESP) and the Authentication Header (AH) are used to further encrypt, authenticate, and verify integrity of the packets.

### IKE gateway:

The Palo Alto Networks firewalls or a firewall and another security device that initiate and terminate VPN connections across the two networks are called the IKE Gateways. To set up the VPN tunnel and send traffic between the IKE Gateways, each peer must have an IP address—static or dynamic—or FQDN (Fully qualified domain name). The VPN peers use pre-shared keys or certificates to authenticate each other mutually. The peers must also negotiate the mode—main or aggressive—for setting up the VPN tunnel and the SA lifetime in IKE Phase 1. Main mode protects the identity of the peers and is more secure because more packets are exchanged when setting up the tunnel. Main mode is the recommended mode for IKE negotiation if both peers support it.

### IKE crypto:

The IKE Crypto profile is used to set up the encryption and authentication algorithms used for the key exchange process in IKE Phase 1, and lifetime of the keys, which specifies how long the keys are valid. To invoke the profile, you must attach it to the IKE Gateway configuration. The following parameters need to match for a successful IKE negotiation: Diffie-Hellman (DH) Group for key exchange, encryption algorithms, and authentication algorithms.

**Diffie-Hellman (DH) group:**

The DH group is for generating symmetrical keys for IKE. The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share.

**Authentication Algorithms:**

sha1, sha 256, sha 384, sha 512, or md5.

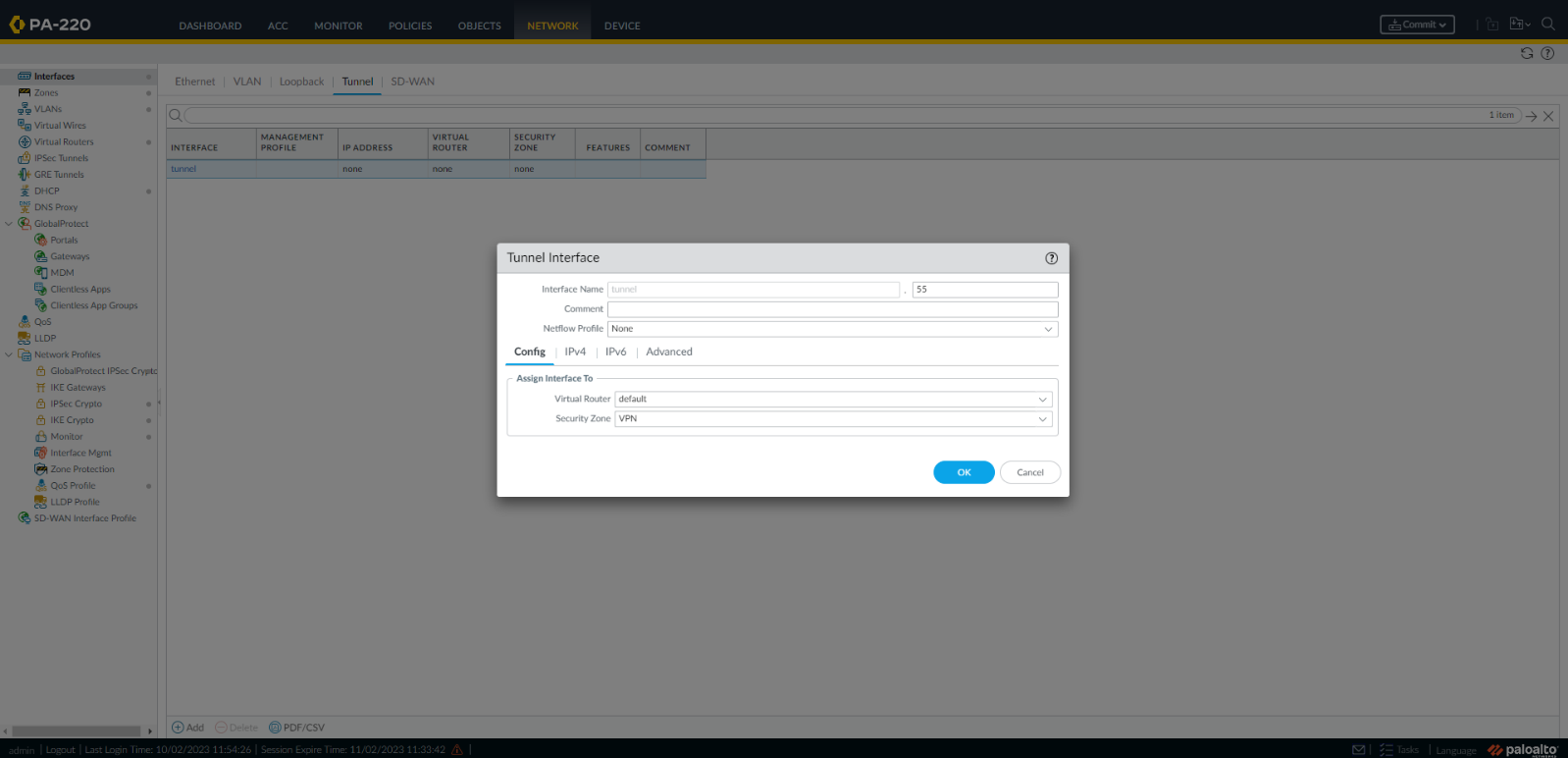
**Encryption Algorithms:**

aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, aes-256-cbc, or des.

### IPsec crypto:

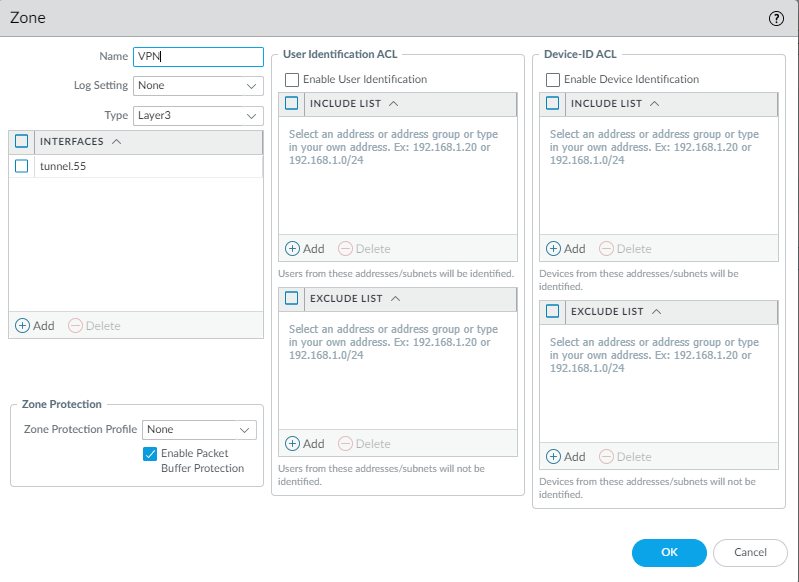
The IPSec Crypto profile is invoked in IKE Phase 2. It specifies how the data is secured within the tunnel when Auto Key IKE is used to generate keys automatically for the IKE SAs. IPSec negotiation will be successful when the following parameters match between the VPN peers: IPSec Protocol (ESP or AH), DH Group (or PFS) for key exchange, Encryption algorithms, and Authentication algorithms. By default, perfect forward secrecy (PFS) is enabled on IPSec tunnels to generate a more randomized key. PFS does this by performing an additional key exchange during IPSec SA negotiation to generate a new shared secret and combines it into the new IPSec SA keys. When configuring PFS, ensure that both the VPN peers have the same PFS configuration.

## Lab Summary:



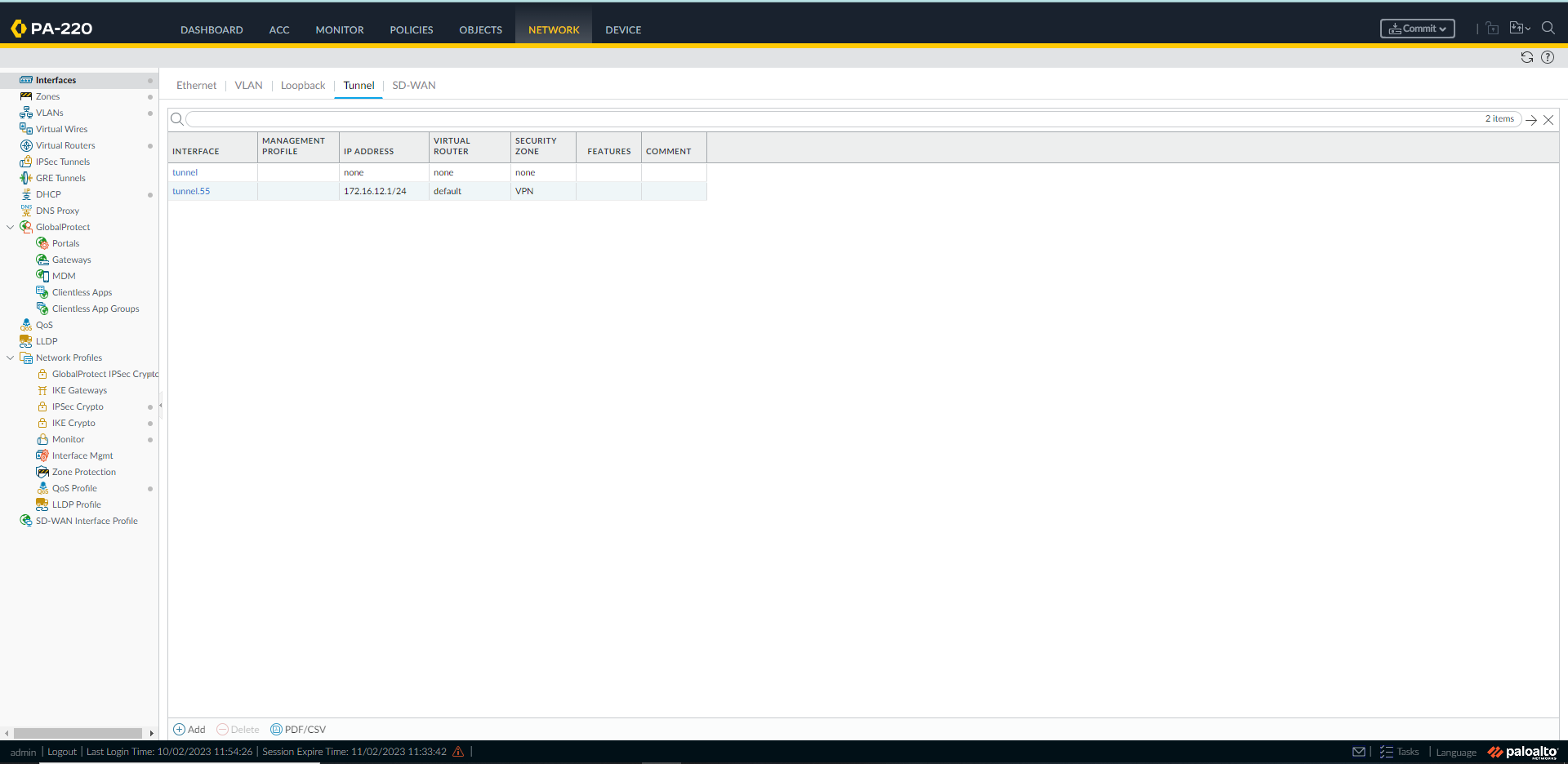
On FW-A under the networks tab go to interface. Once in interfaces go to tunnel and select add at the bottom of the page. For now, leave the security zone as none and select default for Virtual Router. Under IPv4 configured your desired IP, we used 172.17.12.1/24. Later, this IP will be used to connect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

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

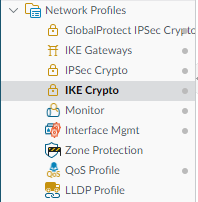
****

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.

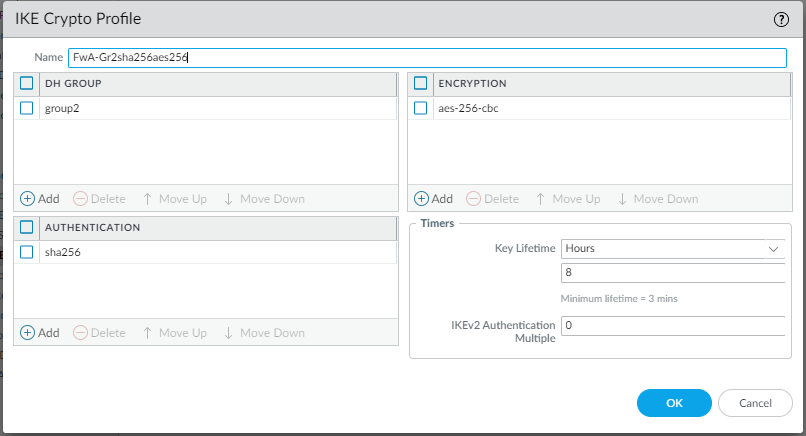
Repeat for FW-B.

****

Your interfaces should now look like this.

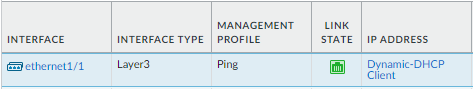


Still under network expand the network profiles and select IKE Crypto select add at the bottom.

****

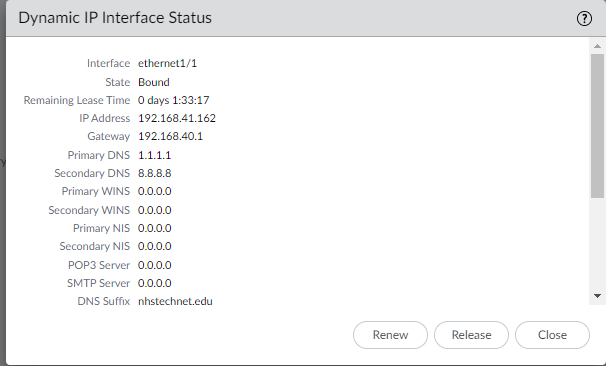
Now in the config box type in any name that you can remember. Select add DH GROUP and click group2. Select add ENCRYPTION and choose aes-256-cbc or other encryption methods. Select add AUTHENTIFICATION and select sha256. You can leave the timer as default.

Repeat for FW-B

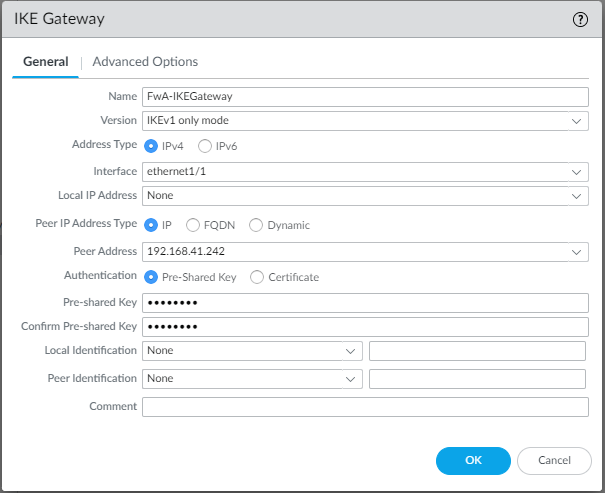
****

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.

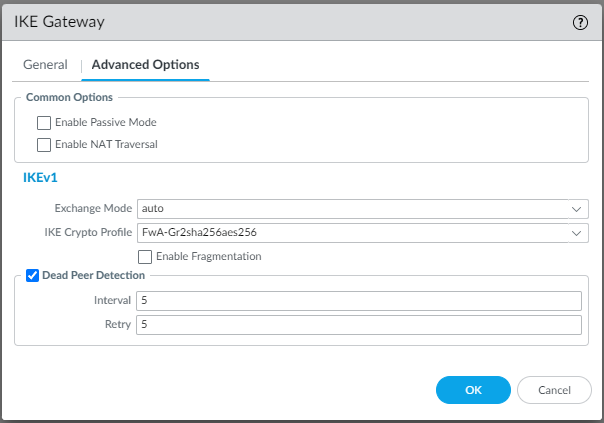
Repeat for FW-B

****

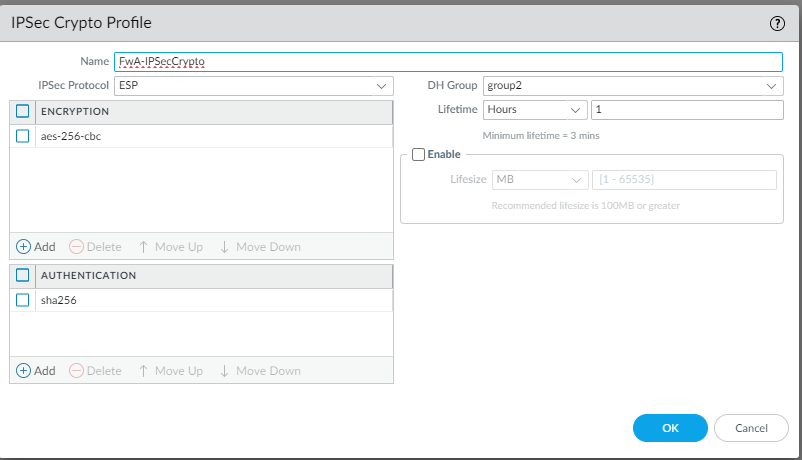
You should see this when you click on dynamic-DHCP Client.

****

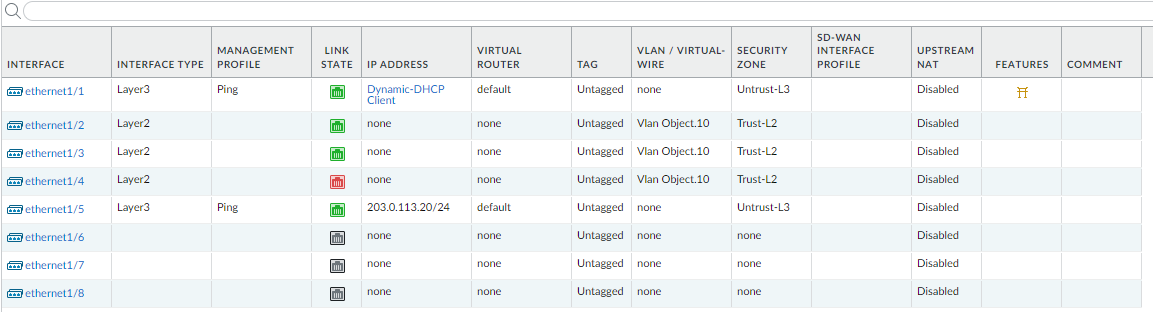
Now go to IKE Gateway under network and create new. Select IKEv1 only mode or any other option just make sure the Firewalls match. Select the interface connecting to the internet.

****

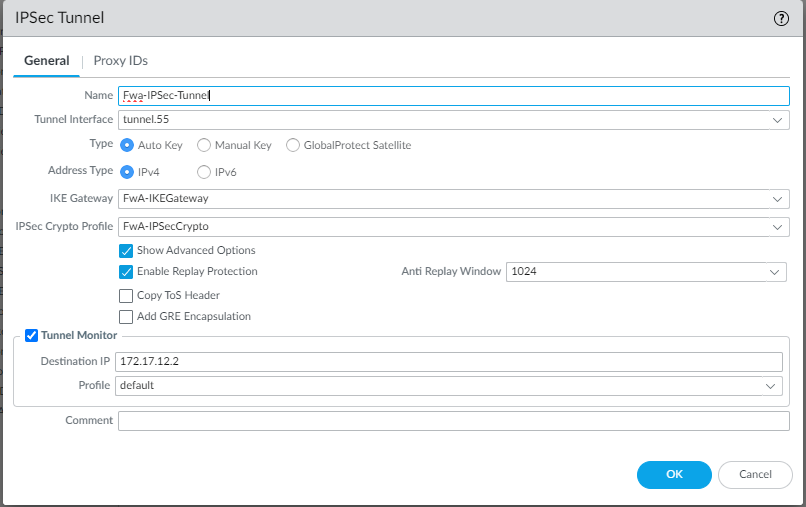
Go to advanced options and configure as shown.

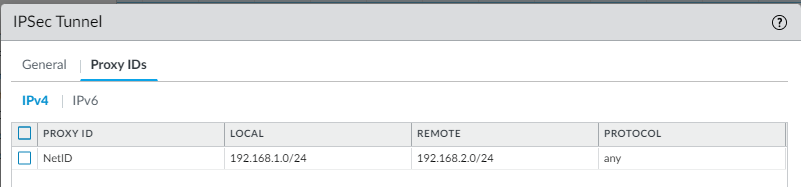
****

Open the IPSec crypto profile, make an encryption and authentication key, and configure as shown.

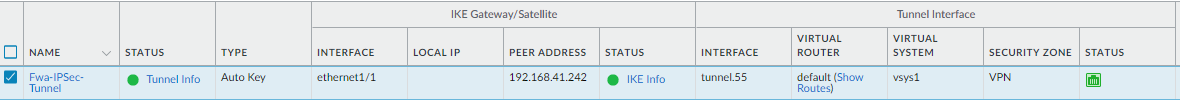
****

Configure the IPSec tunnel as shown.

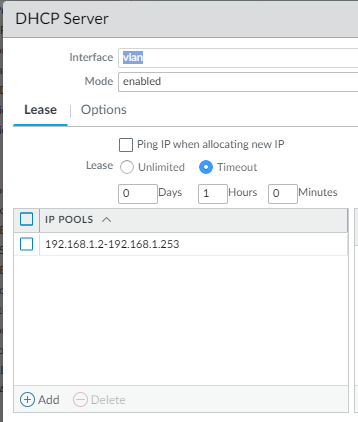
****



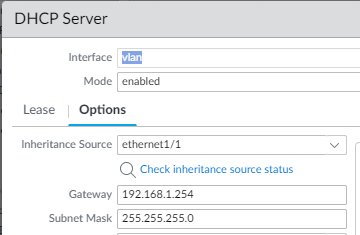
Use the IP of the DHCP as the Local network. Remote is DHCP of other firewall.

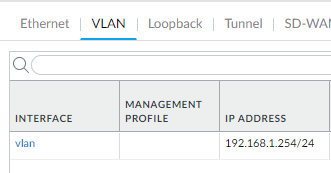


If this is up and it doesn’t work check that your dhcp pool is configured correctly

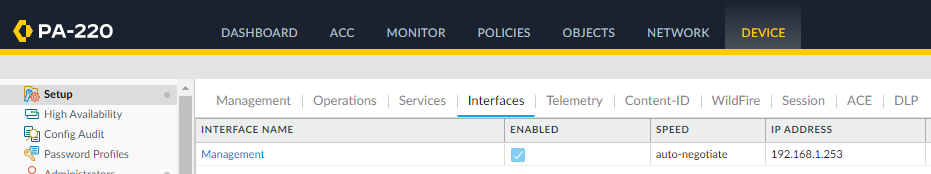
****

Proxy ID matches

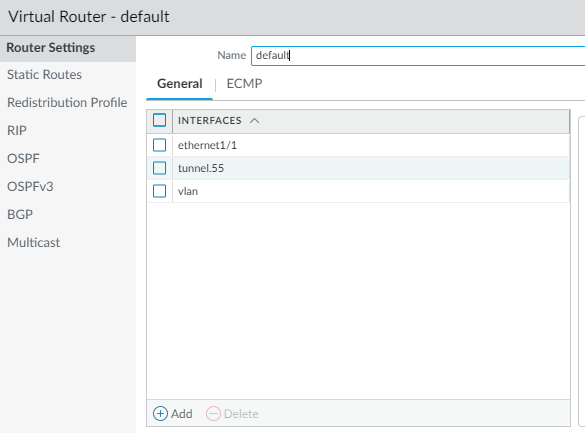


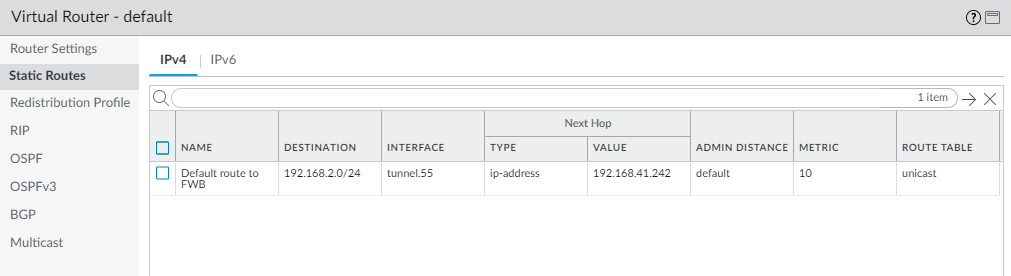


Make sure the VLAN is the gateway and is in the subnet.



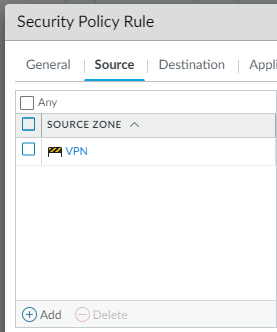
Set the gateway to address of the vlan interface as done in the SOHO config lab, need to be in the same subnet

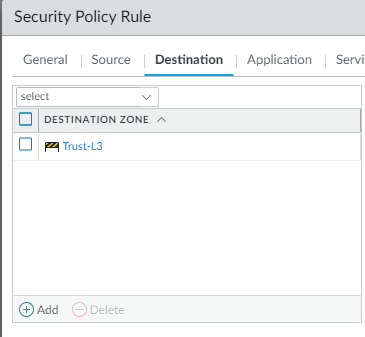
****



Make a static route to send all traffic tagged for the other FW’s network, use the address given to ethernet 1/1 on FW B as the next hop.

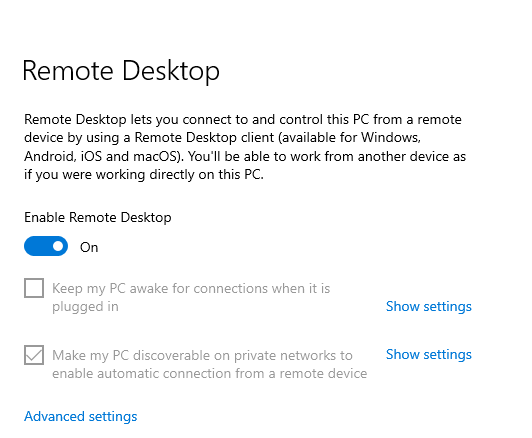
****

****



Go to security policy rules, add a new source zone and set it to the VPN, and add a new destination zone and set it to Trust-L3.

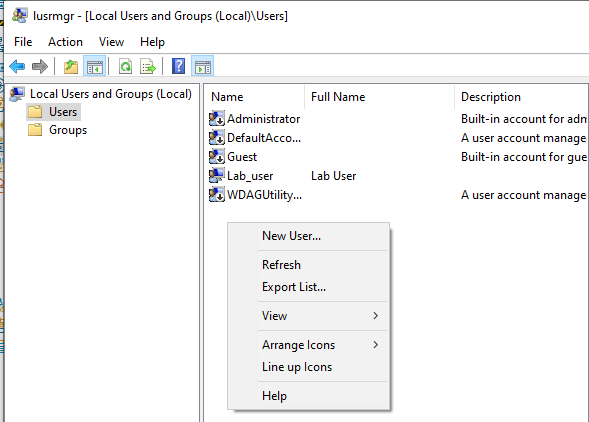
**Your tunnel should now be up and functional.**

****

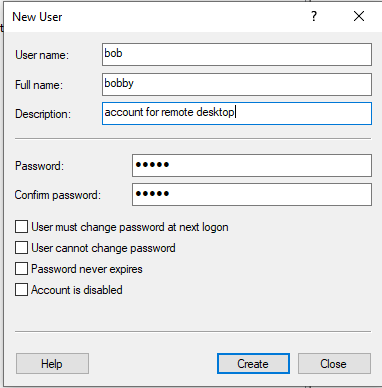
To verify communication between FWs through the tunnel, use Remote Desktop as shown.

If you are on a company or school computer you may need to add a user to remote desktop too to enable communication between FWs.

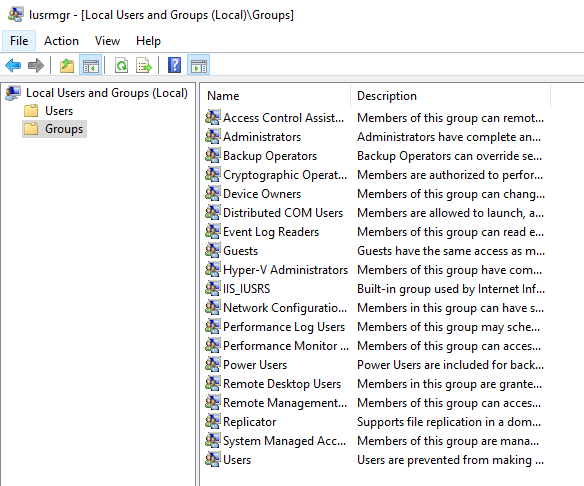
****

****

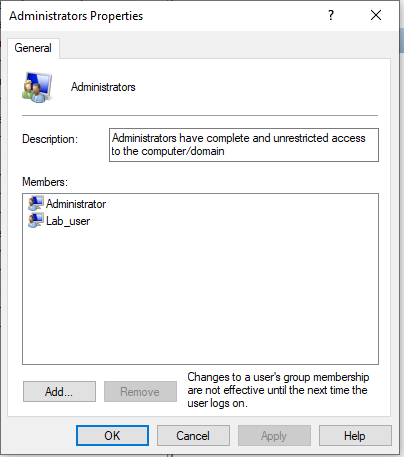
Go to Local Users and Groups, and add a new user.

****

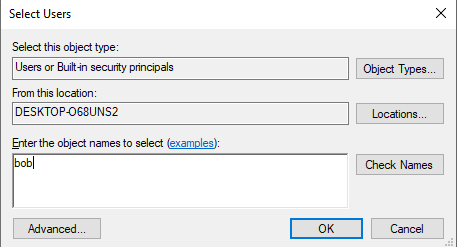
Configure any user name, full name, description, and password.

****

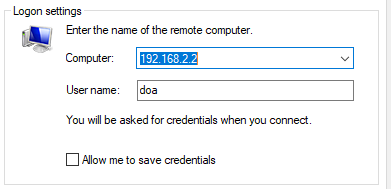
Go to groups.

****

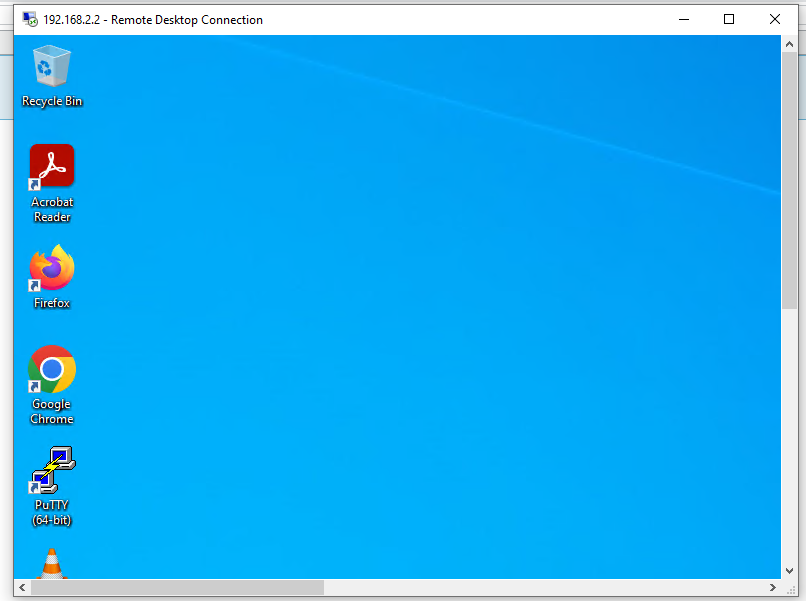
Go to Administrators.

****

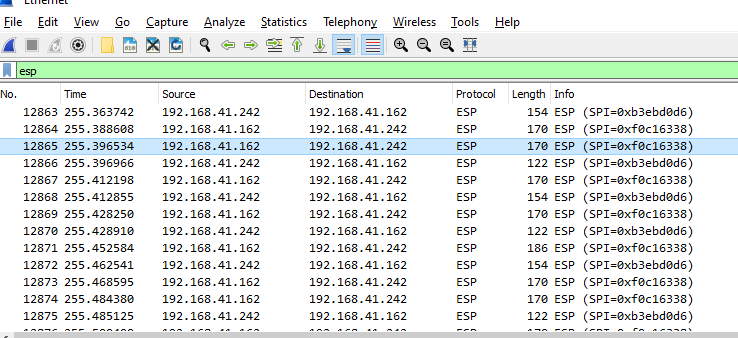
Add your user to the group to make them an admin.

****

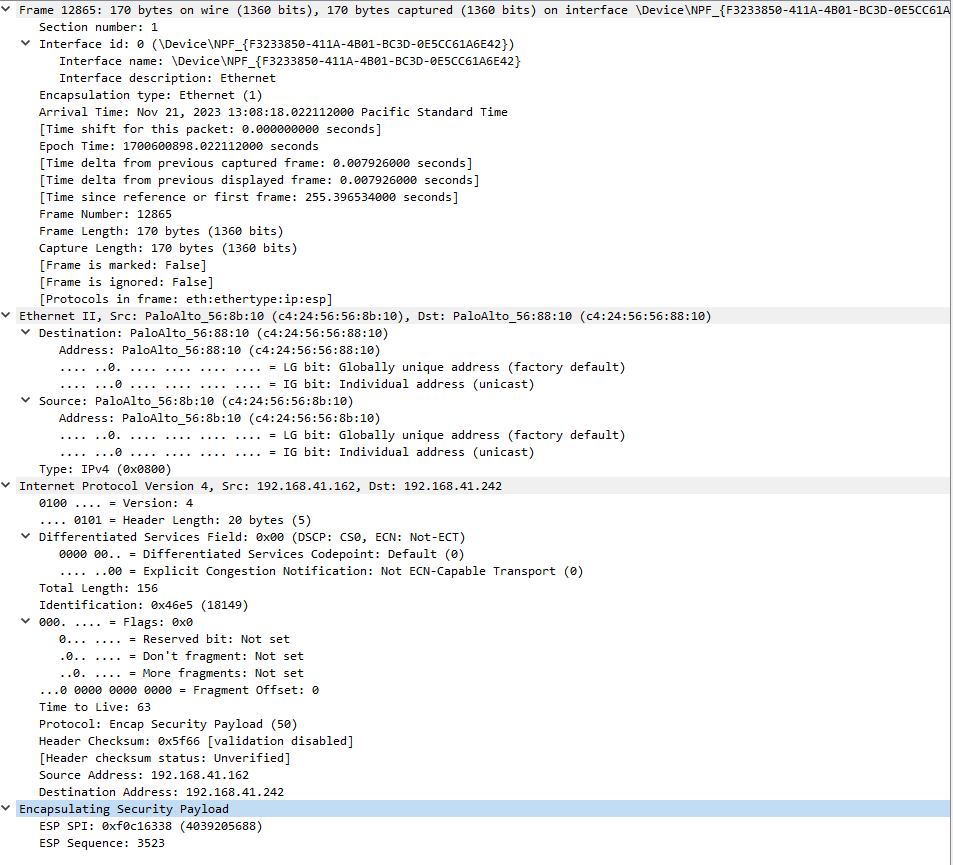
You will be asked for the password of the user created on the other desktop.

****

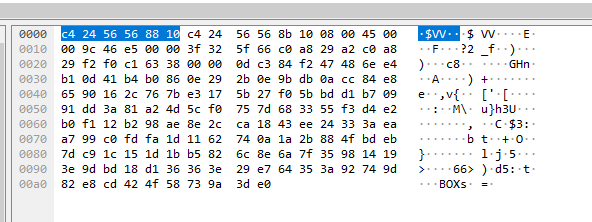
If it works successfully then communication between networks is established.

****

Use a packet sniffer like Wireshark to view the traffic from the PCs going through the firewalls IPSec tunnel.

****

Verify that the packet is from the firewall

****

By seeing that it is an ESP (Encapsulating Security Payload) packet, we know the data is traveling through the tunnel and is encrypted.

## 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 ip's
    - 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

## Conclusion:

The process of setting up a site-to-site VPN between firewalls taught us a lot about Internet Key Exchange (IKE), encryption, authentication, and IPSec. Additionally, throughout the process we became proficient in configuring PA-220 firewalls, especially when using them for secure communication between networks. Most of our issues came from trying to successfully communicate between the firewalls, and many were caused by things outside our control like having limited rack access, or the school network restrictions making PC communication difficult. This shows that we should work on our proficiency in IP, so that in the future we can more effectively troubleshoot. Site-to-Site VPNs are extremely useful tools when data needs to be securely transmitted between networks, such as a corporate network and a branch office network. The ability to set up and maintain a site-to-site VPN tunnel between networks is very valuable and is used often in the corporate networking world to ensure that all employees have secure access to the same resources.

## Sources

<https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/ipsec-vpn-basics>

<https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/get-started-with-ipsec-vpn-site-to-site/site-to-site-vpn-overview>

<https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn/define-cryptographic-profiles/define-ipsec-crypto-profiles>

<https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/ipsec-vpn-basics/internet-key-exchange-ike-for-vpn>

<https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/ipsec-vpn-basics/ipsec-vpn-tunnels>

## Lab Stamp

A paper with a logo

Description automatically generated