Palo Alto PA-410 Initial Configuration/SOHO configuration

Reed Holman | Cybersecurity | 1/3/2023



Purpose:

The point of this lab was to fully set up our firewall to be configured for a SOHO network. Meaning we could have access to the internet and every device on our LAN would automatically get an IP address. We also wanted to update the version of our firewall to the latest edition.

Background Information:

A SOHO configuration is designed for small networks in an office or home office environment. Usually meaning that all your devices om your LAN go through one device (like a Palo-Alto PA 410) to get to the internet. SOHO networks are very basic to set up, that is why they are so useful for small business. A disadvantage is that SOHO networks are often more vulnerable to security attacks.

The firewall will have a port connected to the internet. It will use a DHCP server on the internet to get IP address for devices on the LAN. DHCP stands for Dynamic Host Configuration Protocol and is responsible for assigning IP addresses to devices. It is very useful in any network because it eliminates the need to manually set IP address on every device which will save a lot of time and effort.

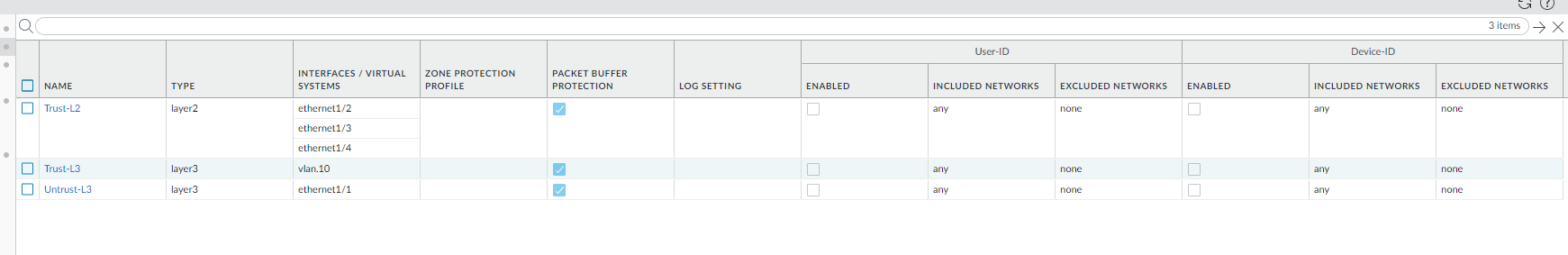
Configurations:

Ethernet 1/1 should go to the internet (default gateway that will act as DHCP server

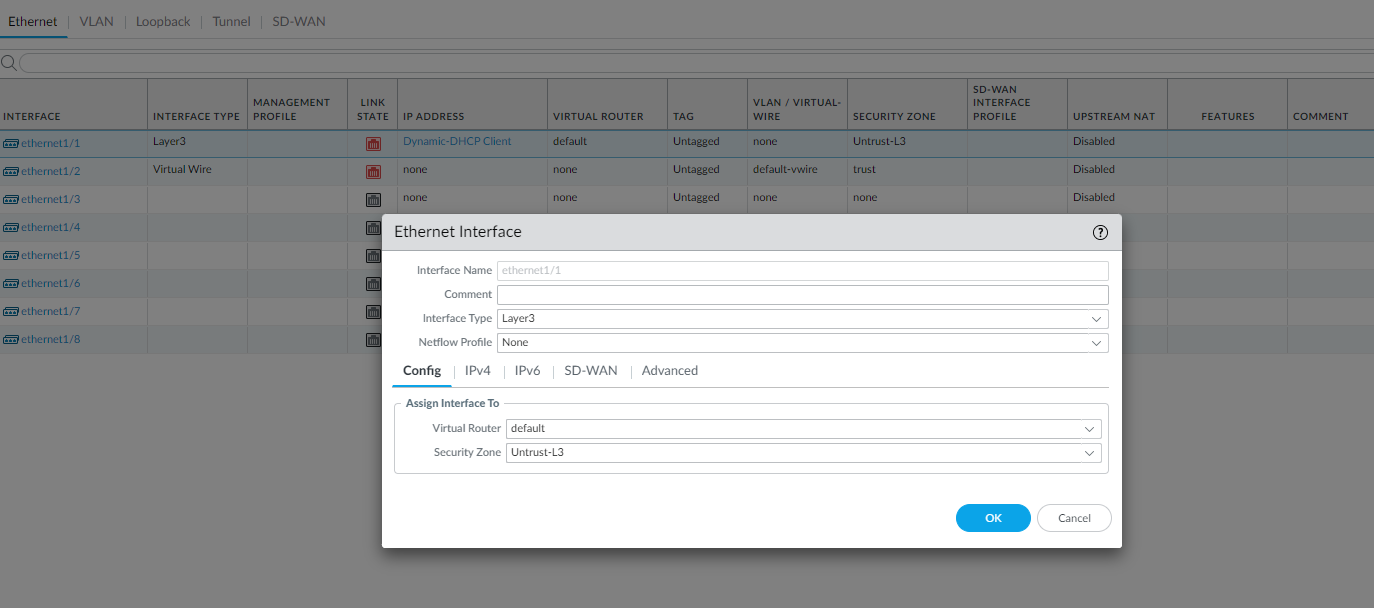
Ethernet 1/2 – 1/3 should connect to one of the PCs. Interface management should connect to another PC.

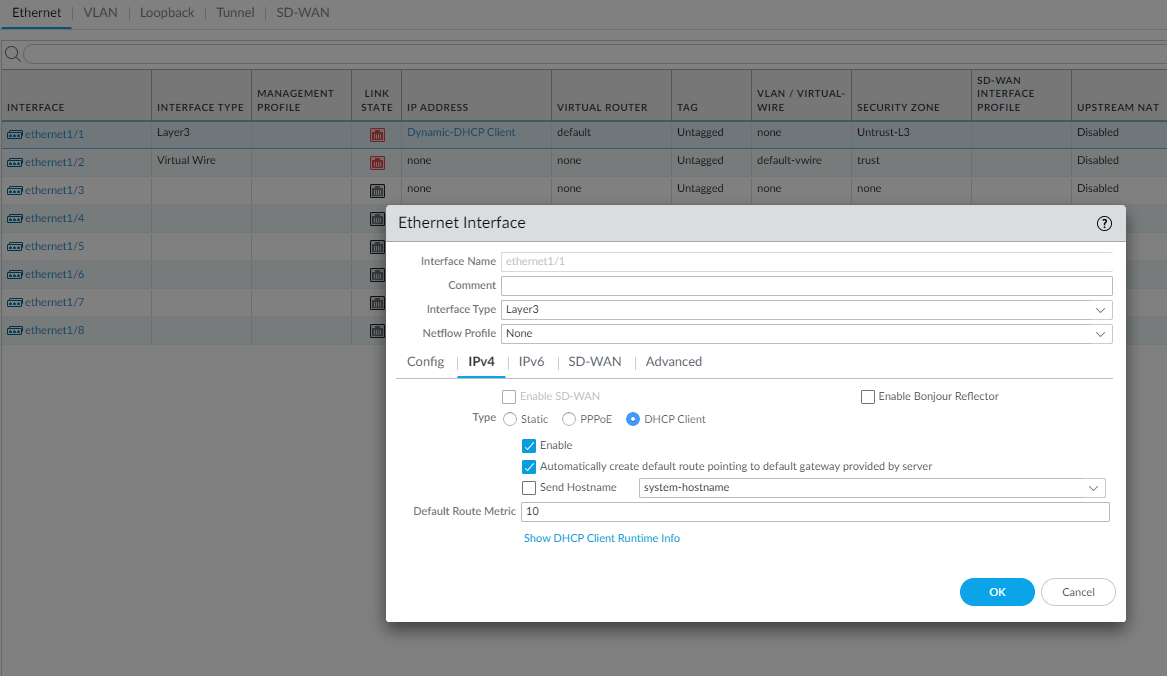
Assign yourself an ip address manually and go to 192.168.1.1 (the management interface ip) on an internet browser.

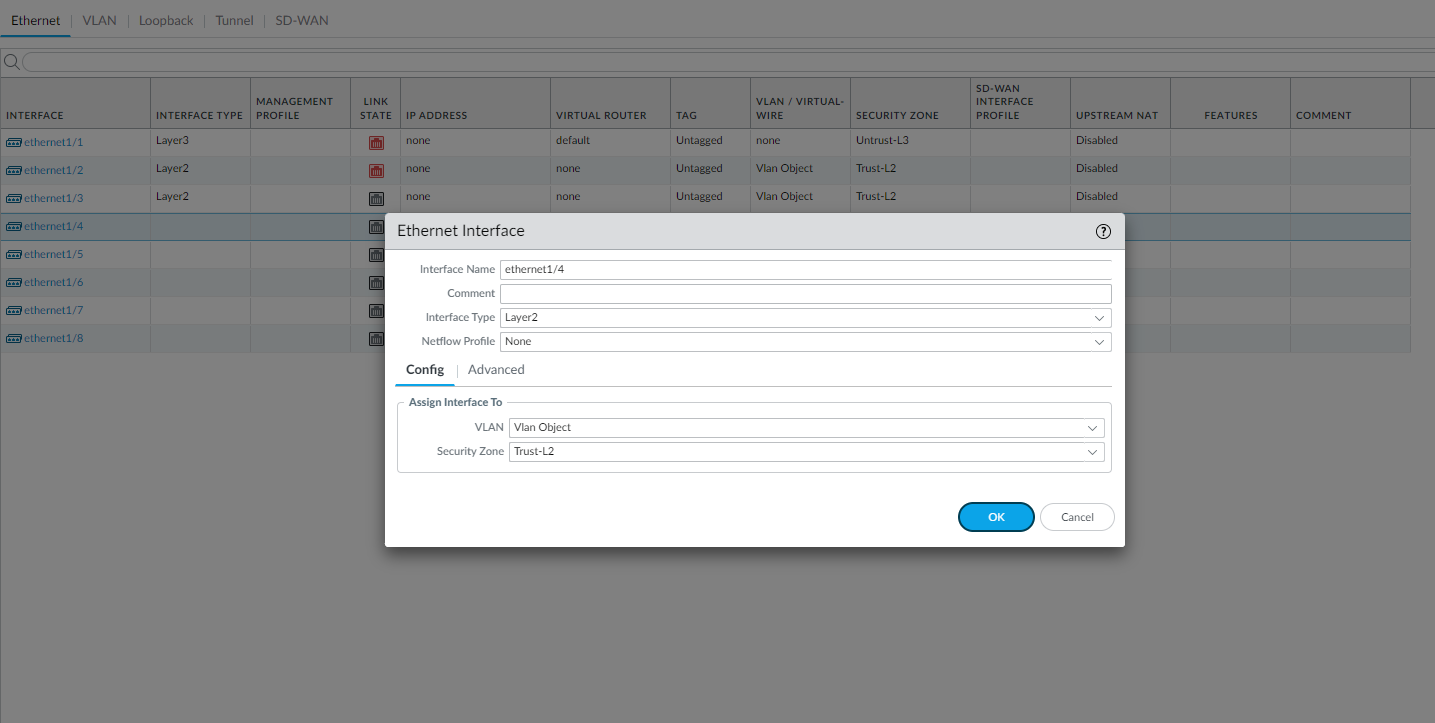
Step 1: Create 3 security zones under Network>Zones. Trust-L2, Trust-L3 and Untrust-L3. The ‘type’ of zone should be L2 or L3, accordingly.



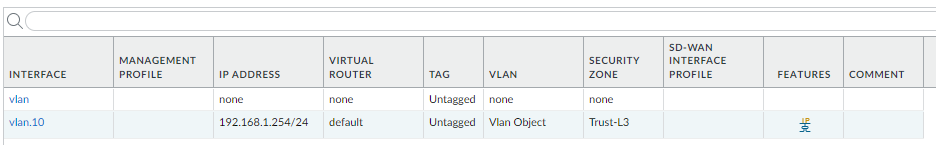
Step2: Go to network>interfaces. Et1/1 should be in layer 3 and in untrust layer 3. Et 1/ 2-4 should be in layer 2 and in trust-L2. Ethernet 1/1 should be a dynamic dhcp client. Virtual router for all should be set to default.



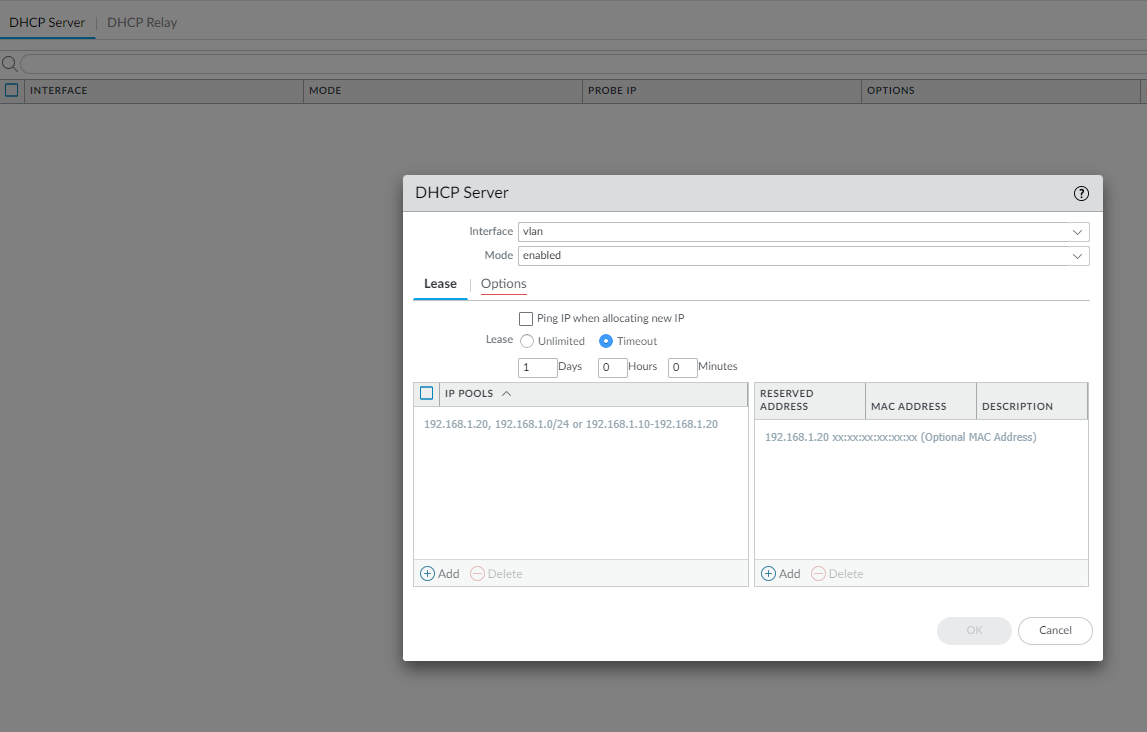


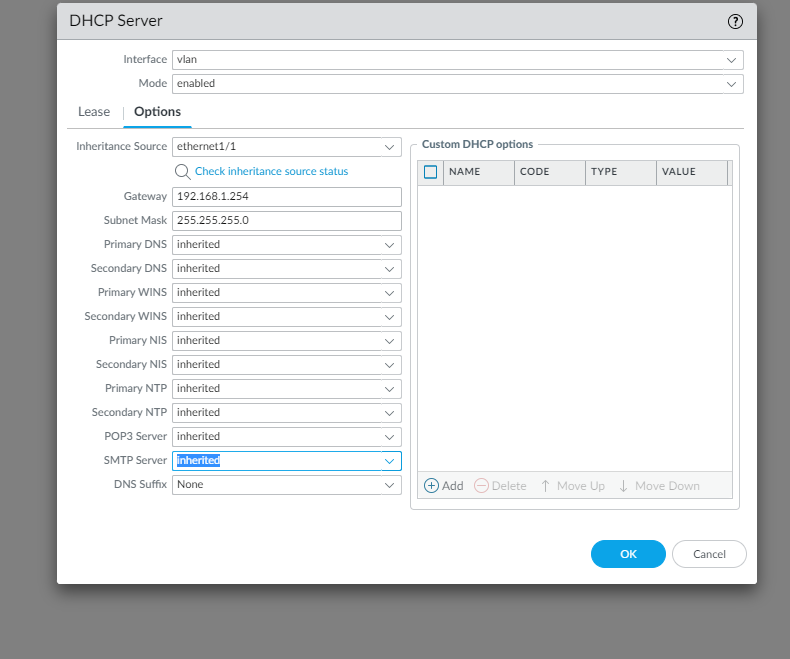


Step 3: Go to network > interfaces > vlans. Click add to add a vlan. Set vlan number. For Vlan, use vlan object and security zone should be trust-L3. For the ip address, use the 192.168.1.254/24 (network that the default gateway is in).

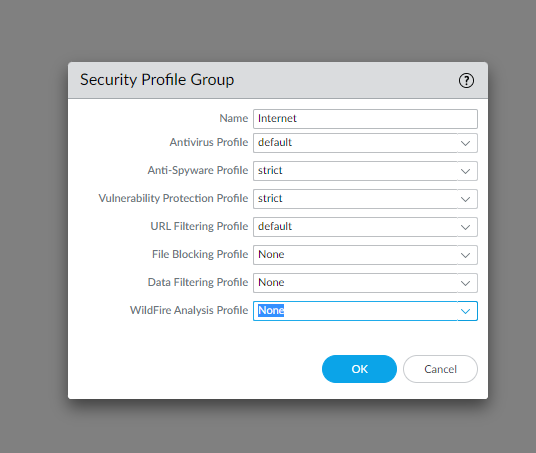


Step 4: Go to network > dhcp. Click add and select vlan for the interface that you just created (e.g., vlan.10). mode should be enabled, lease should timeout in 1 day, and the ip pool should be 192.168.1.2 – 192.168.1.253, or anything in between. Then go to options and select inheritance source to be ethernet 1/1 which is connected to the default gateway. Gateway should be 192.168.1.254 and subnet mask should be /24. Set everything to inherited besides DNS suffix.

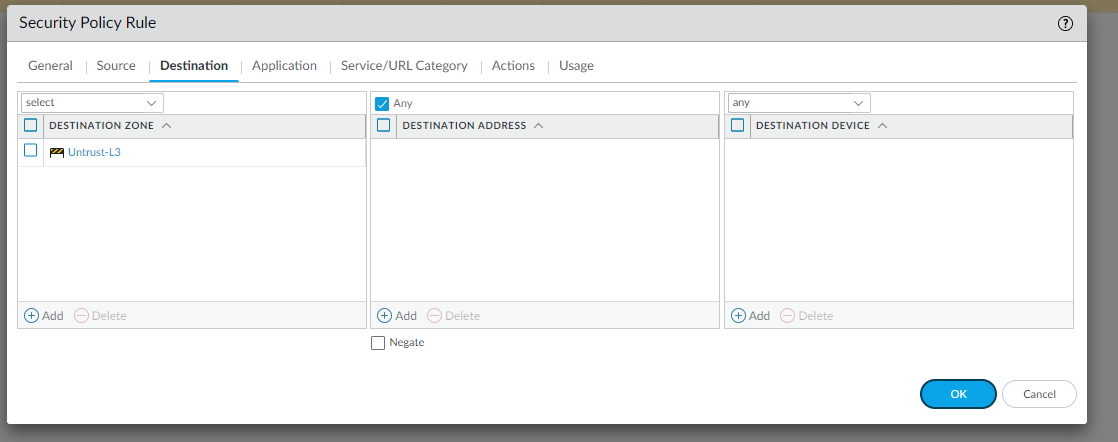




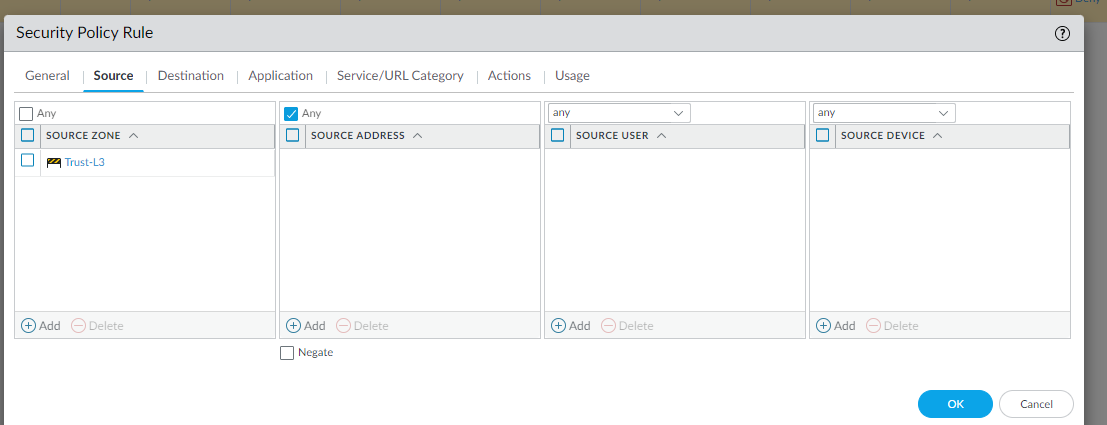
Step 5: go to object > security profile group. Click add and pick name. Settings should be as shown:



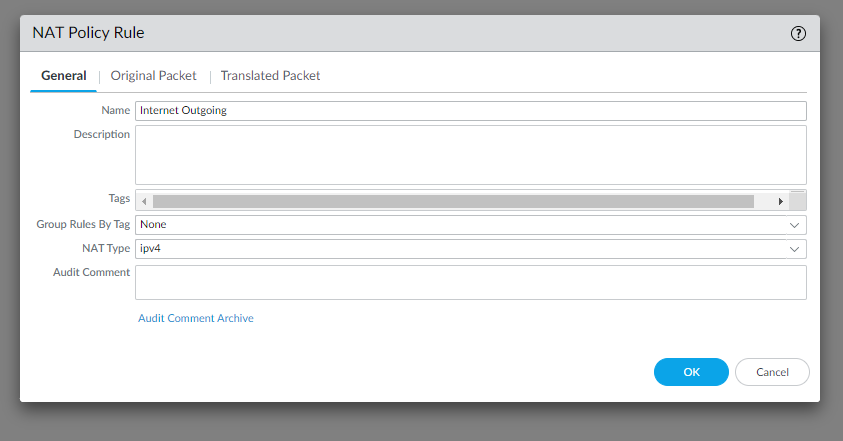
Step 5 cont.: Destination zone should be Untust-L3.



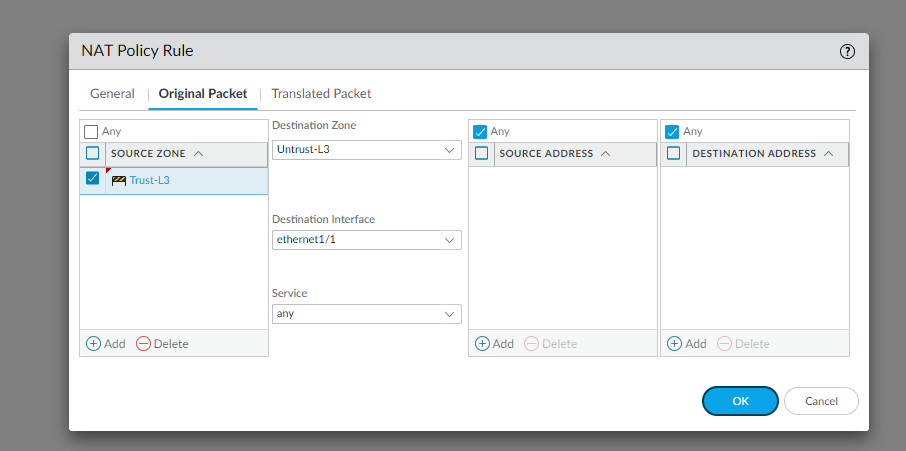
Step 5 cont.: Source should be in trust-L3:



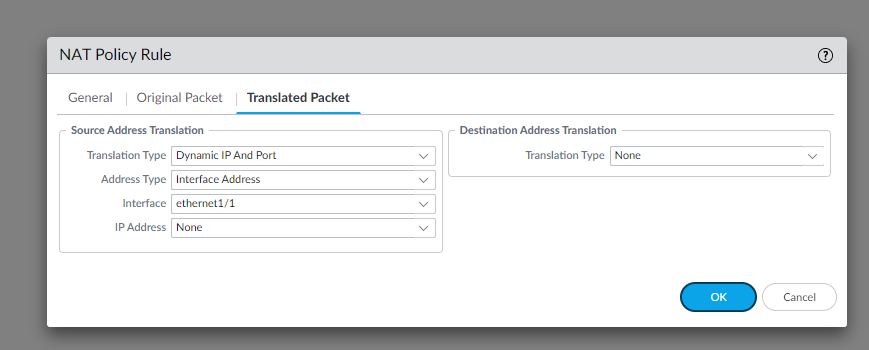
Step 6: Go to policies NAT and click add. Name it internet outgoing and nat type should be ipv4.



Step 6 cont.: Then go to original Packet an configure settings as shown.



Step 6 cont.: Finally, go to translated packet and configure settings as shown:



Done

Problems:

Configuring this was very similar to the other Palo Alto firewall. We had one issue when first configuring our firewall that when we tried to select our vlan for the interface our DHCP server, it wouldn’t let us. We just deleted that vlan and created a new one and that fixed it. Another silly problem we had was that we had a cable that was faulty. It would sometimes randomly stop working, which made it difficult to figure out what the problem was. For a while we thought something was wrong with our configuration, but when we used new cables everything worked all of the time.

Conclusion:

This time around we were able to configure our Palo Alto firewall a lot easier and faster than our first time. We referenced our own lab report to ensure we didn’t miss any steps.