Background:

The purpose of this lab was to set up the new and robust PA-410 firewall, that was completely wiped and in factory defaults, with small office/home office configurations. We wanted to give this firewall the configurations necessary for it to operate in small out small environment. For example, we wanted to configure 3 of its ports to be in the Trust L2 layers so that we could connect it to our 2 computers and the management port. The goal was to make the firewall connect to the internet (default gateway) and give those ports IP addresses via DHCP.

After we factory reset our firewall, we wanted to put some basic configurations so that our 2 computers could connect to it and receive a wired internet connection and get IP addresses from it through DHCP. The firewall also should’ve been setup for any further configurations, such as URL filtering, to work.

In this lab we also upgraded the firewall to the last version 11.0, only this time it was a lot easier because we had experience setting up another palo alto firewall. Due to the identical port layout on the firewall and identical management UI of the two firewalls, we were able to complete this lab by looking at our previous lab write-up without any hiccups whatsoever.

Though we didn’t get to use them as we only setting up SOHO, this new generation of palo alto 400 series firewalls have some useful features. Compared to previous firewalls, this piece embeds machine learning in the software in order to provide exceptional threat protection. It is a solution to newly concocted phishing attacks that are being popularized among hackers. It also uses behavioral analysis to detect IoT devices and make optimal policy recommendations to the user. Services are cloud-delivered and reduce the amount of human error possible. It has also been optimized to be used as a central office firewall, both for hosts and manager.

Lab Summary:

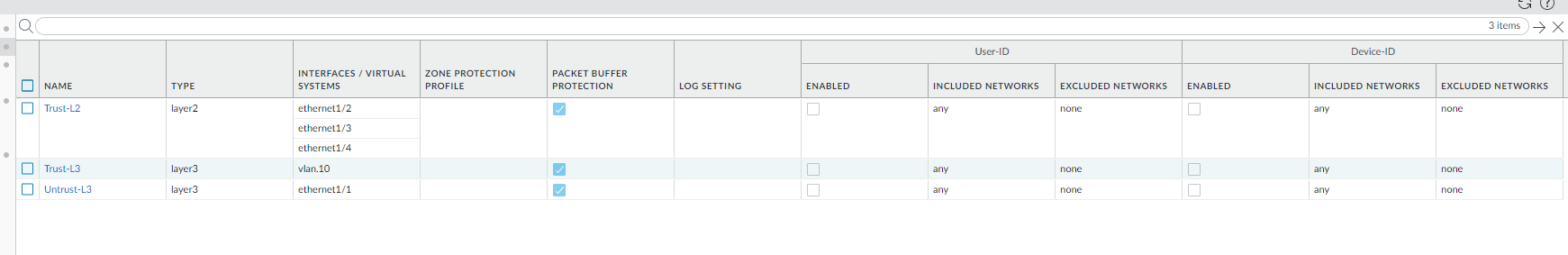
Wires Setup:

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

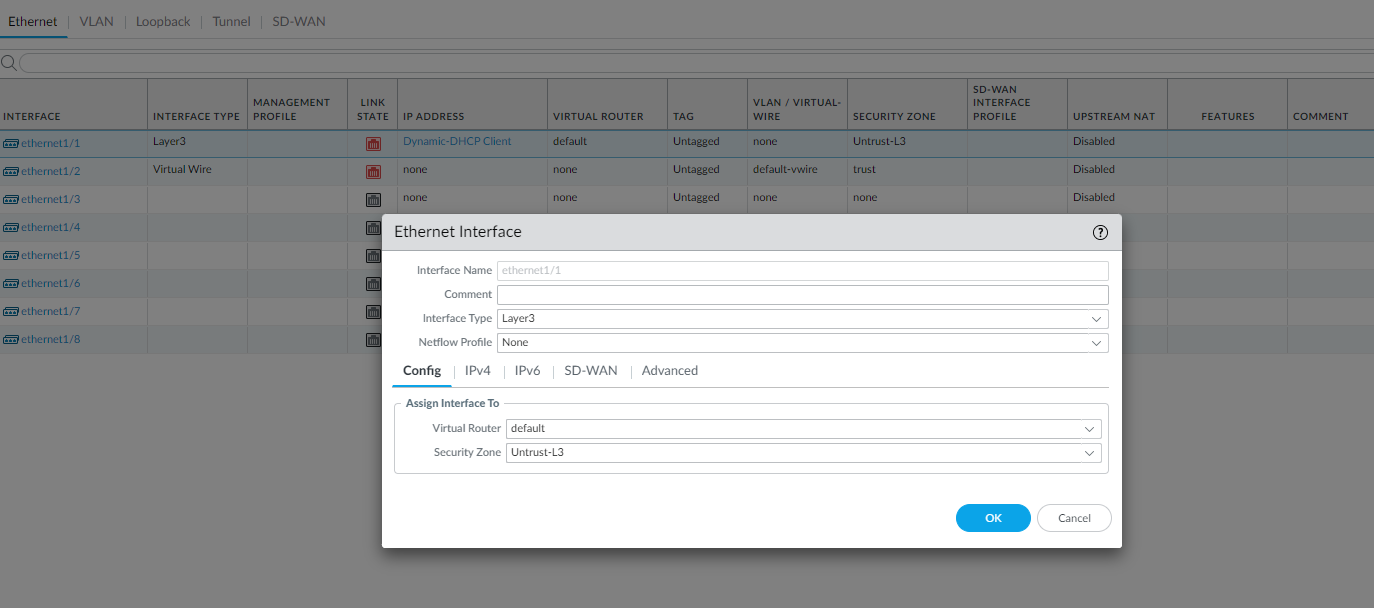
Ethernet 1/2 – 1/3 should connect to one of the PCs. Interface management should connect to another PC.

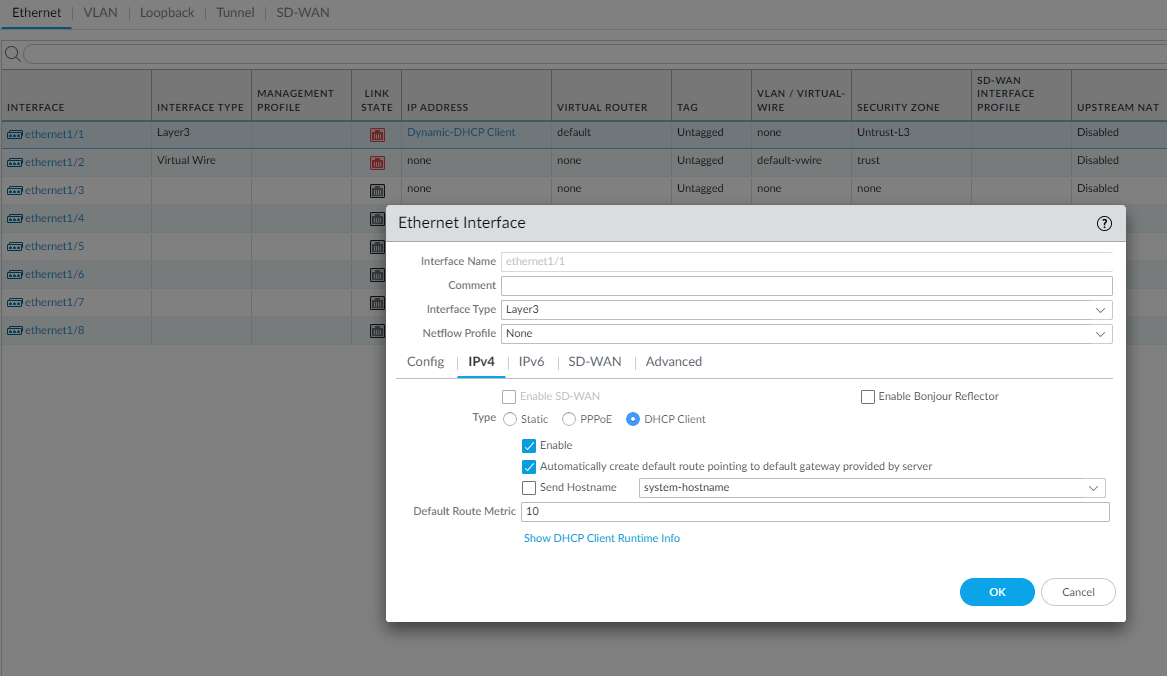
Assign yourself an ip address manually and go to 192.168.1.1 (the management interface ip) on an internet browser.

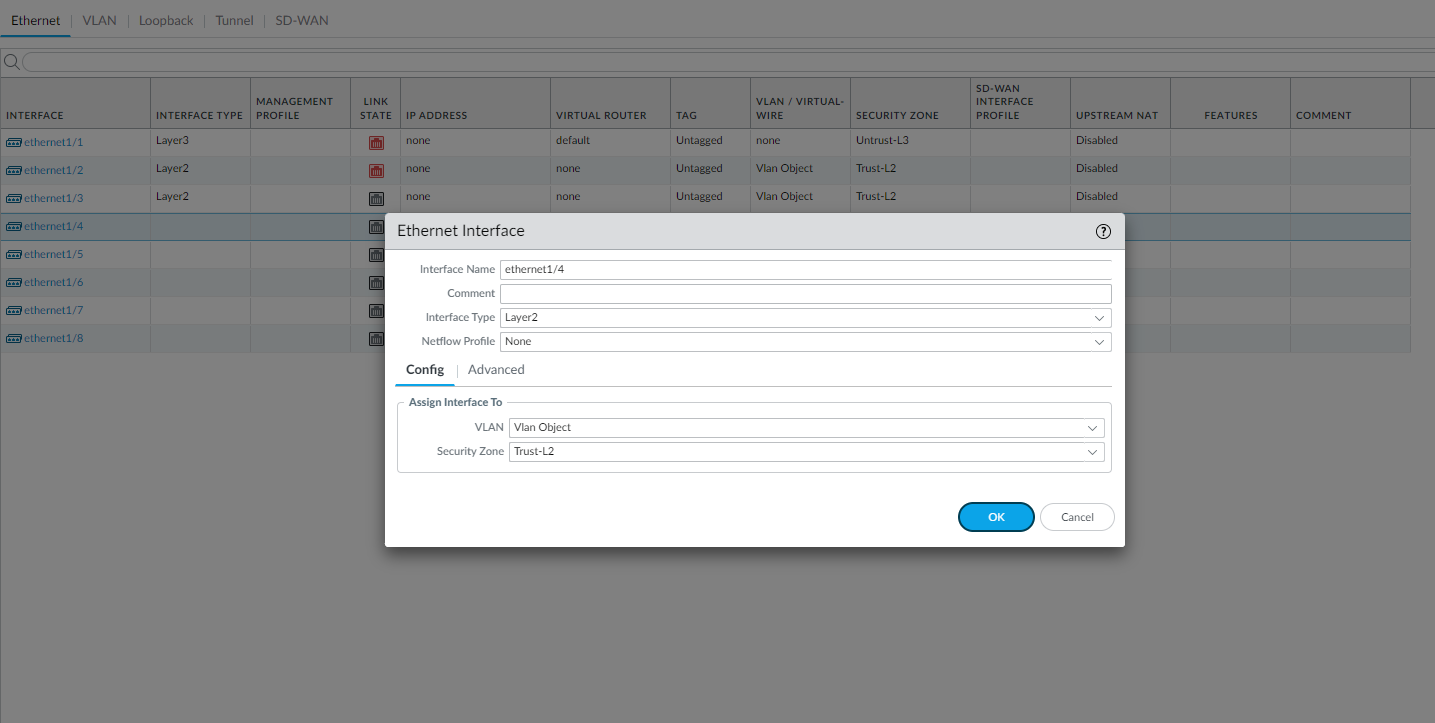
Step 1: Create 3 security zones under Network>Zones. Trust-L2, Trust-L3 and Untrust-L3. The ‘type’ of zone should be L2 or L3, accordingly.



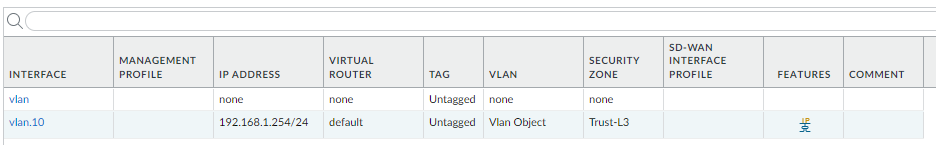
Step2: Go to network>interfaces. Et1/1 should be in layer 3 and in untrust layer 3. Et 1/ 2-4 should be in layer 2 and in trust-L2. Ethernet 1/1 should be a dynamic dhcp client. Virtual router for all should be set to default.



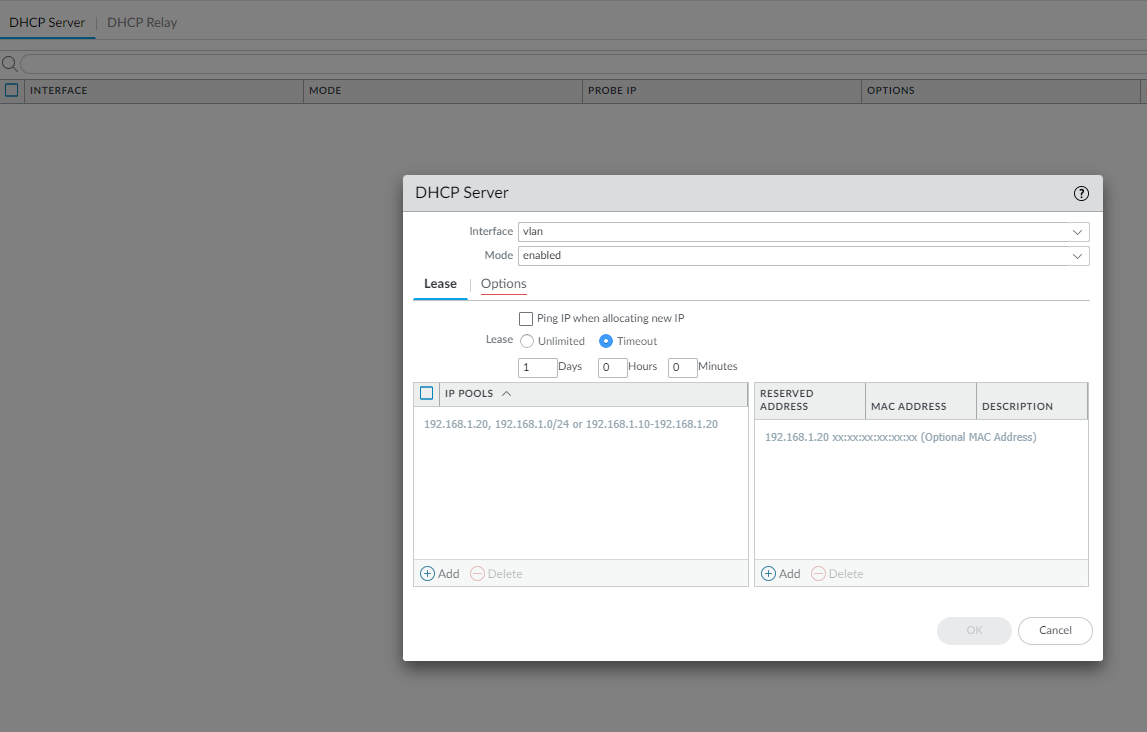


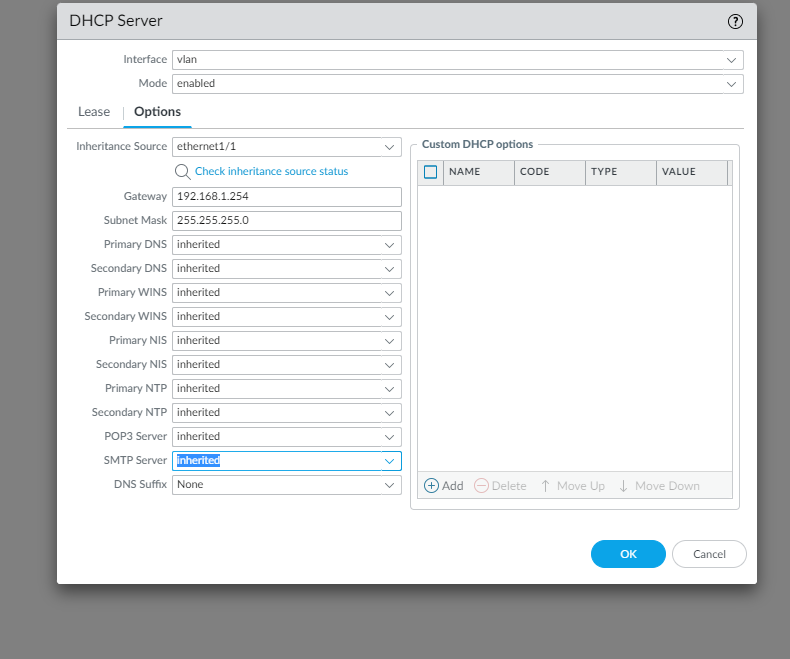


Step 3: Go to network > interfaces > vlans. Click add to add a vlan. Set vlan number. For Vlan, use vlan object and security zone should be trust-L3. For the ip address, use the 192.168.1.254/24 (network that the default gateway is in).

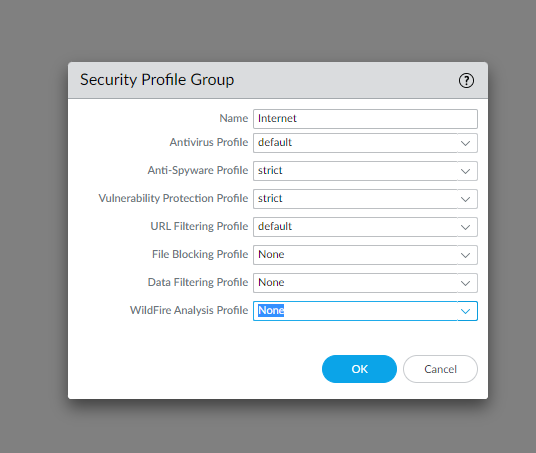


Step 4: Go to network > dhcp. Click add and select vlan for the interface that you just created (e.g., vlan.10). mode should be enabled, lease should timeout in 1 day, and the ip pool should be 192.168.1.2 – 192.168.1.253, or anything in between. Then go to options and select inheritance source to be 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.

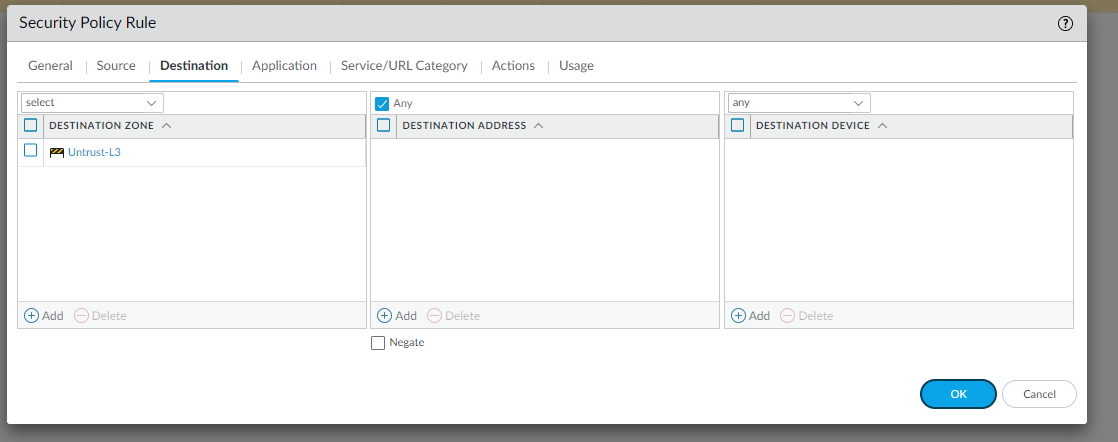




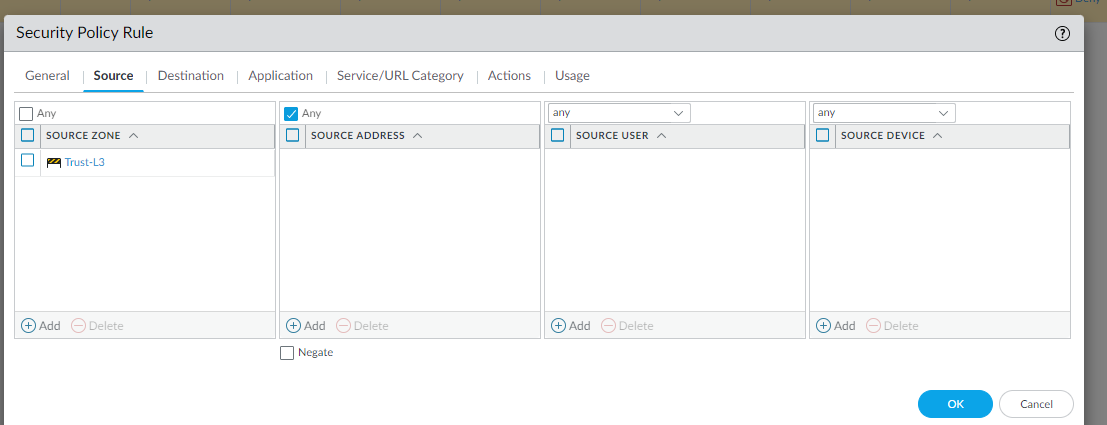
Step 5: go to object > security profile group. Click add and pick name. Settings should be as shown:



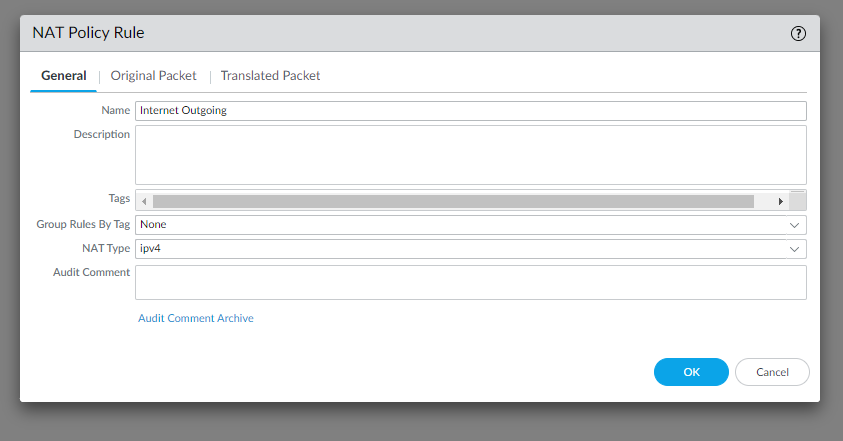
Step 5 cont.: Destination zone should be Untust-L3.



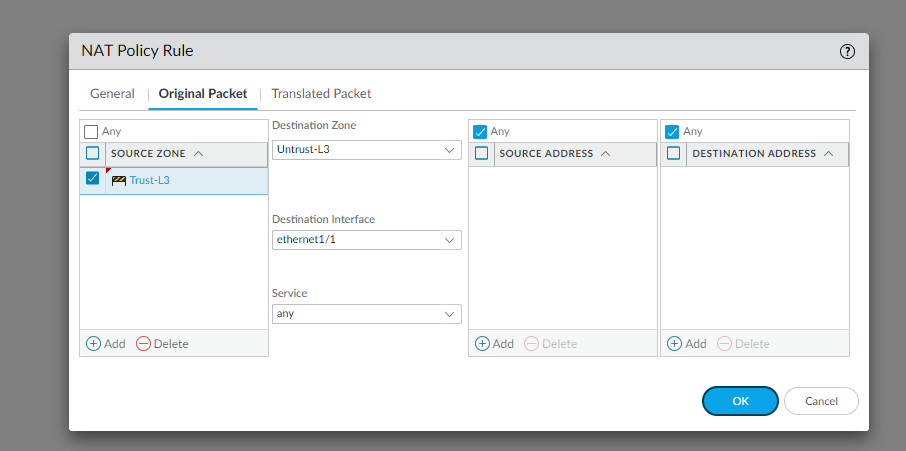
Step 5 cont.: Source should be in trust-L3:



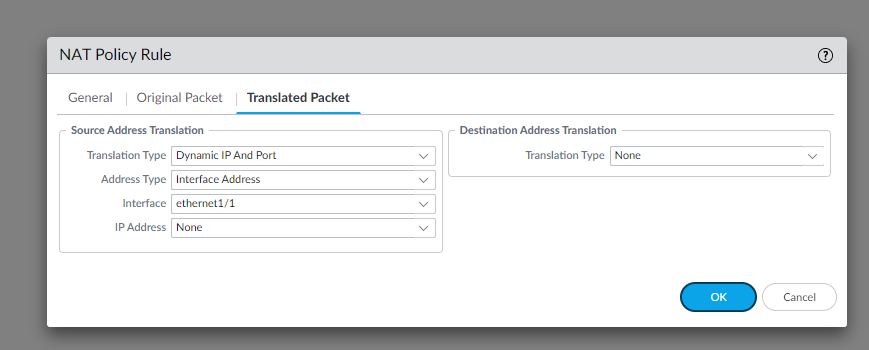
Step 6: Go to policies NAT and click add. Name it internet outgoing and nat type should be ipv4.

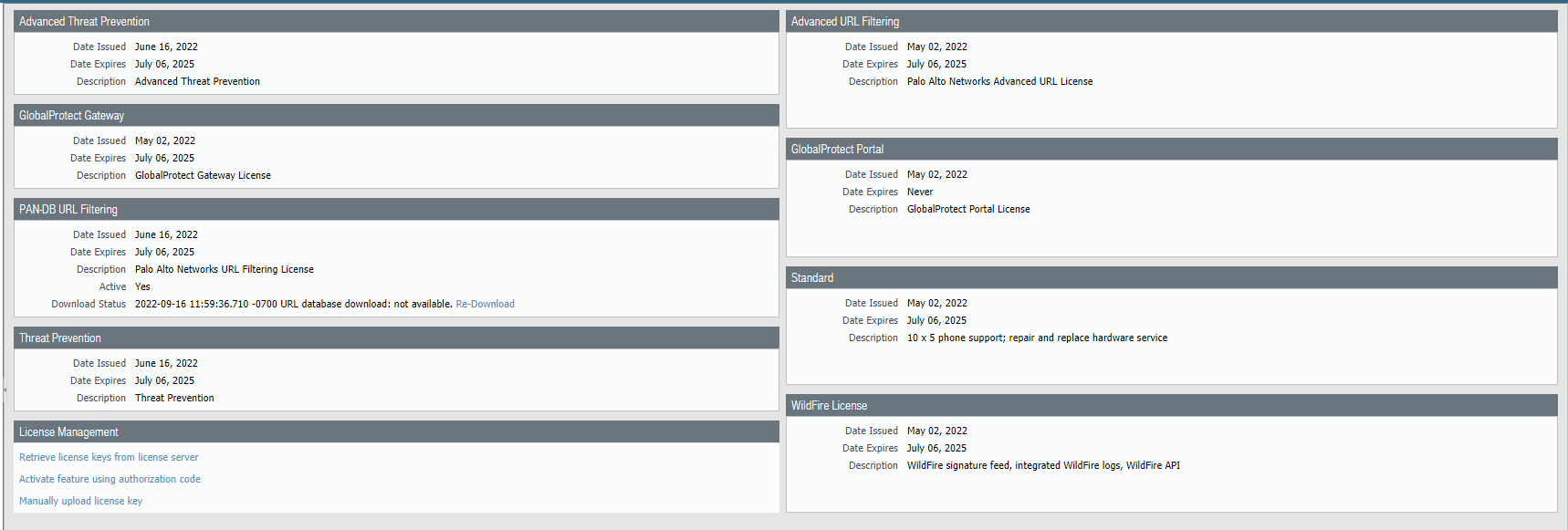


Step 6 cont.: Then go to original Packet an configure settings as shown.

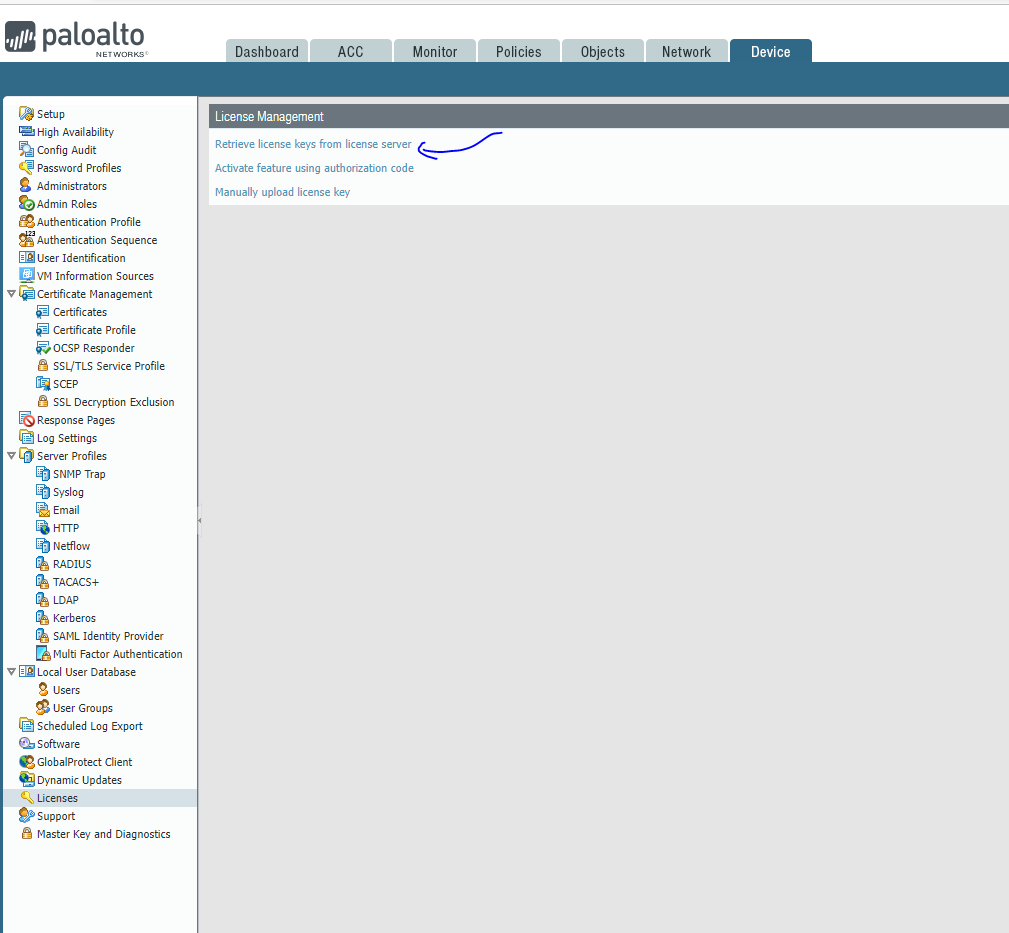


Step 6 cont.: Finally, go to translated packet and configure settings as shown:

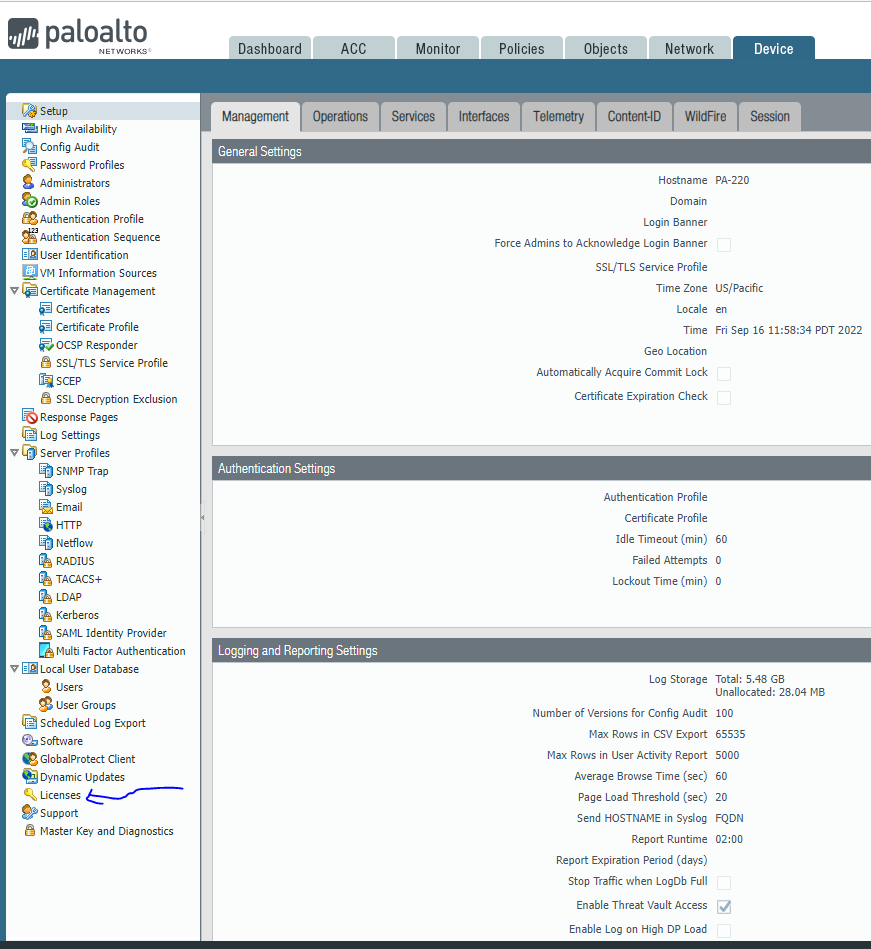




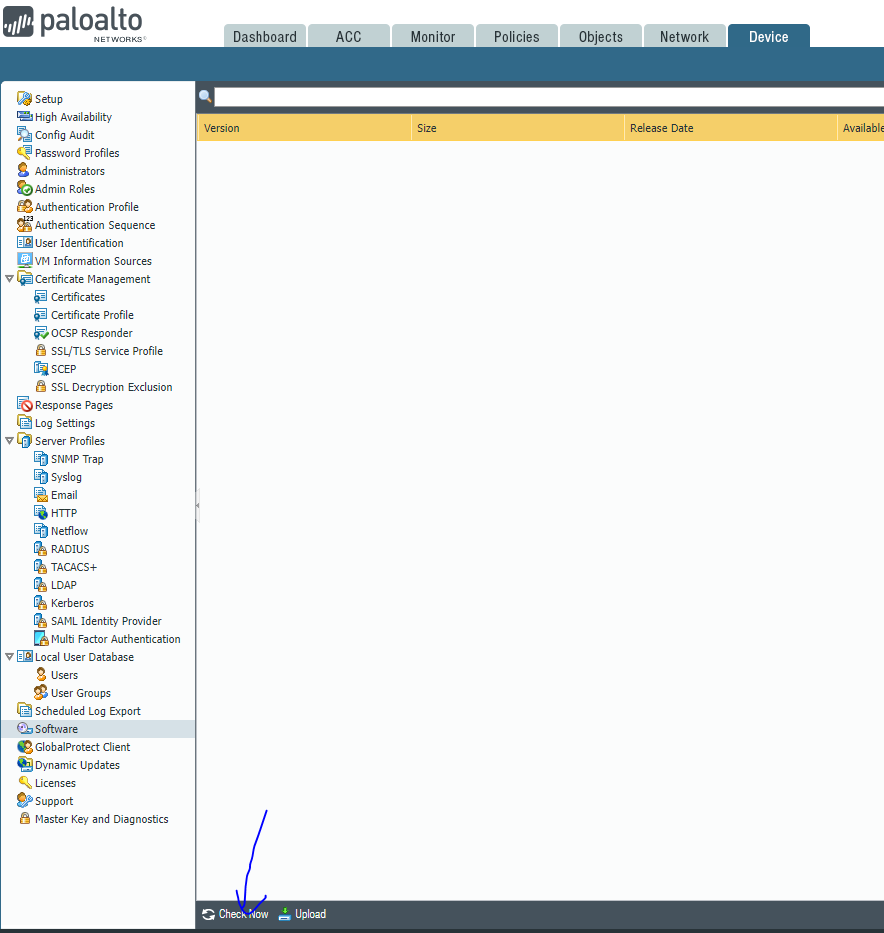
Step 7: Go to retrieve new licenses



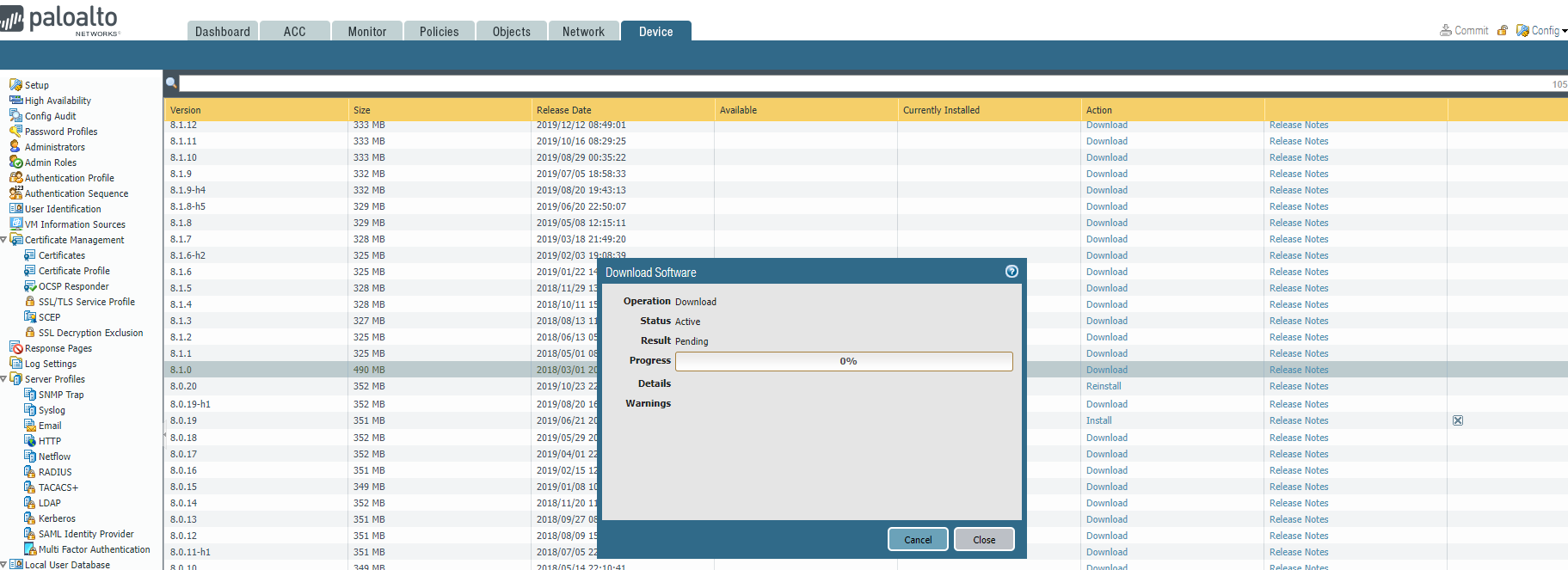
Step 8: Click Retrieve keys from license server



Step 9: Click Licenses



Step 10: Click check now for new versions that are available



Step 11: Do something else while waiting for download.

END!

Problems

As we had already configured this firewall with this exact UI before, we were done with the lab in less than 20 minutes. The overwhelming majority of the lab was actually spent trying to turn on the firewall and during the updating process.

Conclusion

In all fairness, we didn’t use newest features of the firewall, so it seems a bit odd to comment on its performance compared to the previous palo alto. I will say, though, that the updating process was a lot less buggy, which is a good thing.