LAB 2 – SOHO Configuration

P5 – Cybersecurity

Sirjan Singh

Lab 2 – PA-220 SOHO Setup

Background Info/Purpose: The purpose of this lab was to set up our PA-220 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.

This lab was an important precursor to the next lab which was updating the firewall because this enabled the firewall to connect to the internet. Without a connection to the internet, it would not be possible to update as the updates are installed online.

Lab Summary:

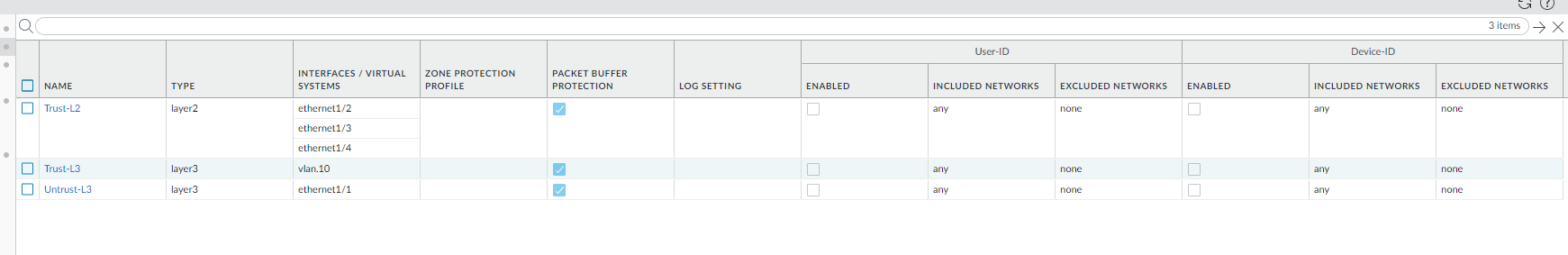
Wires Setup:

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

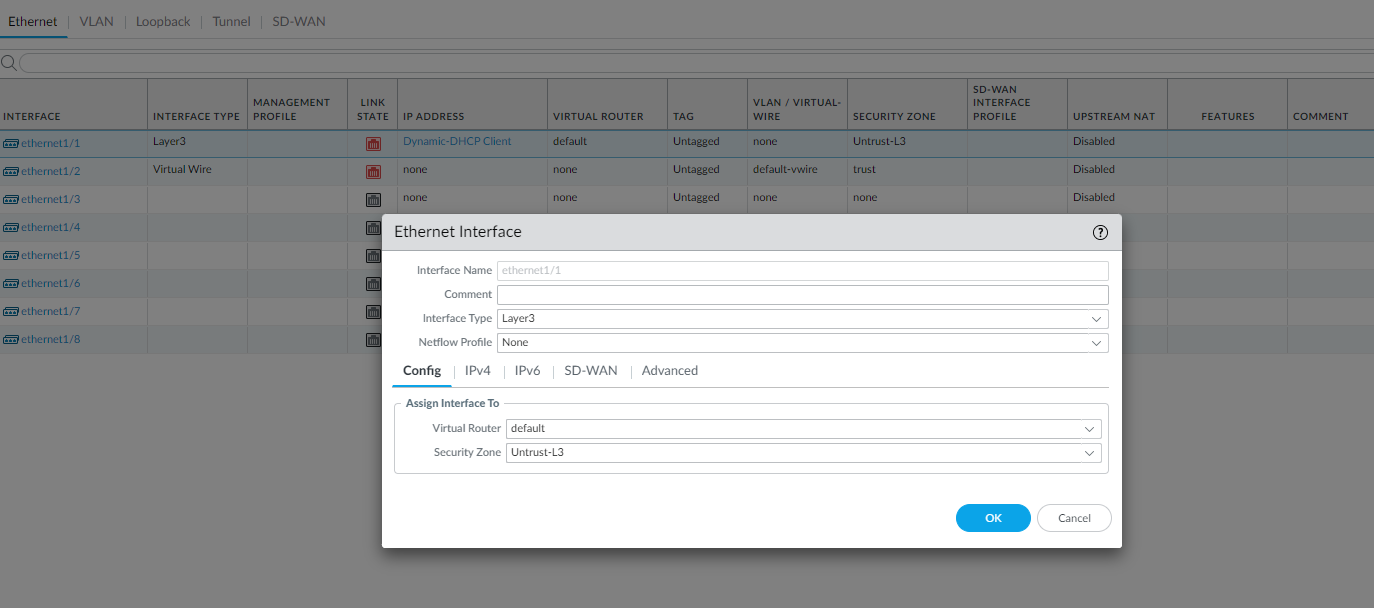
Ethernet 1/2 – 1/3 should connect to one of the PCs. Interface management should connect to another PC.

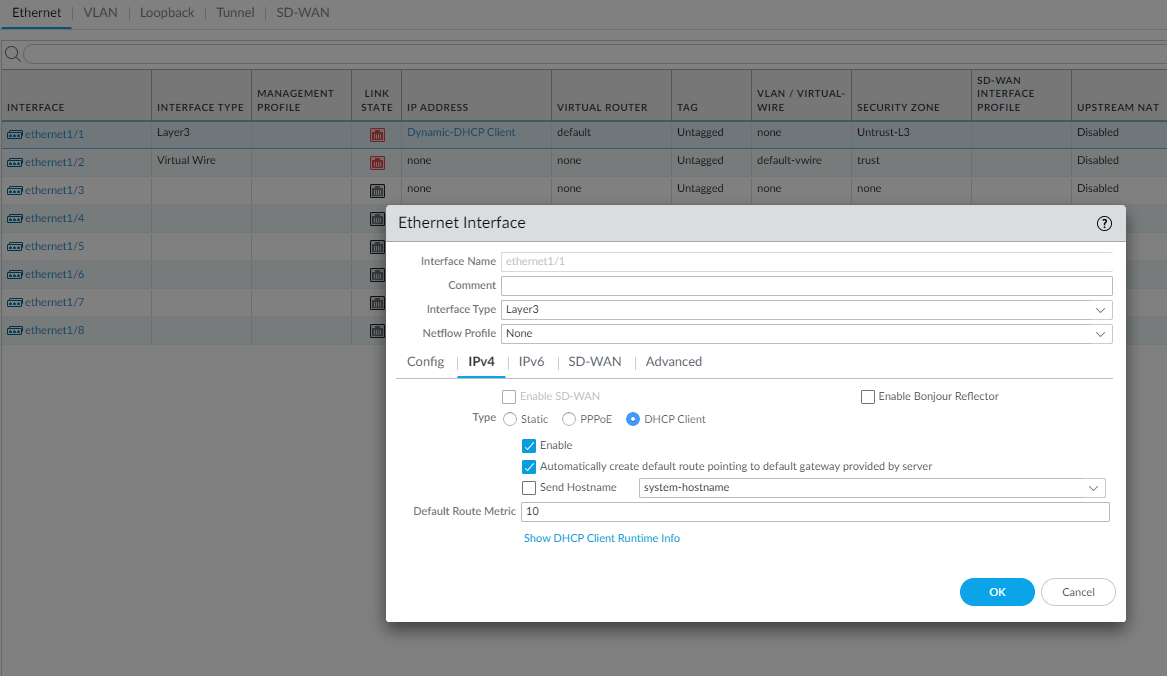
Assign yourself an ip address manually and go to 192.168.1.1 (the management interface ip) on an internet browser.

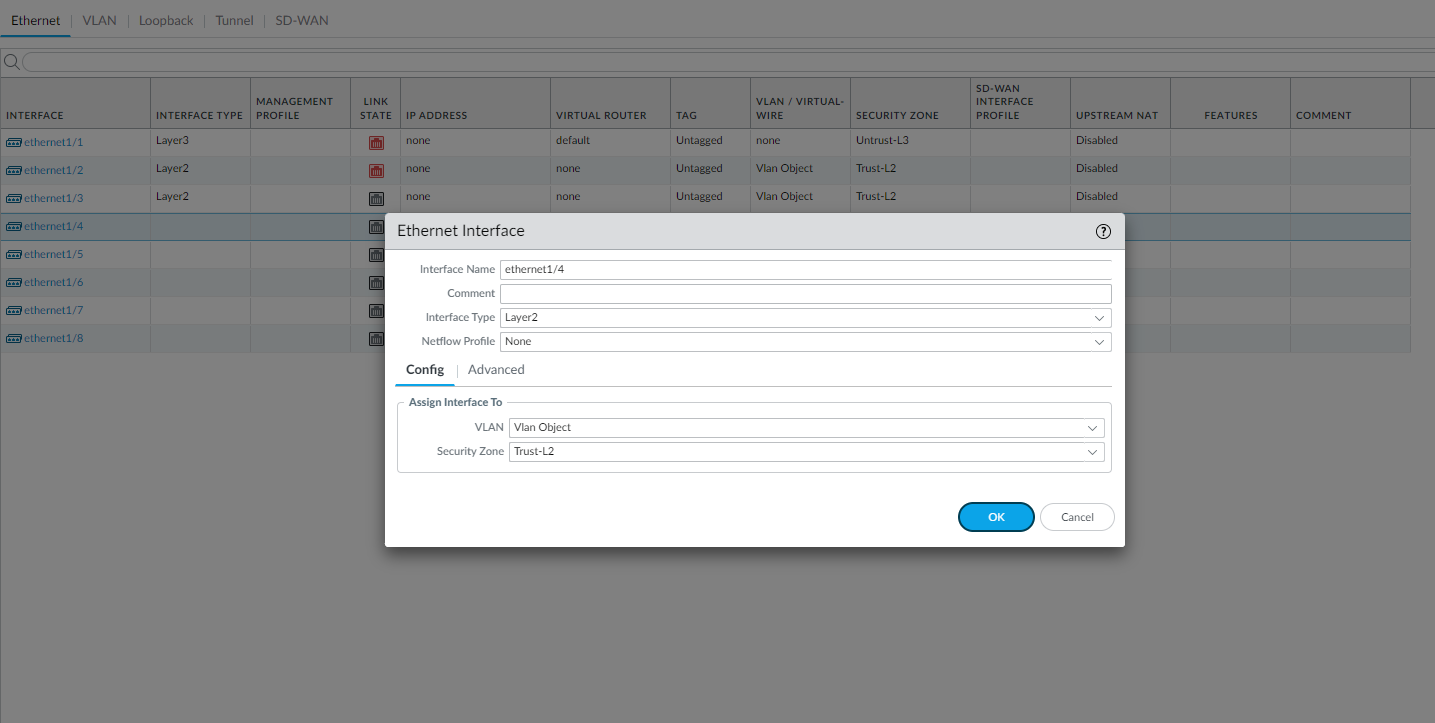
Step 1: Create 3 security zones under Network>Zones. Trust-L2, Trust-L3 and Untrust-L3. The ‘type’ of zone should be L2 or L3, accordingly.



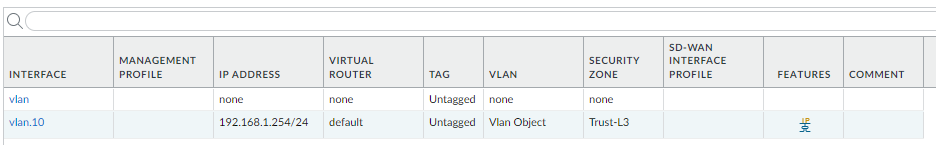
Step2: Go to network>interfaces. Et1/1 should be in layer 3 and in untrust layer 3. Et 1/ 2-4 should be in layer 2 and in trust-L2. Ethernet 1/1 should be a dynamic dhcp client. Virtual router for all should be set to default.



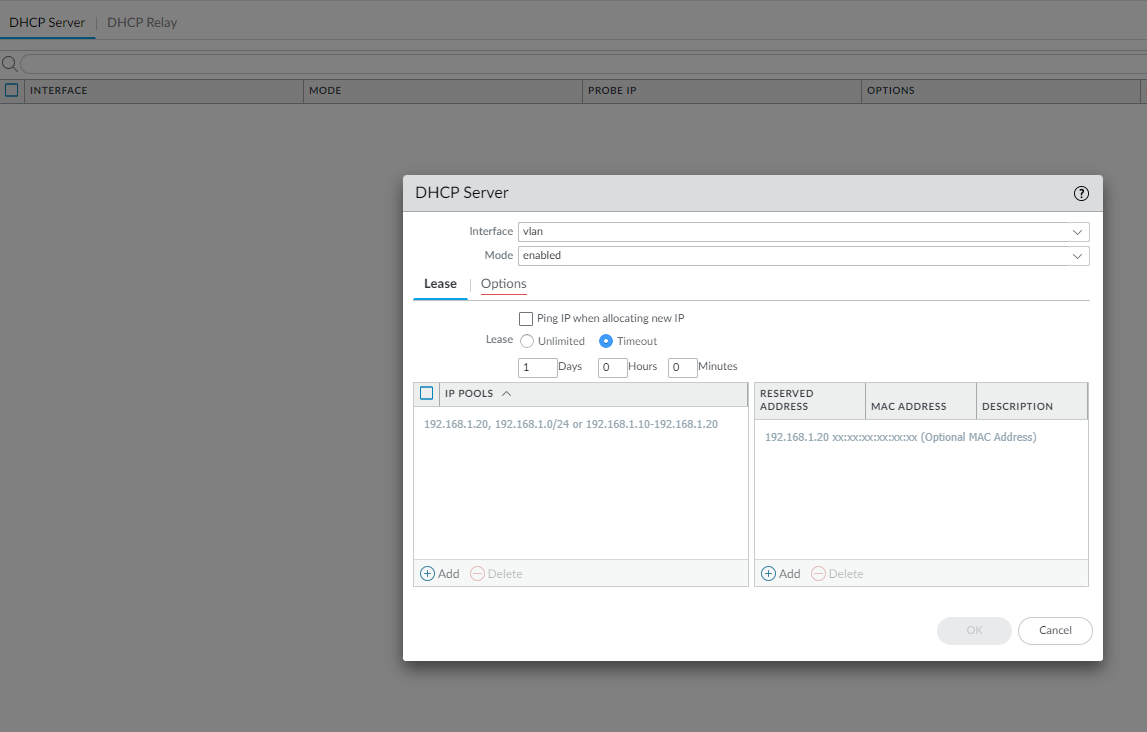


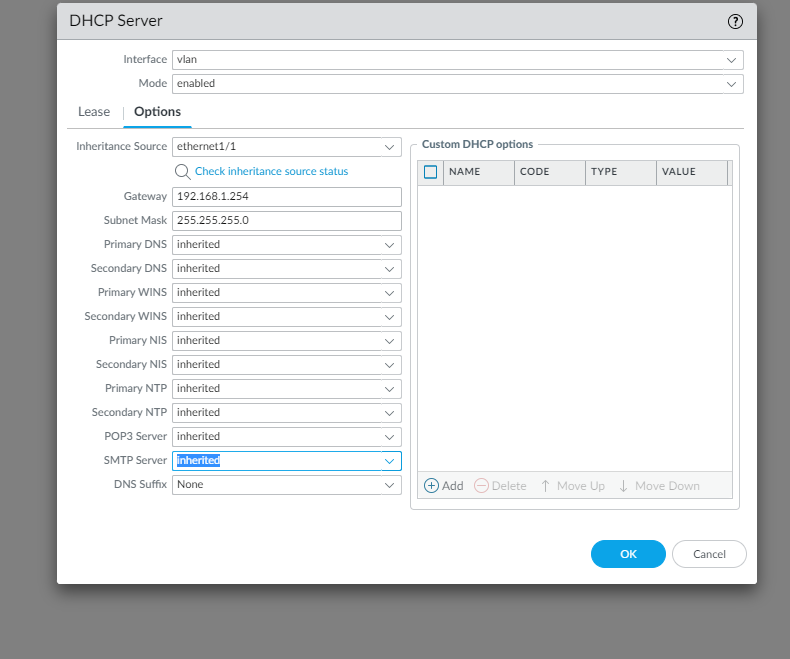


Step 3: Go to network > interfaces > vlans. Click add to add a vlan. Set vlan number. For Vlan, use vlan object and security zone should be trust-L3. For the ip address, use the 192.168.1.254/24 (network that the default gateway is in).

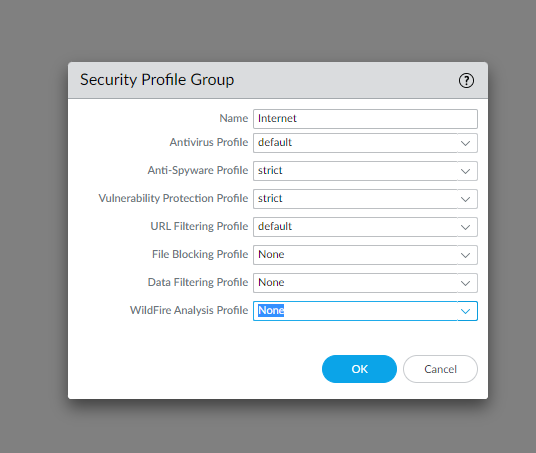


Step 4: Go to network > dhcp. Click add and select vlan for the interface that you just created (e.g., vlan.10). mode should be enabled, lease should timeout in 1 day, and the ip pool should be 192.168.1.2 – 192.168.1.253, or anything in between. Then go to options and select inheritance source to be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

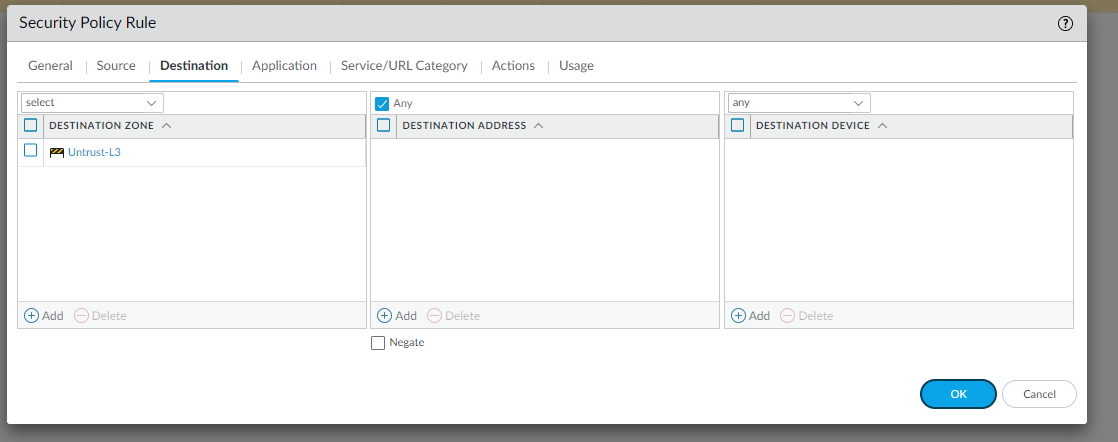




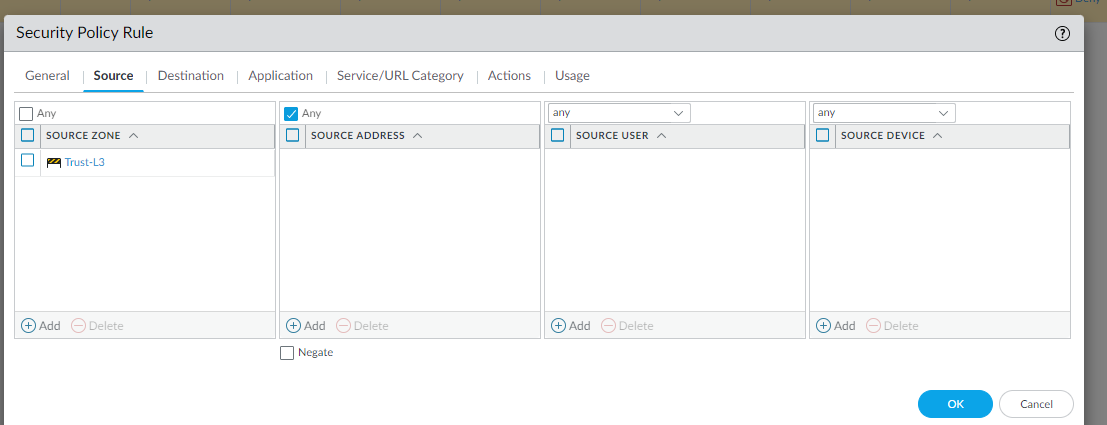
Step 5: go to object > security profile group. Click add and pick name. Settings should be as shown:



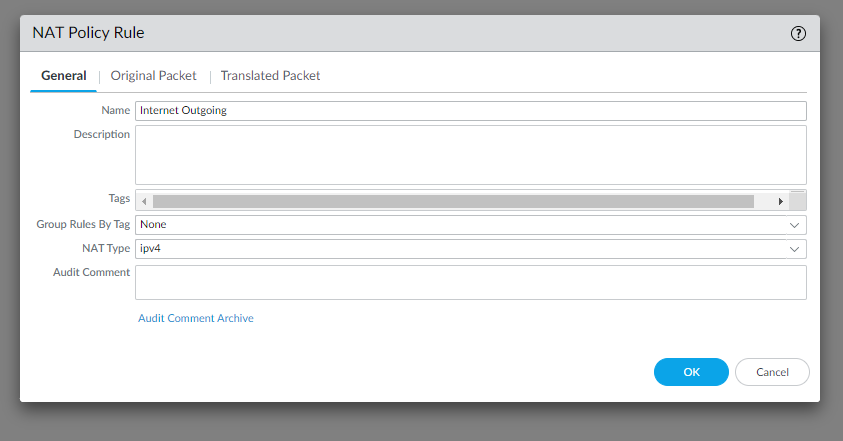
Step 5 cont.: Destination zone should be Untust-L3.



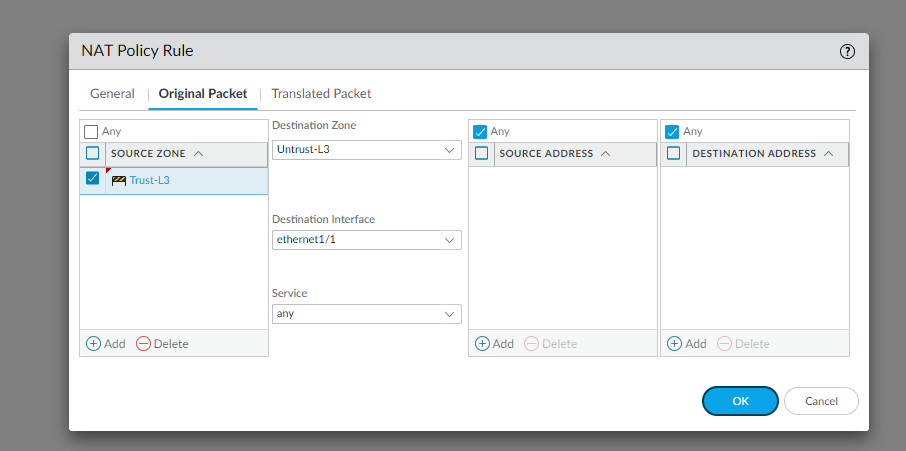
Step 5 cont.: Source should be in trust-L3:



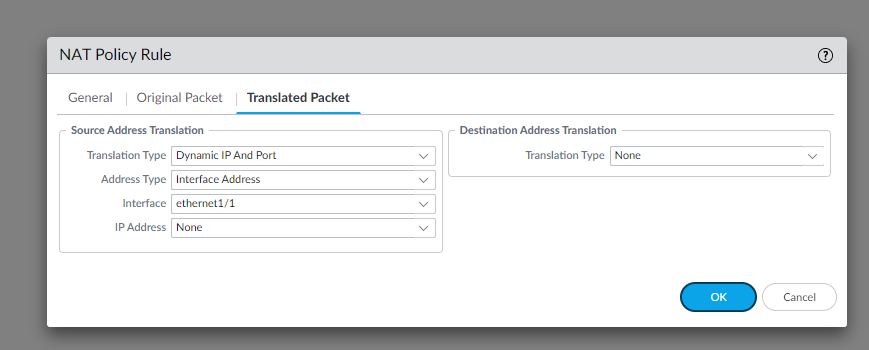
Step 6: Go to policies NAT and click add. Name it internet outgoing and nat type should be ipv4.



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:



END!

Lab Commands/configurations: No commands required for this lab because we didn’t use the console, only web interface to manage firewall as shown in lab summary.

Problems: we encountered many problems during this process. The first one was that when we tried to commit changes after making zones, we weren’t able due to invalid virtual wires. The solutions were to delete the virtual wires and then it worked.

Another major problem we faced was that when we tried to configure out DHCP server, the management interface did not let us pick the vlan.10 that we had created. The reason for this was that we had set the vlan to be a DHCP client, but we were supposed to manually enter the default gateway’s network (192.168.1.254/24).

A silly problem that we ended up having to solve multiple times was that our pcs weren’t able to detect the wired ethernet connection. This was because our ipv4 settings weren’t in DHCP mode.

Conclusion: This lab taught us how to troubleshoot a problem that we made due to a very tiny error that restricted the DHCP server from working. After these configurations all work, you no longer need to connect the management port of the firewall to your pc. You can instead connect your management interface to one of the interfaced that is configured to be in trust-L2. You can connect both your pcs to such ports too, and then both your pcs can access the management interface as it is in the same LAN.

Teacher Signoff: