Palo Alto Firewall SOHO Configuration

Reed Holman | Cyber Security | 10/3/2022



Purpose: The purpose of this lab was to set up our PA-220 firewall that had no previous configuration. We wanted to set up our firewall with a Small Office Home Office configuration. We would set up layers of security on different ports and configure one port to reach the internet.

Background Info: A SOHO configuration is designed to be optimized for a small LAN setup. This allows for effective communication between a small number of devices and a way for them to access the internet.

On the firewall itself we created three different security zones. The purpose of these zones we created is to have different polices depending on what type of traffic needed to be allowed. We then configured our ethernet 1/1 port to connect to the internet and we assigned it to the appropriate security zone.

We also need to set up a VLAN and put our Layer 2 ports in that VLAN. A Layer 2 port is a port that uses a physical address and communicates only within our LAN. A VLAN is a Virtual local area network which also lives in layer 2. You can create multiple VLANs within a single LAN. We also needed to configure an Outbound Internet Security Policy. This was where we were able to make changes to how our firewall accessed the internet.

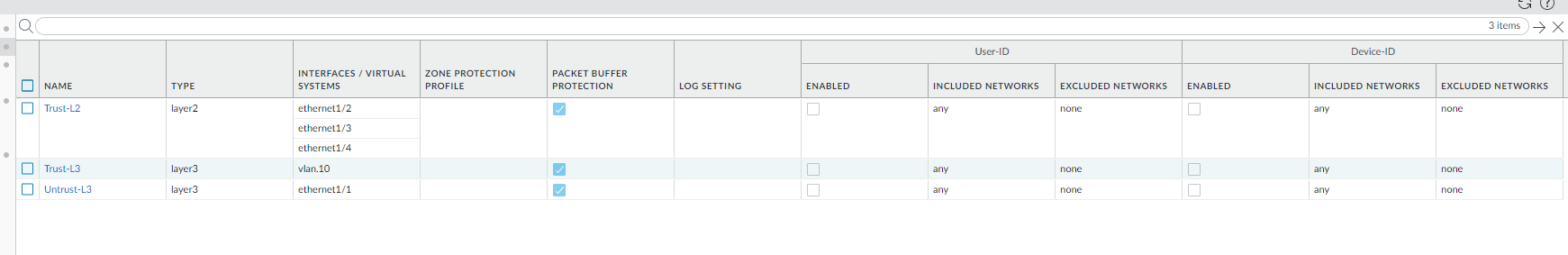
Wires Setup:

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

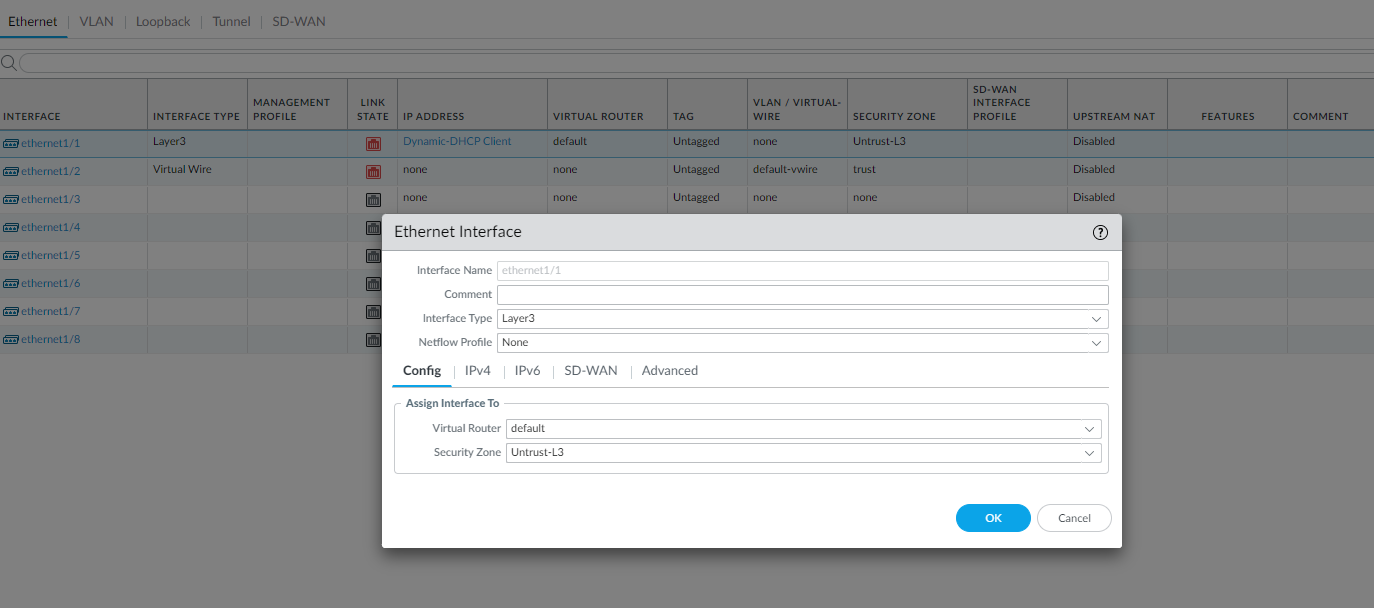
Ethernet 1/2 – 1/3 should connect to one of the PCs. Interface management should connect to another PC.

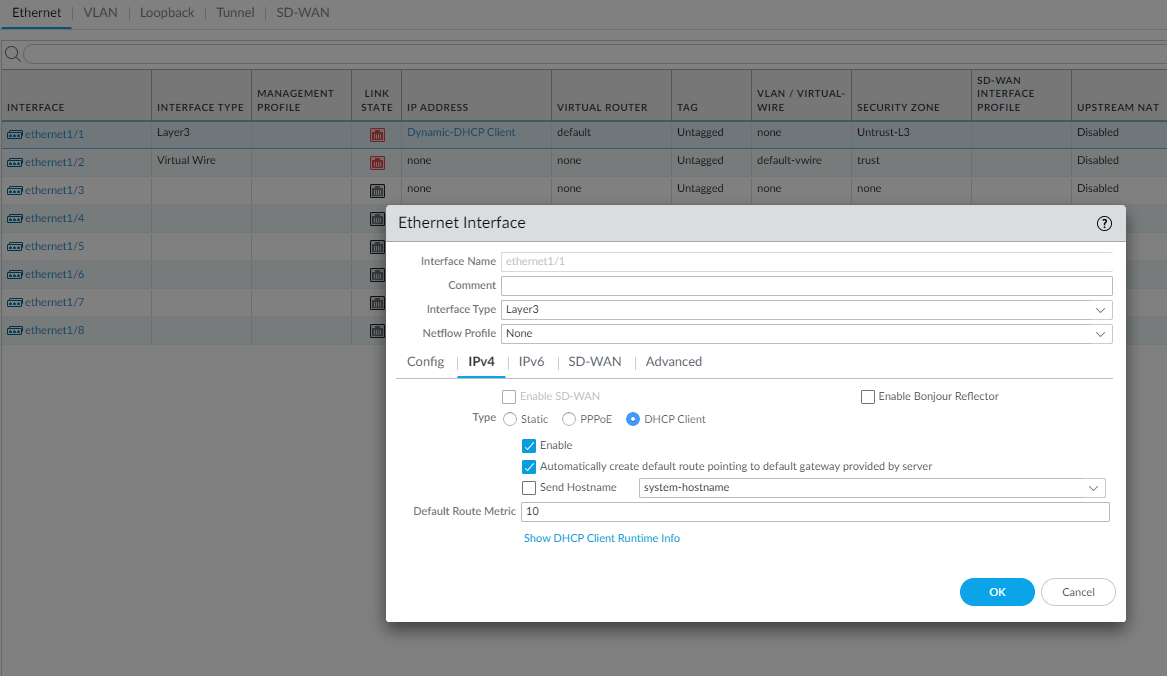
Assign yourself an ip address manually and go to 192.168.1.1 (the management interface ip) on an internet browser.

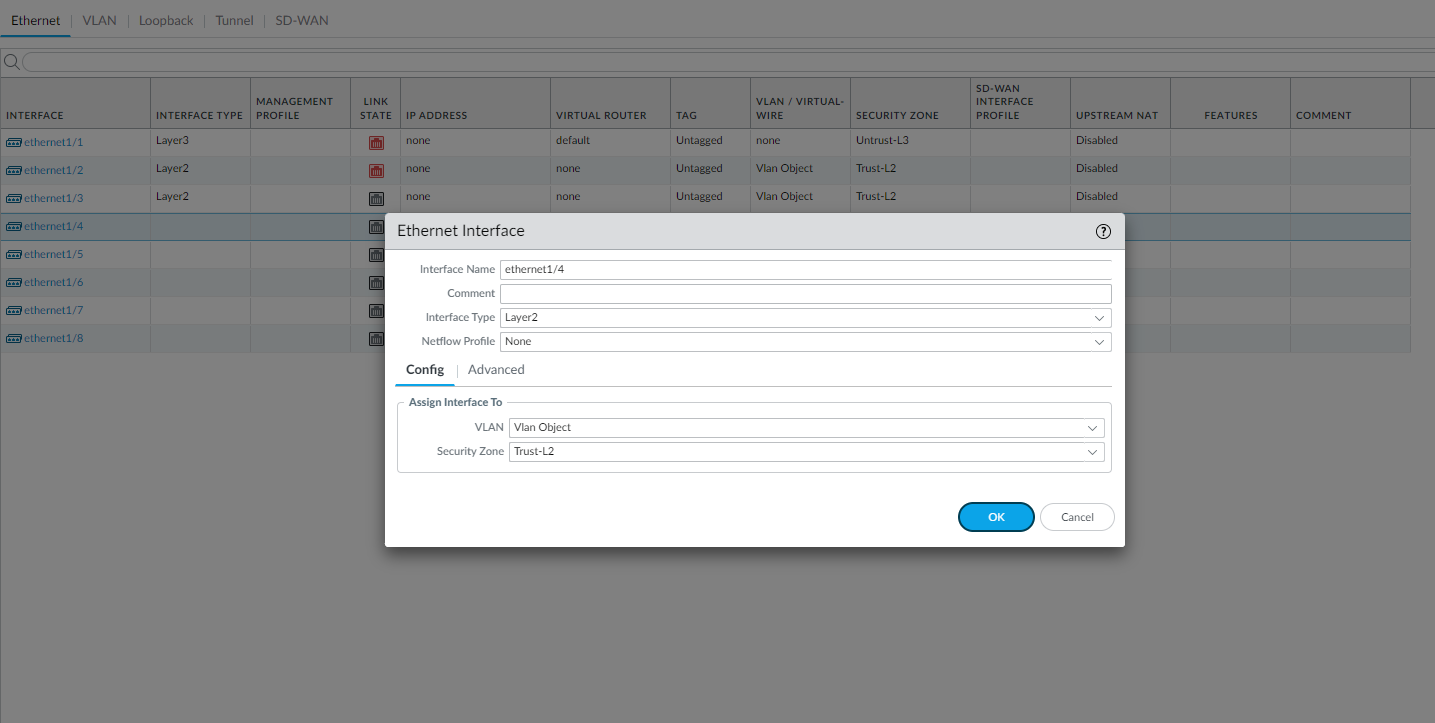
Step 1: Create 3 security zones under Network>Zones. Trust-L2, Trust-L3 and Untrust-L3. The ‘type’ of zone should be L2 or L3, accordingly.



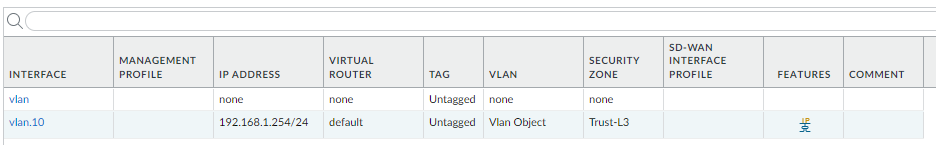
Step2: Go to network>interfaces. Et1/1 should be in layer 3 and in untrust layer 3. Et 1/ 2-4 should be in layer 2 and in trust-L2. Ethernet 1/1 should be a dynamic dhcp client. Virtual router for all should be set to default.



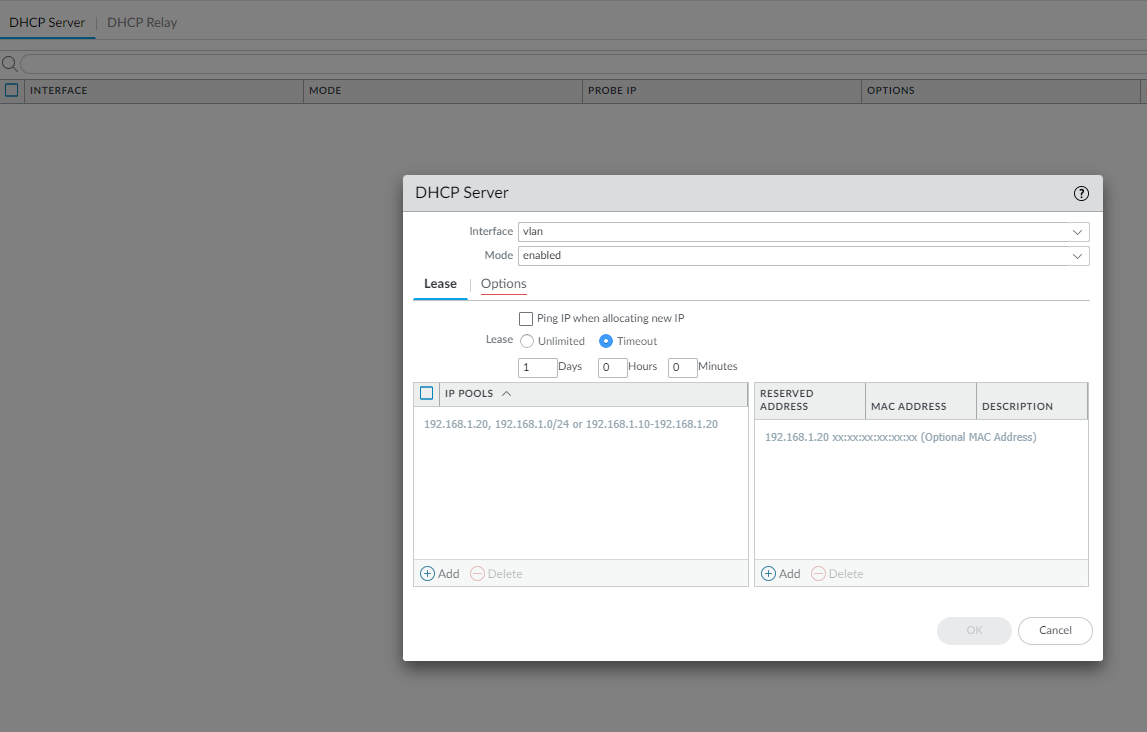


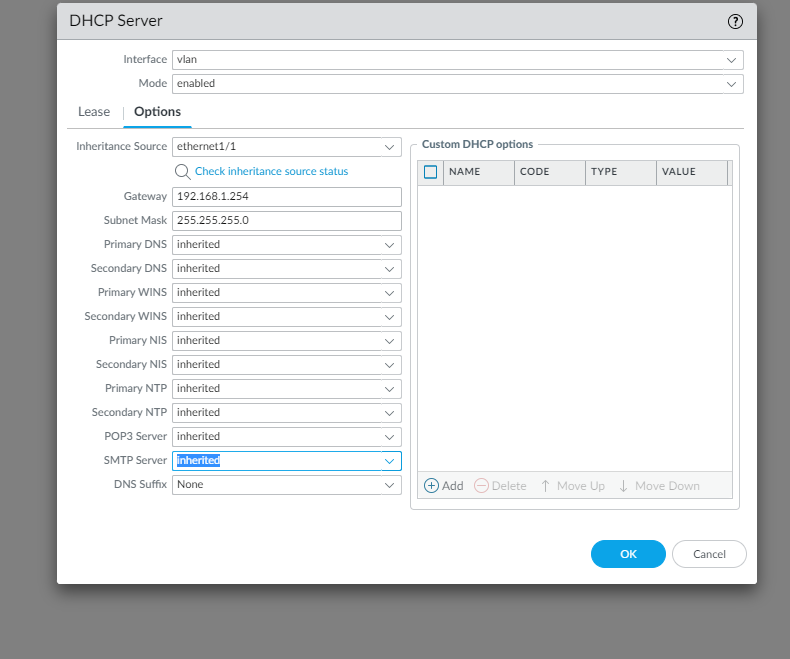


Step 3: Go to network > interfaces > vlans. Click add to add a vlan. Set vlan number. For Vlan, use vlan object and security zone should be trust-L3. For the ip address, use the 192.168.1.254/24 (network that the default gateway is in).

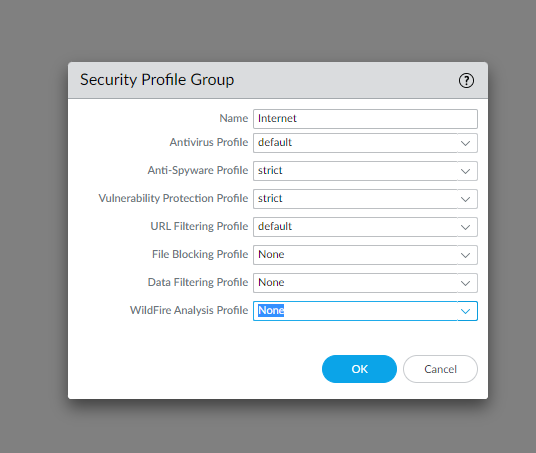


Step 4: Go to network > dhcp. Click add and select vlan for the interface that you just created (e.g., vlan.10). mode should be enabled, lease should timeout in 1 day, and the ip pool should be 192.168.1.2 – 192.168.1.253, or anything in between. Then go to options and select inheritance source to be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

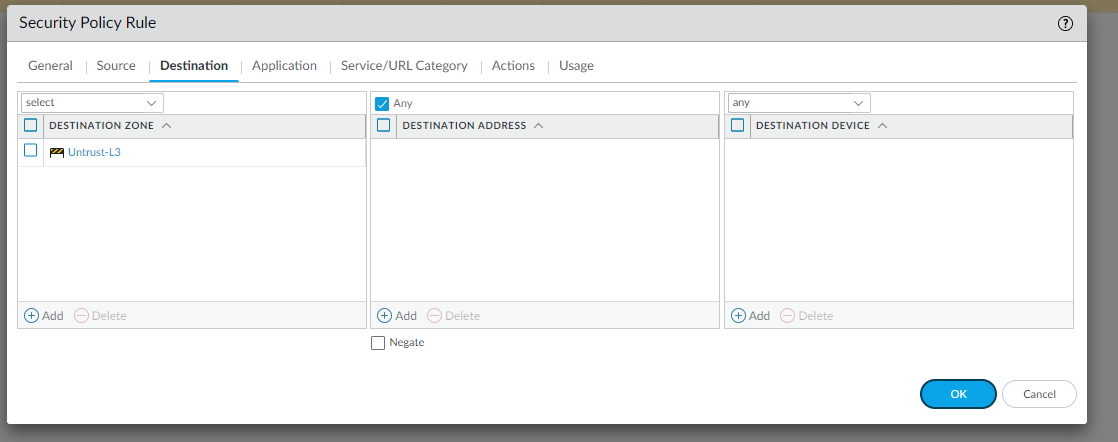




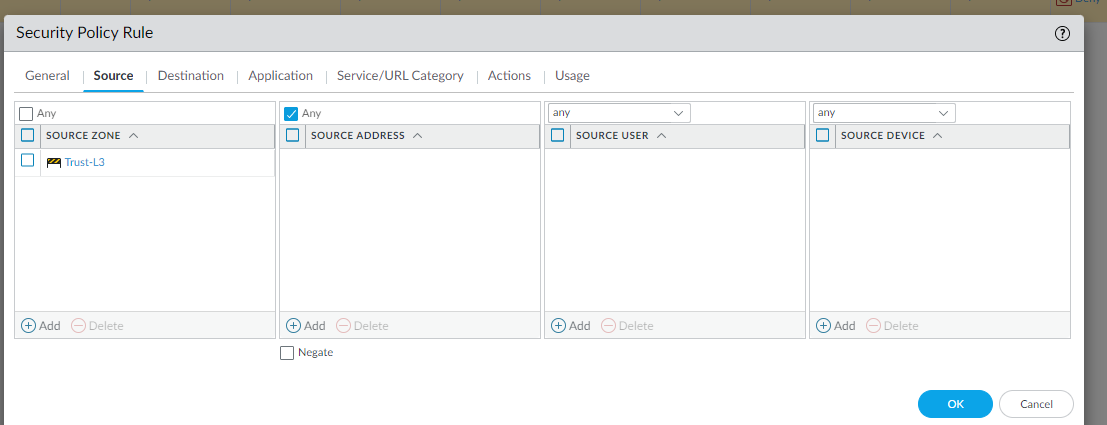
Step 5: go to object > security profile group. Click add and pick name. Settings should be as shown:



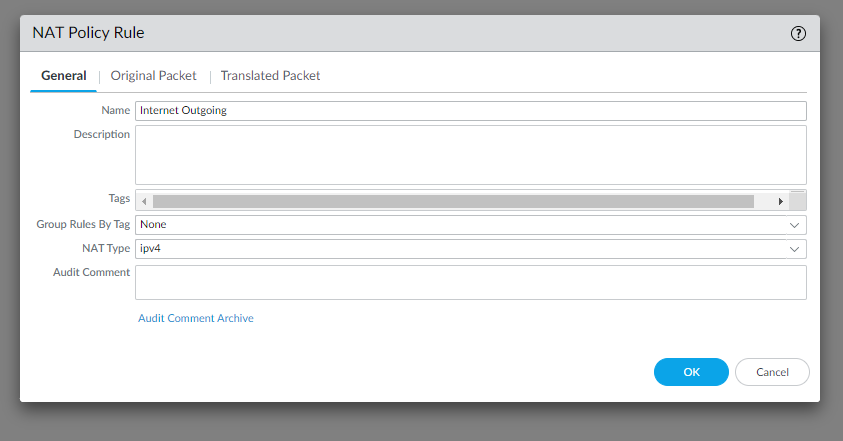
Step 5 cont.: Destination zone should be Untust-L3.



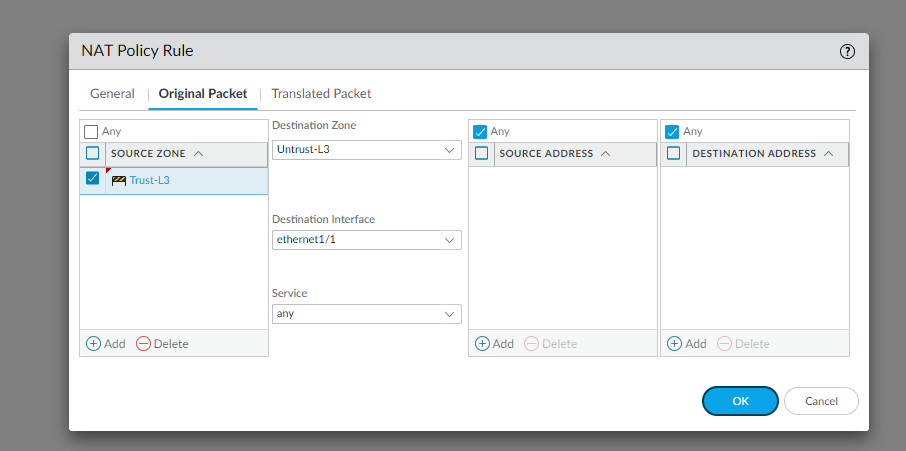
Step 5 cont.: Source should be in trust-L3:



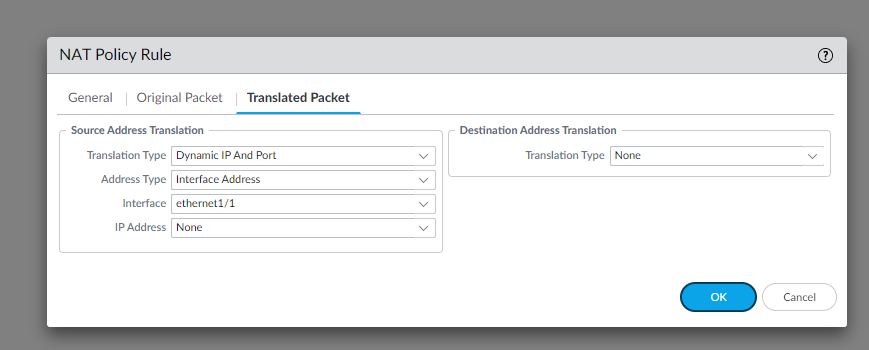
Step 6: Go to policies NAT and click add. Name it internet outgoing and nat type should be ipv4.



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:



Done

Problems: We had quite a few problems with this configuration. One of the first problems was when we got an error when trying to commit our changes. This was due to the fact that we still had virtual wires on our firewall. Once we deleted those wires, we were able to commit.

Another problem we had was when setting up our DHCP client. It would not let us select the new vlan we created. We had the vlan configured as a DHCP client. That was the issue and once we changed it manually to our default gateway it worked.

The final problem we had was that we did not have our computers set up with DNS so we could not get an IP from the firewall.

Conclusion: This taught us how to successfully configure our router with a SOHO configuration. How important it is to get the DHCP server to be working and fully function. It taught us how once fully configured you no longer need to plug directly into the management port. You can connect the management port to another interface you already configured that is in the same trust layer. That allows you to access the management port from a different interface and have multiple pcs in the management interface at the same time.