

**PALO ALTO 410 SOHO**

****Brendon Ahn | Cybersecurity | 2022-2023

**Purpose:**

To configure SOHO on the new Palo Alto 410 Firewall

**Background:**

The PA 410 is a newer version of the PA 220. The configuration of the two are very similar but there are some new things. There is a mode now where you have to switch to manually configure. This mode is called ZTP and you have to configure on the firewall to switch the mode and then reset. There are less rules in the ZTP mode so you don’t have to delete any pre existing rules. You still have to delete the virtual wire to set up SOHO though.

The GUI looks the same as the most recent GUI update for the PA 220 with some minor almost unnoticeable change. The Firewalls speed is still a little bit slow, but it feels faster than the 220. There are less ports on the 410 but the 410 comes with a much sleeker look. It has 2 USB ports a console port and 7 ethernet ports. It has one management port. This is very different from the PA 220.

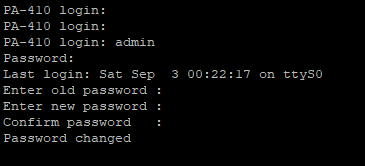
SOHO itself runs smoothly and configuring the PA 410 had very little issues. The Configuration took 1 try the only thing that I expected that wasn’t there was because the startup time was very long. If there was a difference between the 410 and 220 startup time, there wasn’t much as they both took 10 minutes +. Because we got the Firewall new there was no need to factory reset which was nice.

**Lab Summary:**

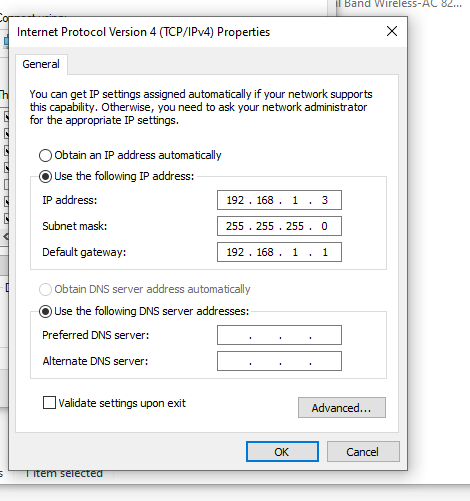
We had to setup SOHO configuration like on the PA 220 on the newer PA 410 that we got new from Mr. Mason

**Lab Procedure:**

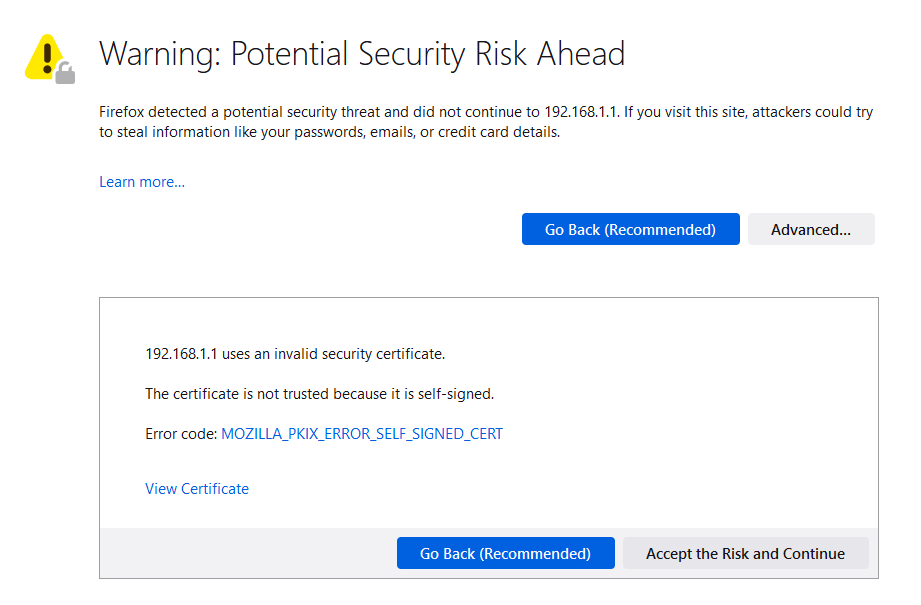
1. Configure a new password - Default is Username: admin password: admin



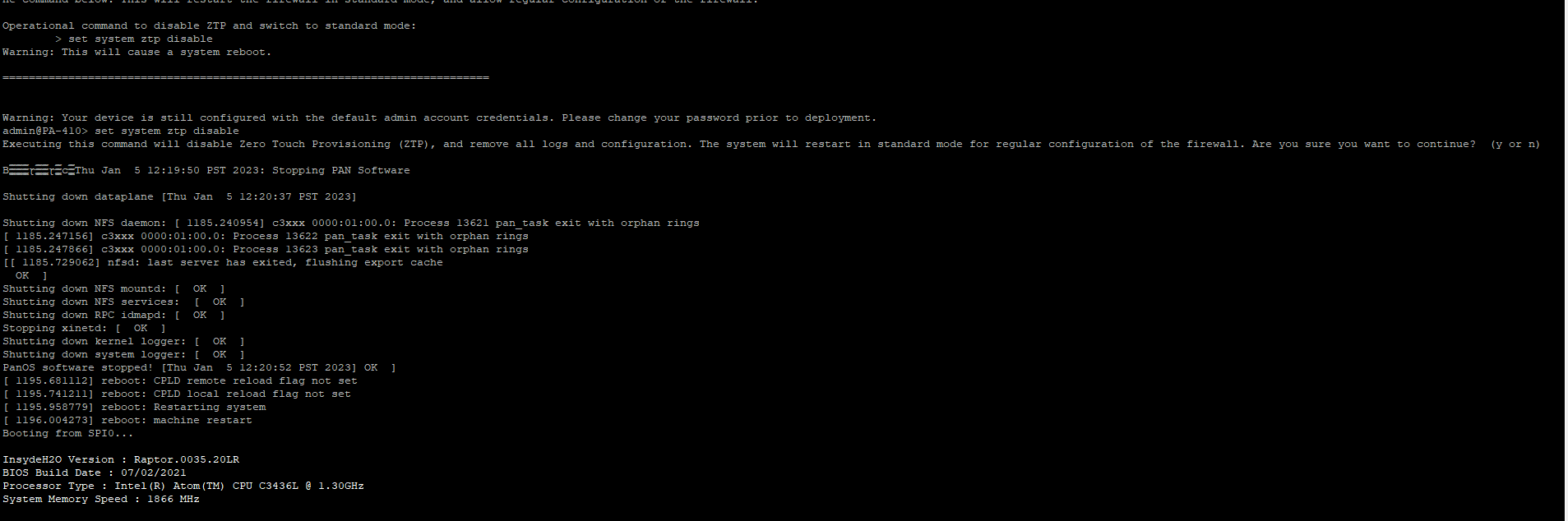
1. Change your ipv4 address to one in the 192.168.1.0/24 range that isn't 192.168.1.1



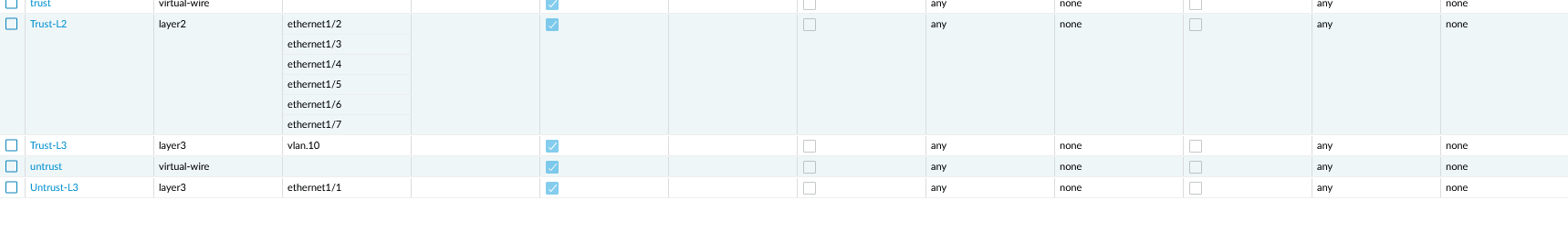
1. Go to [https://192.168.1.1](https://192.168.1.1/) and accept risks and continue



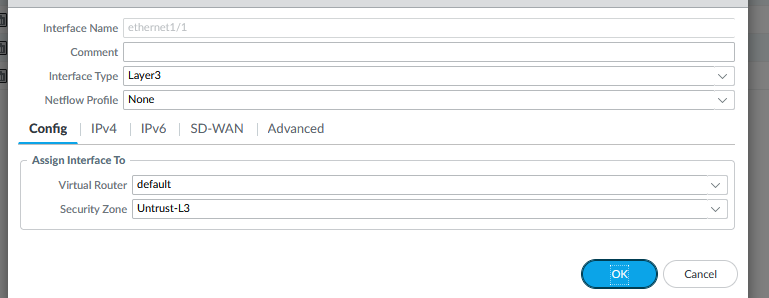
1. Step 4 do a set system ztp disable command to go from ztp mode to standard for configuration



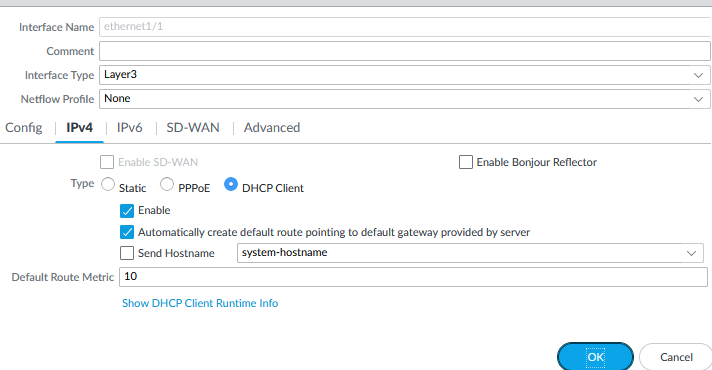
1. Create Security Zones 1. Go to: Network > Zones and click Add. 2. Create 3 zones: Untrust-L3, Type Layer3 Trust-L3, Type Layer3 Trust-L2, Type Layer2



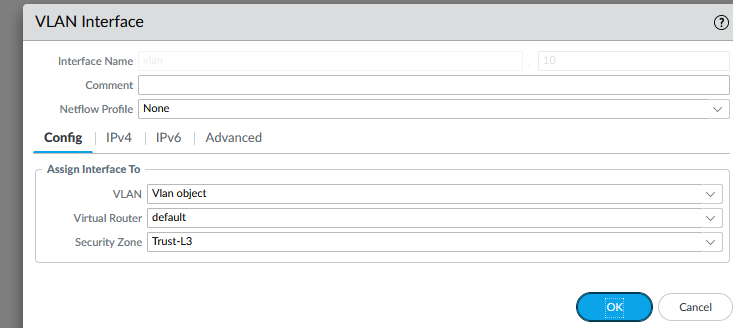
1. Go to Network > Interfaces on the WebGUI and configure ethernet 1/1. 2. On Config Configure the ethernet1/1 Interface Type as Layer3. Set Virtual Router to default. Set Security Zone to Untrust-L3



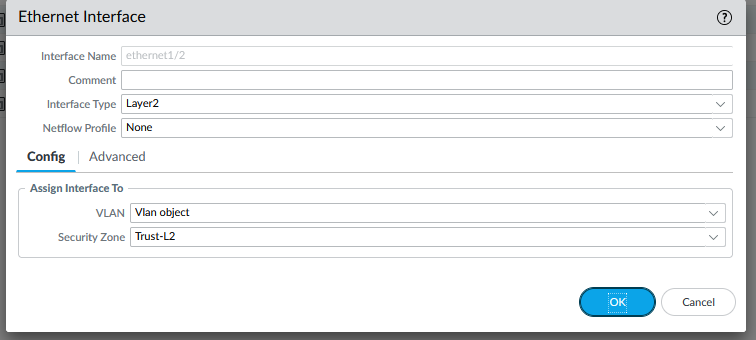
1. Under IPv4 click DHCP Client



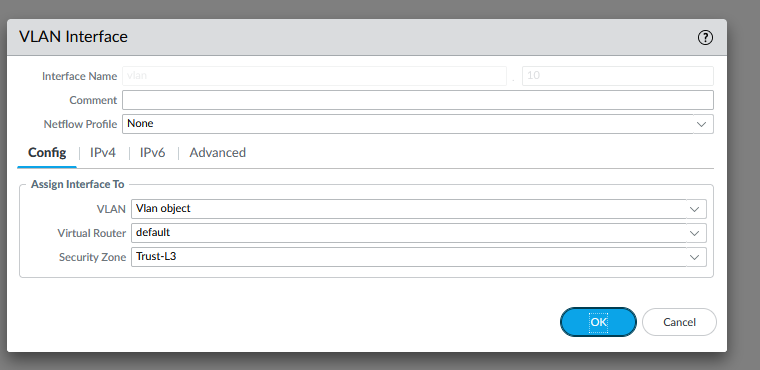
1. Create a VLAN Object 1. Go to Network > VLANs and click Add. 2. Enter a name and select 'v' for VLAN Interface

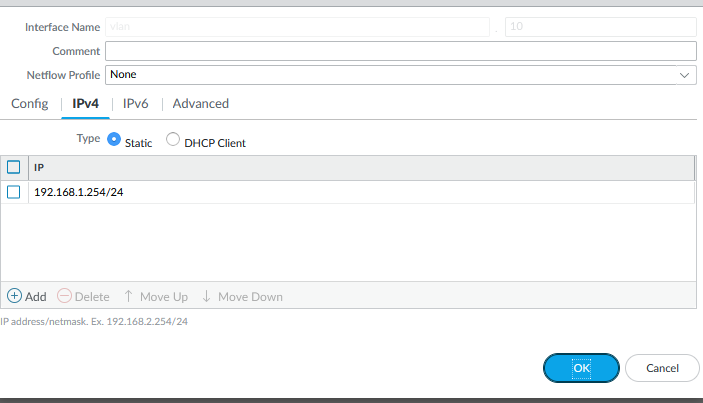


1. Go to Network > Interfaces > Ethernet. 2. Edit the following settings for the ethernet1/2, ethernet1/3 and ethernet1/4 interfaces: Interface Type: Layer2 Netflow Profile: None VLAN: VLAN Object Security Zone: Trust-L2// Do all interfaces

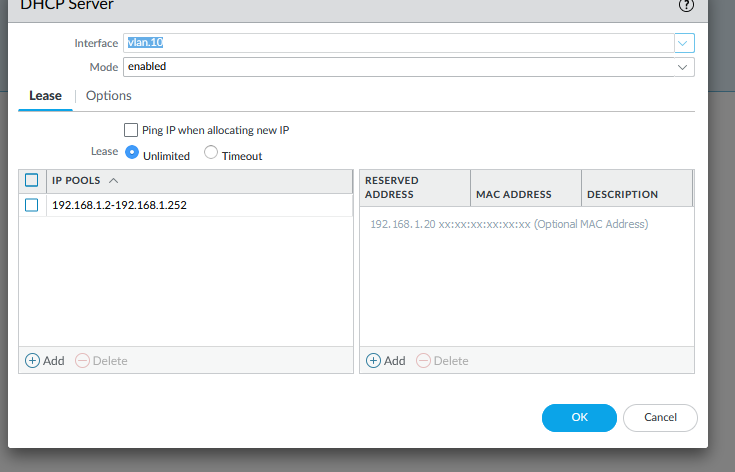


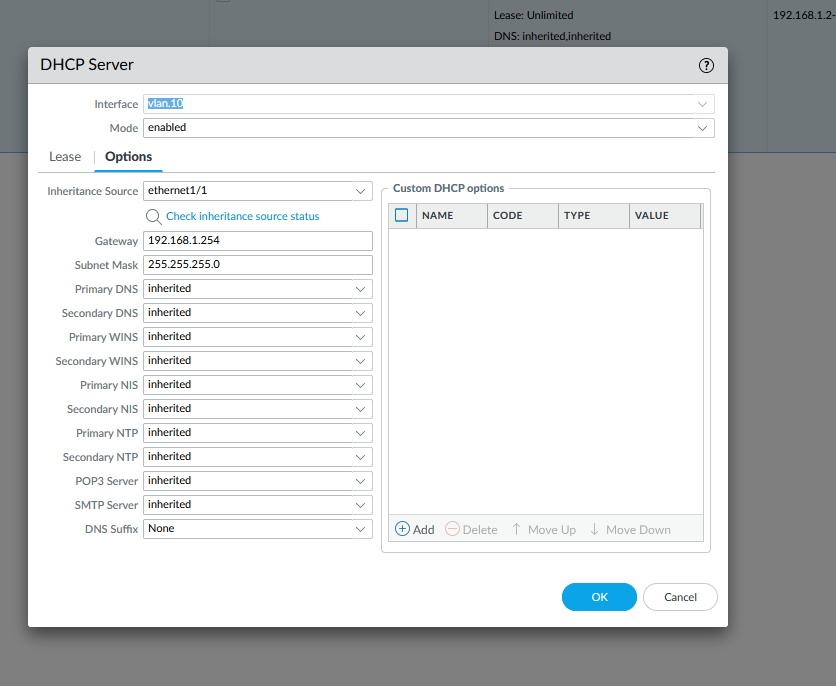
1. Configure the VLAN Interface Go to Network > Interfaces > VLAN and edit the following settings: Config tab VLAN: VLAN Object Virtual Router: default Security Zone: Trust-L3. Click Add and enter IP address 192.168.1.254/24



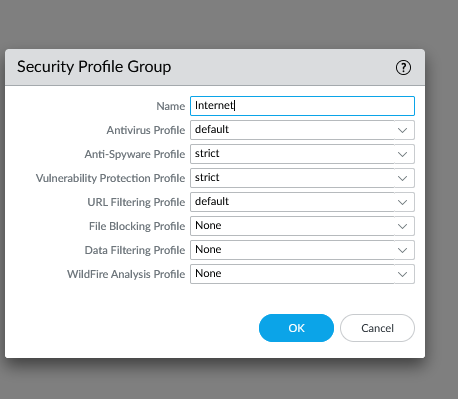


1. Configure the DHCP Server 1. Go to Network > DHCP > DHCP Server. 2. Click Add. 3. Edit the DHCP Server settings, as shown:

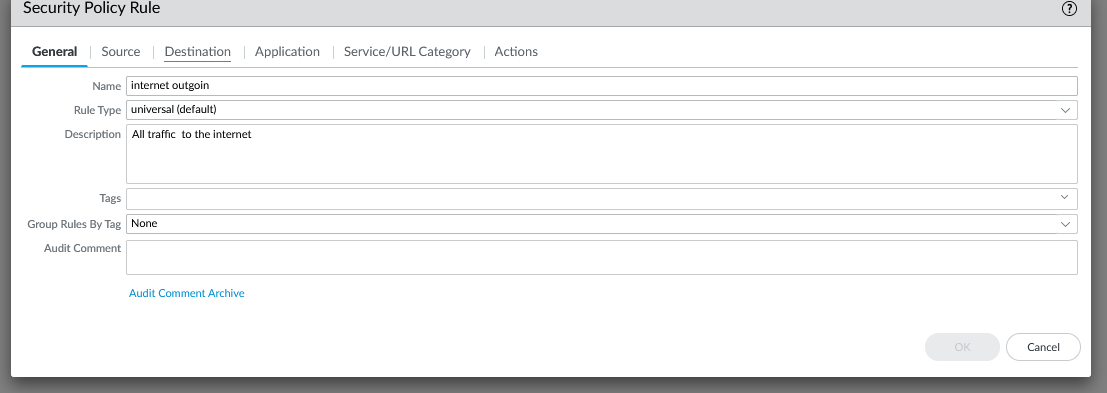


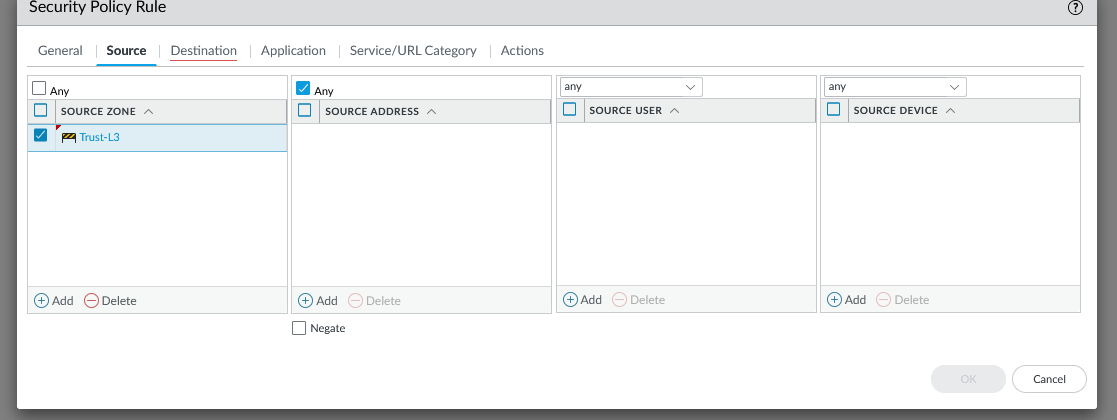


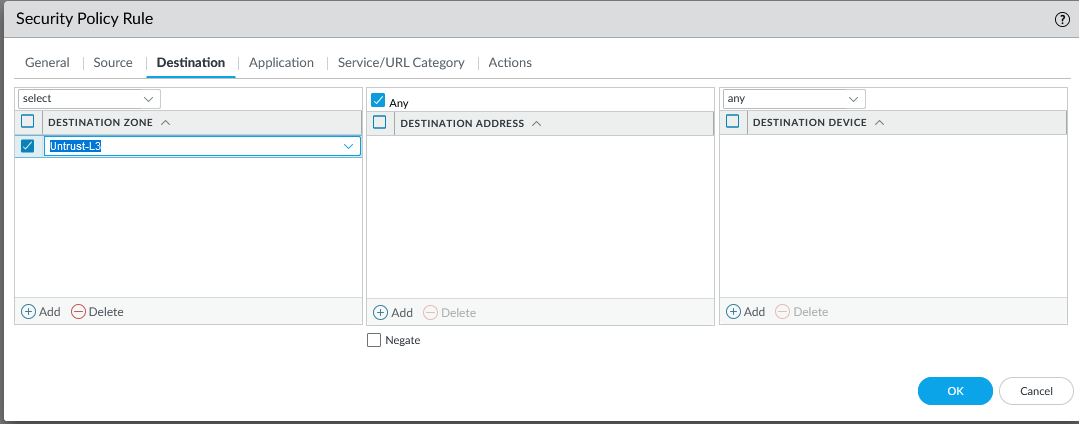
1. Define a Security Profile Group 1. Go to Objects > Security Profile Groups and click Add. 2. Edit the following Security Profile Group settings as desired:

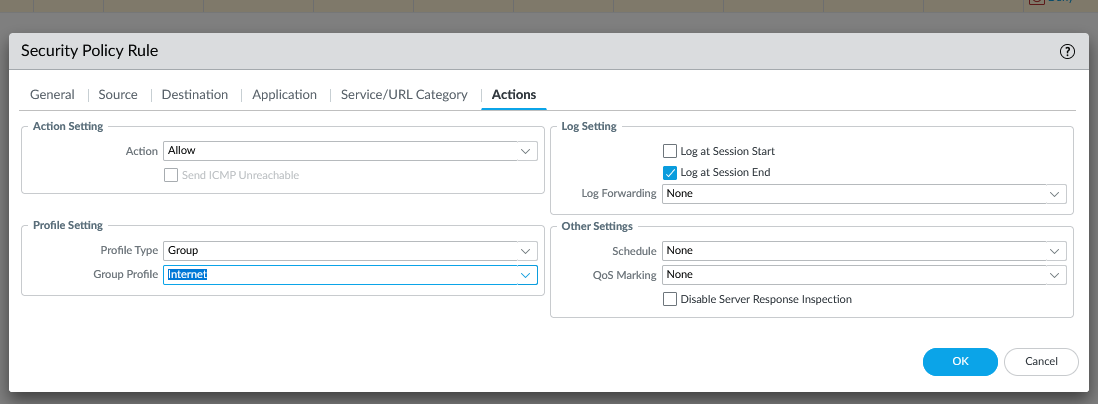


1. Configure Outbound Internet Security Policy 1. Go to Policies > Security and click Add. 2. Enter a Name and Description: Add the source zone Add the destination zone: Specify the action as Allow and complete the Profile Setting:

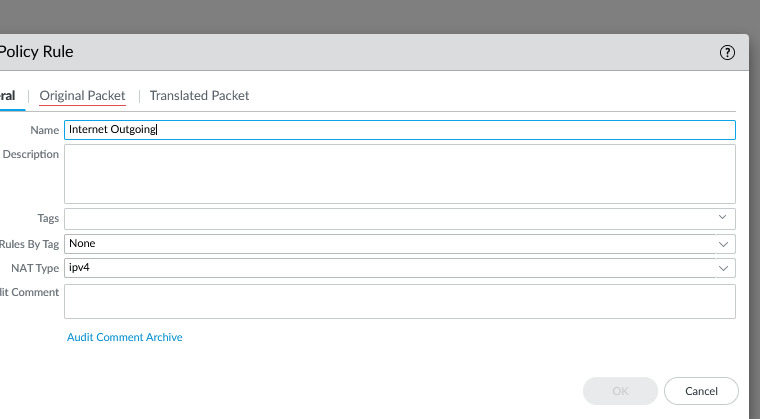


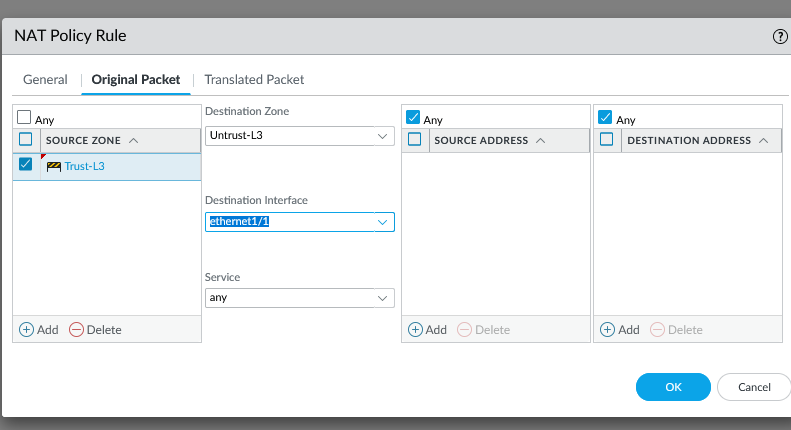


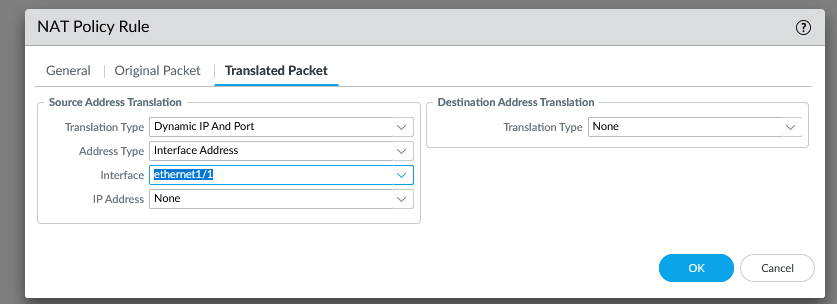




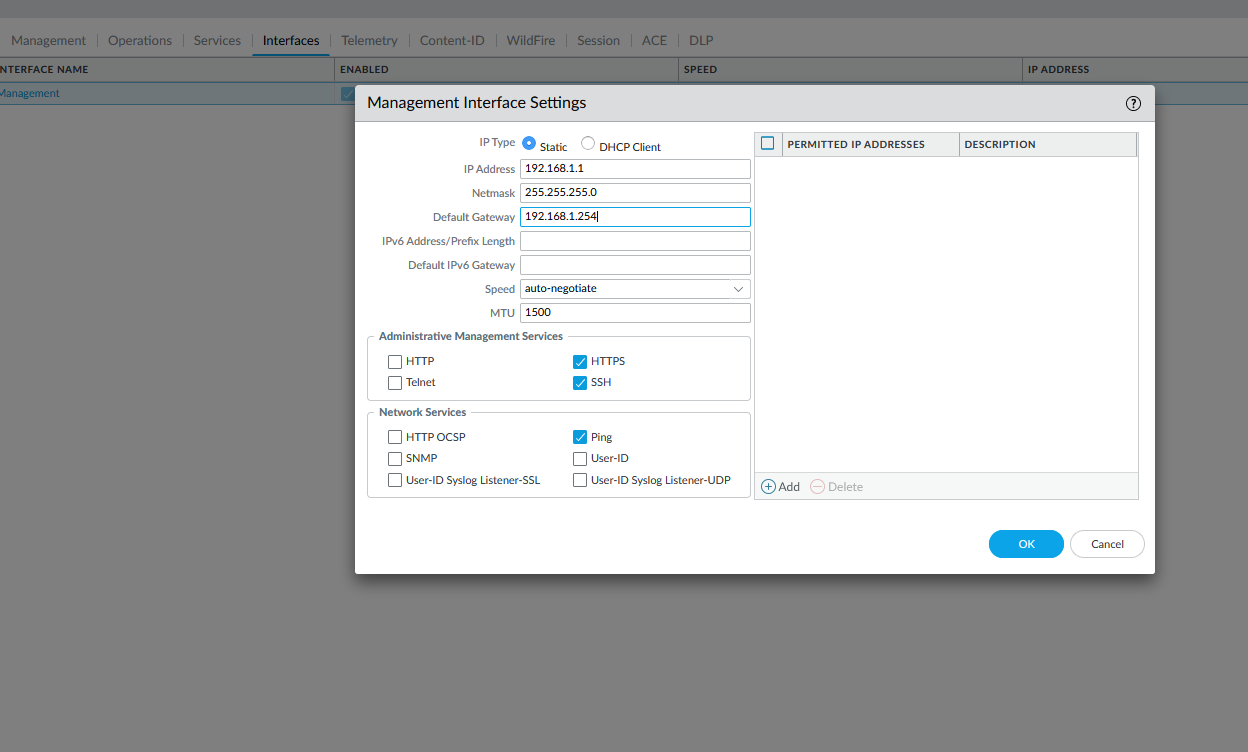
1. Configure Outbound Internet NAT Policy 1. Go to Policies > NAT and click Add. 2. Enter a Name and check IPv4 for NAT Type: On Original Packet, specify the Source Zone, Destination Zone, and Destination Interface: On Translated Packet, set: Translation Type: Dynamic IP And Port Address Type: Interface Address Interface: ethernet1/1



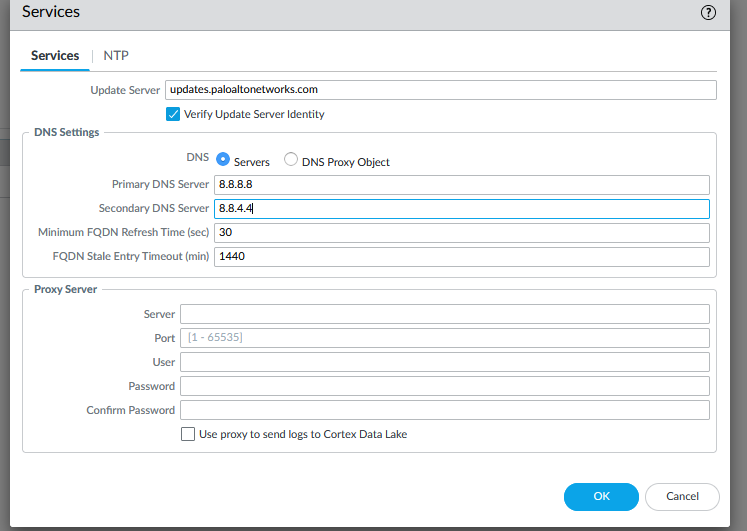




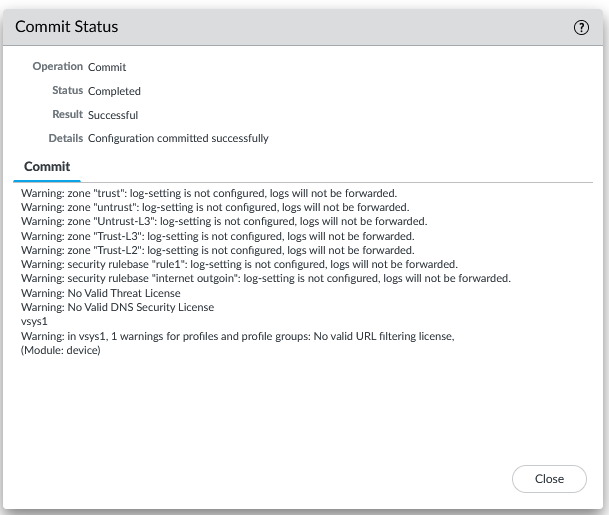
1. Configure the MGMT IP Go to Device > Setup > Management and specify the following Management Interface Settings: IP Address Netmask Default Gateway



1. Set DNS for MGMT 1. Go to Device > Setup > Services. 2. Enter the DNS server IPs. For example: Google DNS IP's 8.8.8.8 and 8.8.4.4. Note: This should already have been configured to install licenses on the device. If the licenses have not been installed on the device, then the firewall will not be able to reach the license server with these settings



1. Delete Vwire
2. Commit



**Problems:**

There were no issues with the configuration, but my partner was sick for the day we configured this, so it took a longer time than expected

**Conclusion:**

We configured SOHO on the new PA 410 just like on the PA 220 with no real issues. The speed of the PA 410 still left room to be desired, but the configuration felt smooth and easy.