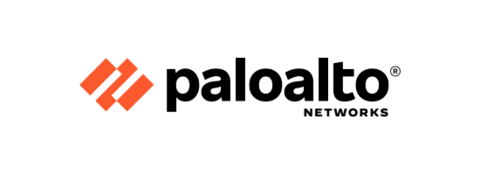


Palo Alto 410 SOHO Configurations

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose:**

The purpose of this lab was to configure SOHO on a Palo Alto 410 firewall.

**Background:**

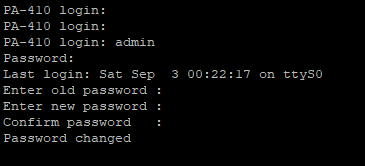
The Palo Alto 410 firewall, a newer version of the Palo Alto 220 router, allows us to prevent and see unknown threats and secure everything. The Palo Alto 410 firewall is one of the most effective SMB firewalls, with high quality performance with a management interface which is very easy to configure.

PA 410 firewalls are meant for 25-50 users, with 930 Mbps VPN throughput and with 1.7 Gbps firewall throughput. The PA 410 is quite reliable to protect security environments for a SOHO network. SOHO networks are single or small office/home office networks, which are used by privately-owned businesses that need to reach the internet for work. It’s crucial that their work is protected from viruses and other security threats since the businesses are mainly on the internet, and a Palo Alto 410 is an effective firewall to use for this.

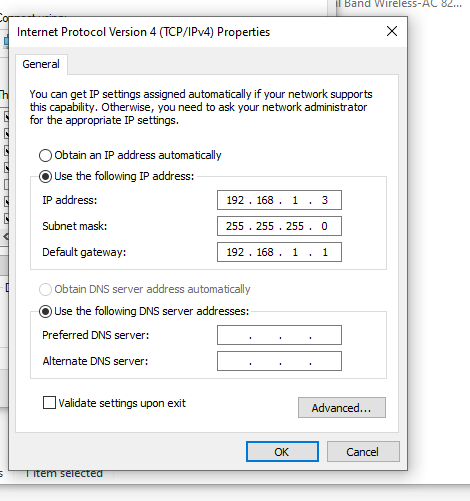
The Palo Alto 410 firewall not only prevents malicious activity concealed in encrypted traffic, but also identifies and categorizes all applications, on all ports, all the time, with a full layer 7 inspection. This enforces security for a network, specifically our SOHO network as configured in this lab.

**Lab Procedure:**

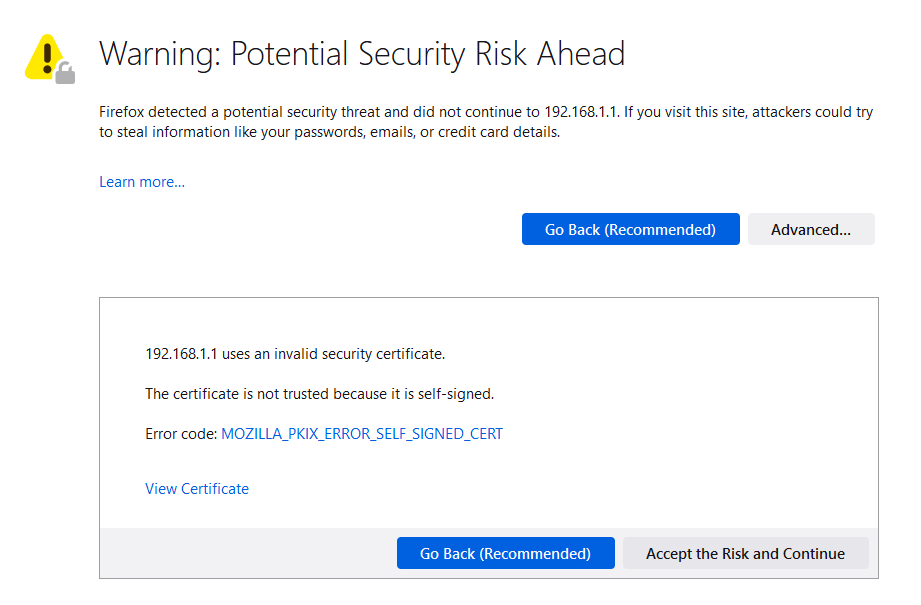
1. a new password - Default is Username: admin password: admin



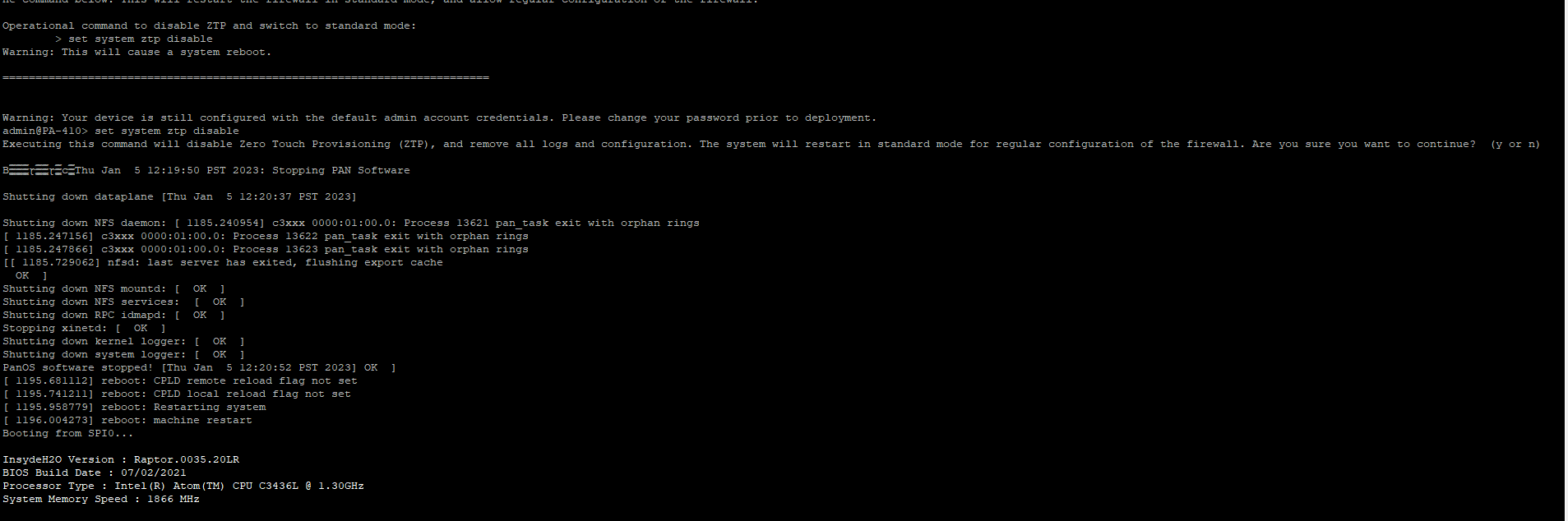
1. Change your ipv4 address to one in the 192.168.1.0/24 range that isn't 192.168.1.1



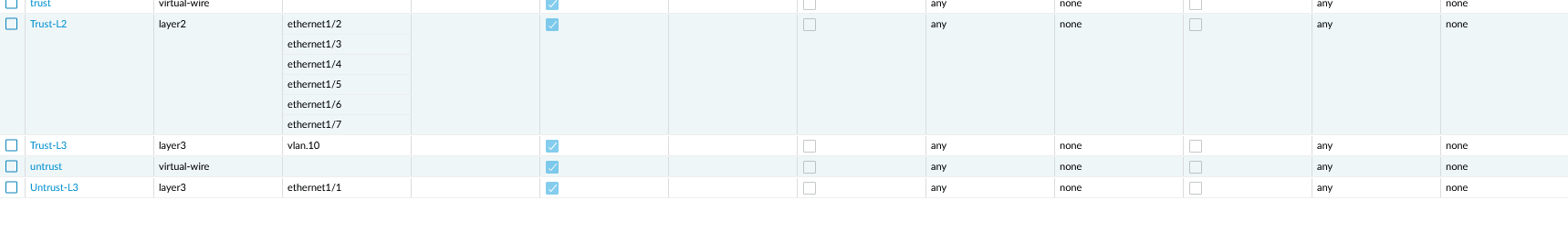
1. Go to [https://192.168.1.1](https://192.168.1.1/) and accept risks and continue



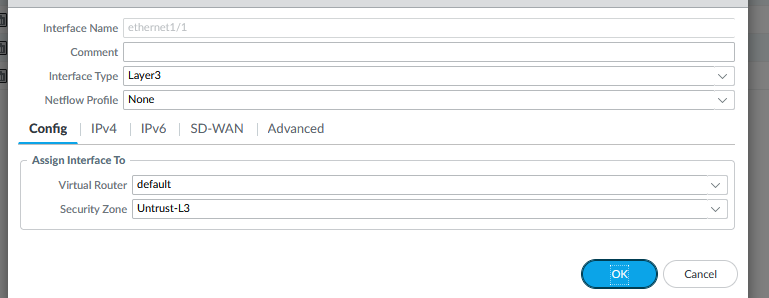
1. Step 4 do a set system ztp disable command to go from ztp mode to standard for configuration



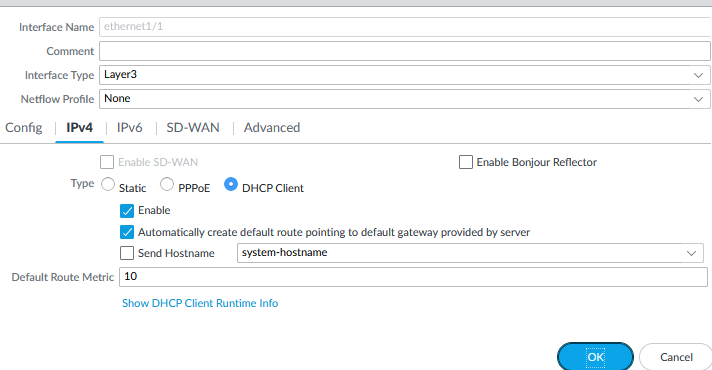
1. Create Security Zones 1. Go to: Network > Zones and click Add. 2. Create 3 zones: Untrust-L3, Type Layer3 Trust-L3, Type Layer3 Trust-L2, Type Layer2



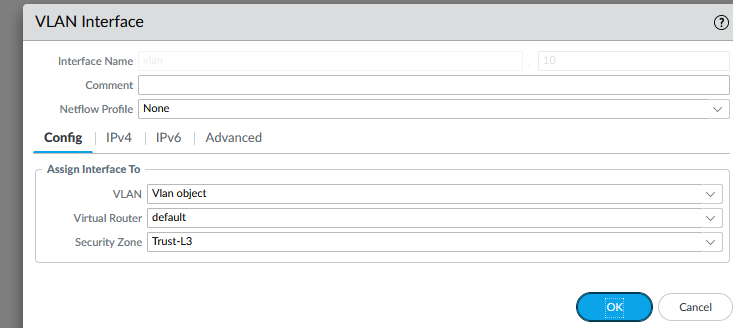
1. Go to Network > Interfaces on the WebGUI and configure ethernet 1/1. 2. On Config Configure the ethernet1/1 Interface Type as Layer3. Set Virtual Router to default. Set Security Zone to Untrust-L3



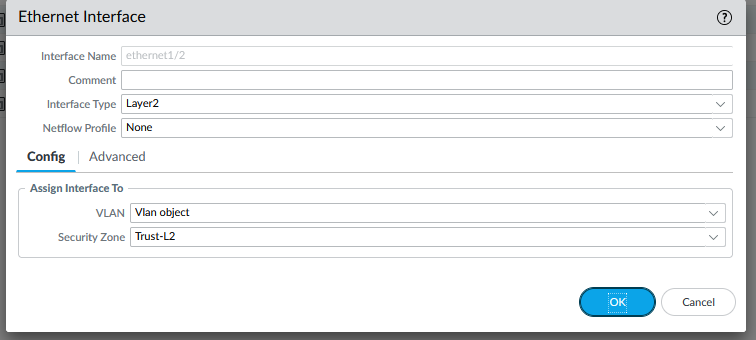
1. Under IPv4 click DHCP Client



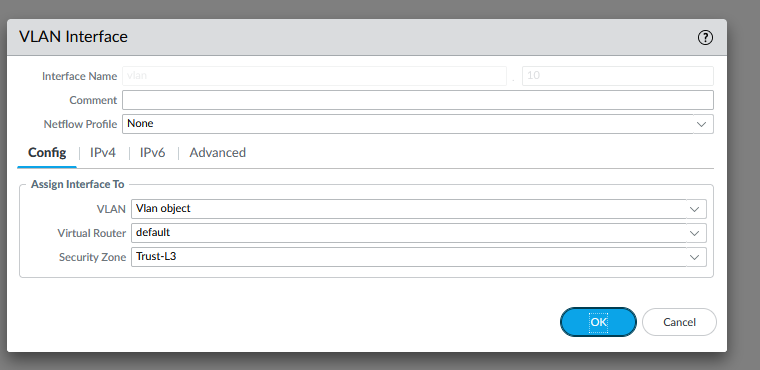
1. Create a VLAN Object 1. Go to Network > VLANs and click Add. 2. Enter a name and select 'v' for VLAN Interface

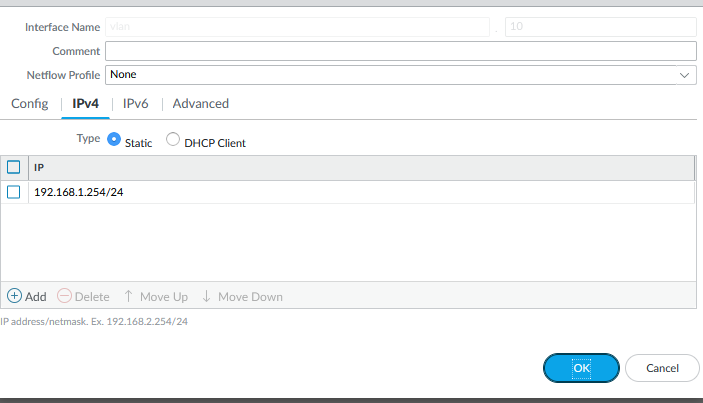


1. Go to Network > Interfaces > Ethernet. 2. Edit the following settings for the ethernet1/2, ethernet1/3 and ethernet1/4 interfaces: Interface Type: Layer2 Netflow Profile: None VLAN: VLAN Object Security Zone: Trust-L2// Do all interfaces

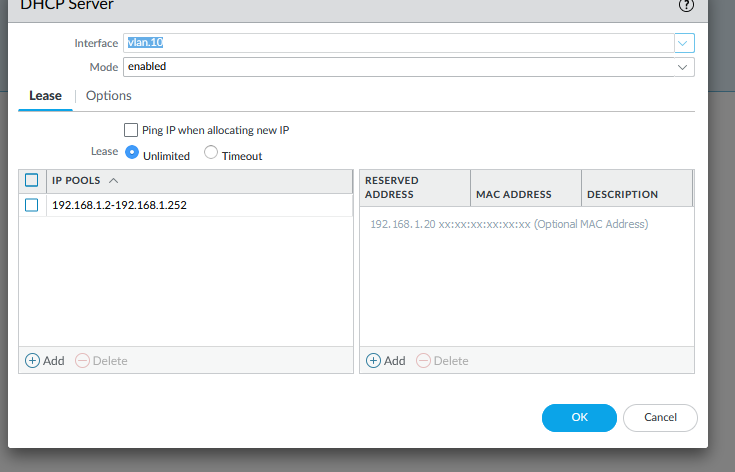


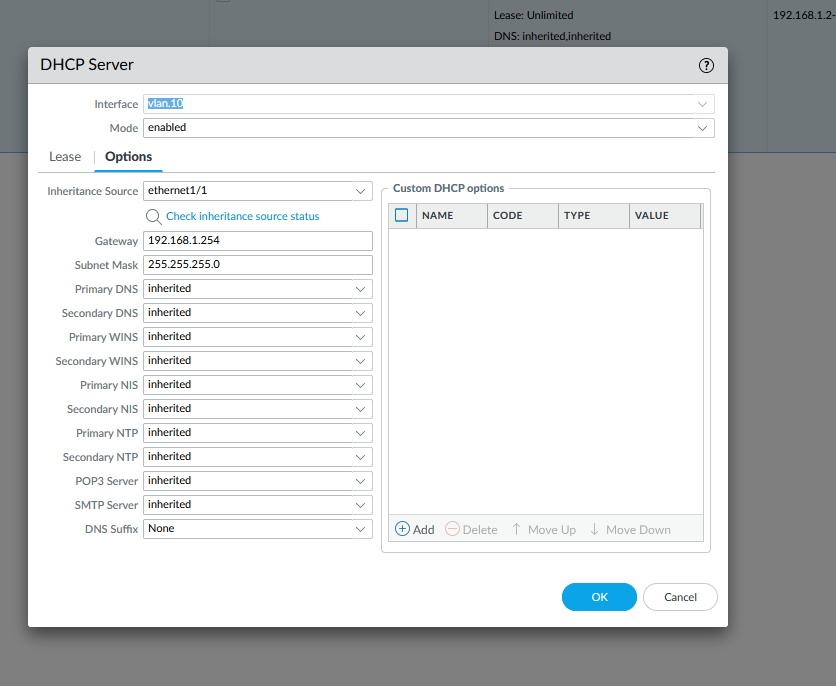
1. Configure the VLAN Interface Go to Network > Interfaces > VLAN and edit the following settings: Config tab VLAN: VLAN Object Virtual Router: default Security Zone: Trust-L3. Click Add and enter IP address 192.168.1.254/24



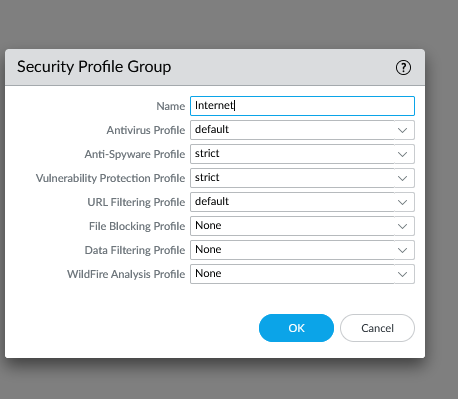


1. Configure the DHCP Server 1. Go to Network > DHCP > DHCP Server. 2. Click Add. 3. Edit the DHCP Server settings, as shown:

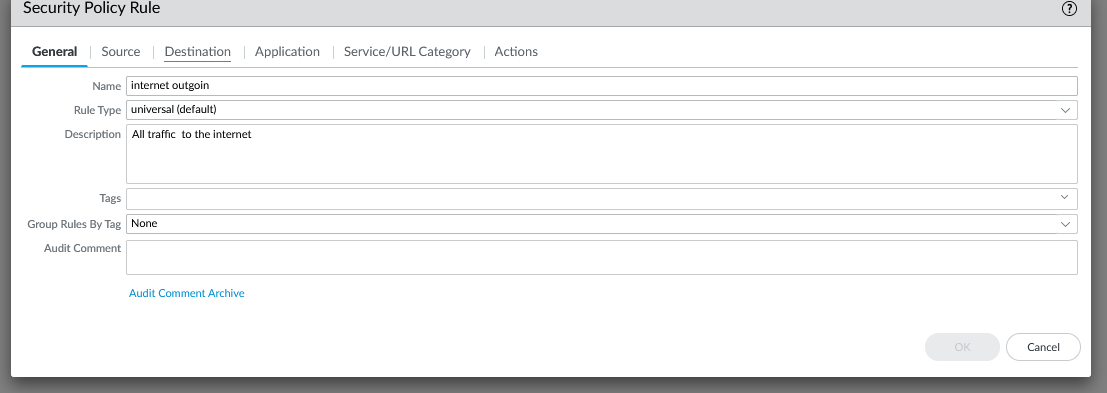


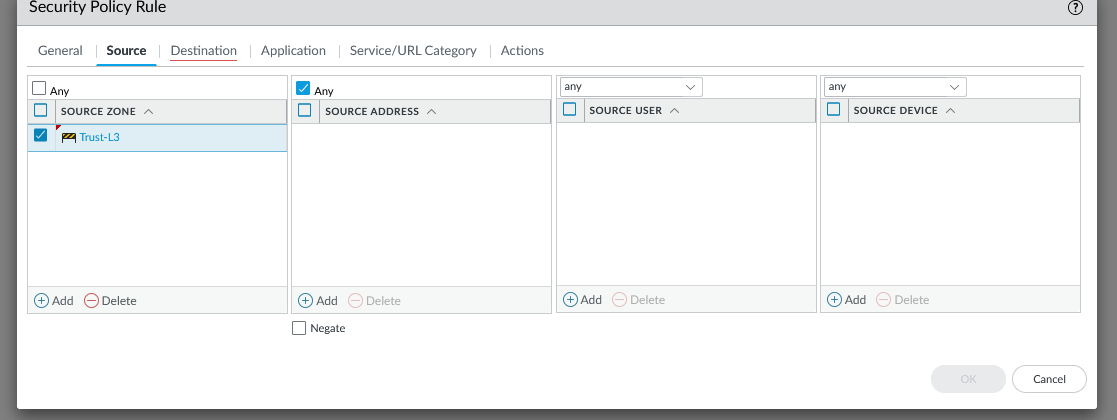


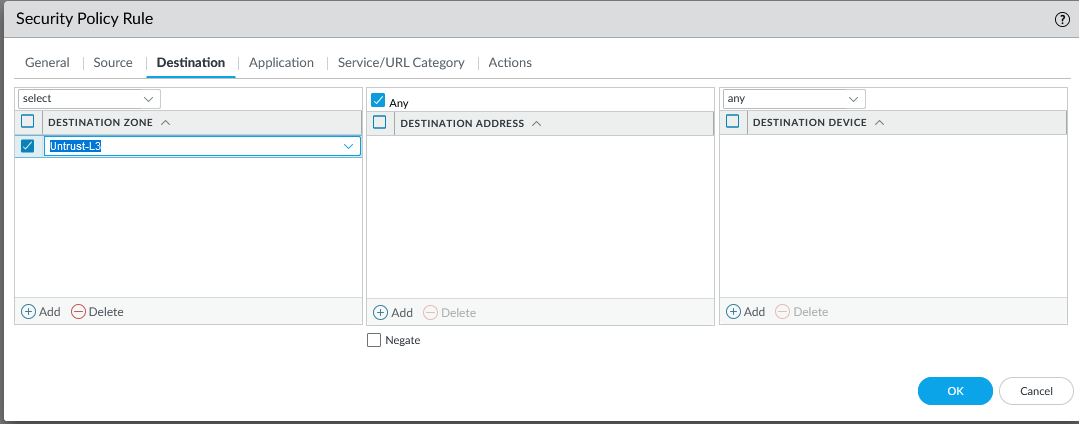
1. Define a Security Profile Group 1. Go to Objects > Security Profile Groups and click Add. 2. Edit the following Security Profile Group settings as desired:

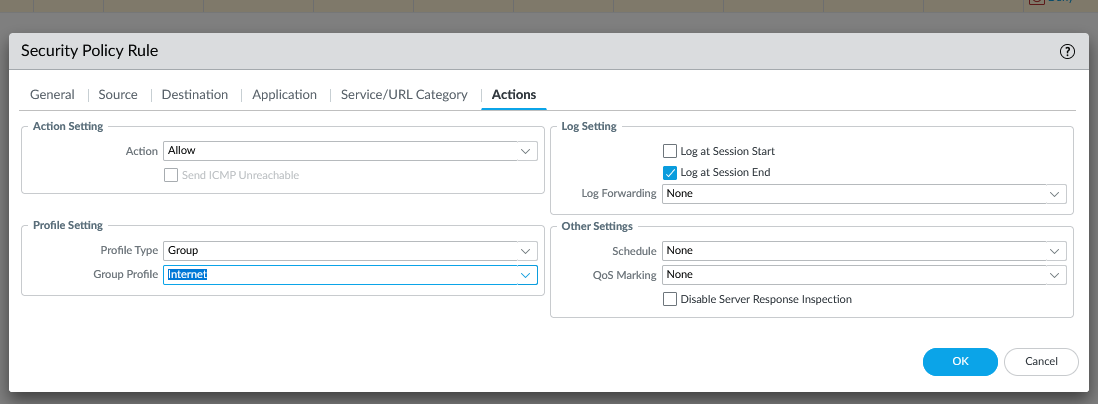


1. Configure Outbound Internet Security Policy 1. Go to Policies > Security and click Add. 2. Enter a Name and Description: Add the source zone Add the destination zone: Specify the action as Allow and complete the Profile Setting:

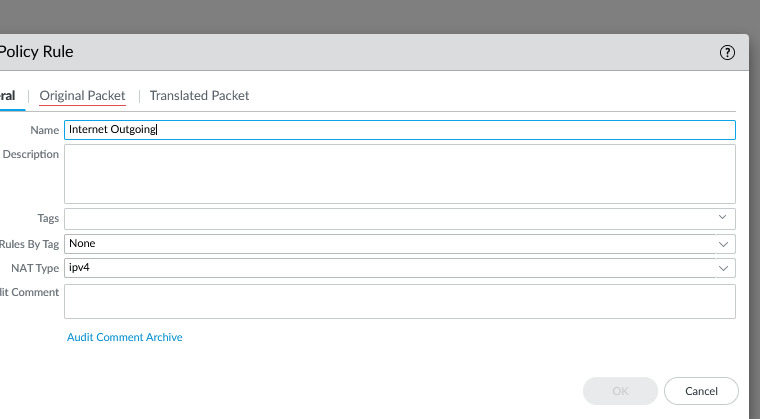


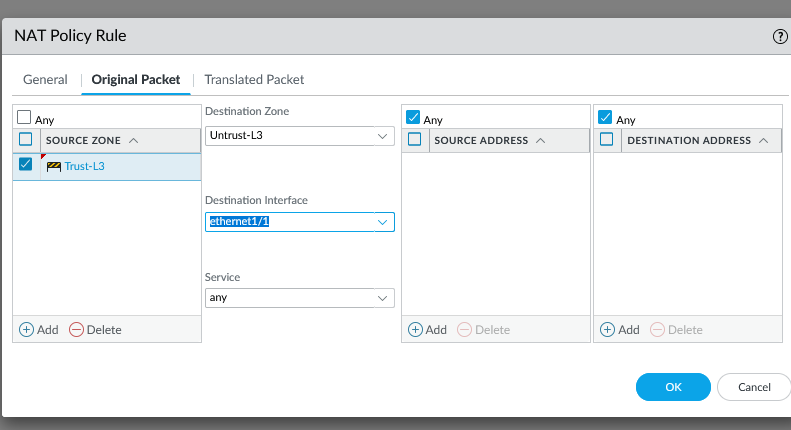


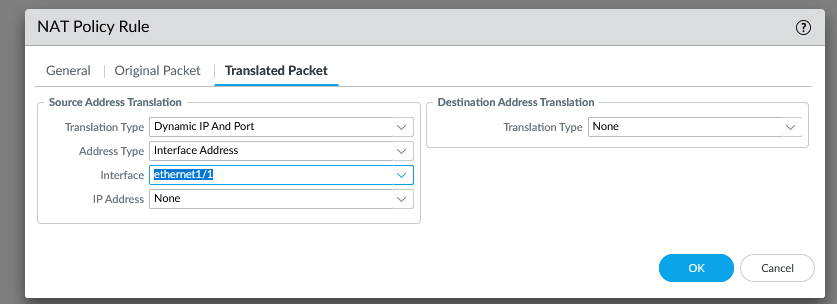




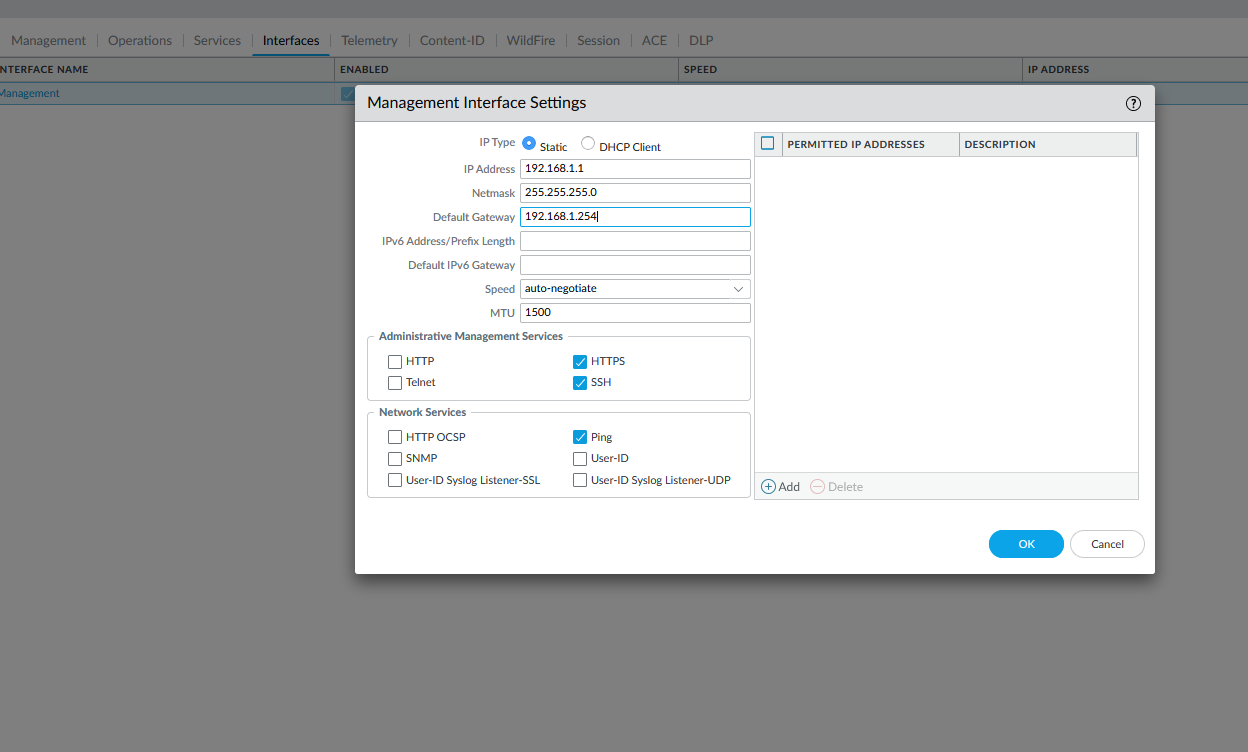
1. Configure Outbound Internet NAT Policy 1. Go to Policies > NAT and click Add. 2. Enter a Name and check IPv4 for NAT Type: On Original Packet, specify the Source Zone, Destination Zone, and Destination Interface: On Translated Packet, set: Translation Type: Dynamic IP And Port Address Type: Interface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



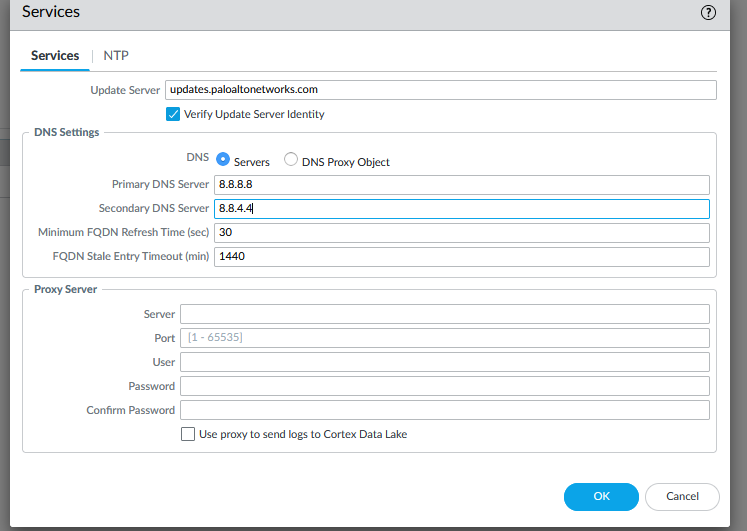




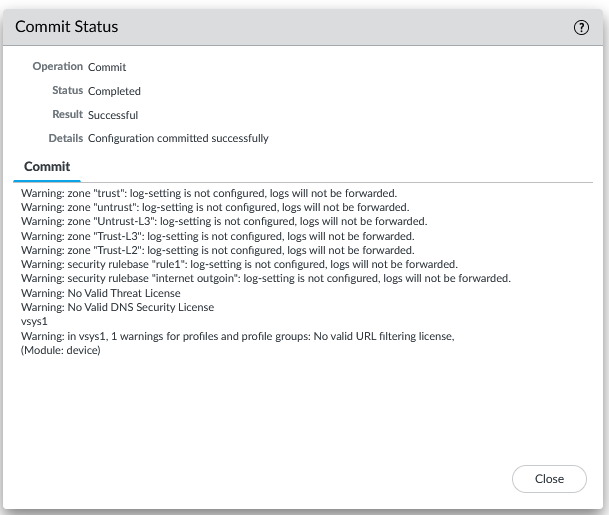
1. Configure the MGMT IP Go to Device > Setup > Management and specify the following Management Interface Settings: IP Address Netmask Default Gateway



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:**

The lab went smoothly with little to no issues at all, however, due to sick days of one of our group members, the lab took longer than expected to complete.

**Conclusion:**

In this lab, we configured a SOHO network with a Palo Alto 410 firewall.