

Palo Alto Pa-410 Setup

Evan Choi | Cisco Cybersecurity | 1/31/2023

**Purpose**

The purpose of this lab is to setup a Palo Alto PA-410 firewall so we can setup a Small Office Home Office (SOHO) configuration with it. We did a lab similar to this but with an older version, the PA-220.

**Background Information on lab concepts**

The Palo Alto PA-410 is a firewall released in the 400 series lineup, and it’s the smallest and most accessible one of its class. This firewall is considered the World’s first ML-Powered Next Generation Firewall, which is an advanced version of the traditional firewall, which makes authentication decisions based on the context of the user, content and application. This firewall advertises as having many capabilities, such as preventing malicious activity concealed in encrypted traffic, identifying and categorizing all applications with 7 layer inspection, enforcing security for users at any location, delivering a unique approach to packet processing with Single-Pass Architecture, and being a machine learning powered firewall, making it a very strong firewall for a 25-50 user network.

A SOHO network stands for Small Office/Home Office network, and they are essentially small LANs. They usually consist of less than 10 computers and are meant to be used by small businesses. Similar to other LANs, they are made up of wireless and wired computers. Their main purpose is to connect multiple computing devices on a single network so they can share information effectively with other connected users in their organization.

When creating a SOHO network, you need to configure your firewall so it can access the internet, and you also need to access the management web GUI so you can configure policies and zones.

A security zone is a way to group physical and virtual interfaces on a firewall so you can control and log the traffic that goes through certain interfaces on your network. Interfaces on a firewall must be assigned to a security zone before it can process traffic. Zones can be assigned multiple interfaces of the same type (layer2, layer 3, or tap interfaces), but an interface can only belong to a single zone. To create a security zone you need to name the zone, assign interfaces to the new zone create, and more. There are four main types of zones that you can use:

* **Tap Zone:** Used with SPAN/RSPAN, allowing you to monitor traffic
* **Virtual Wire:** Used to bind two interfaces within a firewall (also known as Transparent Firewall)
* **Layer 2:** Used when switching between two or more networks
* **Layer 3:** Used when routing between two or more networks.

A Security Policy is a key element of cybersecurity. They are used to determine whether to block or allow the session based on specific attributes on incoming traffic. These attributes can be the source and destination Security Zone, the source and destination IP address, the application, the user, and the service. The firewall will match all passing traffic against a session, and each session will be matched against a Security Policy rule. Once a session match happens, the bidirectional traffic in that session will be applied to the corresponding Security Policy rule. If traffic doesn’t match any already defined rules, the default rules will be applied. The default rules are predefined, allowing all intrazone traffic and denying all interzone traffic. However, you can override these rules and change some settings such as tags, action, log settings, and Security Profiles.

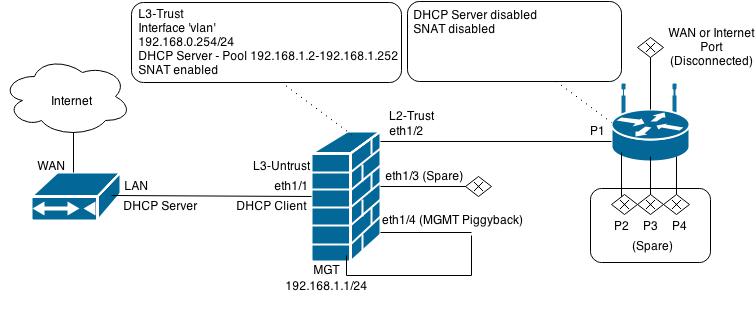
A Security Profile is an addition to Security Policies. When traffic is allowed by the Security Policy, the Security Profile helps you define an **allow but scan** rule, scanning allowed application for threats including viruses, malware, spyware, and DDOS attacks. Traffic matching the allow rule that’s defined in the Security Policy will have the corresponding Security Profile applied for further content inspection rules like antivirus checks and data filtering. Multiple Security Profiles can be combined to create a Security Profile group which can be treated as a unit and added to Security Policies in a single step.

**Lab Summary**

In this lab, I used a Palo Alto PA-410 firewall to setup a SOHO configuration. We used completely new PA-410 firewalls, so we did not have to reset them like the PA-220s. When starting the device, the startup prompts were very similar to those of the PA-220, with the only difference being a prompt for Zero Touch Provisioning (ZTP), where we used the command **set system ztp disable** to enter the standard mode instead. After entering the standard mode, we changed the PC’s IP address to 192.168.1.1, and we entered that IP address into a web browser to access the webGUI.

The Palo Alto GUI menu for the PA-220 and PA-410 are identical so the SOHO configuration process was very familiar to us.

**Network Diagram**





**Procedure**

1. Connect a **Console cable** to the **Console** port on the palo alto
2. You will be prompted to change the password.

A picture containing text

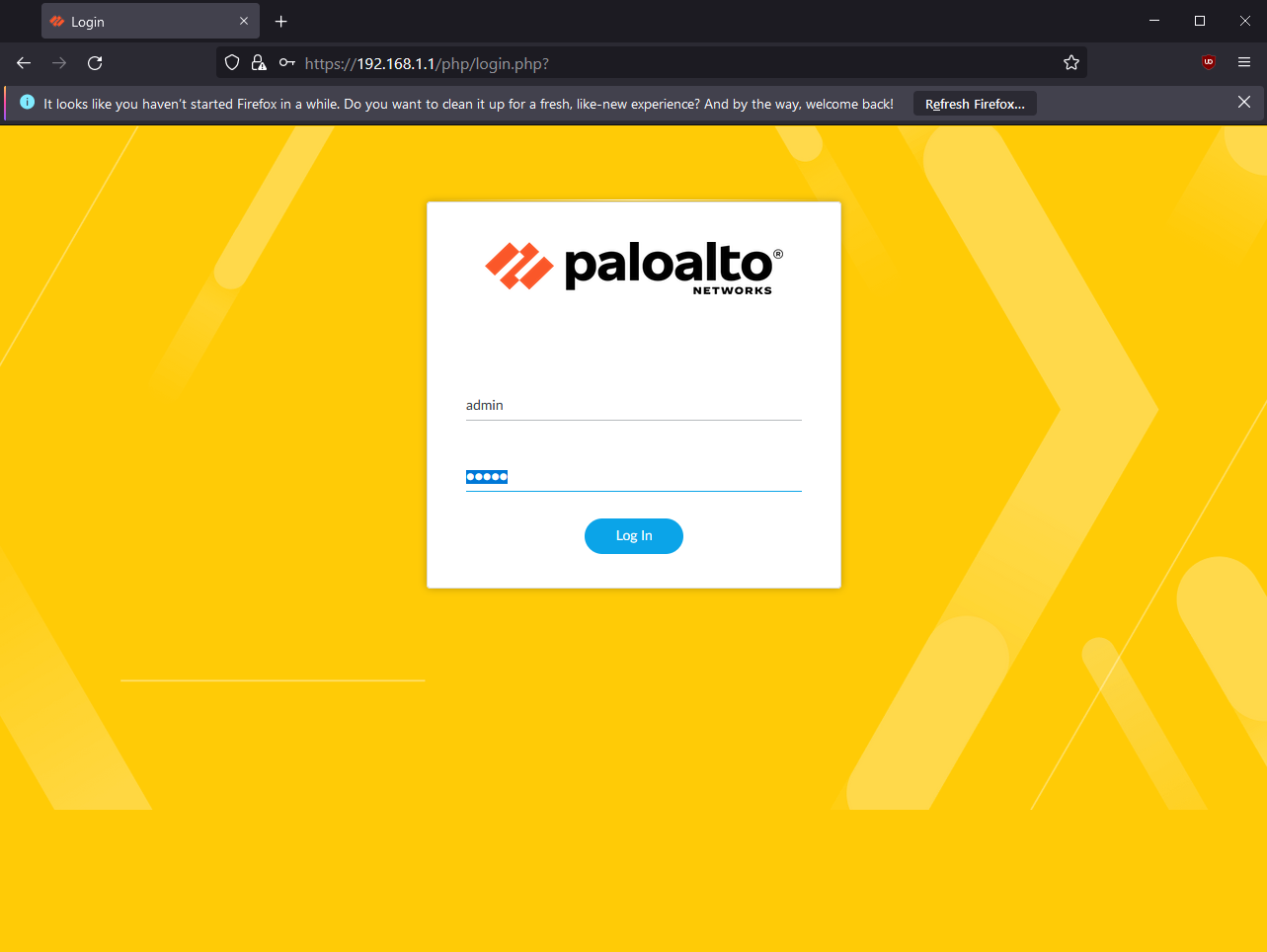
Description automatically generated

1. Next, disable ZTP with the following command **set system ztp disable.**

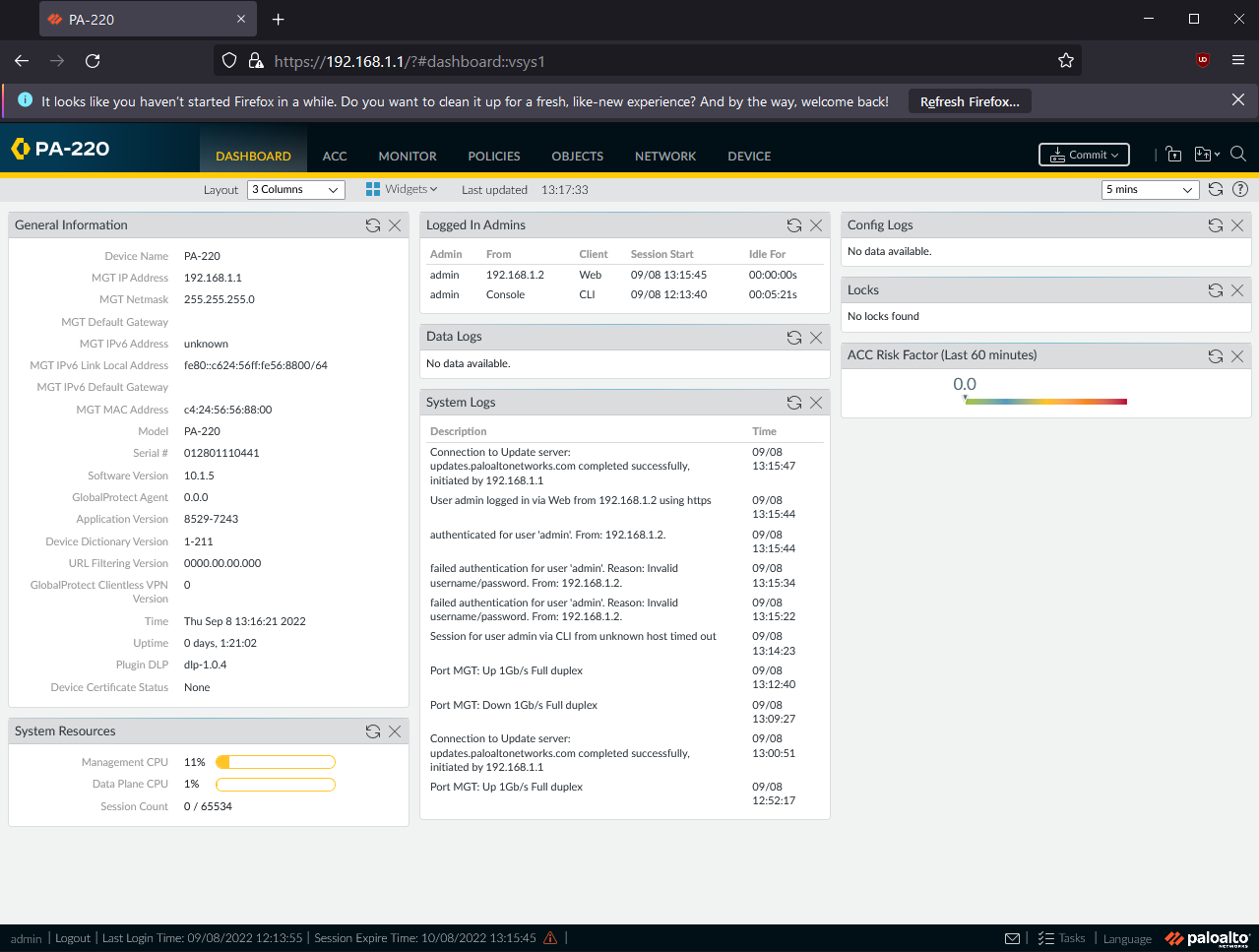
Text

Description automatically generated

1. Configure the Ethernet port of your computer to have an IP address of 192.168.1.1 and a netmask of 255.255.255.0.
2. Open a **web browser** (preferably Firefox) and type[**https://192.168.1.1**](https://192.168.1.1)**.** A web GUI like the one below should appear. The default credentials are: username: admin, and password: admin, but they may be changed to the username and password you set in the factory reset lab.



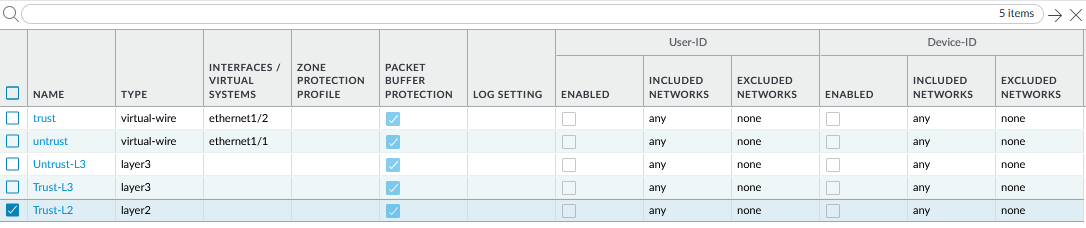
1. After logging in, the following dashboard should appear. At the very top, press the **Network** tab then click **Zones.**



1. Click the **Add** button, and create the following 3 zones:

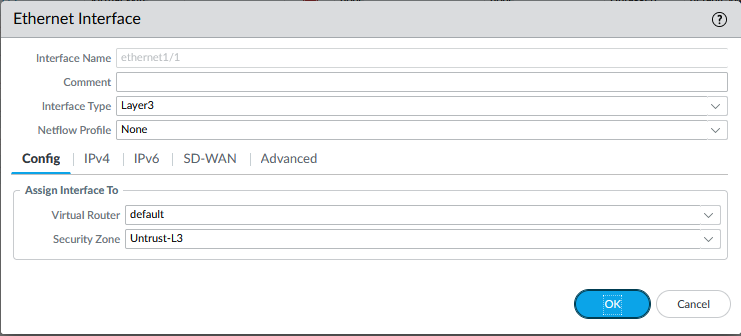
* Name: Untrust-L3, Type: Layer 3
* Name: Trust-L3, Type: Layer 3
* Name: Trust-L2, Type: Layer 2

You should end up with something like this:

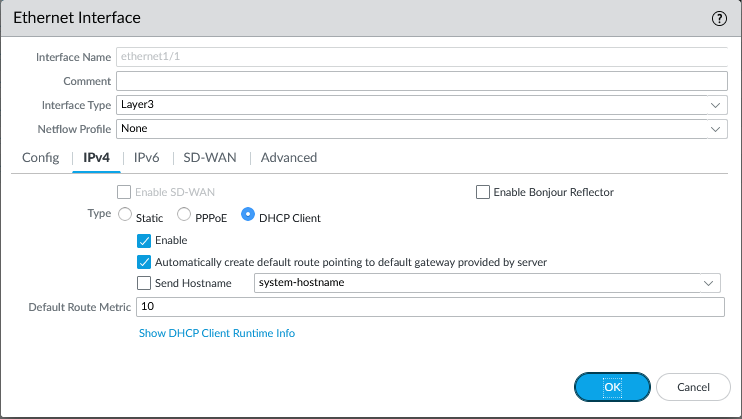


1. Now, connect a **UTP cable** from your ISP modem to your Palo Alto firewall, through **ethernet1/1.**
2. Go to the **Network** tab, and press **Interfaces.** Configure **ethernet 1/1** with the following:

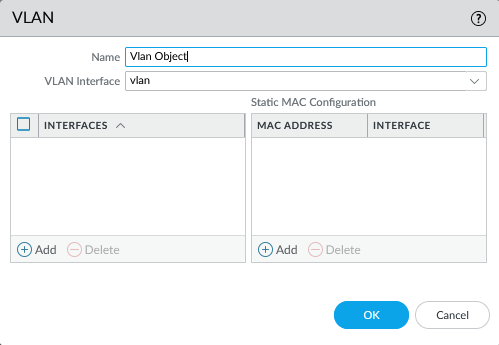
* Interface Type: Layer 3
* Virtual Router: default
* Security Zone: Untrust-L3



1. Still under **ethernet 1/1,** go to the **IPv4** tab and set the Type to **DHCP Client.** There should be a check mark next to **Enable** and a check mark next to **Automatically create default route pointing to default gateway provided by server.** It should look like the image below.



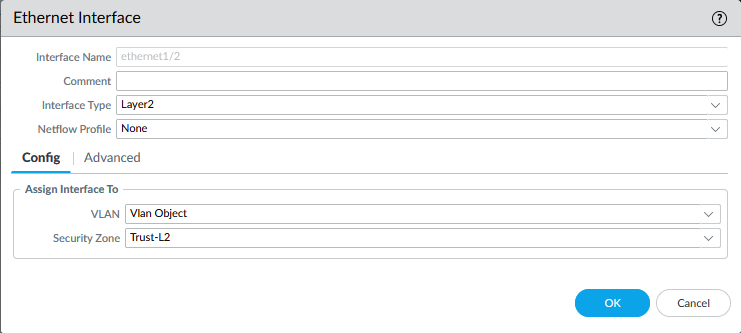
1. Now you will create a VLAN Object. Go to the **Network** tab and click **VLANs.** Click **add.** Enter a name and select **vlan** for the VLAN Interface. I named mine **Vlan Object.**



1. Now you will configure the Layer2 Ports and VLAN Object. Go to the **Network** tab, then click **Interfaces**, then click **Ethernet.** For the ethernet1/2, ethernet1/3, and ethernet1/4 interfaces, change the settings to the following:

* Interface Type: Layer2
* Netflow Profile: None
* VLAN: VLAN Object
* Security Zone: Trust-L2

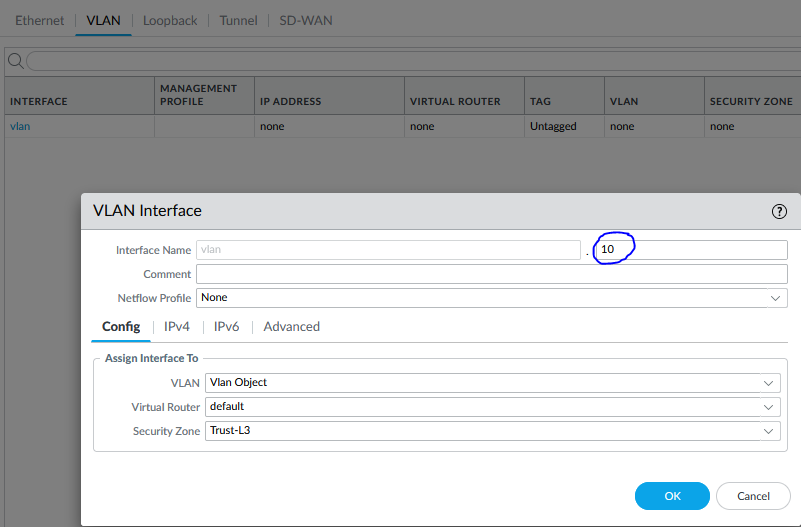
It should look like the following, for each of the respective ethernet ports



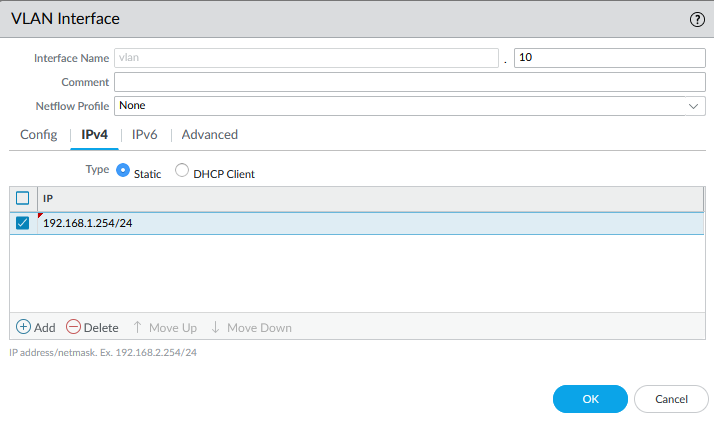
1. Now you will configure the VLAN interface. Go to the **Network** tab, click **Interfaces,** then click **VLAN.** In the **Config** tab, configure the following:

* VLAN: VLAN Object
* Virtual Router: default
* Security Zone: Trust-L3

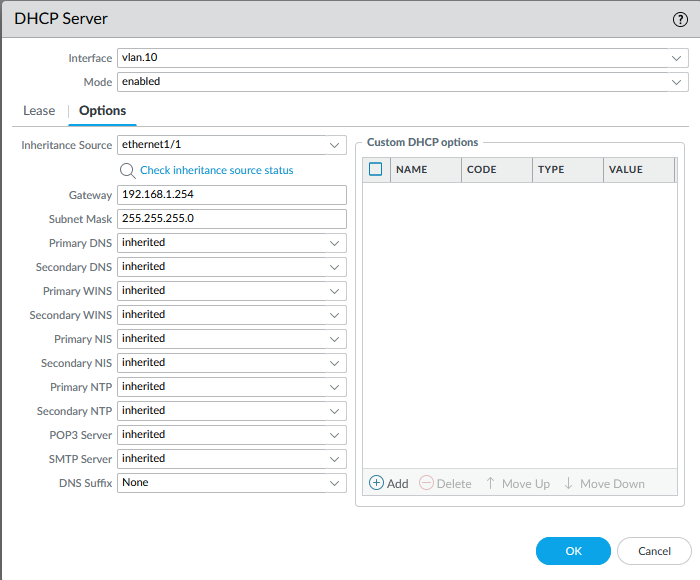
Also, put a **10** in the box on the top right.



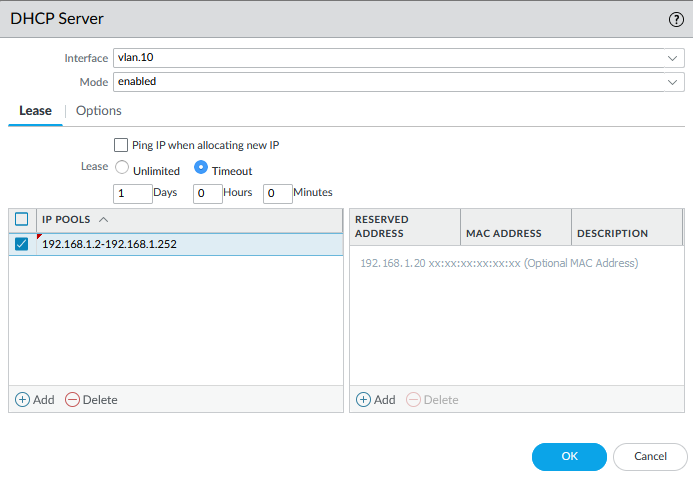
1. Now, go to the **IPv4** tab, click the **Add** button in the bottom left, and enter the IP address, 192.168.1.254/24. Click **Ok.**



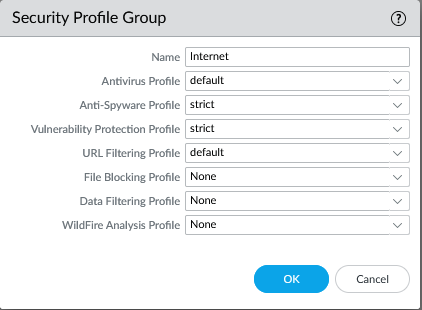
1. Now you will configure a DHCP server. Go to the **Network** tab, click **DHCP,** then click **DHCP Server.** Edit the settings to look like the image below.



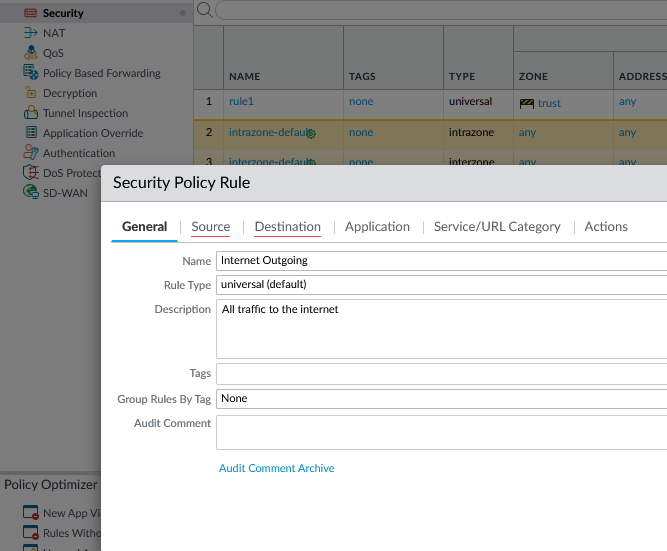
1. Under the **Lease** tab, configure the following:



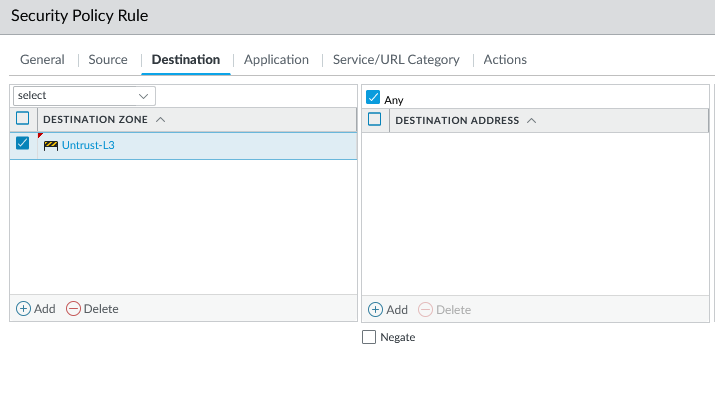
1. Now you will define a security profile group. Go to the **Objects** tab and click **Security Profile Groups.** Click **Add.** Change the settings to the following:



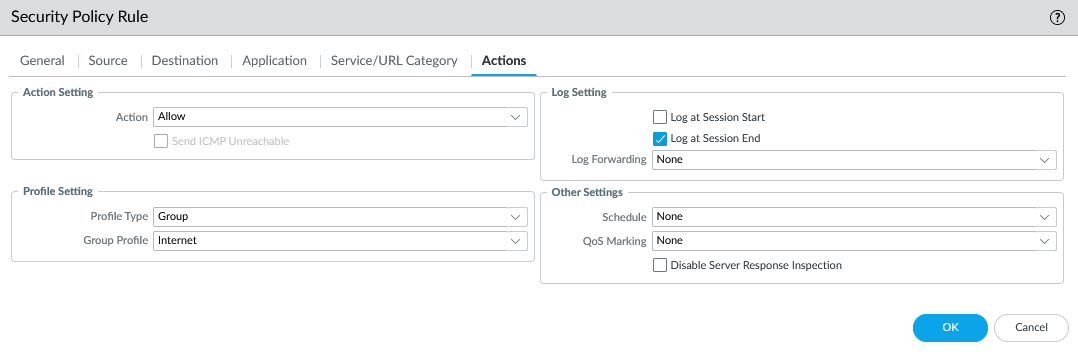
1. To the configure the Outbound Internet Security Policy, go to the **Policies** tab, and click **Security.** Click **Add.** Enter a **Name** and **Description** like shown below:



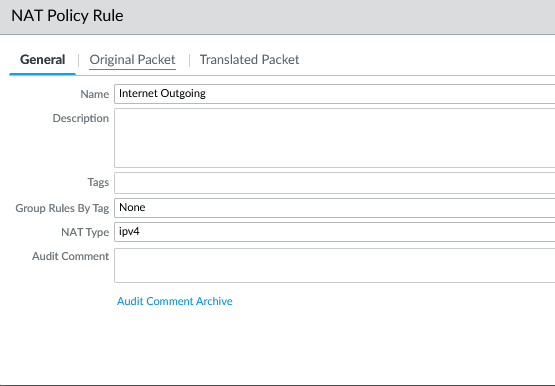
1. Go to the **Source** tab and add **Untrust-L3** to the Source Zone and under the **Destination** tab and add **Untrust-L3** to the Destination Zone.



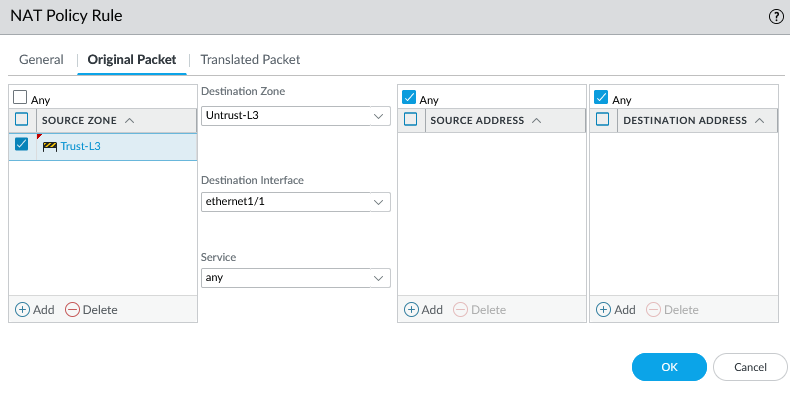
1. Go to the **Actions** tab and change the settings to match the following image:



1. You will now configure the Outbound Internet NAT Policy. Go to the **Policies** tab and click **NAT.** Click the **Add** button and enter a name and select IPv4.

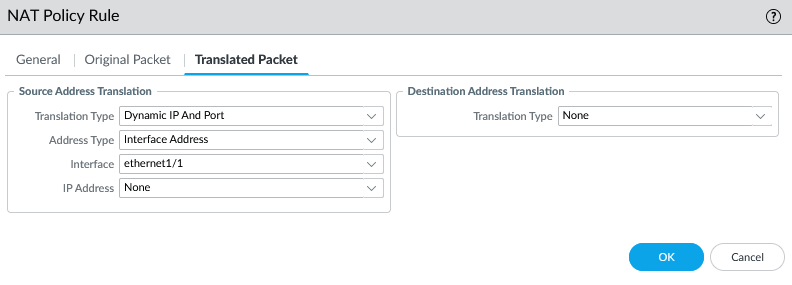


1. Go to the **Original Packet** tab and specify the **Source Zone, Destination Zone,** and **Destination Interface.**

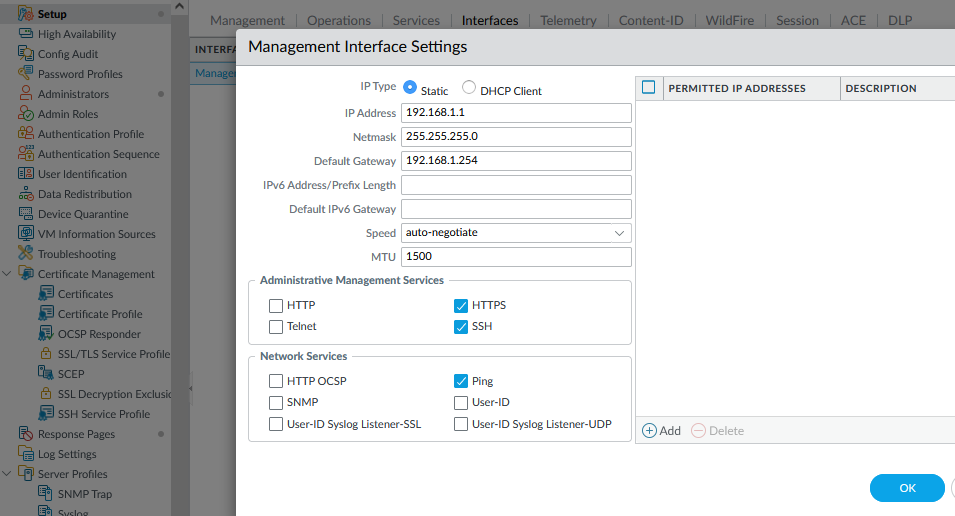


1. Go to the **Translated Packet** tab and edit the following:

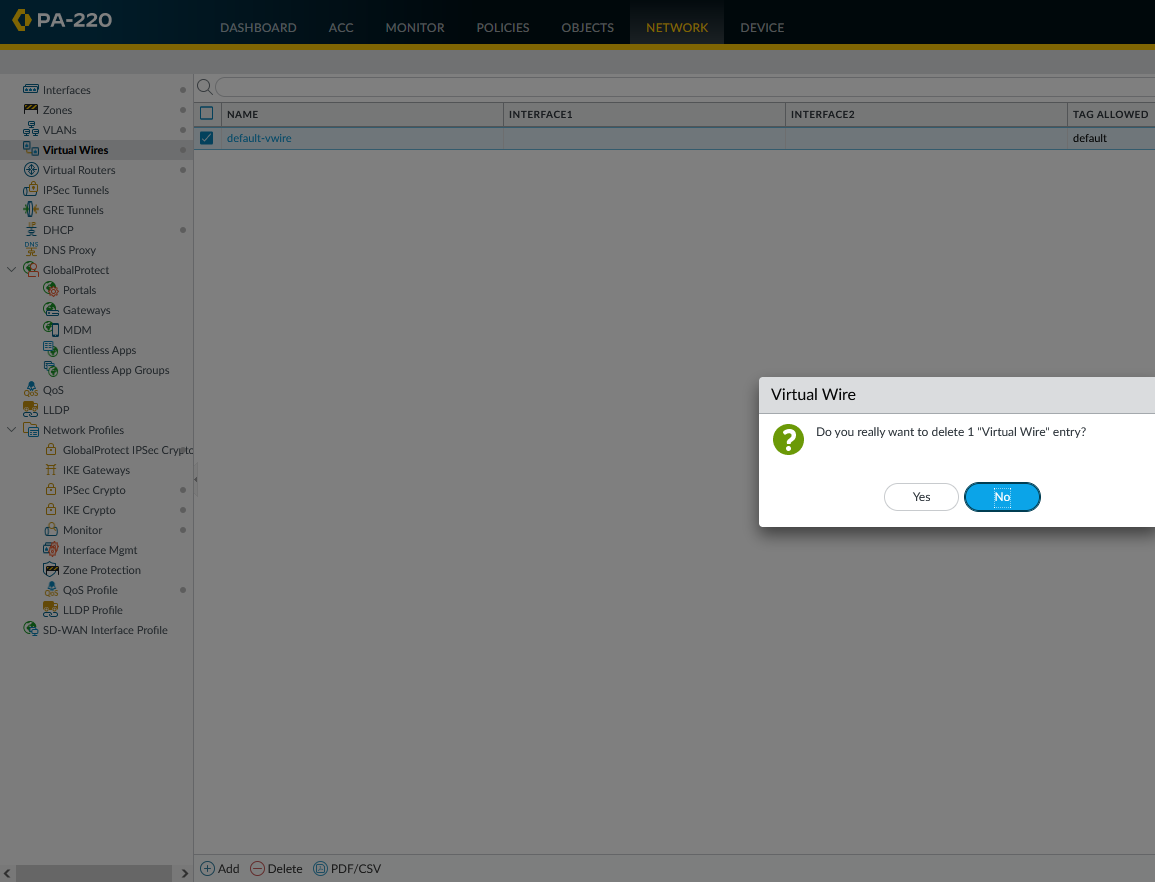
* Translation Type: Dynamic IP And Port
* Address Type: Interface Address
* Interface: ethernet1/1



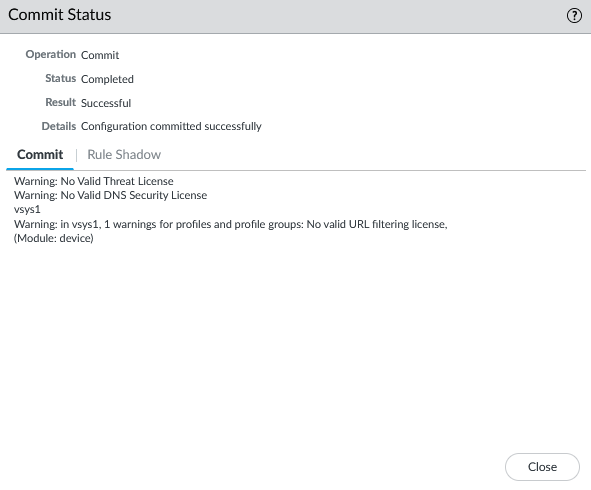
1. Now you will configure the MGMT IP. Go to the **Device** tab, click **Setup,** and click **Management.** Configure the IP Address, Netmask, and Default Gateway.



1. Now, you will delete the default-vwire. Go to the **Network** tab, click **Virtual Wires,** and click delete on **default-vwire.**



1. To save all your changes, at the very top, press the **Commit changes button.** A message like this should appear if successful.



**Problems**

With us being familiar to the SOHO configuration, the setup of that worked successfully, but we had an error that was unique to the new firewall we were using, that being Zone Touch Provisioning.

After disabling ZTP using the **set system ztp disable** command, the firewall rebooted. However, we were never able to access the webGUI on the PC’s we were using. It would preset us with a web page saying Error 404: Not Found. We solved this issue by testing our NVMe drives on a different PC and figured out that the issue was PC sided. We figured out that the issue was being we had changed the TLS while troubleshooting in our previous lab (Lab 6 – Cisco ASA 5505). After using a different drive, where TLS hadn’t been changed, we were able to login to the firewall’s webGUI, and finish configuring the SOHO network.

Graphical user interface, application, Word

Description automatically generated

The image above is the error we experienced in this lab.

**Conclusion**

In this lab, we used a completely new Palo Alto PA-410 firewall to configure a SOHO network. With use having experience configuring a SOHO network, the lab was pretty straightforward for us, with our only problems being issues with the NVMe drive we were using. In conclusion, this lab allowed us to practice creating SOHO configurations on Palo Alto firewalls more, while also challenging us to problem solve issues relating to our hardwire.

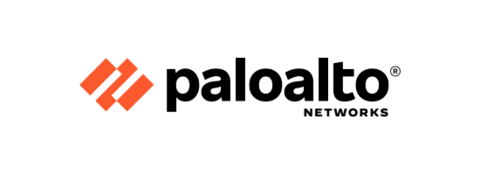
**Teacher Signoff Page of Lab Completed**

The stamp below recognizes that

Evan Choi

has completed

**Lab 7 – Palo Alto PA-410 Setup**

 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

Period 5