|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto PA-410 Initial Configuration/SOHO configuration** | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

Purpose

The purpose of the lab was to learn how to set up or create a SOHO configuration on the Palo Alto PA-410 fire wall.

Background information

Palo Alto Firewalls are highly used in Enterprise networks. Compared to other firewall brands, Palo Alto firewalls don’t use up a ton of network bandwidth. And Palo Alto firewalls can even allow a user to monitor, inspect, and protect traffic at a high rate. Palo Alto Firewalls can monitor and control the applications that are allowed to work on a user’s network. And unlike other firewalls, Palo Alto Firewalls don’t identify applications by standard ports. Instead, they identify applications by monitoring all network traffic. And has cloud-based threat protection, for defending your network against almost any attack. By setting SOHO configuration you can Install Licenses Configure Dynamic Updates Configure Interfaces, VLANs, appropriate switch tagging Setup DHCP Server(s) Configure Zones Configure Network Address Objects Create Security Policies Create NAT Policies Ingress and Egress. The PA-410 is a firewall created by Palo Alto Networks. It is the first MIL-Powered next-generation firewall that prevents any unknown threats. Which includes inline, proactive, Realtime protection for enterprises. Upgrading the Palo Alto Firewall to the latest PAN-OS release ensures it remains stable, safe from known vulnerabilities and exploits but also allows you to take advantage of new features of the latest update. Palo Alto Networks firewall needs to have a license in order to access and download the updates or other features.

Lab summary

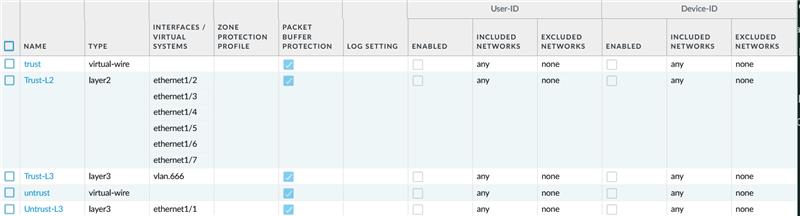
### To begin the configurations, you need to first connect a UTP cable from your computer to the Palo Alto Networks firewall. Next configure a IP and netmask for the computer and Firewall. To access the management console, go to a web browser with the firewall’s IP address and type in your password and username. After logging into Pan OS, you need to first create security zones. Go to Network Zones and Click add to create 3 zones. Next Connect a UTP cable from the ISP modem to the Palo Alto Networks firewall, port. On the console Go to Network, then Interfaces on the WebGUI and configure ethernet by setting the Ethernet interface as layer 3 set router to default and set security zone. On IPv4 Type as DHCP Client, enable and automatically default route pointing to default gateway provided by server. We then need to create VLAN Object, then Configure the Layer2 Ports and VLAN Object by configuring the settings. After Creating VLAN we configured the VLAN Interface setting the config and enter IPv4 address. Next would be creating the DHCP Server and then editing the DHCP Server settings. After this we would define a Security Profile Group, configure Outbound Internet Security Policy, configure Outbound Internet NAT Policy, configure the MGMT IP and Set DNS for MGMT. Finally, we would commit to the changes to finish the SOHO configuration.

Lab commands

* admin@PaloAlto> request disable-ztp [Used to disable Zero Touch Provisioning on a Palo Alto]
* admin@PaloAlto# set cli config-output-format (set/xml) [Used to change how to view the Palo Alto configuration, in XML or set format]

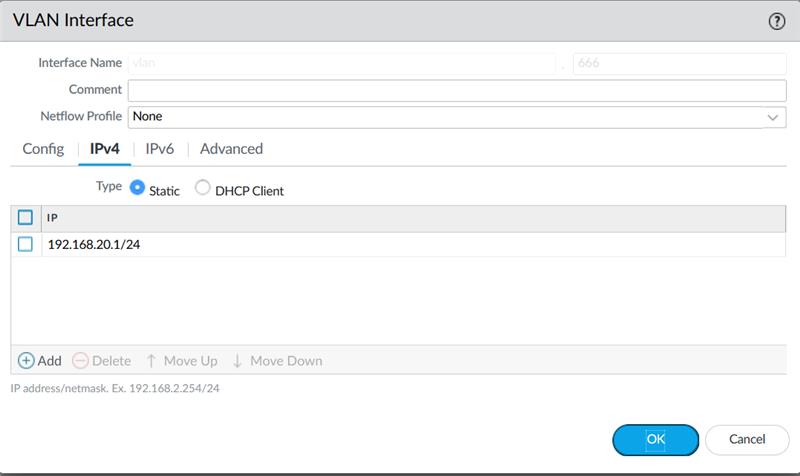
Configurations

Security Zones:

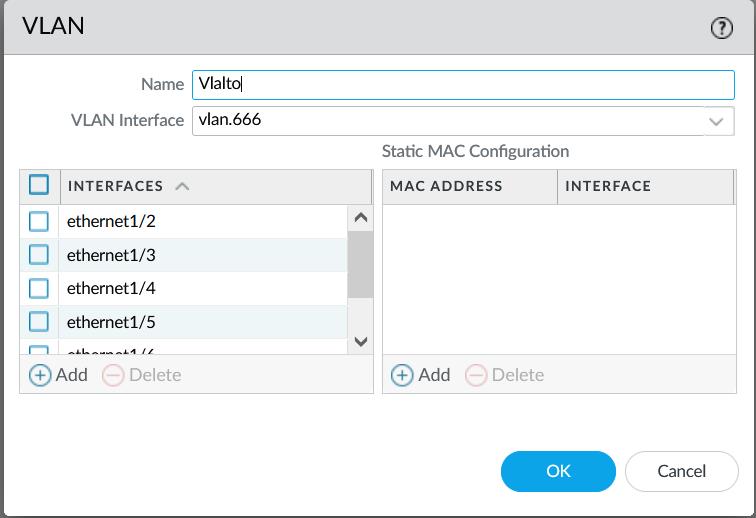


VLAN Interface:

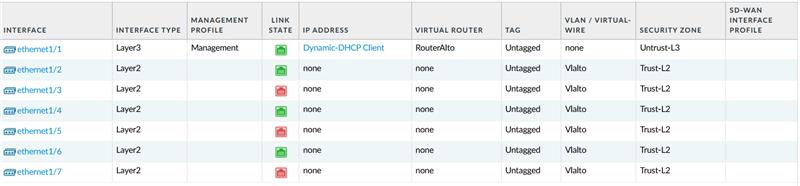




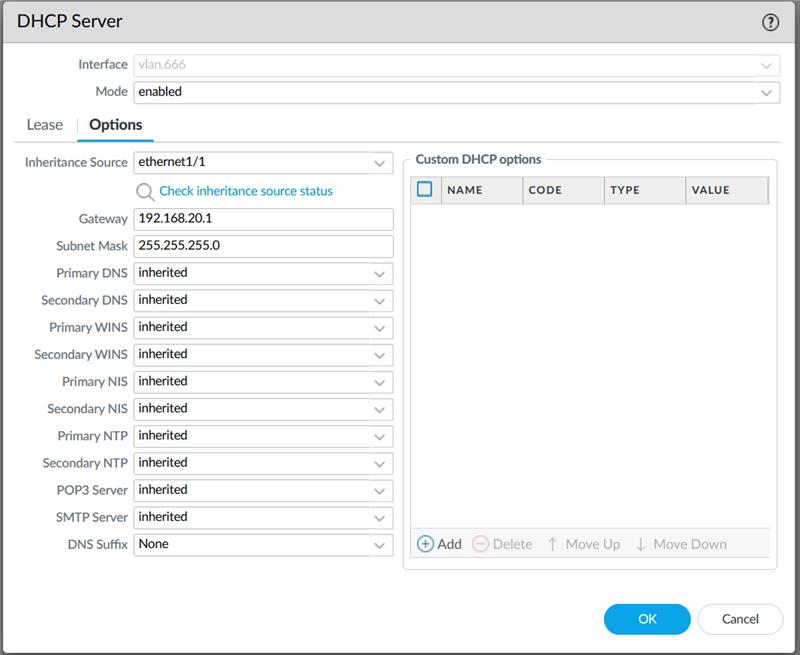




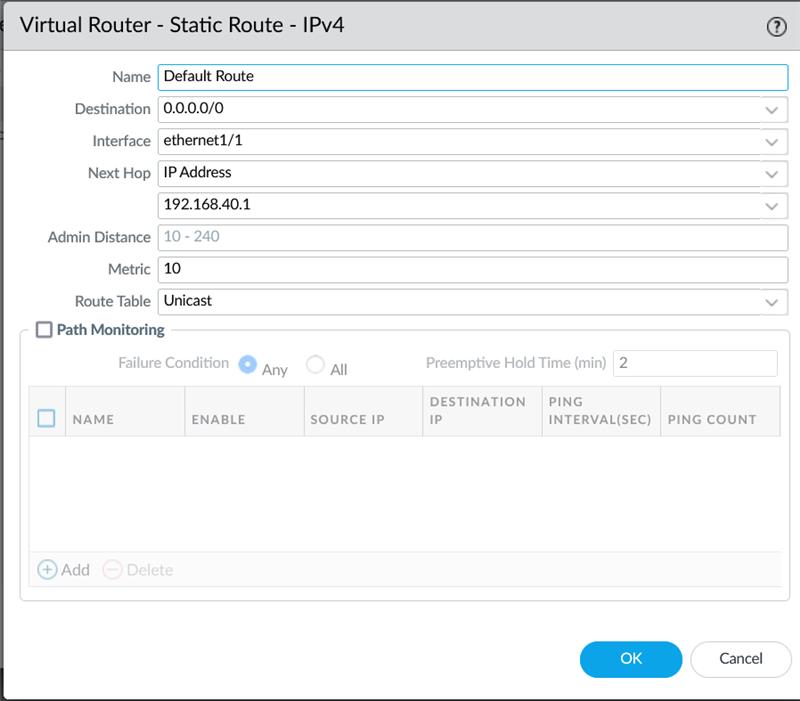
Configured the internet outgoing interface and local LAN interfaces:



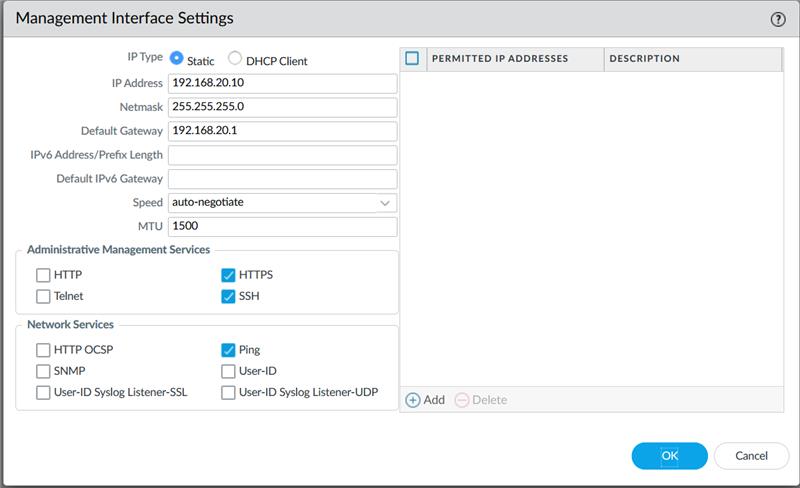
Configured DHCP Server for the LAN interfaces:



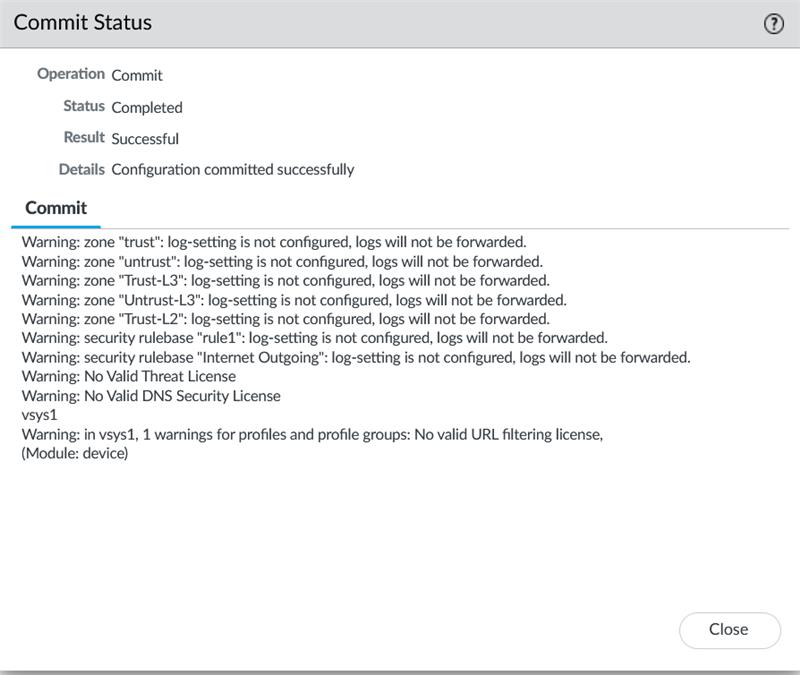
Configured default route for the Virtual Router:



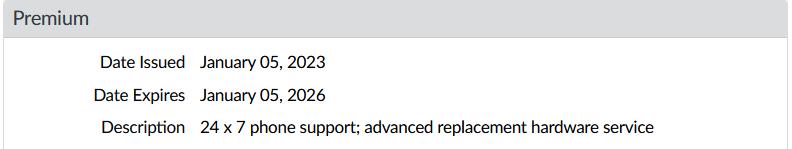
Management Interface settings:



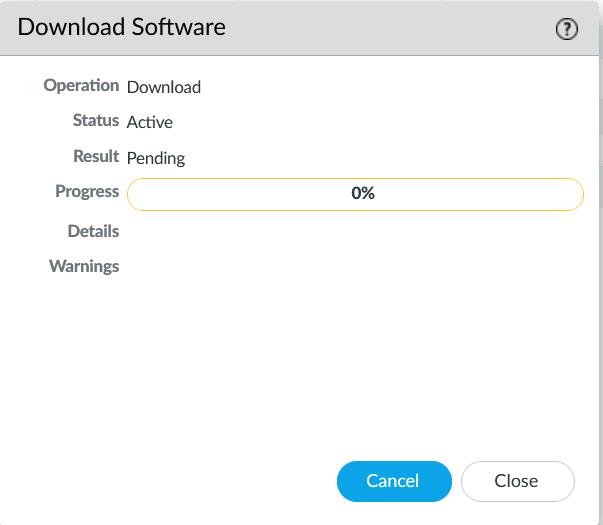
Commit setup changes:

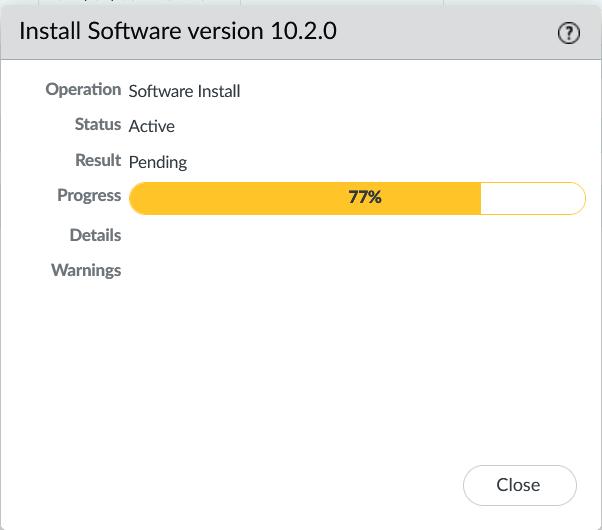


Retrieved Licenses from server:



Downloading Software Updates:





Problems

We have not encountered any major problems while configuring the lab. But we did encounter some small mistakes that stopped our progress. First, we had a problem with the internet outgoing interface not being connected, despite it being connected to another device. This problem was fixed by setting a management profile on it in the advanced settings of the interface. This enabled us to license the device successfully. Another problem we faced was when updating the Palo Alto was when PanOS version 10.2.0, it required some content update. We assumed that we needed to install 10.1.8-h2. And then after installing the needed content update from Dynamic Updates. Finally, we were able to install version 10.2.0.

Conclusion

The objective of the lab was to be able to set up or create a SOHO configuration on the Palo Alto PA-410 fire wall. During this prosses of figuring out updates and license it allowed us to practice and allowed us to familiarize ourselves with Palo Alto Firewall management console. During the lab we encountered some small troubles that we learned from, but we were able Factory Reset a Palo Alto Firewall by the end and access the Managment console using the new logins on the Palo Alto Fire Wall. We were able to set up a Palo Alto Firewall Network that would be connected to the internet and protect our network, retrieve the license for the Palo Alto Firewall and upgrade the operating system to the latest version Firewall.