|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto Firewall 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 (A220) 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.

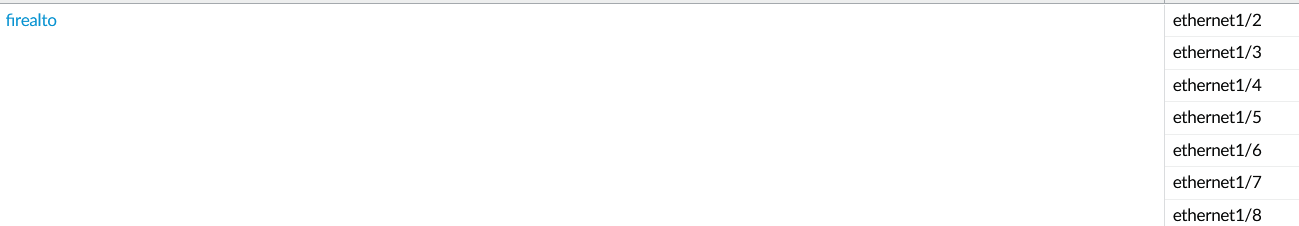
Lab Summary

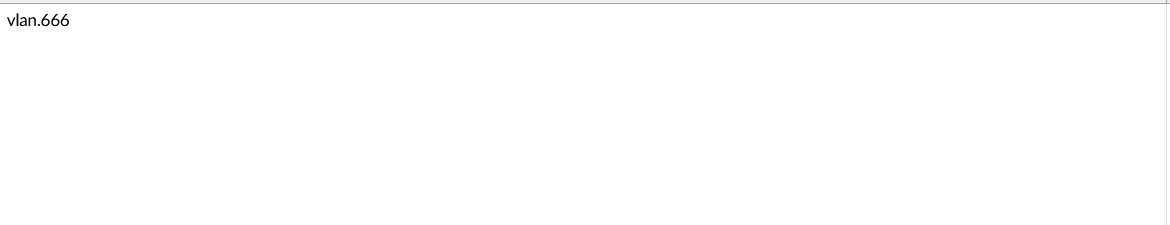
### To begin the configurations, you need to first connect a UTP cable from your computer to the Palo Alto Networks firewall. Next configure a IP and netmask for the computer and Firewall. To access the management console, go to a web browser with the firewall’s IP address and type in your password and 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.

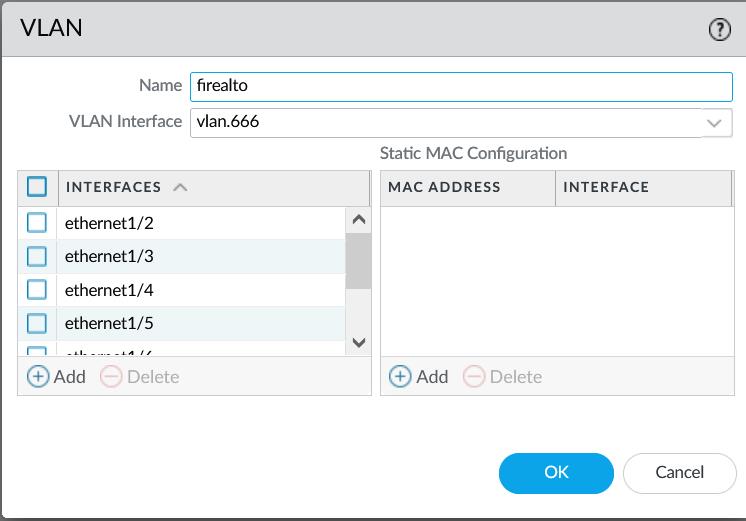
Lab Topology

|  |  |  |
| --- | --- | --- |
| **Device/Interface** | **IP Address** | **Default Gateway** |
| PC1 & PC2 | DHCPv4 | 192.168.10.1 |
| F1 (Palo Alto) | DHCPv4 | 192.168.40.1 |
| F2-8 (Palo Alto) Vlan 666 | DHCPv4 | 192.168.10.1 |
| Vlan 666 (Palo Alto) | 192.168.10.1/24 | 192.168.10.1 |
| Virtual Router (Palo Alto) | 192.168.10.1/24 | 192.168.40.1 |
| Management (Palo Alto) | 192.168.10.10/24 | 192.168.40.1 |

Configurations

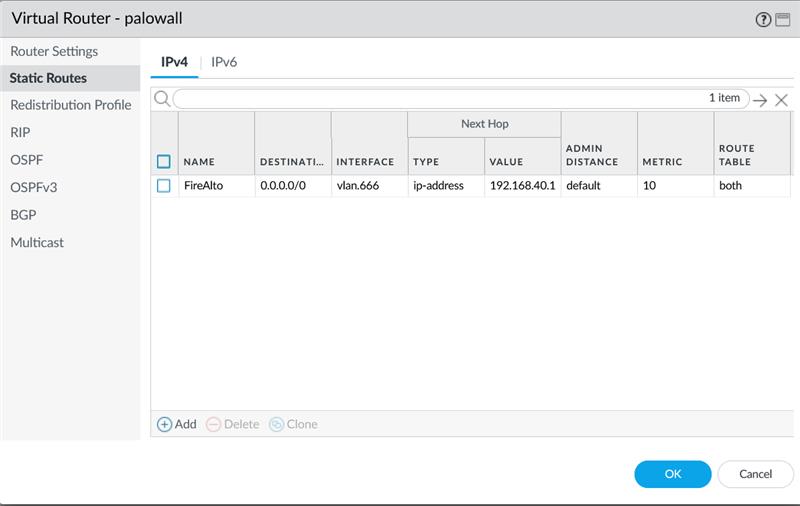




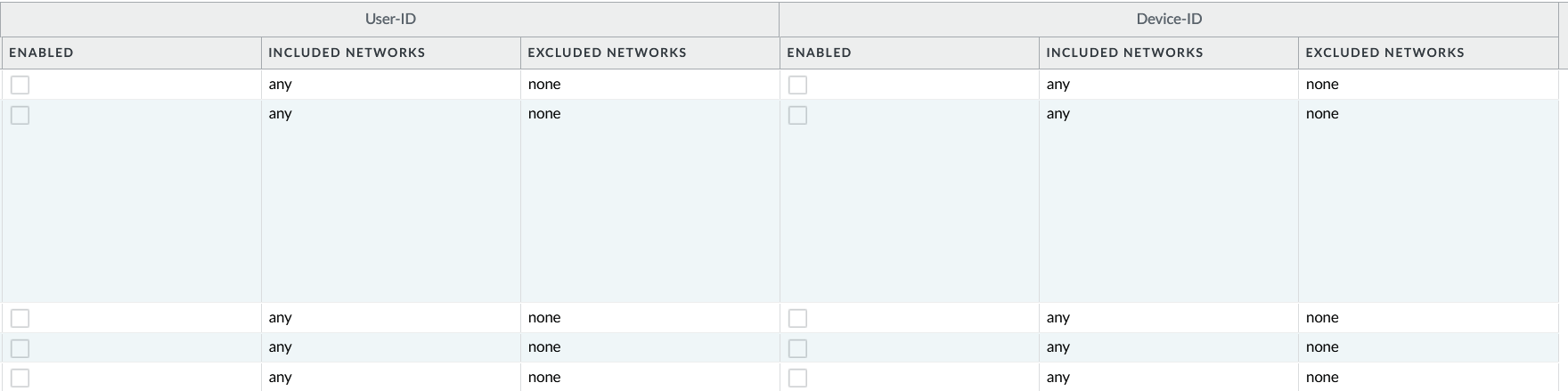


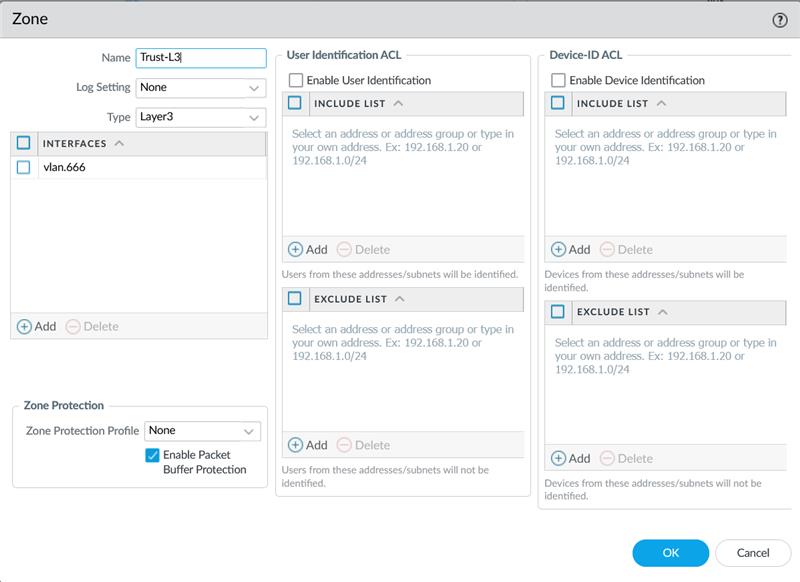


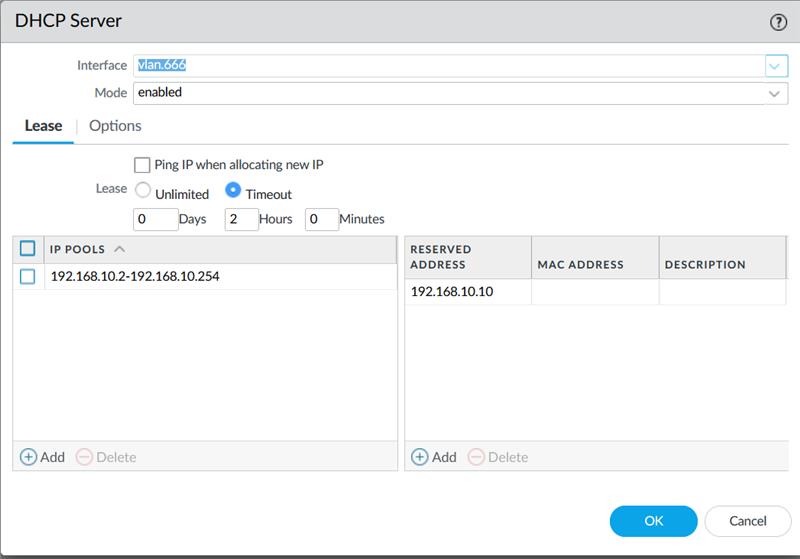


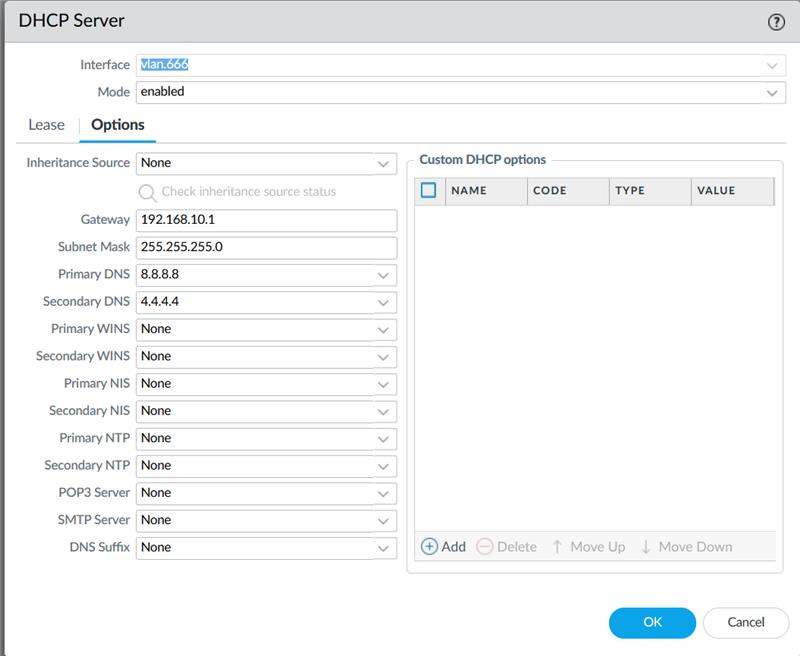




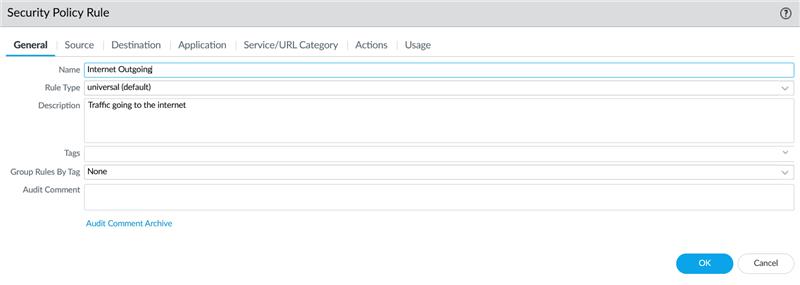


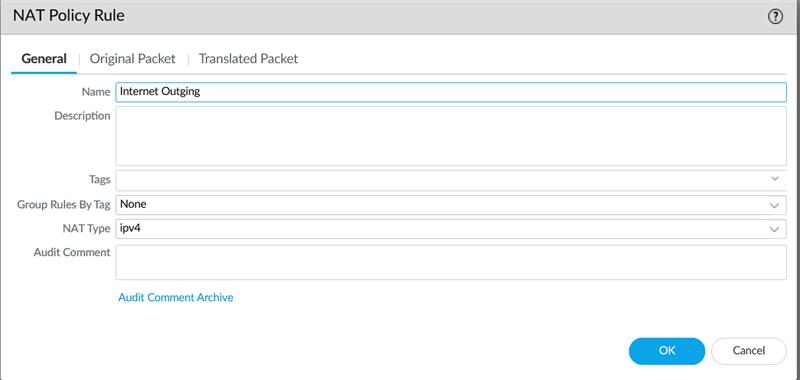


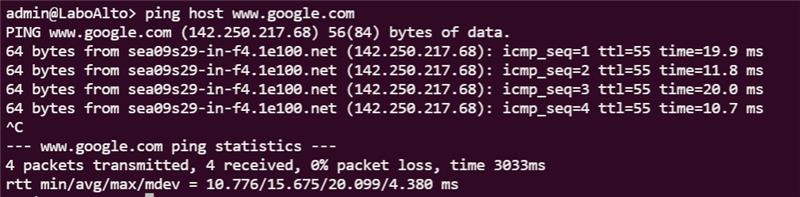












Problems

We have not encountered any major problems while configuring the OSPF lab. But we did encounter some small mistakes during the lab. one problem was Palo Alto does not connect to the internet, but when devices are connected to LAN ports the devices do have access to the internet. By going through the configuration instructions, we found that there were some things that were misconfigured, and then we were fixed to connected to the internet after a reboot. Another problem was that when we wanted to commit changes, Palo Alto would not commit changes due to an unused virtual wire interface. We fixed the problem by deleting the virtual wire interfaces. These were the major problems we encountered

Conclusion

The objective of the lab was to be able to set up or create a SOHO configuration on the Palo Alto (A220) 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.