SOHO

*Palo Alto – Main Configuration*

Adv Cisco Cybersecurity – Lab 2

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 2: PA 220 – SOHO Configuration*

**Purpose**

The objective of the lab was to understand and configure the Palo Alto Firewall for Small Office Home Office (SOHO) configuration. That is, through accessing the Palo Alto GUI, to configure network and interface elements of the firewall to allow protected access to the internet. The internet should be able to be accessed wiring through the PA 220.

**Background Information**

Configuring the firewall to be able to access the internet is the most important step in setting up a firewall for use. However, to configure the policies, zones, and ports, the management port needs to be accessed. Palo Alto has a management web Graphical User Interface (GUI) that contains all the menus that control the configuration of the device. During the setup, we create zones and policies for configuration ready for the Internet.

A Security Policy is the essential building block of cybersecurity. Security Policies are the configured rules that determine whether to block or allow the session based on the incoming traffic’s attributes – the source and destination IP address, the source and destination ports, the application, the user, the service, and its corresponding security zone. The firewall attempts to match the traffic with the session and evaluates its decision and resulting actions depending on predefined rules. If it is matched with the defined rules, the Security Policy action is applied to bidirectional traffic in that session. For traffic that doesn’t match any defined rules, the default rules allow all intrazone traffic and deny all interzone traffic. It’s important to note that Authentication Policies are processed before Security Policies. This leads to zones.

A Security Zone is a Palo Alto networking concept which acts as a virtual “zone” that includes switches, interfaces, ethernet connections, and VLANs, and more. Firewalls *won’t* process traffic from any interface unless it is part of a Security Zone. One use of a security zone is that it can serve as a demilitarized zone that includes multiple VLANs with backup firewalls. Zones are created in this lab to separate external and internal traffic for the outbound and inbound interfaces, respectively, since it is required for the interfaces to be attached to a zone.

A Security Profile can be interpreted as an extension of a Security Policy rule. If traffic matches the “allow” rule defined by the Security policy, Security Profiles are applied to **scan traffic**, scanning for threats, viruses, DDOS attacks, and other cybersecurity threats. They are not used to determine traffic flow, but simply to scan traffic after the application or category of site is allowed. Multiple Profiles can be congregated to a Security Profile Group so only the group needs to be applied to a Security Policy, rather than several individual Profiles. Palo Alto has default Profiles for the elements of a firewall. These are used for the lab.

Palo Alto firewalls also have a lot of Interface and Zone configurations options. This provides the flexibility that serves many needs in real world deployments. Zones have 4 main types:

* **Tap Zone**. Passively monitoring traffic to their servers without any changes to the network infrastructure. Done using the SPAN/mirroring feature coming from the ports of a switch. Allows visibility of application, user, and content, but is unable to control traffic.
* **Virtual Wire**. Using Virtual Wire interfaces, the firewall can be inserted into an existing topology without any changes to the network infrastructure. Allows administrators to monitor and control traffic, supporting features like App-ID, User-ID, Content-ID, NAT and decryption.
* **Layer 2**. Switching can be performed between LANs. Capable of having Access and Trunk Links from 802.1Q trunking. Provides increased security and visibility within the internal network.
* **Layer 3**. Routes traffic between multiple interfaces, each with an IP address and attached security zone. Interfaces can obtain an IP address from a configured DHCP server in this mode. This deployment option is the most popular.

Physical Ethernet interfaces, as they have to be part of a zone, naturally follow the same 4 types above, along with other unique ones, such as the Aggregate Interfaces and High Availability (HA) types. Logical interfaces (Layer 3) can be a VLAN, Loopback, Tunnel, or Decrypt Mirror interface.

Layer 3 deployments are used most for the interfaces in this lab since the firewall needs to be able to route IP addresses to the internet and back.

**Lab Commands**

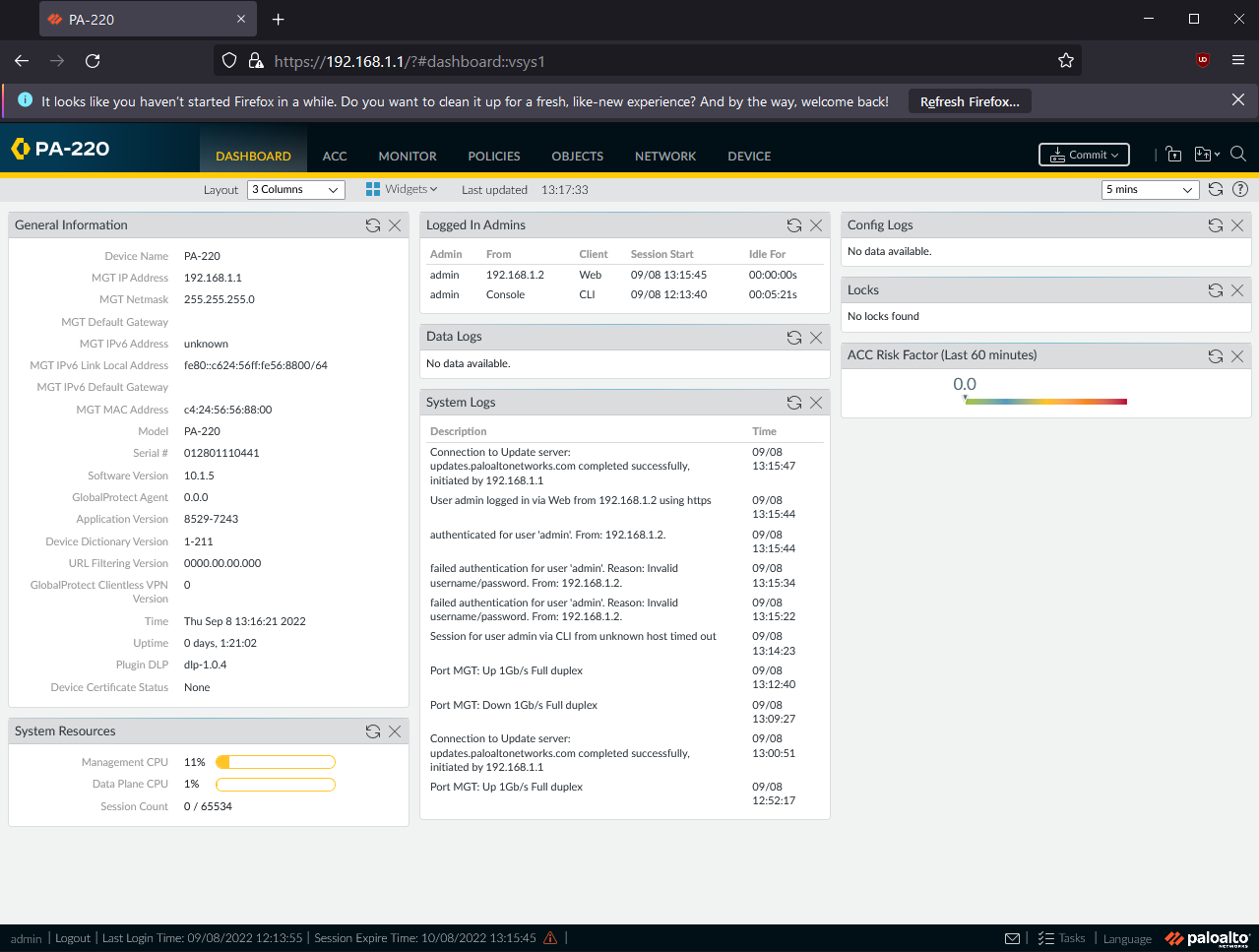
Most configuration was done through a web Graphical User Interface (GUI). However, there are a few show commands on the CLI that are useful in seeing IP configurations relating to the management interface.

**show system info***–* Displays the Management Interface’s IP address, netmask, default gateway settings, among many other loaded configuration. This is similar to a general show running-configuration for Cisco routers.

**show interface management** *–* Displays interface level details such as speed, duplex, etc. for the Management Interface.

**Lab Summary**

This process is complex and has many steps. Configuration follows portions of the general SOHO setup here: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFkCAK>.

 First, the Graphical User Interface (GUI) of the Palo Alto needs to be accessed. By accessing the Management Port through an ethernet, which has a default management IP of 192.168.1.1, we can access the webGUI by inputting that management IP address into a browser. Mozilla Firefox was used. However, the PC’s address has to be in the subnet of the IP address to access it. So, we changed the PC IPv4 address to 192.168.1.2. Entering the management GUI by entering 192.168.1.1, the browser greets us with the Palo Alto login screen. The credentials should be the same as the ones configured during factory reset (See *Lab 1: Factory Reset*). The GUI should have multiple tabs and many menus.

The main dashboard of the webGUI. Note the Management Interface Address is default, at 192.168.1.1.

Next, Security Zones need to be created. Three zones were created, one “outbound” Layer 3 zone, and 2 “inbound” zones, one that is Layer 3 and another that is Layer 2. Of the 8 Ethernet ports, the first one – port ethernet1/1 – will be used to connect to the internet. At this point, connect a UTP from this interface to the switch or router that ultimately routes to the ISP modem. The firewall should not be linked to the Internet. Then, Configure ethernet1/1 to the outbound security zone (named Untrust-L3 in this lab) and have it retrieve addresses via DHCP.

After assigning ethernet1/1 to be an outbound interface, the other physical interfaces should be inbound. This means that a VLAN should be created that encompasses those inbound interfaces. Create a VLAN object before configuring 3 Ethernet interfaces to be assigned to that VLAN object. Also configure those interfaces to be a part of the Layer 2 inbound Security Zone. An issue we faced was assigning the VLAN to be a part of a default VLAN interface which was not properly configured (see *Problems*). This was later solved by assigning to the VLAN interface we create.

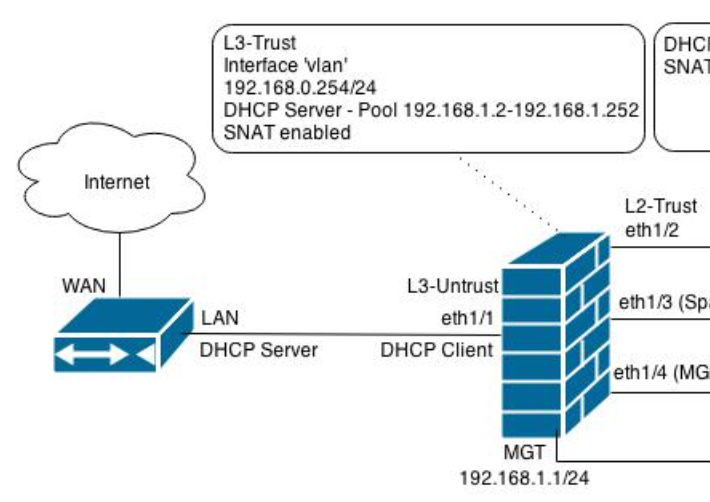
Continuing, configure a VLAN interface, preferably not numbered “one” for best practice, and assign it to the inbound Layer 3 zone and the created VLAN object. This will be the gateway for the DHCP server. By assigning the DHCP to a physical interface, the DHCP will source DHCP leases through it. This means that the DHCP server will retrieve all its information from that interface and gateway, inheriting other information it can. Afterwards, create a pool that doesn’t include any conflicting, used addresses. At the end, the DHCP server should be functional.

Lastly, we will create a security profile group that will be applied to an Outbound Internet Security Policy, and again for the Outbound Internet NAT policy. Each Security Policy requires a source and destination zone, and these will originate in the trusted inbound zone and push through to the untrusted outbound zone. These policies are essential to remain secure and protected while accessing the internet.

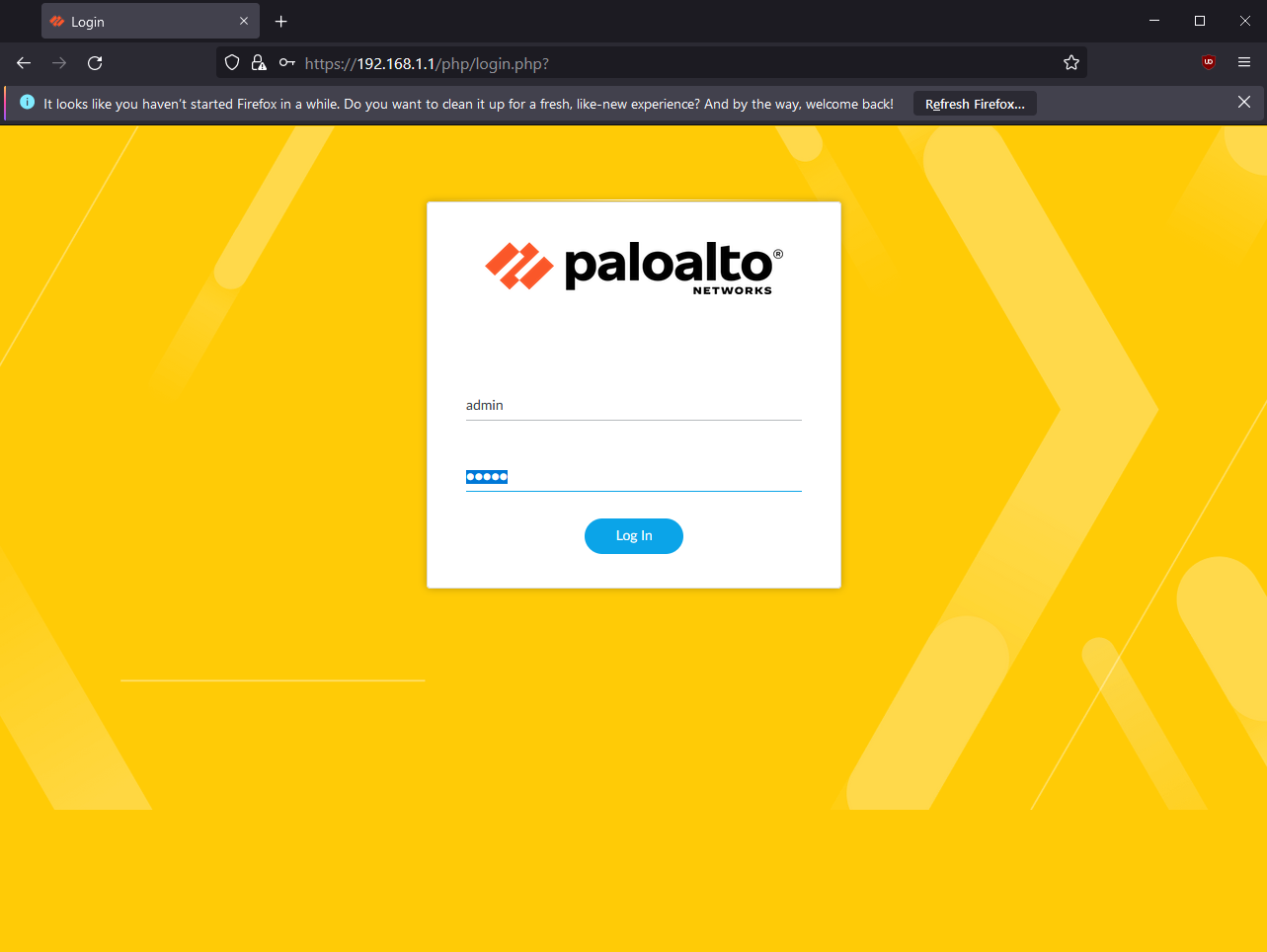
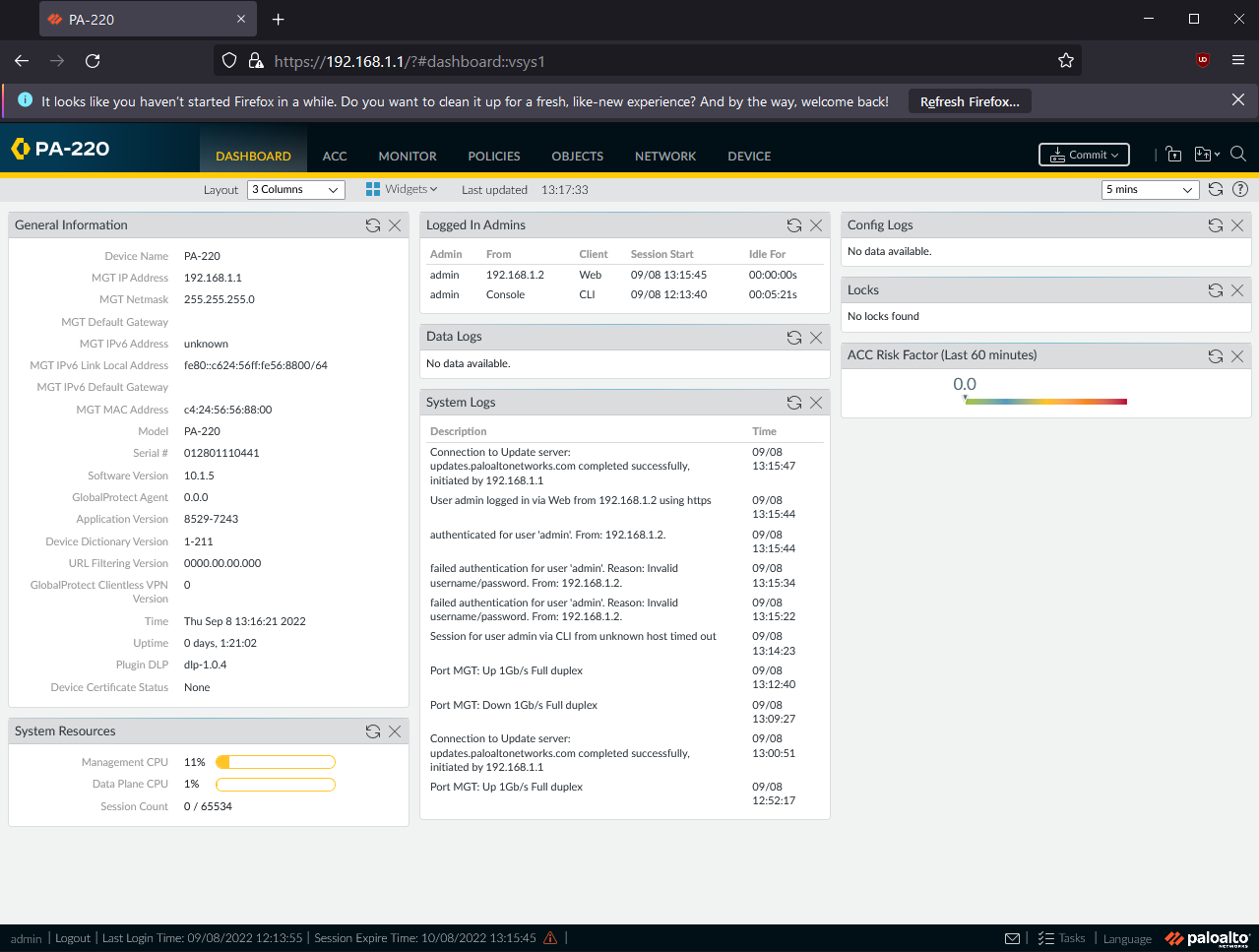
Optionally, you can change the Management Interface to accept different services like HTTPS, SSH, Ping, etc. as well as general addressing changes. DNS servers should also be changed and configured to a valid DNS server for proper function.

Once changes have been committed in the WebGUI, the SOHO configuration is up and functional. Wired connections via ethernet through the firewall should have proper internet access as well as its policies protecting the client computer.



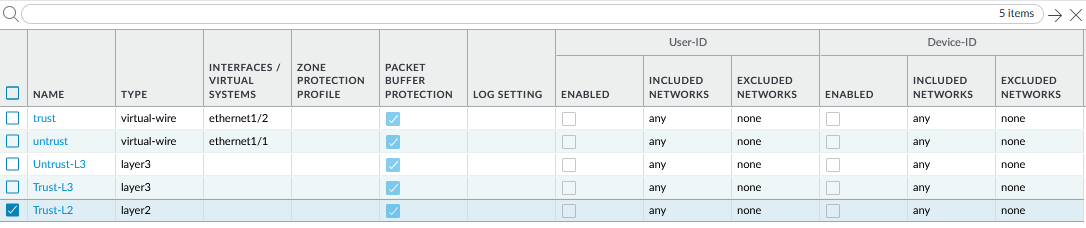
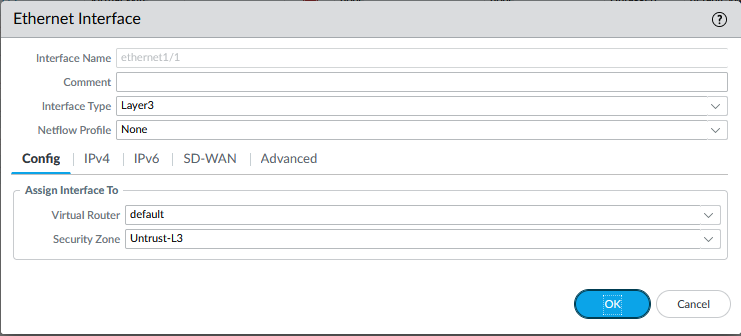
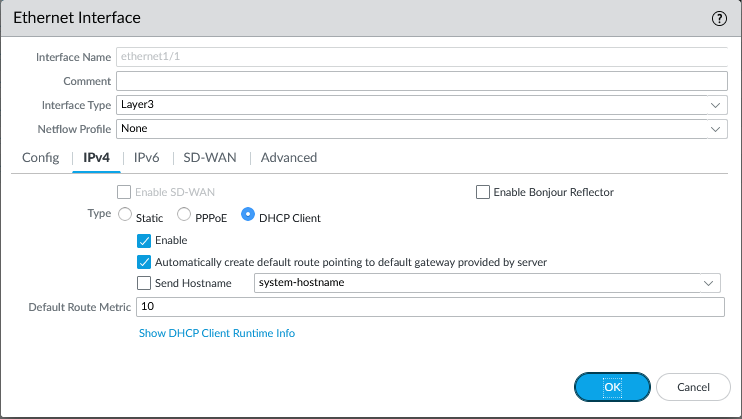


**Procedure**

**** Change the PC’s Ethernet interface address to one inside the 192.168.1.1/24 subnet and connect to the management port.

Access the WebGUI by opening a browser and entering the default management IP, 192.168.1.1. Credentials are admin by default for both fields but the password must have been changed during factory reset (See Lab 1: *Factory Reset*)

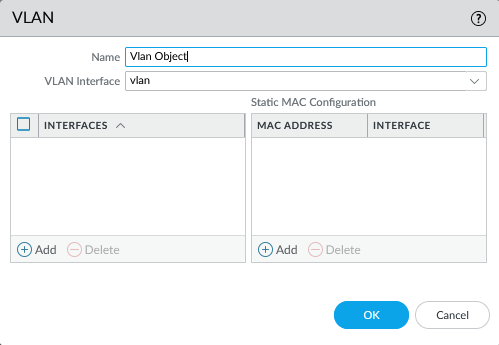
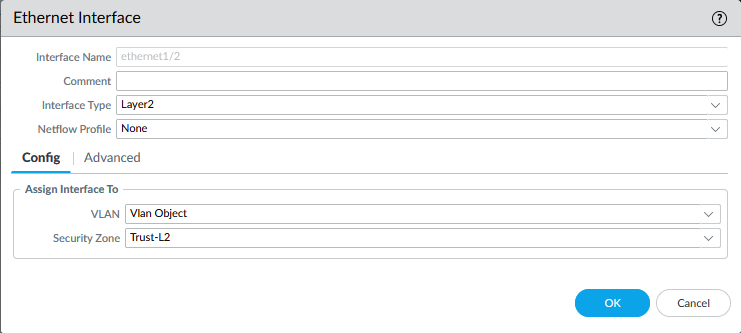
The main dashboard of the WebGUI.

****

As it is a Layer 3 interface, IPv4 must be configured. Choose it to be a DHCP client.

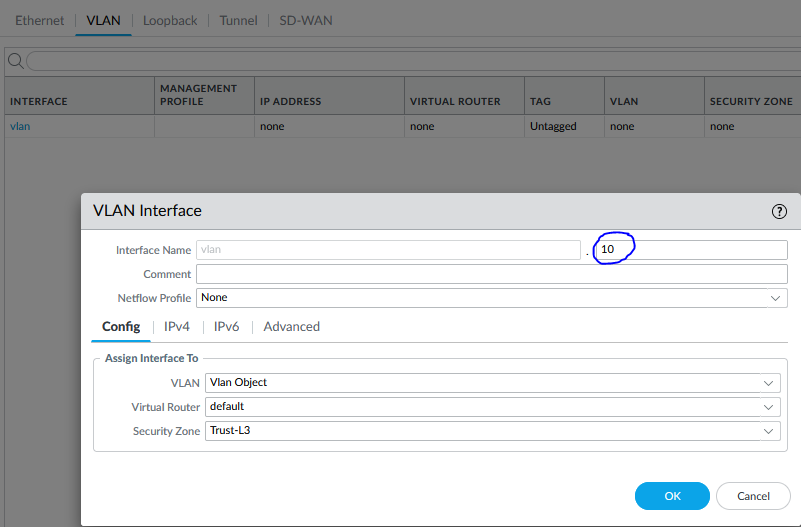
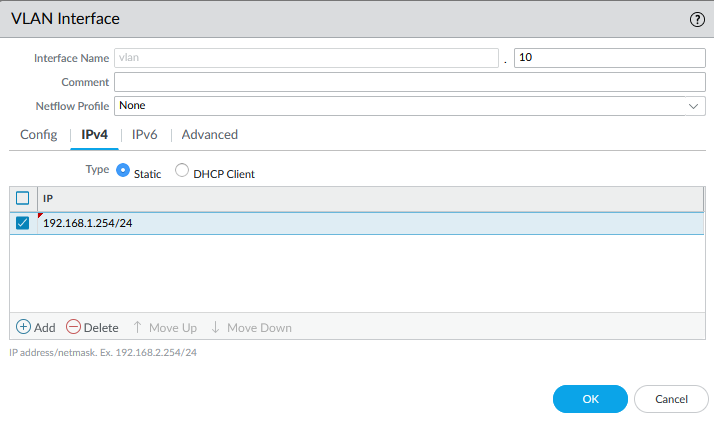
Configure the ethernet1/1 interface to be assigned to the outbound zone.

Create Security Zones. One outbound zone, two inbound zones.

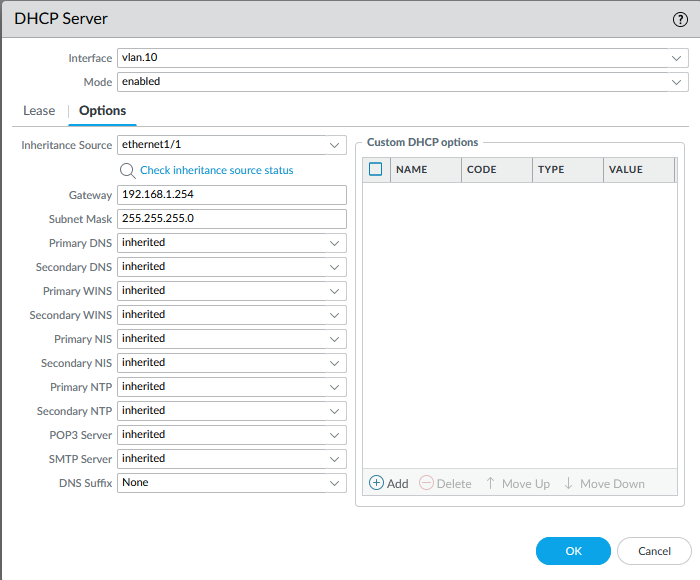
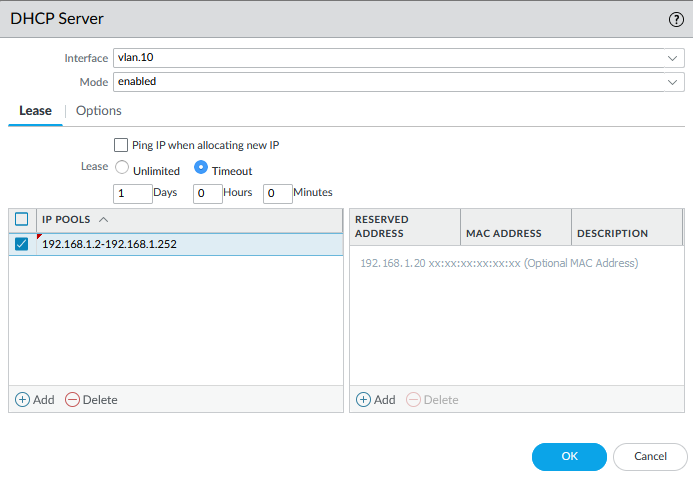
****

Configure the rest of the Ethernet Interfaces to be Layer 2 and attached to the internal Security Zone and VLAN. Interfaces ethernet1/2, 1/3, and 1/4 were repeated and configured for this lab.

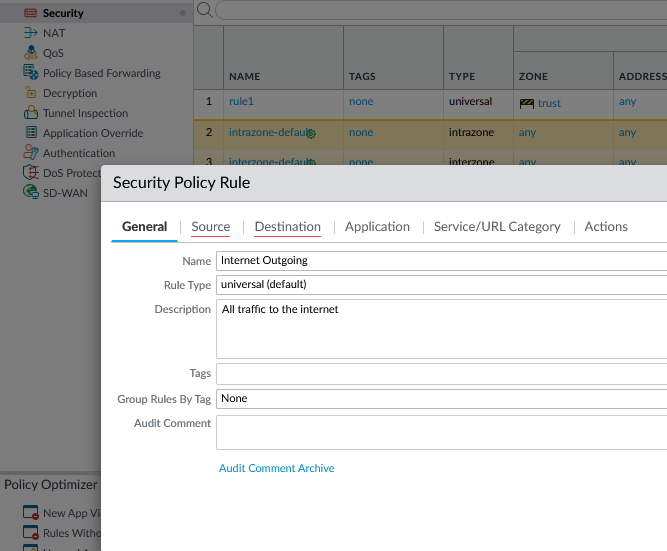
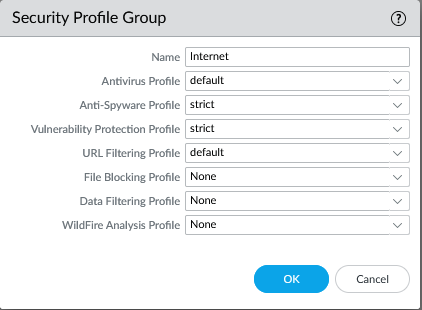
Create a VLAN. This VLAN was named “Vlan Object.” Assign it to a vlan interface.

****

Create a VLAN interface. Do not number it “1” for best practice, as vlan.1 is reserved for other uses in certain circumstances.

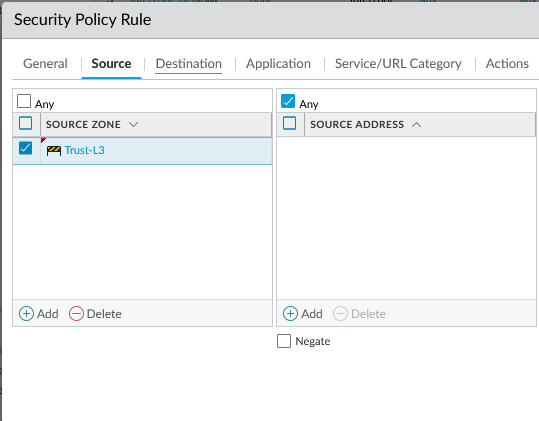
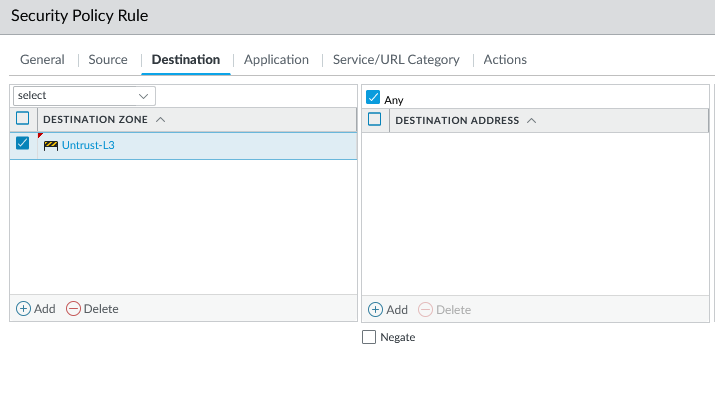
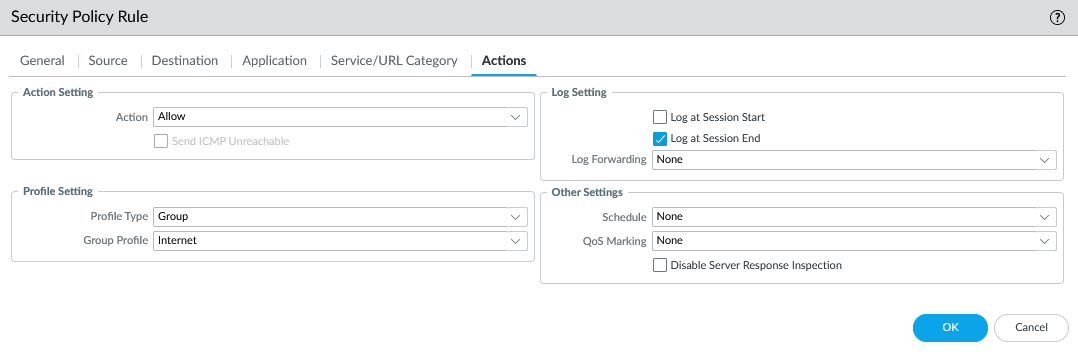
****

Create the DHCP Server to retrieve and inherit information from ethernet1/1, the interface that is tied to the outbound interface. Assign the gateway to the vlan interface IP. Finally, create the IP pool. The rest of the host addresses are used.

****

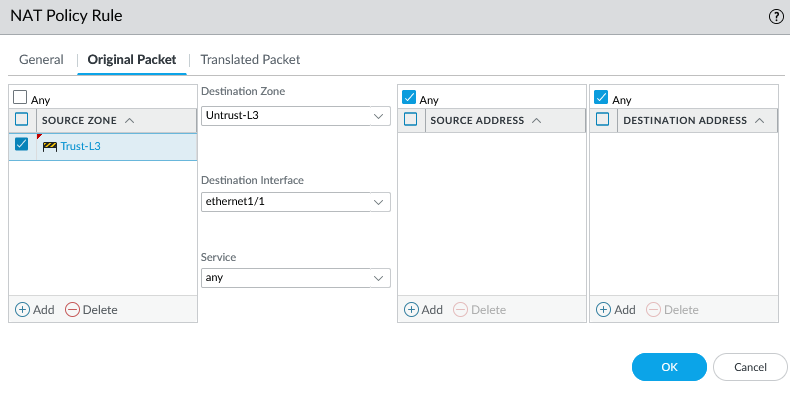
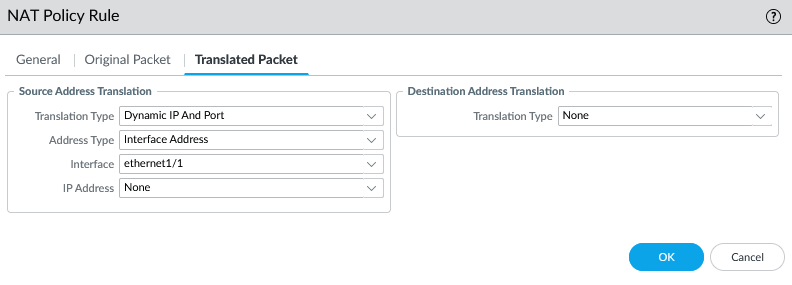
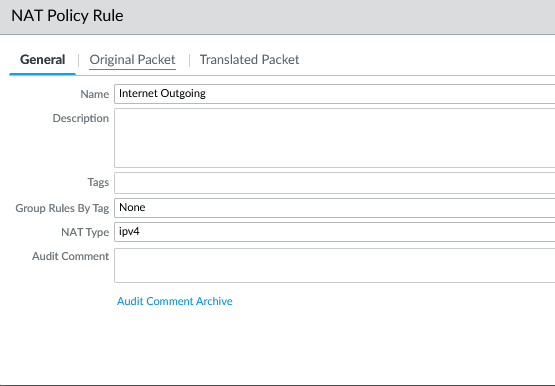
Create a Security Policy Rule. Make it a universal rule as well as giving it an optional brief description.

Create a Security Profile group, consisting of many Palo Alto default Profiles. This will be applied to the Security Policies.

****

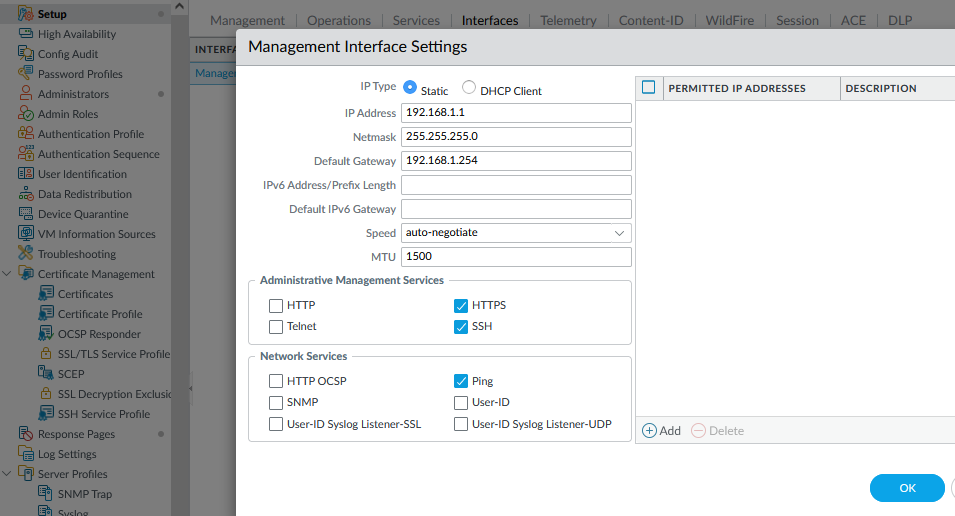
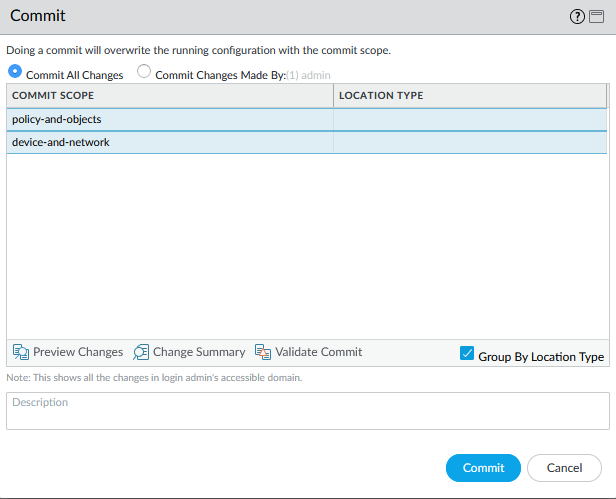
Let it be an “allow” action and assign the profile group.

Assign source and destination zones. It is sourced in the inbound zone, and destination to the outbound zone.

****

Similarly, create a NAT policy rule with the corresponding source inbound and destination outbound zone. The outbound interface is ethernet1/1.

Configure translated packet settings, too, including Translation type and interface.

****

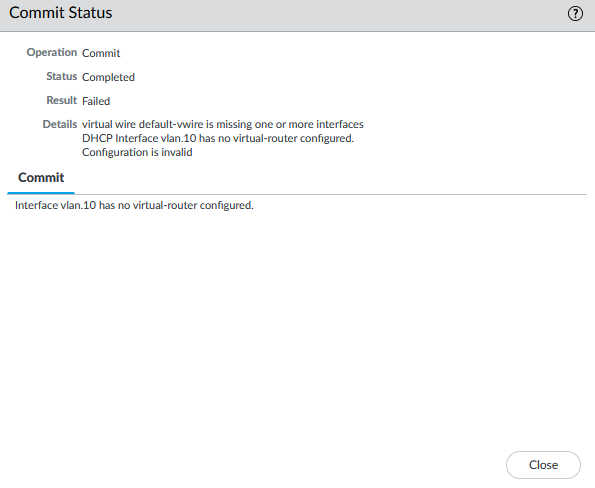
Select “Commit” and commit changes to save all configurations to the firewall. The firewall should now be functional. Completion continued in *Problems* section.

For best practice, configure the Management Interface to a new IP and allow certain administrative management services. We kept the interface address default.

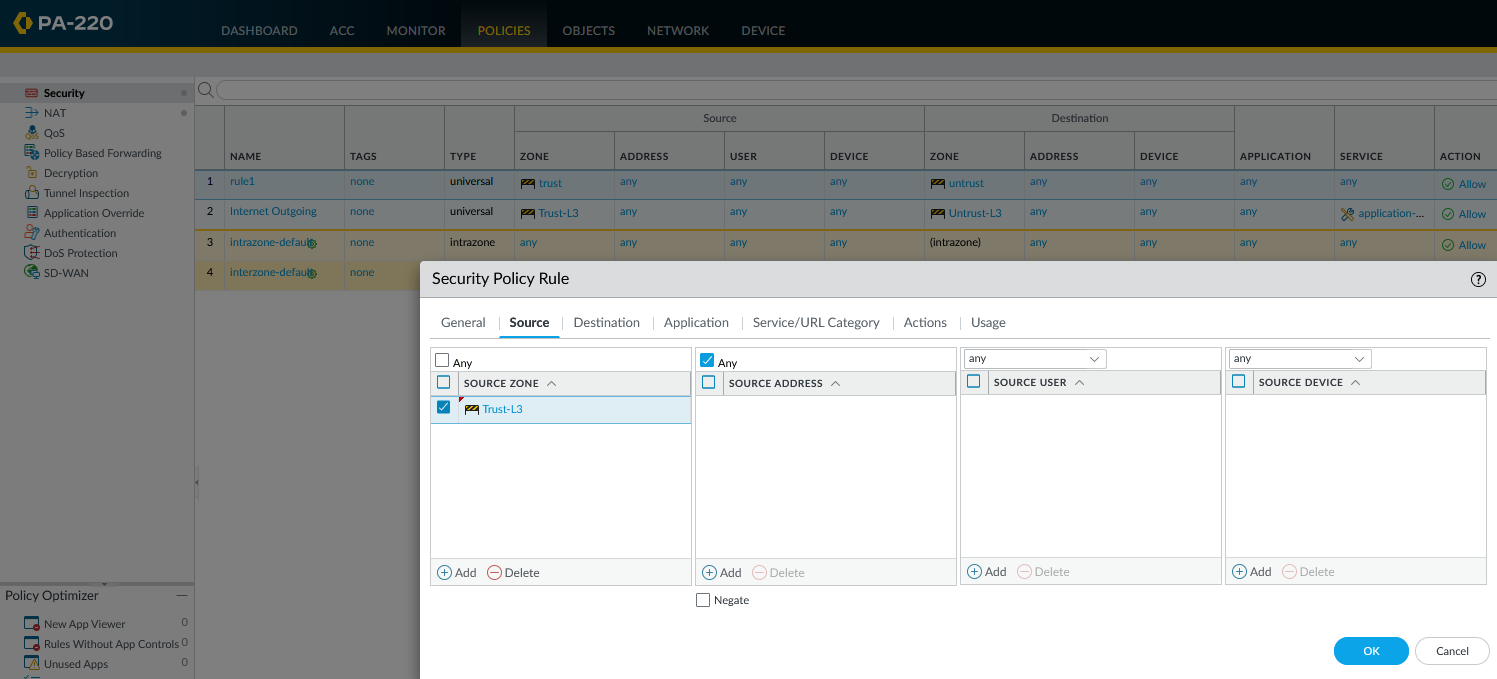
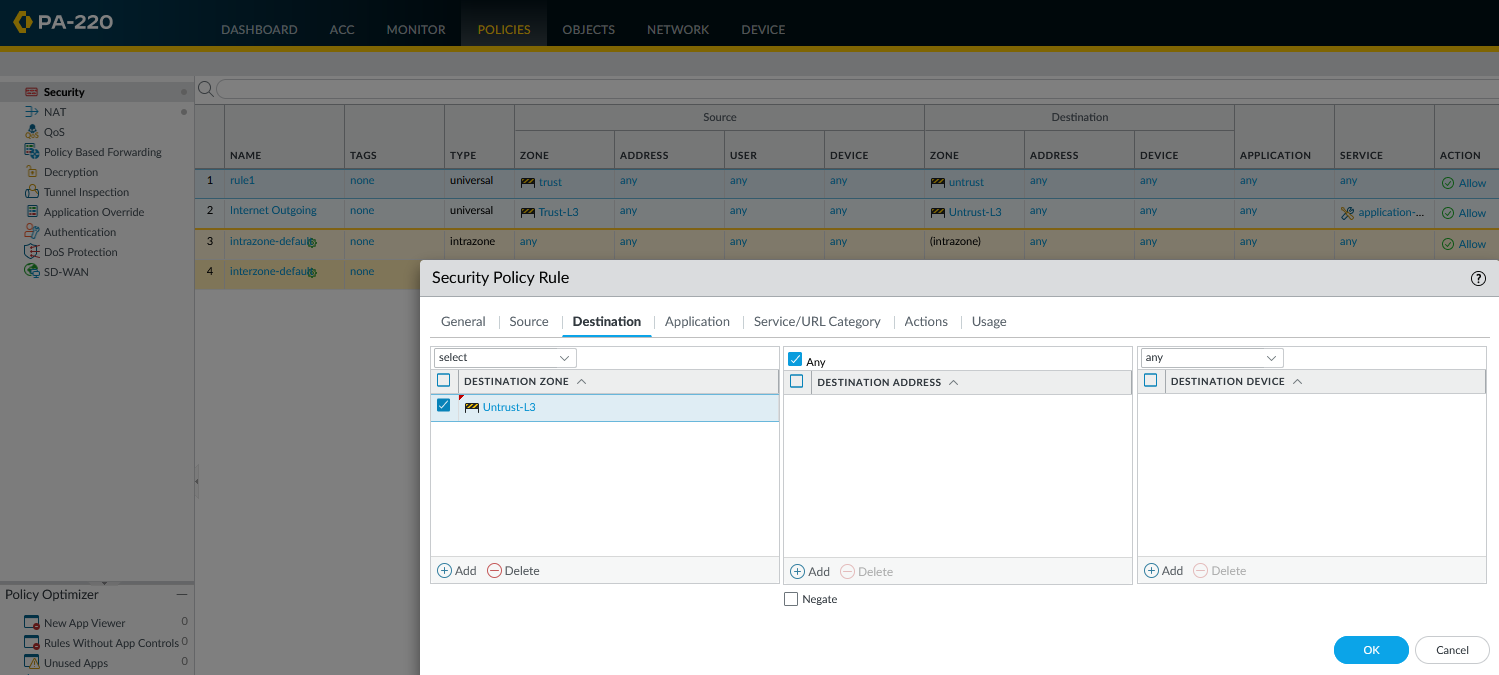
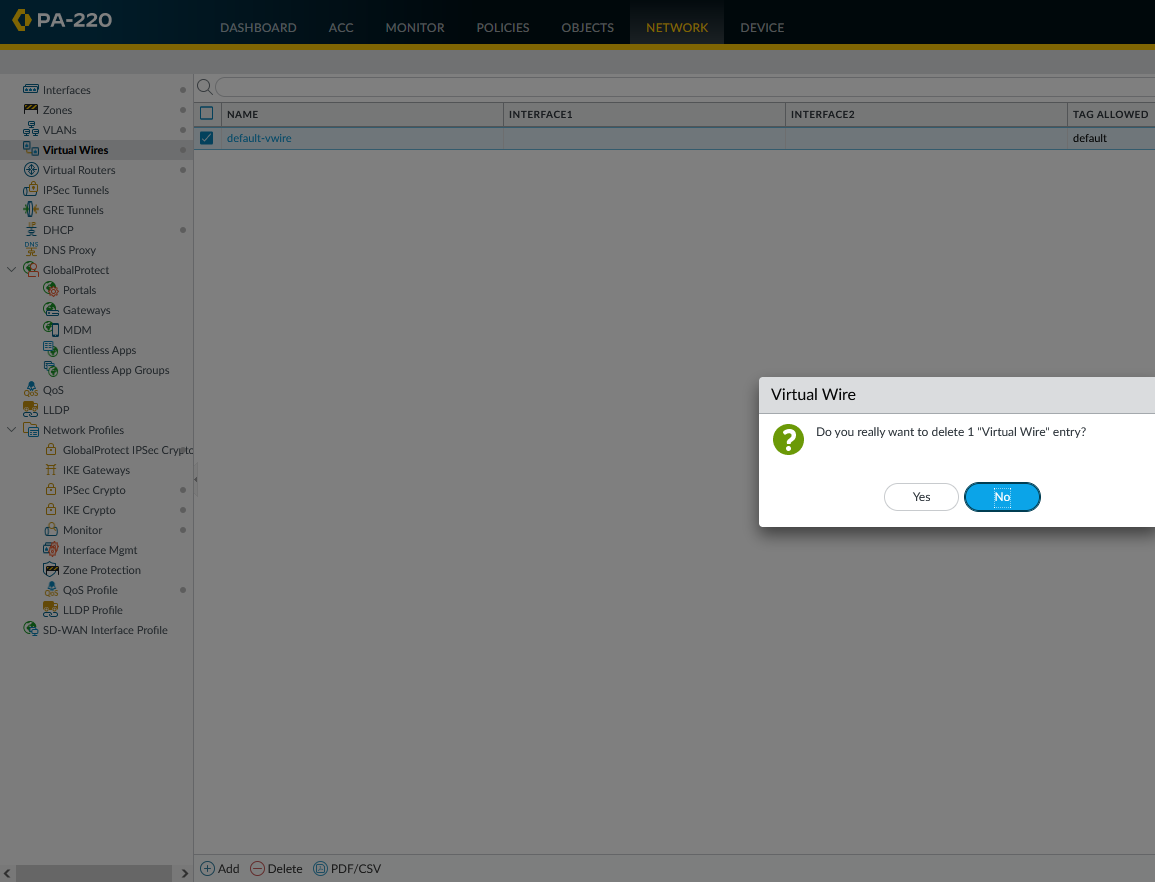
**Problems**

There were many problems of all scales. Some were small, IP addressing issues while others required new profiles or zones to be configurated to recuperate functionality. The first problem started off with simply not being able to access the web GUI via Ethernet into the Management Port. We didn’t know the PC address had to be changed, nor did we know that it couldn’t be the default address of 192.168.1.1. With just a few swift changes, such as changing the PC’s address to 192.168.1.2, we managed to access the web GUI.

VLAN interface. In the SOHO configuration forum that we followed, the VLAN object is attached to the default VLAN. However, it followed an older version of the PAN-OS. Newer versions created more VLANs and its detail options, including numbering the VLAN interface. This meant that the VLAN object has be assigned to the new VLAN interface, or else the VLAN functions simply did not work with the Layer 2 Ethernets. Tying everything to the VLAN interface solves this issue. The default vlan is not needed anymore.

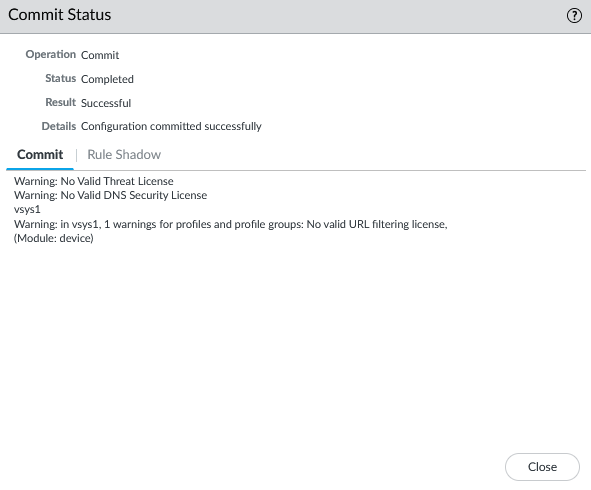
 After the main configuration, there was a substantial commitment issue. Committing changes means saving the settings to the router, and it didn’t allow us to commit due to a Virtual Wire issue: the default-vwire is missing one or more interfaces. As virtual wires have been assigned to the default elements of the configuration, they aren’t properly set up. By navigating the parts of the firewall such as the default policy rule’s source and destination zones, we first remove all elements connecting and utilizing the virtual wire interface. Then, the solution is complete by deleting the vwire interface. Committing changes are then successful, and only the interfaces that we have configured remain.

Commitment failed due to default-vwire misconfiguration.



Delete Virtual Wire.

Change source and destination zones of the default Security Policy Rule named “rule1” so it does not rely on default vwire.



Without Virtual Wire, and not needed in SOHO configuration, commitment status is complete.

We also had trouble with accessing the internet. While directly connected, the client computers still were unable to access the internet, whereas through other means, such as WiFi or to a router, internet access was fine. We learned that this issue derived from the lack of a default gateway on our PC. By switching the IPv4 address to be obtained by the DHCP server, accessing the router through the firewall let us access the internet as it should.

The last minor conflict was taking our time figuring out how to connect to the management interface through the main L2 zone rather than having to directly connect to the MNGT port. This was done by “jumpering” the cable from the MNGT port to the main LAN within the L2 zone. This means that accessing the LAN from outside the firewall, one may access the WebGUI. This is useful and often used in real world and industry deployments.

**Conclusion**

This was a long and convoluted process. However, achieving this configuration as a great accomplishment that is incredibly practical. From the use of the management port to the navigation of the web GUI, and finally to the designation of different Ethernet ports bound to different zones, this lab holistically taught us the different properties of the firewall as we interweaved through all of its interface utilities.