**Diamond Headscape with a body of water

Description automatically generated**

**SOHO Palo Alto**

**Configuration**

Ryan Chen

10/5/2024

**Purpose:**

The primary purpose of this lab is to setup a basic small office home office configuration suitable for the PA-220 firewall. This configuration involves setting appropriate VLANs, trust/security zones, and DHCP configurations in order to provide client machines with access to the internet. As a result, basic SOHO configuration provides an easy, gentle introduction to Palo Alto firewall utilities and functions.

**Background Information:**

Barebones configuration is commonly referred to as a SOHO or Small Office/Home Office setup. Traditionally, this means that the network will be used at a small scale for a limited number of clients. As a result, the config is robust at a small scale, and easy to setup. Despite these advantages, SOHO networks are often limited in future growth and must be upgraded to support anything larger scale.

Before utilizing a firewall, configuration must be done in order to prepare the device for use by clients. This involves setting up Dynamic Host Configuration Protocol (DHCP) to automatically provide client machines with IP addresses, which ensures that all devices can reach to the internet.

Our lab makes use of an upstream internet provider that already has DHCP leasing system set up for its clients. Thus, as a client, we can configure the firewall to receive a DHCP address on a specified interface, and then internally host a DHCP server to provide local clients with internet access. This would mimic a normal scenario where an ISP gives out a DHCP address for your upstream connection.

Leasing addresses is the act of giving out a specific IP address from a pool of addresses for clients connected. These addresses have a “lifespan” attribute attached to them, and after the time is up, they will need to renew another address. This ensures addresses are always moving in circulation, which is optimal in a network where devices are constantly connecting and disconnecting to the internet, such as a SOHO network.

To follow best practices, we must also adhere to basic security principals to ensure that traffic is tagged accordingly. Palo Alto provides Security Zones for this purpose. These zones are logical ways to group physical and virtual interfaces on the firewall and can be used for future monitoring and filtering. By default, traffic is restricted to within the zone, but can be configured using Security Policy Rules to allow multiple zones to communication with each other.

Within this lab, security zones and VLANs are used to separate trusted and untrusted interfaces/regions. Virtual Local Area Networks, or VLANs are used to separate physical interfaces through software, aka logical means. They operate on networking devices to segment traffic based on the address number. This allows devices to communicate specifically with other devices in a defined address number. Devices that are not in the same VLAN must be configured in order to allow them to communicate with each other. The inbound interface that acts as a DHCP client is configured as Untrusted, since traffic is coming in from the internet. The port facing the LAN side that assigns DHCP addresses is Trusted since it is internal to the firewall/network.

**Lab Summary:**

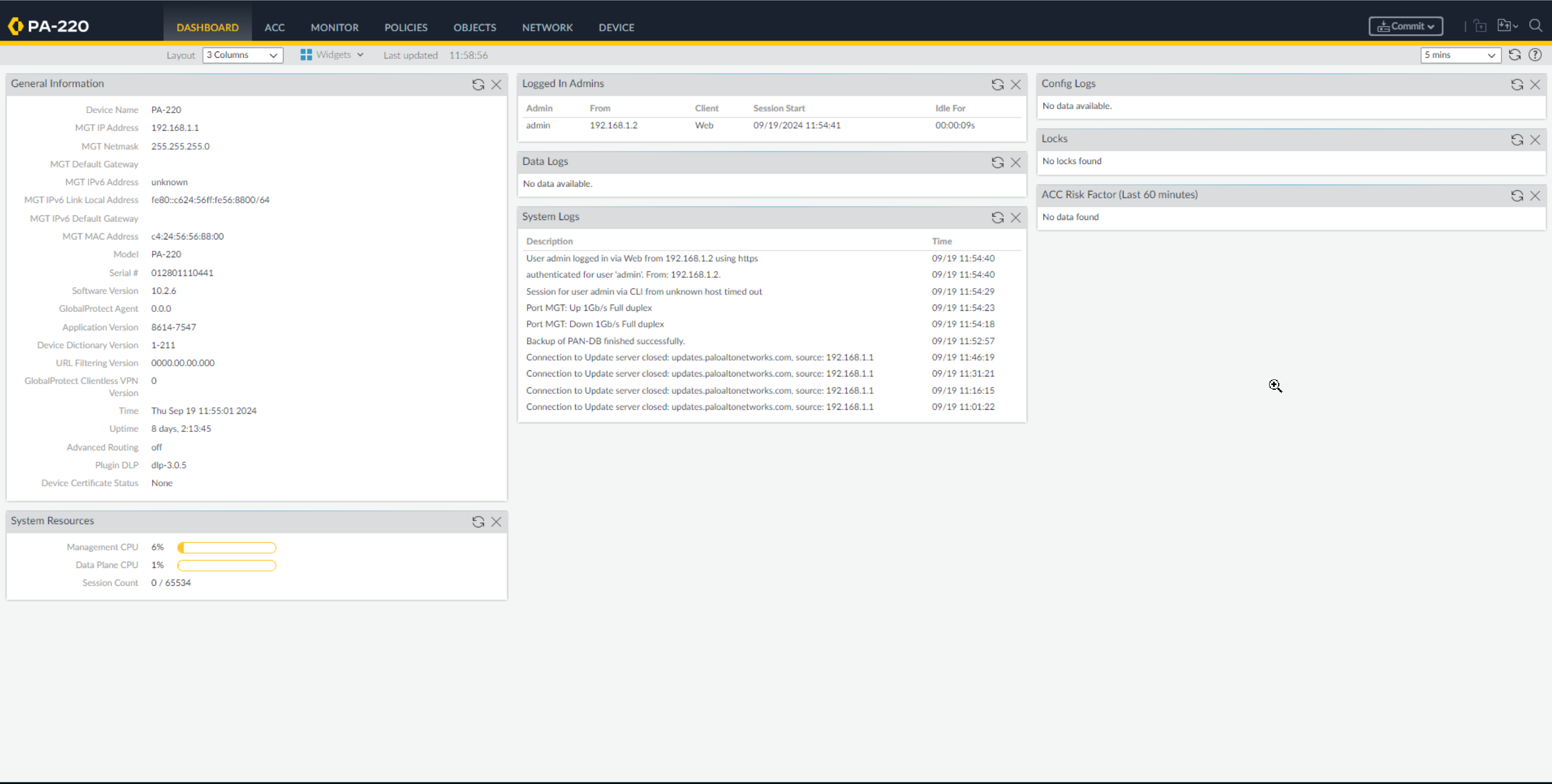
This lab involves a few relatively simple steps. First, DHCP is configured both inbound and outbound, providing internet connectivity to individual devices on the network. We can accomplished this by setting the outbound interface to act as a DHCP client and receive an address from an upstream DHCP provider (ISP). Then, we can configure the inbound interface to host a DHCP server that dynamically allocates addresses to all connected devices. Along this process, we should tag the interfaces using the correct VLANs and Security Zones for easier configuration in the future.

Once this is done, we should configure a Security Policy to allow traffic to flow through, which will establish internet connectivity if the DHCP server has already leased out the addresses. NAT should also be given a policy to allow the inner DHCP server addresses to be translated outward to the address given to the outbound port. This is crucial in allowing the clients to all reach the internet using one single ISP address.

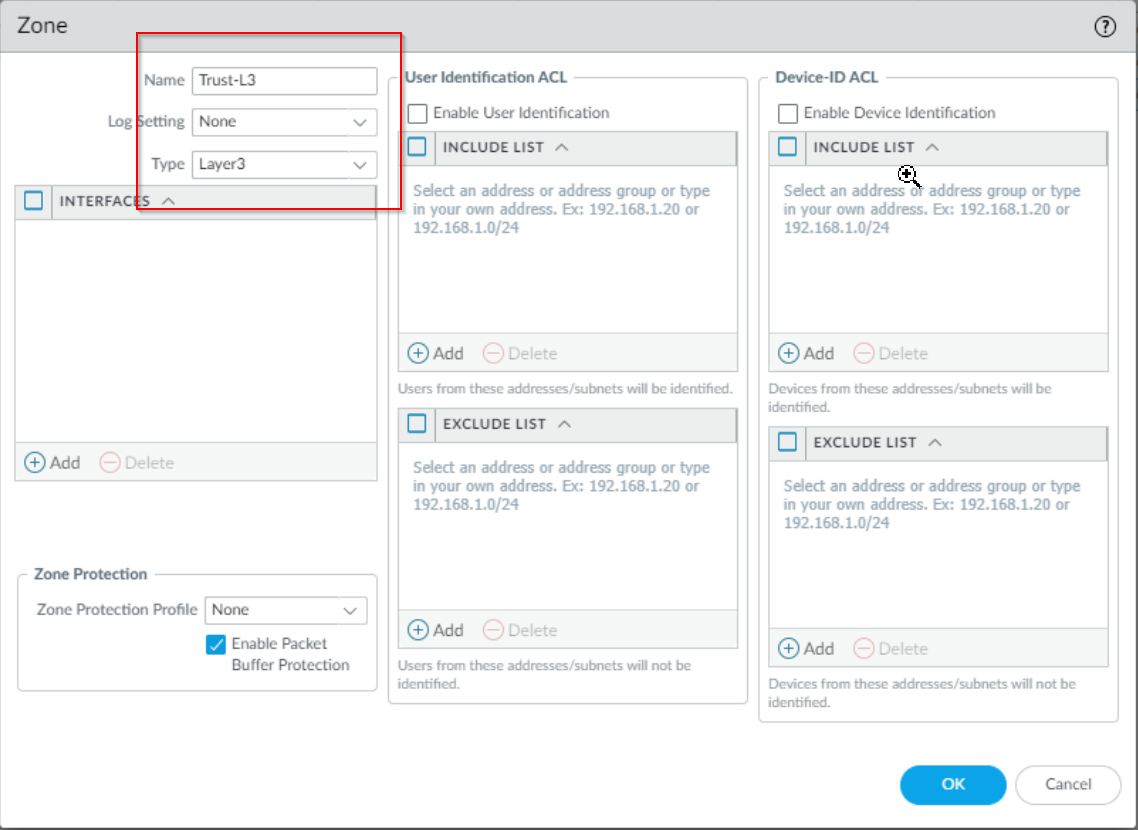
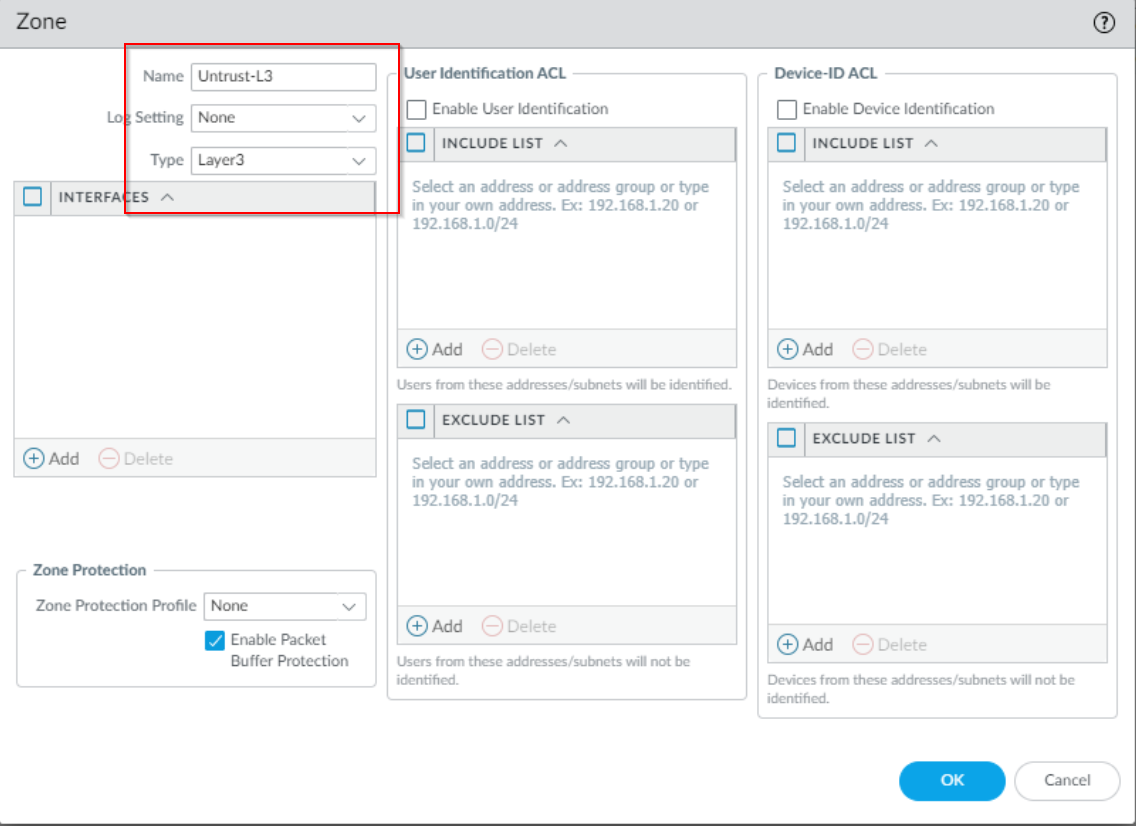
Finally, we can set the default management IP for future configuration and the default DNS servers to allow clients to automatically surf the internet. DNS is necessary so that domain names (such as <https://google.com>) is directly translated to the corresponding IP.

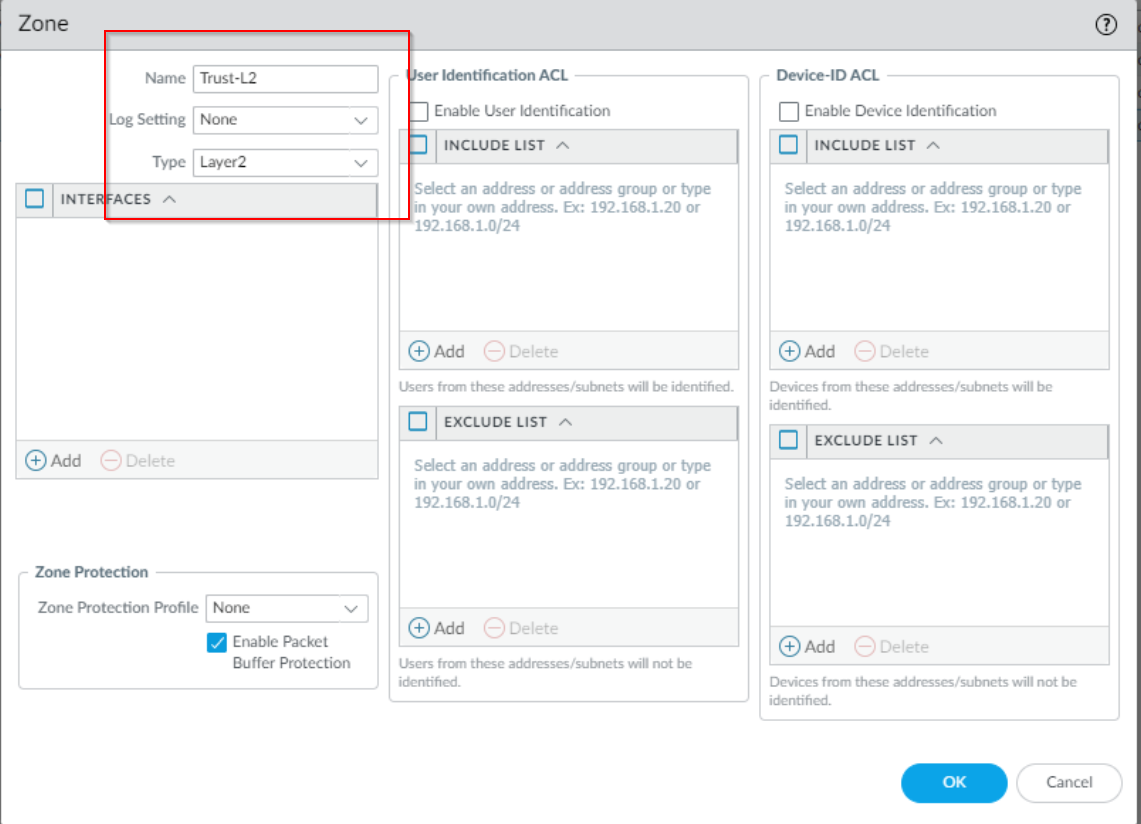
**Lab Commands:**

1. Ensure the interface is up and running, with nothing wrong on the dashboard. Make sure you can reach the firewall at the default address.

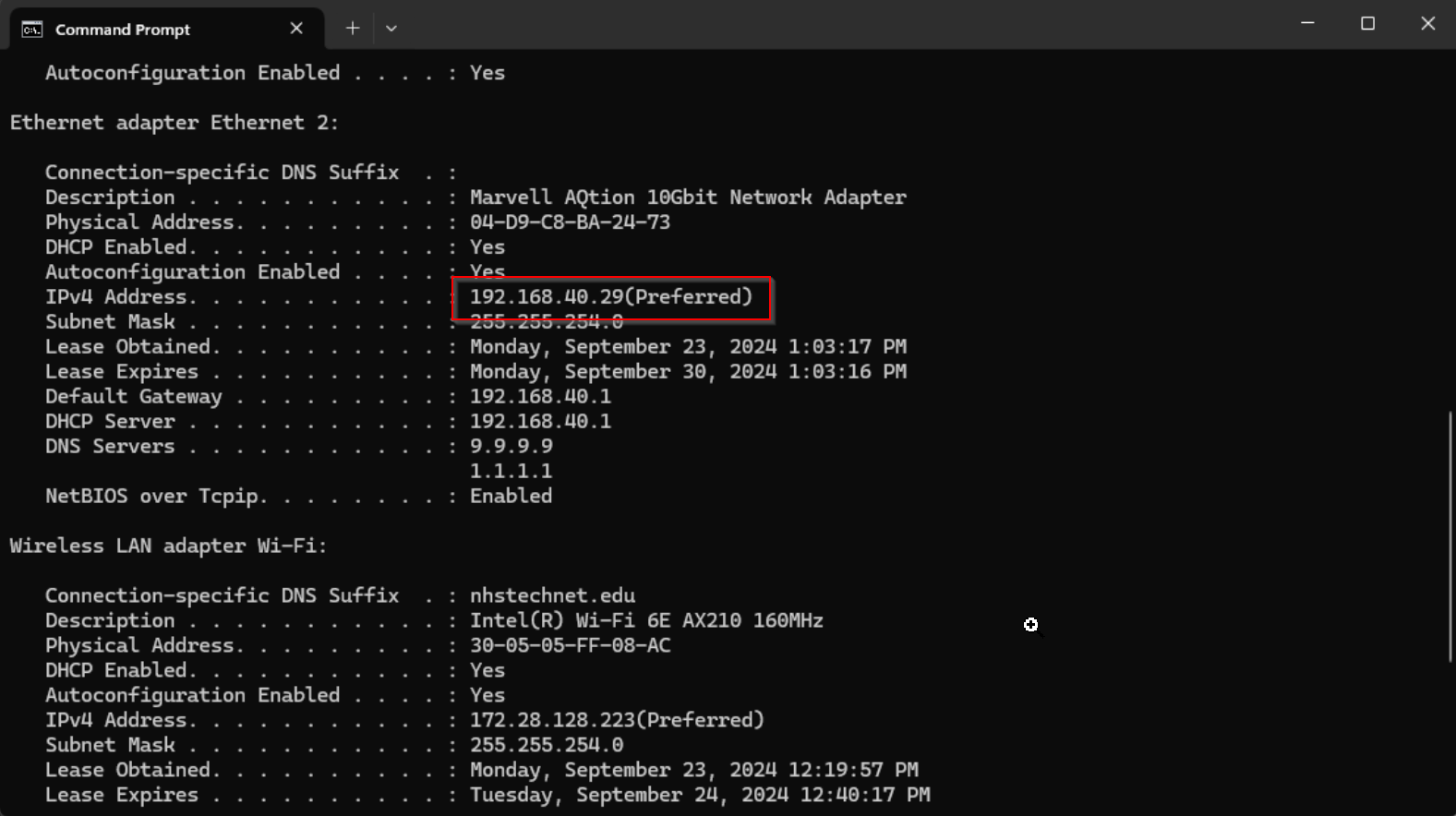


1. Make the Security Zones: Trust-L2, Trust-L3, Untrust-L3.

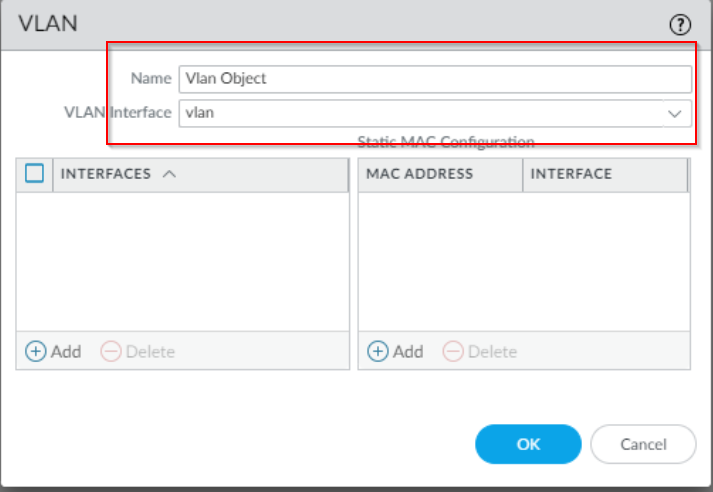




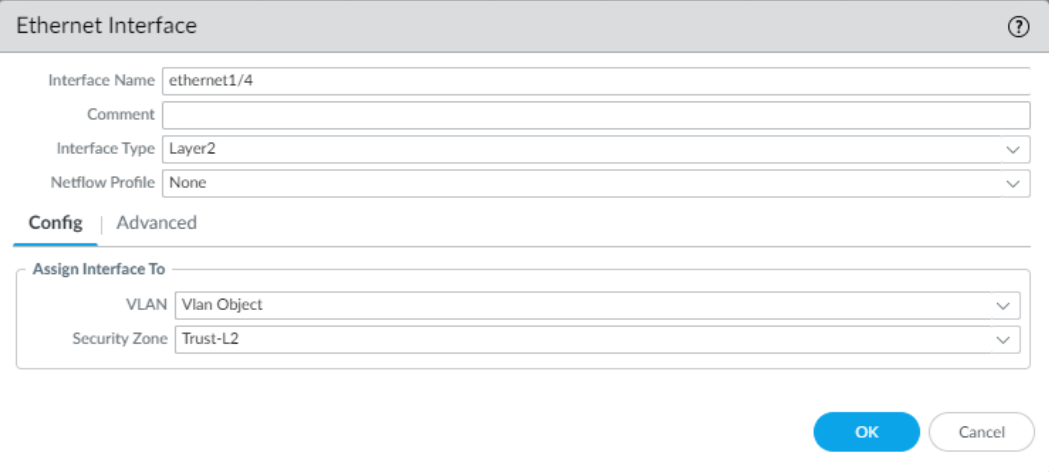
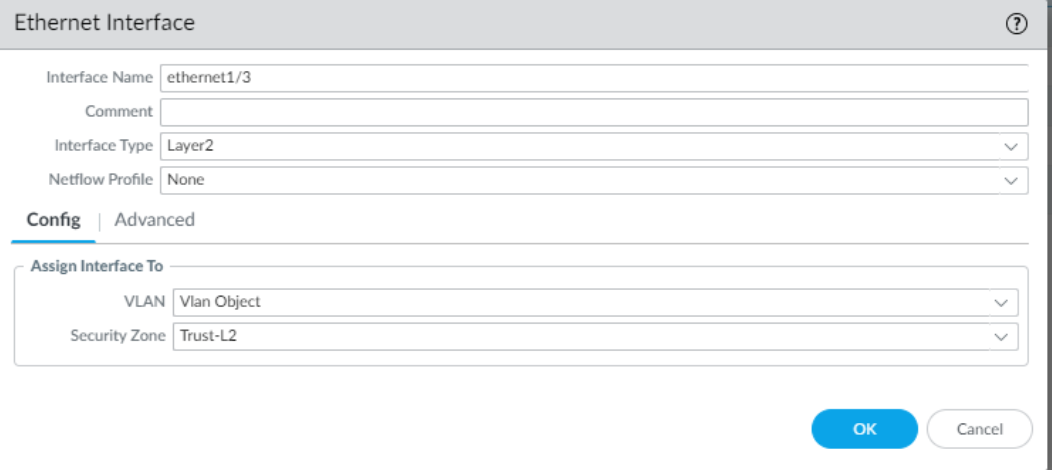
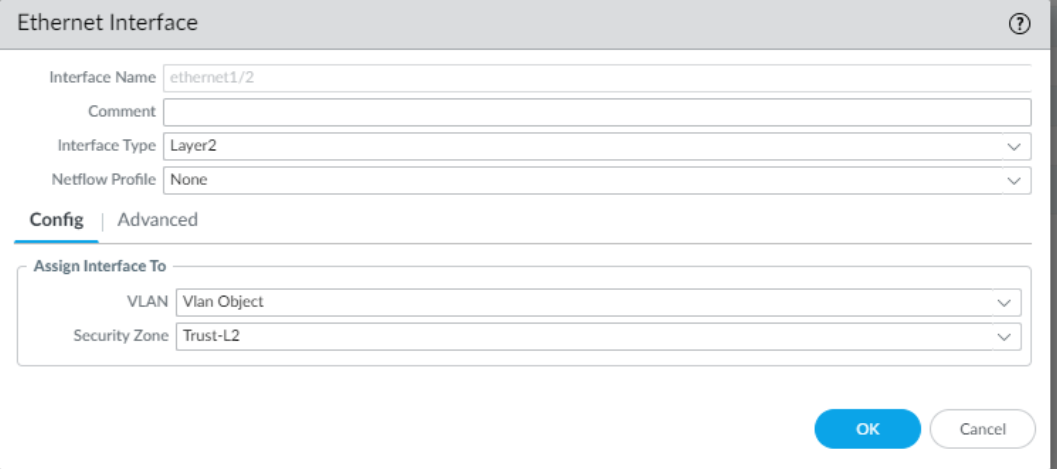
1. Before assigning an interface to DHCP, ensure that the upstream ISP is assigning an address. This is to reduce troubleshooting if configuration does not work on the firewall.



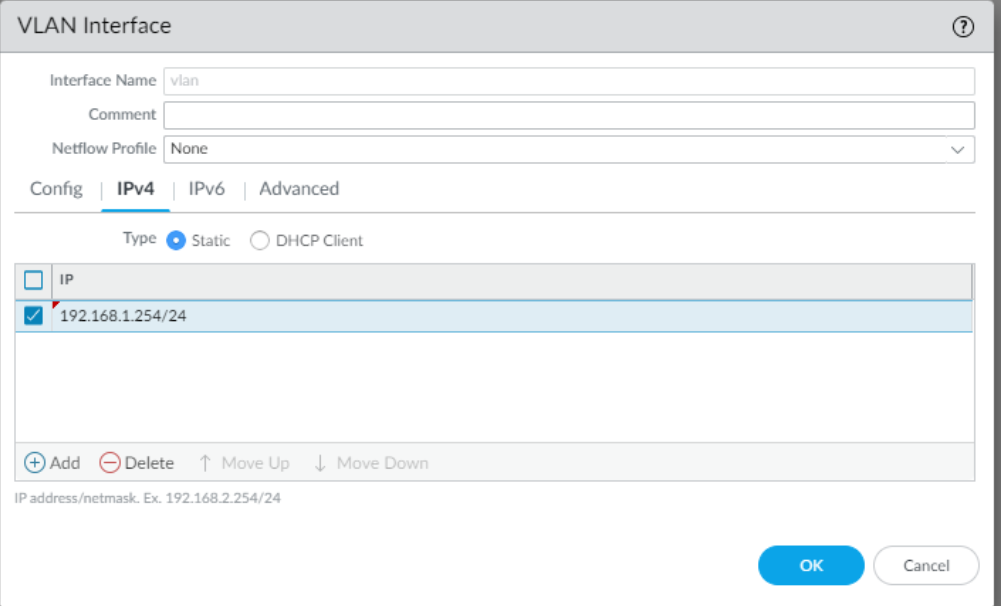
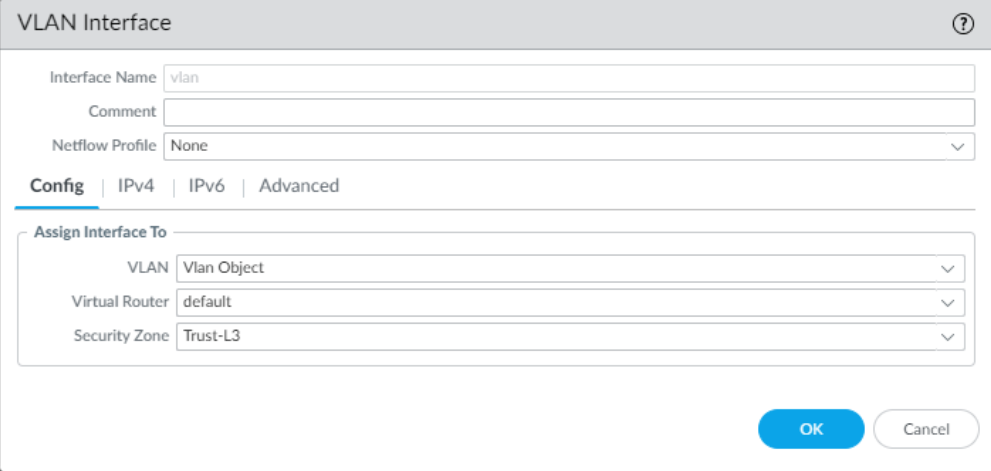
1. Create your VLAN object.



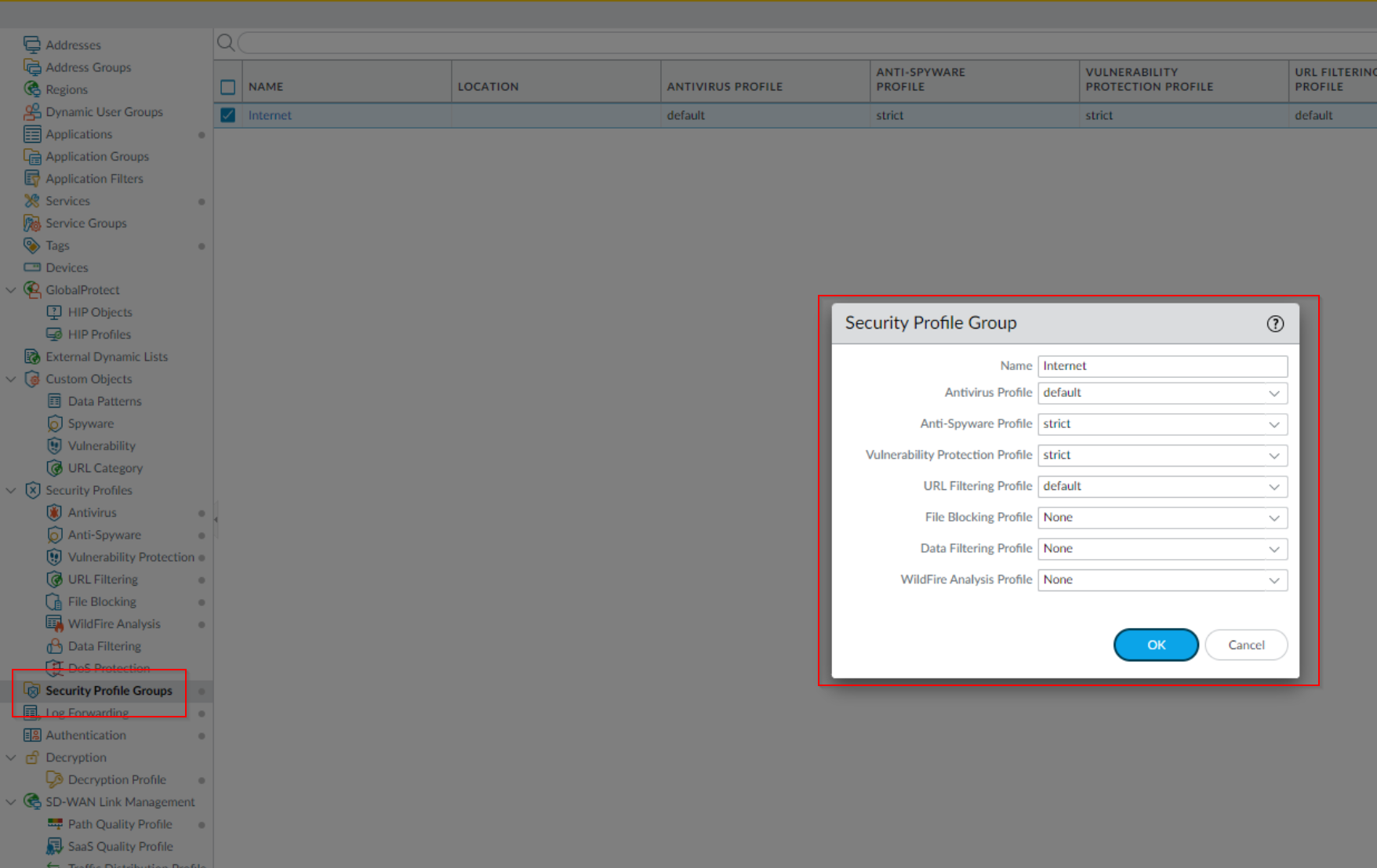
1. Configure your interfaces appropriately with the correct VLAN and Security Zone.



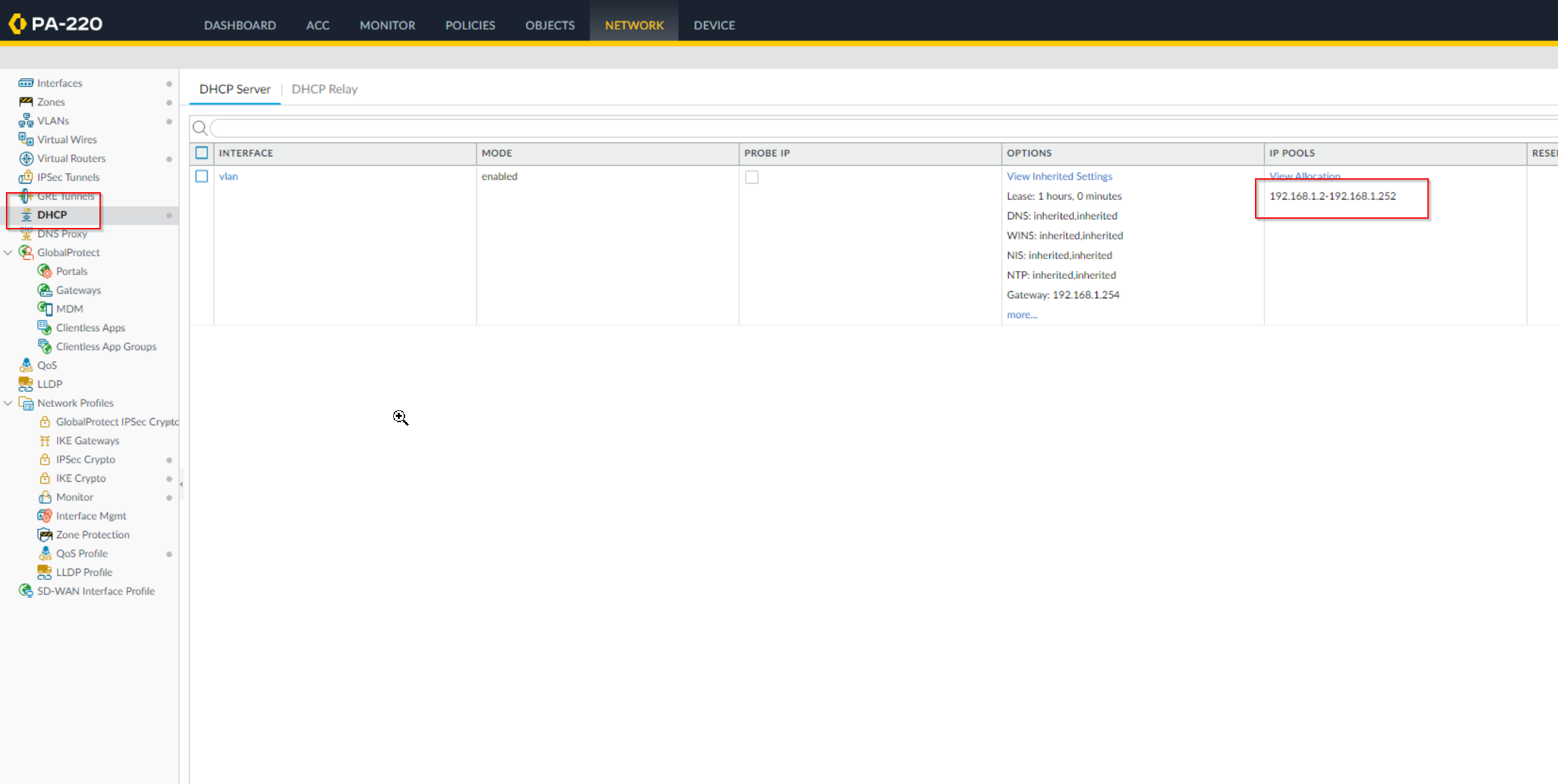
1. Configure the VLAN interface.

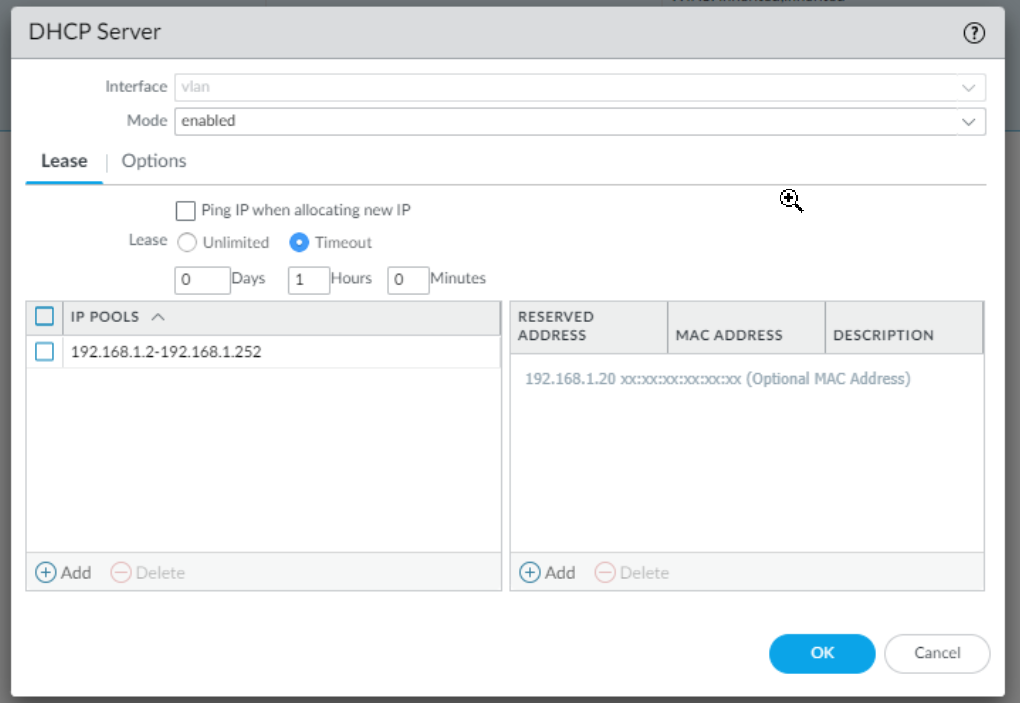


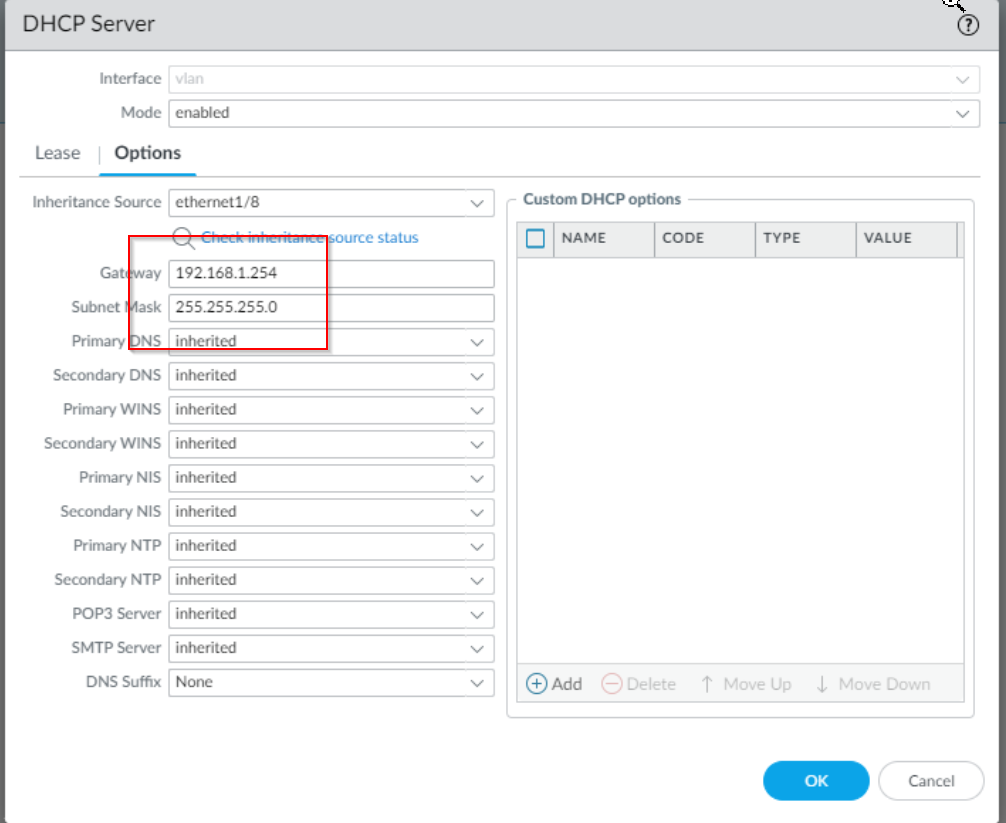
1. Assign your Security Profile group. Select the default.



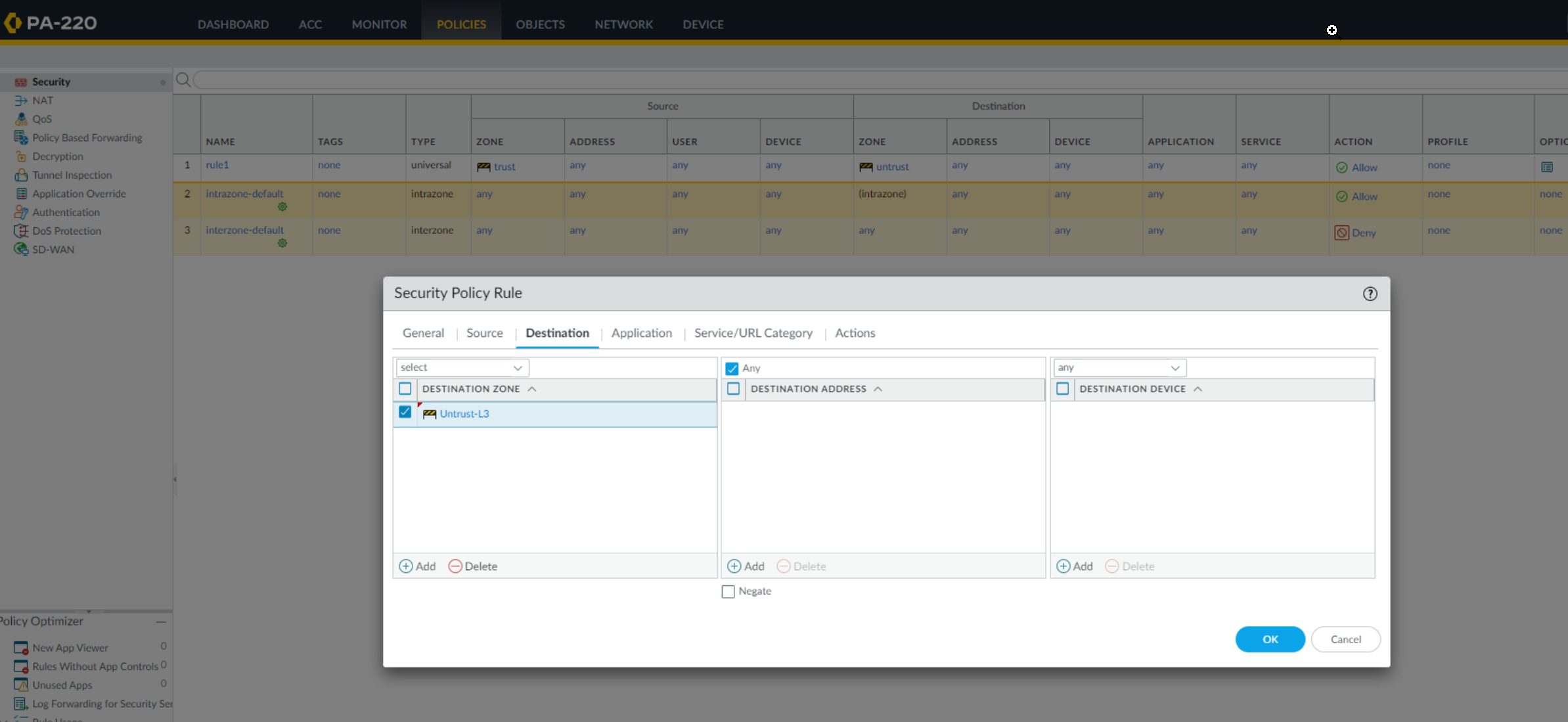
1. Now, configure your DHCP server with the following :

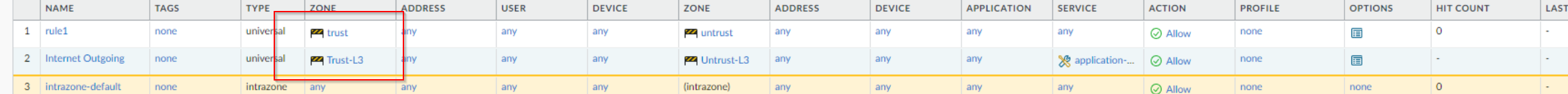




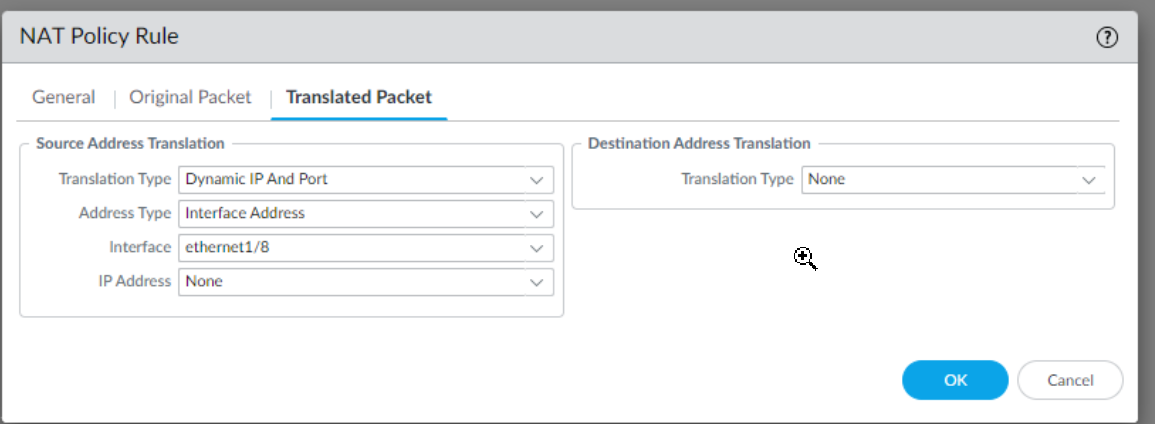
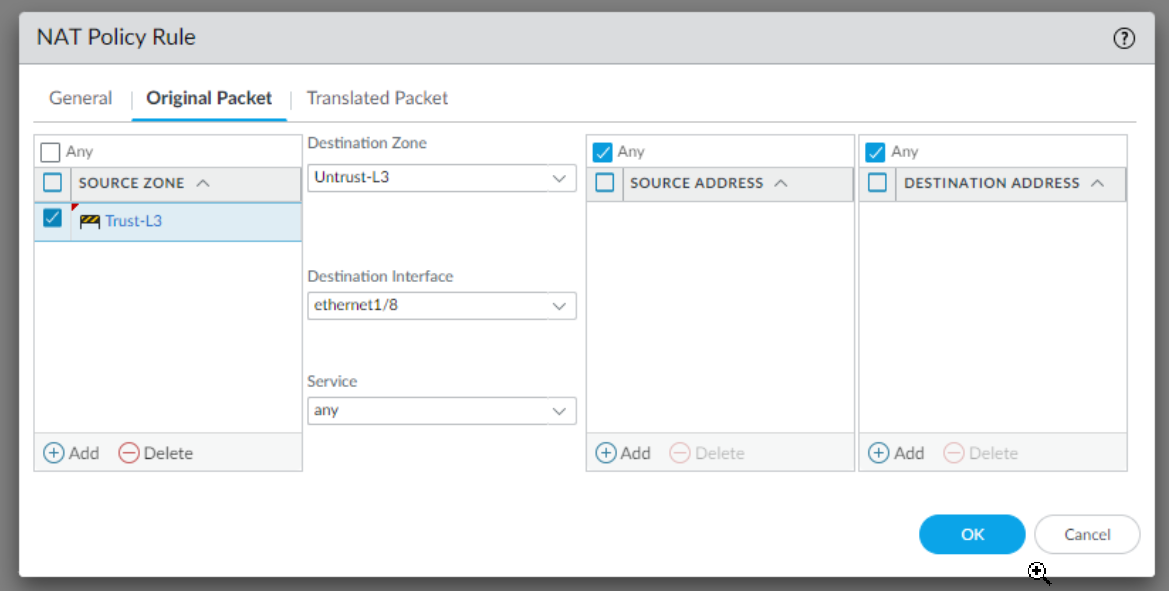
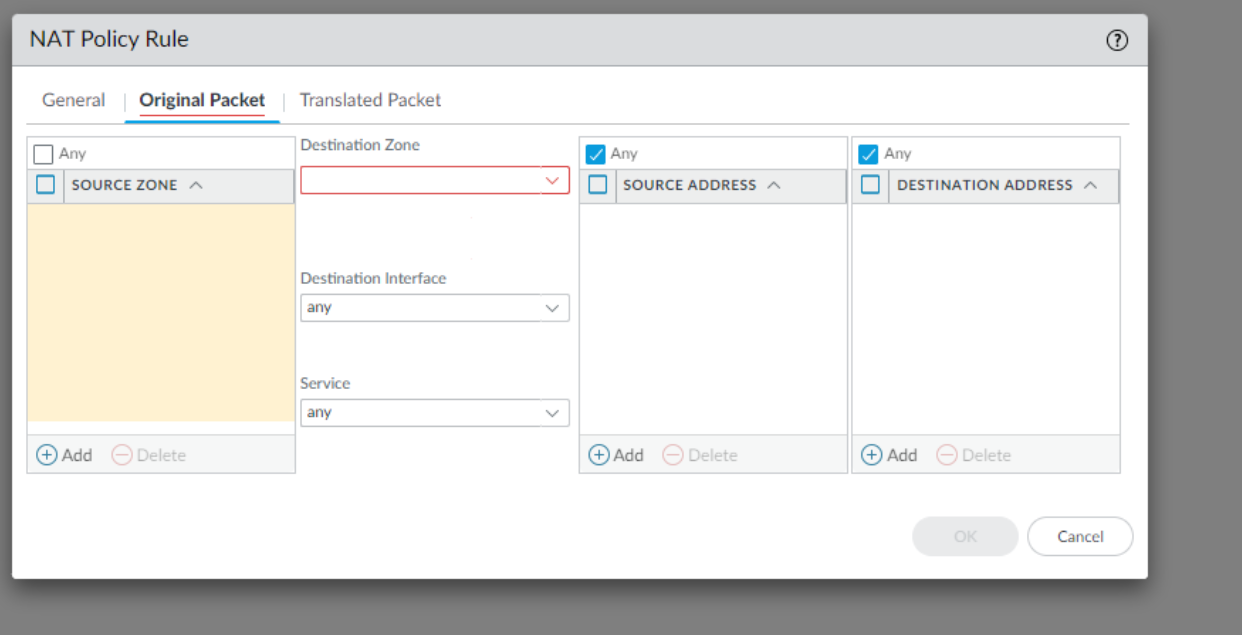
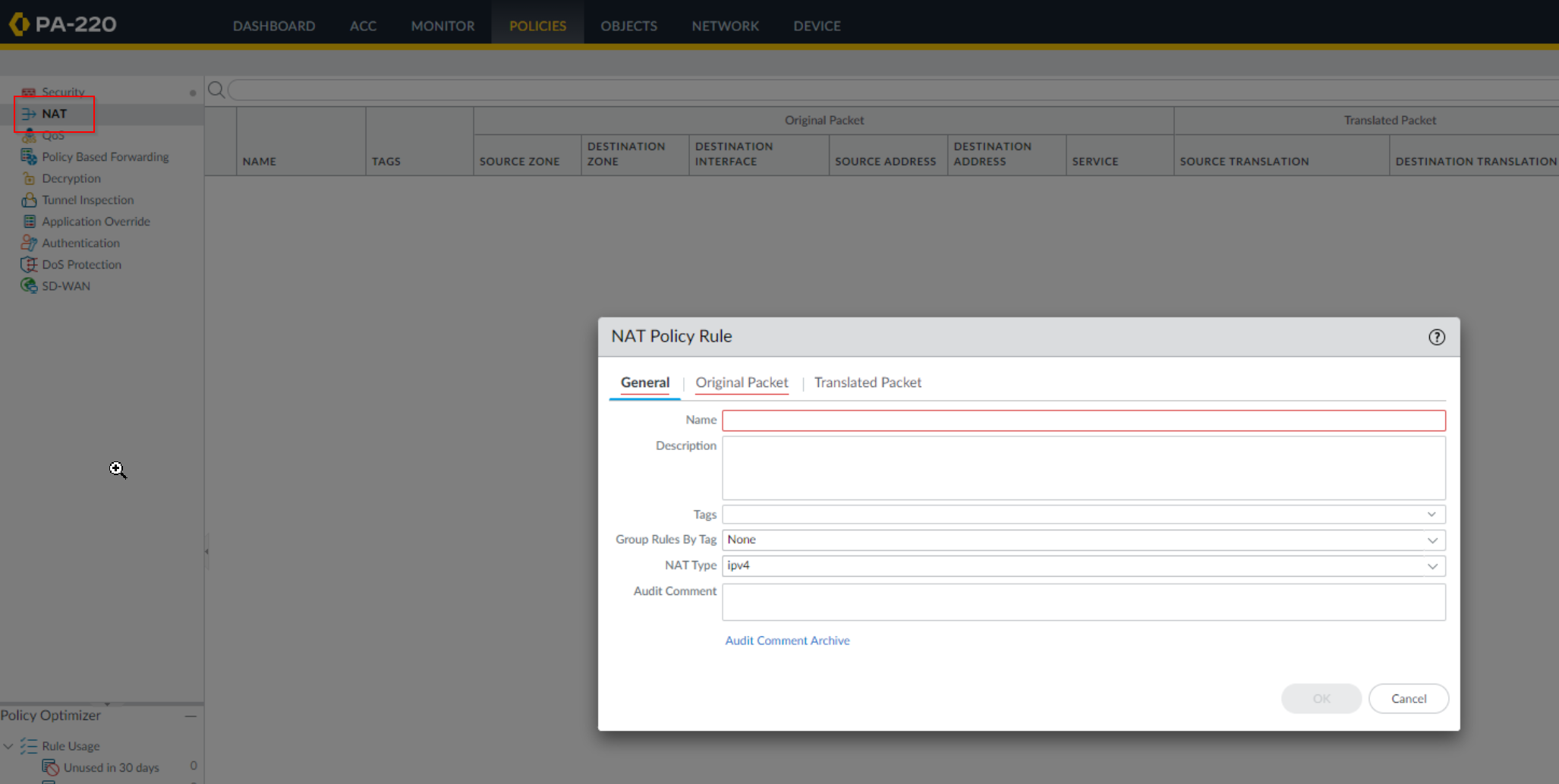


1. Create new Security Policies to allow Untrust regions to send to Trust regions.

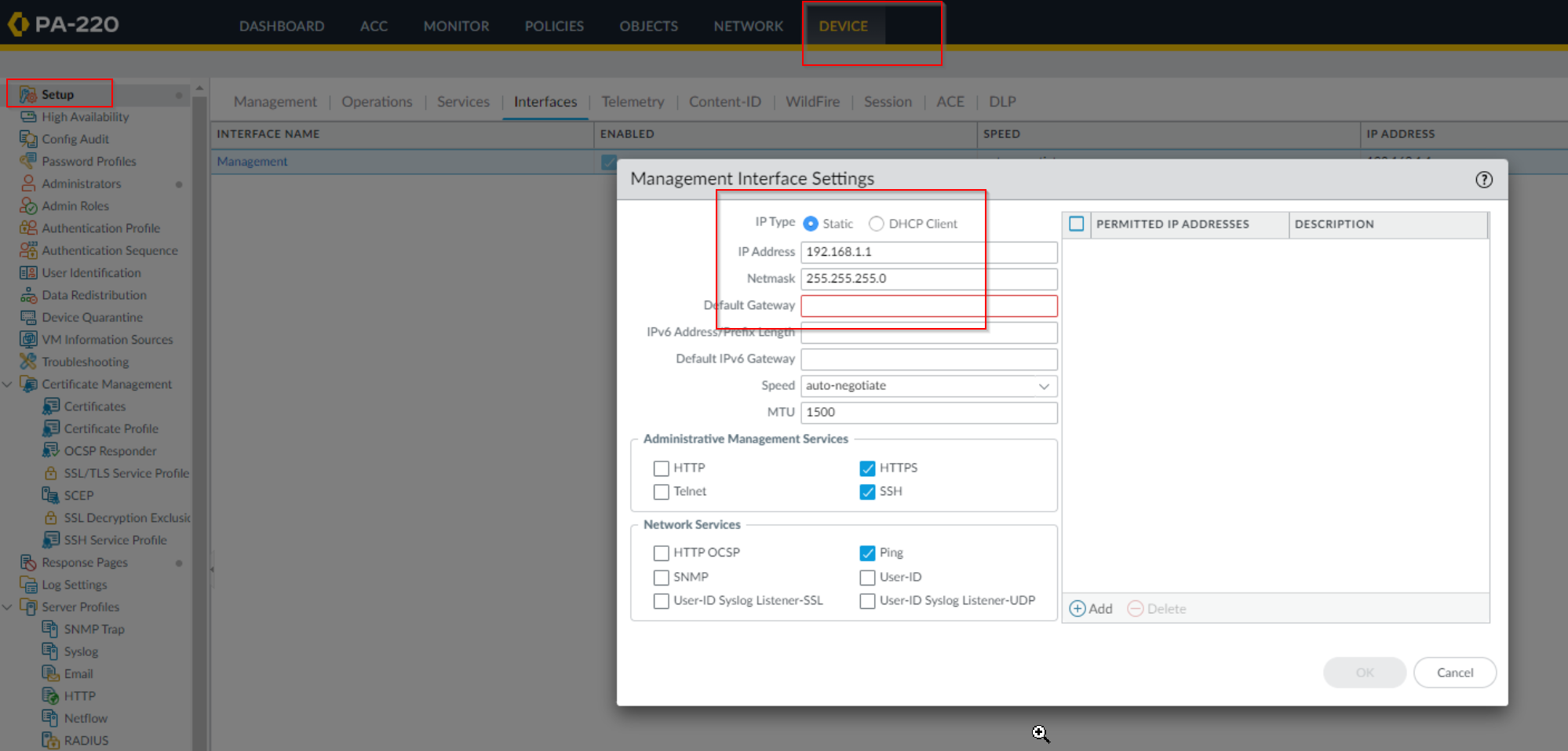




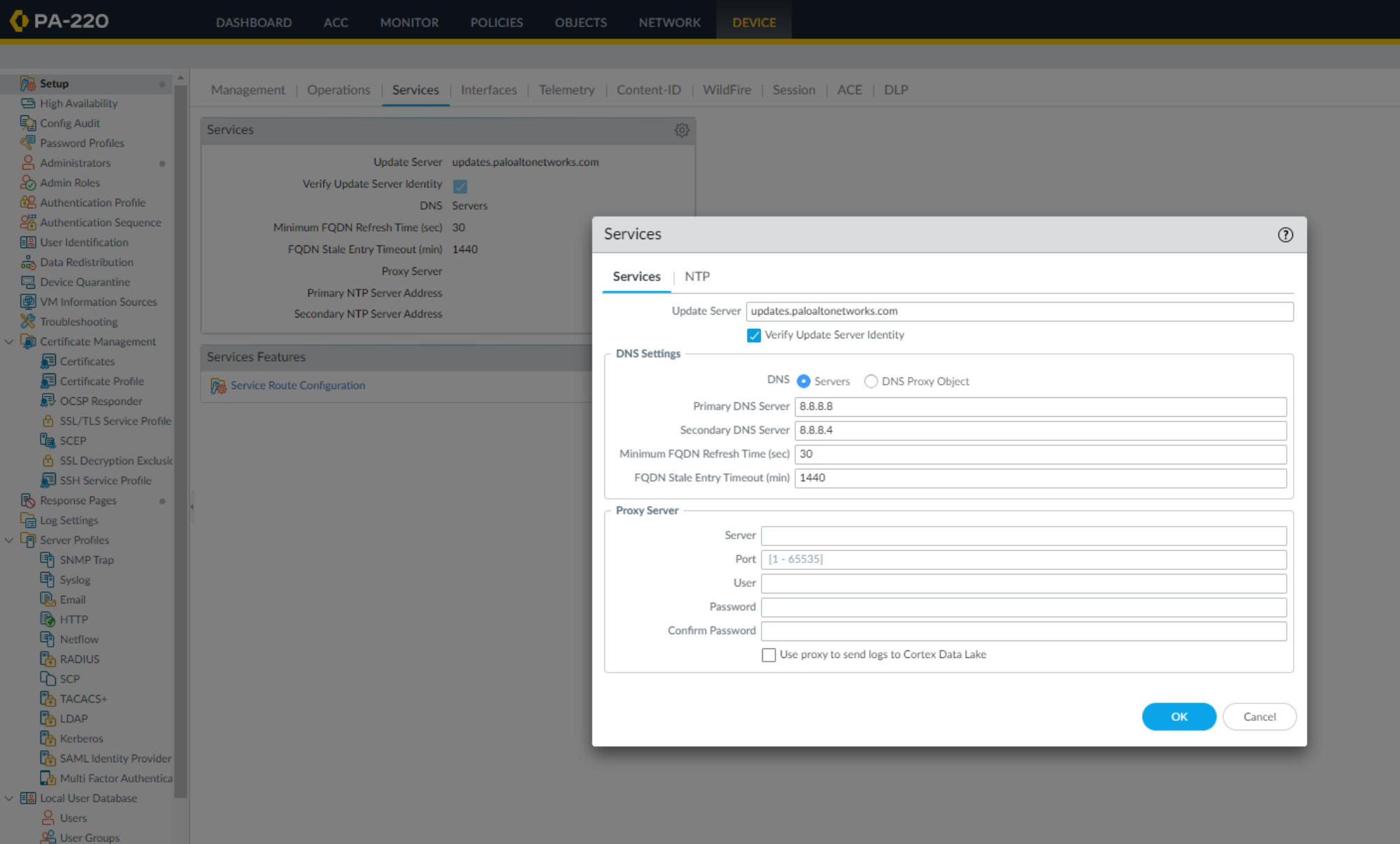
1. Create a NAT policy to enable DHCP clients to reach the internet.



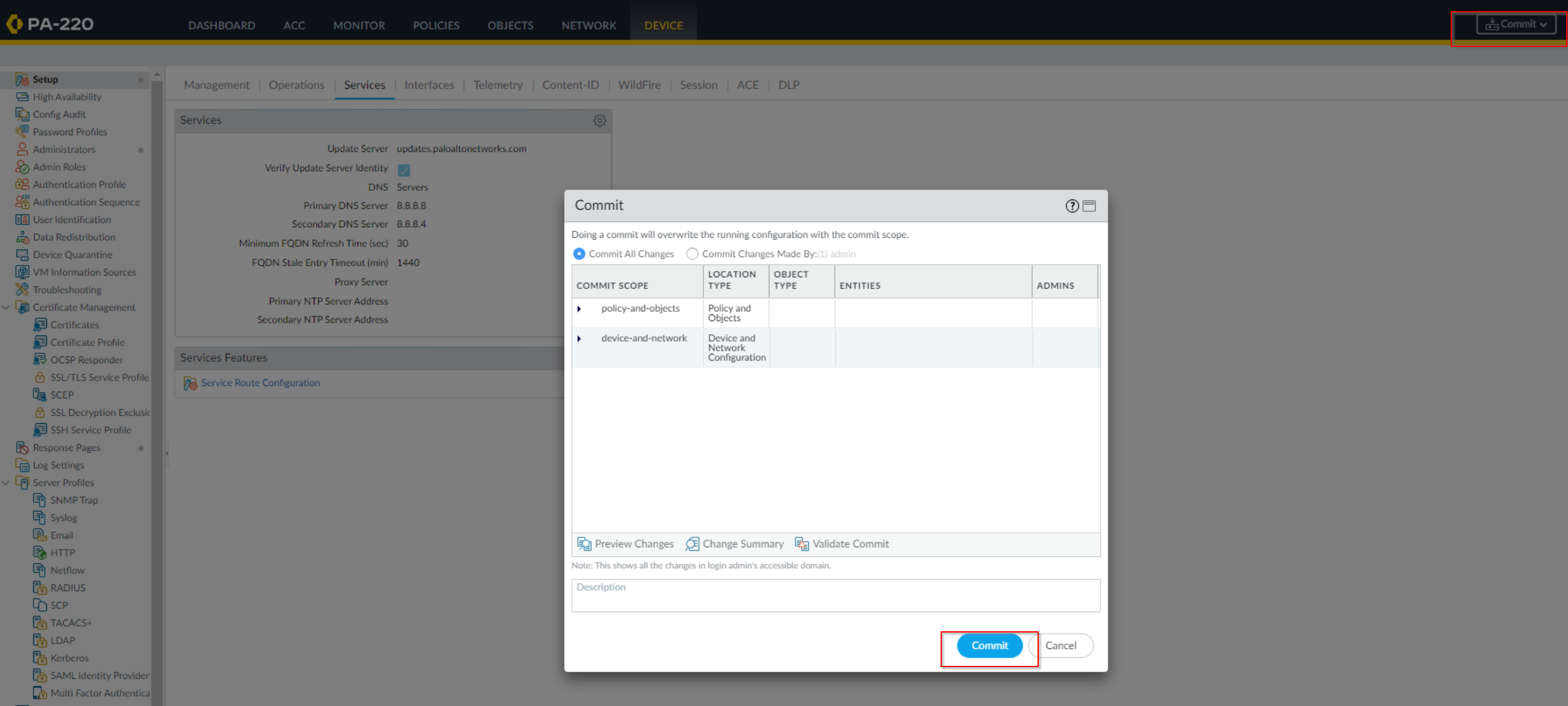
1. Finally, set the default management IP information so that the firewall can be accessed on the new network.

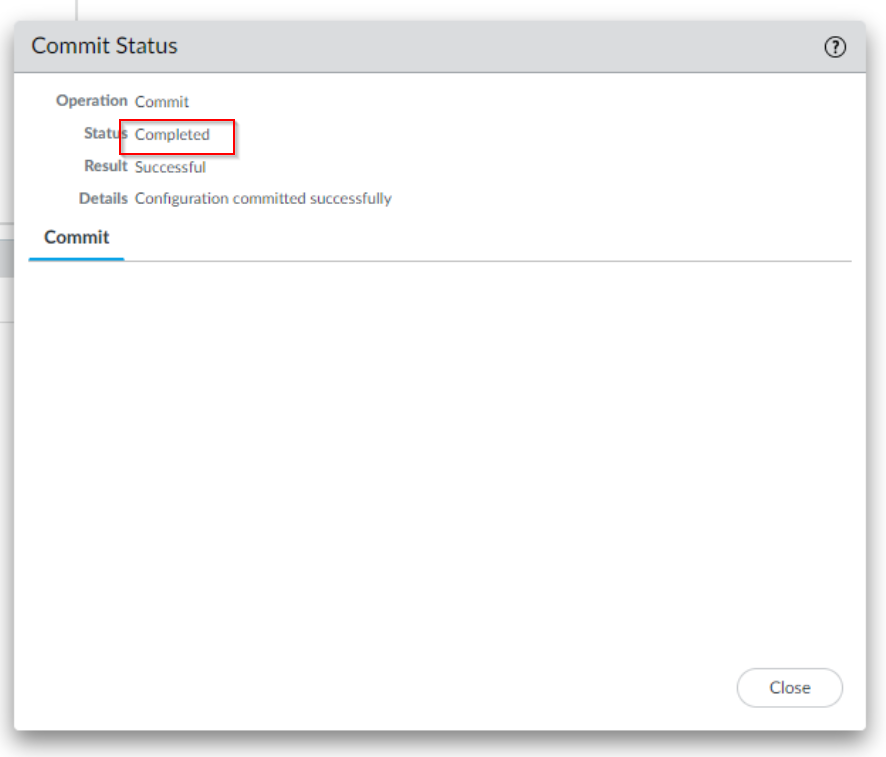


1. Set the DNS server.



1. Finally, commit the changes to ensure that it is saved to the firewall. After the firewall loads, all configurations should be applied.





**Problems:**

1. **“Invalid interface ethernet0/x”**

We faced an odd issue involving DHCP configuration on the individual interfaces. At first, when we followed steps to assign an interface to be a DHCP client, it would not display any lease information. When we tried to renew or release DHCP, a generic error message popped up, stating that the interface was “invalid”. After a lot of trial error and several firewall resets, we realized that this was due to the default virtual wire not being deleted. After deleting the virtual wire and committing changes, we were able to successfully obtain a DHCP lease from upstream.

1. **Firewall Loading Time**

Palo Alto firewalls take quite a while to load all utilities. At first, we did not realize this, and mistakenly thought that our firewall was bugged due to an inability to reach the web interface through the default IP. However, after waiting a few more minutes, all lights on the front of the firewall turned green. The web interface is then available through the default IP 192.168.1.1.

**Conclusion:**

Overall, this lab was a good introduction to what functions Palo Alto firewalls have, what specific issues might arise when configuring them, and how to resolve said issues. Through the configuration, we learned how a basic SOHO firewall configuration functions and how it is structured, as well as how to configure it.

URL Filtering Signoff Sheet

Ryan Chen, P3-4 Cisco Cybersecurity, Mr. Mason

