Sarkar, Mohul (Student)

PA-220 SOHO Configuration

Mohul Sarkar

**Purpose:**

The purpose of this lab is to create a firewall for a small office/home office (SOHO) using a PA-220 firewall.

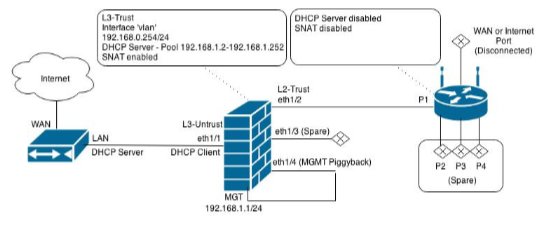
**Background Information on Lab Concepts:**

I gained background information on CLI configuration on the PA-220 router from factory resetting it and entering the Palo Alto web interface. I also have experience working with SOHO networks from previous labs. Previous configurations using different networking protocols ties in majorly to the concepts of PA-220 SOHO configuration.

**Lab Summary:**

This lab demonstrates the firewall properties of the PA-220 and how to implement that on a simple SOHO topology. Using knowledge from previous labs, coupled with the familiarization of Palo Alto interface, this lab combined two learned concepts. The SOHO network is utilized when the network is larger than a residential network but a lot smaller than an enterprise network. It is a package of all devices in a single router and has a user-friendly rather than a command-line interface.

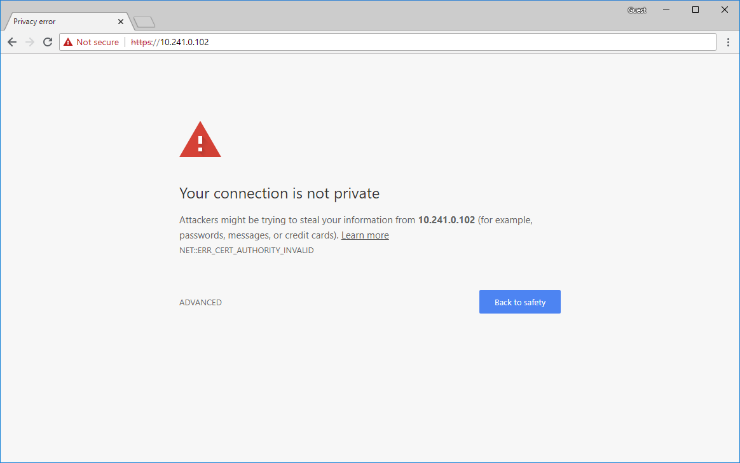
**Lab Reference Topology:**



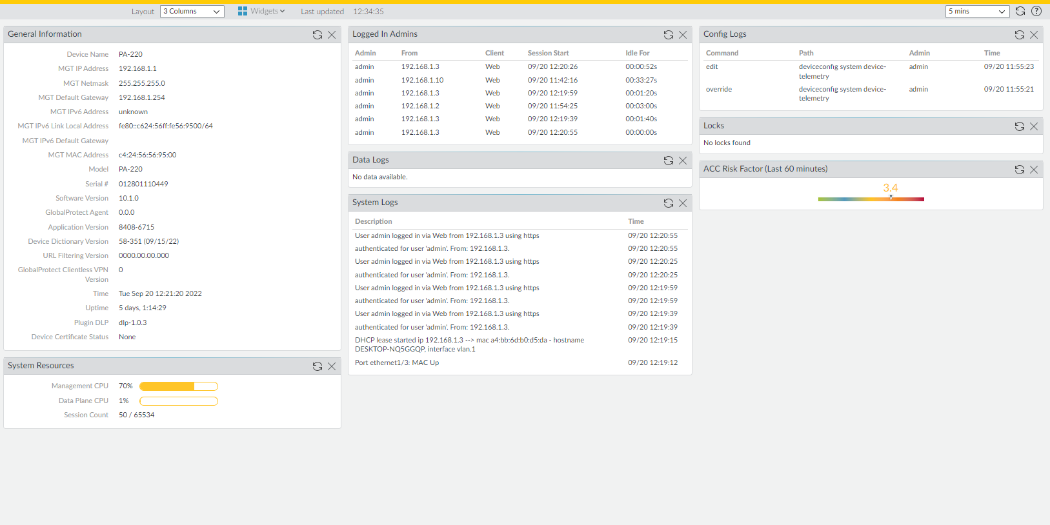
**Lab Configuration:**

1. Once you get the PA-220 login, enter the default credentials of admin/admin.
2. Set an ip address, netmask and gateway onto the interface to be able to access PA-220 through the web interface
3. Enter configuration mode by entering “configure” in the command line
4. Assign an IP address and other information. (Ex: set deviceconfig system ip-address 10.241.0.104 netmask 255.255.0.0 default-gateway 10.241.0.254 dns-setting servers primary 8.8.8.8 secondary 8.8.4.4).
5. Now test being able to access PA-220 through web browser by entering IP address as URL along with “https://” (Ex: https://10.241.0.104)

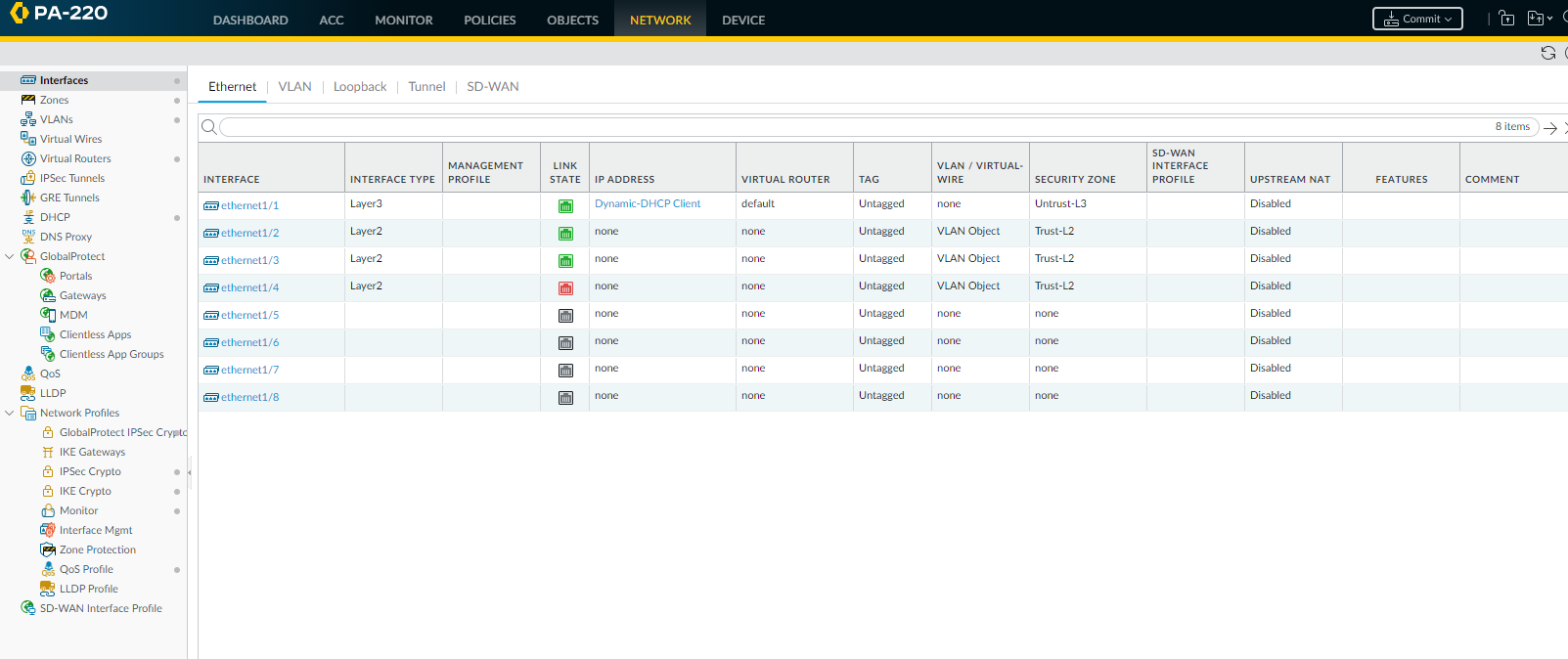
To access the web interface, you must accept the default self-signed certificate. This can be accessed by clicking advanced on the unsafe prompt screen and proceeding to website.



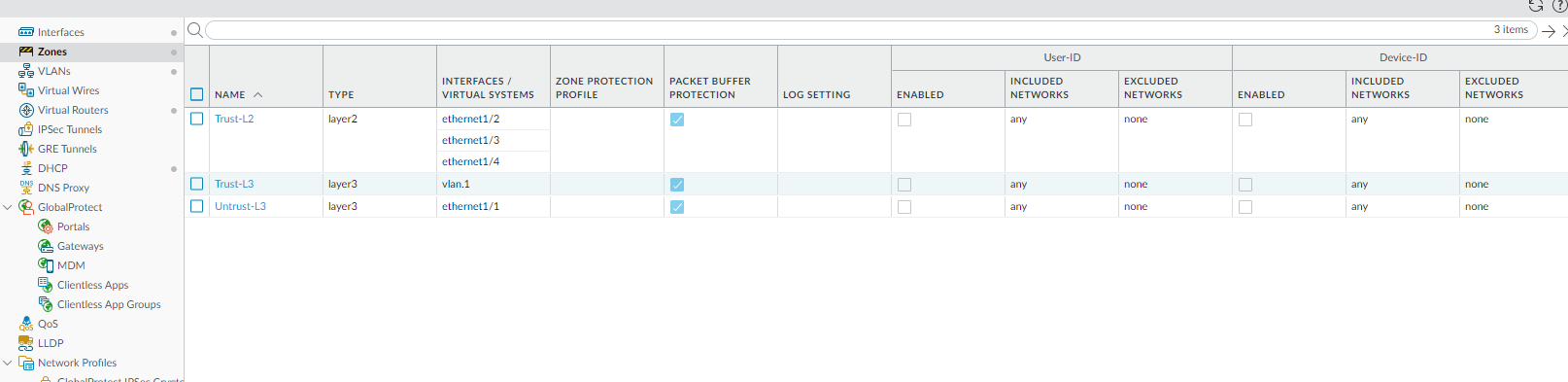
1. Once in, set the admin password to something unique and create yourself a personal ID.
2. To create your own admin account, enter Devices> Administrators> Add and then fill in the mandatory screens of Name, Password, Confirm Password and Administrator Type (set to super-user).
3. With this new super-user account, you can now pull down your licenses. You can do this by entering Device tab, Licenses, Retrieve license keys from license server. If this fails to work, make sure that you set up your DNS server during the configuration of the PA-220’s interface and the same IP address you chose for internet access.



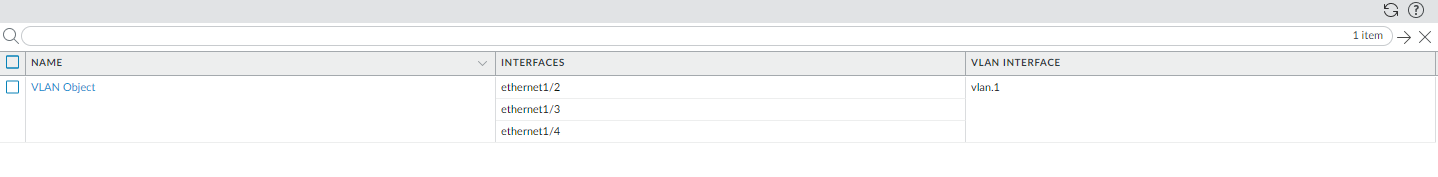
1. To begin internet configuration, enter the Network tab, then navigate to Zones. Create 3 new zones named:
   1. Untrust-L3, Layer 3
   2. Trust-L3, Layer 3
   3. Trust-L2, Layer
2. Navigate to Network tab, Interfaces and enter ethernet 1/1. Configure the ethernet to Layer3, set the Virtual Router to default and set the security zone to Untrust-L3. Add a static route pointing to the ISP’s next hop by entering Network> Virtual Routers> “default> Static Routers



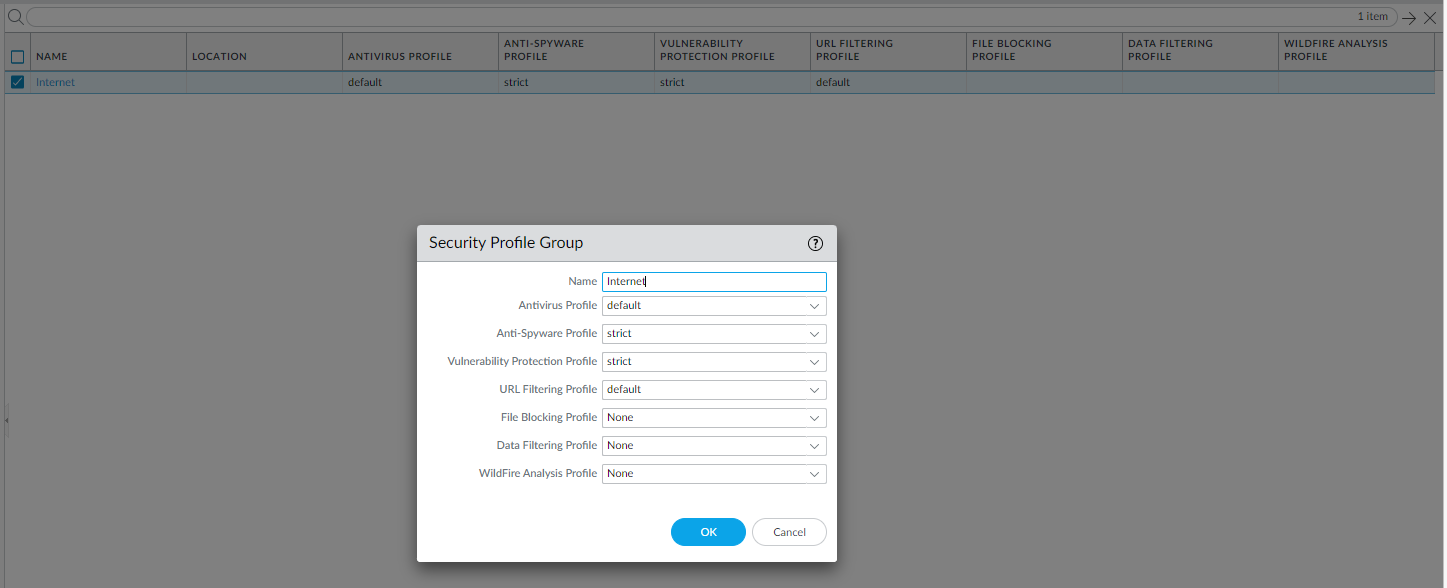
1. To connect to the wireless router, create a VLAN object in the VLAN tab. Set the interface to Layer 2, the NetFlow Profile to None, the VLAN to VLAN Object and the Security to Trust L-2.



1. Go into the VLAN tab once again and add a new VLAN Object with all default settings and Security Zone Trust



1. Add Security Profile Group with the spyware and vulnerability on strict



1. Next enter Dynamic Updates and click through and check for recent system updates
2. After this, you have finished configuration of your Palo Alto firewall.

**Problems:**

Some problems I had with this lab was getting the configurations to connect with one another. I realized later I had made a mistake when I was configuring the VLAN where I set the Trust zones incorrectly. After rebooting the router and correcting this mistake, my connectivity to the internet through the PA-220 was successful.

**Conclusion:**

I learned how to configure SOHO for a PA-220 firewall. I was able to debug VLAN issues and learned how the zones in Palo Alto work. I was able to navigate through the different tabs in the Palo Alto networking interface and properly configure each of the fill boxes. I was able to update the system and configure it to its latest edition.