A building with many windows

Description automatically generated

**Purpose:**

The purpose of this lab is to gain hands-on experience with configuring our PA220 firewall for a Small Office/Home Office (also known as SOHO) network environment. We were tasked to establish internet connectivity, security policies, and other network-related settings. This lab provides the foundational skills needed for future tasks in managing cybersecurity for small business environments, especially for Palo Alto specific firewalls.

**Background:**

SOHO networks are local area networks (LANs) involving a small number of people and are designed to support smaller environments such as home businesses or small offices whilst still providing security and reliability. In a SOHO environment, the firewall ensures unauthorized users or threats cannot gain access to sensitive information within the network while allowing internal users to communicate with the internet. To do this, the firewall establishes security zones, enforces security policies, and facilitates other measures to monitor inbound and outbound traffic. We have been assigned to configure these measures.

This is the first lab using Palo Alto’s Graphical User Interface which is where all SOHO configurations will be made. GUIs are the visual components of applications, allowing users to control their programs using interactive elements such as buttons, and icons instead of commands in command-line interfaces.

In this lab, there are also numerous important networking concepts, one of them being Domain Name System (DNS) which translates human-readable domain names such as amazon.com or google.com into IP addresses. This allows devices to communicate with external internet resources or other websites. Another key concept is security zones. Security zones are logical segments of a network that categorize, or separate devices based on their trust levels. Typically, a trustworthy network is kept separate from untrusted and external networks, and devices in the same security zones have similar trust levels. Security policies are pre-defined rules that determine what traffic is allowed to pass through security zones. Lastly, Network Address Translation (NAT) translates private IP addresses to public IP addresses, enabling devices on private networks to communicate with public network devices in our case, sources over the internet.

**Lab Summary:**

In this lab, we physically connected our PA220 firewall to the internet and logged into the Palo Alto GUI. Once connected, we configured the necessary network interfaces, created security zones, and set up other miscellaneous security policies. We also set up DNS, DHCP and NAT as essential parts to our network. By the end of the lab, we had successfully configured the firewall for a SOHO environment.

**Lab Procedure:**

1. Plug PA220 into the power supply using the provided power cord.
2. Connect a rollover cable from the PC to the firewall’s console port.
3. Connect an ethernet cable from the PC to the firewall’s management port.
4. Log into the Palo Alto GUI. The default username and password will both be “admin”. The first thing you will see is the dashboard which looks like the following.

A screenshot of a computer

Description automatically generated

1. At the top of the page, click Network and select Zones. Then select “Add” at the bottom left of the page to create a new security zone.

A screenshot of a computer

Description automatically generated

1. Create 3 security zones called Untrust-L3, Trust-L3, and Trust-L2. Change the zone names and type of zone accordingly. Select “OK” to save each security zone.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. After all security zones have been configured, the security zone page should look like the following.

A white paper with a yellow border

Description automatically generated with medium confidence

1. Stay in the Network tab but select Interfaces. This is what the page should look like. Select “Add Aggregate Group” at the bottom left of the page to create a new network interface.

A screenshot of a computer

Description automatically generated

1. Under the “Config” tab, configure port 1/1 as a layer 3 interface and assigning it to the Untrust-L3 security zone. Set the virtual router to the default setting as well.

A screenshot of a computer

Description automatically generated

1. In the same window, select the “IPv4” tab and select “DHCP Client” for the type. Click “OK” to save all settings for this network interface.

A screenshot of a computer

Description automatically generated

1. This is what the network interfaces page should look like. The settings just configured should show up for ethernet1/1.

A screenshot of a computer

Description automatically generated

1. Stay in the Network tab and select the VLANs tab. This is what the page should look like. Select “Add” at the bottom left corner of the page to create a new VLAN.

A screenshot of a computer

Description automatically generated

1. In the new window, set an appropriate name and select “vlan” for the VLAN interface field. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. Go back to the Interfaces tab. Add the rest of the ports to the VLAN we just created. For ports 1/2, 1/3, and 1/4, set their interface type to Layer2 and assign them to the VLAN object we just created.

A screenshot of a computer

Description automatically generated

A white and blue rectangular object with black lines

Description automatically generated with medium confidence

A blue and white rectangular object with white lines

Description automatically generated

1. Under Network, click the VLAN tab. This is what the page should look like. Select the pre-existing interface: vlan.

A screenshot of a computer

Description automatically generated

1. Under the Config tab, assign the interface to the created VLAN and set the security zone to Trust-L3.

A screenshot of a computer

Description automatically generated

1. Select the “IPv4” tab and enter a static IP address. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. Stay on the Network tab and select DHCP. This is what the DHCP page should look like. Select “Add” in the bottom right corner to create a new DHCP server.

A screenshot of a computer

Description automatically generated

1. In the new window, configure the DHCP server settings like the following. Assign the server to the created VLAN interface, set the lease as “Timeout” for an hour, and give it an appropriate IP address pool.

A screenshot of a computer

Description automatically generated

1. Click on the “Options” tab, and input the appropriate inbound port, gateway IP address, and subnet mask. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. At the top of the page, click on the Objects tab. Under Objects, select Security Profile Groups. This is what the main page should look like. Click “Add” at the bottom left of the page to create a new security profile group.

A screenshot of a computer

Description automatically generated

1. In the new window, set the security profile group settings to the following. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. At the top of the page, click on the “Security” tab. Click on the Security page. This is what the main page should look like. Click “Add” in the bottom left corner to create a new security policy.

A screenshot of a computer

Description automatically generated

1. In the new window under the General tab, give the security policy a name and description.

A screenshot of a computer

Description automatically generated

1. In the same window, select the Source tab. Click “Add” to select a security zone, and choose Trust-L3.

A screenshot of a computer

Description automatically generated

1. In the same window, select the Destination tab. Click “Add” to select a security zone, and choose Untrust-L3.

A screenshot of a computer

Description automatically generated

1. Then, select the Actions tab. Set the action setting as “Allow”, the profile type as “Group”, and the group profile as “internet”. Also configure it so it logs at the end of each session. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. The new security policy should show up on the Security Policies page. Our new policy is on line 2.

A screenshot of a computer

Description automatically generated

1. Staying in the Policies tab, open the NAT page. This is what the NAT page should look like. Click “Add” in the bottom left corner to create a new NAT policy.

A screenshot of a computer

Description automatically generated

1. Select the “Original Packet” tab. Click “Add” to add the Trust-L3 source zone. Set the destination zone as Untrust-L3 and the destination interface as port 1/1.

A screenshot of a computer

Description automatically generated

1. Select the “Translated Packet” tab. Set the translation type as “Dynamic IP And Port” and set the source interface to be port 1/1. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. This is what the NAT page should look like. The NAT policy we just created should show up.

A screenshot of a computer

Description automatically generated

1. At the top of the page, select the Device tab and go to the Setup page. Click on the “Interfaces” tab. This is what the page should look like. Click on the Management interface.

A screenshot of a computer

Description automatically generated

1. Give the firewall’s management interface an appropriate IP address, subnet mask, and default gateway like the following. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. On the Setup page, click on the “Services” tab. This is what the services page should look like. Select the “Service Route Configuration” link.

A screenshot of a computer

Description automatically generated

1. Enter the appropriate IP addresses for the primary and secondary DNS servers. For this lab, our primary DNS server is 8.8.8.8, and secondary DNS server is 8.8.4.4. Click “OK” to save all settings.

A screenshot of a computer

Description automatically generated

1. This is what the services page should look like. The IP addresses of the DNS servers should show up.

A screenshot of a computer

Description automatically generated

**Problems:**

This lab was relatively straightforward like the previous lab as we followed a set procedure, but we make an important error in our process. We plugged a cable connecting one of the ports we configured on our firewall and a port on our router. However, we chose the wrong port which caused an infinite loop and eventually led to the CCNP network being flooded with DHCP requests, thus crashing everyone’s workstations. With the help of Mr. Mason, we were able to identify the incorrect port and eventually fix our topology.

We also had a minor error when we tried to commit our configurations, but we got back the error message, “virtual wire default-vwire is missing one or more interfaces”. To solve this issue, we navigated to the Virtual Wires tab on the left sidebar and deleted the default wire from the listing and restarted our commit.

**Conclusion:**

In this lab, we learned how to set up a PA220 firewall for a SOHO network. We got to explore PAN-OS and set up security zones, security policies, and NAT. Overall, it was a successful lab and gave us a better understanding of how to set up small and secure networks.

**Sign Off:**

A close-up of a document

Description automatically generated