A close up of a sign

Description automatically generated

**Purpose**

The purpose of this lab is to learn the basics of a Palo Alto PA-220 firewall. Specifically, this lab outlines how to factory reset a PA-220 firewall, in the realistic case where the device is unable to boot. Understanding the basics of Palo Alto firewalls is a valuable cybersecurity industry skill which we focus on in this lab.

**Background Information**

Palo Alto Networks, founded in 2005, revolutionized the cybersecurity industry with its advanced technology in network security, and is now one of the leading cybersecurity companies of the world. Along with innovation, Palo Alto Networks works towards social impact, encouraging the improvement of Internet security, as it created the Cyber Threat Alliance in 2014 with well-known cybersecurity companies: Fortinet, McAfee, and NortonLifeLock. With this social impact and by developing the first next-generation firewall and early innovative approaches to advance traditional firewall capabilities, the company expanded rapidly, enhancing its products and launching new products beyond physical firewalls, such as cloud-based security services and the PAN-OS operating system.

The firewall we refer to in this lab is a **Palo Alto PA-220**, a compact, next-generation firewall catered towards medium-sized businesses or company offices. In a small, scalable form, the PA-220 firewall offers powerful security features and are ideal for companies that are looking for comprehensive network protection without overly complicated installation. These firewalls are great for severe environments as well, like power plants, oil and gas facilities, building management systems, or healthcare networks. These firewalls are comfortable to use, since they have no noisy fans, which reduces noise and power usage; eight Ethernet ports; and dual power adapters for added power redundancy. The installation and set-up processes for PA-220s are simple as well, as we discover in this lab.

This lab requires the usage of PAN-OS, the security operating system designed to control Palo Alto firewalls. PAN-OS was launched by Palo Alto Networks for enhanced security features, including intrusion prevention system (IPS), anti-virus, and anti-spyware. PAN-OS works towards providing features beyond those available to traditional firewalls, being able to handle next-generation firewalls with advanced threat prevention, user identification, and application control. The OS can also support applications without port or IP information, making application identification and control much more flexible. The centralized management system of PAN-OS makes it work-friendly, allowing users to manage, edit, and monitor multiple firewalls at once with a single interface through Palo Alto Networks’ Panorama, with either a web-based application or a command-line interface.

**Lab Summary**

1. Connect the PA-220 firewall to power using the power adapter. You can also connect two for additional redundancy.
2. Connect a console cable from the firewall’s “Console” port to a computer.
3. Use a terminal console, PuTTY, to connect to the firewall device.
4. Power on to reboot the device.
5. Enter maintenance mode in PuTTY and go into the PAN-OS.
6. Press ‘Enter’ until the *Factory Reset* option appears. Click on it.
7. If told to reboot, do so. You may need to wait several minutes.

**Lab Commands**

**maint**Entered in the PA-220 boot up menu. Enters the firewall into maintenance mode.   
This is the only command required to complete this lab.

**Lab Configurations**

Console into the PA-220 firewall, power on the device, and open PuTTY.  
Log in with default ‘admin’ credentials shown below.

A black background with a black square

Description automatically generated with medium confidence

You may need to change the password if the screen reads:

A black screen with white text

Description automatically generated

Once logged in, the screen should look like this during the boot sequence:

Enter maint command to boot to maintenance mode.

A screenshot of a computer

Description automatically generated

Once in maintenance mode, you should see this screen. Press ‘Enter’ to continue.

A screenshot of a computer

Description automatically generated

Arrow down to *Factory Reset* and click ‘Enter’ to display the following menu.

A screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generated

Arrow down to Factory Reset and press ‘Enter.’

A computer screen shot of a computer program

Description automatically generated

Now your Palo Alto PA-220 has been reset.

**Problems**

Due to the simplicity of this lab, problems faced were minimal. One of the issues that slowed our process down was being unable to enter the maint command in within the allotted time from the command-line interface. This step us three attempts to successfully complete.

**Conclusion**

This lab introduces the Palo Alto PA-220 firewall and demonstrates the factory reset process that can be performed in the case of password recovery or the device’s inability to boot. Understanding this lab is crucial for the usage of Palo Alto devices in upcoming labs.