

**Purpose:**

The purpose of this lab is to introduce and explore the PA220, a Palo Alto firewall device that we will be continually using throughout this course. To prime the device for use, we were tasked to factory reset the firewall to clear any remaining configurations or passwords so that we can apply our own necessary configurations.

**Background:**

A firewall is a portion of the network that is designed to act as a boundary between a trusted network and the outside world. Firewalls are often used to prevent unauthorized access into a network and to stop malicious threats from infiltrating while still allowing traffic from inside the network to communicate with the Internet. This is done through having a set of security rules that monitors traffic moving both in and out of the trusted network. Firewalls are a fundamental part of any network because it provides privacy and data located within the trusted network from being stolen or leaked, which is essential for online safety and reassures network users that they are protected while online.

The firewall that we are working with in this lab is the PA220, which is designed by Palo Alto Networks. Palo Alto Networks is a globally recognized cybersecurity company based in California that specializes with firewalls and cloud-based cybersecurity. They also have a Linux-based operating system called PAN-OS that runs on all their firewall products. This is important context for using the firewall since every company has different interfaces and protocols, so it is important to properly and thoroughly understand how to use based on the device and operating system.

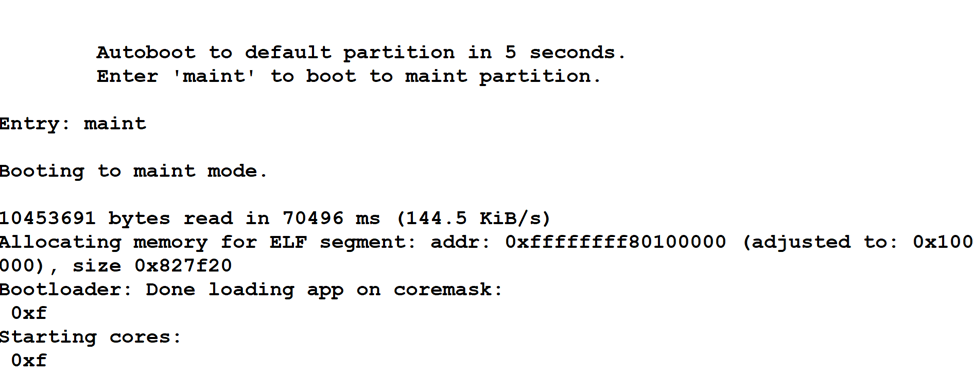
Another essential concept to understand for this lab is factory reset. A factory reset is process that wipes the configuration memory of the device and resets it to its factory settings, or the state that it is in as it leaves the factories. Factory resetting is useful as a last resort troubleshooting method, such as to clear existing password configurations. This is the exact scenario that we are given for this lab, so it is important to understand why we are performing a factory reset onto our firewall.

**Lab Summary:**

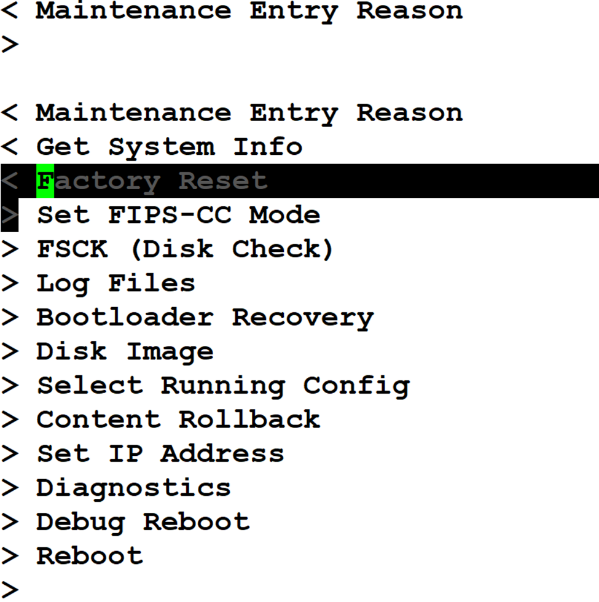
In this lab, we performed a factory reset onto our PA220 firewall. Prior to factory resetting, we had to first physically connect the firewall to the power supply and our PC, then wait for the firewall to initialize enough to enter maintenance mode. Once in maintenance mode, we can navigate the menu and complete the factory reset.

**Lab Procedure:**

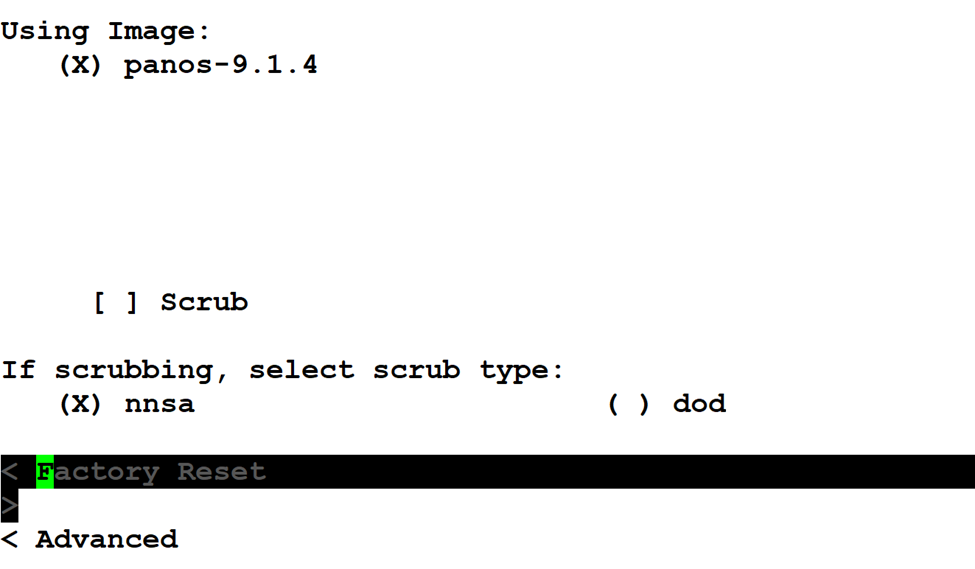
1. Plug PA220 into power supply using a power cord. The power supply ports were located on the middle column of the racks.
2. Connect a console cable from the PC to the firewall’s console port.
3. Power on the PC and allow for the PA220 to initialize its boot sequence.
4. Type “maint” when prompted to by the boot sequence screen to enter maintenance mode and disrupt normal startup.



1. Once you enter the firewall’s maintainence mode, use the up and down arrow keys to navigate the menu. Select Factory Reset.



1. Confirm the factory reset by pressing Enter on your keyboard.



1. The factory reset is now underway. Wait until the firewall indicates that the factory reset procedure has been completed, then reboot the desktop and firewall system.

**Problems:**

This lab was relatively straightforward, and no part of the process was particularly hard to perform. The primary problem that our lab group ran into was catching the short five second window to enter maint mode. The first time around, we failed to type “maint” in time and the firewall proceeded to initialize as normal. We figured out that power cycling the firewall would restart its boot sequence and give us another chance to enter maintenance mode without any repercussions besides spending 5-10 minutes waiting on the firewall.

**Conclusion:**

In this lab, we learned how to factory reset a PA220 firewall if we ever need to wipe all of our configurations. We also practiced navigating the PAN-OS and prepared our firewall for future use. While we ran into relatively few issues, our group still worked together to overcome challenges and adapt to using an unfamiliar device.