A group of men posing for a picture

Description automatically generatedA black text on a white background

Description automatically generatedA logo with red and blue text

Description automatically generated

Palo Alto PA-220 Factory Reset Procedure

Joshua Widjaja

P5 Advanced Cisco Cybersecurity

Mr. Mason

**Purpose:**

The purpose of this lab was to mainly learn how to factory reset the Palo Alto PA-220 Firewall without a password. Along with this main concept, came other key essential lessons such as knowing how to regain control of the firewall safely, understanding the boot process, and resetting the device without wiping the firewall of important information.

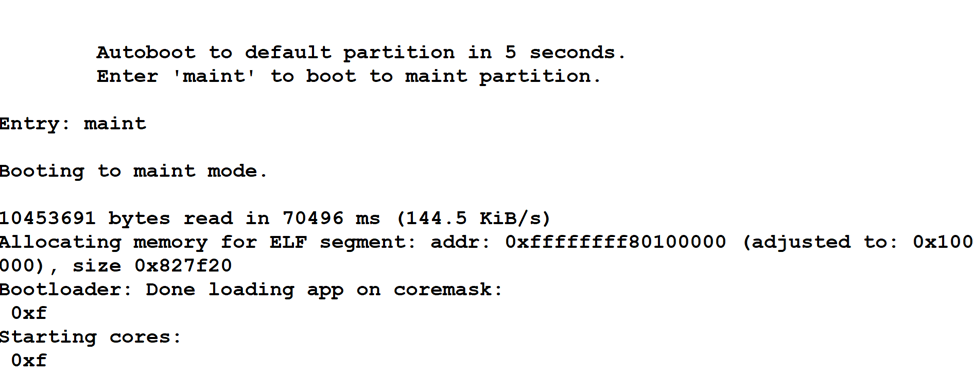
**Background Information:**

|  |  |
| --- | --- |
| **What is a Firewall?** | * A firewall monitors and controls the incoming and outgoing network traffic. * Essentially, it’s a wall protecting an internal network from an external network. * As a network engineer you can choose which traffic comes in and the level of authorization needed to gain certain access. * Through the use of network segmentation (dividing the network) on the firewall, you can control what parts of each network can reach one another. * Based on the security policies configured on the firewall, your network can choose whether to allow or block certain incoming traffic. * Firewalls are key to network security, as it can block suspicious traffic and can intercept threats before reaching internal systems. |
| **Factory Reset** | * Restores a device to its original state when it was first created in Palo Alto. * Removes settings, previous configurations, and data. * It is best practice to issue a factory reset before making your own configurations on the device. * Incredibly helpful for troubleshooting because a factory reset could eliminate software issues by removing corrupted data. |
| **Palo Alto** | * Palo alto networks was founded in 2005 by Nir Zuk, a former engineer from Check Point and NetScreen Technologies * Zuk created the business after realizing that network security would increasingly gain importance as networks became more complex. |
| **PA-220 Firewall** | * The firewall we used in this lab is a next generation firewall. * Designed for smaller networks but provides the same level of security features as the larger Palo Alto firewalls. * The physical descriptions include compact, no fan, 8 ethernet port openings. * Advanced threat prevention and easy to manage in smaller environments. |

|  |  |
| --- | --- |
| Types of Firewalls | Description |
| Hardware Firewall | * A physical device placed in between the network and the host (computer) * Found typically in server room |
| Software Firewall | * Acts as a service in virtual machines to secure network environments in the cloud. * Types of software firewalls include container firewalls, virtual firewalls, cloud firewalls, and managed service firewalls. |
| Next Generation firewall (NGFW) | * More advanced firewalls and better security solutions. * NGFW contains features to control application traffic and to locate threats in the cloud. * Closer examination of data to identify potential threats |
| Packet Filtering Firewall | * Operates at the network layer. * Controls the flow of data packets between different networks. * Packet is blocked if it doesn’t meet the established rules. |
| Proxy Firewalls | * Operates at the application letter. * Filters messages between external servers and the client. |

**Lab Summary/Configurations:**

1. Find a power source to plug into our PA-220 Firewall.
2. Connect the console cable from the console port of the computer to the firewall console port.
3. Wait for the firewall to turn on to reboot the device.
4. During the boot sequence you will receive a message stating “enter maint” to boot to maint partition.



1. Type maint and hit enter to enter maintenance mode.
2. You will receive a large display menu. Arrow down to **Factory Reset** and press enter.

A screen shot of a computer

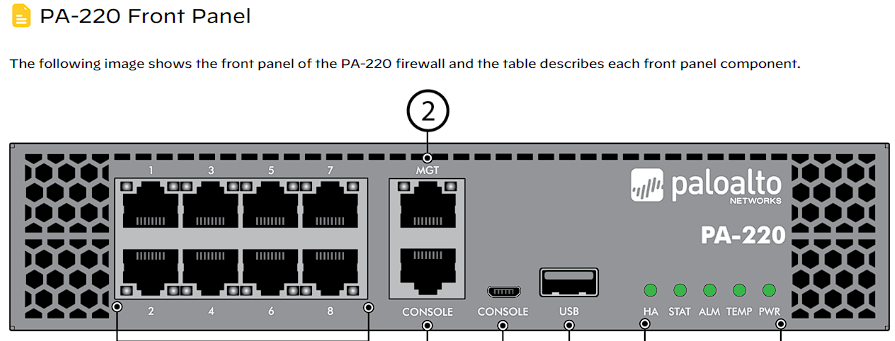
Description automatically generated

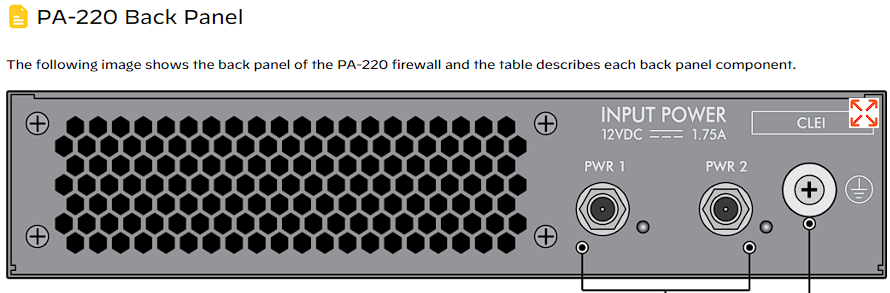
1. You will see the display menu that will confirm the factory reset. Select **Factory Reset** and press enter again.

A screenshot of a computer program

Description automatically generated

**PA-220 Firewall Diagram:**





**Problems:**

Although this lab was pretty straight forward after we got the hang of it, it did come with its fair share of problems. First of all, our cable management wasn’t so organized, and we didn’t have as much easy access to our firewall as we would’ve liked. We then re-organized the wiring and were able to place the firewall close enough for our console cable to run from the firewall to the console port of our computer. This was my first time booting up a PA-220 firewall, so I didn’t expect the boot sequence screen to read “autoboot to default partition in 5 seconds.” Therefore I missed my 5 second window to enter the maint partition. We ended up rebooting the Firewall from step 1 to get back to that 5 second window. Once that window came, I didn’t mess it up this time because I learned from my previous mistake.

**Conclusion:**

Other than a few small hiccups throughout this lab, we were able to successfully factory reset a PA-220 switch. I liked this lab as a great introduction heading into configuring firewalls because of the essential skills we picked up along the way.