# Palo Alto PA-220 Firewall Factory Reset

Andrew Pai

9/9/2024

## Purpose:

The purpose of this lab was to factory reset a Palo Alto PA-220 firewall. This allowed our team to recover access to the firewall and create our own login credentials as well as gain an understanding of the PA-220's boot sequence and maintenance mode.

## Background Information:

Palo Alto Networks is a networking company that focuses on providing cybersecurity and devices to clients. Founded in 2005, Palo Alto started out as a firewalls company before expanding to fields such as endpoint protection, malware prevention, machine learning, and data analysis. Some notable aspects of Palo Alto are that they co-founded the Cyber Threat Alliance, intended to raise the standard of cybersecurity by pooling information between companies. They also run the Unit 42 Research Team, which is a group of experts dedicated to discover world-wide cyberthreats such as Gorgon, Xbash, and Cannon.

Like mentioned above, Palo Alto specializes in creating firewalls for public use. Firewalls work to watch traffic going in and out of a device and block off any suspicious activity. Because firewalls separate your own network from other networks like the Internet by sitting on a network edge, firewalls can often be crucial in making sure your network maintains secure. Firewalls work by comparing packets being transmitted in and out of the network to a set of rules and deciding to let it pass based on the results. There are many types of firewalls like packet filtering firewalls, proxy firewalls, stateful inspection firewalls, AI-powered firewalls, and next-generation firewalls.

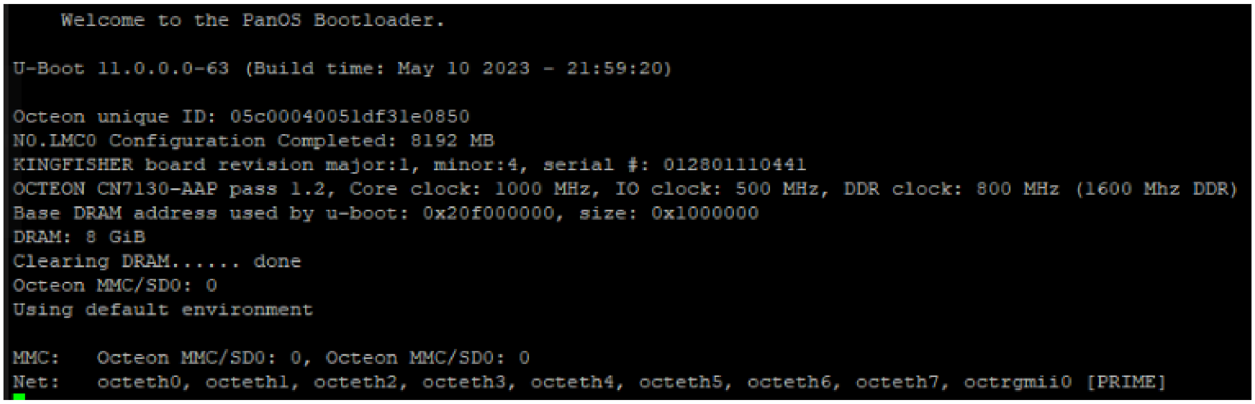
This lab will be focused on the PA-220 firewall that Palo Alto creates, which is a type of next-generation firewall. Next-generation firewalls can provide everything other firewalls like stateful inspection firewalls do, but also provides things like intrusion prevention and URL filtering.

Since firewalls provide such a large amount of security to your network, it is absolutely critical that you know and have the login credentials to your PA-220. In the case that the PA-220 has been passed down and has currently existing login credentials, it is necessary to perform a factory reset which wipes all data, settings, and configurations on the firewall, allowing you to create new login credentials and configure it for your purposes.

## Lab Summary:

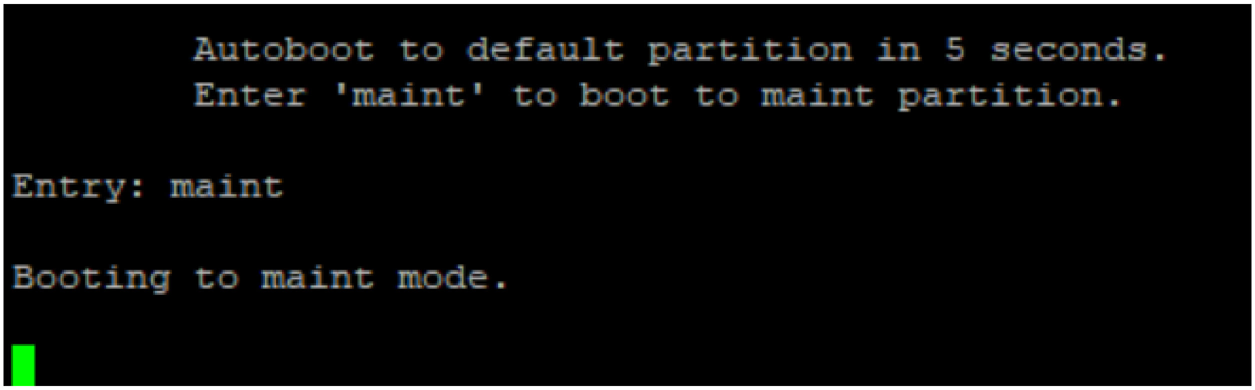
Connect your PA-220 device to a computer using a Console cable and power it on.

This should automatically put your device into bootloader, as shown below.



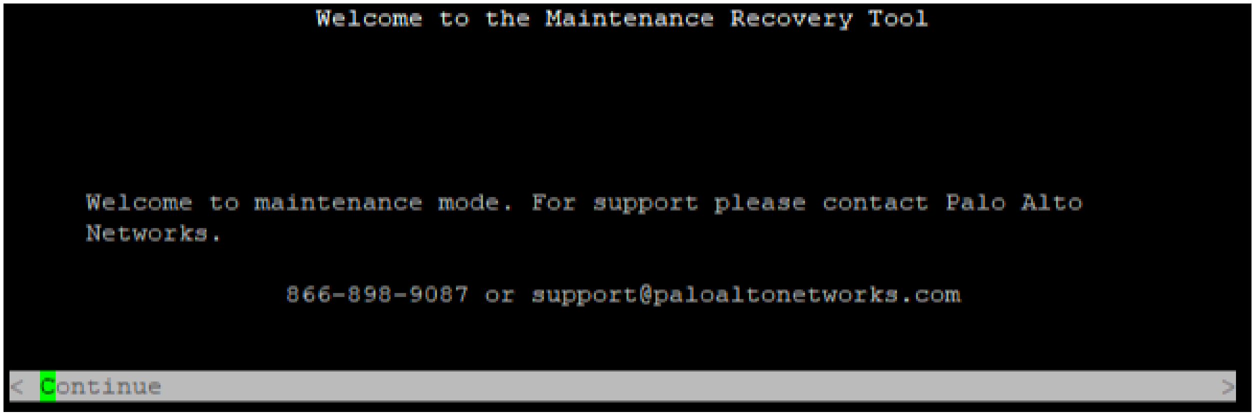
```
    Welcome to the PanOS Bootloader.

U-Boot 11.0.0.0-63 (Build time: May 10 2023 - 21:59:20)

Octeon unique ID: 05c00040051df31e0850
N0.LMC0 Configuration Completed: 8192 MB
KINGFISHER board revision major:1, minor:4, serial #: 012801110441
OCTEON CN7130-AAP pass 1.2, Core clock: 1000 MHz, IO clock: 500 MHz, DDR clock: 800 MHz (1600 Mhz DDR)
Base DRAM address used by u-boot: 0x20f000000, size: 0x1000000
DRAM: 8 GiB
Clearing DRAM...... done
Octeon MMC/SD0: 0
Using default environment

MMC:   Octeon MMC/SD0: 0, Octeon MMC/SD0: 0
Net:   octeth0, octeth1, octeth2, octeth3, octeth4, octeth5, octeth6, octeth7, octrgmii0 [PRIME]
```

Once prompted, enter maintenance mode by typing “maint” into the “Entry” prompt.



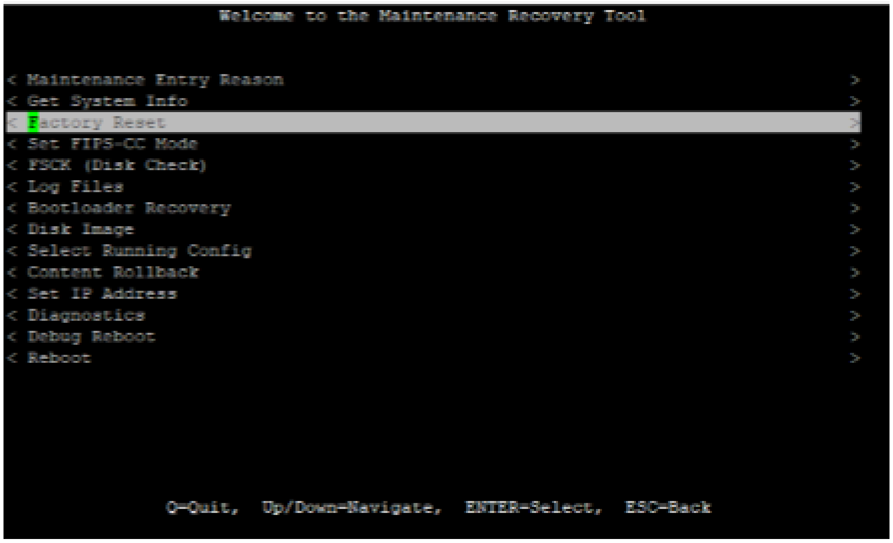
```
        Autoboot to default partition in 5 seconds.
        Enter 'maint' to boot to maint partition.

Entry: maint

Booting to maint mode.
```

Once you’re in maintenance mode, press enter to continue.



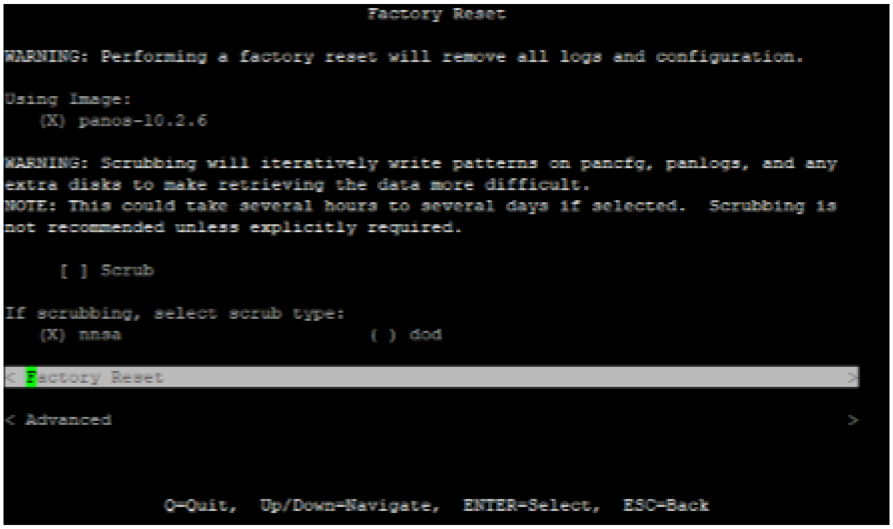
```
                     Welcome to the Maintenance Recovery Tool



    Welcome to maintenance mode. For support please contact Palo Alto
    Networks.

             866-898-9087 or support@paloaltonetworks.com

< Continue                                                              >
```

Inside the maintenance recovery tool, arrow down to “Factory Reset” and press enter.



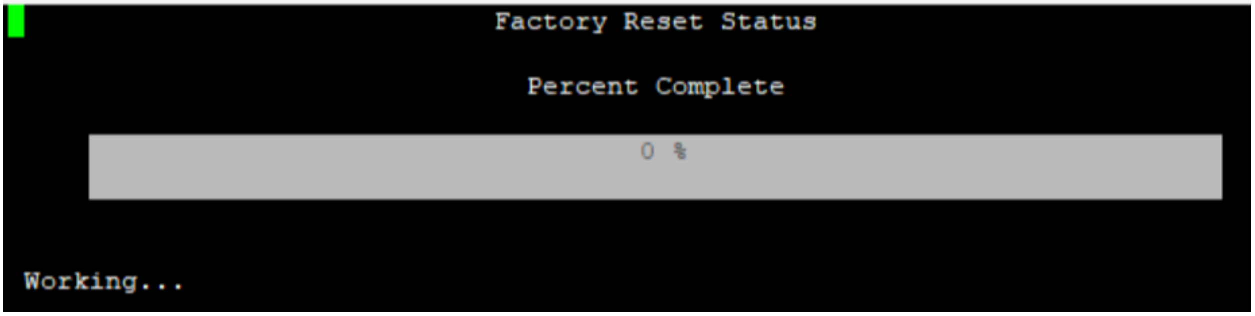
```
                    Welcome to the Maintenance Recovery Tool


< Maintenance Entry Reason                                                >
< Get System Info                                                         >
< Factory Reset                                                           >
< Set FIPS-CC Mode                                                        >
< FSCK (Disk Check)                                                       >
< Log Files                                                               >
< Bootloader Recovery                                                     >
< Disk Image                                                              >
< Select Running Config                                                   >
< Content Rollback                                                        >
< Set IP Address                                                          >
< Diagnostics                                                             >
< Debug Reboot                                                            >
< Reboot                                                                  >








              Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

Confirm that you would like to factory reset your PA-220 by arrowing down to “Factory Reset” in the menu and pressing enter.



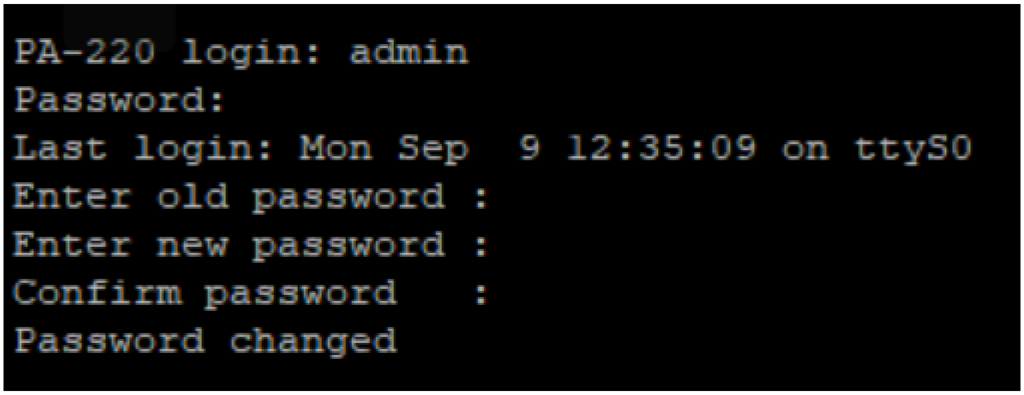
```
                                 Factory Reset

WARNING: Performing a factory reset will remove all logs and configuration.

Using Image:
   (X) panos-10.2.6

WARNING: Scrubbing will iteratively write patterns on pancfg, panlogs, and any
extra disks to make retrieving the data more difficult.
NOTE: This could take several hours to several days if selected.  Scrubbing is
not recommended unless explicitly required.

     [ ] Scrub

If scrubbing, select scrub type:
   (X) nnsa                        ( ) dod

< Factory Reset                                                           >

< Advanced                                                                >



              Q=Quit,  Up/Down=Navigate,  ENTER=Select,  ESC=Back
```

Once factory resetting, your PA-220 will take anywhere from 10-30 minutes to reset.



```
                    Factory Reset Status

                      Percent Complete

                            0 %

Working...
```

Finally, you will be able to reset your PA-220 by using the default login and password of admin/admin for the firewall and setting your own password.



```
PA-220 login: admin
Password:
Last login: Mon Sep  9 12:35:09 on ttyS0
Enter old password :
Enter new password :
Confirm password   :
Password changed
```

## Lab Commands:

The only command used in this lab was the “maint” command, which we entered once the firewall bootloader finished. By entering “maint,” our group was able to the PA-220’s maintenance mode, which allowed us to access various settings of the firewall. In this lab, getting into maintenance mode was used purely to factory reset our machine by selecting the factory reset option.

## Problems:

One of the problems that we had with this lab was mainly the unexpected amount of time that the firewall took to boot up. While we were expecting something around 3-5 minutes for the firewall to boot up, the actual loading time was somewhere around the 20 to 30 minute range. Because the loading time was so much longer than what our group expected, we disconnected and reconnected the firewall to various computers testing if the “problem” was because of a specific cable of computer. This reset our progress every time and caused us to lose time. In the end, what helped us was realizing the 3 lights on the PA-220 would have to all be up for the firewall to have finished loading. This allowed us to gain the patience to wait out the loading period for the firewall and proceed with the factory reset.

## Conclusion:

In conclusion, this lab was meant to factory reset a PA-220 firewall from Palo Alto to let our group set our own login credentials instead of using the credentials set by a previous group. To do this, we simply used maintenance mode and Palo Alto's written tutorial to reset our firewall. The biggest challenges that we faced was the fact that we didn't know how long the firewall should load for, and therefore our preconceptions of load time caused us to reset on progress multiple times. Going forth, our group should simply have more patience or truly confirm if there is a problem before trying to fix anything.