

Factory Resetting a Palo Alto

Evan Choi | Cisco Cybersecurity | 9/8/2022

**Purpose**

The purpose of this lab is to understand how to console into a Palo Alto firewall, factory reset it, and set your own username and password.

**Background Information on lab concepts**

A firewall is a network security device that monitors all incoming and outgoing traffic in a network. It blocks unauthorized traffic and only allows traffic it deems safe. They ensure that there is a safe connection when connecting to the internet. Palo Alto Networks is a cybersecurity company which produces advanced firewalls. Their advanced firewalls provide real-time content scanning and reporting capability that is not provided by any other firewall.

Palo Alto firewalls are accessed using a username and password. If an unknown password is set on the device, it’s important to know how to get the default configurations without the use of a password. To do this you need to know how to factory reset the firewall, which will delete all configurations and return them to the default settings, including the security credentials.

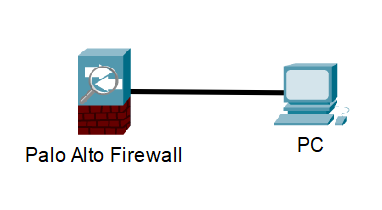
**Lab Summary**

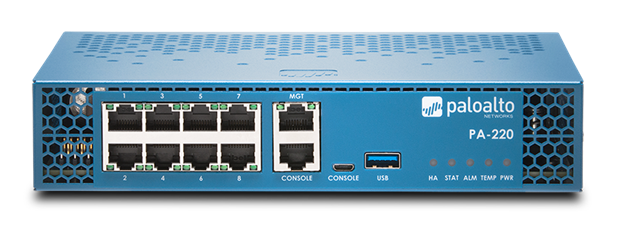
In this lab, I used a Palo Alto PA220 firewall and a console cable to factory reset a Palo Alto PA220 firewall. After consoling into the firewall, I entered maintenance mode and went through steps to factory reset the firewall. Finally, I set configured my own passwords and retired logging in to ensure that it was working properly.

**Lab Commands**

Entry: **maint** – this command will enter maintenance mode in the firewall

**Network Diagram with IP's**

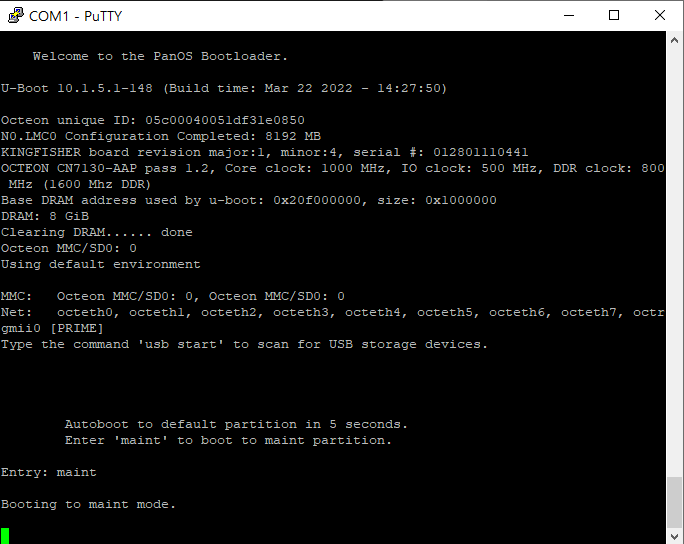




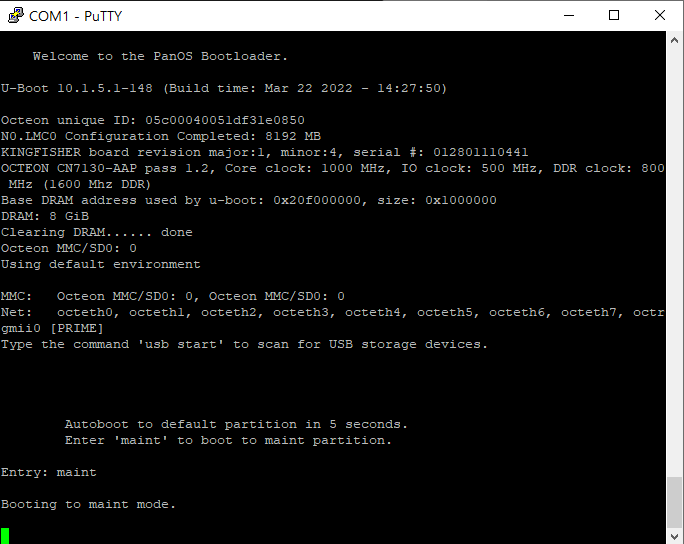


**Procedure**

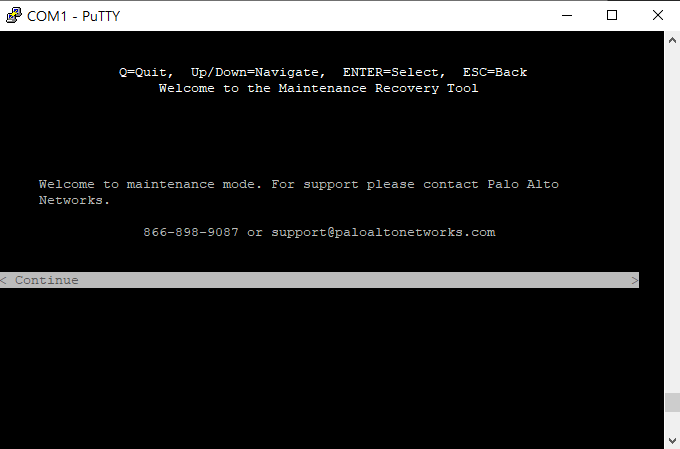
1. Connect a **Console cable** to the **Console** port on the palo alto
2. Power the device on
3. Open PuTTY and the boot sequence screen should appear



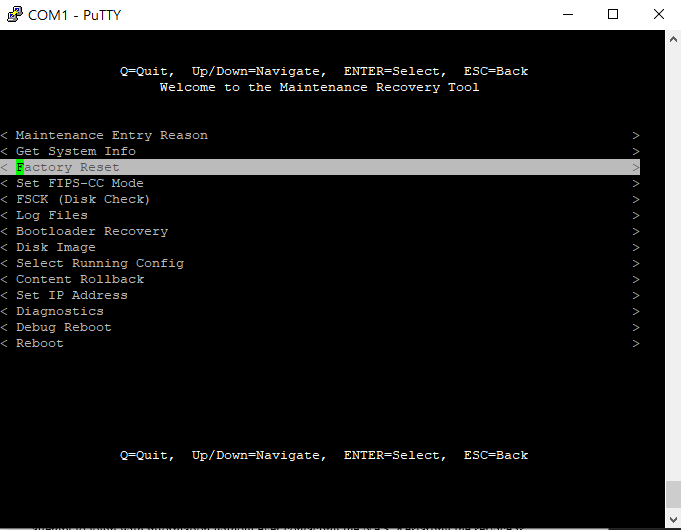
1. To enter maintenance mode type **maint**. You will have 5 seconds to type **maint** after “Entry:” appears. If you don’t type it within that time, you will have to go through the boot sequence again.



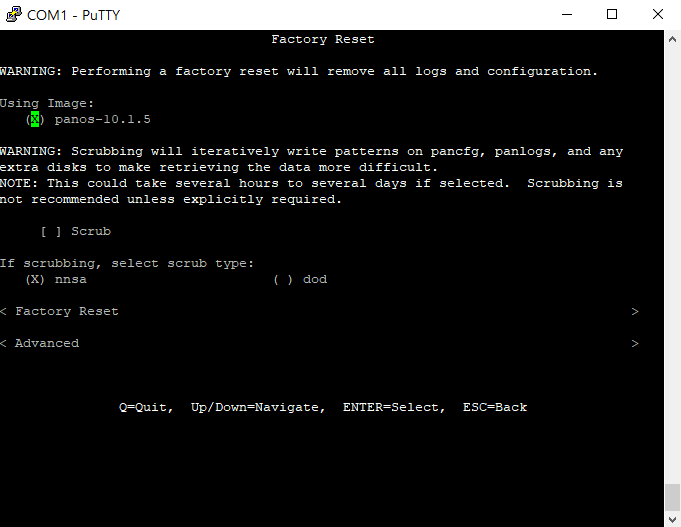
1. The following screen will be displayed once in maintenance mode. Press **enter**



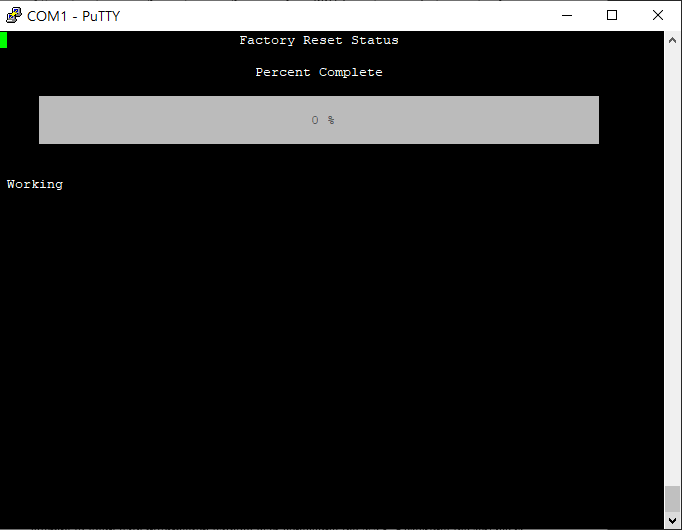
1. Press the **down arrow key** until you get to **Factory Reset.** Press **enter.**



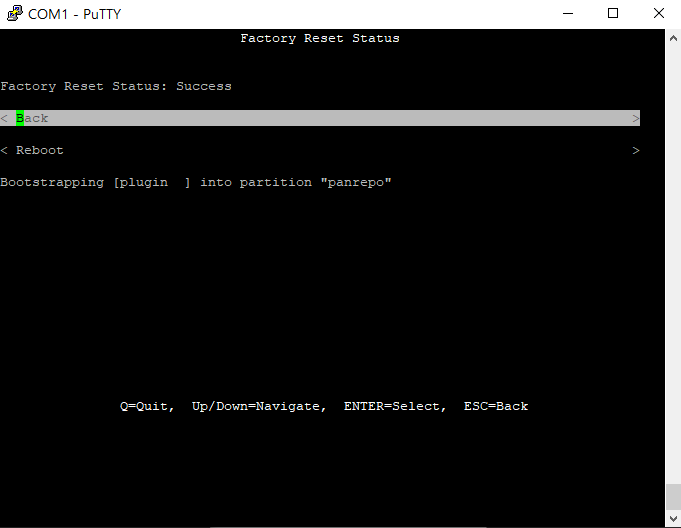
1. The image that you will be using to perform the factory reset should be shown (panos-\_.\_.\_). Press the **down arrow key** until you get to **Factory Reset.** Press **enter.**



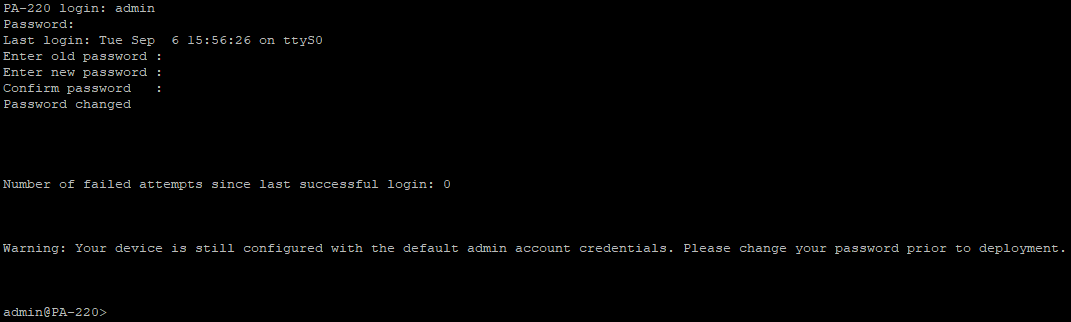
1. The reset status bar will appear, like the one shown below.



1. After the reset is successful, the following screen will appear. Press the **down arrow key** to **Reboot** and press **enter.**



1. Once the firewall reboots, you will be able to set your username and password. You will first be prompted to enter the PA-220 login. The username and password will be the default credentials, which are both **admin.** After typing that, you will be prompted to **“Enter new password.”** Choose your password and make sure to remember it. For the **“Confirm password”** section, enter the same password.



**Problems**

A problem I faced during this lab was getting into maintenance mode. Multiple times when typing to enter maintenance mode there was a 5 second input delay, which would cause us to not have enough time to enter maint within the 5 seconds allowed, causing use to go to the boot sequence repeatedly. We then tried pressing the m key repeatedly but that would end with use typing m multiple times when trying to enter maintenance mode. I figured out that if I waited around 10 seconds and typed maint before anything showed up, it would be entered within the 5 seconds because of the 5 second input delay, allowing me to enter maintenance mode.

**Conclusion**

Factory resetting allows you to reset a firewall to factory settings when there is an unknown username and password, so you can set your own username and password. While going through the factory resetting process there are some steps you need to go through. You will need to use the **maint** command to enter maintenance mode and you will need to navigate through this mode to be able to factory reset your firewall. Although I was having problems entering maintenance mode, I was able to eventually figure out how to get in, allowing me to complete the rest of the lab. Through this lab, I learned how to factory reset a firewall as well as understand what factory resetting is and when it is needed.

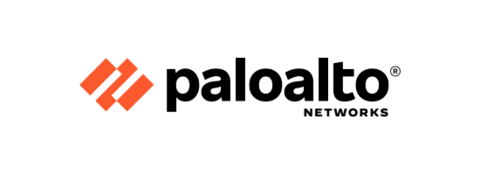
**Teacher Signoff Page of Lab Completed**

The stamp below recognizes that

Evan Choi

has completed

**Lab 4 – URL Filtering**

 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

Period 5