Palo Alto Networks Cybersecurity Academy – Factory Resetting a PA220 Firewall

Colin J. Faletto, CCNA

paloalto NETWORKS

Purpose

This lab serves as an introduction to the world of cybersecurity by documenting one of the most basic functions of a networking device – a factory reset. This lab teaches users how to manage a Palo Alto networking device through the console interface and eases them into the world of firewall management.

Background

Palo Alto Networks is a networking and cybersecurity company from Santa Clara, California. They are a member of the S&P 500. They focus mainly on the business market, creating scalable security solutions for many of the largest companies worldwide.

The Palo Alto PA220 is a firewall sold by Palo Alto Networks. Contrary to Palo Alto's main market, the PA220 is intended for small businesses or home offices. Marketed as a NGFW, or Next-Generation Firewall, the PA220 uses machine learning to identify attacks instead of relying on a simple signature check like traditional firewalls. This technology allows the PA220 to identify undocumented threats and brand-new exploits without intervention from Palo Alto networks themselves. The PA220 also prevents threats by filtering URLs and securing against DNS-based attacks. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The PA220 doesn't have a fan, and instead uses hexagon-shaped vents to passively filter air. The firewall's compact form factor allows it to easily fit alongside existing network devices.

The PA220 is a hardware firewall, meaning it's a physical, tangible device as compared to a virtualized software firewall. By using this legacy form factor, the PA220 can provide a higher degree of reliability as the physical device can be troubleshooted by the end user. With a cloud-based software solution, security is managed remotely by an outside company, meaning that any issues with this outside company could leave software firewall users vulnerable for hours or even days. Hardware firewalls put this control in the hands of the users, allowing security to be implemented immediately by an experienced technician.

One major draw of software-based firewalls is that they can be managed remotely without a physical or local network connection to the firewall. The PA220, despite its form factor, also supports remote management through Palo Alto's Panorama software. Panorama supports a wide range of Palo Alto firewalls and allows them all to be remotely monitored and managed from a single dashboard.

The Palo Alto PA220 runs a piece of software called PAN-OS. In this lab, our firewall is running PAN-OS 8, which is an older version of the software that has reached end-of-life. The software is accessible through multiple interfaces, including through a console

connection and through an HTTP connection on a local network. By default, PAN-OS is protected through an account called *admin*, with a default password set to *admin*.

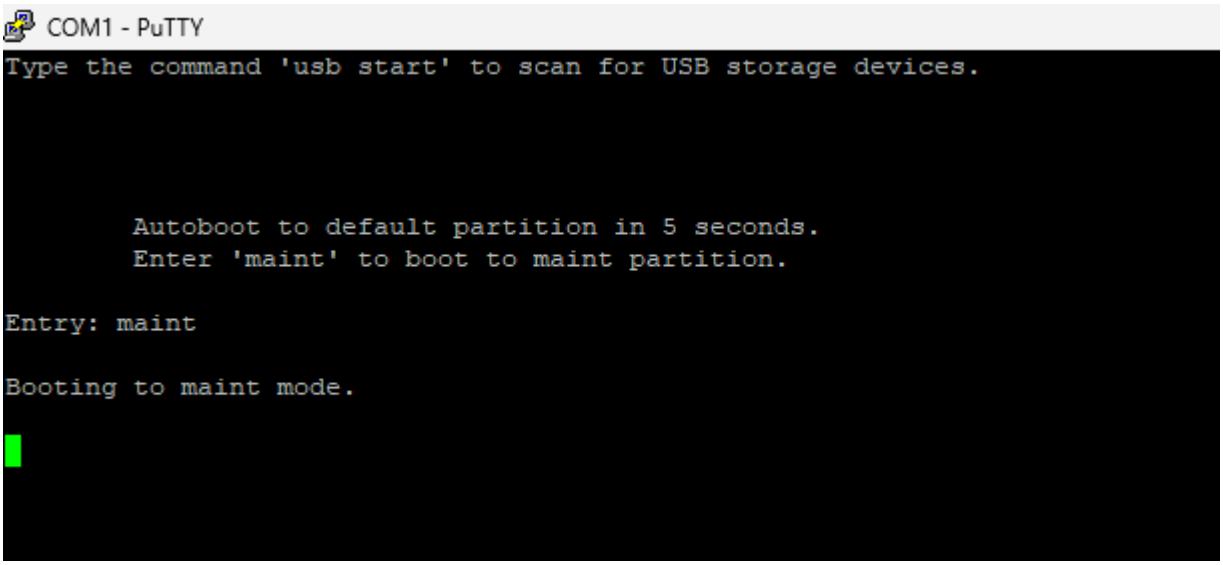
Lab Summary

In this lab, we used the console connection on the PA220 firewall to enter maintenance mode, then after entering maintenance mode, factory reset the firewall.

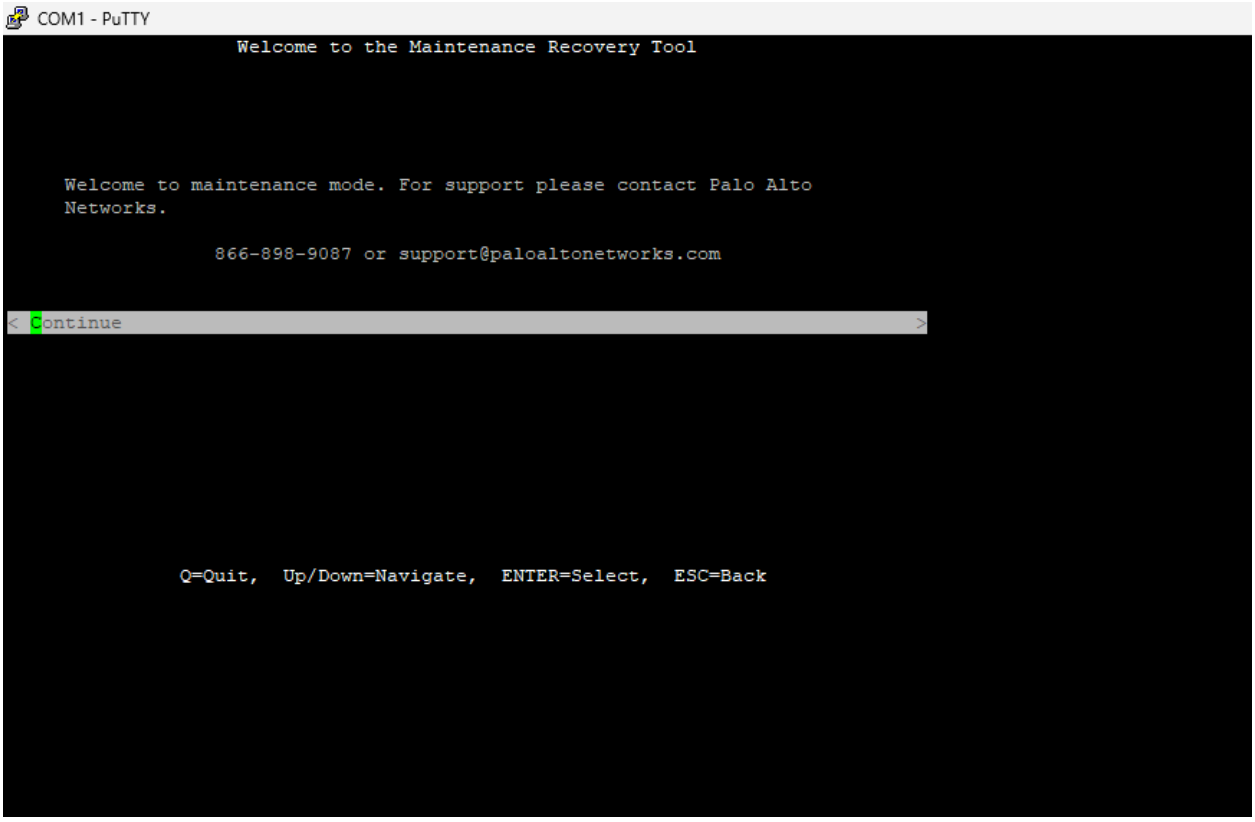
Lab Commands

With the firewall unplugged from power, connect a console cable from the firewall to a computer with a terminal emulator installed. Start the terminal emulator, then plug the firewall into power.

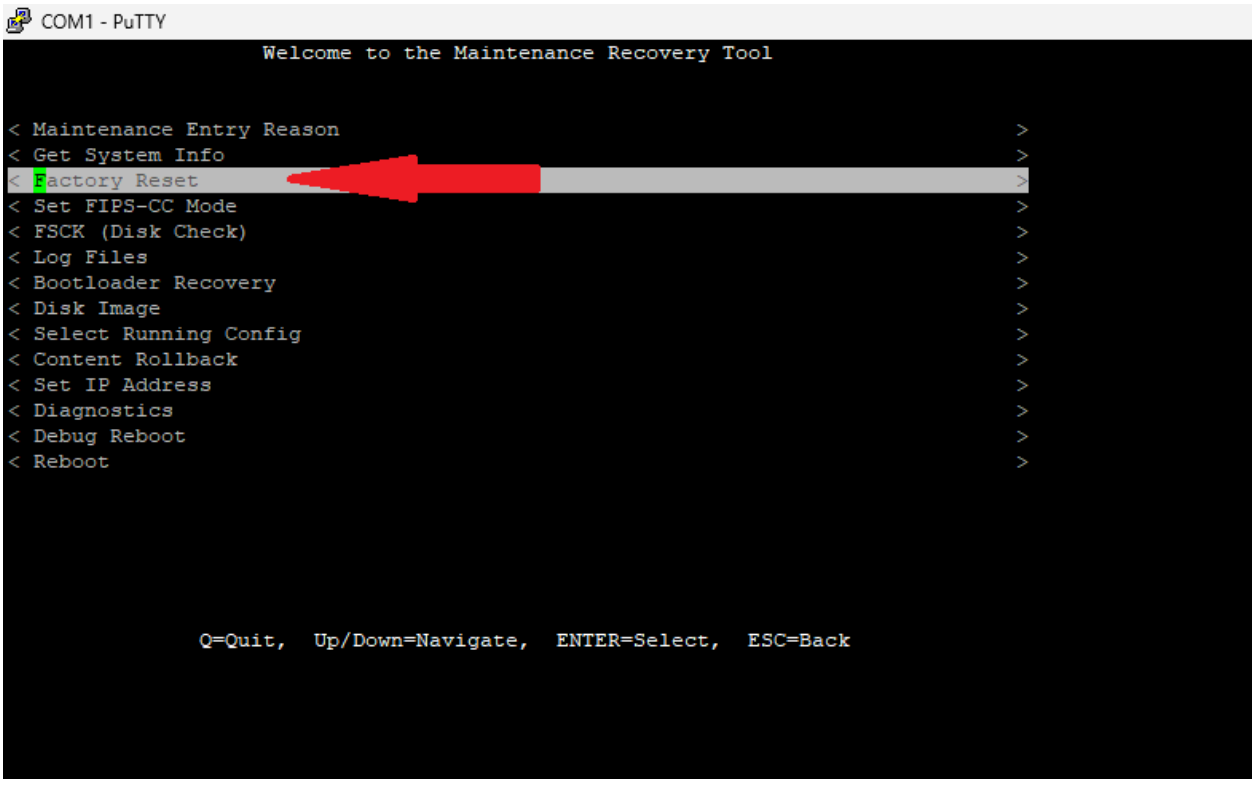
Eventually, you will be prompted with the following: *Enter 'maint' to enter maintenance mode*. Type 'maint' and press Enter.



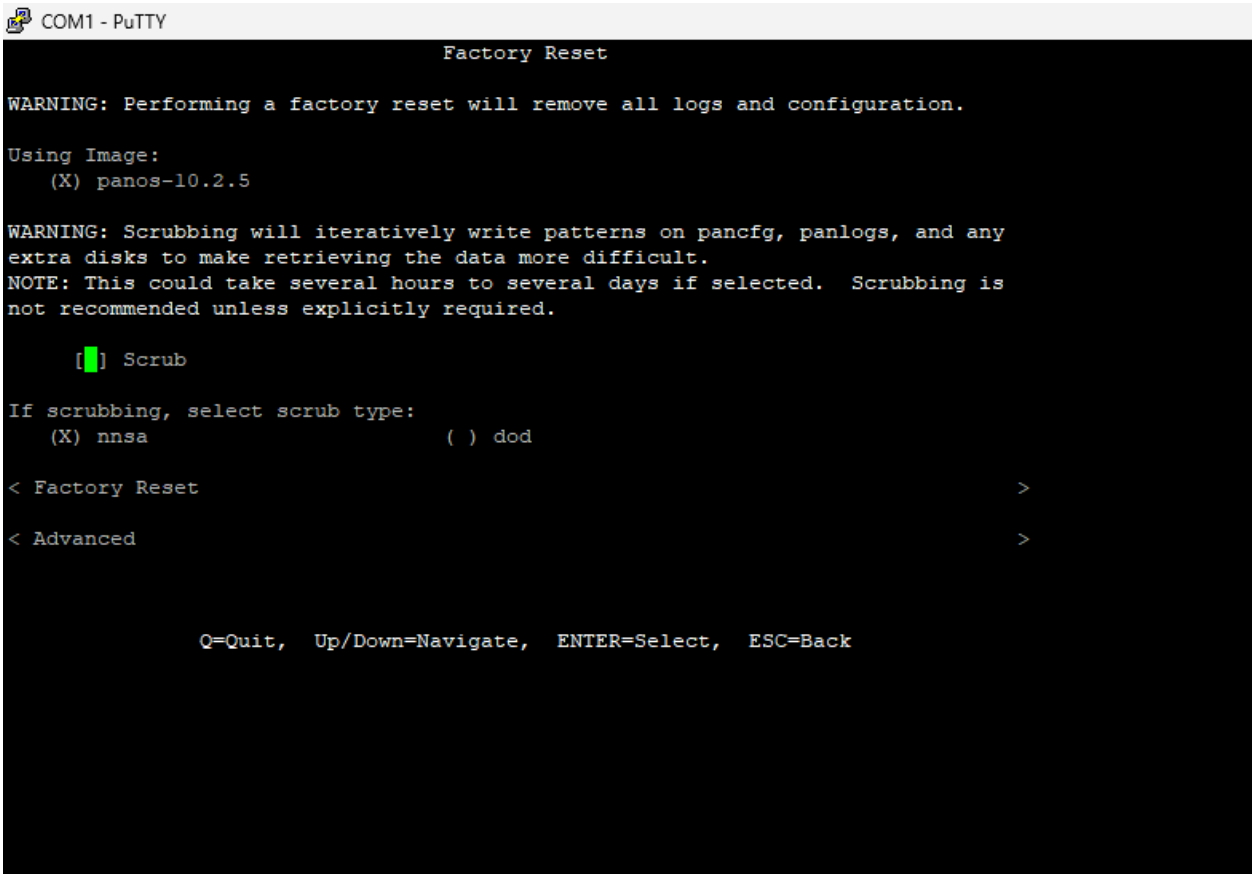
Wait approximately five minutes. You will then be presented with a welcome screen. Press Enter to continue.



You will see the main maintenance mode screen. With the arrow keys, navigate down to 'Factory Reset' and press Enter.



You will then see more options related to factory resetting the firewall. Navigate to ‘factory reset’ and press enter.



Problems

By default, the PA220 will boot into maintenance mode after a factory reset. While this may be confusing for some users, this problem can be remedied by simply selecting *Reboot* instead of *Factory Reset*.

Conclusion

The Palo Alto PA220 was previously a very unfamiliar technology to me, as I have never worked with firewalls before. However, within an hour or two, I developed a strong understanding of the PA220’s console interface and learned its basic maintenance functions. I’m eager to learn what else Palo Alto firewalls have in store, and I’m excited to set these firewalls up in more advanced configurations.