**Palo alto version updates**

Derek Liu Cybersecurity Period 5

Lab #3

**Version Updates on Palo Alto Firewall***Derek Liu*

Purpose

To update an outdated firewall software version to the latest version to better protect networks and defend against cyber threats.

Background Information

After successful configuration of a Palo Alto firewall and connecting it to the internet, it is possible to download and install version updates for the firewall. When accessing a new Palo Alto firewall, the software may not necessarily be the latest version. We have a firewall configured for a SOHO network, but its software version is in 8.0.20 and the most recent version as of September of 2022 is 10.2.2-h2. In this lab, we will update the Palo Alto firewall from version 8.0.22 to version 10.2.2-h2. This is necessary to ensure the firewall has the ability to defend against the ever-changing advances in technology and threats.

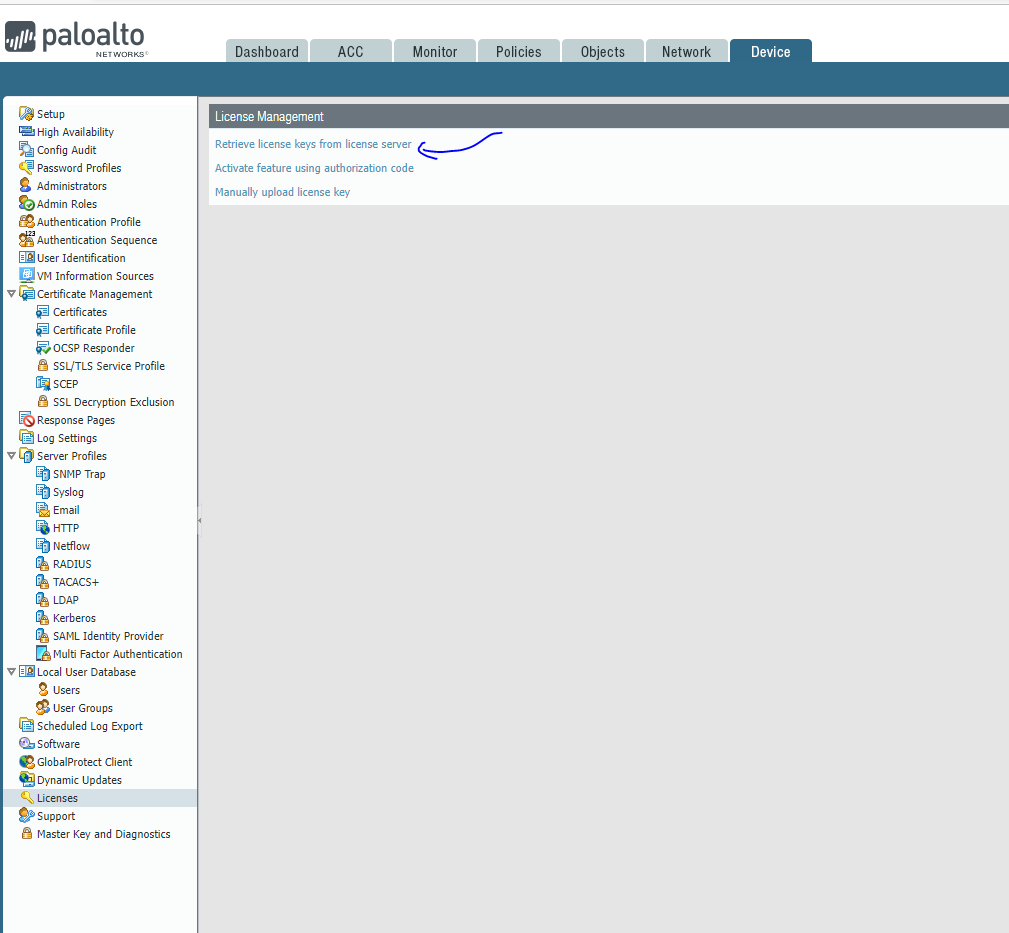
With each version update, new features usually come with it that can increase security and support a zero-trust policy. In the case of version 10.2, it comes with cloud identity engine, PAN-OS OpenConfig Support, administrator level push, and advanced routing engine.

Through the cloud identity engine, Palo Alto firewalls can provide a cloud-based solution to reallocate resources for authentication from the firewall to the cloud. OpenConfig support means that the firewall will allow OpenConfig data models and protocols to automate configuration. Adminstrator-level push allows for configurations to be pushed onto certain managed firewalls. Advanced routing engine assists in creating routing maps while reducing the learning curve. In this lab, we will be updating the firewall to a version that can support these features.

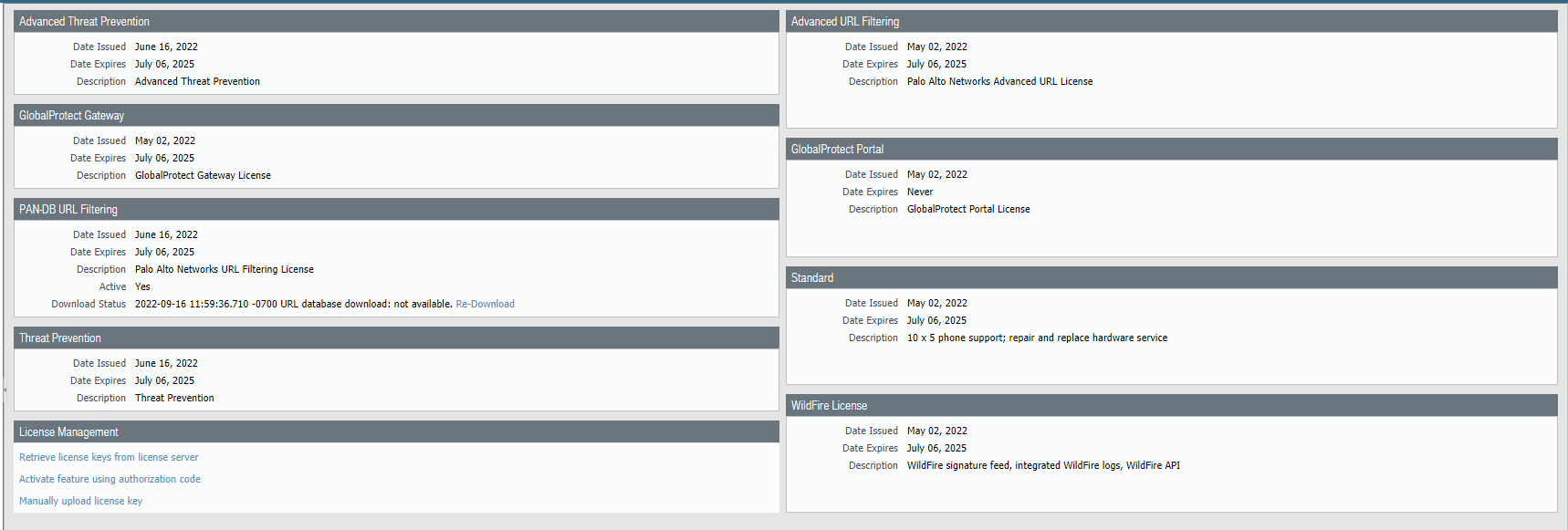
Palo Alto firewalls have a unique update sequence.

Configurations

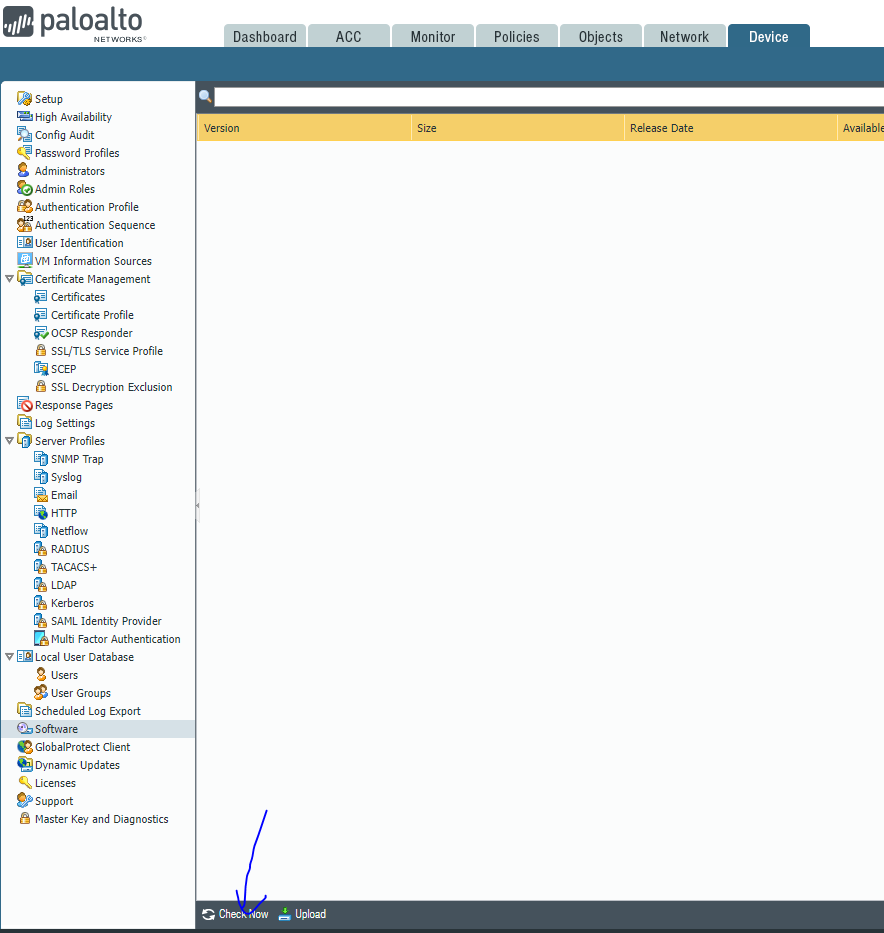
1. The first step would be to log into the firewall through the management interface. We connected the management port to a configured trusted port on the firewall using a copper straight-through cable.
2. After logging into the firewall, go to device -> licenses and then Retrieve license keys from license server.



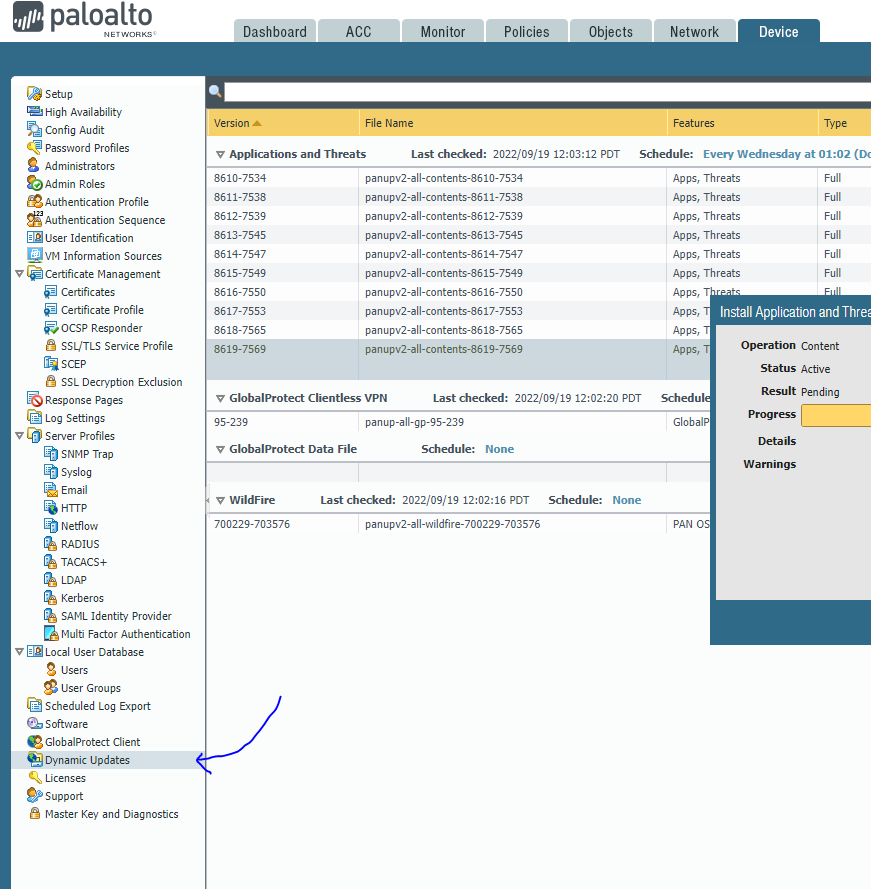
1. The result should look something similar to this:



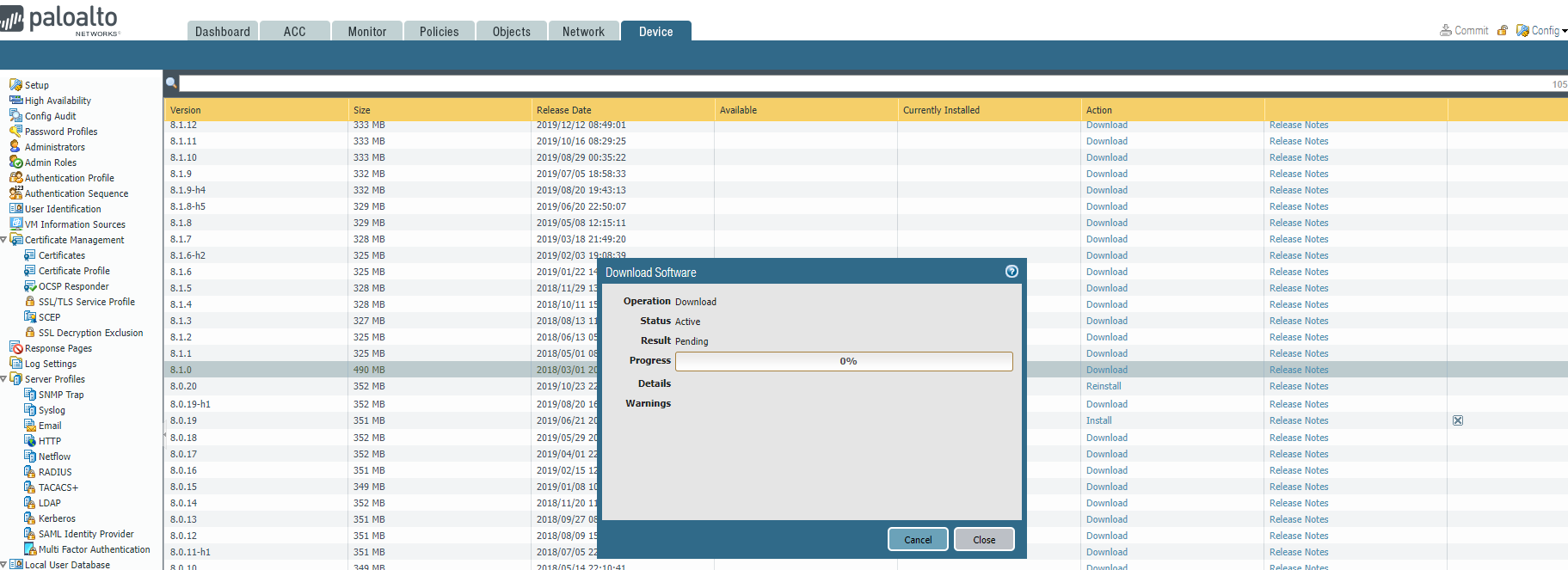
1. Go to Devices -> Software, and click Check Now



1. At this point, you should be able to see the available versions and the version that your firewall is currently on.
2. Go to Device -> Dynamic updates, and download everything applicable (VPN, Wildfire, Global protect)



1. Upgrade the firewall in this order
   1. Download and install the latest software in the third digit of the version (e.g if current version is PAN-OS 8.0.x then install 8.0.20.
   2. After installing the highest version in the third digit, download and install the version that’s one greater on the second digit (e.g. version 8.0.20 to 8.1.0).
   3. After reaching the highest number available for the second digit, upgrade to the version with one greater on the first digit while the second and third digits are 0.



This should be what the update screens look like.

1. Finished

Problems

Due to the complexity of the update process, we ran into a lot of problems. Originally, we tried to update directly to the latest version but ran into the error of having to update to the next version. We also originally didn’t do dynamic updates which prevented us from doing updates. Another problem that we faced was timing out while getting the configuration lock. The problem was fixed after we rebooted the firewall.

Conclusion

In this lab, we updated a palo alto firewall 220 with out-of-date software. After connecting the firewall to the internet, we were able to obtain the license and begin to update the software and install dynamic updates. After successful installation of the newest version, we can start implementing new features on the firewall.