OS & Licensing

*Palo Alto – Updating Software*

Adv Cisco Cybersecurity – Lab 3

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 3: PA 220 – Updating OS & Licensing*

**Purpose**

The objective of this lab was to update the Operating System to its most recent versions. Understanding the procedure in retrieving Licenses was important as well.

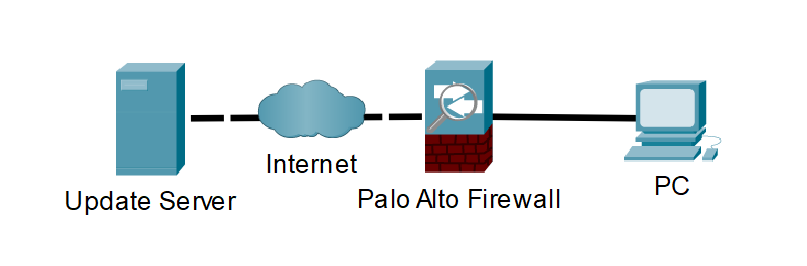
**Background Information**

Palo Alto has Operating System (OS) versions for their hardware firewalls, in which their proprietary name for their OS is called PAN-OS. As of October of 2022, the most recent version is 10.2.2-h2. This OS is where all the features originate from, including a traffic classification technology called App-ID, user identification and authentication called User-ID, and protecting users from phishing attacks, malicious pages, and anomalous user behavior. Ultimately, firewall operating systems determine the policies that can be created and deployed.

Palo Alto fetches licensing data and updates from the Palo Alto Licensing Server at the address: “updates.paloaltonetworks.com.” Certain features of a license have to be bought and activated for use. One example is the GlobalProtect license, which can use basic features like configuring internal gateways but require activated licenses to utilize much of its more important features like VPN and tunneling. On the license menu of the GUI, it displays all the current activated licenses and its corresponding expiration dates. For the OS, updating the version generally employs new best practices and presents new features onto the firewall.

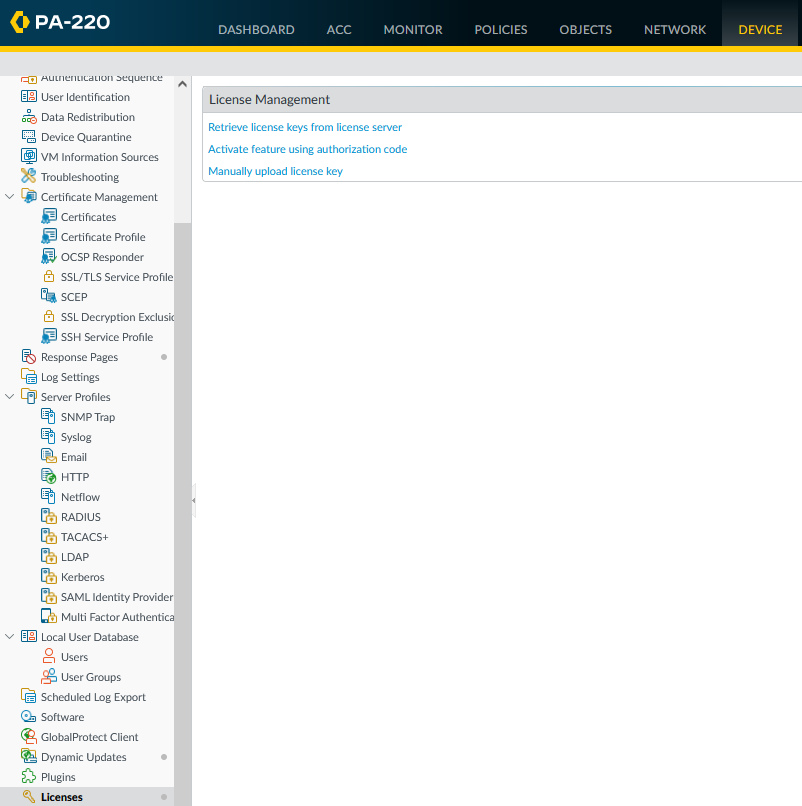
**Lab Summary**

A prerequisite of connecting to the internet via the firewall is necessary. This step was completed in SOHO configuration (See Lab 2: *SOHO*). First, retrieve the licenses under the license management menu under Devices > Licenses in the GUI. If a proper DNS was configured and is properly routing to the update server on the Internet, a large list of licenses (currently active on the device) will appear. Under Dynamic Updates, update all the recent software to its most recent version. The older versions do not need to be downloaded in the process of downloading the most recent ones. Certain Dynamic Updates include Palo Alto Wildfire, Device Dictionary, GlobalProtect VPN, and other general Applications and Threats protection. Independent of these updates, Software Updates upgrade the general Operating System to the newest version. Under Device > Software, these software updates have to be installed in a certain order. To upgrade from a software version 10.1.x to 10.2.x, you must first download the most upgraded update for that segment, before transitioning into the next segment. For example, to get from v10.1.1 to v10.2.2, one must first download the most upgraded 10.1.x version, in this case 10.1.7, before downloading and installing 10.2.1. Then, one can download and install the software version in that segment. It takes about 10-15 minutes to install one new OS update, because the device has to reboot in between each process. At the end, all software is up to date and licenses have been retrieved.

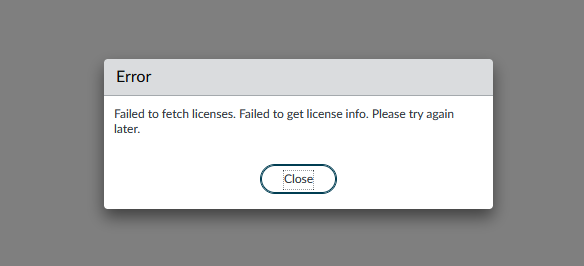
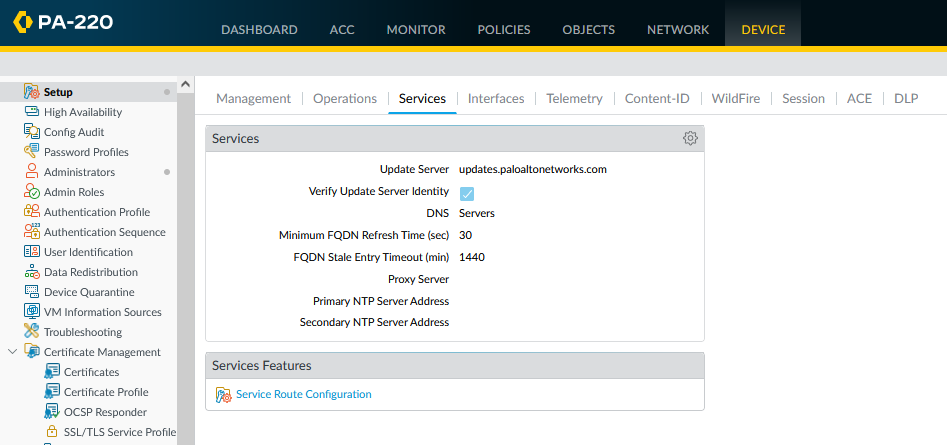


Firewall has to access the update server via the internet.

**Procedure**

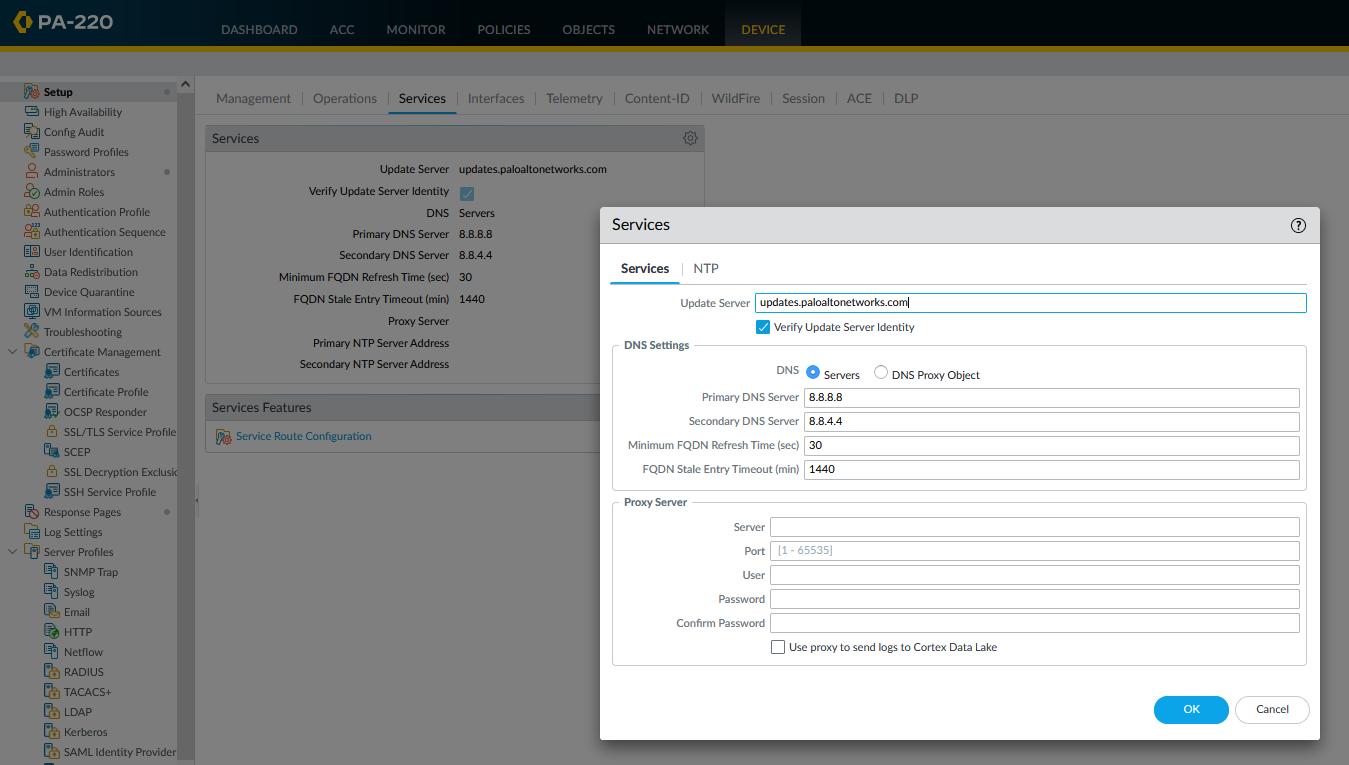
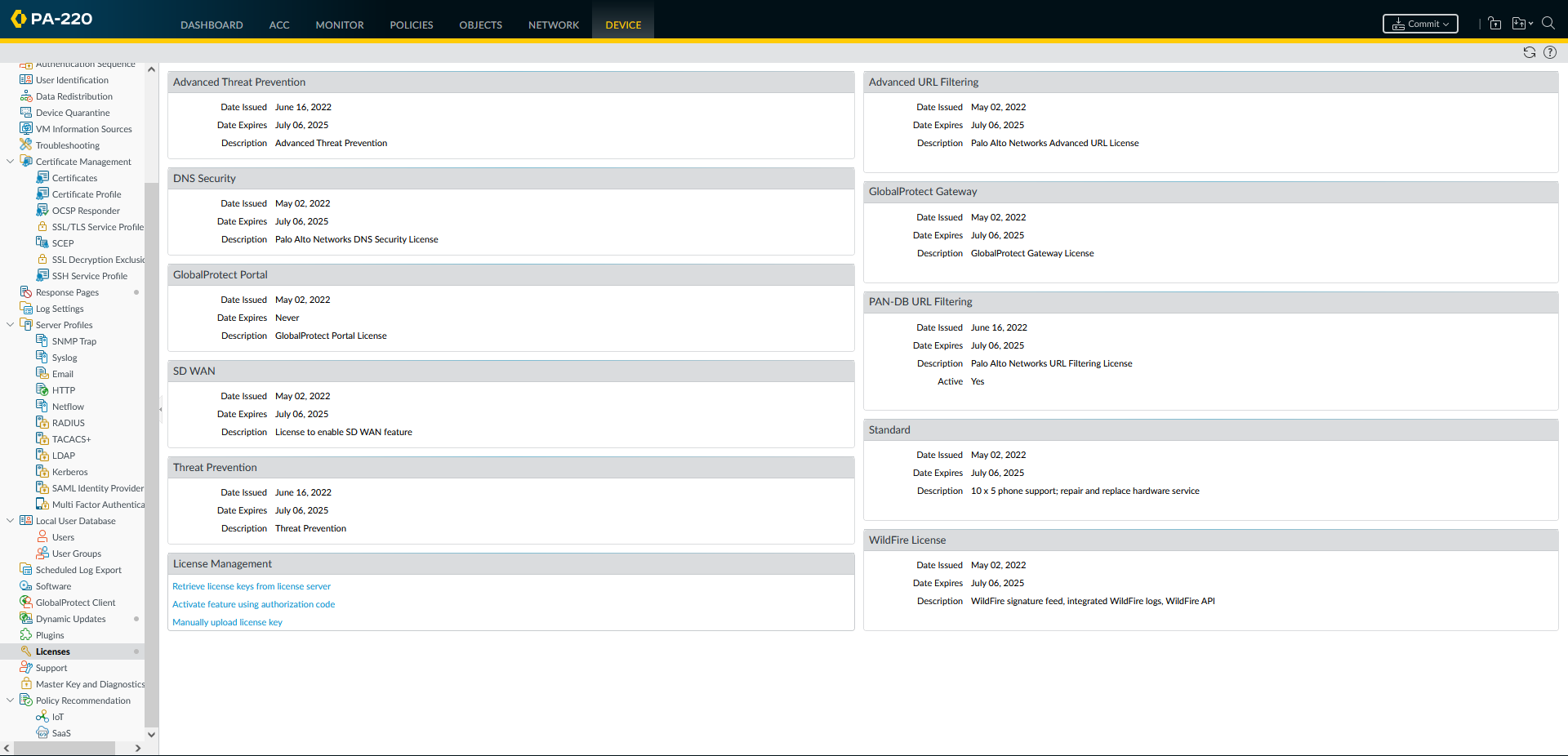
****

Start by going to the License menu under Device > Licenses.

****

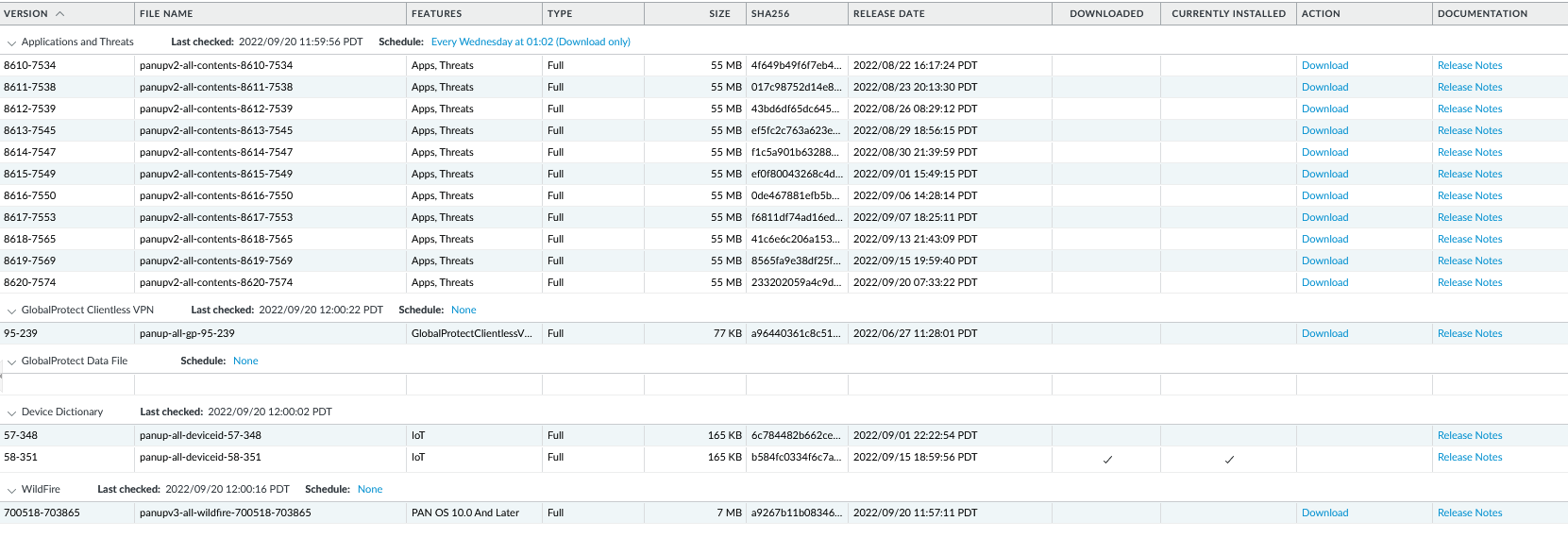
Go to Device > Setup > Services to view DNS service options. Select the settings icon to perform edits.

When attempting to receive license keys, it may fail. If internet connection appears fine, it is most likely a DNS server issue.

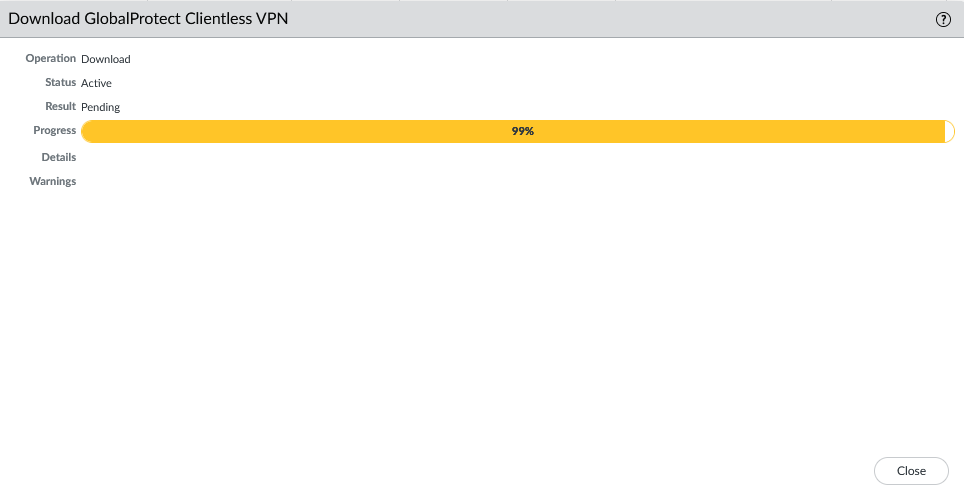
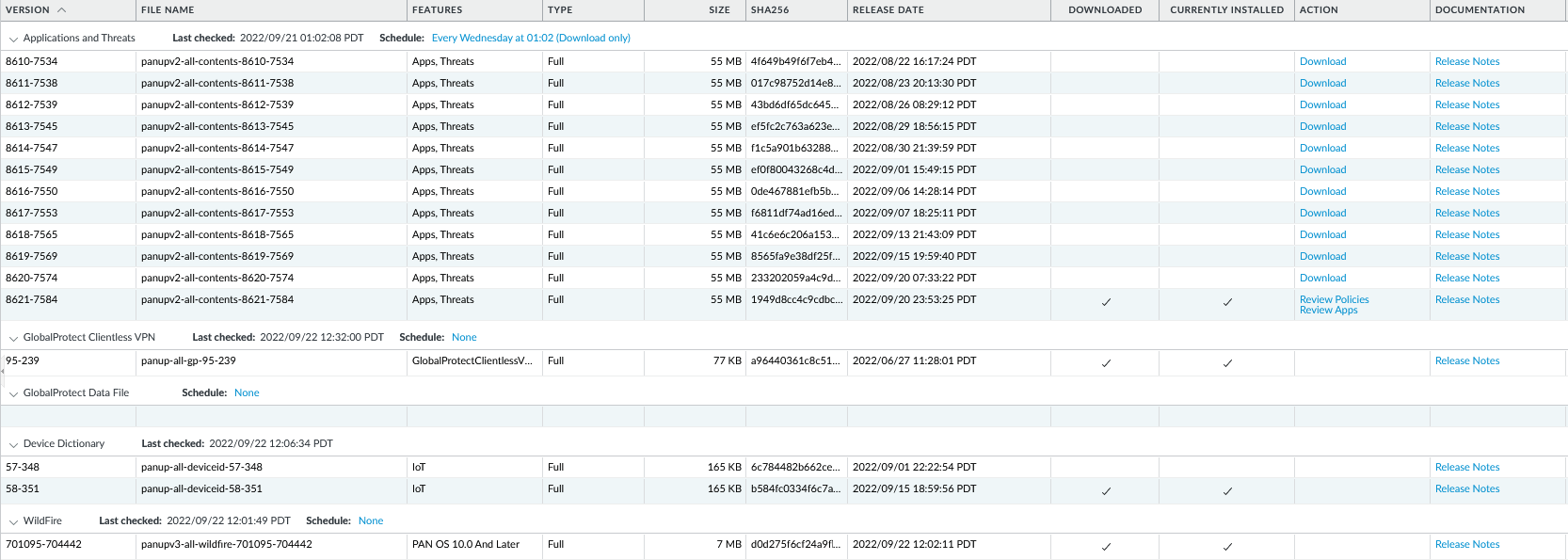
****

Attempting to retrieve license data again, they appeared.

Change Primary DNS server and Secondary DNS server to a working one. A primary address of 8.8.8.8 and secondary address of 8.8.4.4 is the Google Public DNS.

****

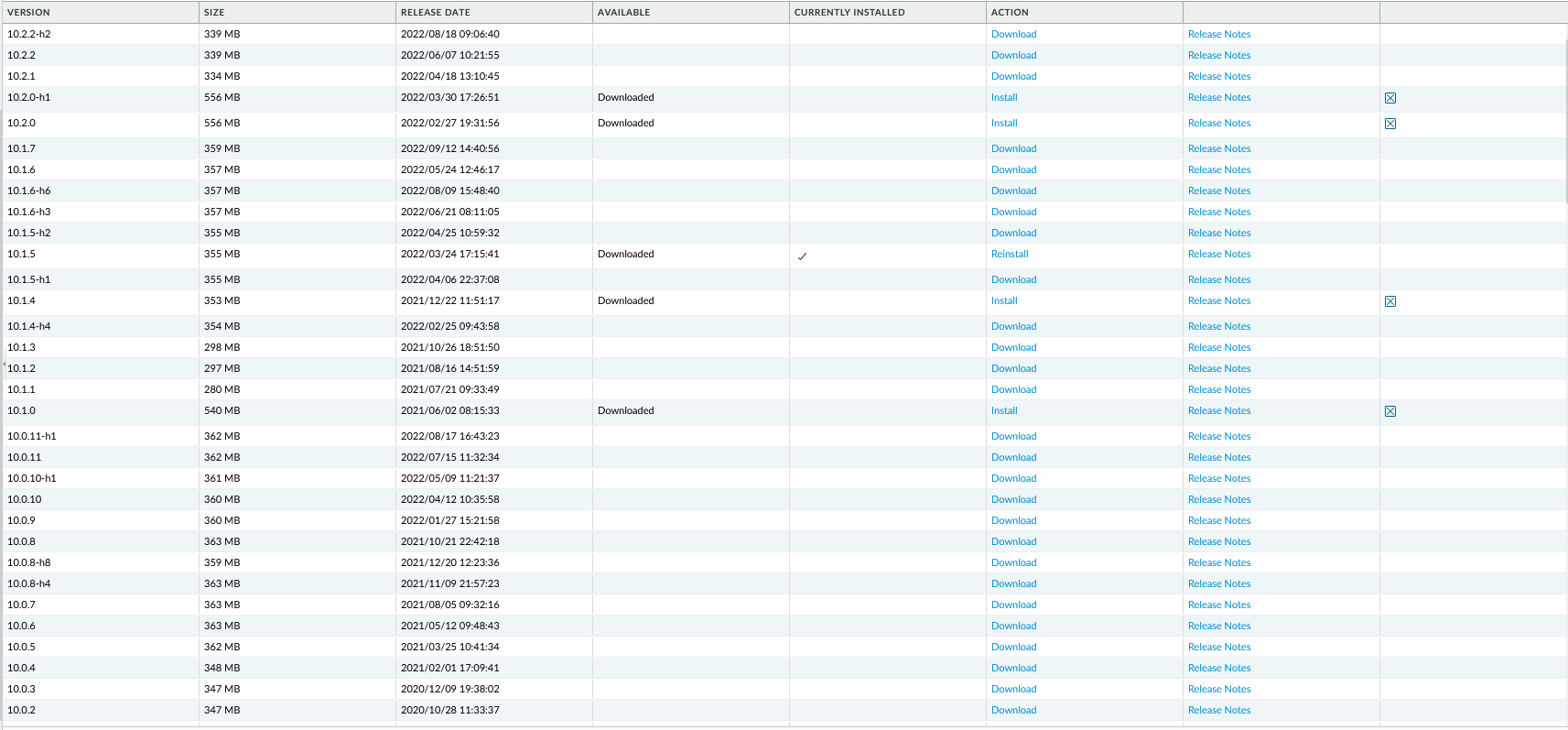
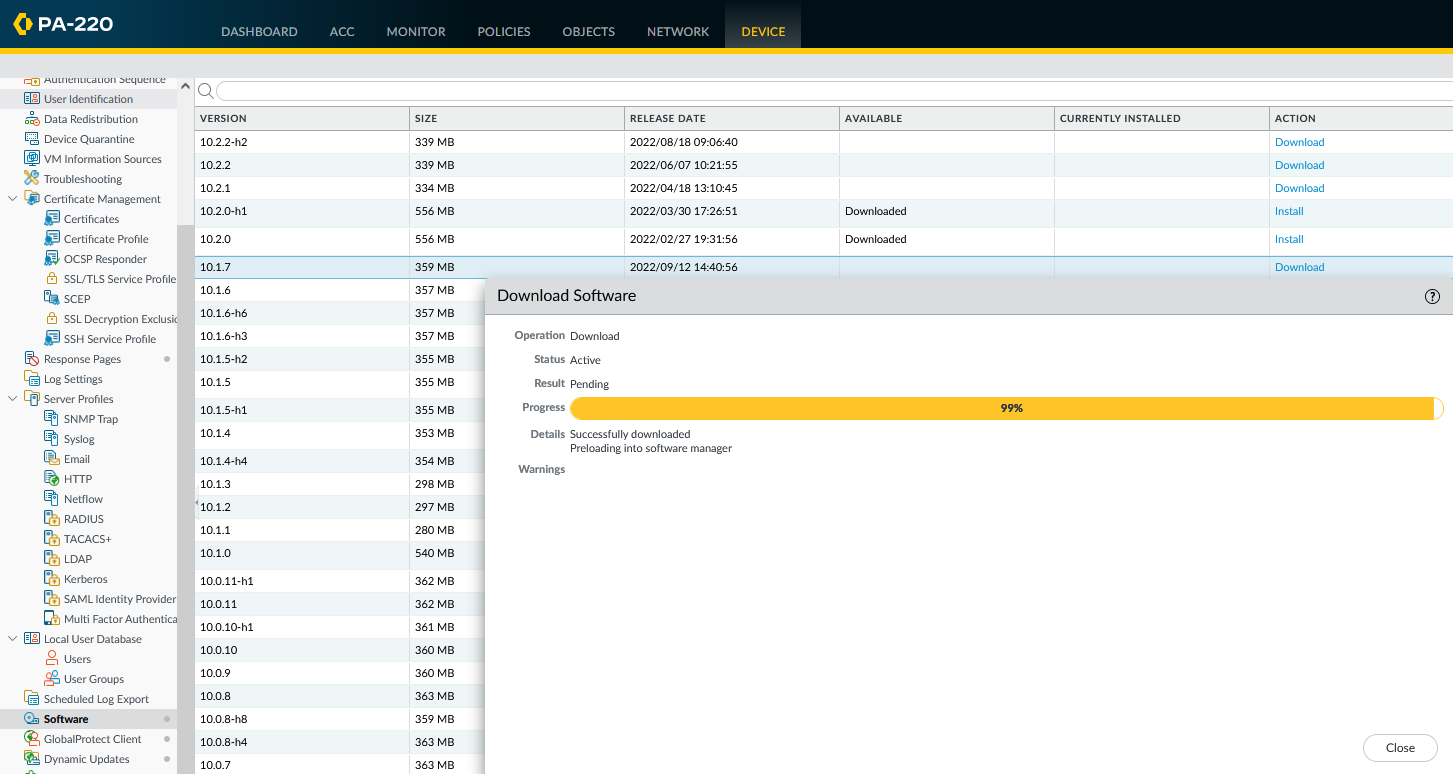
Dynamic Updates above. First download, and then install the most recent version of each category.

****

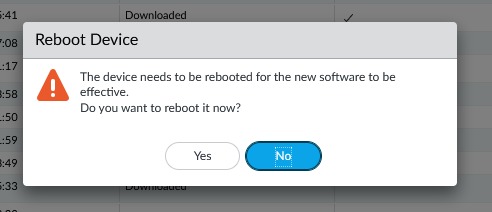
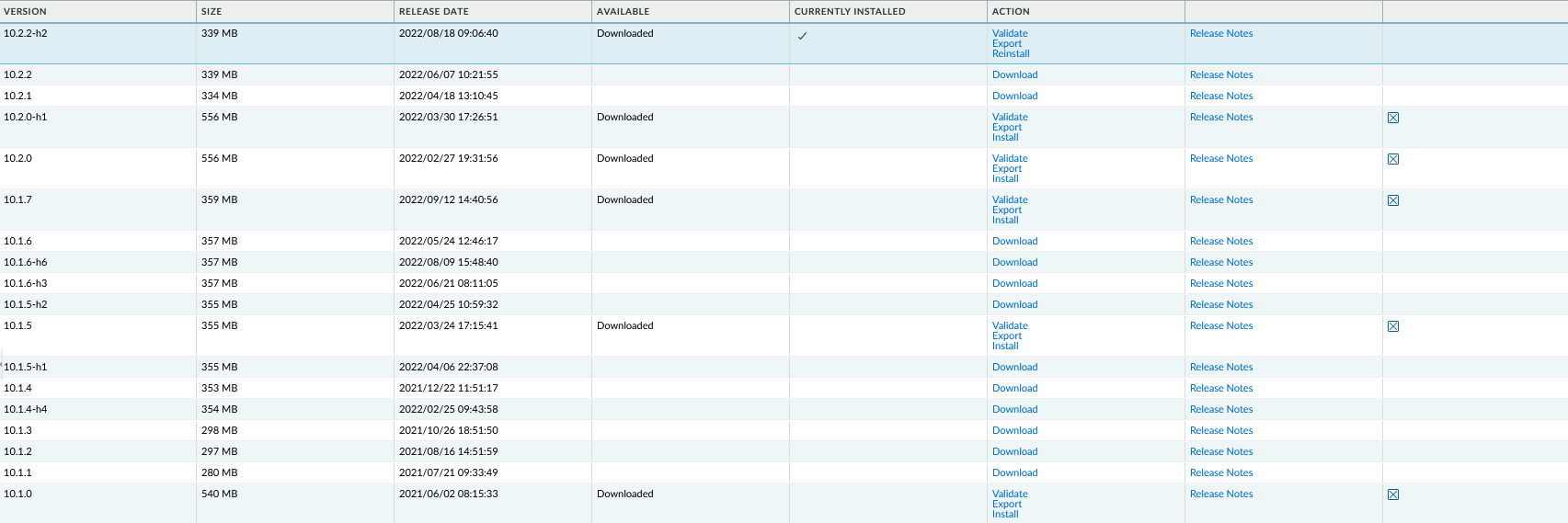
All new Dynamic Updates have been installed.

An example of downloading a dynamic update. This download was the GlobalProtect Clientless VPN new version.

After refreshing the software version list by clicking the “Check Now” button, all OS versions should appear. This is located under Device > Software.

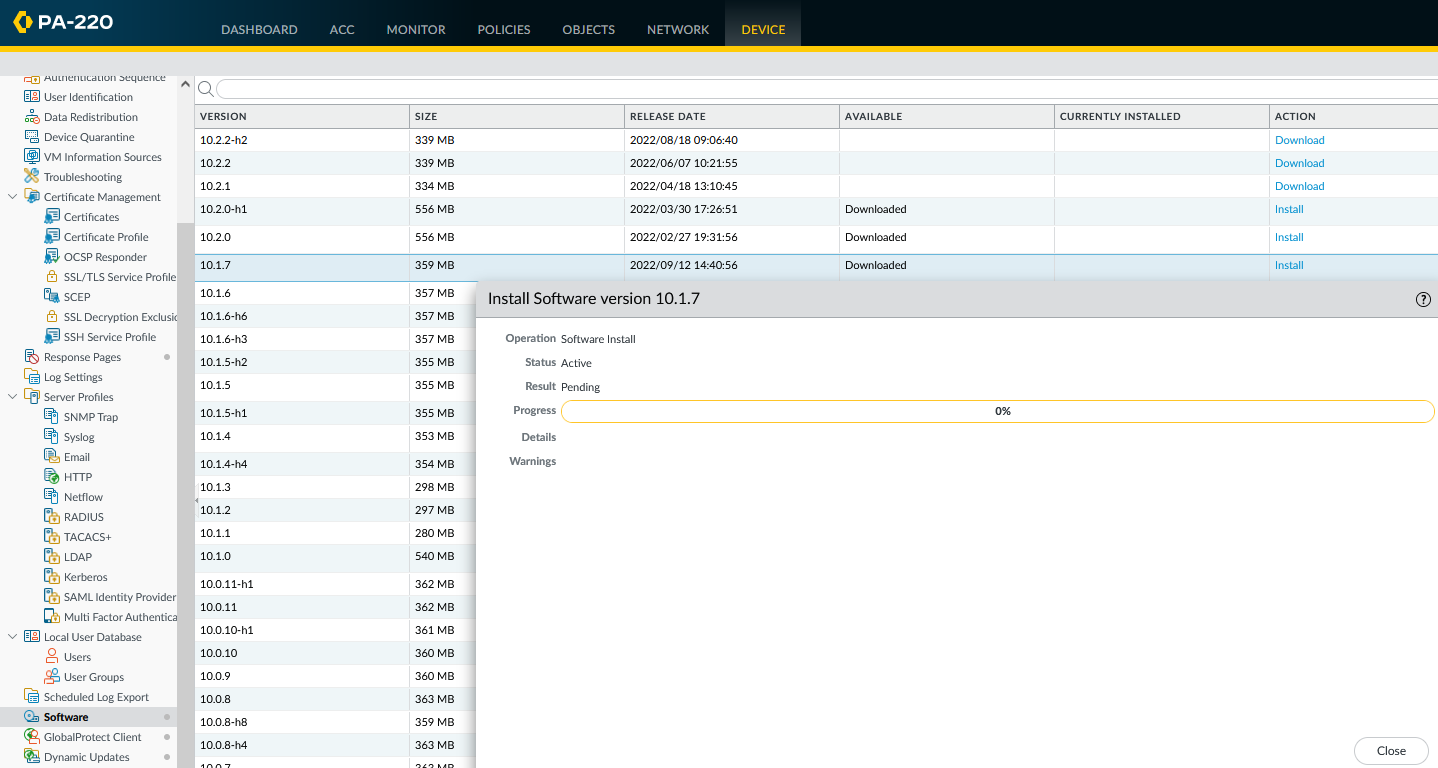
****

In its unique order, download the newest version for that segment. As the version after the factory reset was 10.1.5, we downloaded 10.1.7 before moving to the 10.2.1 line.

****

A reboot is required in between each OS version’s installation. This takes about 10-15 minutes.

After each download, an update must be installed. This is the status bar for installing 10.1.7.

****

Repeat the process for 10.2.1, and 10.2.2 to get to the most recent version. The latest version has finally been installed.

**Problems**

Despite being a straightforward, there were quite a few problems along the way, whose solutions were unclear, as there were many overlapping actions done to resolve the problems. However, we do have a clear solution for one of the biggest problems: the DNS servers. To access the Update Server “updates.paloaltonetworks.com,” the firewall had to have proper DNS address. This solution was indicated in the procedural process and its pictures. We used the public Google DNS servers, consisting of the Primary Address 8.8.8.8 and the Secondary address of 8.8.4.4. Adding a proper DNS address is indeed necessary. The license retrieval, under the Device tab, has been a success. However, we faced the peculiar issue of not seeing the “software” despite having license retrieval. By changing the DNS servers to 1.1.1.1 and 4.4.4.4 for the primary and secondary servers, respectively, the outcome did not change. This time, though, we found and pressed the “Check Now” button towards the bottom of the GUI, and the software updates show up. We do not know if this has a conflict with the chosen DNS server, as the Check Now button was not pressed before changing DNS servers. Checking later, though, the software versions can be accessed regardless of either DNS server. After the DNS issues were resolved, the updates and corresponding reboots functioned as predicted.

**Conclusion**

Updating licensing and software is a small but important step in configuring the firewall for best practice. Although we faced unclear solutions to our issues, this process has been well understood and implemented. From the unique pattern in updating the software versions, to the installment of dynamic updates, and to changing the DNS server, it was a big step towards fully understanding the Palo Alto firewall’s functionalities.