Background

A clientless VPN has all the benefits of a client-based VPN, such as creating a secure connection between a device and network in settings such as corporate. However, it has the added benefit of not requiring installing a software (GlobalProtect) to access the VPN. This VPN can be very helpful for employees of companies working from home and need administrative privileges without opening the network to threats from malicious hacking that could result in loss of confidentiality, integrity and even theft. Clientless VPNs provide an effective way of doing so as you simply type the GlobalProtect Palo Alto address on a search bar a browser and begin to manage the network. It is dynamic because it can work on any machine and does not require one to install software on every single computer that needs to have access to the management of the firewall.

However, clientless does not come without its challenges. It does not offer access to some advanced features that GlobalProtect client-based VPN offers, such as Open VPN, SSTP, or two factor authentication. Some potential threats to the network also become slightly harder to see and detect and mitigate when using the web-version of GlobalProtect instead of the software based.

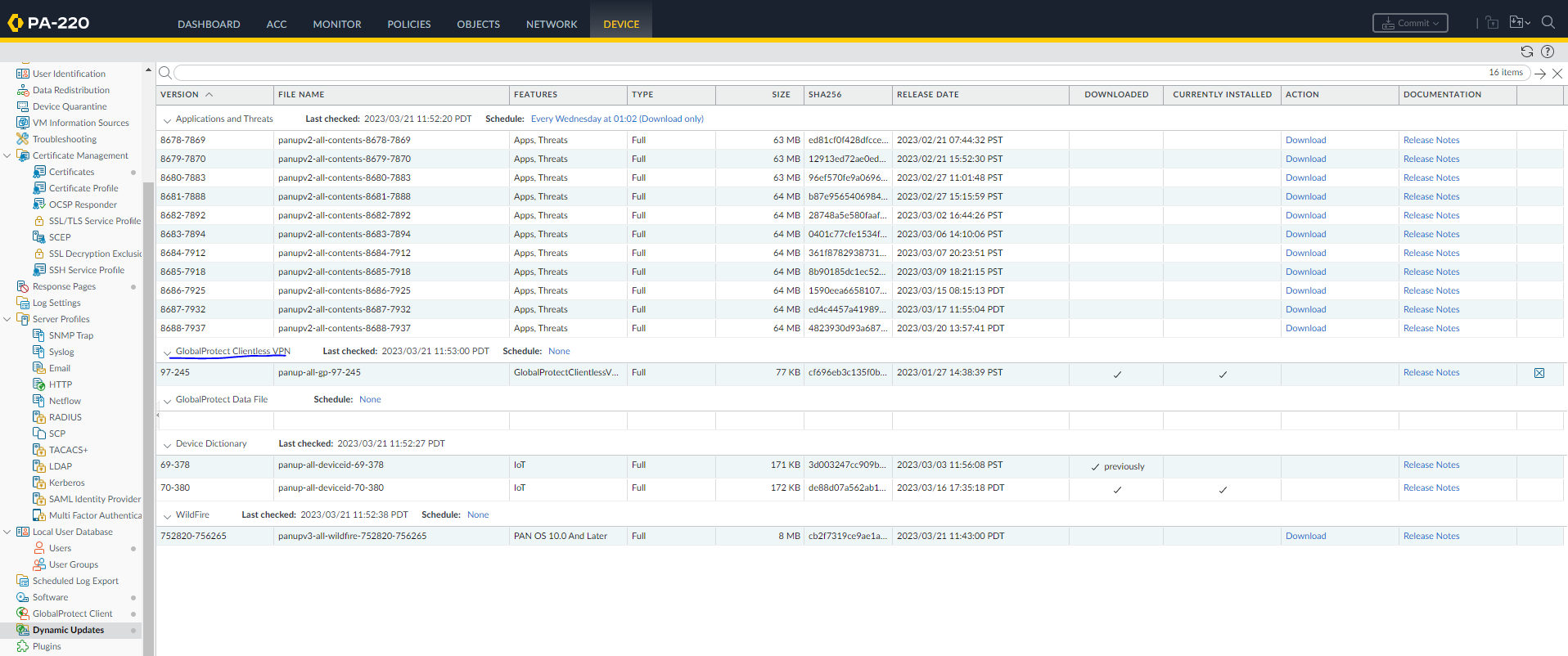
Lab Summary:

A screenshot of a computer

Description automatically generated with medium confidence

\*This lab is a continuation of lab 11 – remote access clientless.

Step 1: First go to licenses, and retrieve clientless GlobalProtect VPN



Step 2: go to Network, Clientless Apps, and configure the following

Graphical user interface, text, application

Description automatically generated

Step 3: Under DNS proxy and configure the following

Graphical user interface, text, application

Description automatically generated

Step 4: Under portal, configure the following

Graphical user interface, text, application

Description automatically generatedStep 5: Double check here

Graphical user interface, application

Description automatically generated

Step 6: Go to Global Protect Portals and enter the following configs Graphical user interface, text, application, table, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Step 7: Now go to agent and enter the following configuration. Double Check IP addresses.

Graphical user interface, application

Description automatically generated

Step 8: Now enter the following address and log instep Graphical user interface, application

Description automatically generated

Step 9: Here you application will openGraphical user interface, application

Description automatically generated

Step 10: Use XAMPP to create a web server. To test, create a basic website using HTML. Once you’re done, it should look like this once you connect to F009.

Graphical user interface, text, application

Description automatically generated

Problems:

The only problem we had during this short lab was that we weren’t able to log in to GlobalProtect. After several trials of checking to see whether our certificates were properly installed, whether we were typing the right address, whether we had the right address and whether we had committed our changes, we realized that the problem was the browser we were using. Interestingly, the website simply failed to load on Chrome after a lot of trials, we used firefox and it worked immediately. We were embarrassed, but realized that firefox is a lot better and has some good features for clientless managing interfaces. From now, we will use that.

Conclusion:

This lab was fairly easy to complete as we already had our basic configuration done from the previous lab. All we had to change was the way were authenticating outside user who were trying to remotely access the network inside. For the last lab, the proof of an established connection was a working RDP, but for this lab it was connection to a web server. Therefore, we had to create a web server using XAMPP so that the remote user could load into something when they accessed out network.