Remote Access VPN

*Clientless VPN*

Adv Cisco Cybersecurity – Lab 11

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

*Lab 11: Palo Alto Remote Access Clientless VPN*

**Purpose**

The purpose of this lab is to set up a clientless remote access VPN. The established VPN tunnel should be able to access internal resources by typing an address into a web browser and entering configured credentials.

**Background Information**

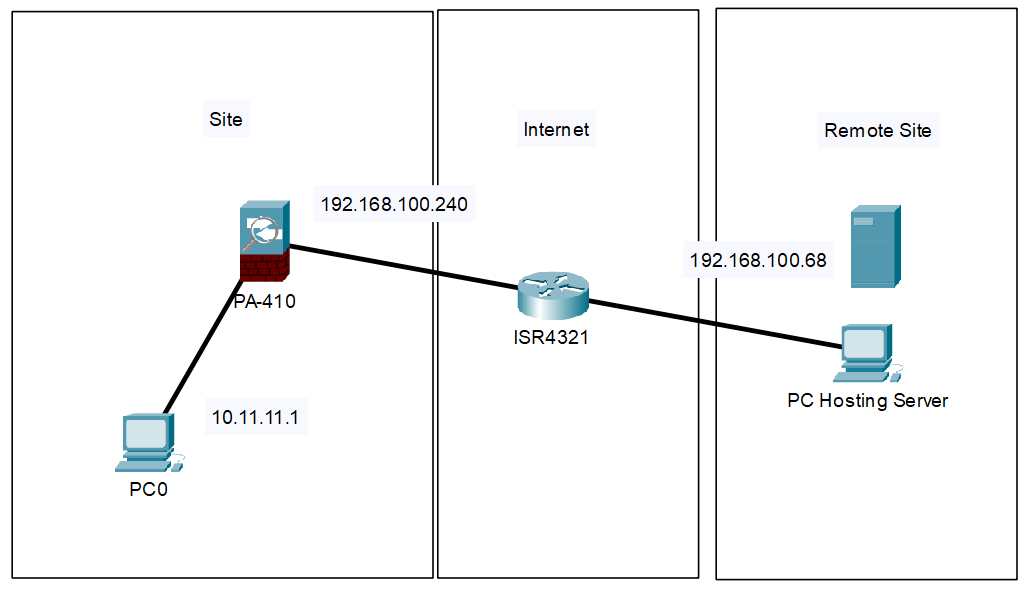
A clientless VPN or browser-based VPN allows for users to access internal resources in a network through a web browser without the need to install software or client-based applications. Although it is still being on hosted on GlobalProtect, the GlobalProtect monitor application and certificate authentication is not the course of action in clientless, but rather to access the interface’s tools directly from a web browser.

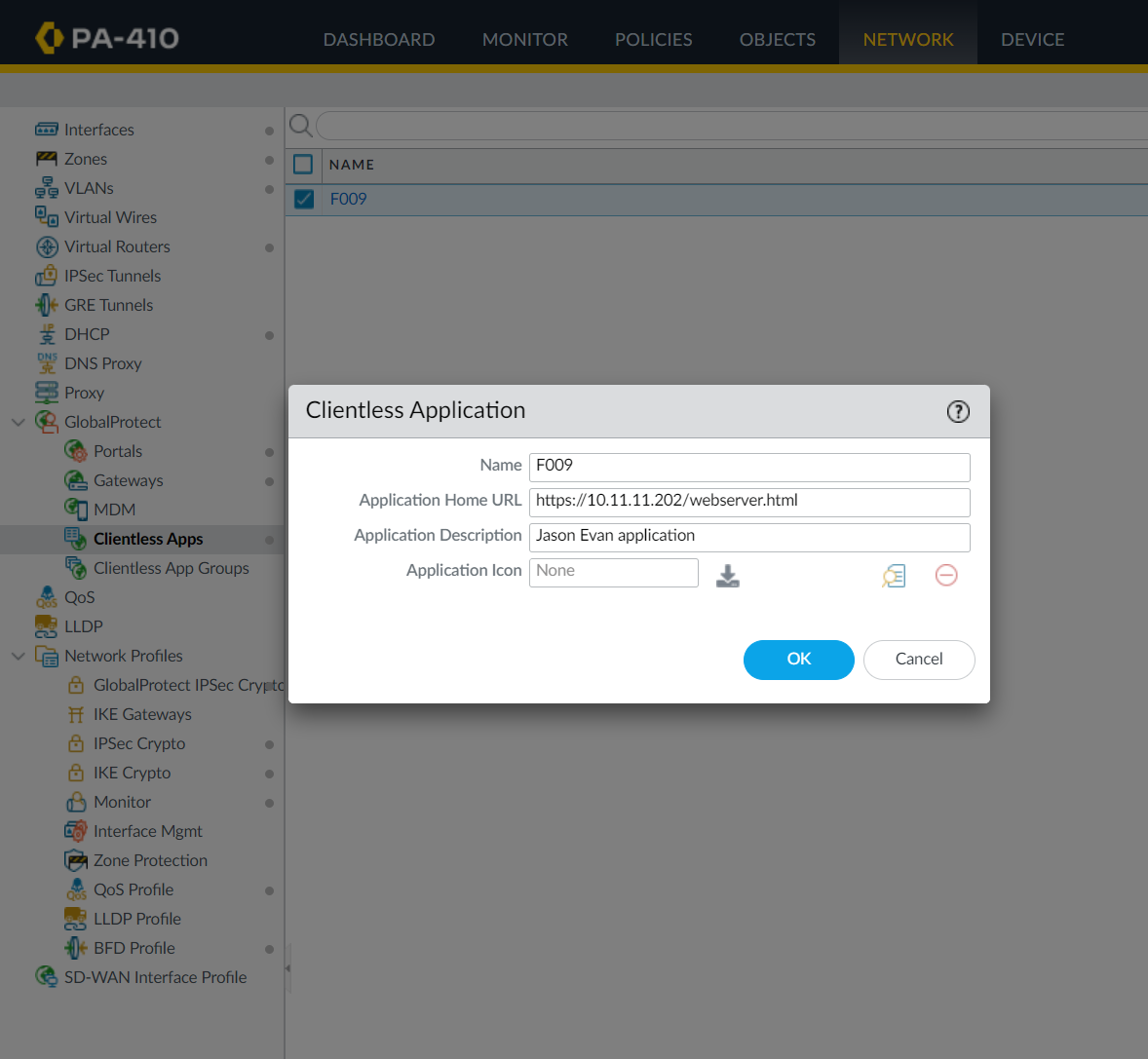
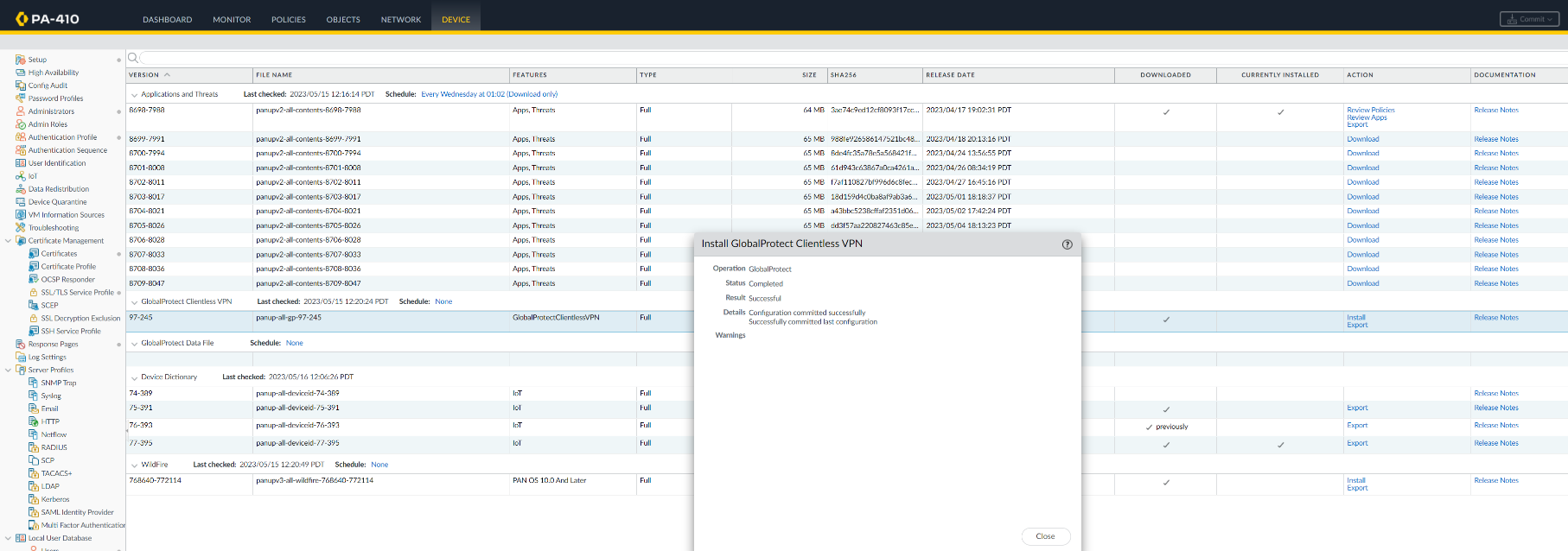
Clientless VPNs are useful when resources need to be accessed from a remote location easily and quickly and from any device. This can be helpful for those working on a public or shared computer that do not have administrative privileges to install software on their devices.

However, clientless VPNs are only able to access web-based applications and are very vulnerable to attacks. Due to its accessibility there is very little layer to security and authentication aside from credentials. They also don’t offer advanced security protocols or features such as split tunneling. Clientless VPNs also are not as secure compared to a traditional VPN since they do not offer advanced security features such as Open VPN, SSTP, or two factor authentication. Another shortcoming is its reliance on web browsers which have a lot of possible vulnerabilities due to their complexity. Clientless VPNs are also not able to provide the same amount of control and visibility as a traditional VPN client which means that potential threats are harder to detect. Ultimately, clientless VPNs are useful and powerful, but are weak in security and limited in its overall control.

**Lab Summary**

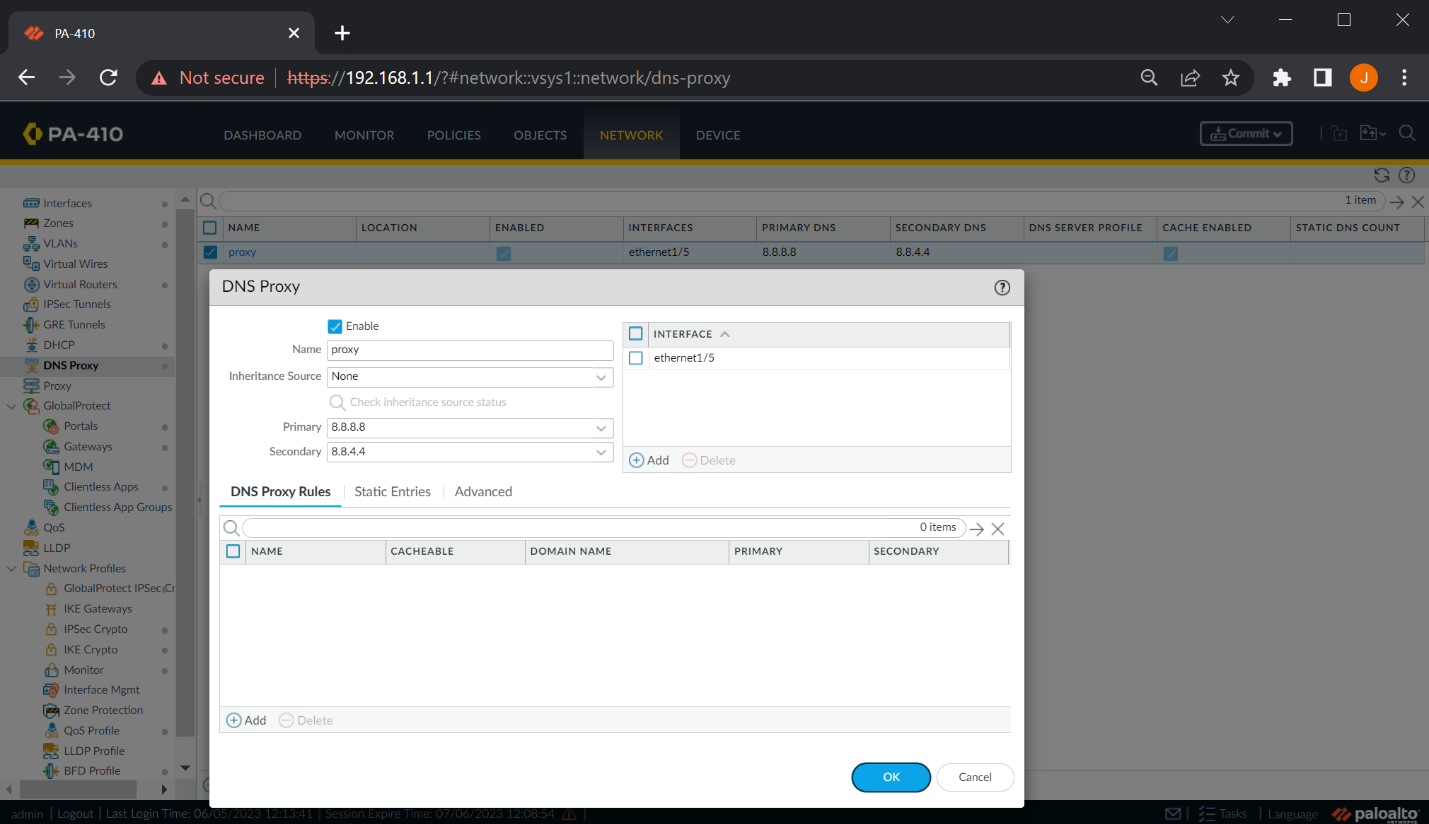
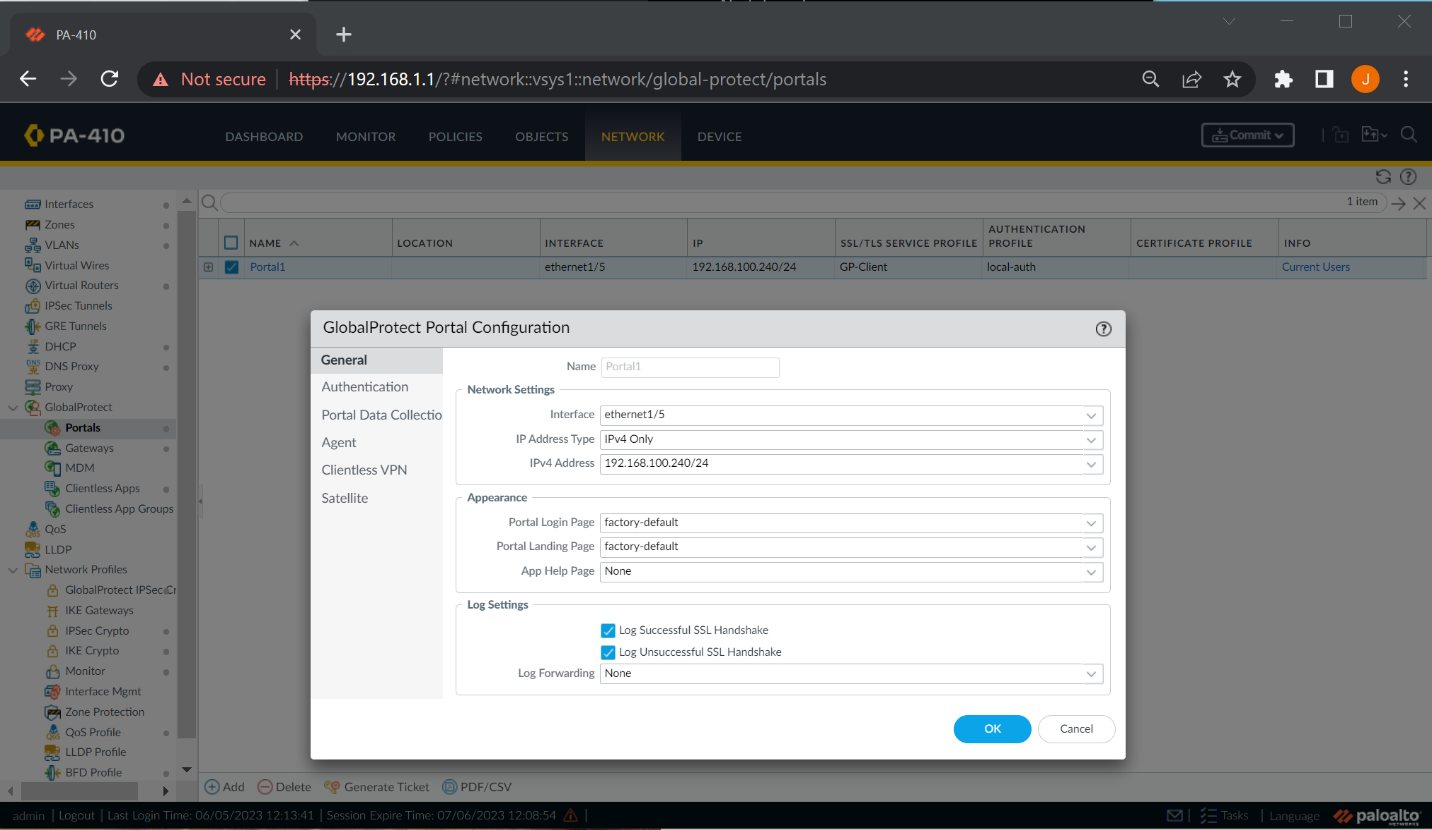
This lab is very similar to the certificates lab, with new configurations added to the GlobalProtect Gateway and Portal “clientless” configurations. Also, an internal web server was hosted on the firewall side, the “site”, to prove that resources could be accessed. We ran an Apache server using an all-in-one XMAPP server generation tool, where it allocates space in the PC’s memory to hosting a server. Since no detailed configurations were needed on the web server, the rudimentary existence of the server was all that was needed to prove the clientless VPN was established. We ran a custom made HTML website on the internal webserver. It was accessed as proof (see *Procedure*).

**Network Diagram with IPs**

**Procedure – All configurations on top of *Lab 10 – Remote Access VPN***

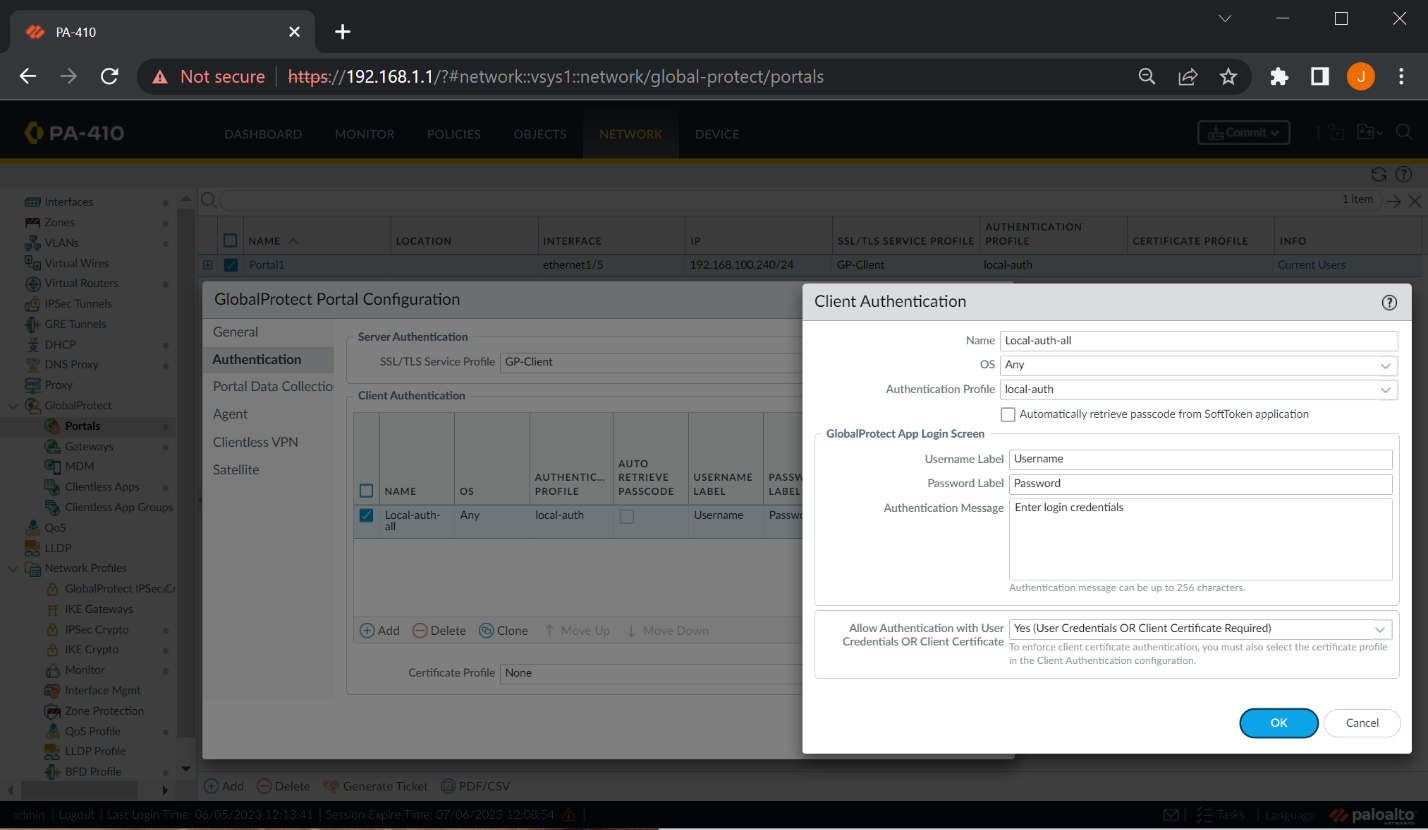
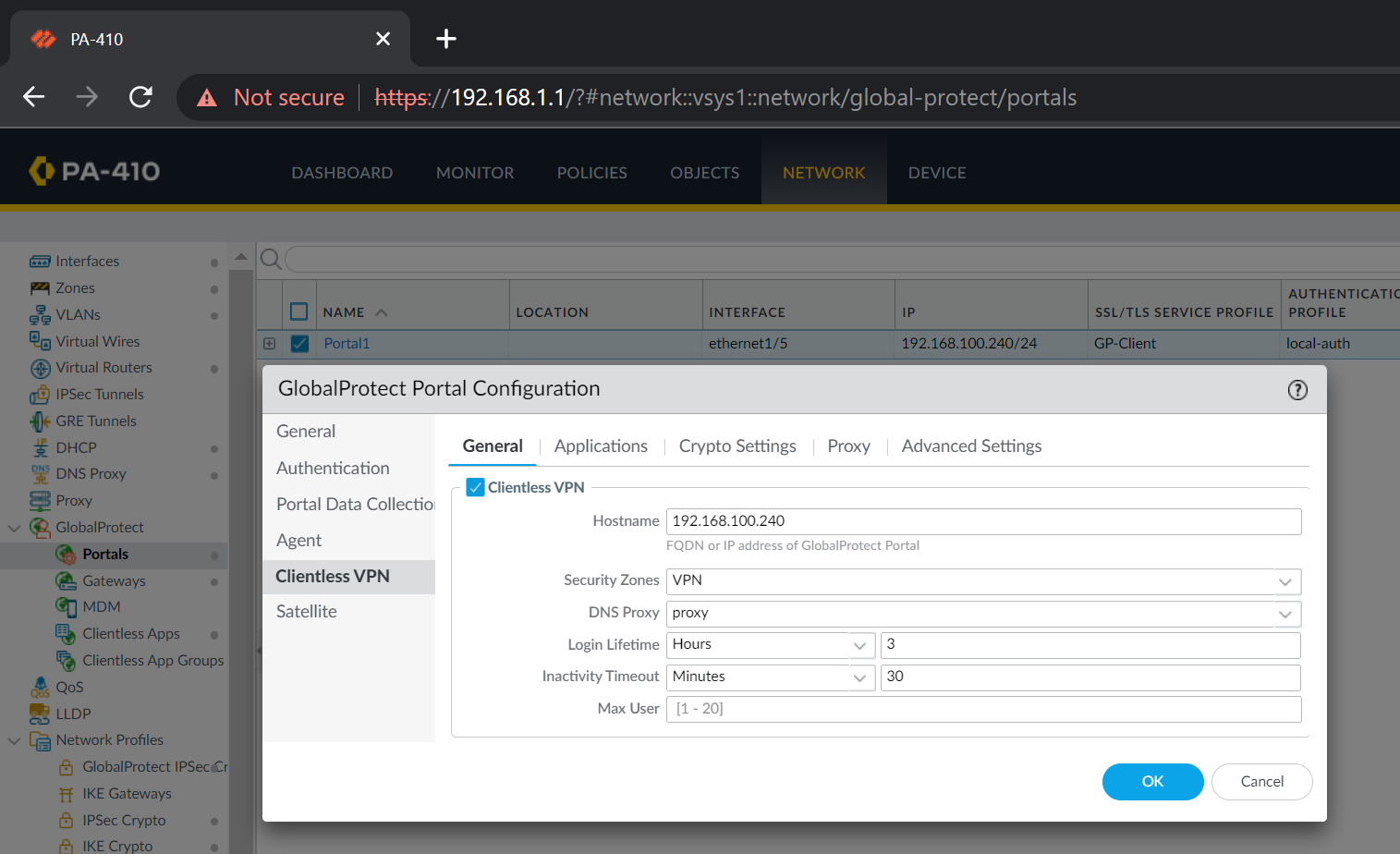
Ensure the GlobalProtect Clientless VPN Dynamic Update is up to date, downloaded, and installed.

Create a clientless app under GlobalProtect and make the address the one of the internal web server. The second part of the address is he name of the webpage or resource added (shown later).



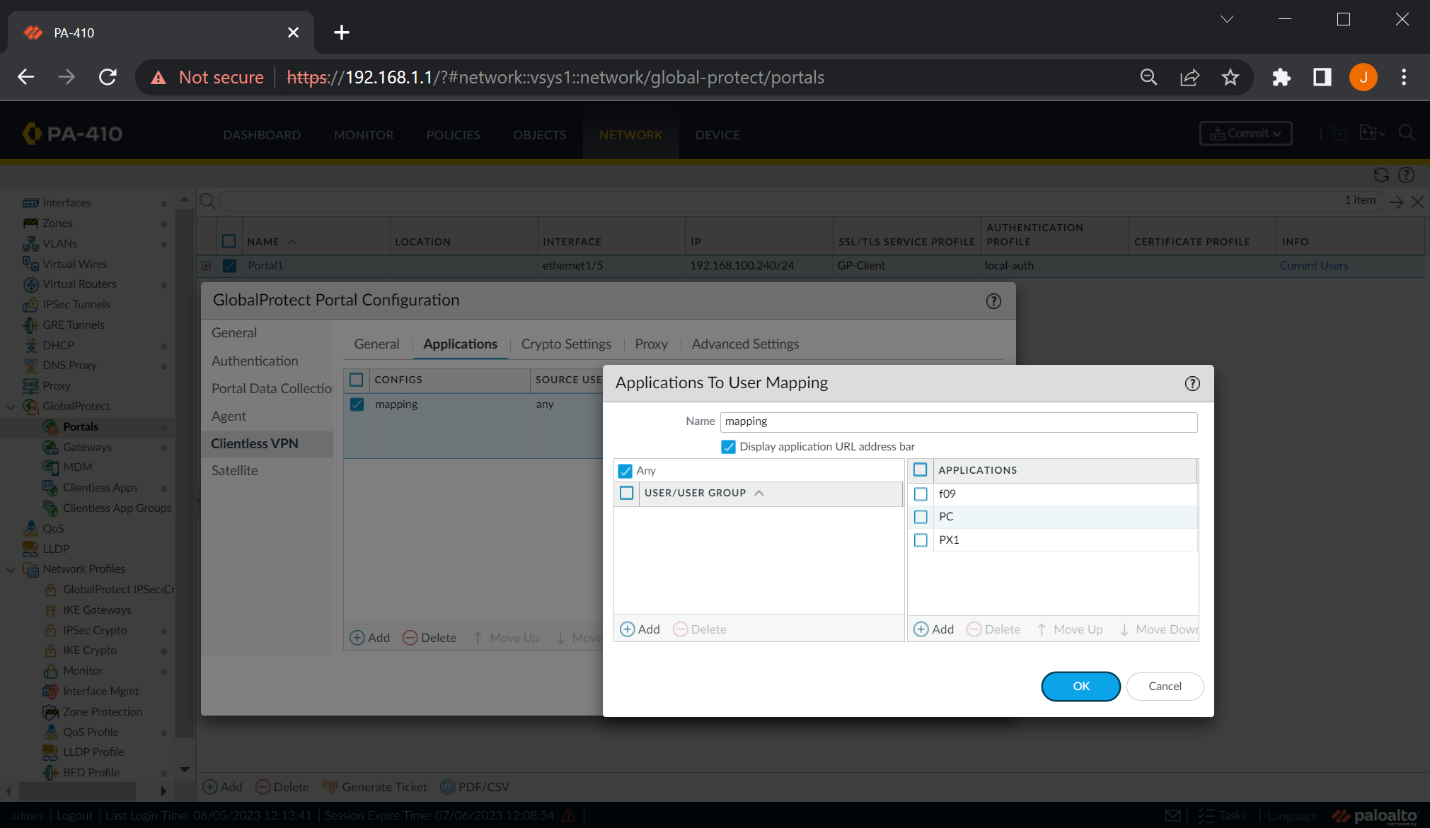
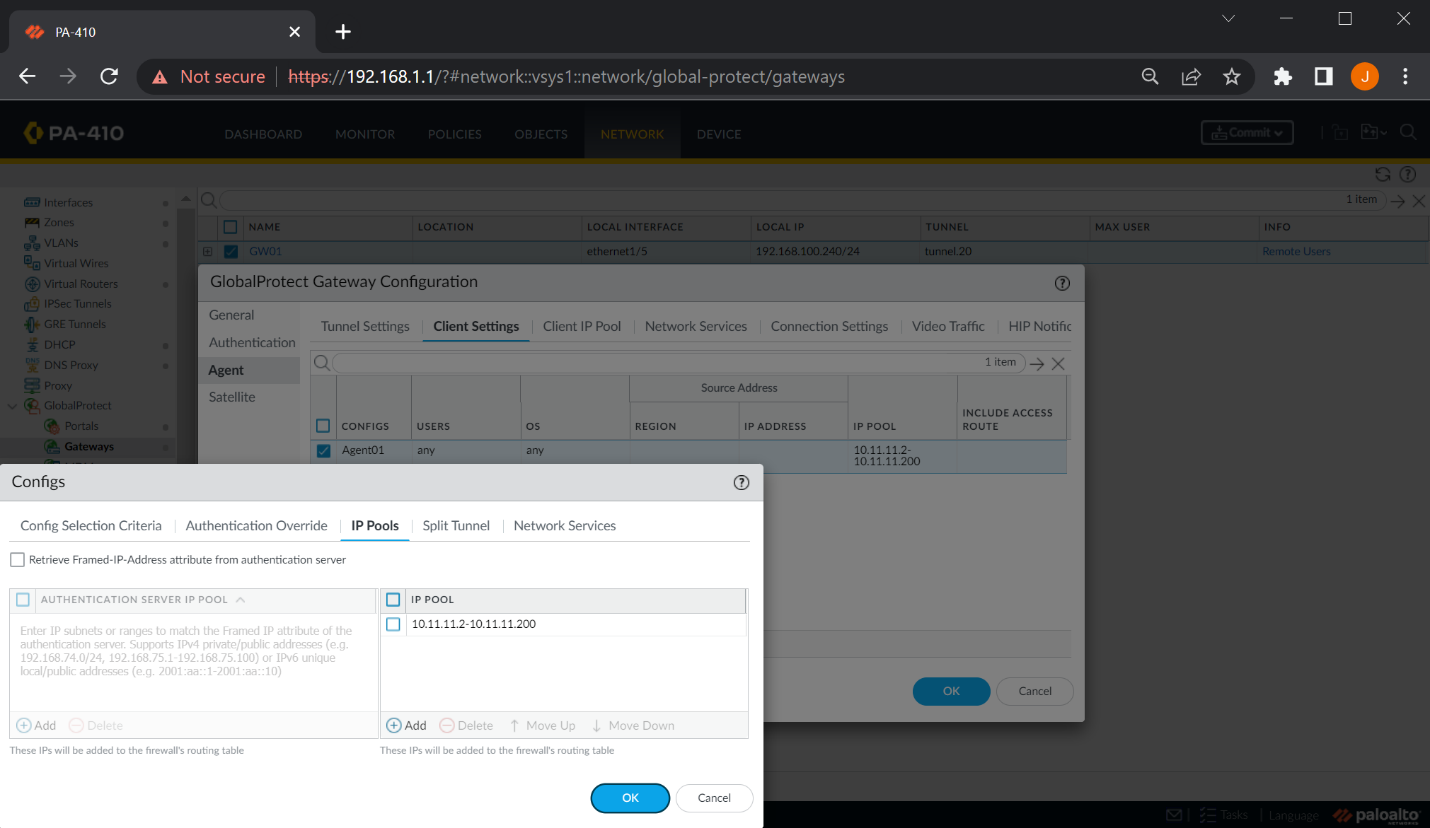
The IP address of 192.168.100.240/24 was used for the outbound interface. This statically assigned address is the main outbound interface. Remote sites point to this address.

Create a DNS proxy and point towards a DNS server for the corresponding outbound interface.



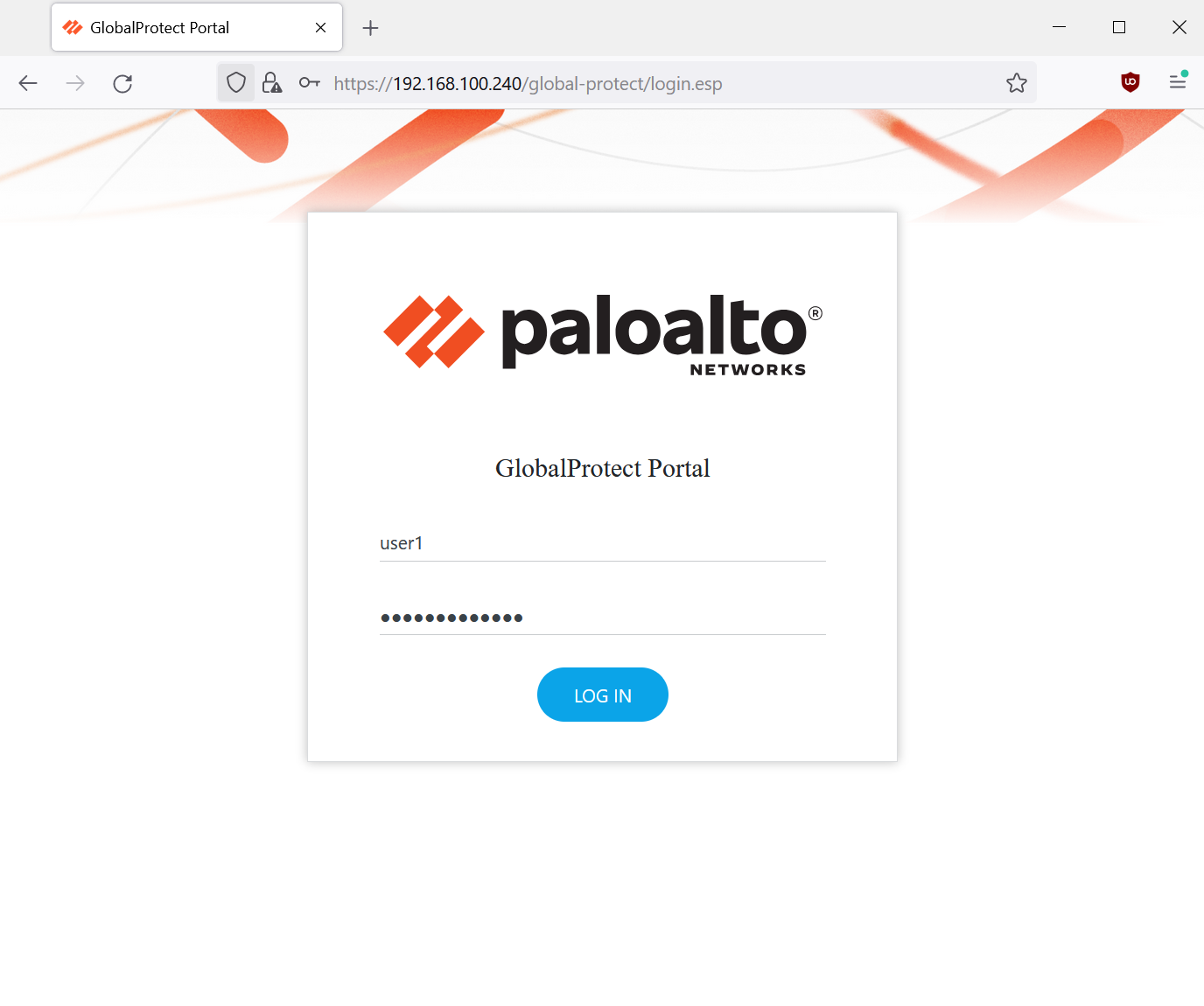
Clientless VPN configurations that use the DNS proxy and use the outbound interface address.

A reminder of the client authentication configurations. Nothing is changed.

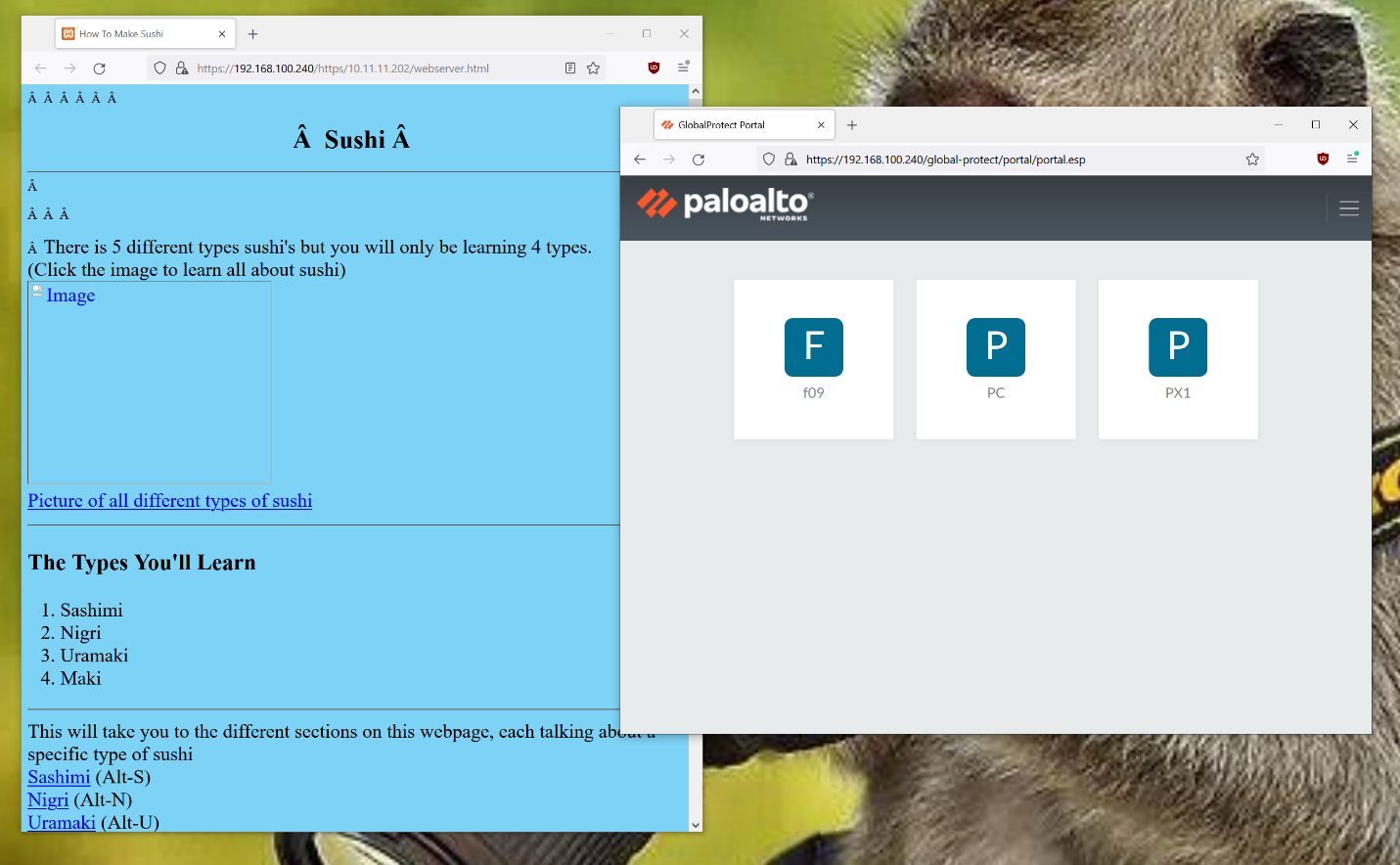
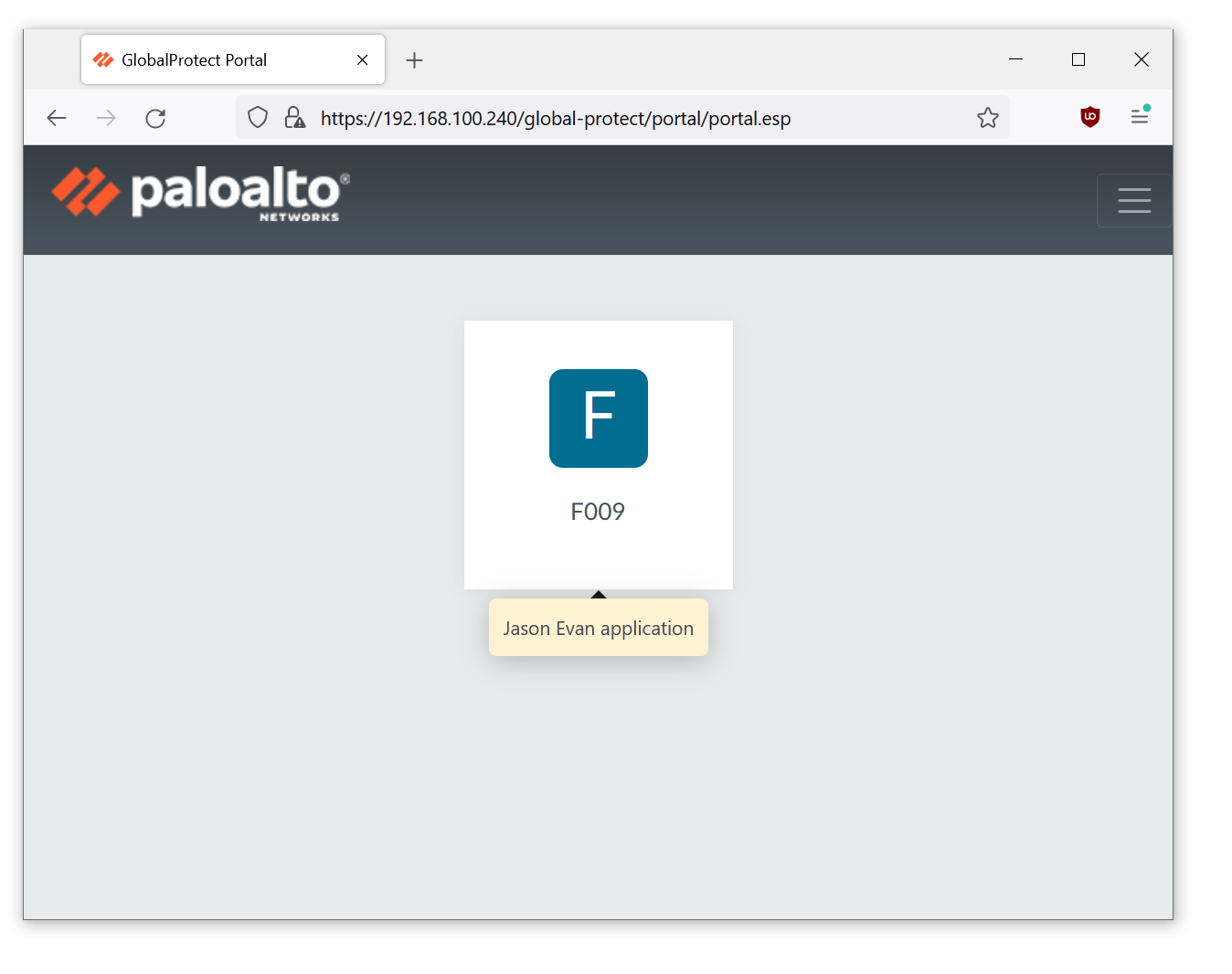


A reminder of the IP pools that give the range of assigned address the firewalls give to connected VPN clients.

Map user to application. This indicates what apps the user can use. Select any to have all users access all applications.

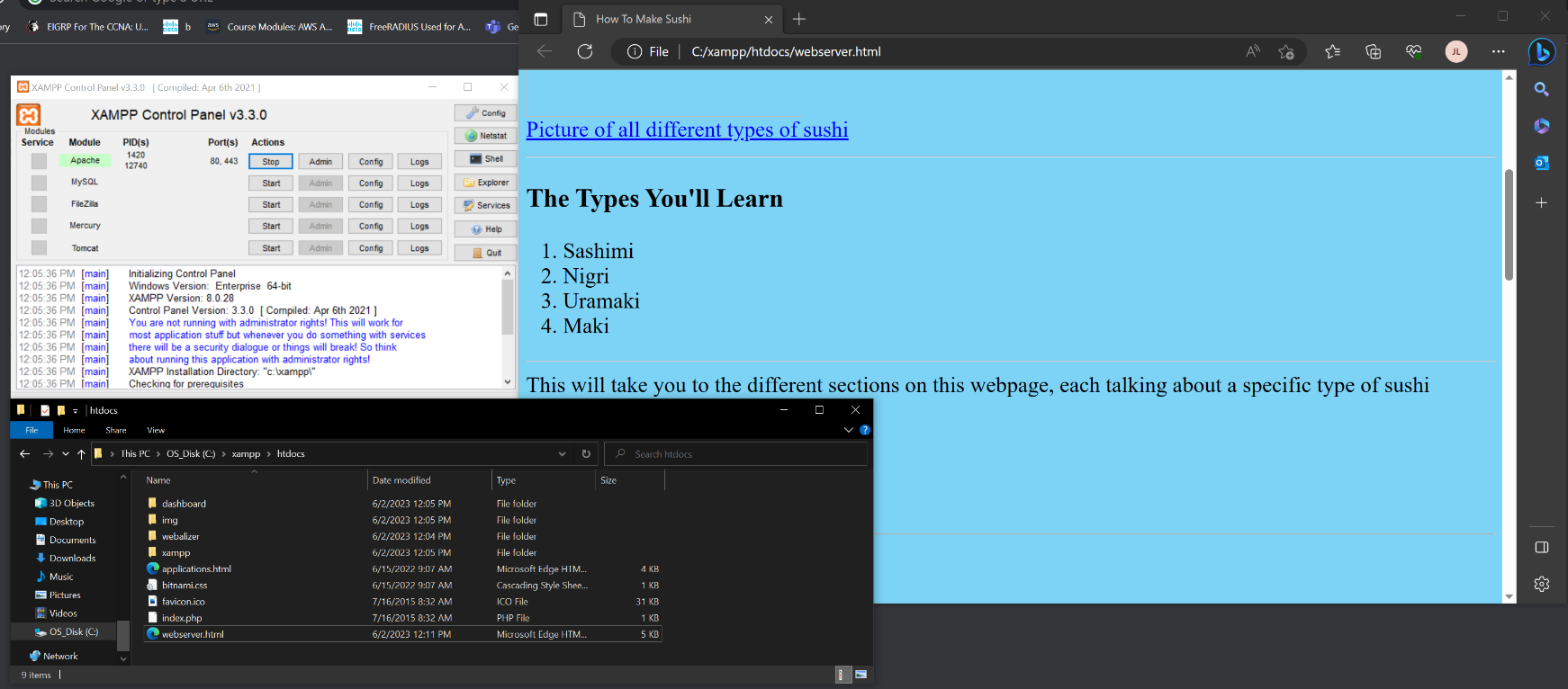


Connect to the GlobalProtect Portal. It should redirect you to a web browser portal rather than the install page for the application. This means that clientless is set up.



This was our portal. We had 3 applications in an application group to make it easy to map, as the mapping could point to the group rather than each individual app. The web server is linked to the f09 application.

The IP address of 192.168.100.240/24 was entered from a remote site. This is a sample image of what the portal looks like, and what hovering on top an application looks like as it gives the configured description.



The web server is running off Apache web server from XMAPP instead of the typical Apache lounge for windows. Upon the files, resources like HTML pages uploaded to xmapp > htdocs in the file explorer is added to the web server and accessible by remote users connected by the clientless VPN.

**Problems**

Although this lab had very similar configurations with minor edits and straightforward changes in the “clientless” tab of the GlobalProtect, the projected configurations did not work due to the similar issues mentioned in *Lab 10 – Remote Access VPN Self-Signed Certificates*. The main issue was still “how a client ported into the SOHO of the firewall allows me to connect to the internet, and then after changing IPs, changing wires, discussing troubleshooting and other elements of the lab, and then changing back to the same configurations and using the same ports, my PC’s access to the internet via the SOHO has been inhibited. After a while, not changing any scheme, it would work. Sometimes, the connection would flicker and would repetitively connect and disconnect. Using my lab partner’s computer, the connection would be consistent. Physical issues with the rack, which is pre-made to connect to the PC’s, hindered consistency with this lab. It made it hard to determine whether a configuration worked or not” (Lab 10).

The quickest way for us to deal with this issue is to use another rack with the same configurations without the same wiring. In other words, we used a different computer that plugged into a different firewall with the same configurations. The internal webserver we accessed was still from the same host computer, the one computer that is still physically consistent. Doing this, our issues relating to hosting an internal web server, directing to the right address, including the proper addressing Domain Name, and more, were resolved with this transition.

**Conclusion**

Being similar to the previous remote access lab in functionality and purpose, using the same configuration, setup, and knowing what problems we may encounter greatly aided in reducing the chances of errors. Isolating the configuration’s changes helped us narrow the focus of the clientless portion of GlobalProtect, and it became much easier to recognize what change caused which issue, and thus this lab was able to move smoothly and quickly.