Palo Alto PA-220 Global Protect VPN Lab

Andrew Pai

Period 5 Cybersecurity

Purpose:

The purpose of this lab was to configure the Global Protect VPN on our Palo Alto PA-220 firewall. This will allow desktops to remotely connect with other desktops that are on a different network.

Background Information:

This lab focuses on implementing the Global Protect VPN on our Palo Alto PA-220 firewall. VPNs, or Virtual Private Networks, are a way for Internet users to act as if they were connected to their own private network while accessing the Internet. This allows users to stay anonymous and keep their otherwise public data protected and private. Common uses of VPNs by the average person may include things like avoiding Internet censorship, protection of data, or accessing resources only available on networks in a different location. For corporations, VPNs can play a large role in allowing employees to access their business' network from a different area, letting them work remotely.

The main reason that people use VPNs is to protect their Internet traffic. Most of the time when people access the Internet, much or all of their data is public and unencrypted. Connections to the user's Internet Service Provider from their device leave much of their information vulnerable to either being logged by the ISP or being taken by malicious activity. As such, people use VPNs to avoid these data logs and attacks.

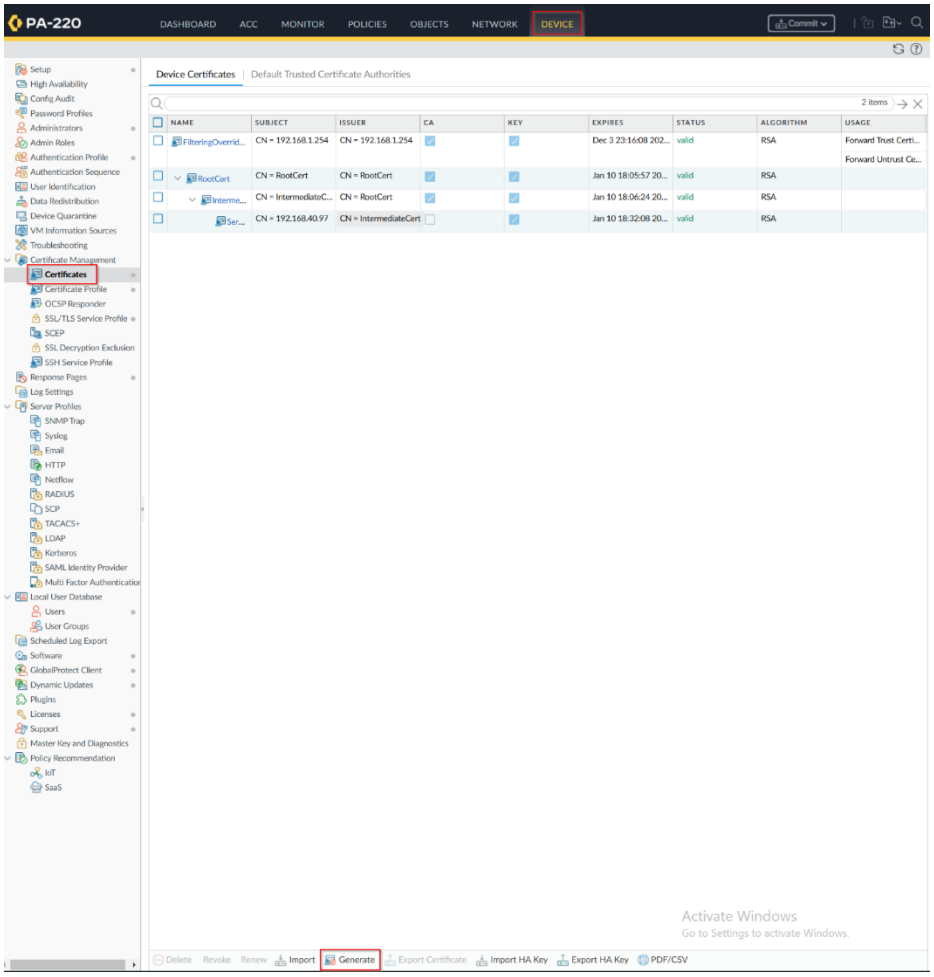
VPNs work through creating a tunnel between the user and the ISP so that user traffic isn't as unprotected as it was before. In creating this tunnel, there are three main components: the VPN client, VPN server, and the Internet itself. As compared to normal Internet usage, which would be the client and Internet, there's a VPN server inserted between the two that's in charge of decrypting and encrypting data so that it's protected. This happens by the VPN client connecting to the VPN server, which authenticates that the client actually has the credentials and authority to access the server. Once this tunnel is established between your VPN client and server, data passed between the client and server is encrypted and hidden from the ISP when it's sent out to the Internet.

The VPN that we're going to be using in this lab is the Global Protect VPN, which is Palo Alto's VPN. Global Protect is mainly unique compared to some other common VPN's because it can work in conjunction with the Palo Alto

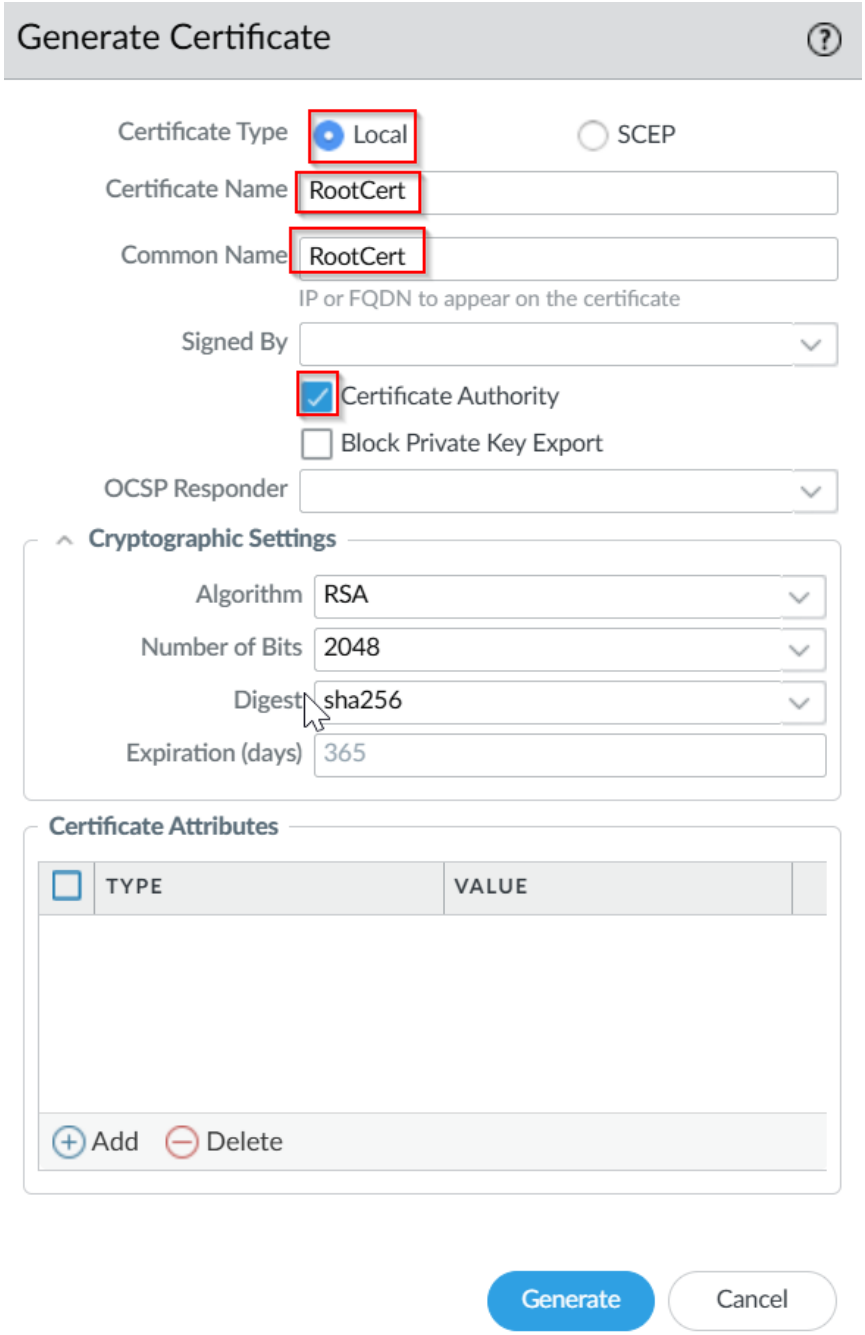
PA-220's firewall policies, allowing for users to reap the benefits of both a VPN and a firewall. However, it's also a flexible VPN to use for both mobile and desktop environments and can also check on the security and antivirus software that a device has before letting it enter the network. For this lab, we'll be using Global Protect to have one of our desktops connect to our network remotely to showcase a common situation where employees may have to work from home.

Lab Summary:

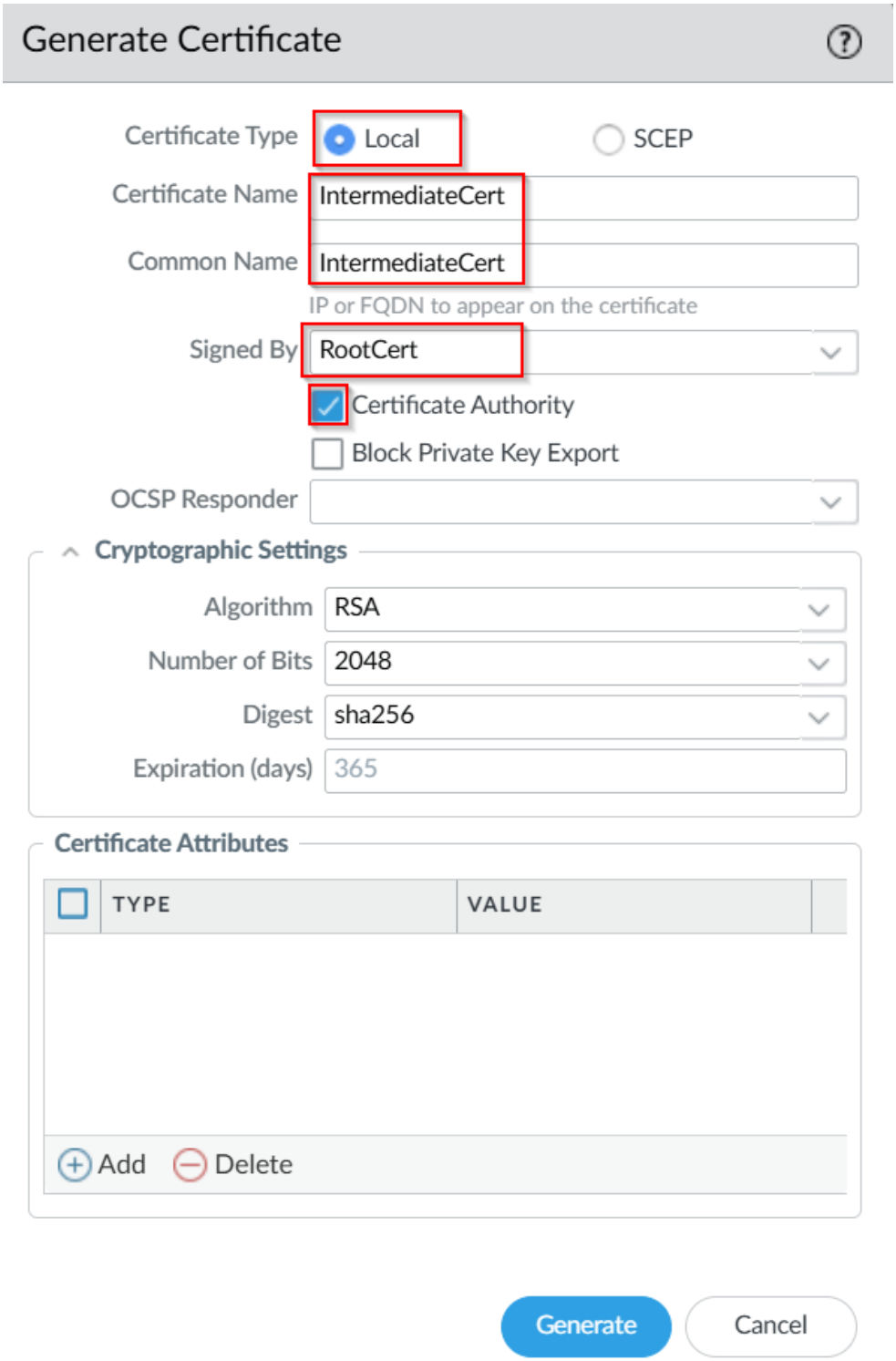
The first step of configuring Global Protect is to configure the PA-220 and end device certificates. In the firewall GUI, navigate to "Device" on the top taskbar and then "Certificate Management" and "Certificates" on the left. Click "Generate" on the very bottom of the screen.



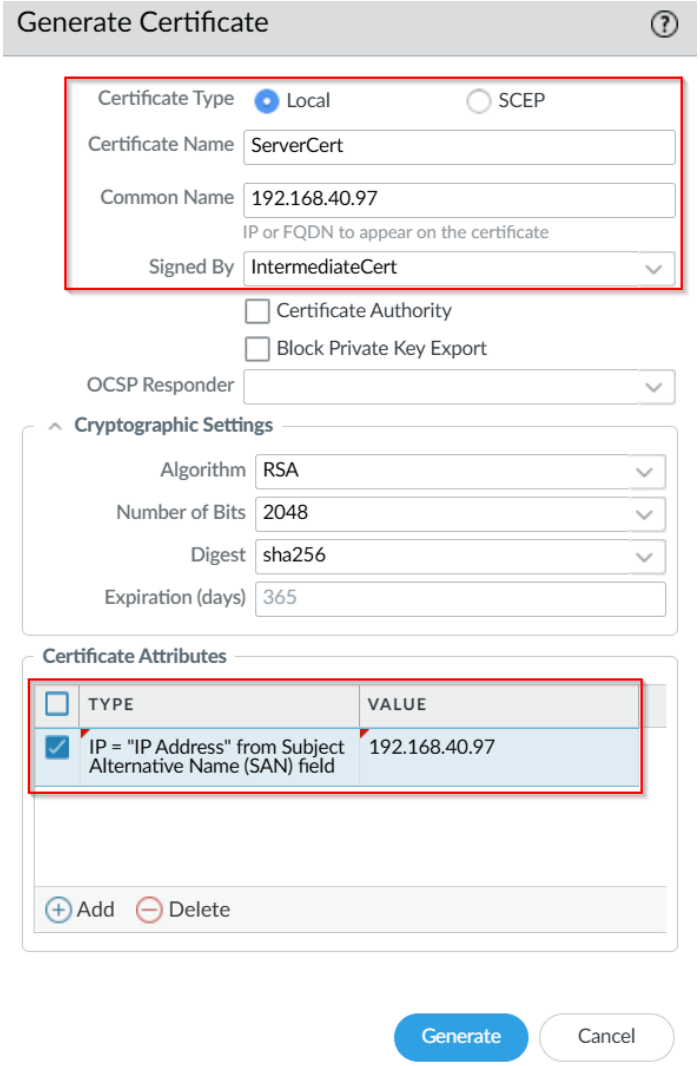
Configure a Local Certificate for your Root Certificate, naming it something like “RootCert.” Ensure that Certificate Authority is checked off. This certificate will not be signed off by any other.



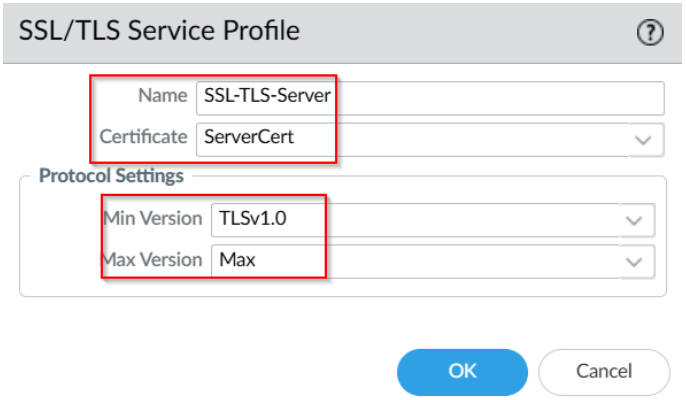
Generate a new certificate, this one called “IntermediateCert.” This certificate will be Local as well, but will be signed off by the “RootCert” certificate we just made.



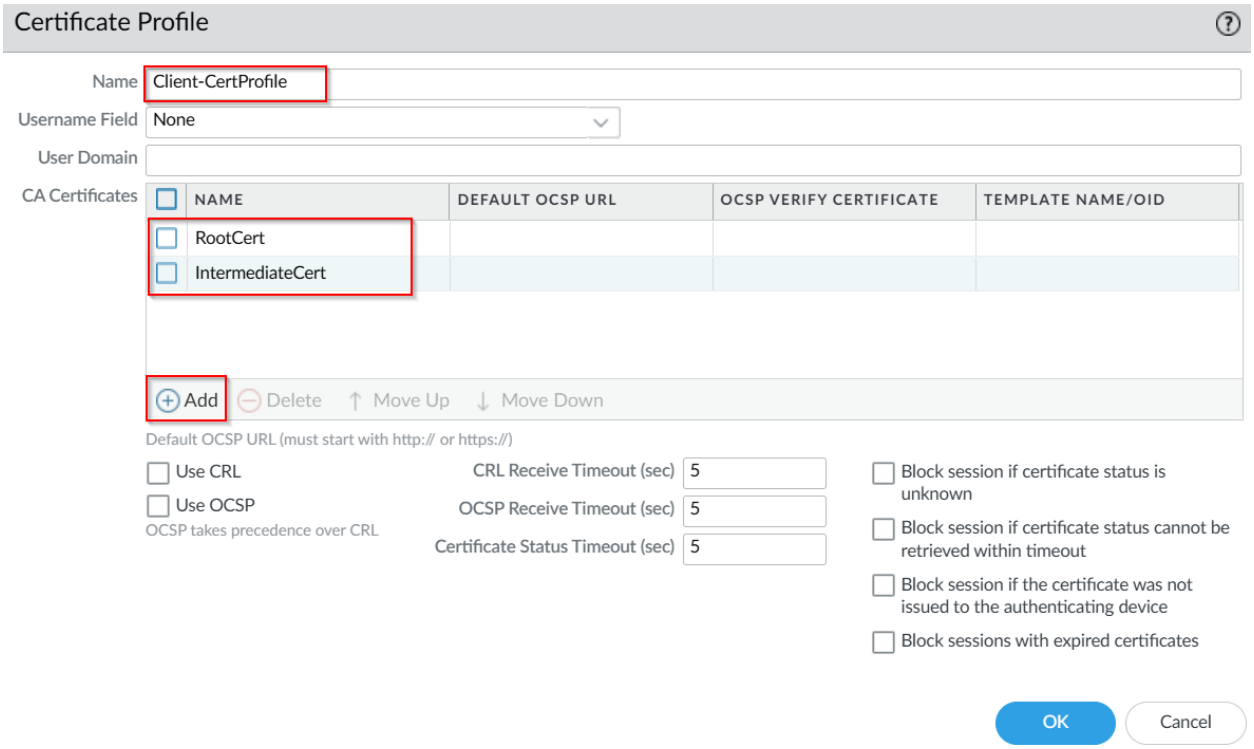
Finally, create another certificate named "ServerCert," which is signed off by the "IntermediateCert" just made. This certificate's Common Name should be the IP of your Global Protect Portal. Once generated, export all 3 certificates.



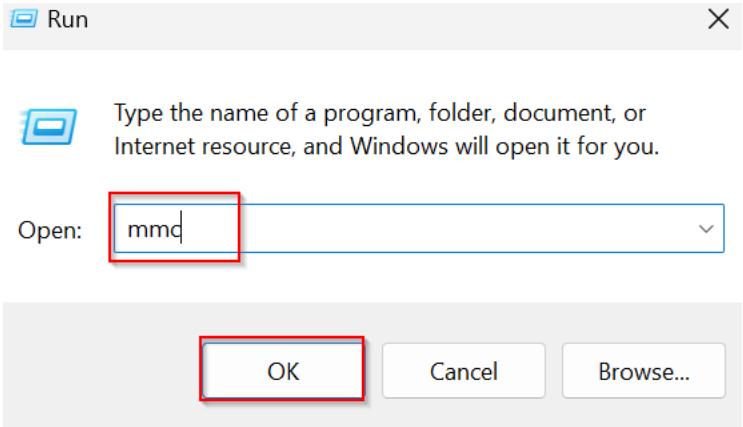
In the GUI, stay in "Device" on the top bar, but navigate to "SSL/TLS Device Profile" and click "Add." Name it "SSL-TLS-Server," and use ServerCert as the Certificate. Put Min Version as TLSv1.0, and Max Version as Max.



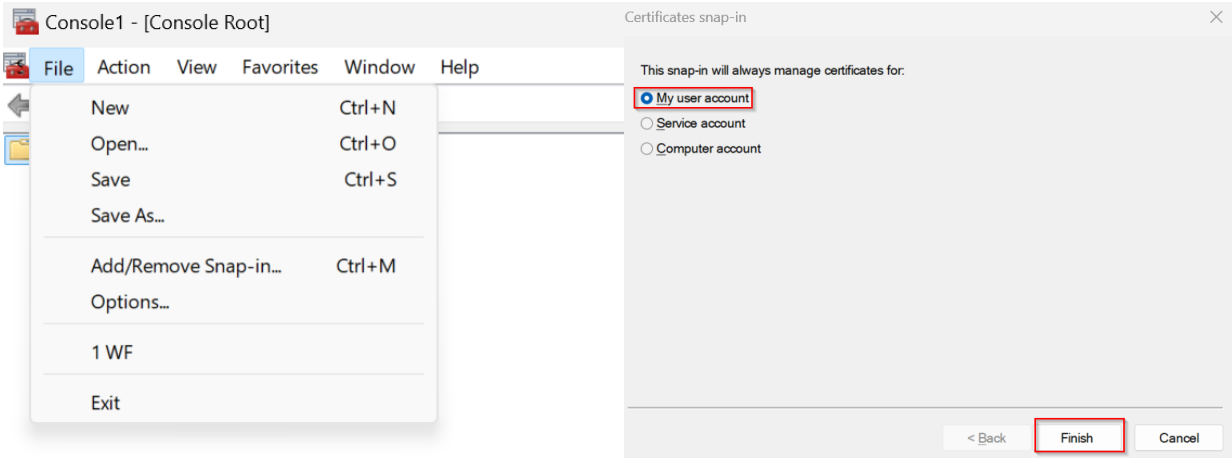
Navigate to “Certificate Management” and then “Certificate Profile” on the GUI’s left taskbar and click “Add.” Choose an appropriate profile name like “Client-CertProfile,” and click “Add” and choose both RootCert and IntermediateCert to add.



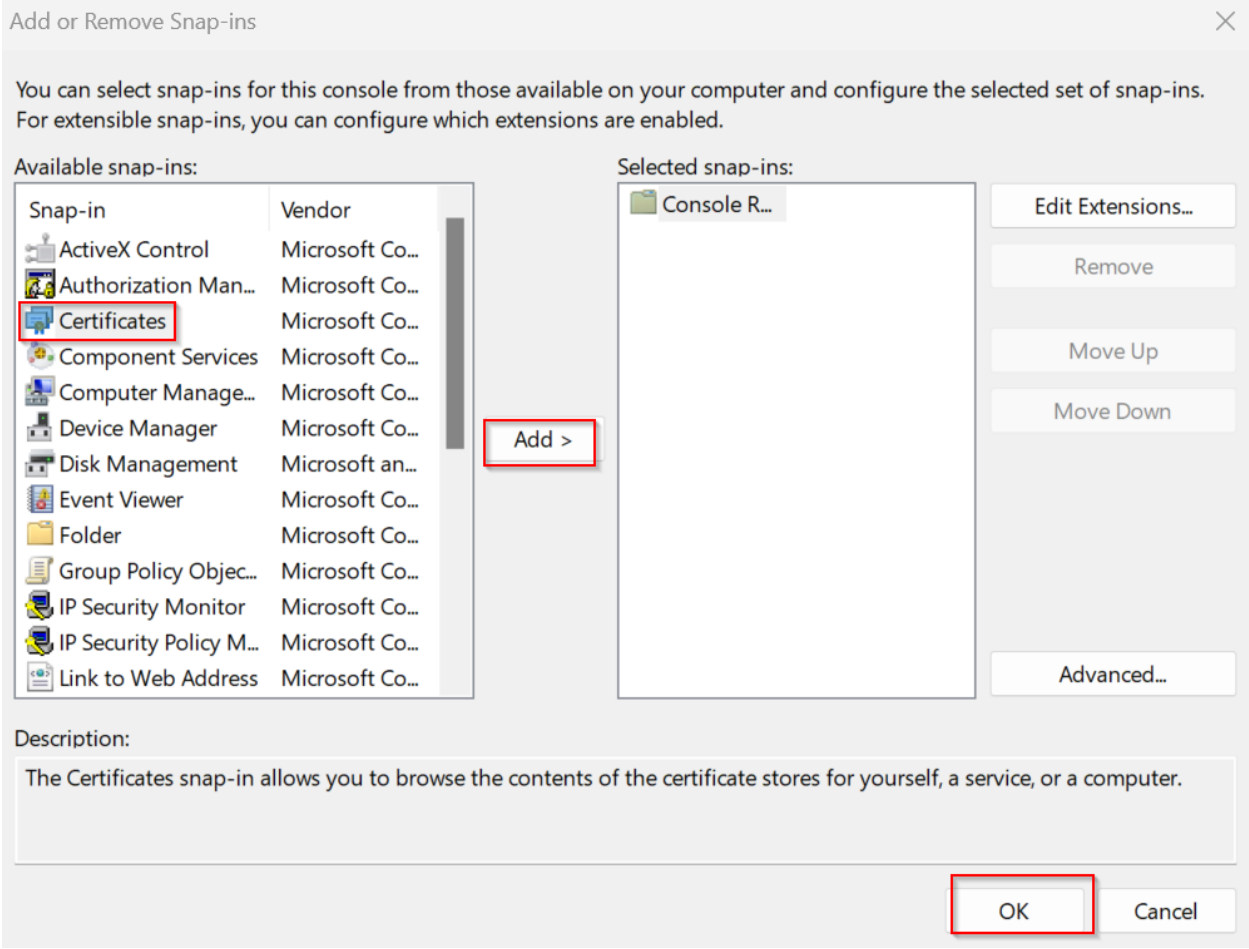
Now that we have the certificates, we’ll add them to your device. Using the key commands WIN+R, type “mmc” into the Run Dialog window that pops up.



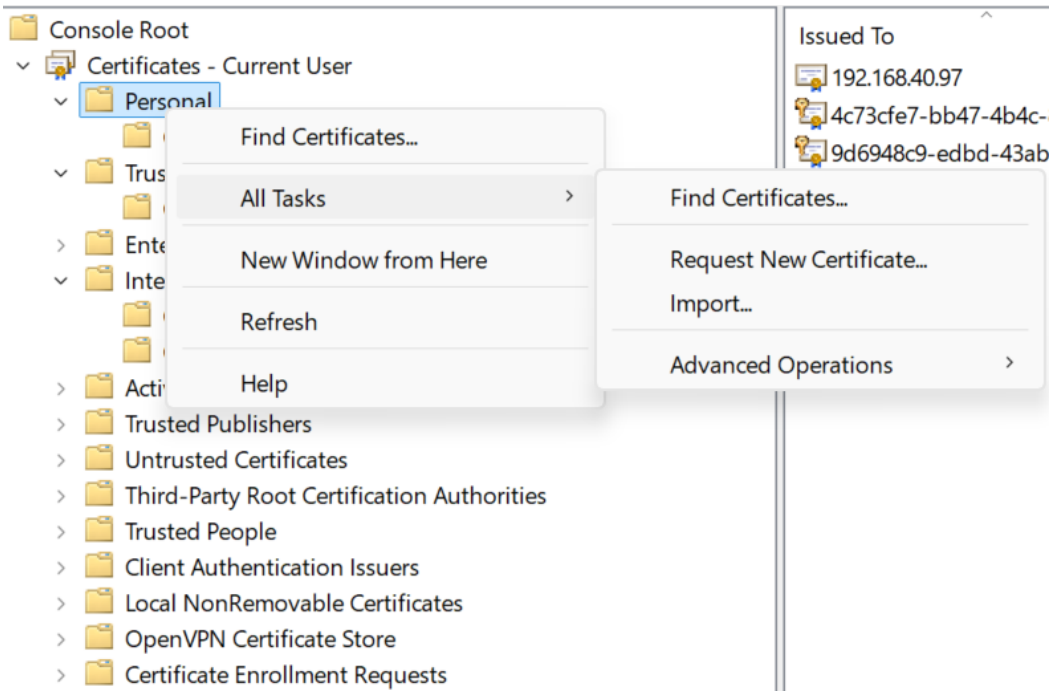
In the Console Root, click “File” on the top left and then “Add/Remove Snap-in.” Choose “My user account” if prompted to choose between user, service, and computer account.



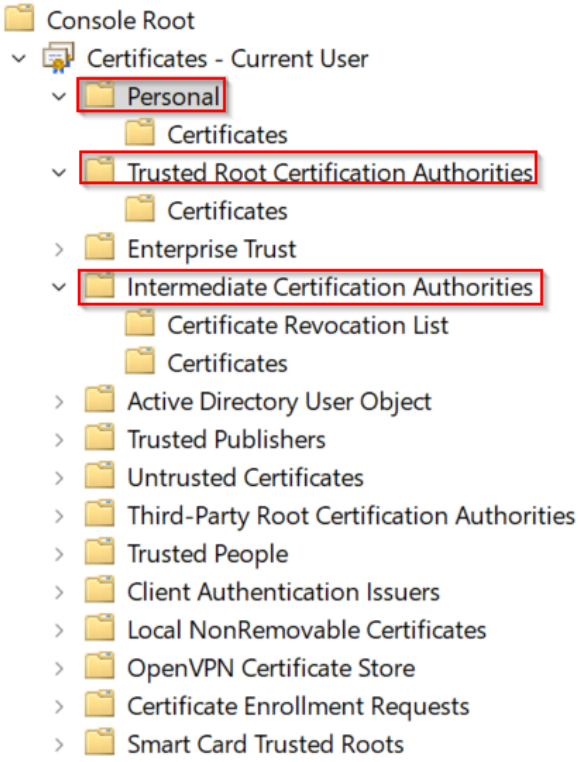
Select “Certificates,” “Add,” and then “Ok.”



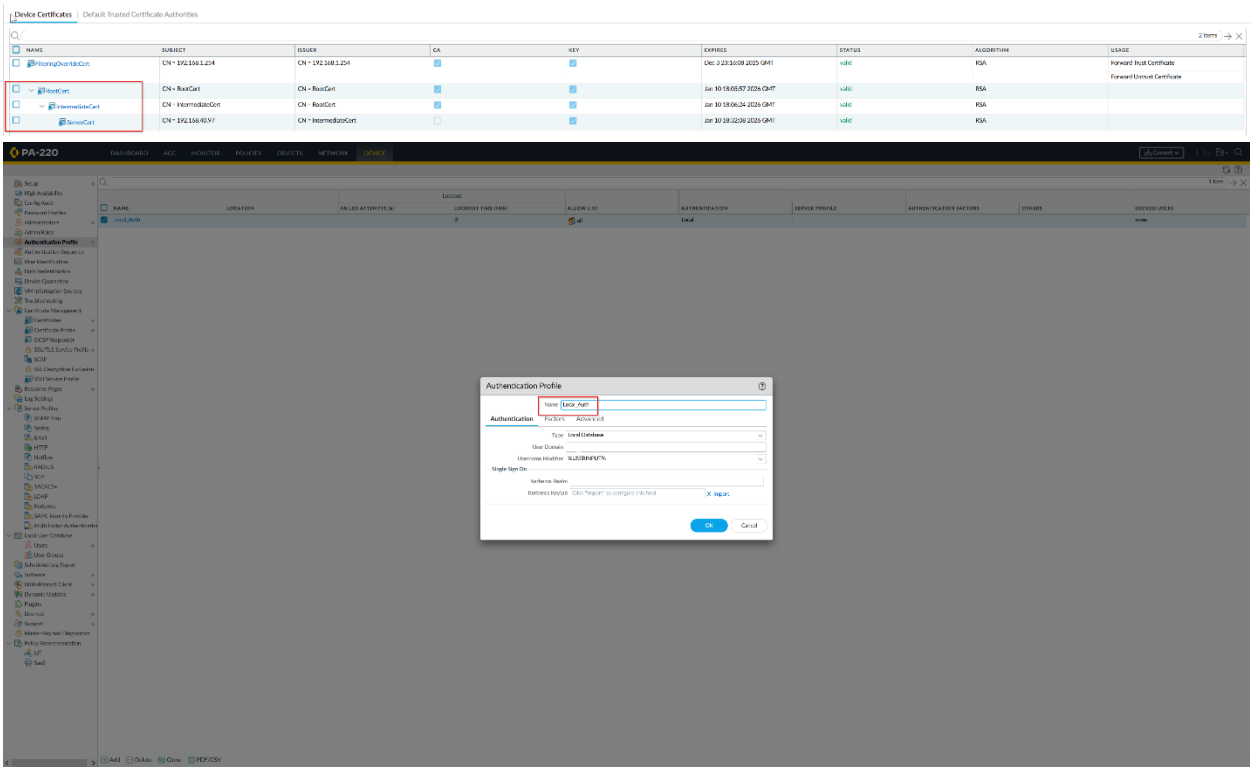
Navigate to “Console Root,” “Certificates – Current User,” and then “Personal.” Right click this “Personal” folder and then click on “All Tasks” and “Import.” Select the ServerCert to be imported to this folder.



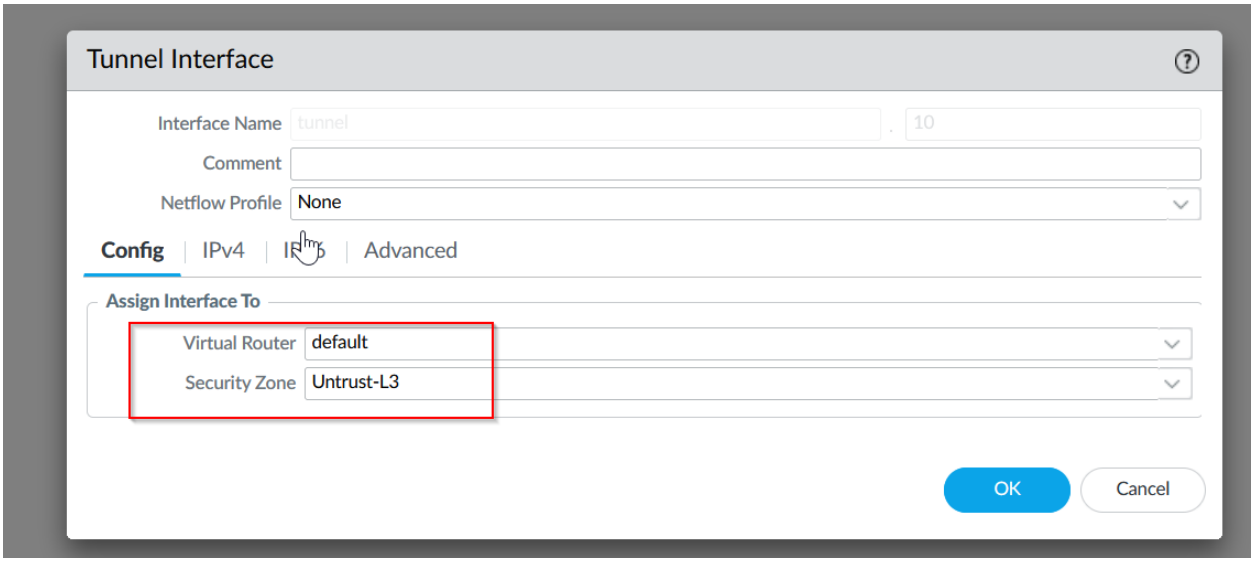
Follow the previous steps to import the Root Certificate into "Trusted Root Certification" and the Intermediate Certificate to "Trusted Intermediate Certification Authorities."



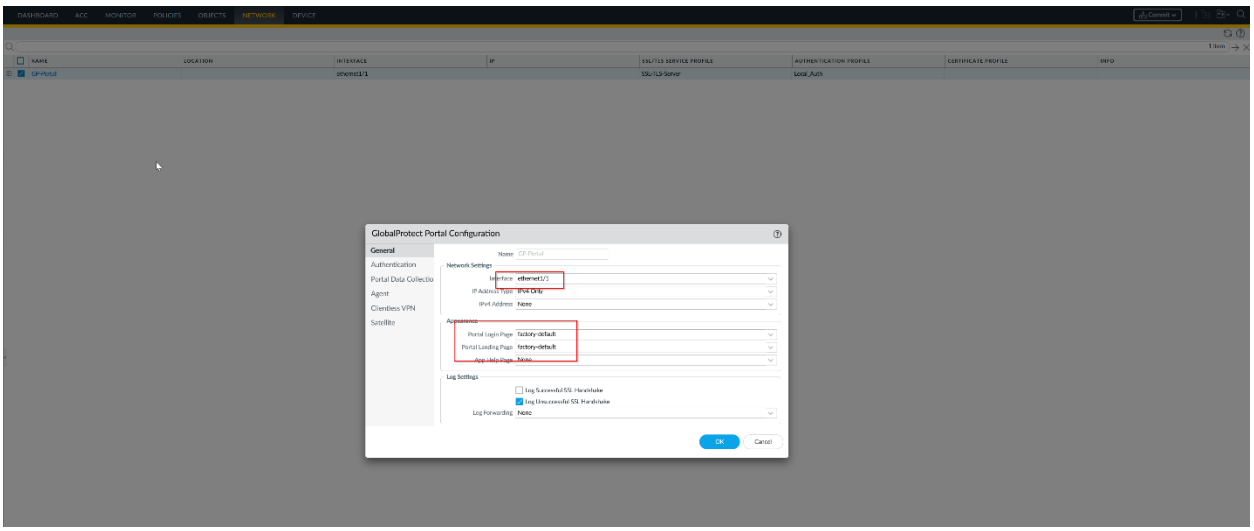
Return to the firewall GUI. Navigate back to “Device” on the top taskbar and then “Authentication Profile” on the left, and “Add.” Type should be Local Database, and you should name it something like “Local_Auth.”

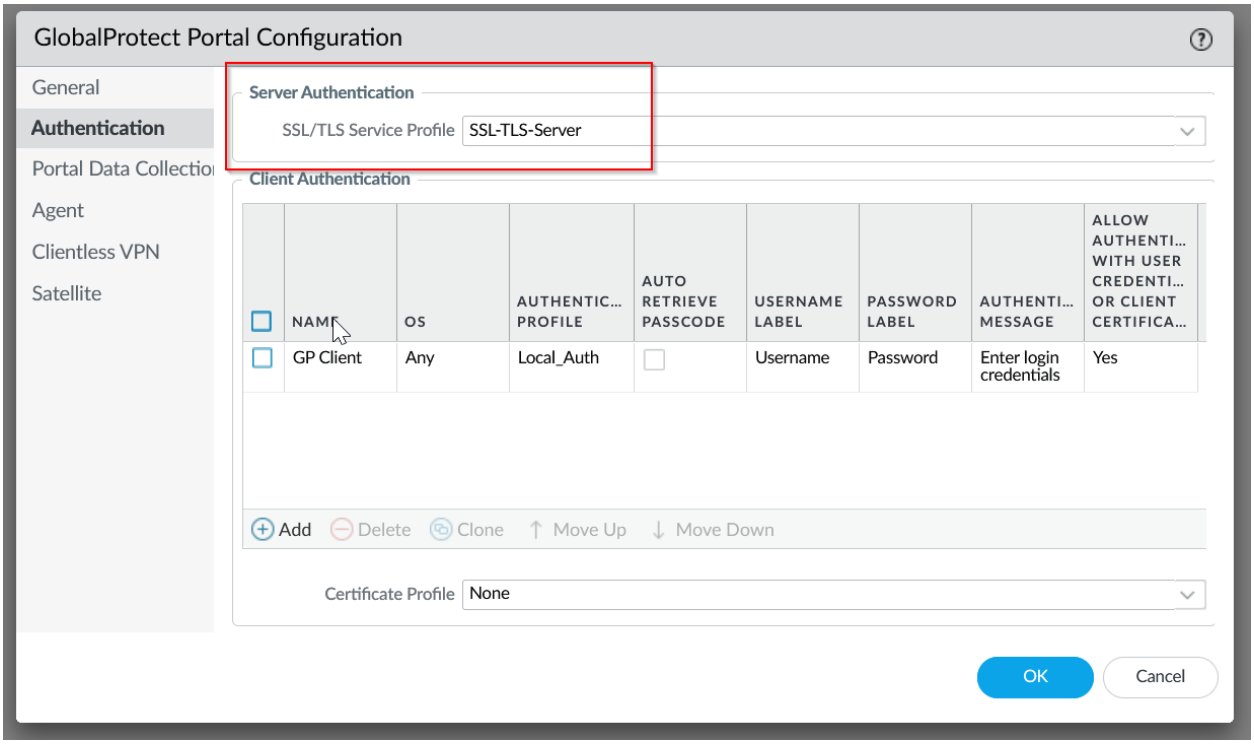


Navigate to “Network” on the GUI’s top taskbar, and then “Interfaces” and “Tunnel” on the left. Add a new interface. The Security Zone is “Untrust-L3,” or whatever outward security zone is on your firewall.

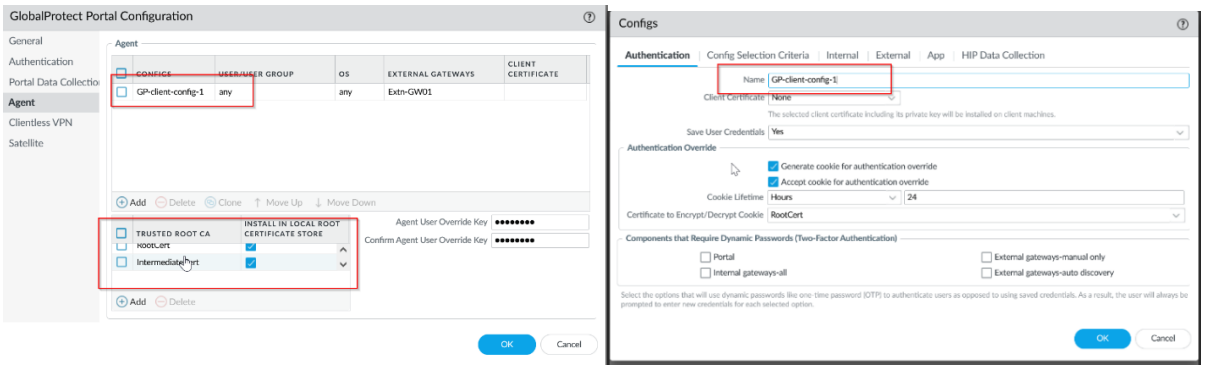


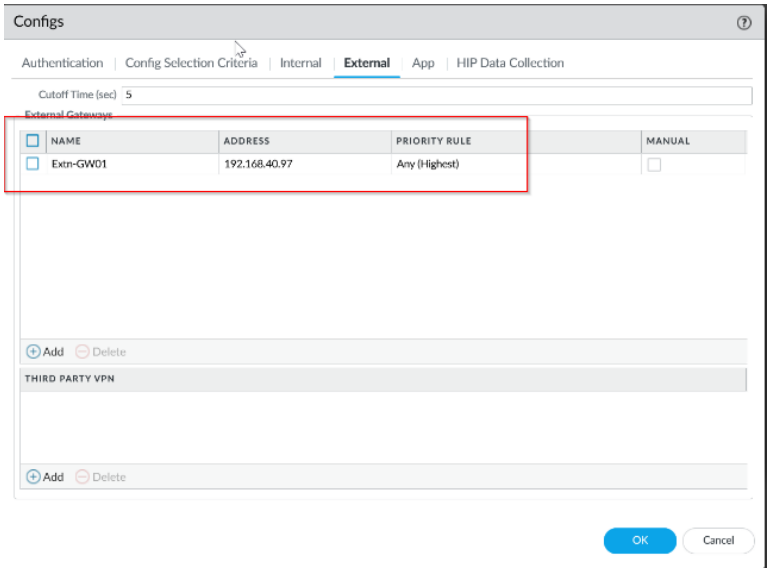
Navigate to “GlobalProtect” and “Portals” on the left and add a new one. The interface for this portal should be the outward interface on your firewall. Once done with the name and interface, click on “Authentication” and make sure the Service Profile is set to “SSL-TLS-Server.” OS is Any, and Auth Profile is Local_Auth.



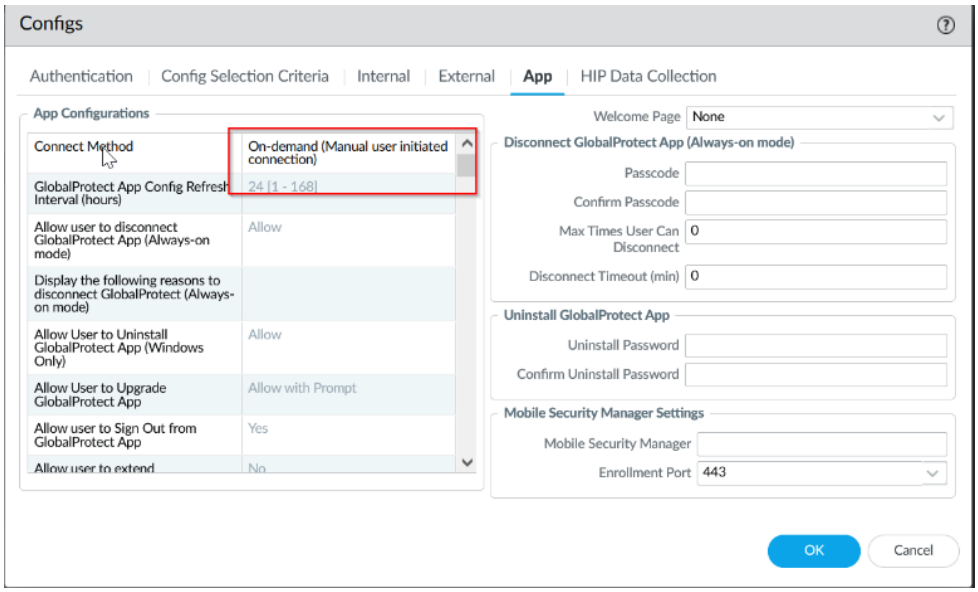


Once finished with the Authentication tab, navigate to “Agent.” Create a name, navigate to “External” and add a gateway with the ServerCert’s Common Name as the IP.

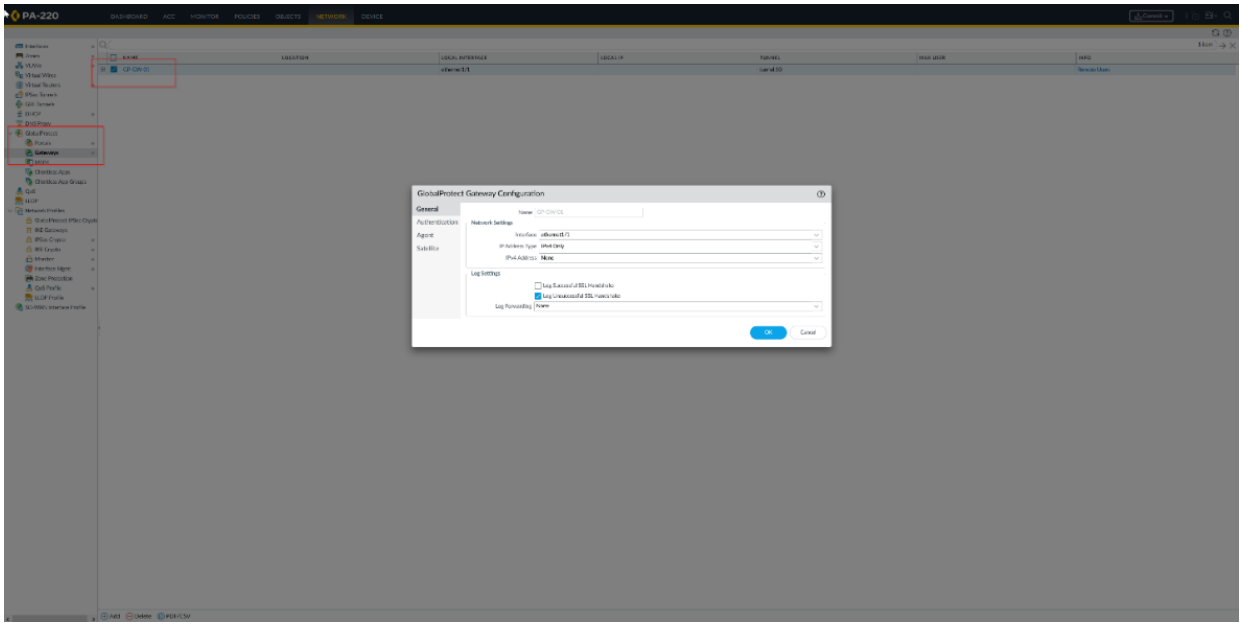




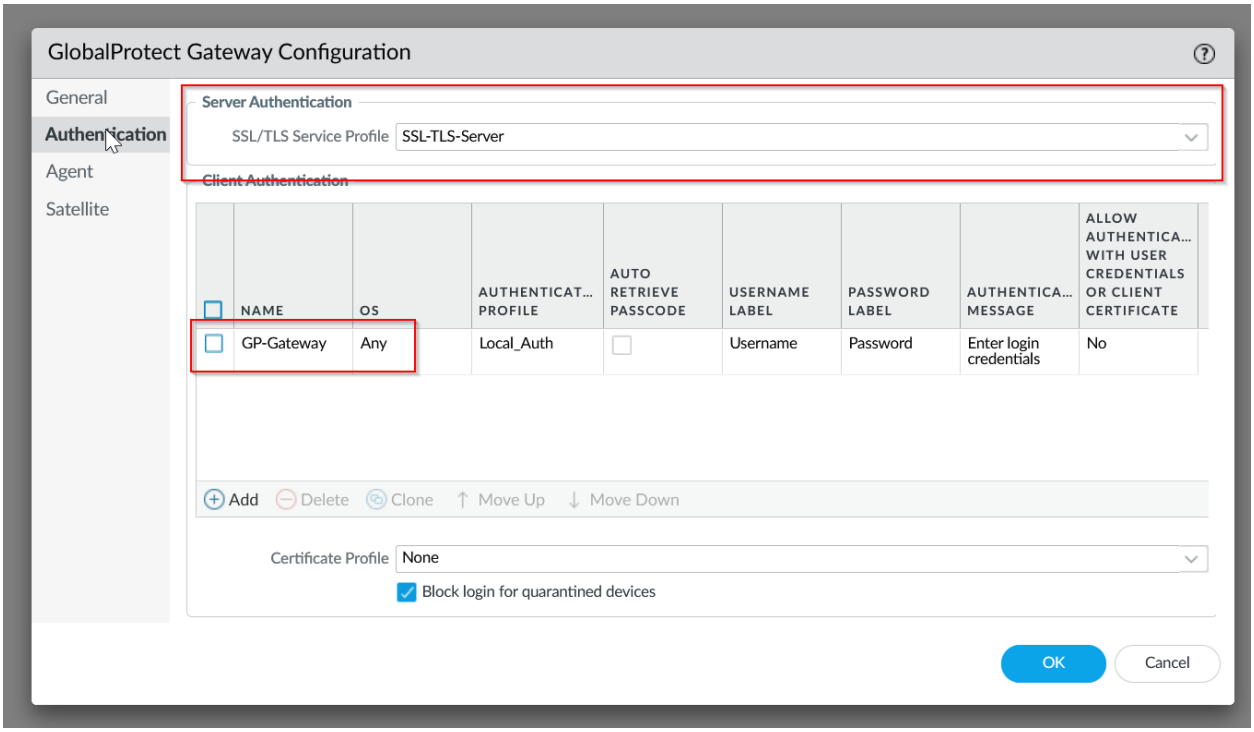
Navigate to “App” and make sure the Connect Method is On demand.



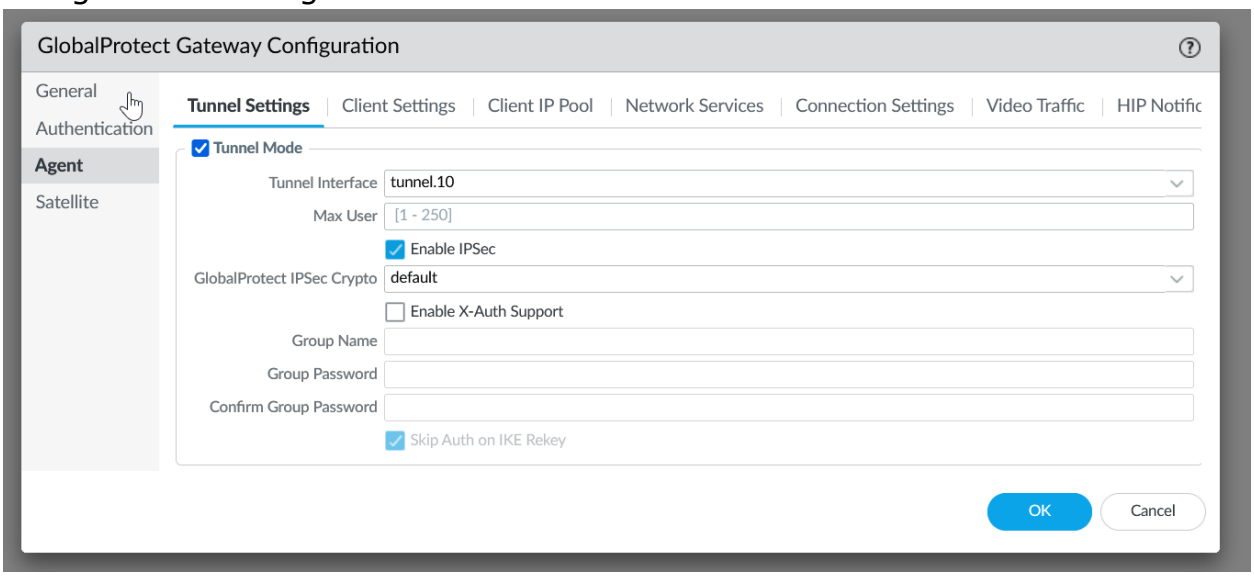
Navigate back to “Network” under the top taskbar of the GUI, and then “GlobalProtect” “Gateways” on the left. Name the gateway and use the same interface as before.



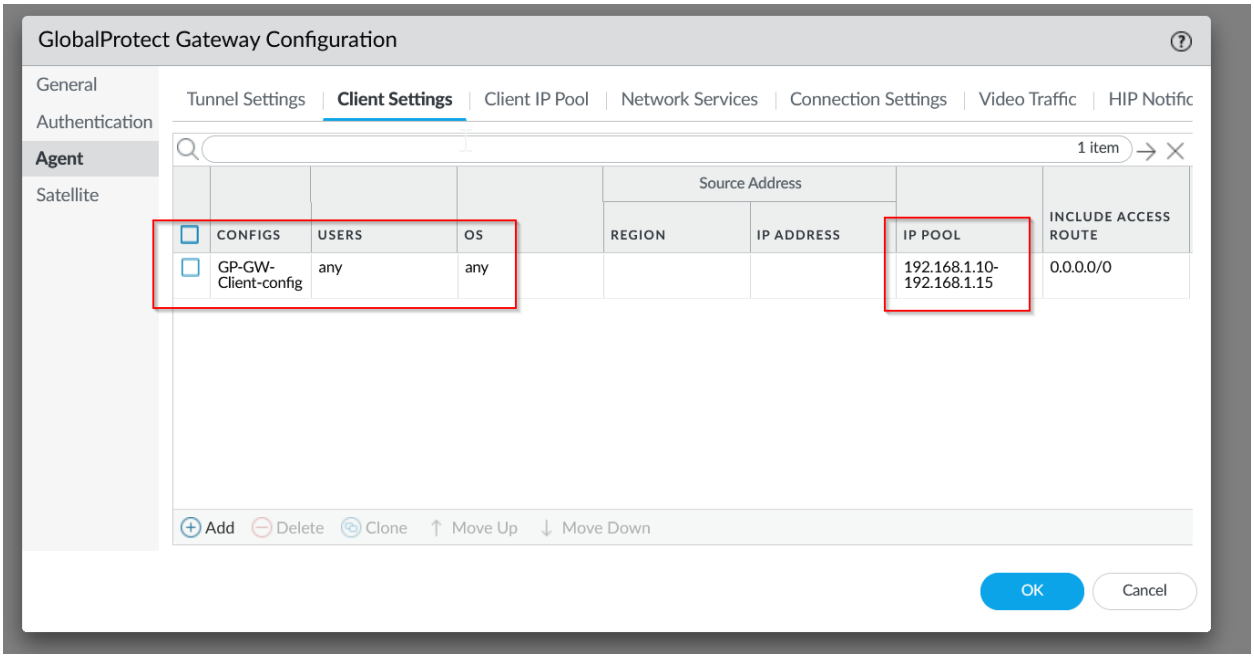
Click “Authentication” and select the previous SSL server we created. Add a new Client Authentication with the previous Authentication Profile created.



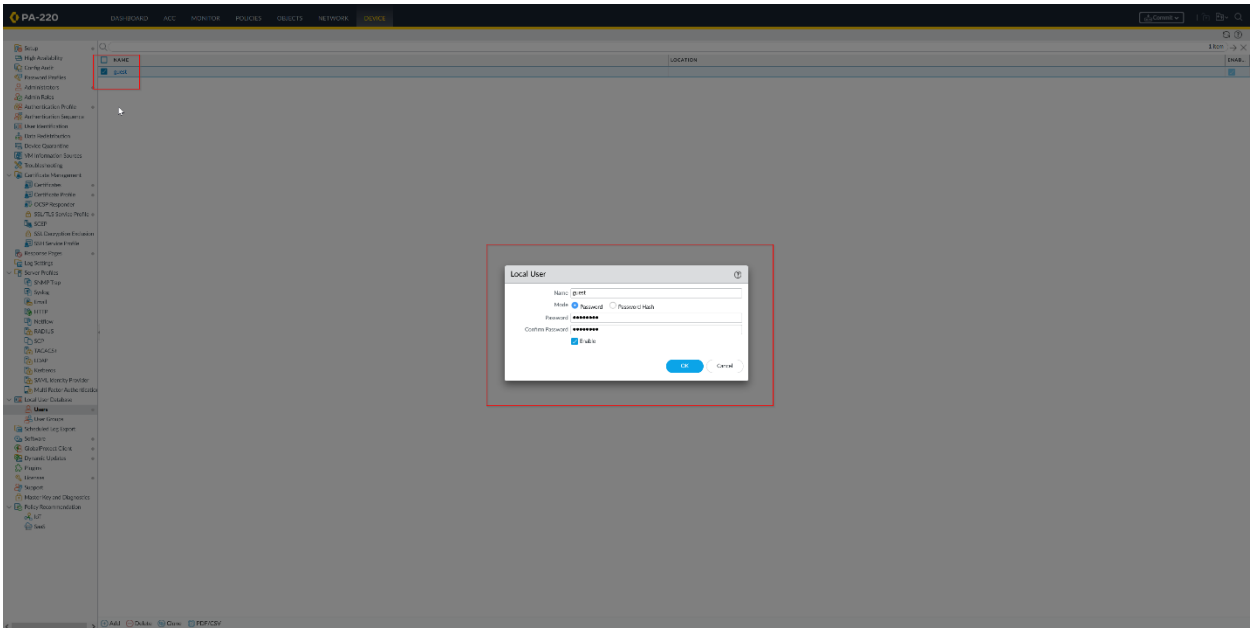
Navigate to the “Agent” tab and enable IPSec.



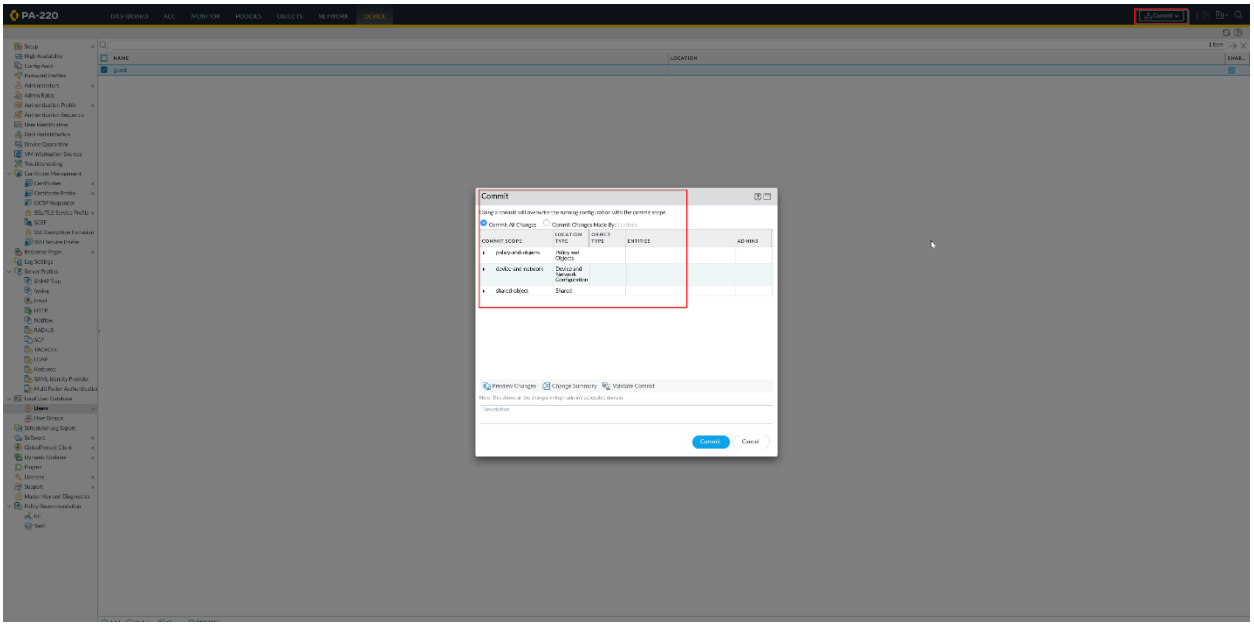
Navigate to the Client Settings under Agent and add an IP pool for end users.



In order to test our Global Protect, navigate to “Device” and “Local User Database” and “Users” on the left taskbar. Make a new user.

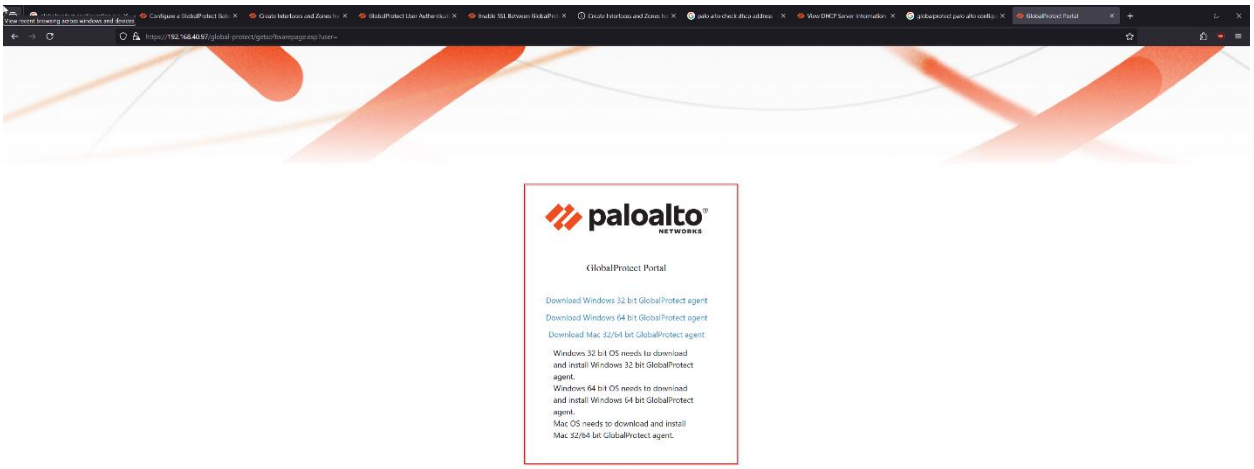


Commit the changes made to the firewall so far.

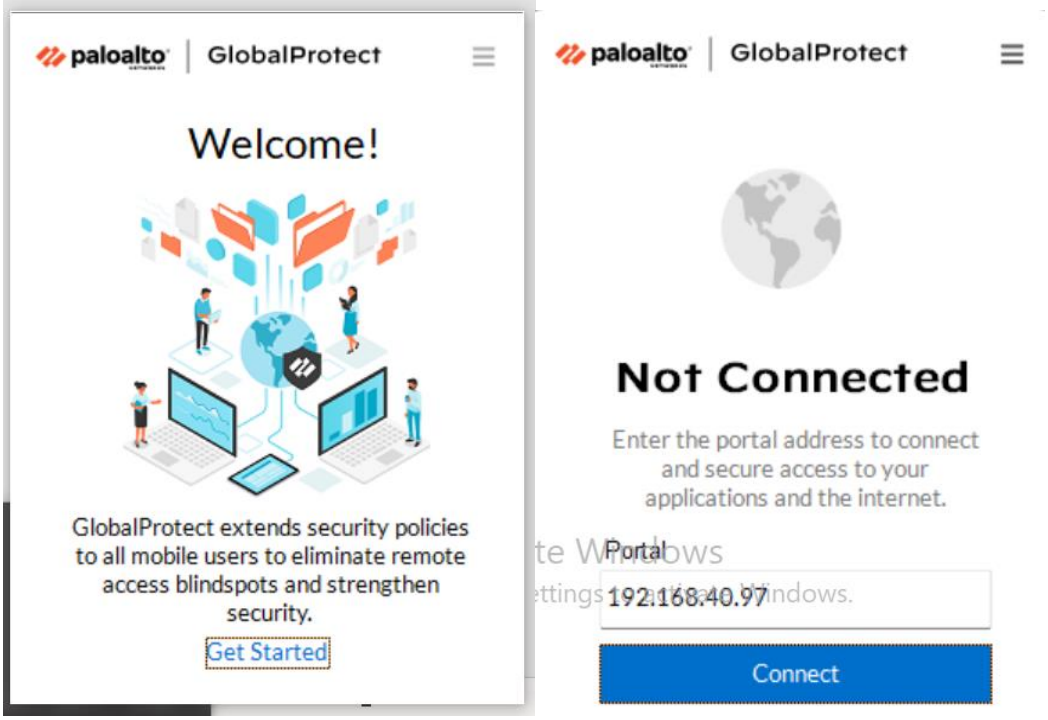


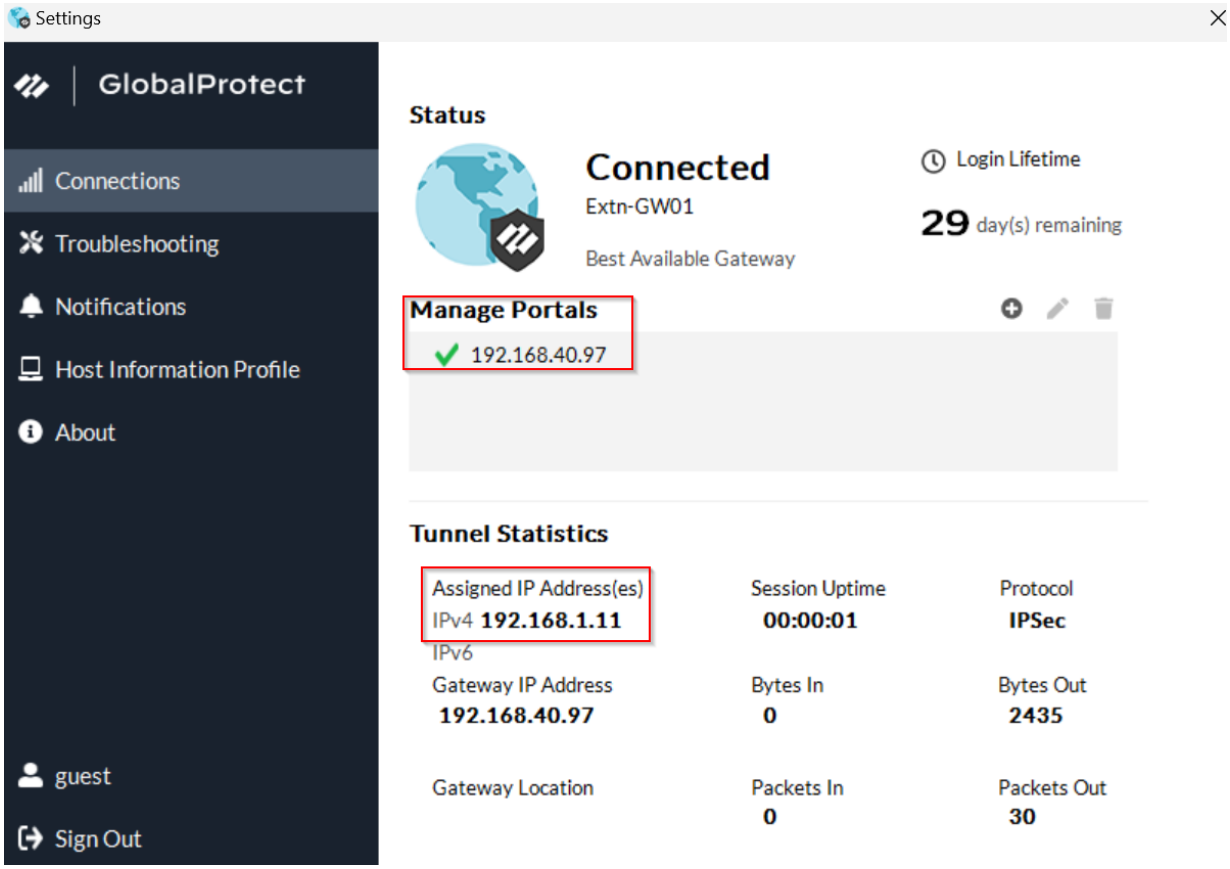
Using the IP address from your portal, enter the user credentials you've just made. Then, download the client.


paloalto
NETWORKS
GlobalProtect Portal
guest
LOG IN

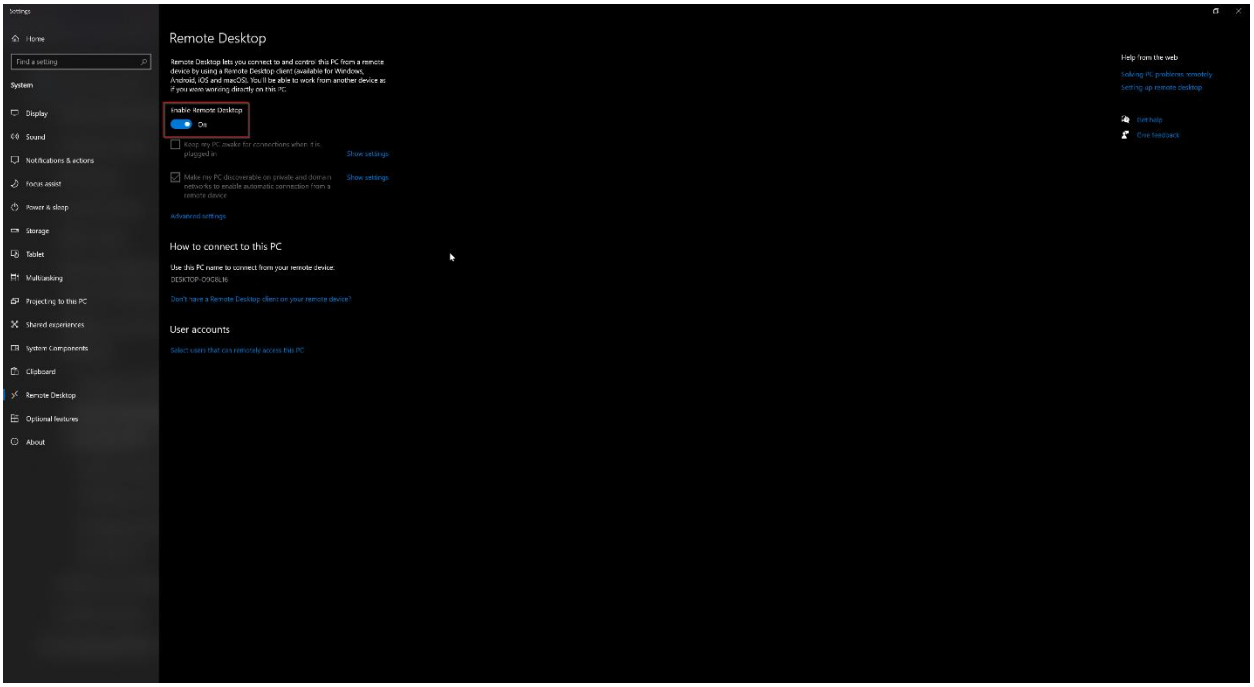

paloalto
NETWORKS
GlobalProtect Portal
Download Windows 32 bit GlobalProtect agent
Download Windows 64 bit GlobalProtect agent
Download Mac 32/64 bit GlobalProtect agent
Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

Once your app has been downloaded, click get started and use the portal IP address again. This will connect you to your VPN.

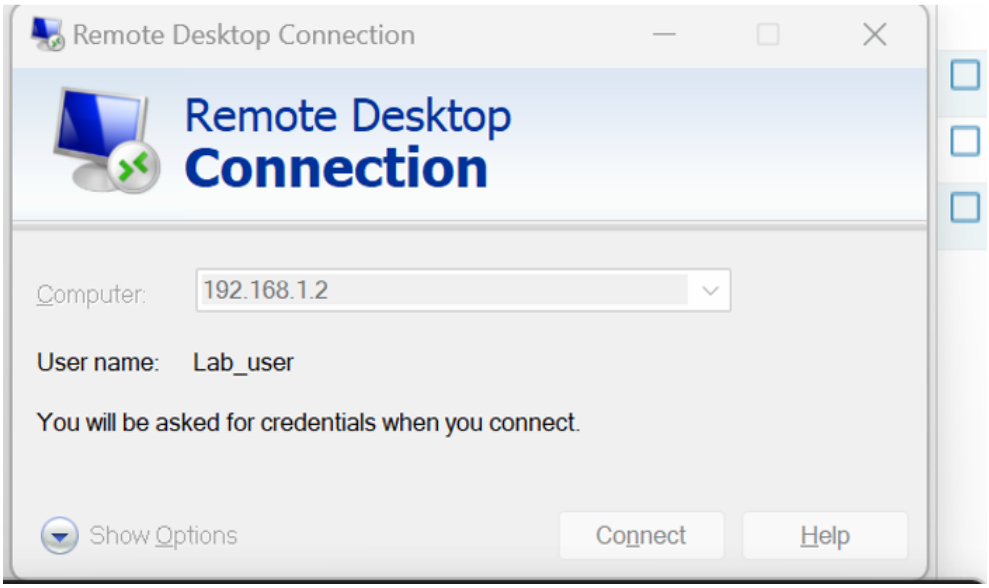




To test this VPN, we'll be using one desktop on the firewall network and another desktop off the network. The desktop off the network should be the one with all the certifications. On the firewall desktop, go to Settings, System, and then Remote Desktop. Enable Remote Desktop.



On your desktop off the network, use the Global Protect app and Device A's IP address to connect to Device A. Once you've entered your credentials, you'll be able to access the desktop on the firewall even without being in the network.



To check this, we can use Wireshark to look at the traffic on the firewall desktop. From the image below, we see that the firewall desktop is communicating with the desktop off the network that has an IP of 192.168.1.11, an automatically assigned IP from Global Protect. The protocol is RDP, or Remote Desktop, meaning that we've succeeded in configuring Global Protect.

Source	Destination	Protocol	Length	Info
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1109	
192.168.1.11	192.168.1.2	TLSv1.2	350	Application Data, Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1287	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	73	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	1279	
192.168.1.2	192.168.1.11	TLSv1.2	479	
192.168.1.11	192.168.1.2	TLSv1.2	341	Application Data, Application Data
192.168.1.11	192.168.1.2	TLSv1.2	118	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	54	ACK,OVERHEAD
192.168.1.2	192.168.1.11	TLSv1.2	105	Application Data
192.168.1.2	192.168.1.11	TLSv1.2	1051	
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	53	ACK,OVERHEAD
192.168.1.11	192.168.1.2	TLSv1.2	97	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26596 Win=62692 Len=0
192.168.1.2	192.168.1.11	TLSv1.2	229	
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	111	Application Data
192.168.1.11	192.168.1.2	TLSv1.2	104	Application Data
192.168.1.2	192.168.1.11	TCP	54	3389 → 64635 [ACK] Seq=11374 Ack=26696 Win=64000 Len=0
192.168.1.11	192.168.1.2	TLSv1.2	106	Application Data
192.168.1.2	192.168.1.11	RDPUDP2	52	ACK
192.168.1.2	192.168.1.11	TLSv1.2	1279	

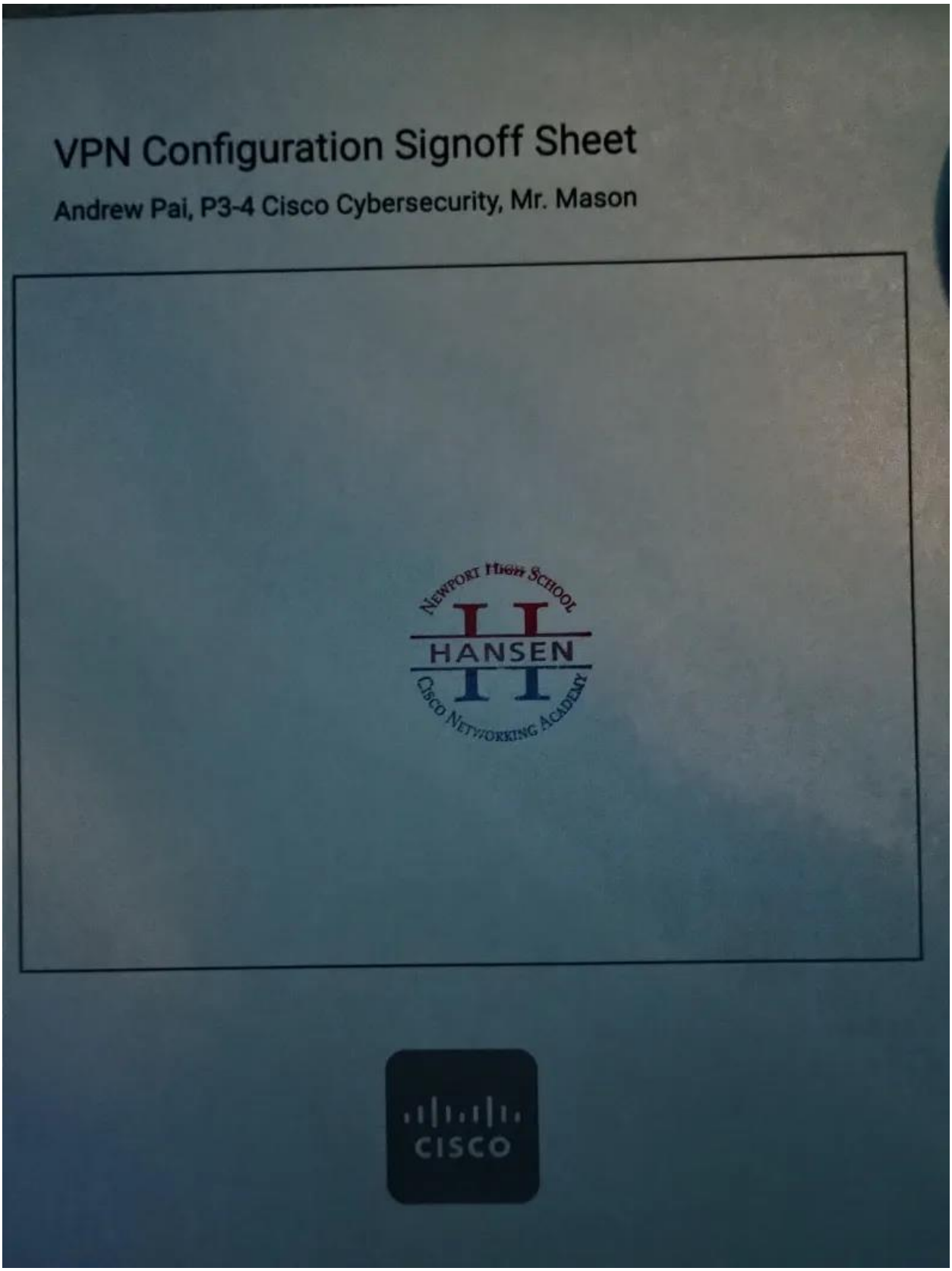
Problems:

The only problem that our group had with this lab was downloading Global Protect from the portal. Initially, when we tried to download the app, we didn't get anything from the file and were unable to. After figuring out that the problem lay in our not having installed the Global Protect app onto our firewall, we were able to fix this and install the app to our firewall to then download the app to our computer from the portal.

Conclusion:

In conclusion, Virtual Private Networks are an important method for employees to access business networks from remote locations or for Internet users to protect their data. The VPN setup in this lab was mostly dedicated to the first application of VPNs mentioned and included our group setting up a remote desktop connection. To do this, we used various configurations of the Palo Alto PA-220 GUI as well as the Global Protect App to connect to remote desktops.

Lab Signoff:


VPN Configuration Signoff Sheet
Andrew Pai, P3-4 Cisco Cybersecurity, Mr. Mason
Newport High School
HANSEN
Cisco Networking Academy
CISCO