Palo Alto Networks Cybersecurity Academy – Configuring GlobalProtect RAVPN on a PA220 Firewall

Colin J. Faletto, CCNA

paloalto NETWORKS

Purpose

This lab expands upon our knowledge of the PA220 by introducing us to the world of VPNs. Setting up a remote access VPN provides valuable insight on how to create and secure a private tunnel into a firewall's internal network, which is extremely valuable to businesses requiring work-from-home cybersecurity solutions.

Background

Palo Alto Networks is a networking and cybersecurity company from Santa Clara, California. They are a member of the S&P 500. They focus mainly on the business market, creating scalable security solutions for many of the largest companies worldwide.

The Palo Alto PA220 is a firewall sold by Palo Alto Networks. Contrary to Palo Alto's main market, the PA220 is intended for small office/home office solutions. Marketed as a NGFW, or Next-Generation Firewall, the PA220 uses machine learning to identify attacks instead of relying on a simple signature check like traditional firewalls. This technology allows the PA220 to identify undocumented threats and brand-new exploits without intervention from Palo Alto networks themselves. The PA220 also prevents threats by filtering URLs and securing against DNS-based attacks. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The PA220 doesn't have a fan, and instead uses hexagon-shaped vents to passively filter air. The firewall's compact form factor allows it to easily fit alongside existing network devices.

Palo Alto firewalls run on an operating system called PAN-OS. PAN-OS can be controlled through two methods: a Graphical User Interface (GUI) and a Command-Line Interface (CLI). The GUI is accessible through an HTTP connection and displays in any modern web browser. The HTTP connection is available through the firewall's MGT port and by default, is accessible at http://192.168.1.1. The firewall has a default username and password of *admin*.

The latest version of PAN-OS is PAN-OS 11.2 Quasar, which was released in May 2024. In this lab, our firewall is running PAN-OS 8, which has reached end of life and is no longer supported.

PAN-OS's GUI has a variety of settings and tools to control advanced functionality of the router. The GUI's default page is a dashboard that displays vital information, such as console messages and link states of ports.

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-

10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

A virtual private network, or a VPN, is a method of creating a secure tunnel between networks. VPNs allow computers that are physically located offsite to be treated the same as computers physically inside of a network. There are two primary types of VPNs: remote access (RAVPN) and site-to-site, which create private tunnels for individual computers and entire networks respectively. In the business world, VPNs are often used to allow employees working from home to access company resources located on internal servers. VPN services are commonly sold commercially, allowing consumers to connect to private network-sharing servers. These servers are often located in multiple countires or regions, enabling consumers to spoof their location and hide network traffic from their ISP.

GlobalProtect is a Remote Access VPN service developed by Palo Alto networks. The service requires a client program which runs on outside computers and supports all three major operating systems. GlobalProtect is heavily integrated into Palo Alto firewalls such as the PA220, which includes a gateway to allow connections from the service and a web portal to download the client. GlobalProtect puts a large emphasis on security, exemplifying the principle of least-privilege access and including a wide variety of configurable security options.

Remote Desktop Protocol, or RDP, is a Microsoft-proprietary protocol that allows a user to remotely view and control a connected Windows PC. RDP employs a client/server model, with the client being included on all versions of Windows and the server being exclusive to the operating system's higher tiers. RDP uses port 3389 with both TCP and UDP. RDP was introduced during Microsoft's transition from MS-DOS to the NT kernel with Windows NT 4.0 Terminal Services Edition, and the server has been included on every version of Windows (other than Home) since XP.

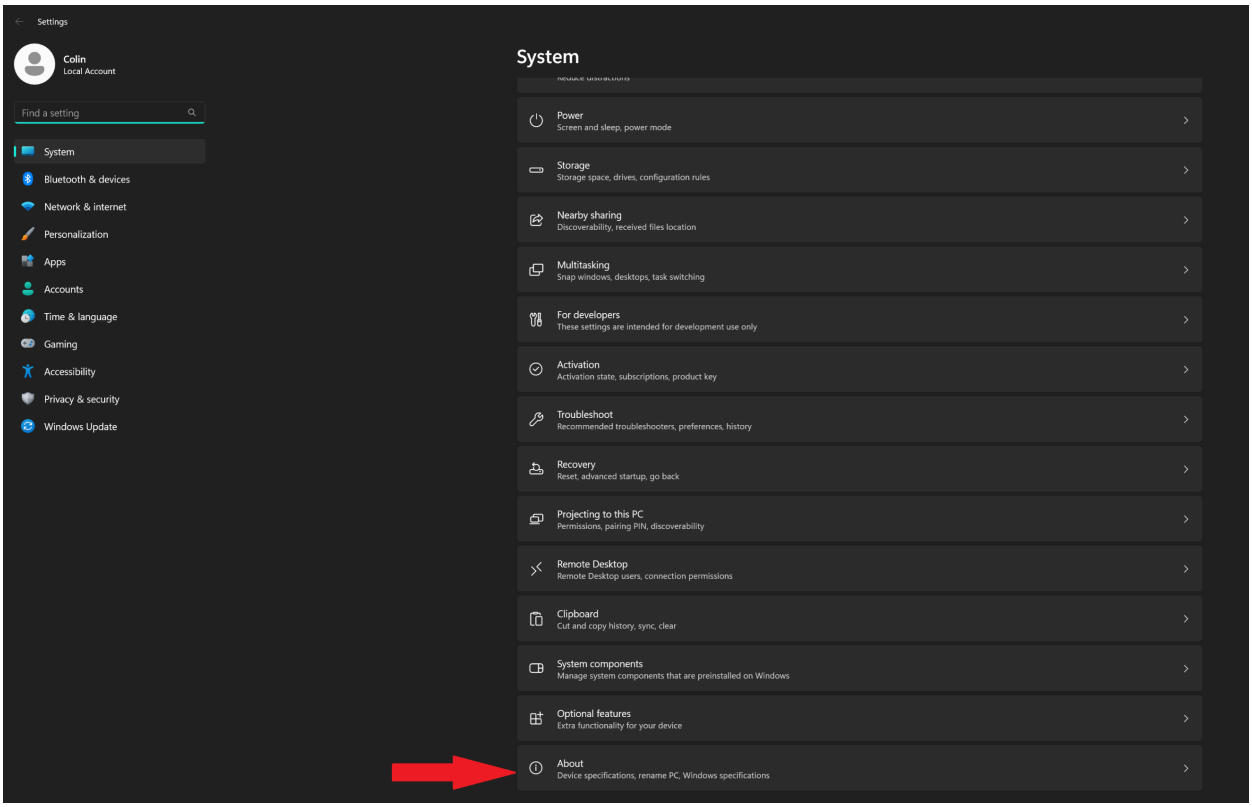
Lab Summary

In this lab, we configured Microsoft's remote desktop protocol (RDP) on two Windows computers: one on the PA220's internal network and one just outside the PA220's network. We then set up Palo Alto's GlobalProtect remote access VPN on the firewall, including credentials for the outside user and a portal page to download the GlobalProtect client.

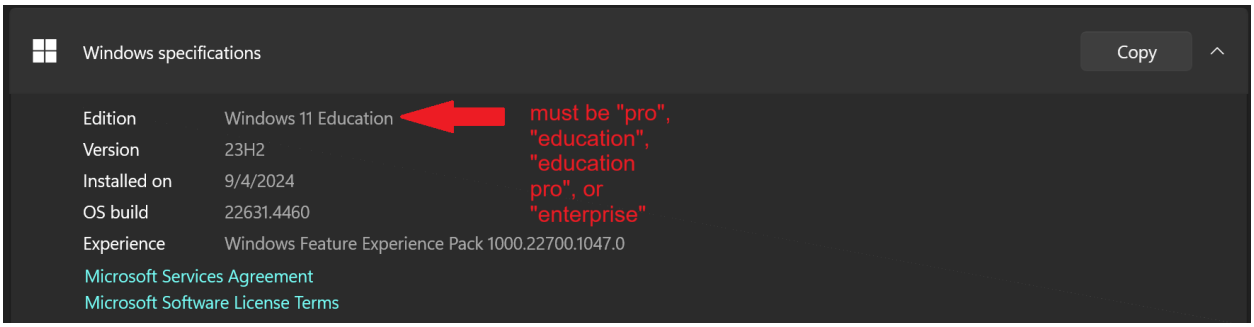
Lab Commands

Configuring Remote Desktop

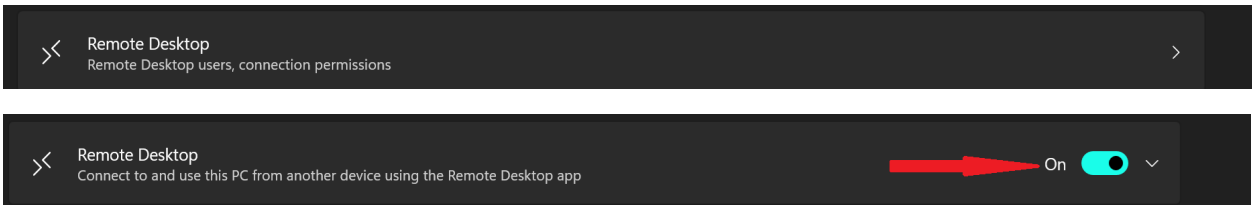
On the internal Windows PC, press (Win+I) to open the settings app. Click into the "About" section.



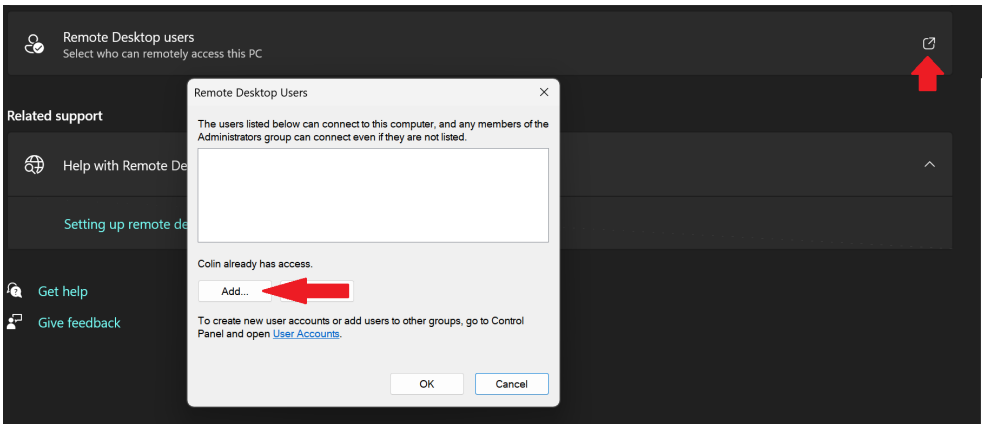
Make sure that you are running Windows 11 Pro, Education, Education Pro, or Enterprise. **Windows 11 Home doesn't support a Remote Desktop Server connection**. It can, however, be used on the external client PC.



In the settings menu, go to System > Remote Desktop and turn on "Remote Desktop".

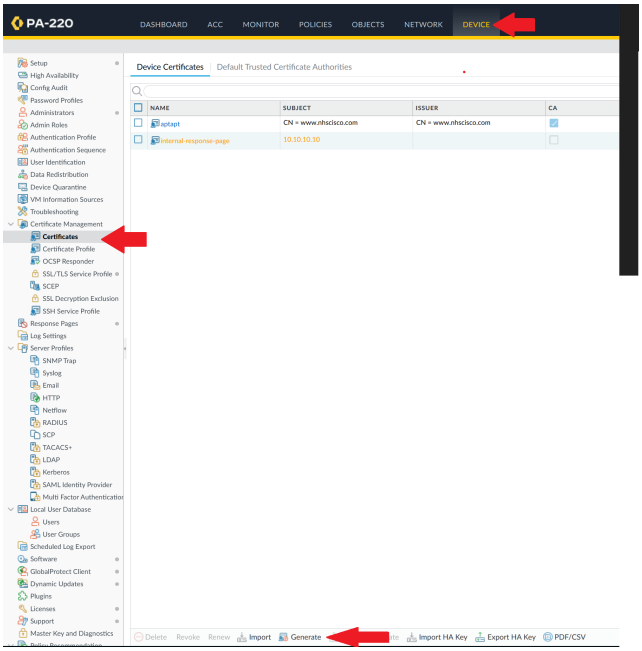


Click on "Remote Desktop Users". If the user account you want to connect to isn't an administrator, you will have to manually add it here using the "Add" button.

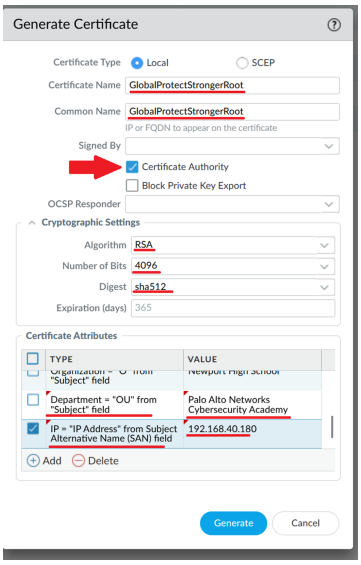


Generate Certificates

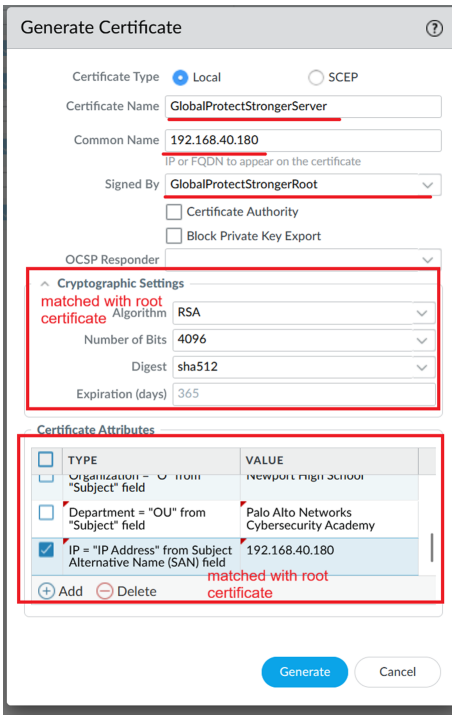
In the PA220 web interface, navigate to Device > Certificate Management > Certificates and click Generate.



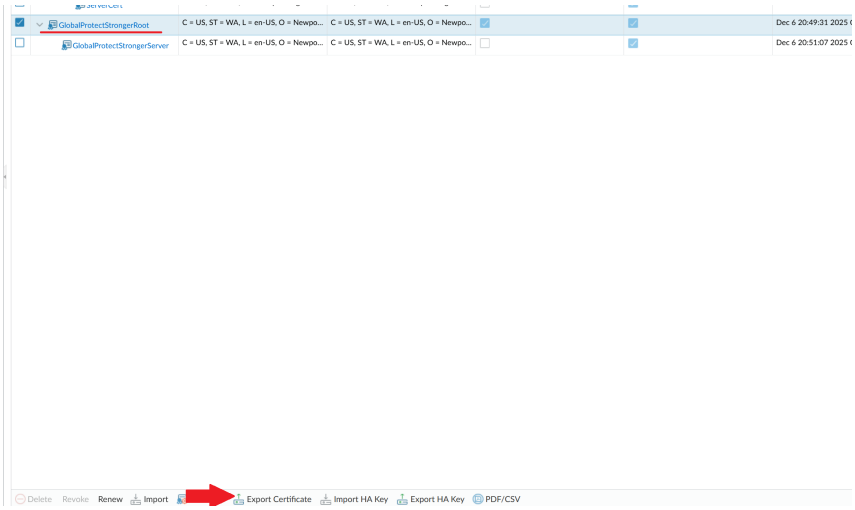
First, generate a root certificate. Give a Certificate Name and Common Name that make sense for the context, and make sure that the Certificate Authority box is checked. Under Certificate Attributes, assign appropriate values for the Country, State, Locale, Organization, and Department Fields, and make sure that the IP Address field is set to the outward-facing IP of the firewall. Optionally, increase the default cryptographic settings to higher values to increase the security of your certificates.



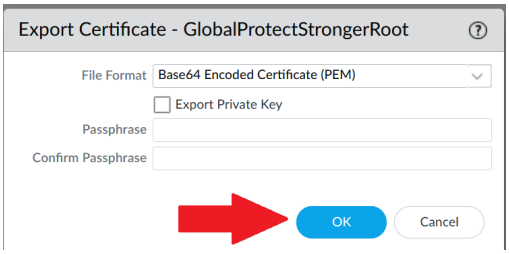
Next, generate your server certificate. Make sure that the Common Name is the outward-facing IP address of the firewall, and that the certificate is signed by the root certificate you generated earlier. Match the cryptographic settings and certificate attributes with the values configured in the root certificate.



Export your root certificate by selecting it and clicking Export Certificate.

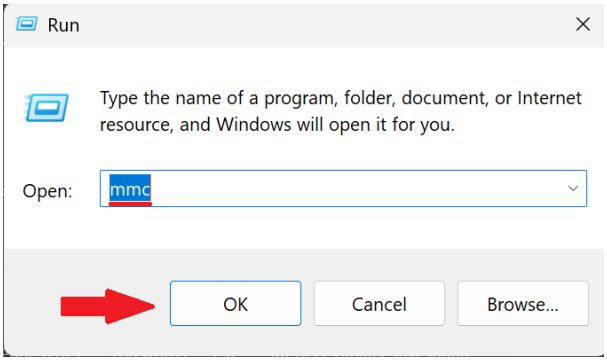


Click “OK” to confirm downloading the certificate. Make sure to note down the file’s download location.

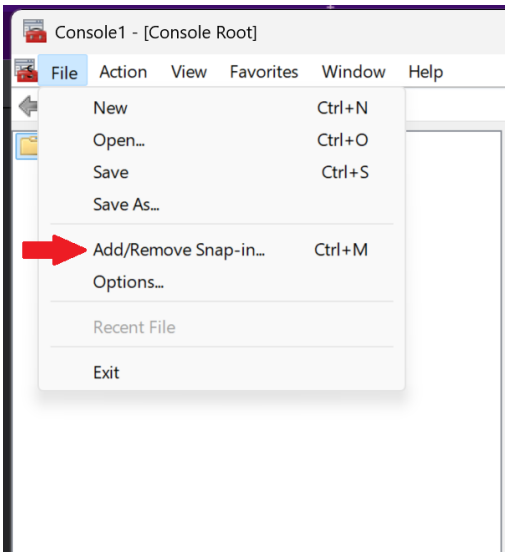


Import Certificates

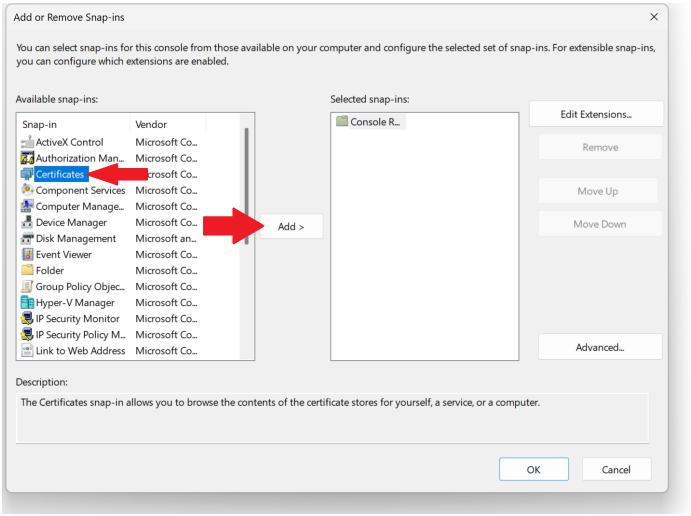
On your outside PC, open the Run dialog (Windows+R) and type “mmc”.



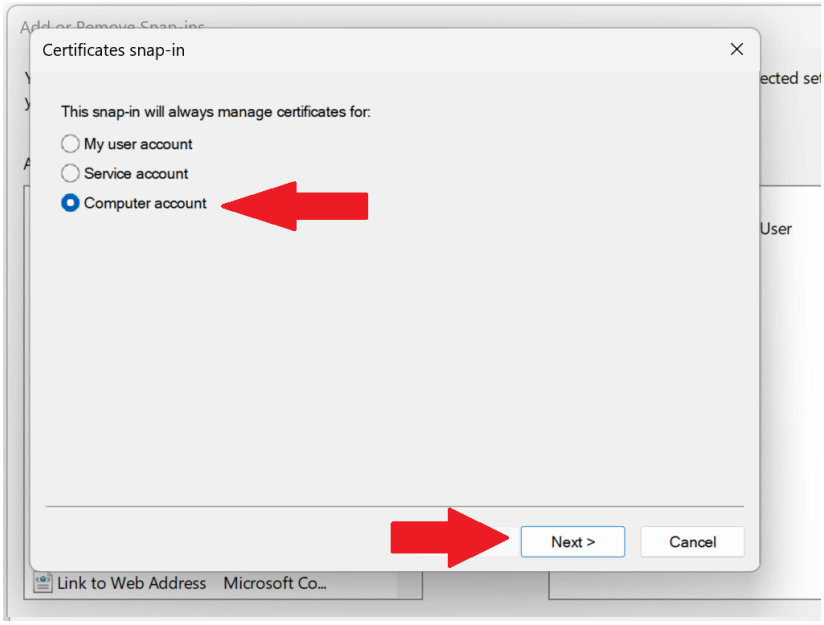
In the resulting window, click File > Add/Remove Snap-in.



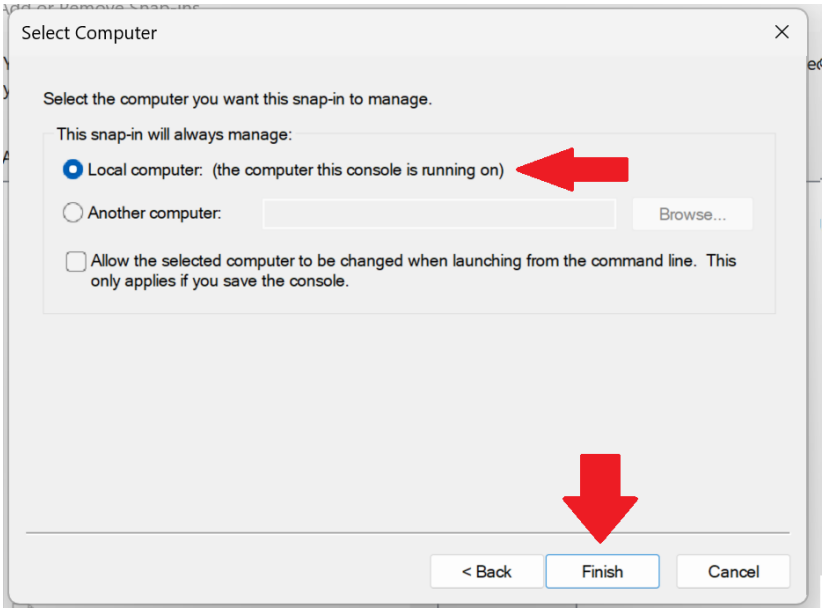
In the resulting window, click on Certificates > Add.



In the resulting window, click on Computer Account > Next.

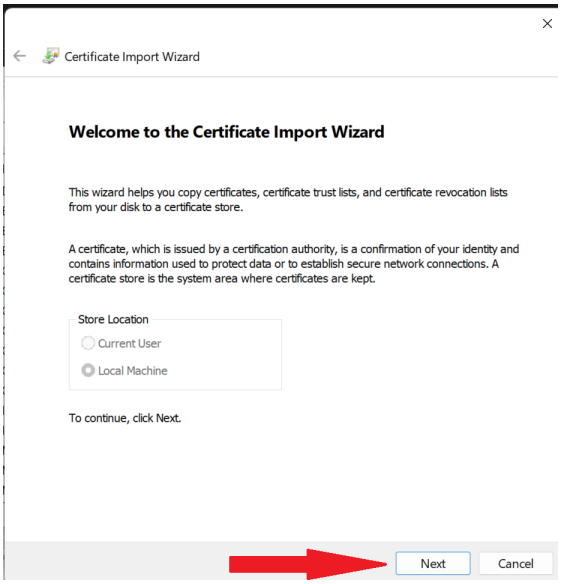


Make sure Local Computer is selected, and click Finish.

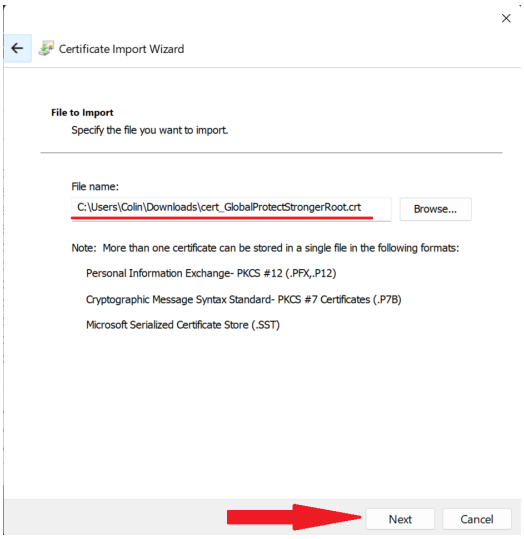


Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

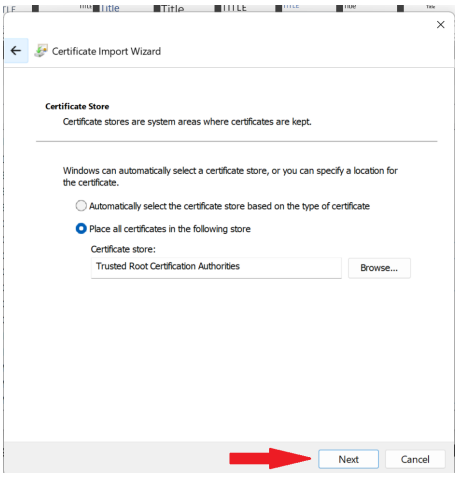
Click “Next”.



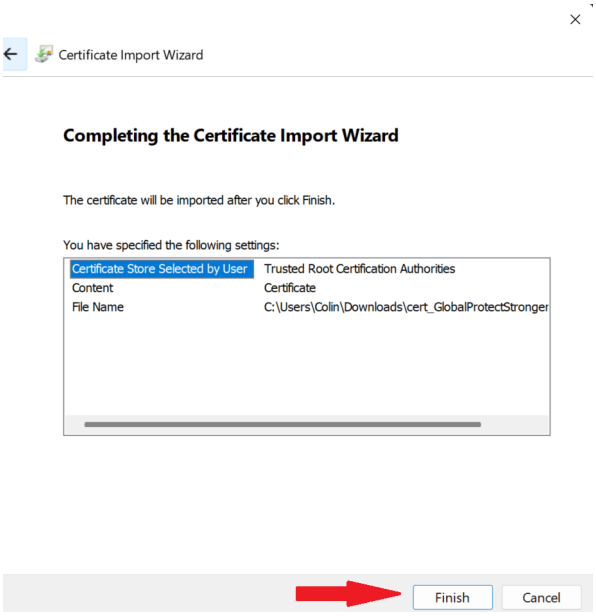
Select the certificate file downloaded earlier, then click “Next” again.



Leave the certificate store location setting as the default value, then click “Next”.

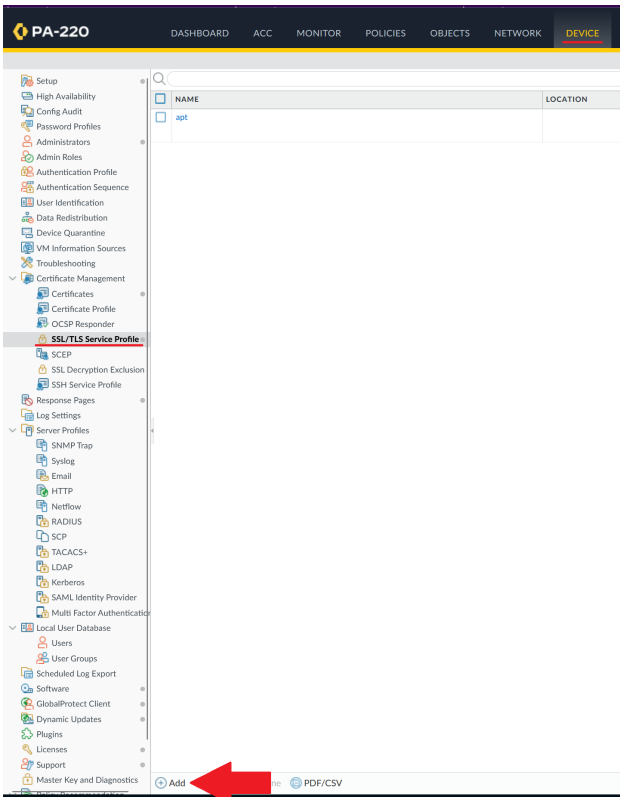


Click “Finish” to confirm the certificate import.

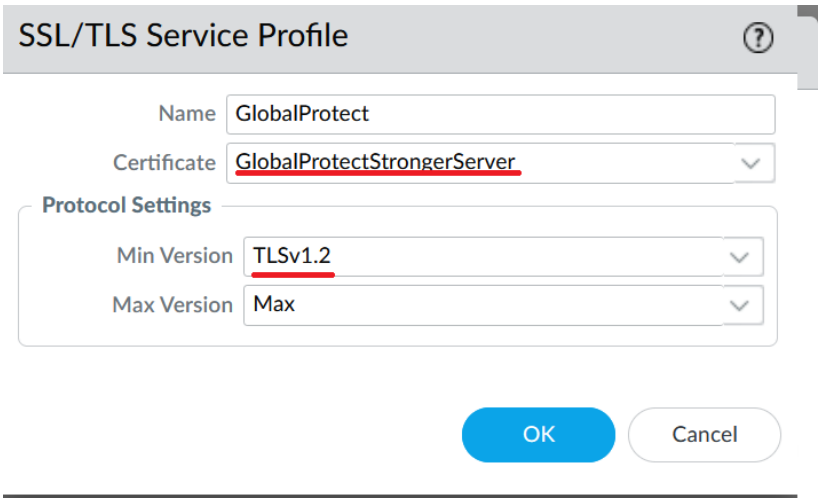


Firewall Configuration

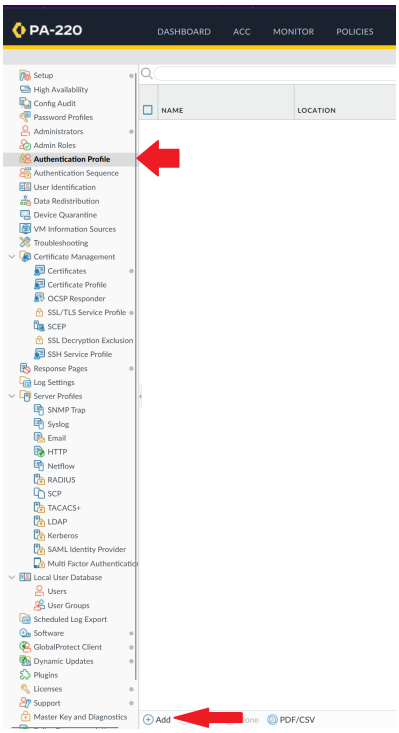
Back on the PA220, go to Device > SSL/TLS Service Profile, and click “Add”.



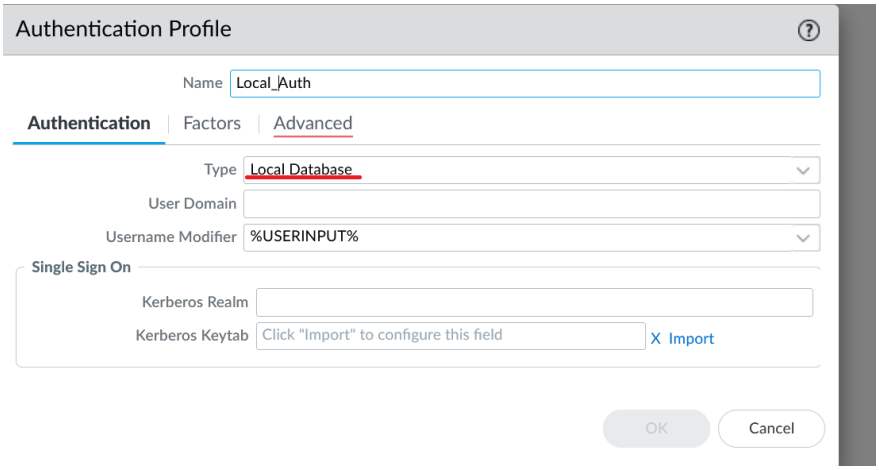
Make sure this profile uses the server certificate you set up earlier. Optionally, set the minimum TLS version to a more secure version (in this case, we used TLS 1.2)



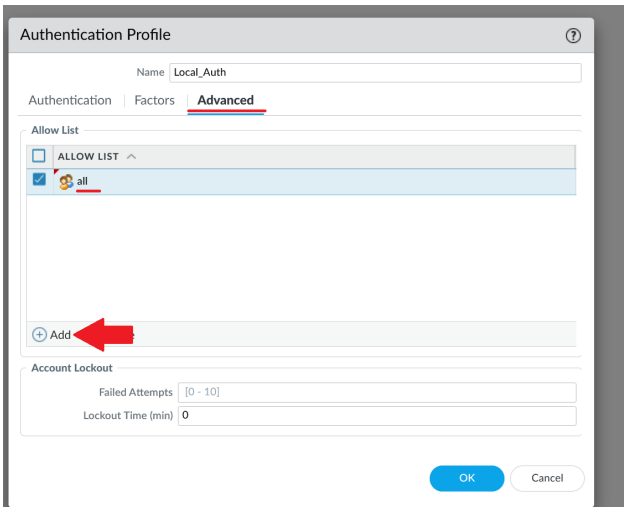
Next, go to “Authentication Profile” (still under Device) and click “Add”.



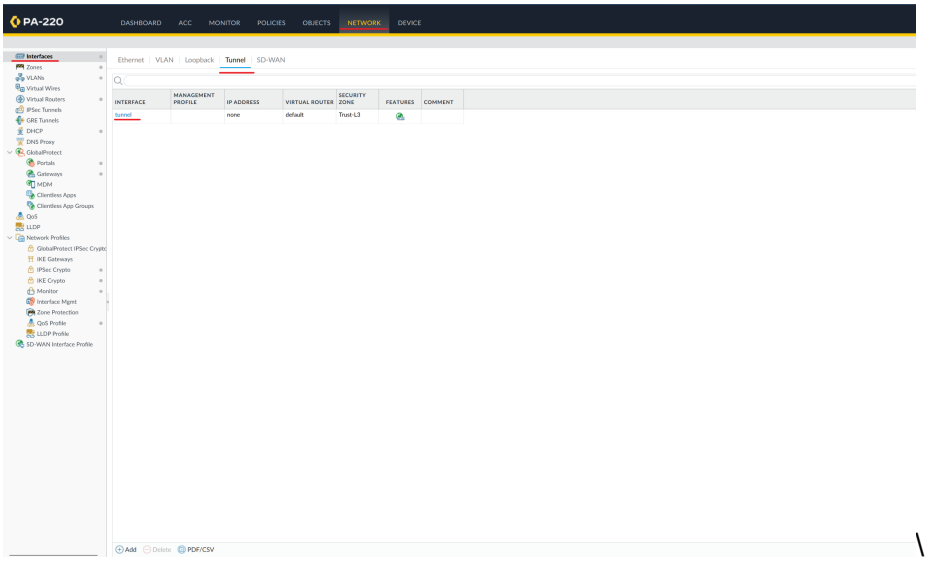
Give this profile an appropriate name and set the database type to “Local Database”.



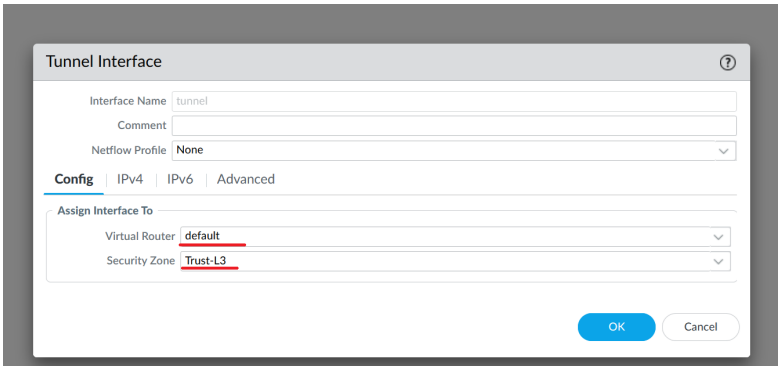
Under “Advanced”, click “Add” and type “all”.



Go to Network > Interfaces > Tunnel and click on the “tunnel” interface.

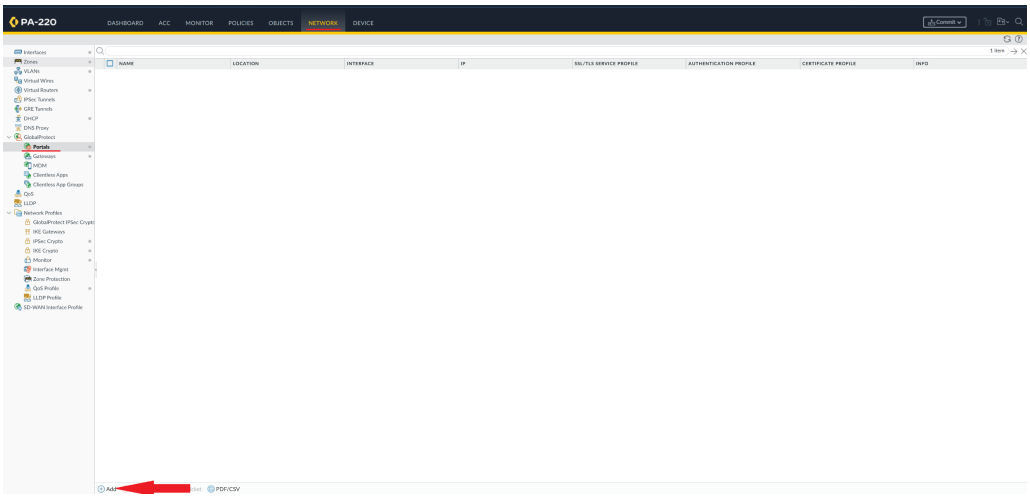


Under “Config”, configure the same virtual router and Layer 3 security zone used on your inside network.

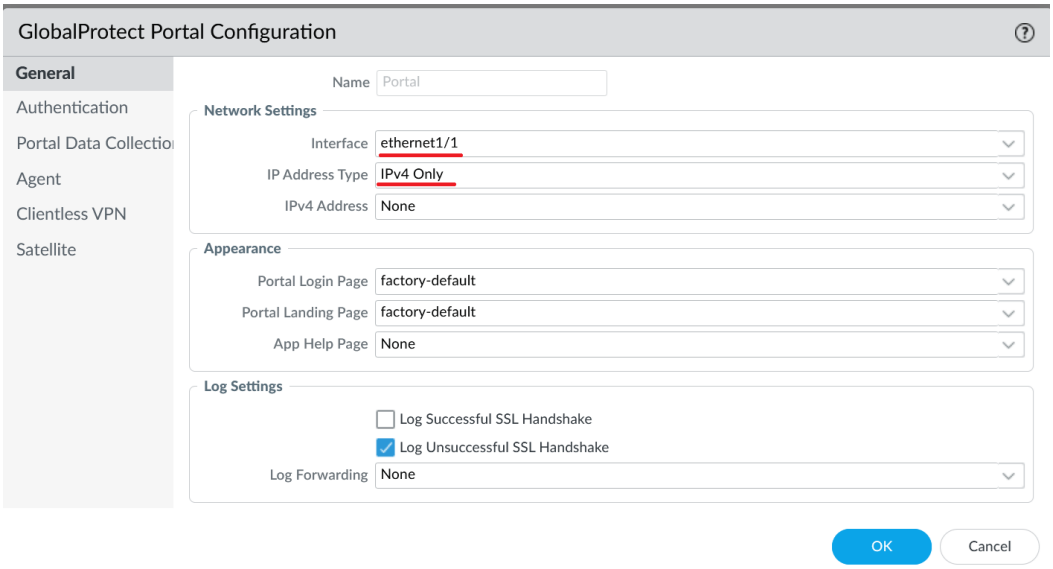


Go to Network > GlobalProtect > Portals and click “Add”.

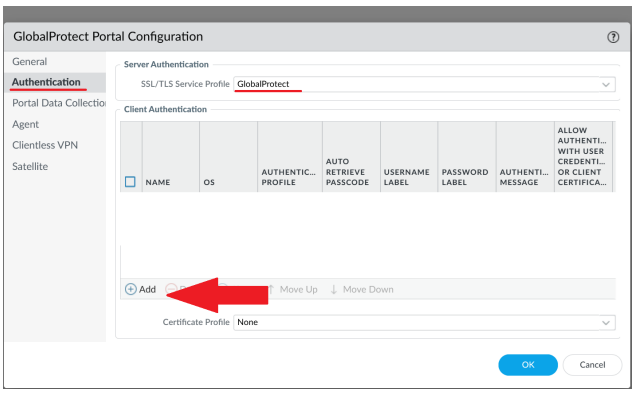
paloalto NETWORKS



Specify the outward-facing ethernet interface and set the address type to “IPv4 only”.

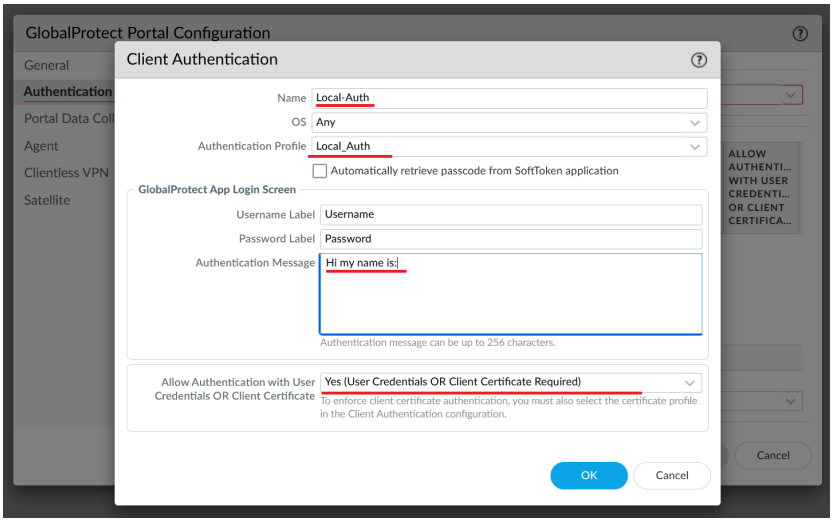


Under the “Authentication” tab, specify the SSL/TLS service profile you created earlier and click “Add”.21

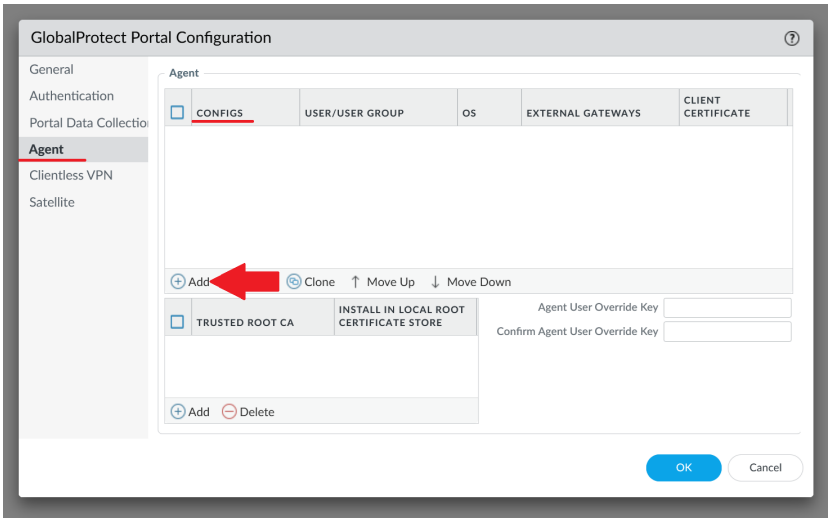


paloalto NETWORKS

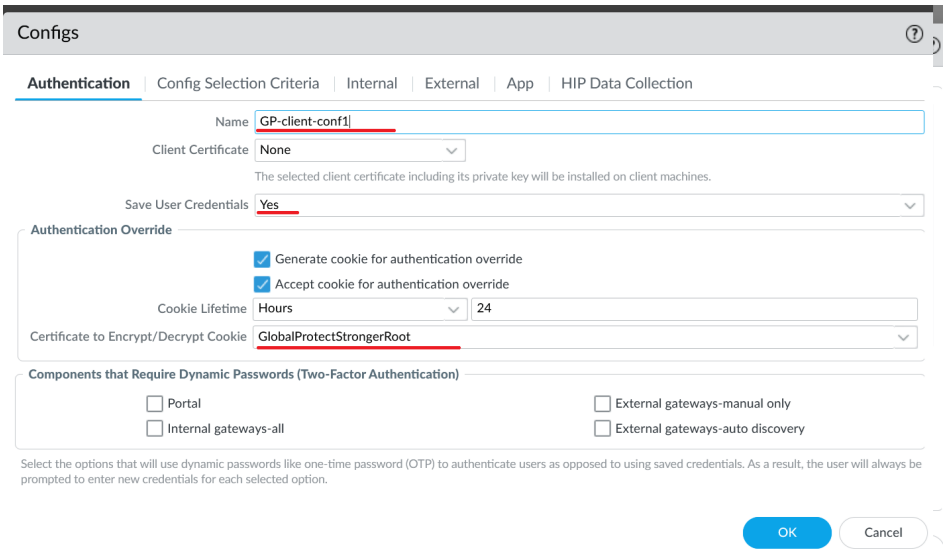
Give the client authentication profile an appropriate name and specify the authentication profile you created earlier. Create an appropriate authentication message and make sure clients can either authenticate with user credentials or client certificates.



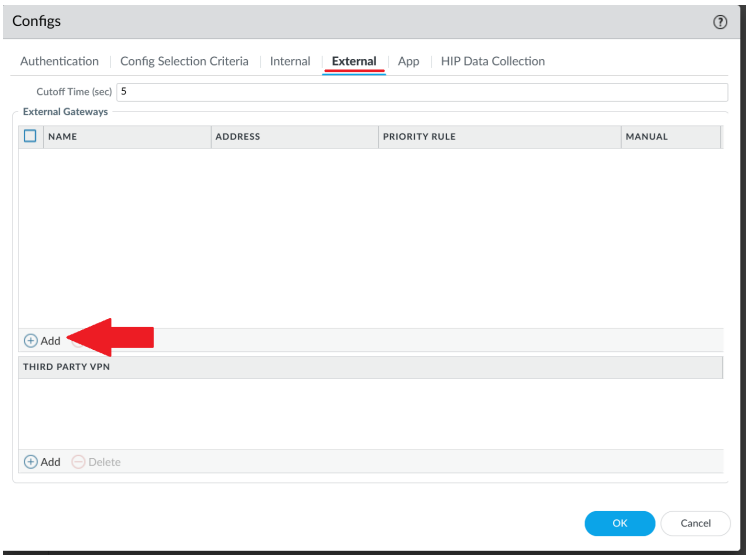
Under Agent > Configs, click “Add”.



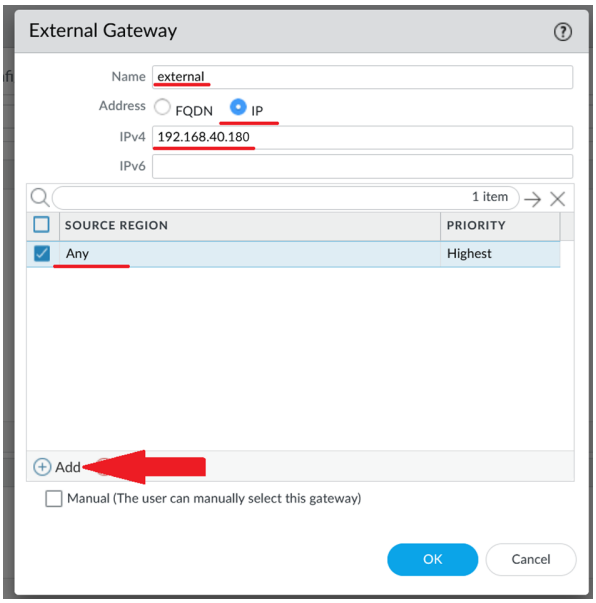
Give the config an appropriate name, and make sure to save the user credentials. Make sure the Authentication Override certificate is set to the root certificate created earlier.



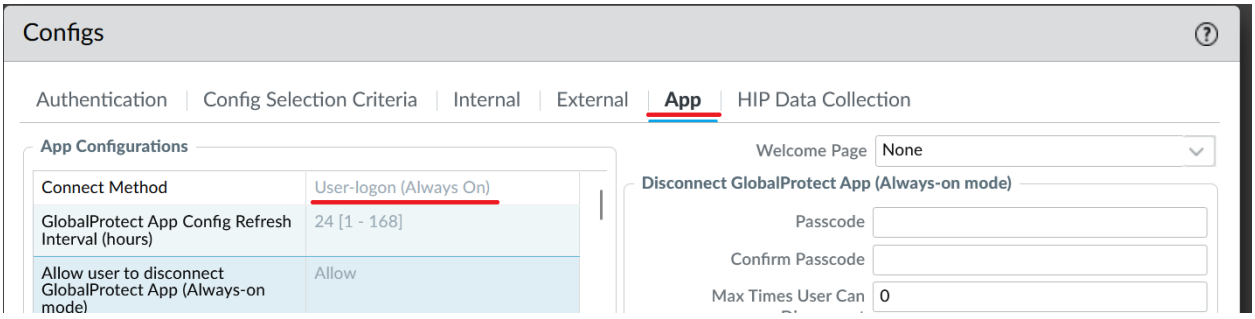
Under “External”, click “Add”.



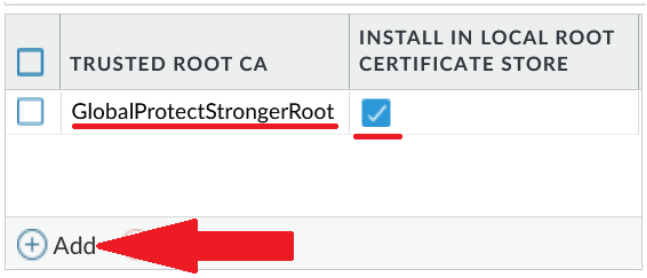
Give the gateway an appropriate name, set the mode to “IP”, and set the IP to the outward-facing IP of the gateway. Under “Source Region”, click “Add” and set it to “Any”.



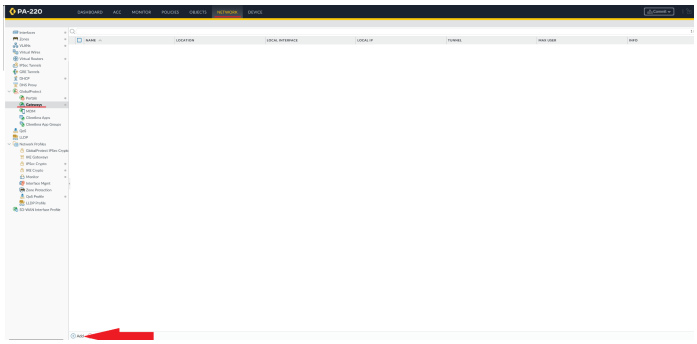
Click “OK” on the External Gateway window. Under “App”, set the connect method to “User-logon (Always On)”.



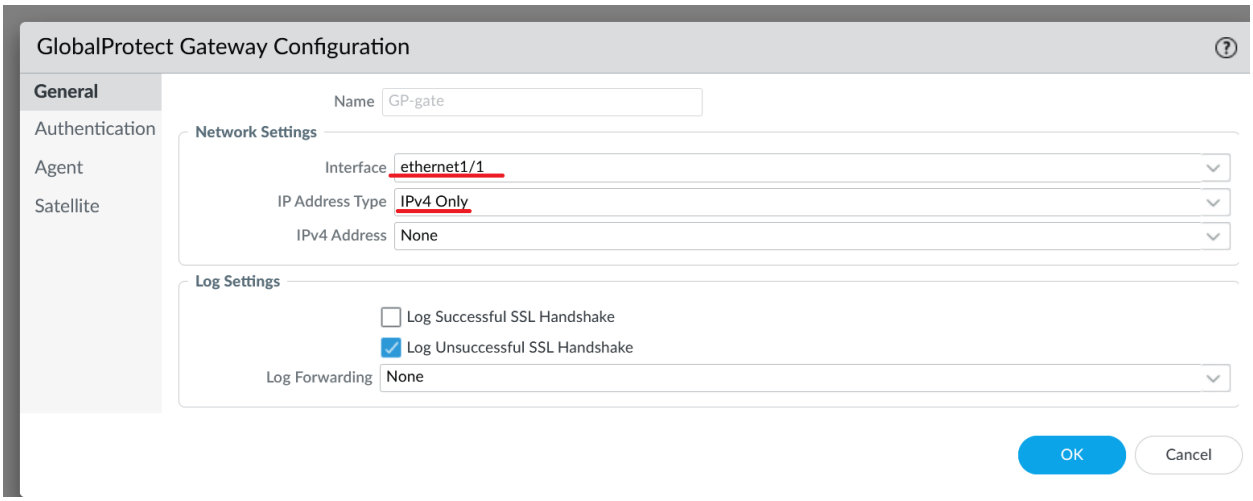
Click ok on the Configs window. Under “Trusted Root CA”, click “Add”, add the root certificate created earlier, and click “Install in local root certificate store”.



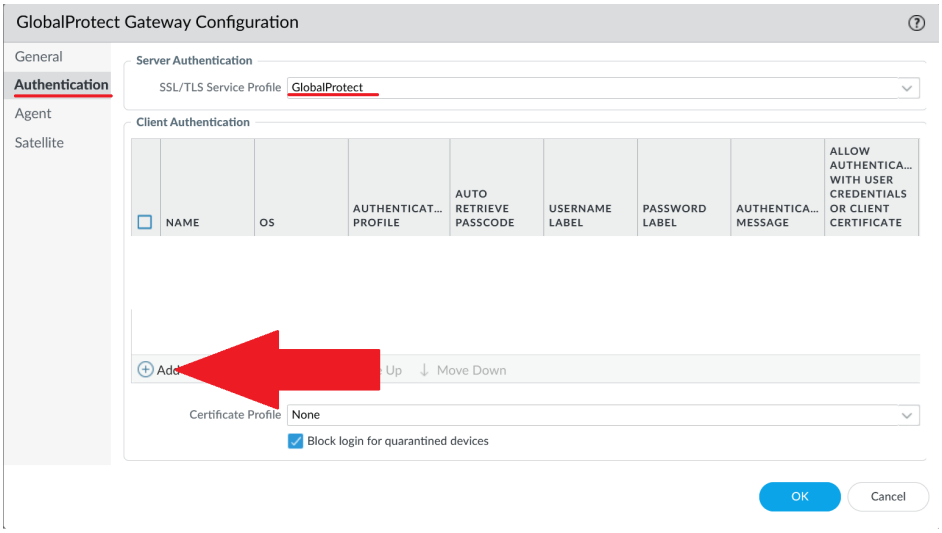
Go to Network > Gateways and click “Add”.



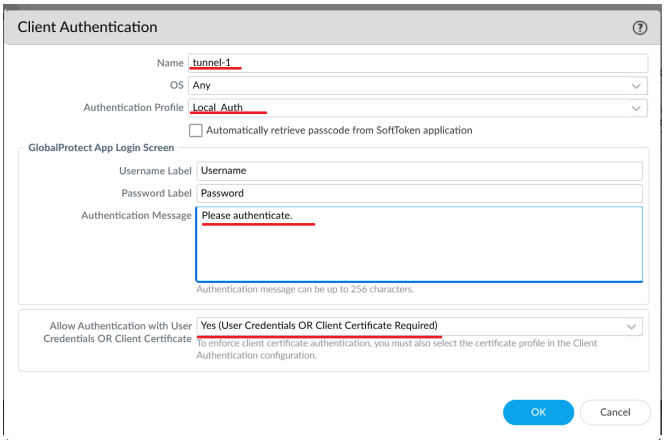
Set the interface to the outward facing interface of the firewall and leave the IP address type as “IPv4 only”.



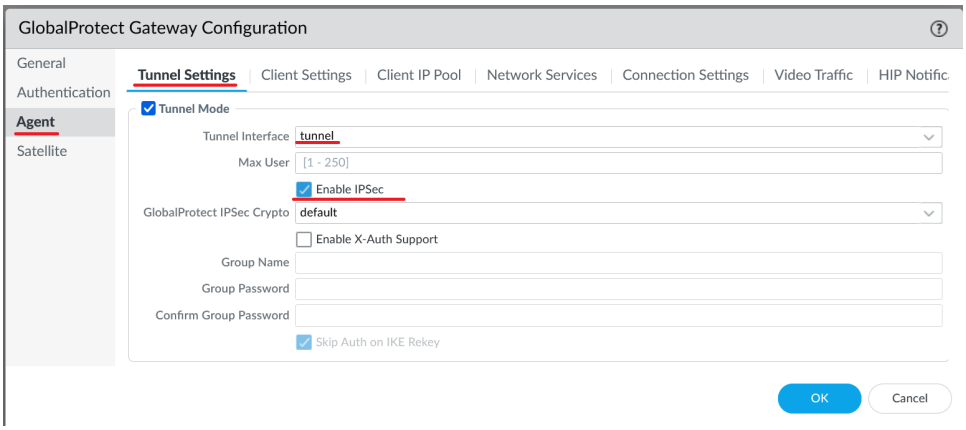
Under “Authentication”, set the SSL/TLS service profile to the profile you created earlier, and under client authentication, click “Add”.



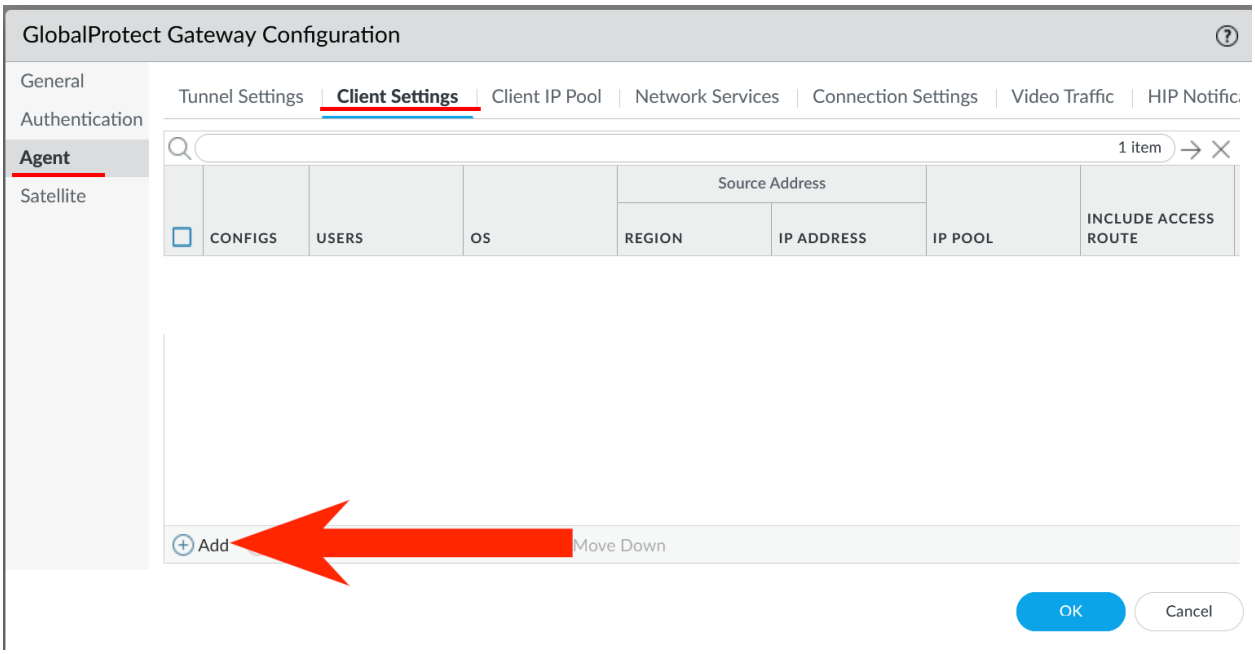
Configure an appropriate tunnel name, and set the authentication profile to the profile created earlier. Configure an appropriate authentication message, and allow authentication with user credentials OR a client certificate.



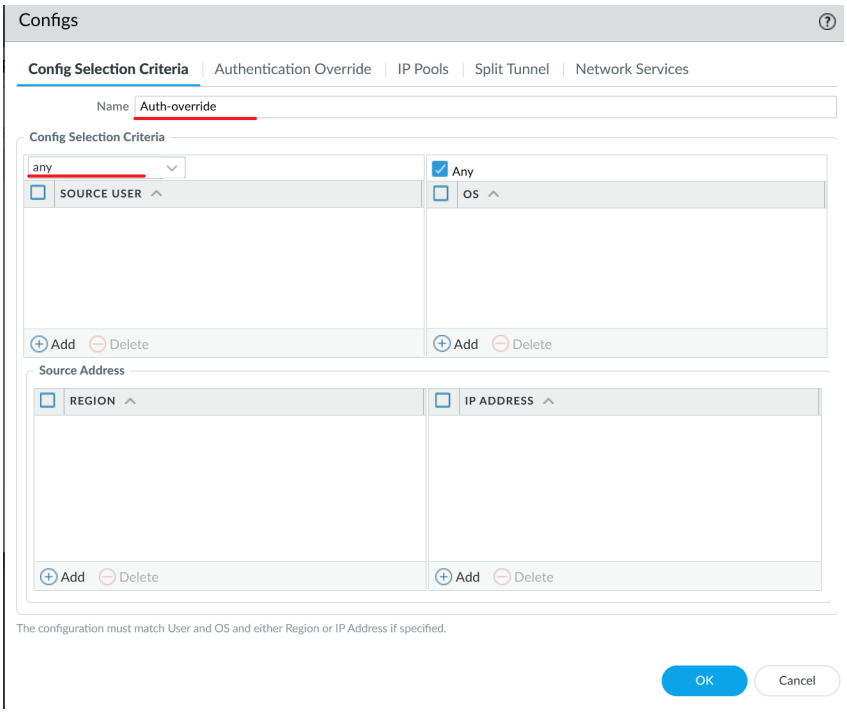
Under Agent > Tunnel Settings, set the tunnel interface to the interface created earlier, and make sure to enable IPsec.



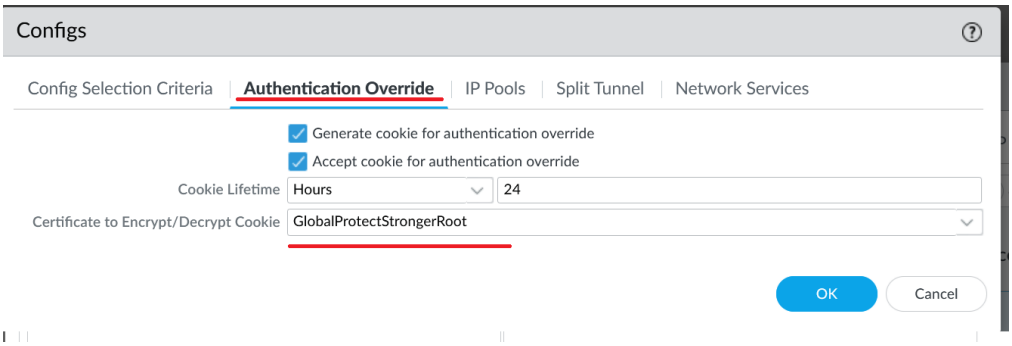
Under “Client Settings”, click “Add”.



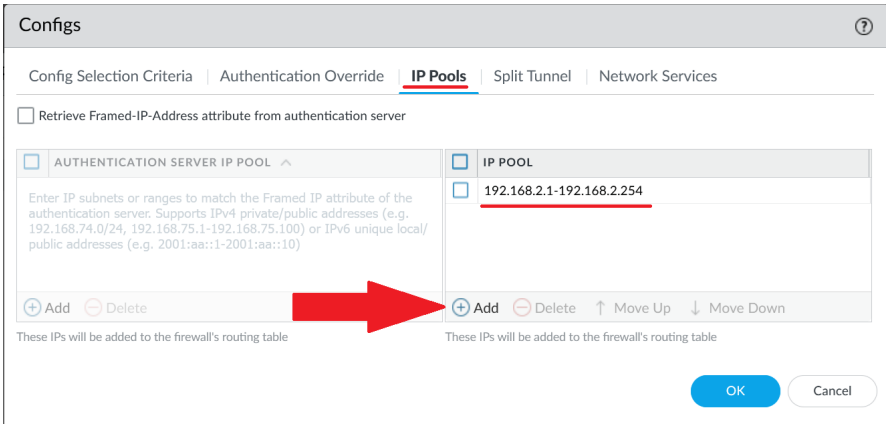
Give the configuration an appropriate name, and set the config selection criteria to "any".



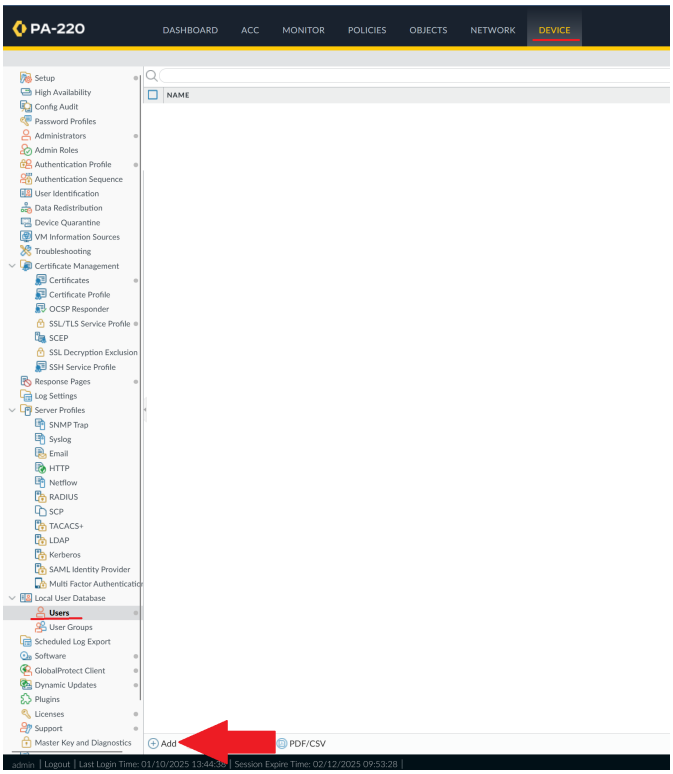
Under "Authentication Override", set the certificate to decrypt/encrypt the cookie to the root certificate created earlier.



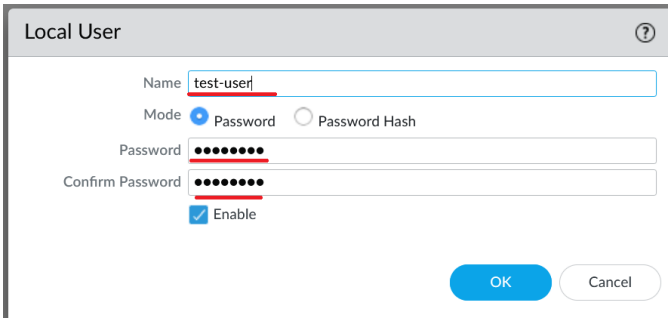
Under “IP Pools”, click “Add” and specify a valid range of IP addresses. These addresses will be dynamically allocated to clients by the GlobalProtect gateway.



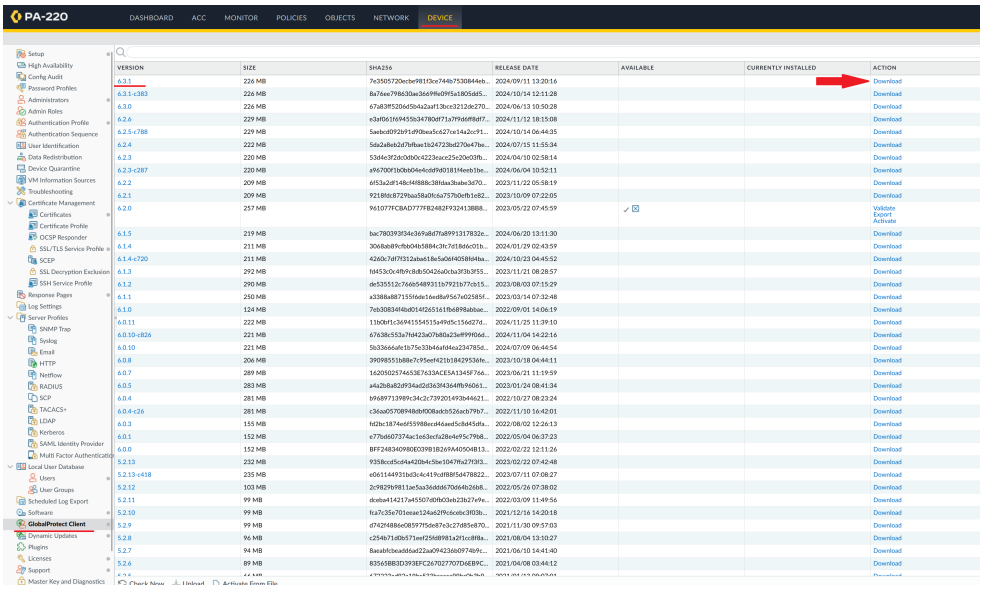
Under Device > Local User Database > Users, click “Add”.



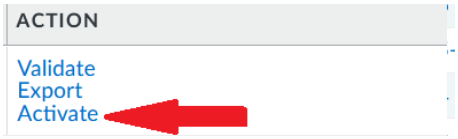
Configure an appropriate username and password.



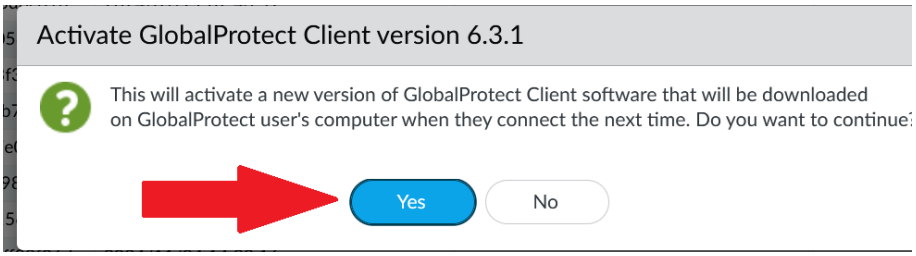
Under GlobalProtect Client, download the latest client version.



Once downloaded, click “Activate”.

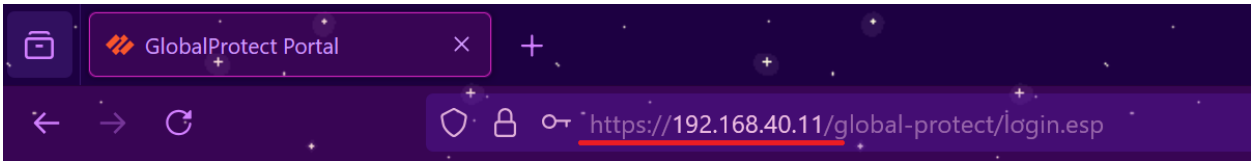


Click “Yes” to confirm.

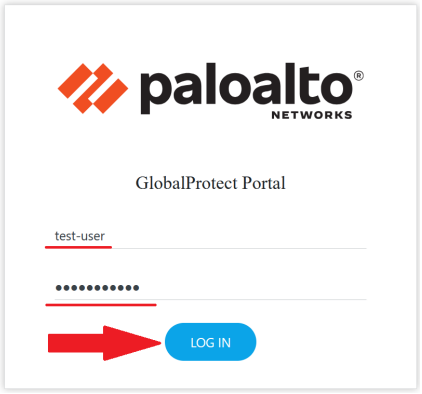


Connecting to the VPN

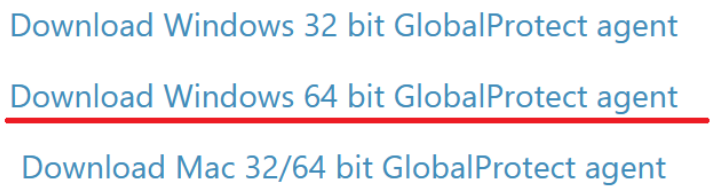
Switch to the outside computer. From a web browser, navigate to the outward-facing IP of the firewall.



Log in with the username and password created earlier.

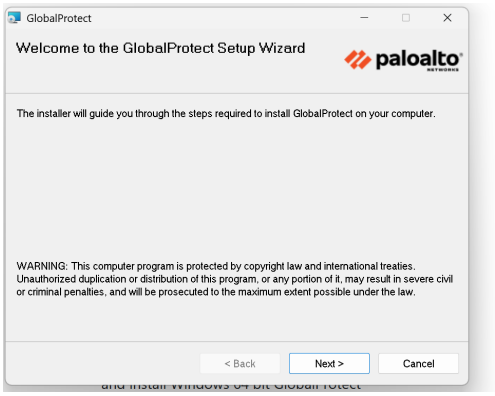


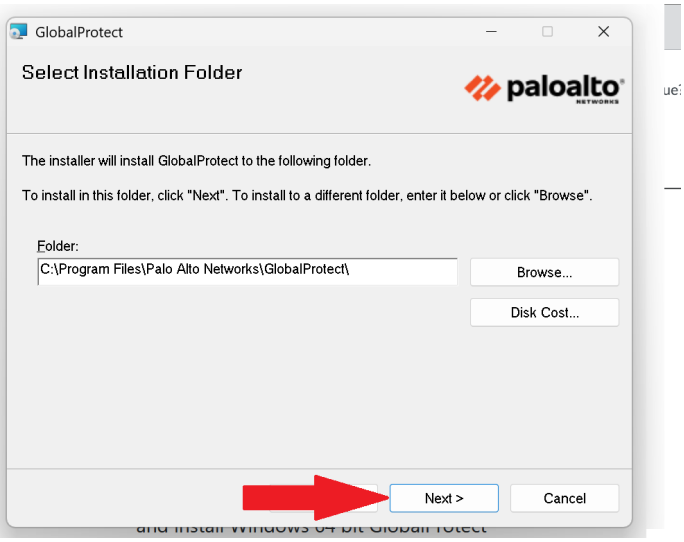
Download the appropriate GlobalProtect agent for the OS/architecture of the outside computer (in this case, Windows 64 bit).

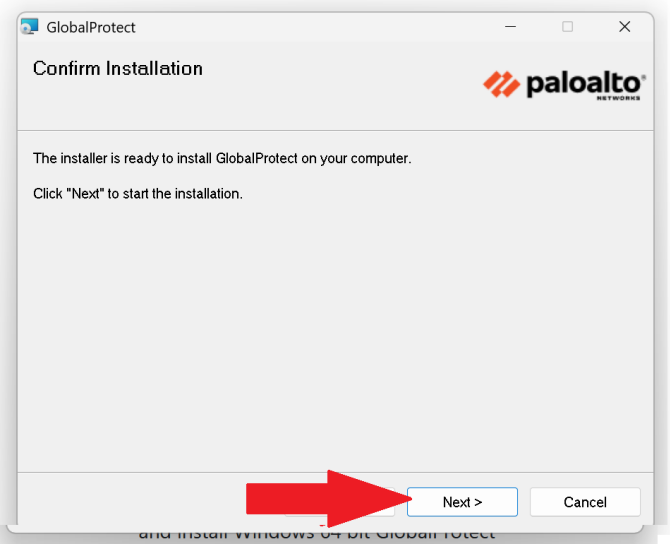


Open the downloaded installer file.

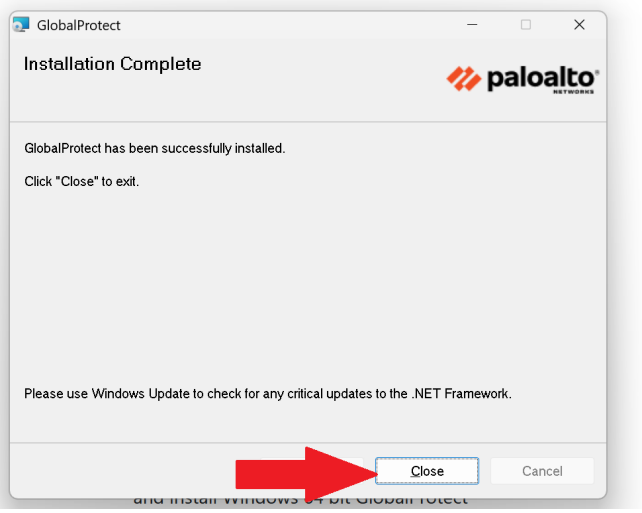
Click “Next” through the installation process.





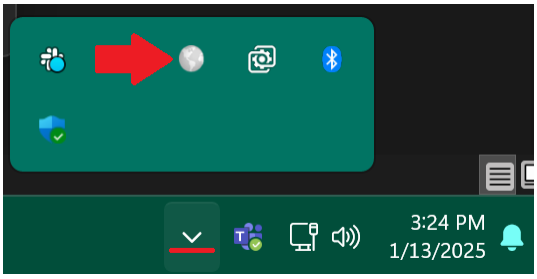


Click “Close” once the installer finishes.

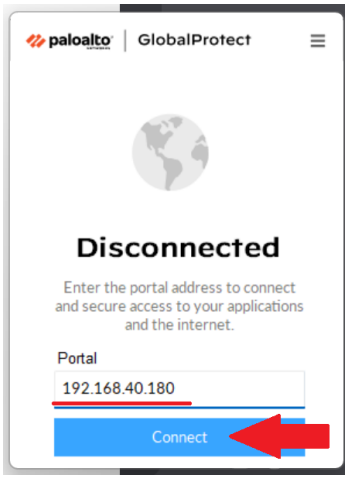


paloalto NETWORKS

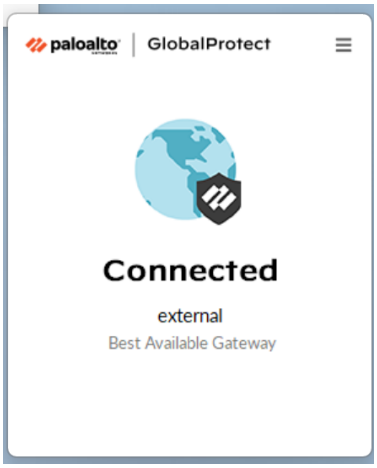
Open the GlobalProtect client from the system tray (it may be in the overflow section).



Enter the outward-facing IP of the firewall and click “Connect”.



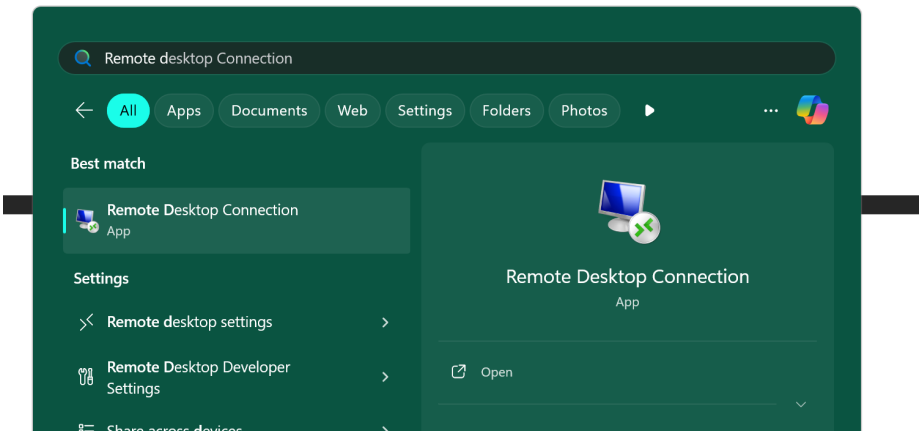
You should see the following success message:



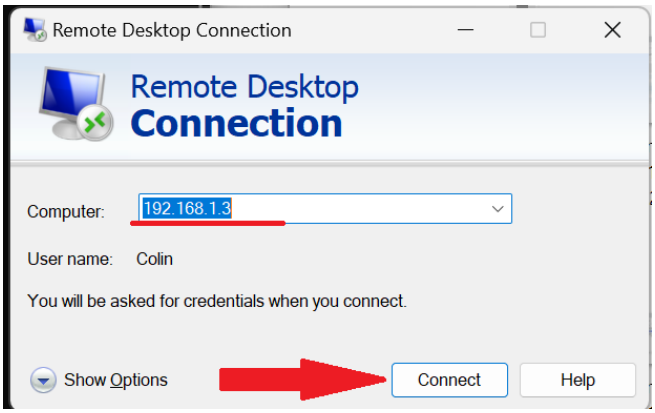
From the command prompt, run the `ipconfig` command. You should see that an address has been assigned from the IP range configured earlier.

```
C:\Users\Ram>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.2.3
```

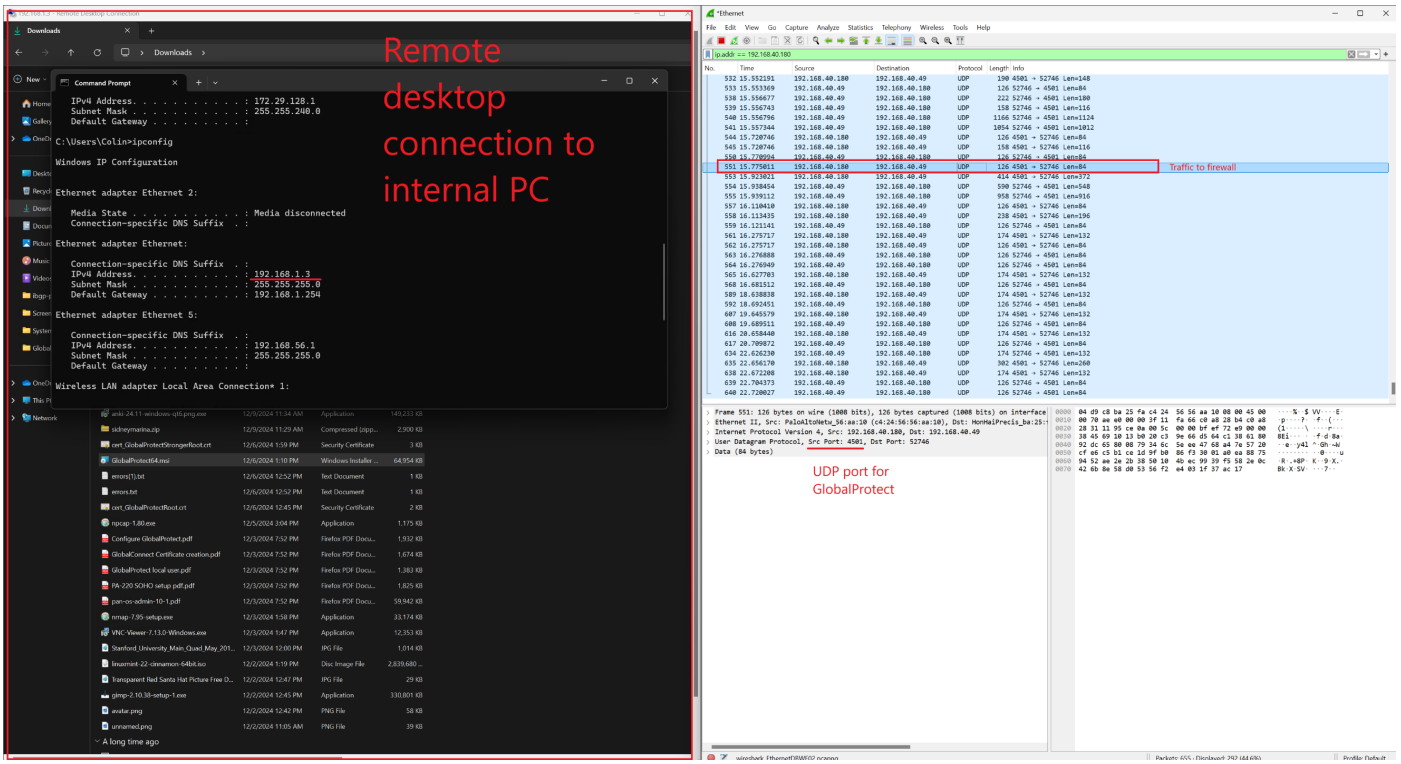
Open the remote desktop connection client.



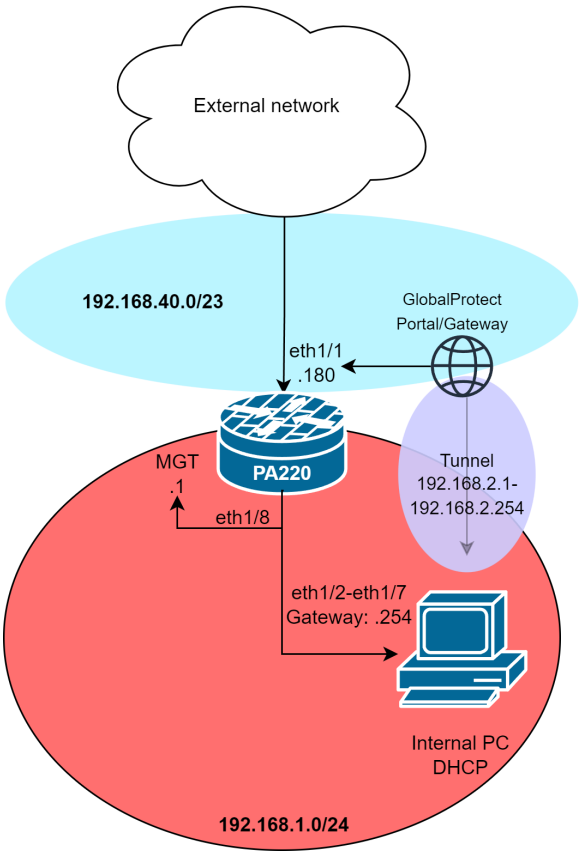
Enter the private IP of the internal computer, and click “connect”.



The remote desktop connection should establish, as shown below. By opening wireshark, you should see traffic to the firewall using port 4501 (the UDP port GlobalProtect uses).



Network Diagram



Problems

- We originally had issues with Windows RDP, which refused to connect even with both computers on the internal network. The fix for this was simply restarting both PCs.

Conclusion

To wrap up, this lab provided ample insight into the GlobalProtect VPN client and server, and how to create a secure private tunnel into a Palo Alto firewall. This information, being both niche and in-demand, is highly valued in the networking industry, and I'm very grateful to have had this opportunity to learn. Overall, this lab wasn't too difficult, and I'm very confident I could replicate this lab's setup in a real-life SOHO environment.

Signoff