



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

Colin J. Faletto, CCNA

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 countries 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.

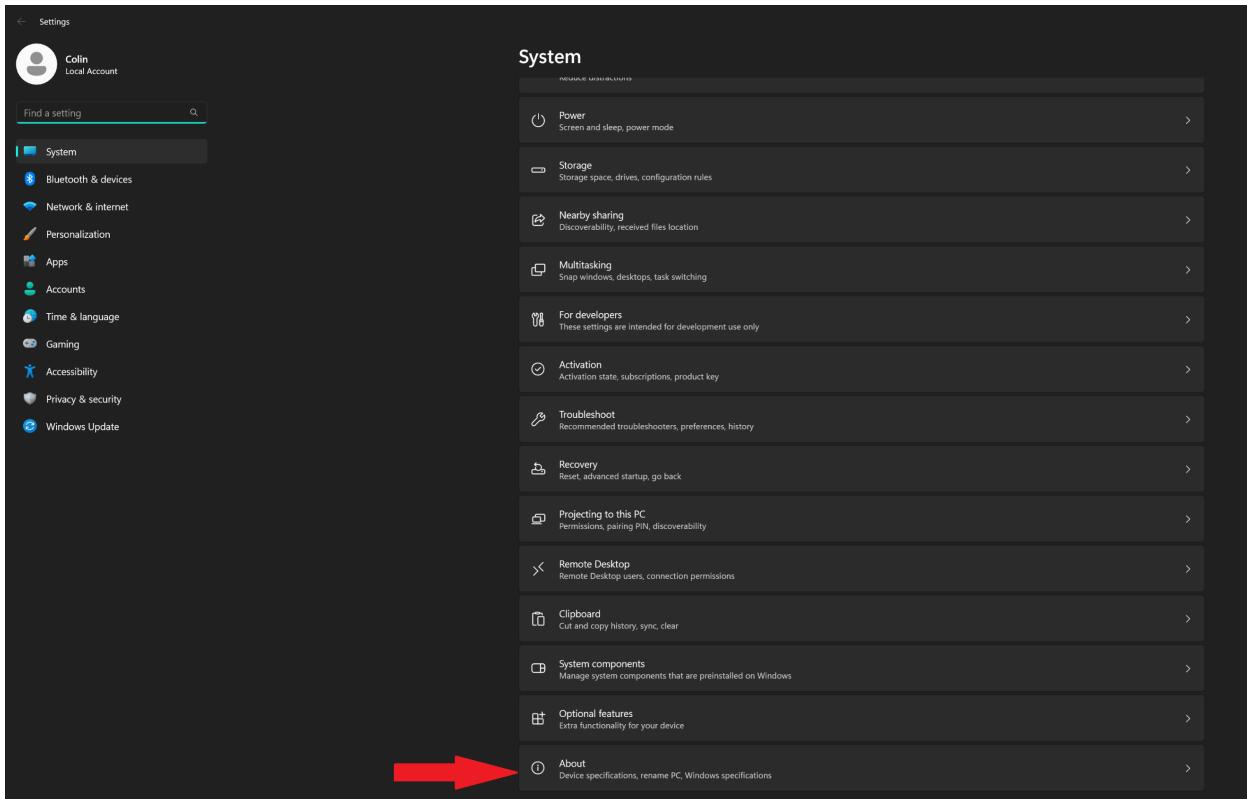
Lab Summary

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.

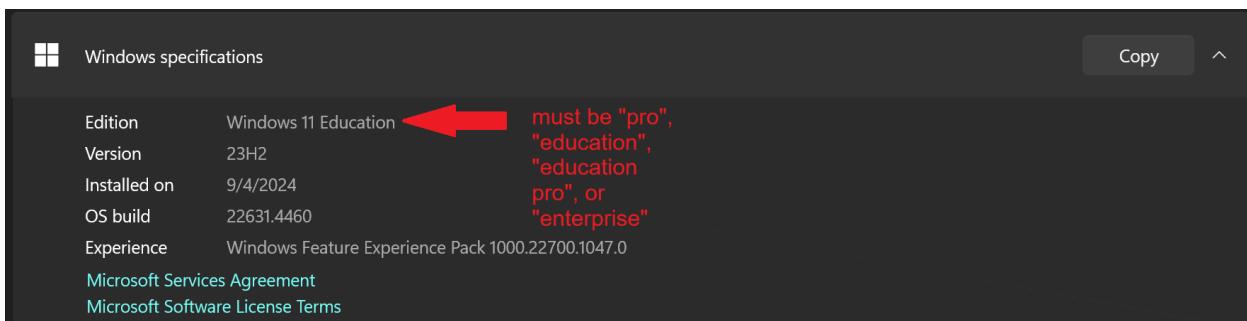
Lab Commands

Configuring Remote Desktop

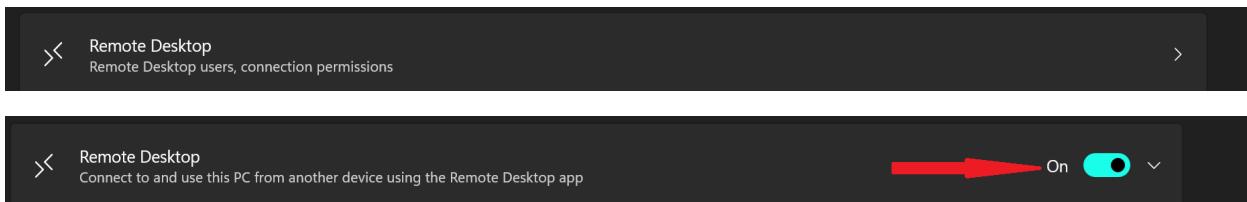
On the internal Windows PC, press (Win+I) to open the settings app. Click into the "About" section.



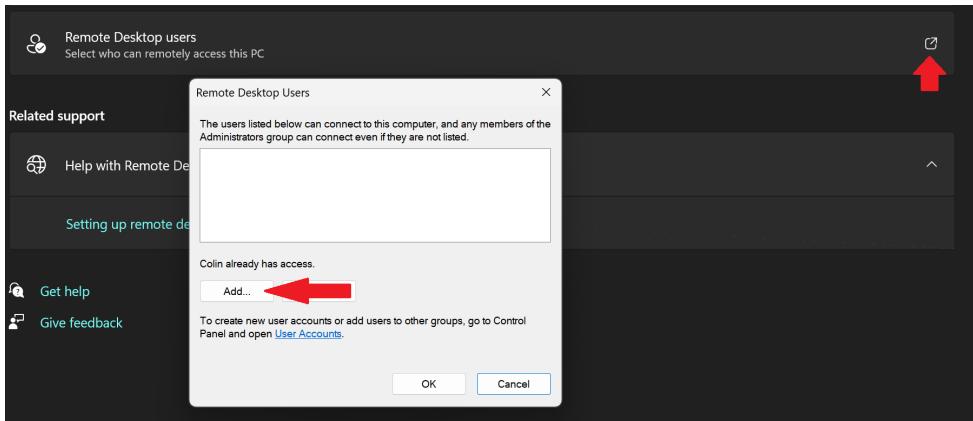
Make sure that you are running Windows 11 Pro, Education, Education Pro, or Enterprise. **Windows 11 Home doesn't support a Remote Desktop Server connection**. It can, however, be used on the external client PC.



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

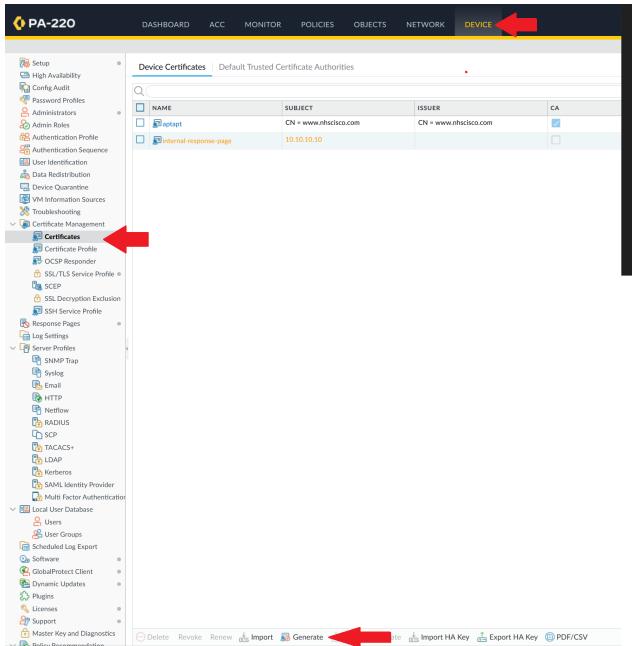


Click on “Remote Desktop Users”. If the user account you want to connect to isn’t an administrator, you will have to manually add it here using the “Add” button.



Generate Certificates

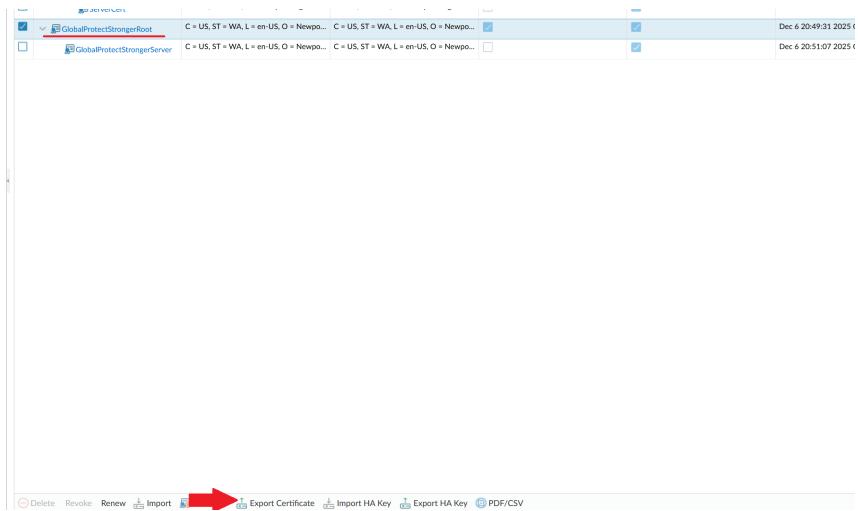
In the PA220 web interface, navigate to Device > Certificate Management > Certificates and click Generate.



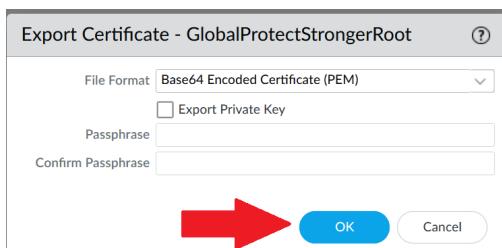
First, generate a root certificate. Give a Certificate Name and Common Name that make sense for the context, and make sure that the Certificate Authority box is checked. Under Certificate Attributes, assign appropriate values for the Country, State, Locale, Organization, and Department Fields, and make 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.

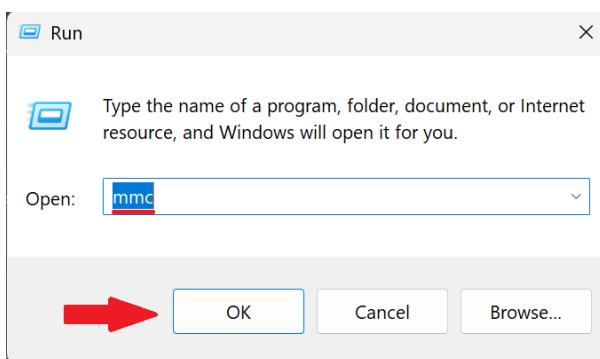


Click “OK” to confirm downloading the certificate. Make sure to note down the file’s download location.

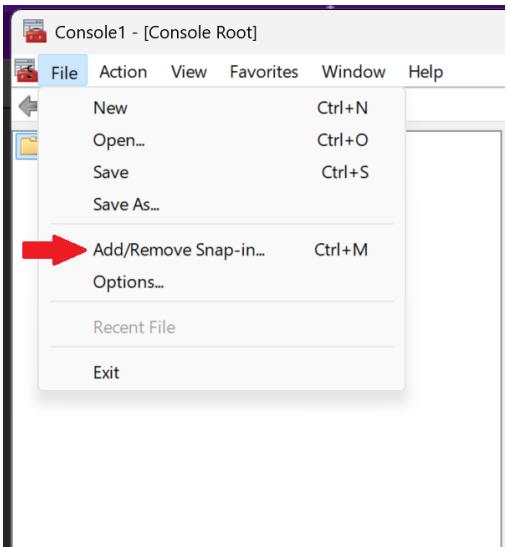


Import Certificates

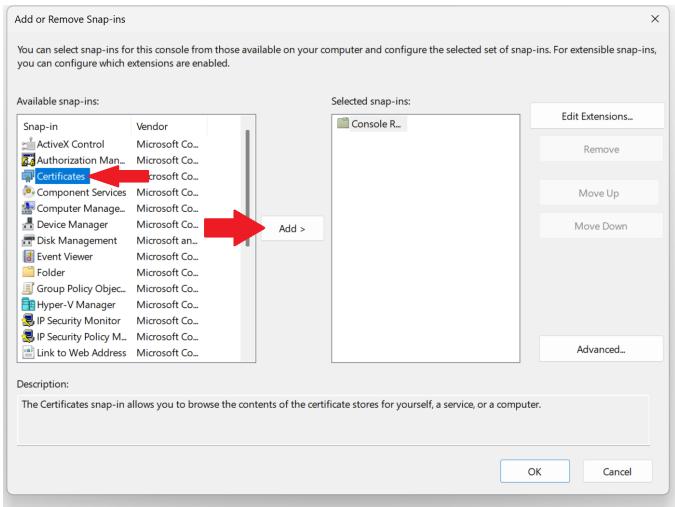
On your outside PC, open the Run dialog (Windows+R) and type “mmc”.



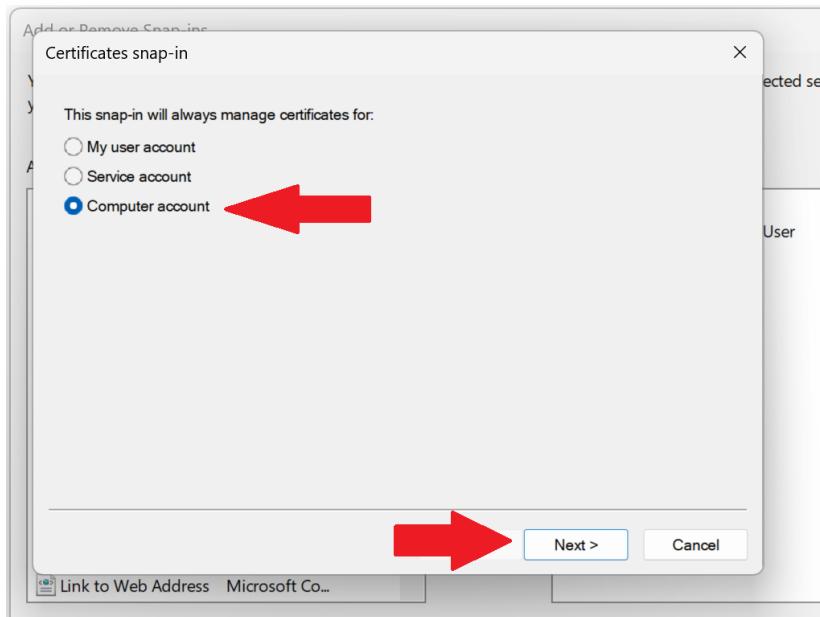
In the resulting window, click File > Add/Remove Snap-in.



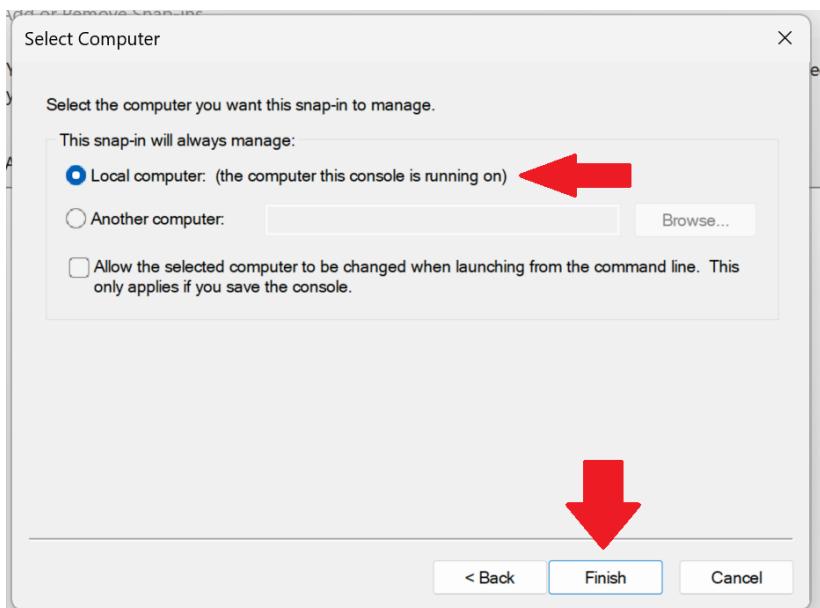
In the resulting window, click on Certificates > Add.



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



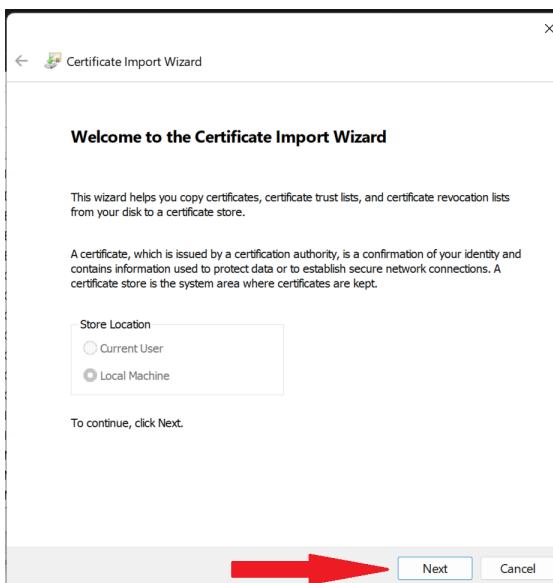
Make sure Local Computer is selected, and click Finish.



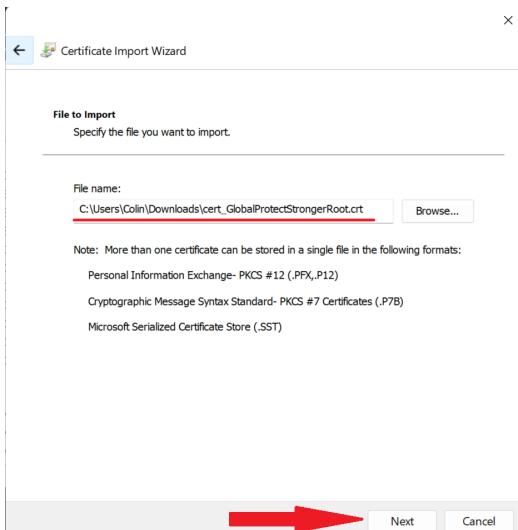
Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Term...
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authentication...	Sectigo (AAA)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authentication...	DigiCert Baltimore R...		
CCNPBigBoy	CCNPBigBoy	1/7/2024	Server Authentication	<None>		
CCNPBigBoy	CCNPBigBoy	4/4/2024	Server Authentication	<None>		
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authentication...	Certum Trusted Net...		
Certum Trusted Network CA 2	Certum Trusted Network CA 2	10/6/2046	Client Authentication...	Certum Trusted Net...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certification	8/1/2028	Client Authentication...	VerSign Class 3 Pub...		
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestamp...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time -	DigiCert CS RSA4096...		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root CA	11/9/2031	Time Stamping, Sec...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication...	DigiCert Trusted Ro...		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authentication...	DST Root CA X3		

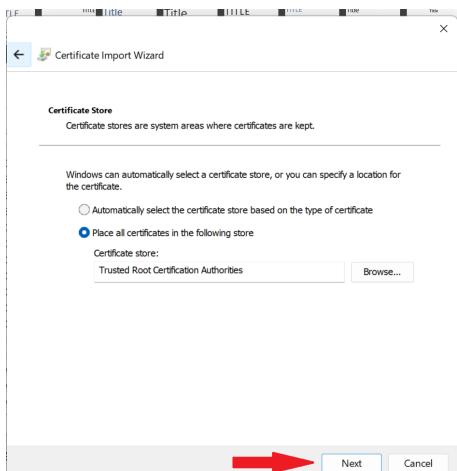
Click “Next”.



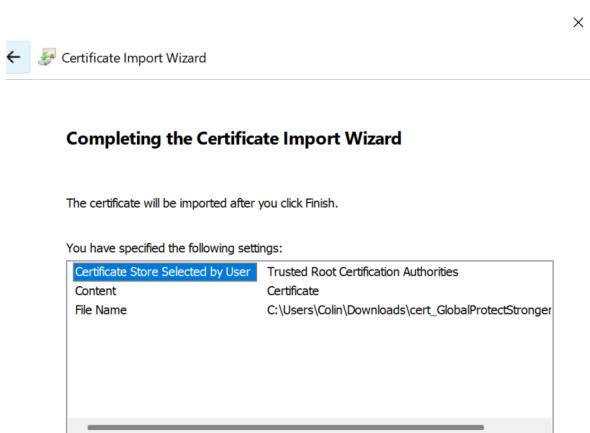
Select the certificate file downloaded earlier, then click “Next” again.



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

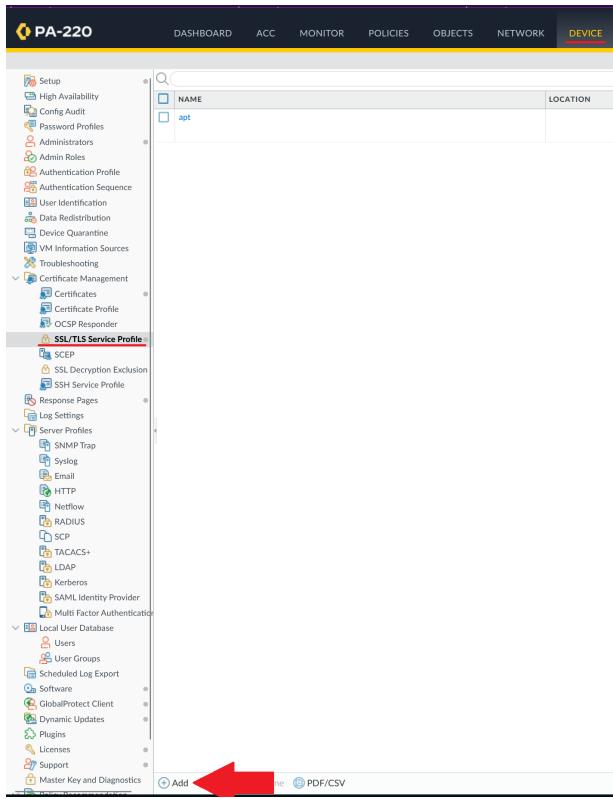


Click “Finish” to confirm the certificate import.



Firewall Configuration

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



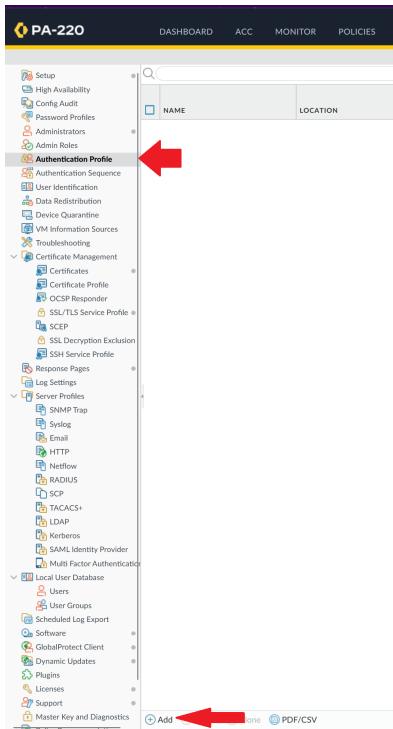
Make sure this profile uses the server certificate you set up earlier. Optionally, set the minimum TLS version to a more secure version (in this case, we used TLS 1.2)

SSL/TLS Service Profile

Name	GlobalProtect
Certificate	GlobalProtectStrongerServer
Protocol Settings	
Min Version	TLSv1.2
Max Version	Max

OK **Cancel**

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”.

Name	Local_Auth
Authentication	
Type	Local Database
User Domain	
Username Modifier	%USERINPUT%
Single Sign On	
Kerberos Realm	
Kerberos Keytab	Click "Import" to configure this field
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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

Authentication Profile

Name: Local_Auth

Authentication | Factors | **Advanced**

Allow List

ALLOW LIST

+ all

+ Add

Account Lockout

Failed Attempts: [0 - 10]

Lockout Time (min): 0

OK Cancel

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

PA-220

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Interfaces

Ethernet VLAN Loopback Tunnel SD-WAN

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
tunnel	none	default	default	Trust-L3		

Add Delete POF/CSV

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

Tunnel Interface

Interface Name: tunnel

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

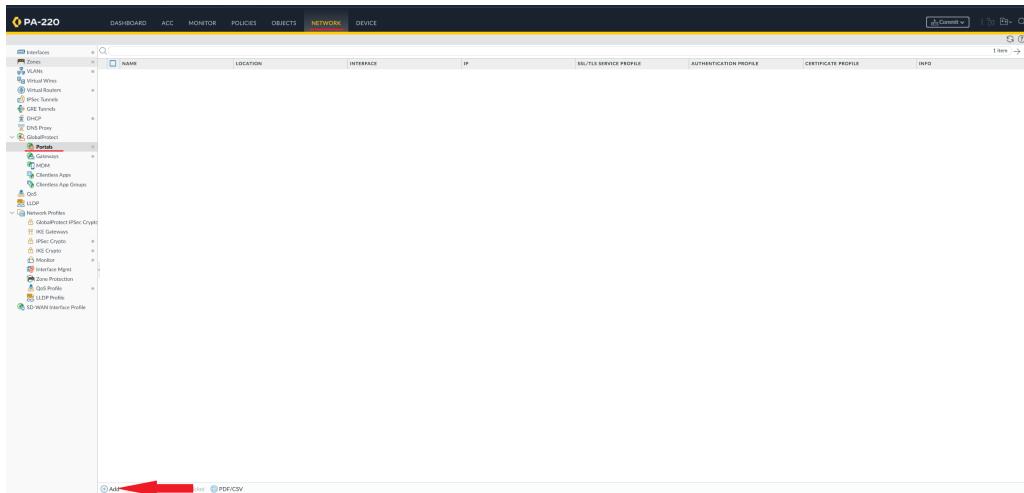
Assign Interface To

Virtual Router: default

Security Zone: Trust-L3

OK Cancel

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



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

GlobalProtect Portal Configuration

General

Name	Portal
Authentication	Network Settings
Portal Data Collection	Interface: ethernet1/1
Agent	IP Address Type: IPv4 Only
Clientless VPN	IPv4 Address: None
Satellite	Appearance
	Portal Login Page: factory-default
	Portal Landing Page: factory-default
	App Help Page: None
	Log Settings
	<input type="checkbox"/> Log Successful SSL Handshake
	<input checked="" type="checkbox"/> Log Unsuccessful SSL Handshake
	Log Forwarding: None

OK **Cancel**

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

GlobalProtect Portal Configuration

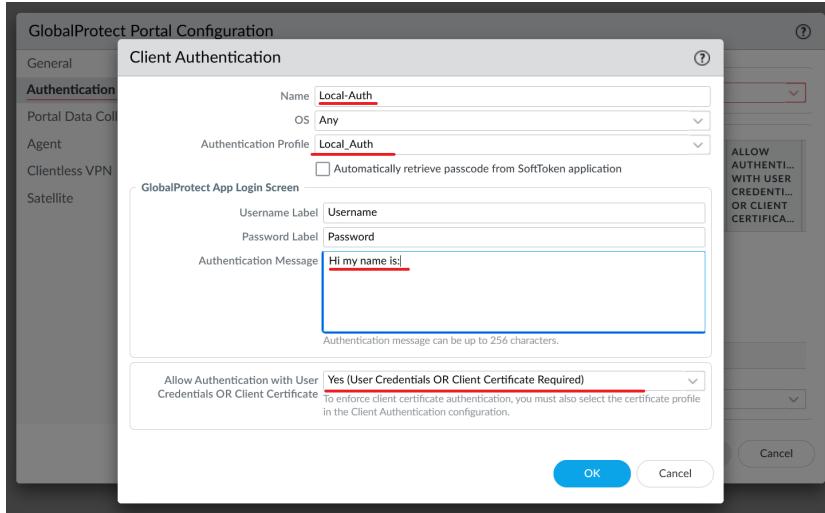
General

Authentication

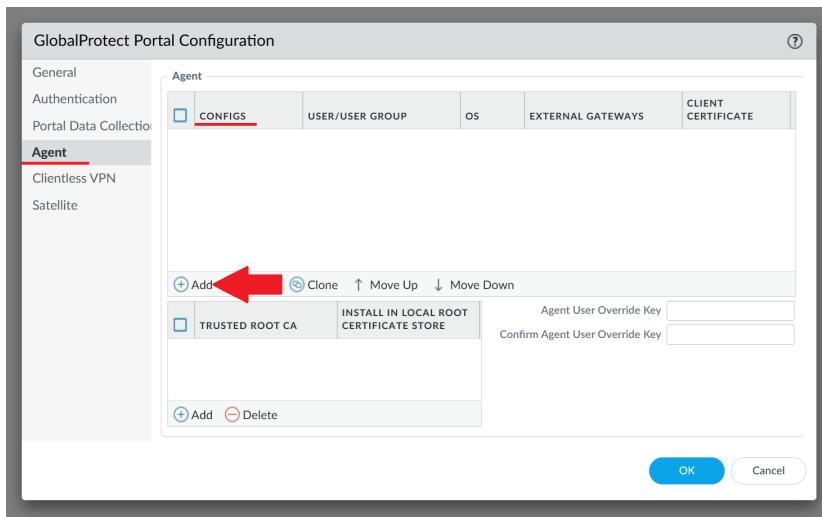
Server Authentication	SSL/TLS Service Profile: GlobalProtect																
Client Authentication	<table border="1"> <thead> <tr> <th>NAME</th> <th>OS</th> <th>AUTHENTIC... PROFILE</th> <th>AUTO RETRIEVE PASSCODE</th> <th>USERNAME LABEL</th> <th>PASSWORD LABEL</th> <th>AUTHENTI... MESSAGE</th> <th>ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...								
NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...										
<input type="button" value="Add"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>																	
Certificate Profile: None																	

OK **Cancel**

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.

Configs

Authentication | Config Selection Criteria | Internal | External | App | HIP Data Collection

Name	GP-client-conf1
Client Certificate	None
The selected client certificate including its private key will be installed on client machines.	
Save User Credentials	Yes
Authentication Override	
<input checked="" type="checkbox"/> Generate cookie for authentication override <input checked="" type="checkbox"/> Accept cookie for authentication override Cookie Lifetime Hours 24 Certificate to Encrypt/Decrypt Cookie GlobalProtectStrongerRoot	
Components that Require Dynamic Passwords (Two-Factor Authentication)	
<input type="checkbox"/> Portal <input type="checkbox"/> External gateways-manual only <input type="checkbox"/> Internal gateways-all <input type="checkbox"/> External gateways-auto discovery	
Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.	

OK **Cancel**

Under “External”, click “Add”.

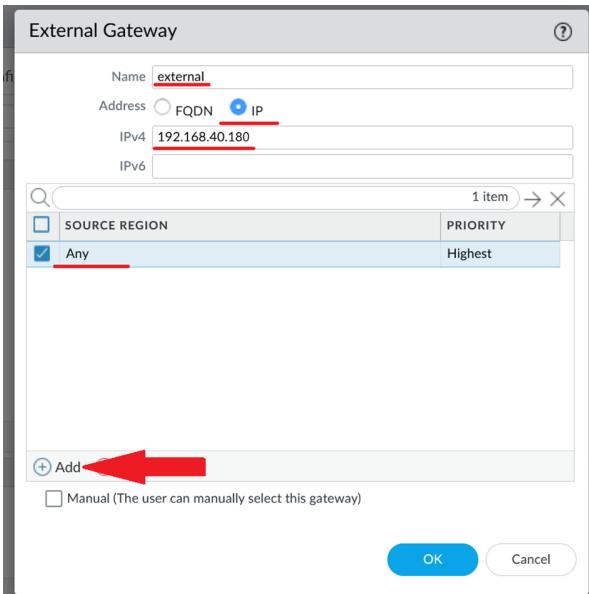
Configs

Authentication | Config Selection Criteria | Internal | **External** | App | HIP Data Collection

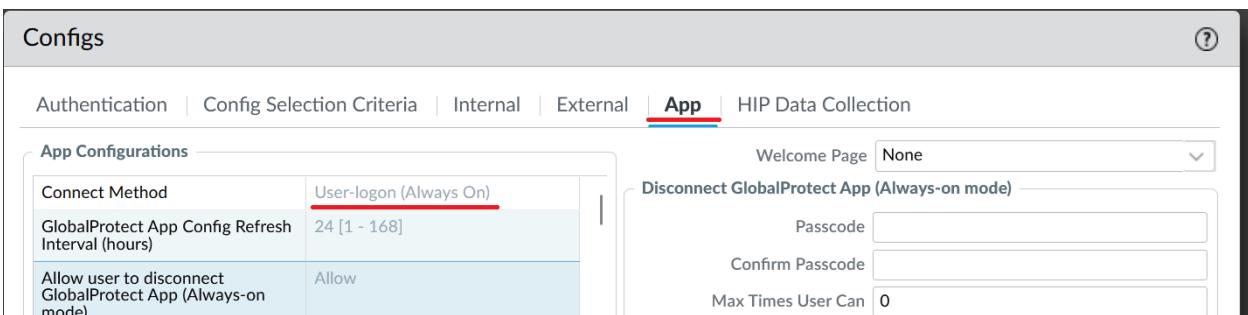
Cutoff Time (sec)	5										
External Gateways											
<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>NAME</th> <th>ADDRESS</th> <th>PRIORITY RULE</th> <th>MANUAL</th> </tr> </thead> <tbody> <tr> <td colspan="5">THIRD PARTY VPN</td> </tr> </tbody> </table>		<input type="checkbox"/>	NAME	ADDRESS	PRIORITY RULE	MANUAL	THIRD PARTY VPN				
<input type="checkbox"/>	NAME	ADDRESS	PRIORITY RULE	MANUAL							
THIRD PARTY VPN											
<input type="checkbox"/> Add <input type="checkbox"/> Delete											

OK **Cancel**

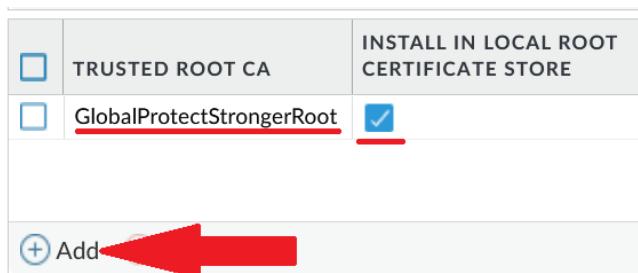
Give the gateway an appropriate name, set the mode to “IP”, and set the IP to the outward-facing IP of the gateway. Under “Source Region”, click “Add” and set it to “Any”.



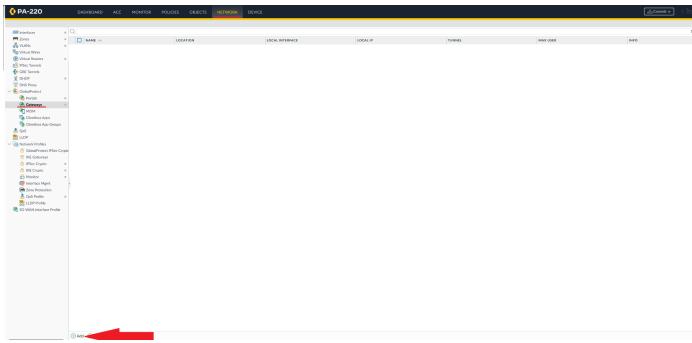
Click “OK” on the External Gateway window. Under “App”, set the connect method to “User-logon (Always On)”.



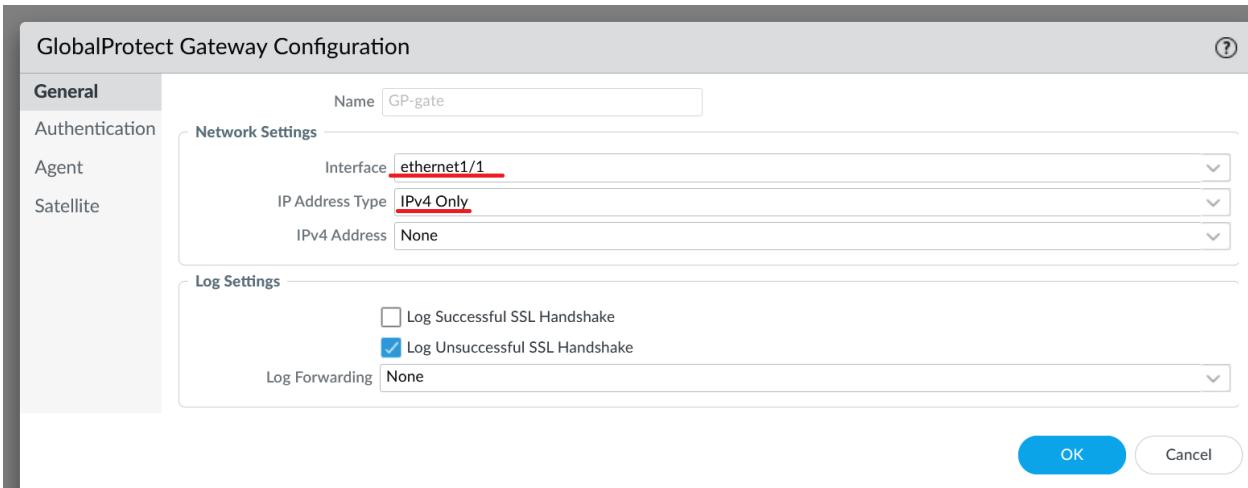
Click ok on the Configs window. Under “Trusted Root CA”, click “Add”, add the root certificate created earlier, and click “Install in local root certificate store”.



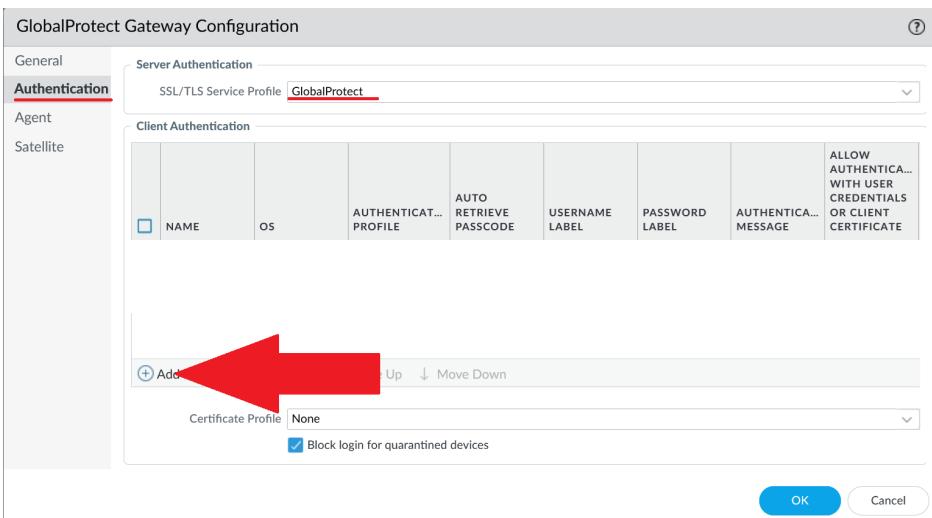
Go to Network > Gateways and click “Add”.



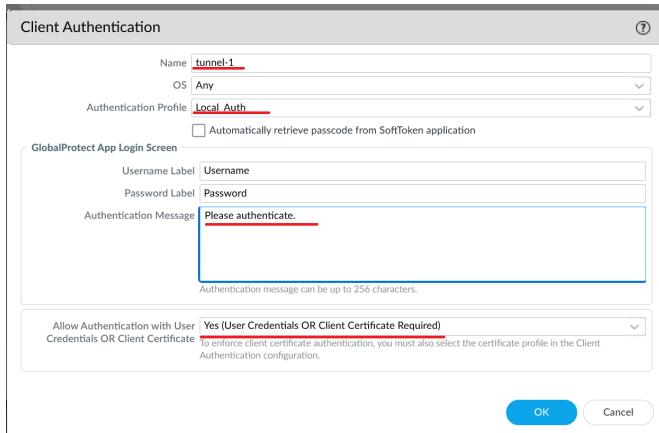
Set the interface to the outward facing interface of the firewall and leave the IP address type as “IPv4 only”.



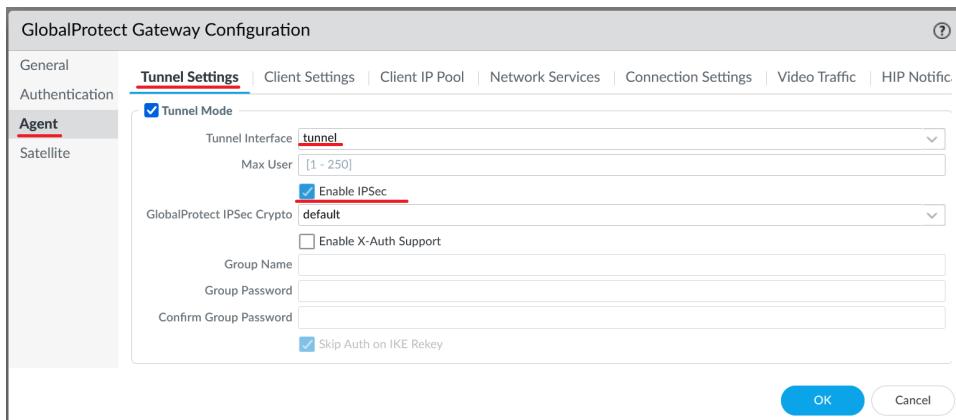
Under “Authentication”, set the SSL/TLS service profile to the profile you created earlier, and under client authentication, click “Add”.



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".

GlobalProtect Gateway Configuration

Client Settings

	Source Address		INCLUDE ACCESS ROUTE
CONFIGS	REGION	IP ADDRESS	IP POOL
USERS			
OS			
<input type="checkbox"/>			

+ Add Move Down

OK Cancel

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

Configs

Config Selection Criteria

Name	Auth-override
any	<input checked="" type="checkbox"/> Any
SOURCE USER	<input type="checkbox"/> OS

+ Add - Delete + Add - Delete

Source Address

REGION	IP ADDRESS
<input type="checkbox"/>	<input type="checkbox"/>

+ Add - Delete + Add - Delete

The configuration must match User and OS and either Region or IP Address if specified.

OK Cancel

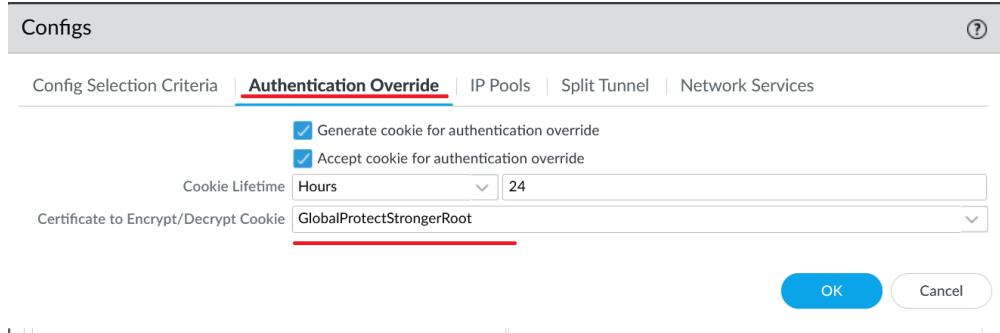
Under “Authentication Override”, set the certificate to decrypt/encrypt the cookie to the root certificate created earlier.

Configs

Config Selection Criteria | **Authentication Override** | IP Pools | Split Tunnel | Network Services

Generate cookie for authentication override
 Accept cookie for authentication override
Cookie Lifetime Hours
Certificate to Encrypt/Decrypt Cookie

OK Cancel



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.

Configs

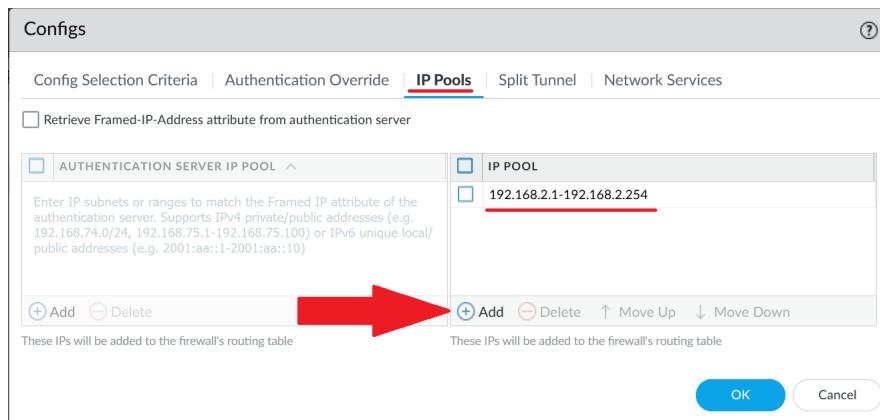
Config Selection Criteria | Authentication Override | **IP Pools** | Split Tunnel | Network Services

Retrieve Framed-IP-Address attribute from authentication server

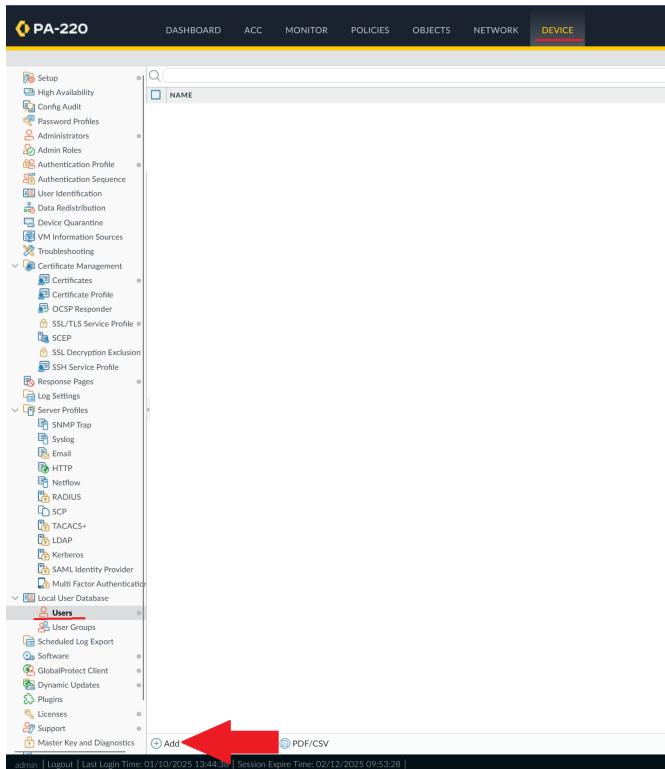
AUTHENTICATION SERVER IP POOL	IP POOL
<input type="checkbox"/>	<input type="checkbox"/> 192.168.2.1-192.168.2.254

These IPs will be added to the firewall's routing table

OK Cancel



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



Configure an appropriate username and password.

A screenshot of the 'Local User' configuration dialog box. The title bar says 'Local User'. The form contains fields for 'Name' (with 'test-user' typed in), 'Mode' (radio buttons for 'Password' and 'Password Hash' with 'Password' selected), 'Password' (containing a masked password), 'Confirm Password' (containing a masked password), and a checked 'Enable' checkbox. At the bottom are 'OK' and 'Cancel' buttons, with 'OK' being highlighted.

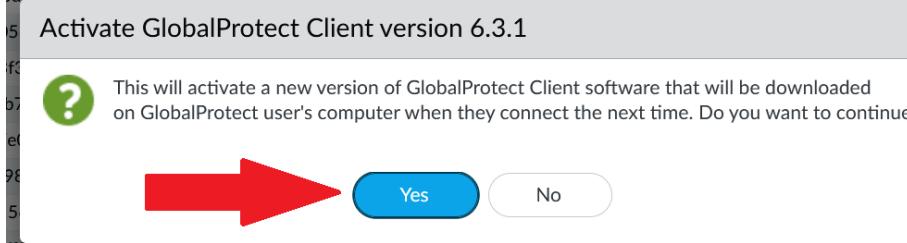
Under GlobalProtect Client, download the latest client version.

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION
6.3.1	231 MB	7/30/2023 08:00:00 +00:00	7/30/2023 08:00:00 +00:00		Download
6.3.1-1383	226 MB	8/7/2023 08:00:00 +00:00	8/7/2023 08:00:00 +00:00		Download
6.2.6	226 MB	6/18/2023 05:45:00 +00:00	6/18/2023 05:45:00 +00:00		Download
6.2.5-788	229 MB	6/16/2023 05:55:37 +00:00	6/16/2023 05:55:37 +00:00		Download
6.2.4	222 MB	5/29/2023 09:00:00 +00:00	5/29/2023 09:00:00 +00:00		Download
6.2.3	220 MB	5/24/2023 08:00:00 +00:00	5/24/2023 08:00:00 +00:00		Download
6.2.3-287	220 MB	5/20/2023 08:00:00 +00:00	5/20/2023 08:00:00 +00:00		Download
6.2.2	209 MB	6/13/2023 05:45:00 +00:00	6/13/2023 05:45:00 +00:00		Download
6.2.1	209 MB	9/18/2023 08:00:00 +00:00	9/18/2023 08:00:00 +00:00		Download
6.2.0	237 MB	9/10/2023 07:55:00 +00:00	9/10/2023 07:55:00 +00:00		Download
GlobalProtect Client	219 MB	bc7803923034619d7049913173732e...	2024/05/02 13:11:30		Download
6.1.5	211 MB	30684789408000000000000000000000...	2024/05/02 02:43:59		Download
6.1.4-720	211 MB	42027079732400000000000000000000...	2024/05/02 04:45:52		Download
SSH Service Profile	292 MB	f0453049f98180000000000000000000...	2023/11/21 08:28:57		Download
SSL/TLS Service Profile	290 MB	d0535126766548900000000000000000...	2023/08/03 07:15:29		Download
SCP	250 MB	a138ba8715900000000000000000000...	2023/03/14 07:32:48		Download
Radius Pages	124 MB	70000000000000000000000000000000...	2022/09/01 14:06:19		Download
Log Settings	229 MB	13040135100000000000000000000000...	2022/09/01 14:06:19		Download
Server Profiles	221 MB	47036533704022000000000000000000...	2024/11/01 14:21:16		Download
SNMP Trap	221 MB	50334466107523304400000000000000...	2024/07/09 06:44:54		Download
Syslog	206 MB	39098550000000000000000000000000...	2023/10/19 09:44:11		Download
Email	6.0.7	120502574655763733AC15A134976...	2023/05/21 11:19:59		Download
HTTP	289 MB	4a2b1a82393400000000000000000000...	2023/05/21 11:19:59		Download
Netflow	283 MB	4a2b1a82393400000000000000000000...	2023/05/21 11:19:59		Download
RADIUS	281 MB	b748971399304207920313494621...	2022/07/27 08:23:24		Download
6.0.0-1205	281 MB	cfa6a070948000000000000000000000...	2022/11/10 16:42:01		Download
6.0.4-26	155 MB	f02b1374059198000000000000000000...	2022/06/02 12:26:13		Download
TACACS+	152 MB	e7920304740136300000000000000000...	2022/05/04 06:37:23		Download
LDAP	132 MB	8f729200000000000000000000000000...	2022/05/04 06:37:23		Download
NetFlow	130 MB	920b45ca440400000000000000000000...	2022/05/04 06:37:23		Download
SAML Identity Provider	122 MB	920b45ca440400000000000000000000...	2022/05/04 06:37:23		Download
Multi Factor Authentication	122 MB	920b45ca440400000000000000000000...	2022/05/04 06:37:23		Download
User Database	235 MB	4e611493100000000000000000000000...	2023/07/11 07:08:37		Download
Users	100 MB	2e929391100000000000000000000000...	2022/05/24 07:38:08		Download
Scheduled Log Export	99 MB	de0ab114217400000000000000000000...	2022/03/09 11:49:56		Download
Software	99 MB	f07c5570100000000000000000000000...	2021/12/14 14:20:18		Download
GlobalProtect Client	99 MB	d742f884600977500000000000000000...	2021/11/30 09:37:03		Download
Dynamic Updates	96 MB	c548710d057100000000000000000000...	2021/08/04 13:10:27		Download
Plugins	94 MB	8aa810eadd5220a09423600000000000...	2021/06/10 14:41:40		Download
Locales	87 MB	83568830391EFC02702707D4E8C...	2021/04/06 03:46:12		Download
Support	87 MB				Download
Logs	87 MB				Download
Master Key and Diagnostics	87 MB				Download

Once downloaded, click “Activate”.

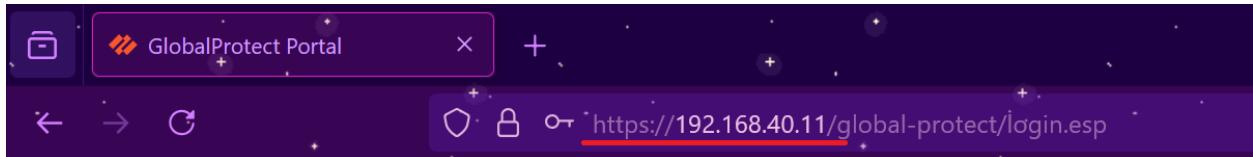


Click “Yes” to confirm.

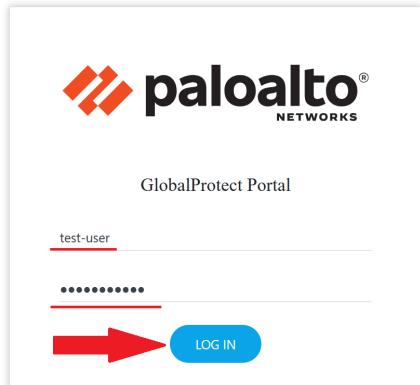


Connecting to the VPN

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).

[Download Windows 32 bit GlobalProtect agent](#)

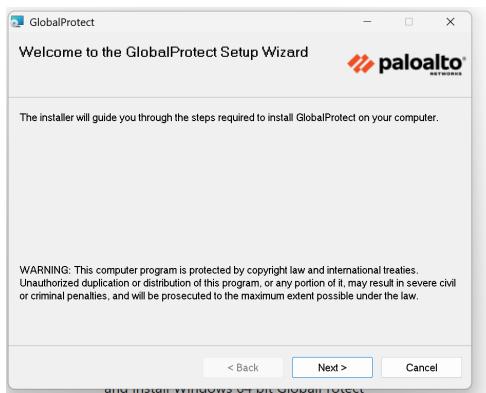
[Download Windows 64 bit GlobalProtect agent](#)

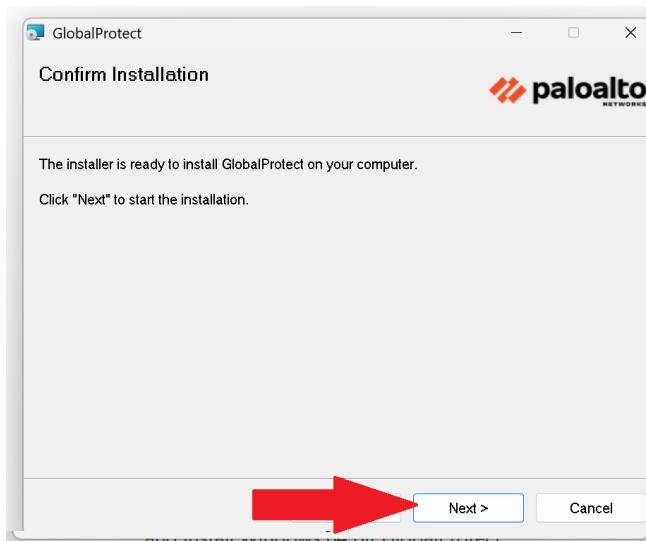
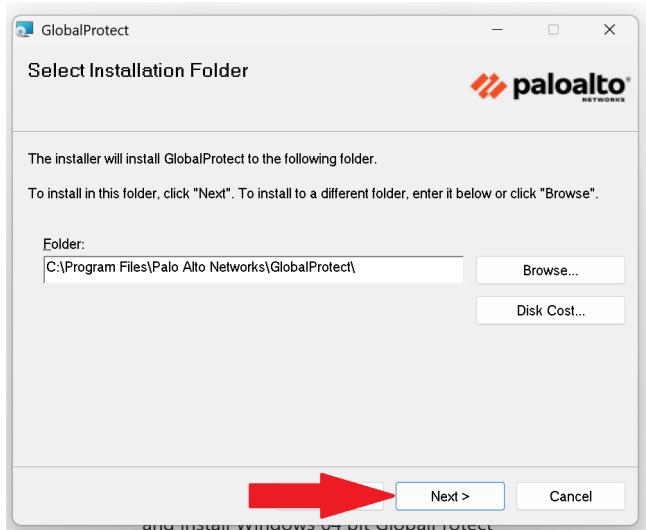
[Download Mac 32/64 bit GlobalProtect agent](#)

Open the downloaded installer file.

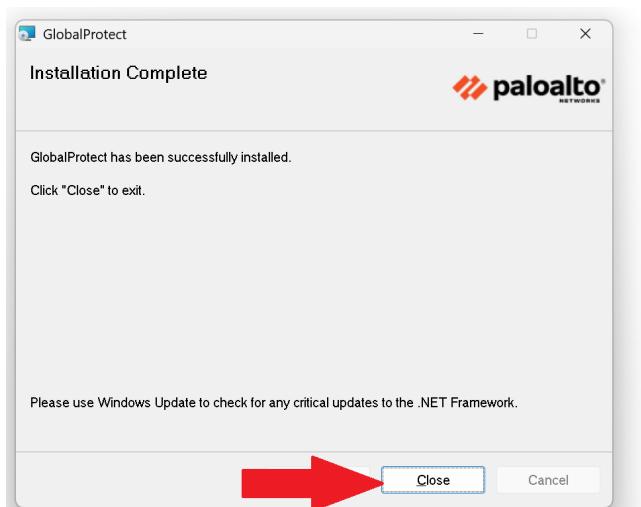


Click “Next” through the installation process.

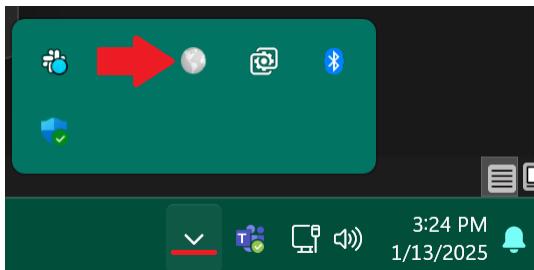




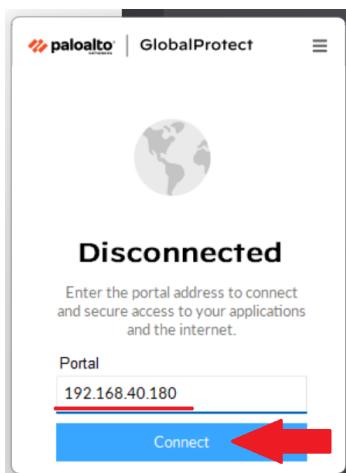
Click "Close" once the installer finishes.



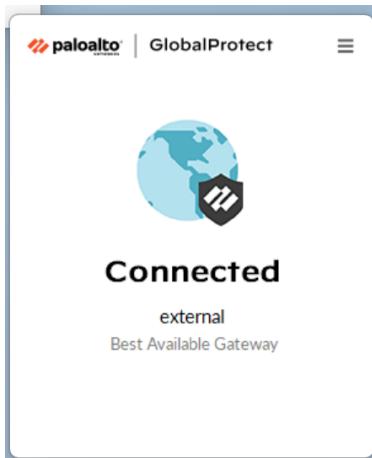
Open the GlobalProtect client from the system tray (it may be in the overflow section).



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.

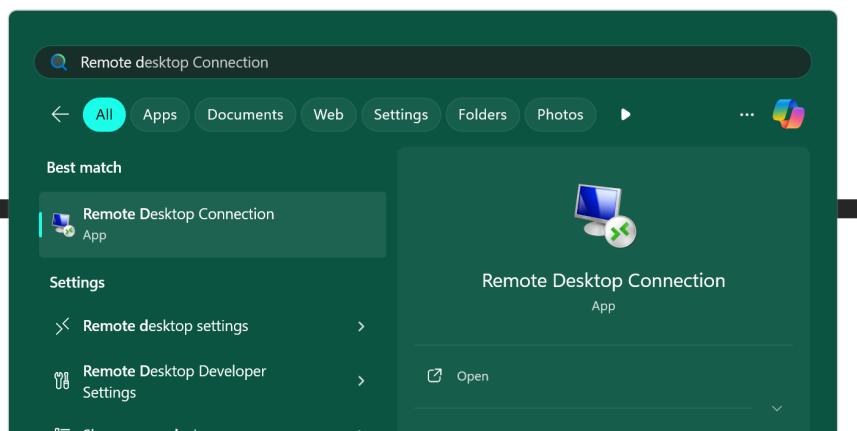
```
C:\Users\Ram>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 5:

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

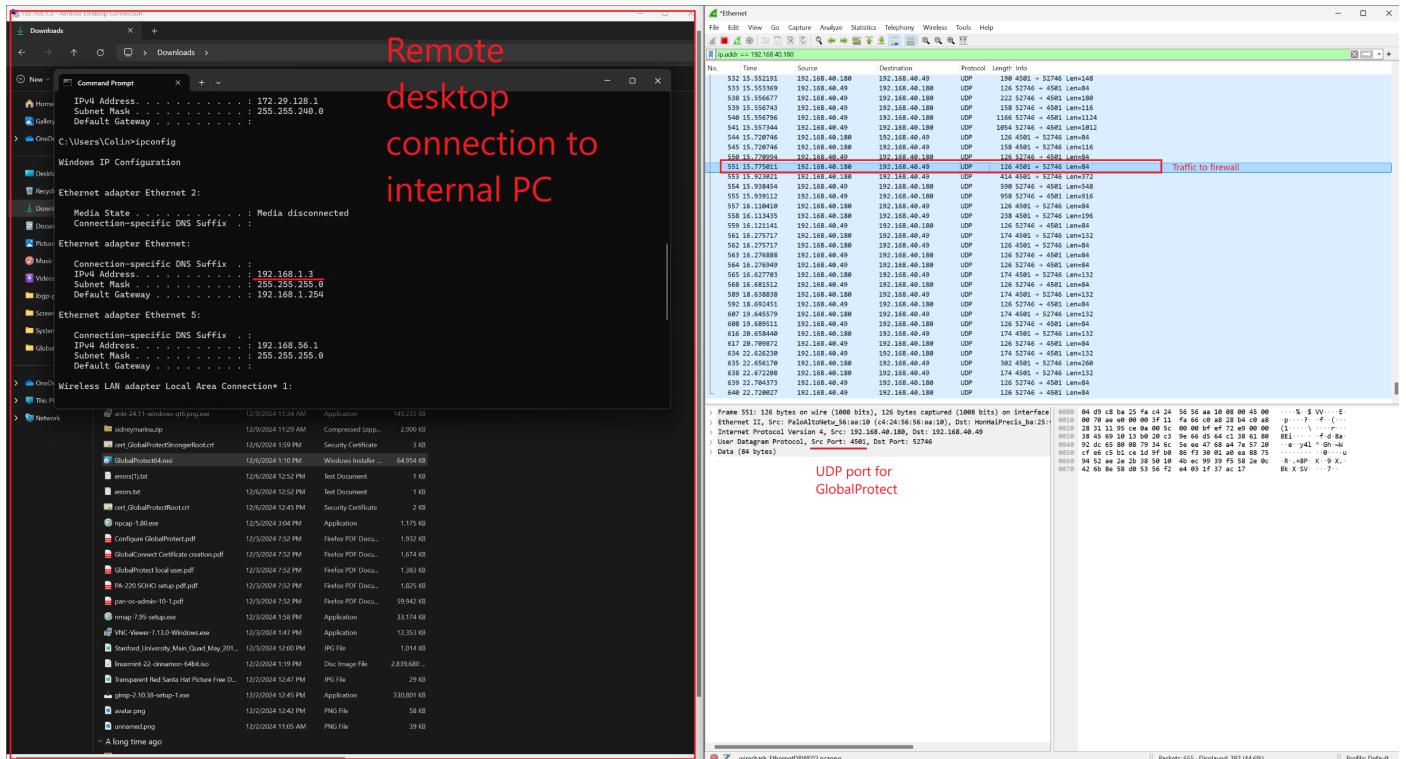
Open the remote desktop connection client.



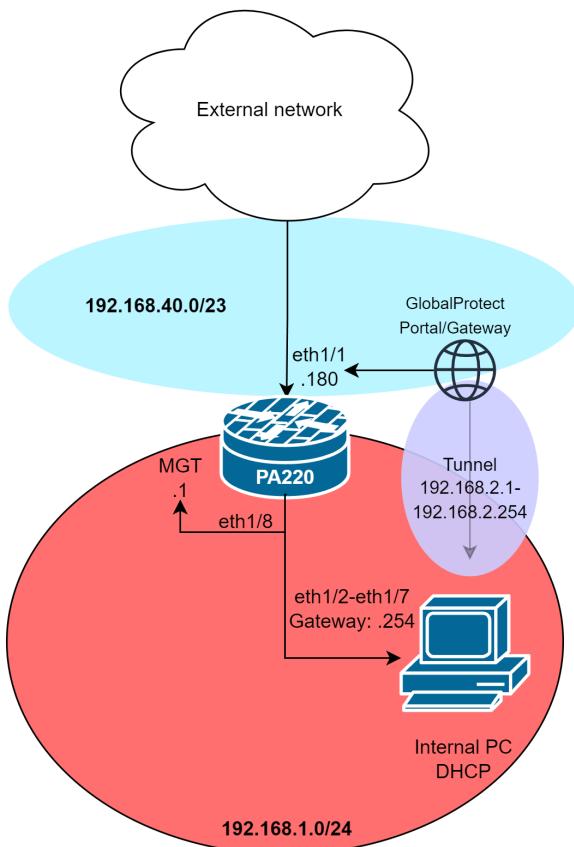
Enter the private IP of the internal computer, and click “connect”.



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.