

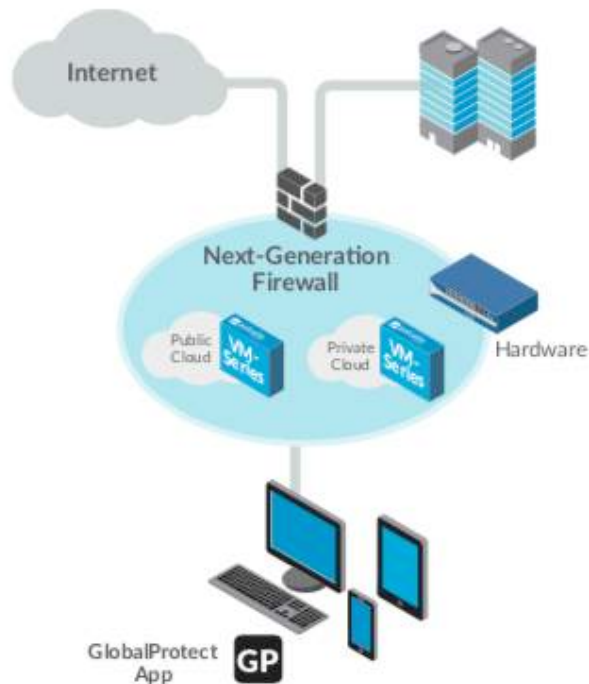
## Overview

Today's security teams must protect their data against modern threats while also providing security for users to:

1. Use the internet
2. Access applications in the data center
3. Access applications in the public cloud or SaaS

Palo Alto Networks **GlobalProtect** (GP) network security for endpoints builds upon familiar mobile security technology: the remote access VPN. The GlobalProtect Agent ensures basic levels of remote connectivity. From this base, GlobalProtect builds more advanced features that transform mobile security... The GlobalProtect solution:


- ✓ Extends NGFW to endpoints
- ✓ Delivers full traffic visibility
- ✓ Simplifies management
- ✓ Unifies policy
- ✓ Stops advanced threats



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

GlobalProtect has 3 main components:

1. GlobalProtect Portal – central point of intelligence – provides management functions for your GlobalProtect infrastructure
2. GlobalProtect Gateway(s) – internal or external - provides security enforcement for traffic from GlobalProtect agents/apps
3. GlobalProtect Clients – Windows/UWP, Mac/iOS, Android/Chromebook, Linux

-  **TIP** – A GlobalProtect implementation requires at least one portal and one gateway.
- ✓ The portal and gateway can be configured on the same firewall.
  - ✓ In the simplest configuration, a single firewall is configured to serve portal and gateway services from the same IP address, which provides end users with VPN access to the internal networks with a minimum of configuration.
  - ✓ If the portal and gateway share an IP address, only one certificate is needed for the firewall.
  - ✓ The portal can act as a certificate authority (CA) for the system (using a self-signed or imported subordinate issuing a CA certificate within the portal), or customers can generate certificates using their own CAs. The portal, gateways, and agents must use certificates signed by the same CA.

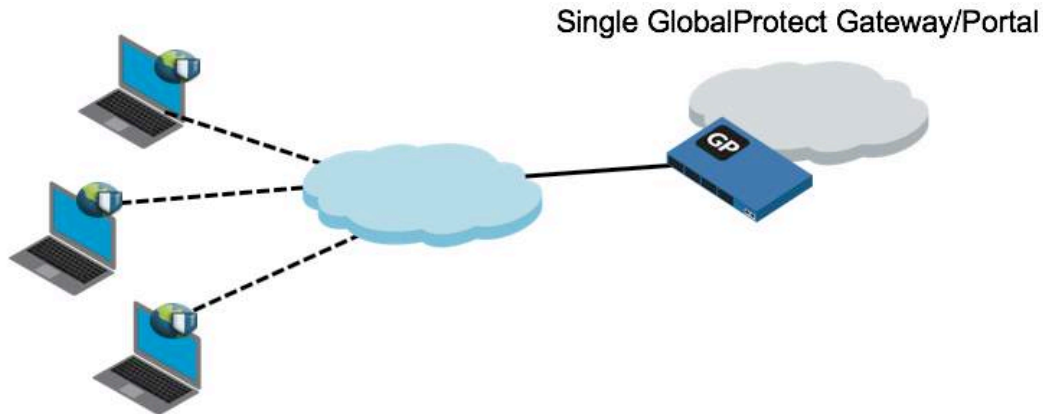
There are some things you can do with GlobalProtect that do not require additional licensing, and there are some advanced GP features that require a GP subscription. The table below shows which features require the subscription.

Subscription Required?	Feature
No	Single, external gateway (Windows and Mac)
No	Single or multiple internal gateways
No	Multiple external gateways
Yes	HIP Checks
Yes	Mobile app for iOS endpoints, Android endpoints, Chromebooks, and Windows 10 UWP endpoints
Yes	IPv6 support
Yes	Linux agent
Yes	Clientless VPN

## Objective

In this lab, we will learn how to implement GlobalProtect for secure remote access, using a single portal / single gateway, a self-signed certificate and local users.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



## Tools

- ✓ Palo Alto firewall
- ✓ Windows or Mac computer with Internet access

## Target Devices

One or more of the following devices may be used as a GlobalProtect Portal or Gateway:

- ✓ Palo Alto hardware appliance firewall
- ✓ Palo Alto VM-series firewall

## Lab Setup

Our lab setup consists of a Palo Alto firewall running PANOS 8.0.11-h1 and 2 remote access clients (1 Windows, 1 Mac) connected outside of the lab firewall (not on an inside zone). It is assumed that the Palo Alto firewall is already deployed on the network and the initial setup has been accomplished, including a layer-3 interface configured with a static public IP address. It is also assumed that the intrazone-default security rule is in effect, permitting all intra-zone traffic.

## Lab Configuration Steps

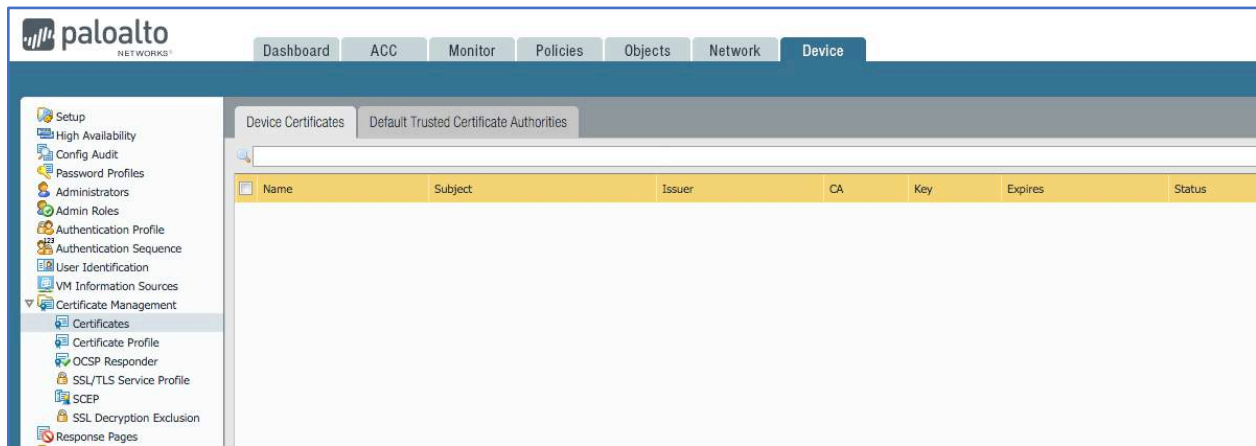
### 1. Prepare the firewall for GlobalProtect - Certificates

#### a. Purpose


GlobalProtect needs multiple certificates, one for the portal and one for each gateway. These certificates are typically signed by a common CA certificate. In this lab we will combine the portal and gateway certificates because these GP functions are combined on the same IP address.

#### b. Location

Certificates are configured in the *Device* tab under *Certificate Management - Certificates* in the left menu and the *Device Certificates* subtab.



#### c. Create CA certificate and GP portal/gateway certificate

- i. Click the Generate button  at the bottom to create a CA certificate.
- ii. Enter a relevant Certificate Name and Common Name, leave Signed By blank, and select the Certificate Authority checkbox.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

Generate Certificate

Certificate Type ☒ Local ☐ SCEP

Certificate Name GlobalProtect-CA

Common Name GlobalProtect-CA

IP or FQDN to appear on the certificate

Signed By

☒ Certificate Authority

OCSP Responder

**Cryptographic Settings**

Algorithm RSA

Number of Bits 2048

Digest sha256


Expiration (days) 365

**Certificate Attributes**

Type	Value
------	-------

+ Add - Delete

Generate Cancel

- iii. Click the Generate button
- iv. Click **OK** to dismiss the successful status window.
- v. Click the Generate button  at the bottom to create another certificate (for GP Portal and Gateway).
- vi. Enter a relevant Certificate Name. Use your firewall outside IP address for the Common Name. Click the dropdown next to Signed By and select the CA certificate that you created in the previous step. Leave the Certificate Authority checkbox unchecked.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

**Generate Certificate**

Certificate Type: ☒ Local ☐ SCEP

Certificate Name:

Common Name:   
IP or FQDN to appear on the certificate

Signed By:

☐ Certificate Authority

OCSP Responder:

**Cryptographic Settings**

Algorithm:

Number of Bits:

Digest:

Expiration (days):

**Certificate Attributes**

Type	Value
------	-------

- vii. Click the Generate button
- viii. Click **OK** to dismiss the successful status window. Your 2 certificates should look something like this in the list of device certificates:

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm
GlobalProtect-CA	CN = GlobalProtect-CA	CN = GlobalProtect-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 9 15:38:33 2019 GMT	valid	RSA
gp-portal-gw	CN = 50.63.202.9	CN = GlobalProtect-CA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Aug 9 15:53:43 2019 GMT	valid	RSA

**TIP** – In a live production environment, as a Certificate Authority, the firewall would need to respond to revocation queries. Not covered in this lab, an OCSP Responder is configured in Device – Certificate Mgt – OCSP Responder (a reference URL is provided at the end of the lab).

**paloalto**

Dashboard ACC Monitor Policies Objects Network Device

Setup  
High Availability  
Config Audit  
Password Profiles  
Administrators  
Admin Roles  
Authentication Profile  
Authentication Sequence  
User Identification  
VM Information Sources  
Certificate Management  
Certificates  
Certificate Profile  
OCSP Responder  
SSL/TLS Service Profile  
SCEP

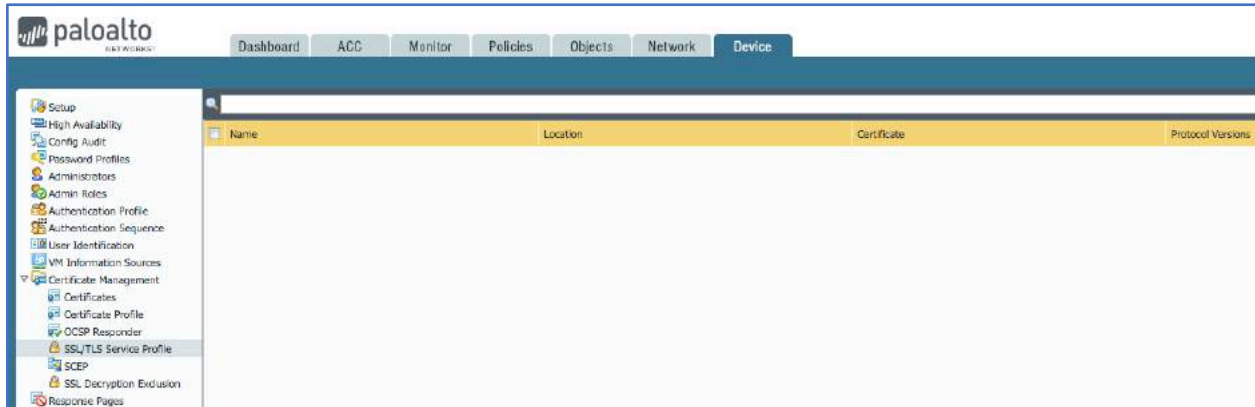
**OCSP Responder**


Name:

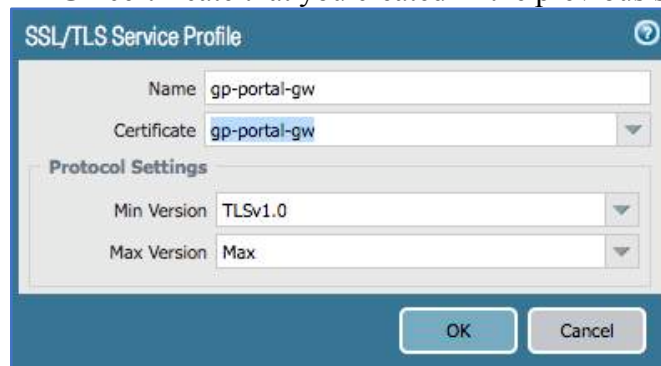
Host Name:   
Enter FQDN, IP, or IP:port address

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- d. Associate the GP certificate with an SSL-TLS Service Profile - configured in the **Device** tab under **Certificate Management – SSL/TLS Service Profile** in the left menu.



- Click the Add button  at the bottom to create an SSL/TLS Service Profile.
- Enter a relevant Name. Click the dropdown next to Certificate and select the GP certificate that you created in the previous step.



- Click **OK** to save the setting

## 2. Configure GlobalProtect User Authentication

### a. Purpose

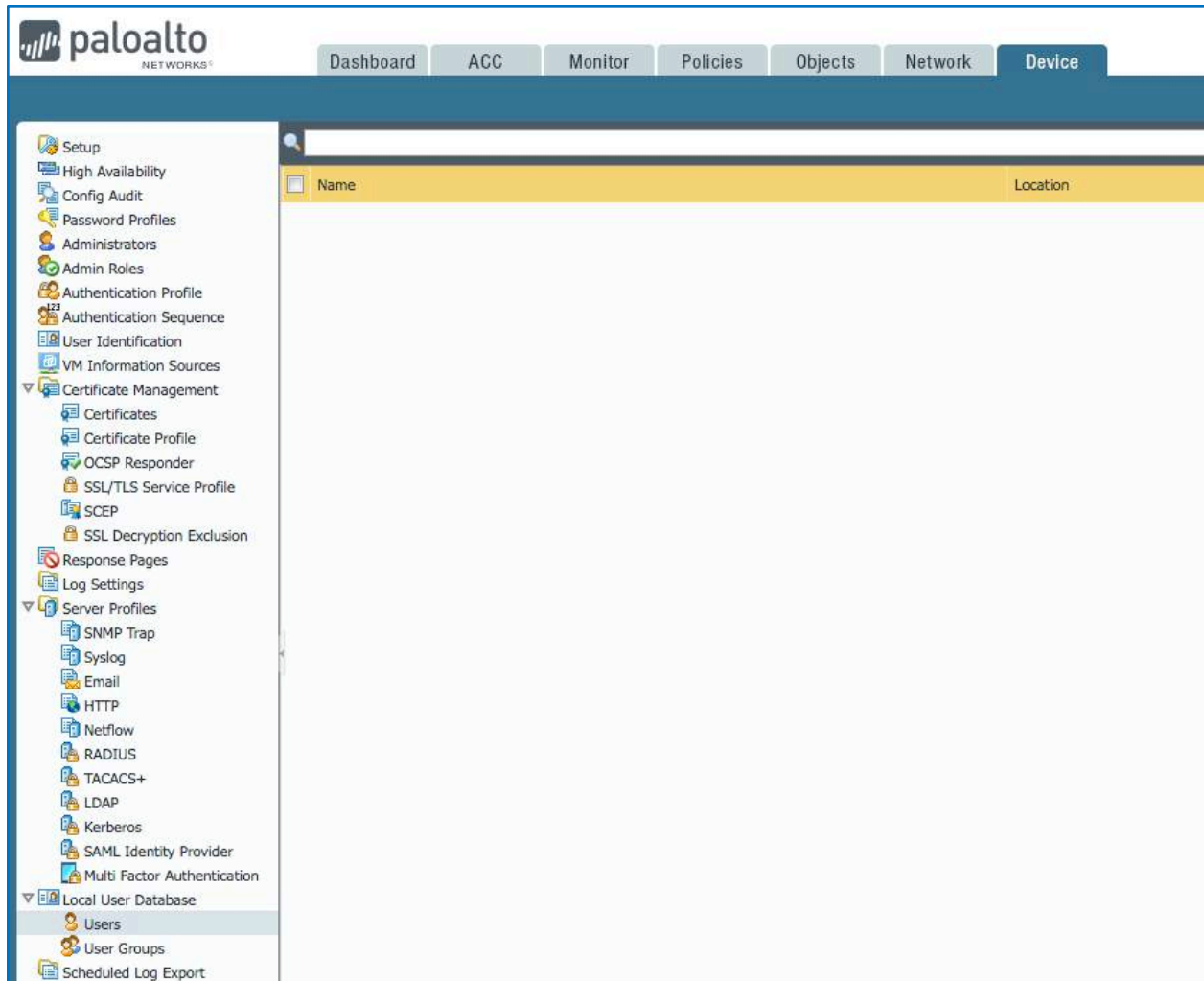
To authenticate users for access to corporate networks... In a production enterprise environment, it's recommended to configure LDAP authentication, preferably coupled with Multi-Factor Authentication. This lab uses local users.

### b. Location


Local users are configured in the **Device** tab under **Local User Database – Users** in the left menu.



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



### c. Create Local Users

- i. Click the Add button  at the bottom to create a local user.
- ii. Populate the user name and password fields, and click **OK**.

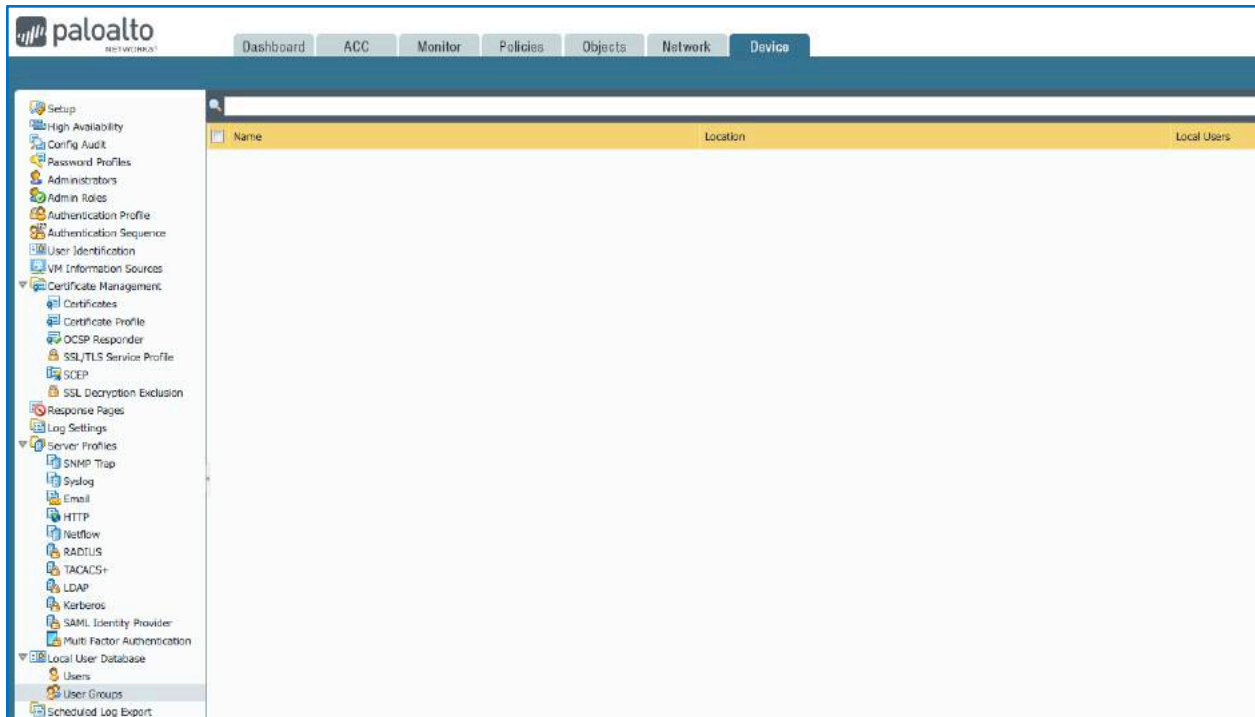
A 'Local User' dialog box is shown. It has a title bar with a question mark icon. Inside, there is a 'Name' field with the text 'gpuser1'. Below it is a 'Mode' section with two radio buttons: 'Password' (selected) and 'Password Hash'. There are two password fields: 'Password' and 'Confirm Password', both containing masked characters. At the bottom, there is a checked checkbox labeled 'Enable' and two buttons: 'OK' and 'Cancel'.



- iii. Repeat this step and create a 2<sup>nd</sup> local user.

### d. Create a Local User Group - configured in the *Device* tab under *Local User Database* – *User Groups* in the left menu.



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



- i. Click the Add button  at the bottom to create a local user group.
- ii. Enter a relevant group name.
- iii. Click the Add button  and select a user that you created in the previous step (twice).




- iv. Click **OK** to save the setting. Your new local user group should look something like this in the list of user groups:


Name	Location	Local Users
gp-users		gpuser1 gpuser2

- e. Associate the Local User Group with an **Authentication Profile** - configured in the **Device** tab under **Authentication Profile** in the left menu.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



- i. Click the Add button  at the bottom to create an authentication profile.
- ii. Enter a relevant Name. Click the dropdown next to **Type** and select **Local Database**.

- iii. Click the **Advanced** tab.
- iv. Click the Add button  under the Allow List section and select the local user group that you created in the previous step.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- v. Click **OK** to save the setting. Your new authentication profile should look something like this in the list of authentication profiles:

Name	Location	Lockout		Allow List	Authentication	Server Profile	Authentication Factors
		Failed Attempts (#)	Lockout Time (min)				
gp-auth		0 (default)	0 (default)	gp-users	Local		

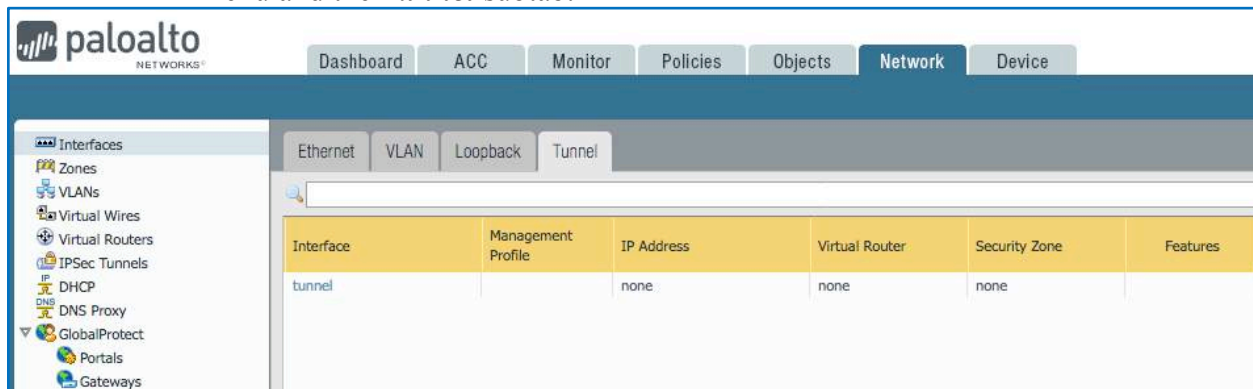
### 3. Configure an External GlobalProtect Gateway and Tunnel Interface

#### a. Purpose

External GP Gateways provide security enforcement and VPN access for remote users. The gateway requires a tunnel interface for external clients.

#### b. Location

Tunnel interfaces are configured in the **Network** tab under **Interfaces** in the left menu and the **Tunnel** subtab.




#### c. Create Tunnel Interface

- Click the Add button **+ Add** at the bottom to create a tunnel interface.
- The read-only Interface Name is set to *tunnel*. In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.

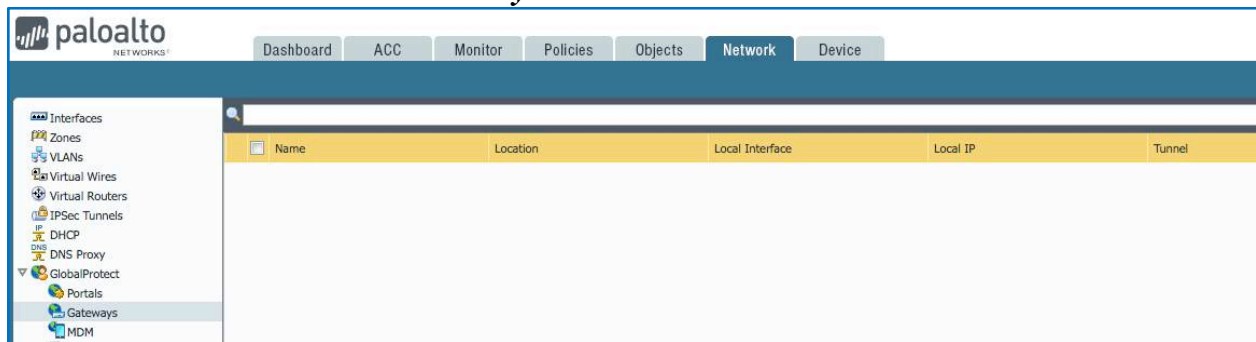
For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>


- iii. Under the **Config** tab, click the dropdown next to **Virtual Router** and select your default router.
- iv. Click the dropdown next to **Security Zone** and select your inside/trust zone.
- v. Click **OK** to save the setting. Your new tunnel interface should look something like this in the list of tunnel interfaces:


Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features
tunnel.100		none	default-vr	inside	

 **TIP** - For more granular control over GP client access into the internal network, create an independent zone for GP-VPN, just note that an additional security rule will be needed to permit traffic flow between the GP-VPN zone and your primary inside/trust zone.

- d. **Configure the External Gateway** - configured in the **Network** tab under **GlobalProtect – Gateways** in the left menu.




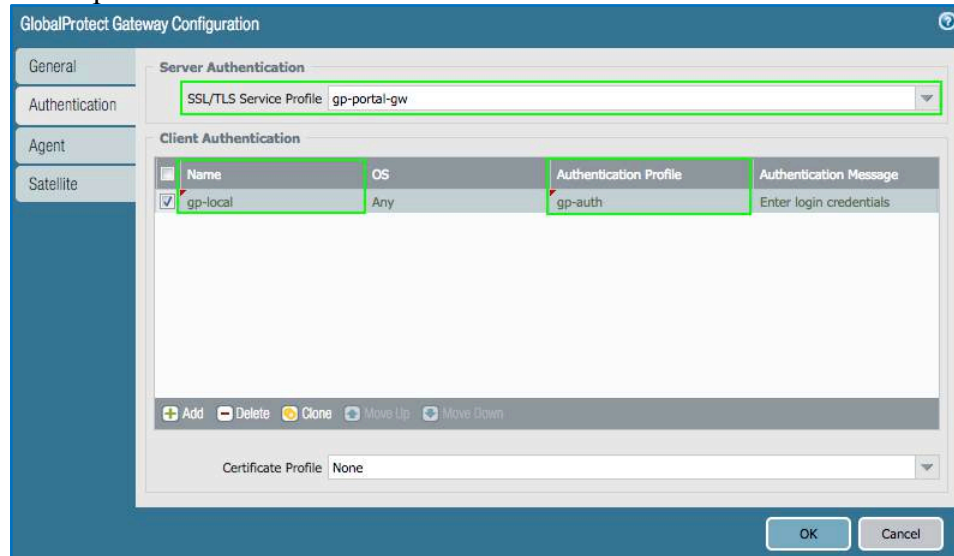
- i. Click the Add button  at the bottom to create a GP Gateway configuration.
- ii. Enter a relevant Name. Click the dropdown next to **Interface** and select your public facing layer-3 interface. Click the dropdown next to **IPv4 Address** and select the public IP address you want to use for GP Gateway.

 **TIP** – A loopback interface can be used in lieu of a physical interface address – this may be useful when adding multiple GP gateways using the same public-facing interface.

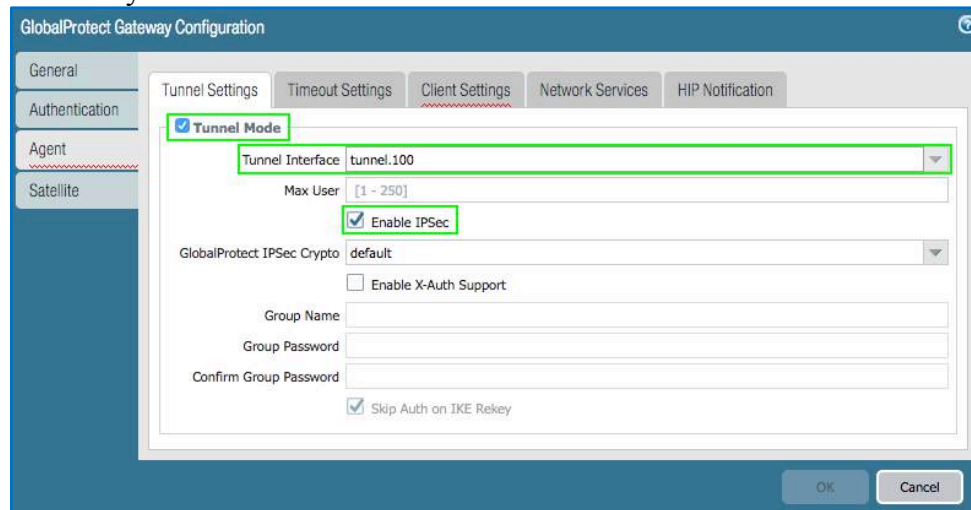
- iii. Click the **Authentication** tab on the left.
- iv. Click the dropdown next to **SSL/TLS Service Profile** and select the profile you created in an earlier step.


For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- v. Under the Client Authentication list box, click the Add button  to create a client authentication configuration.
- vi. Enter a relevant name. Under the **Authentication Profile** field, click **None** to reveal the dropdown, select the authentication profile you created in an earlier step.

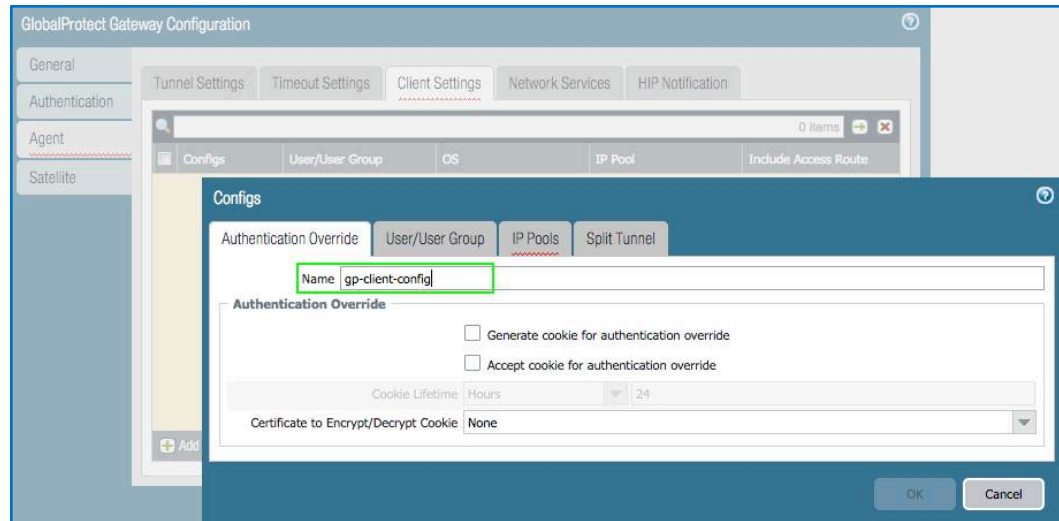



- vii. Click the **Agent** tab on the left.
- viii. Under the **Tunnel Settings** subtab, select the **Tunnel Mode** checkbox.
- ix. Click the dropdown next to **Tunnel Interface** and select the tunnel interface you created in an earlier step.
- x. Verify that the **Enable IPSec** checkbox is selected.

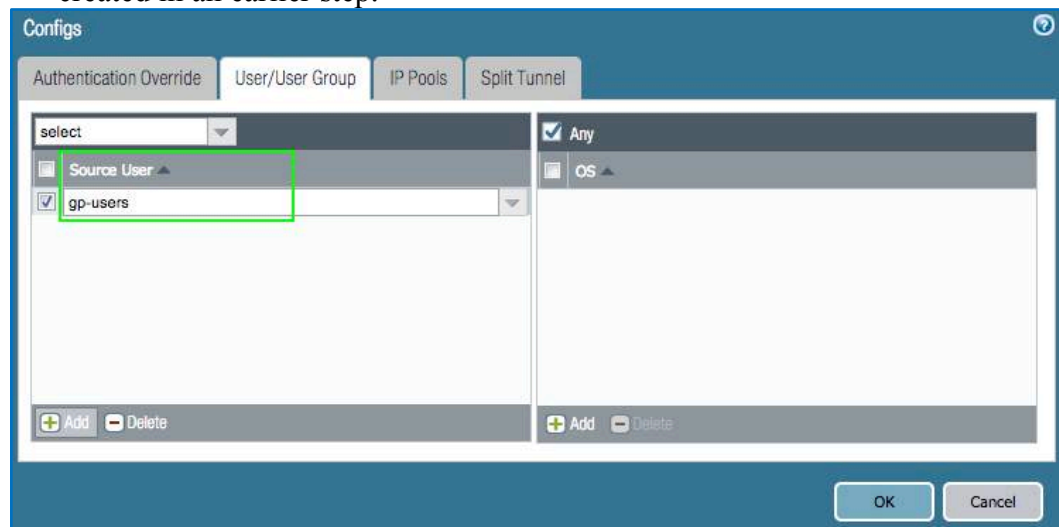


- xi. Click the **Client Settings** subtab, click the Add button  to create a client settings configuration.
- xii. Under the Authentication Override tab, enter a relevant name.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



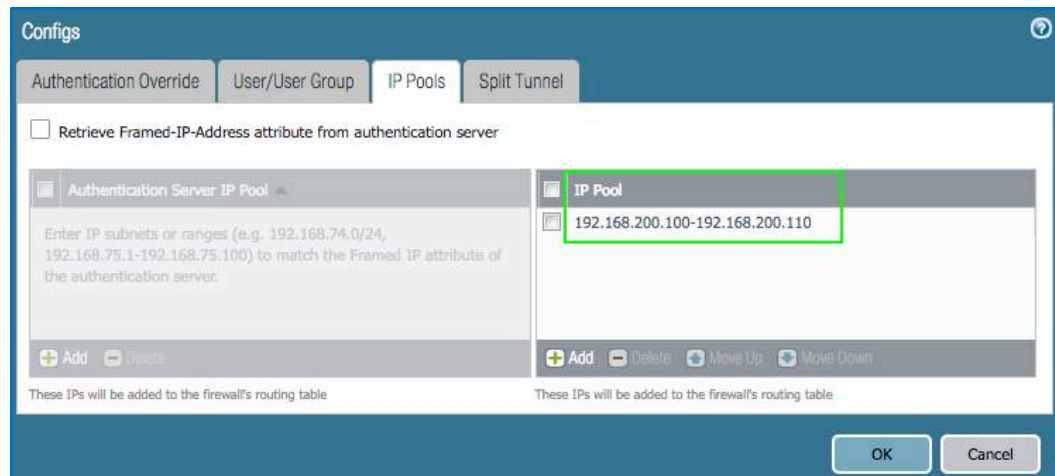
- xiii. Click the **User/User Group** tab. Under the **Source User** list box, click the Add button  and manually enter the name of the *local user group* you created in an earlier step.



- xiv. Click the **IP Pools** tab. Under **IP Pool**, click the Add button  and enter an available IP range for your GP clients.

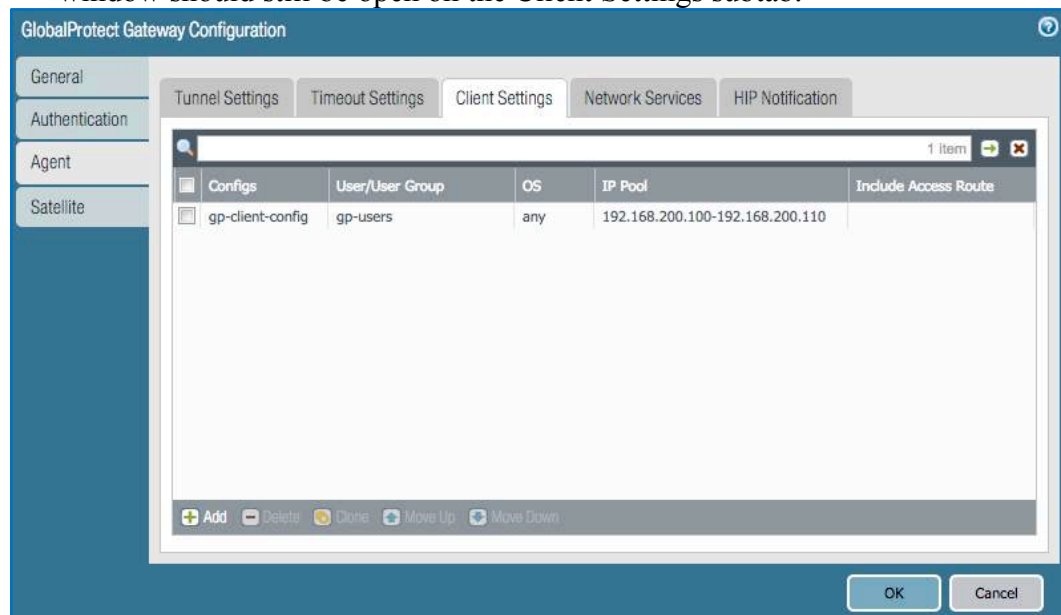


For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



**TIP** – Split Tunneling can be disabled in order to route all remote user traffic through the GP connection, thereby facilitating content-id\* scanning for mobile users (\*additional licensing required).

- xv. Click **OK** to close out the Configs window. The GP Gateway configuration window should still be open on the Client Settings subtab.





- xvi. Click the **Network Services** subtab. Enter public DNS server IP addresses in the **Primary DNS** and **Secondary DNS** fields.



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

The image shows the 'GlobalProtect Gateway Configuration' window with the 'Network Services' tab selected. The 'Inheritance Source' is set to 'None'. The 'Primary DNS' is set to '8.8.8.8' and the 'Secondary DNS' is set to '4.2.2.2', both highlighted with a green box. The 'Primary WINS' and 'Secondary WINS' are both set to 'None'. There is an unchecked checkbox for 'Inherit DNS Suffixes'. The 'DNS Suffix' field contains the placeholder text 'Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)'. At the bottom right are 'OK' and 'Cancel' buttons.

-  **TIP** – To resolve internal domains, enter private DNS server addresses.
-  **TIP** – If configuring Internal GP Gateway, the firewall would also need to be configured as a DNS Proxy.

xvii. Click **OK** to close the GP Gateway configuration window.

Upon expanding your GP Gateways list view, your new gateway should look something like this:

The image shows the Palo Alto Networks GUI with the 'Network' tab selected. The 'GlobalProtect' section is expanded, and the 'Gateways' list is visible. The list contains two entries: 'gp-gateway' and 'gp-client-config'. The 'gp-gateway' entry is highlighted with a green box. The table has columns for Name, Location, Local Interface, Local IP, Tunnel, Max User, and Info.

Name	Location	Local Interface	Local IP	Tunnel	Max User	Info
gp-gateway		ethernet1/3	0/0	tunnel.100		Remote Users
gp-client-config		go-users	any	IP Pool	Authentication IP Pool	Access Route

\*This may be a good point to pause, to validate and commit your changes.

## 4. Configure GlobalProtect Portal

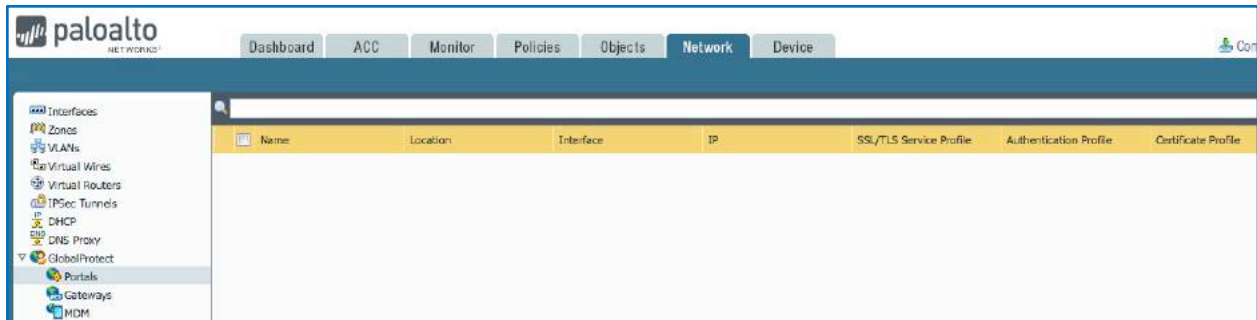
### a. Purpose

The GP Portal provides the management functions for the GP infrastructure. Every endpoint that participates in the GP network receives its configuration from the portal.


### b. Location


GlobalProtect Portals are configured in the **Network** tab under **GlobalProtect – Portals** in the left menu.


For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



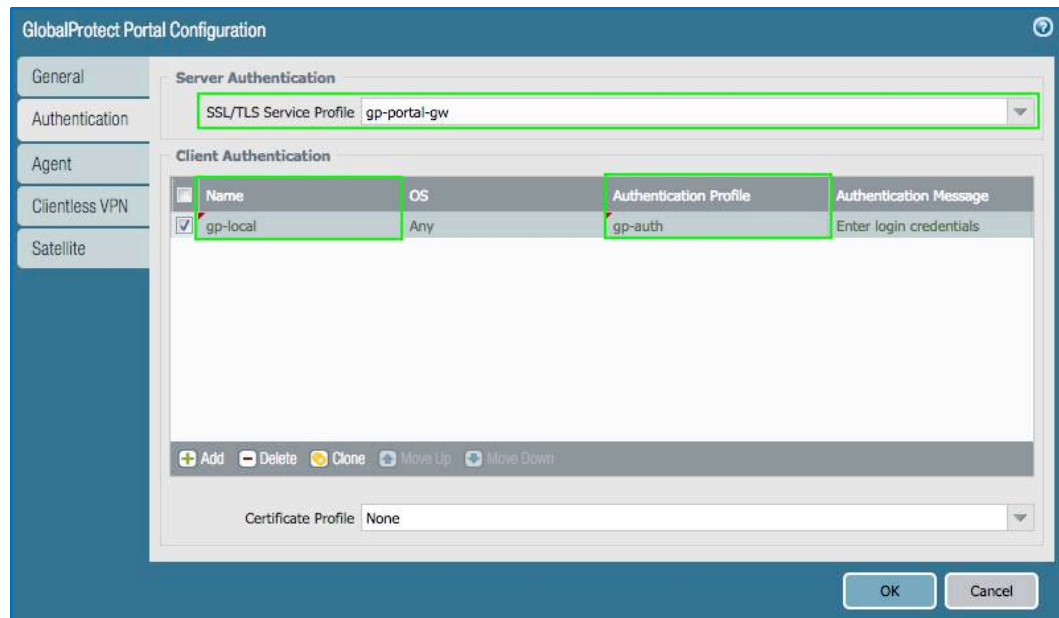
### c. Configure the Portal


- i. Click the Add button  at the bottom to create a GP Portal configuration.
- ii. Enter a relevant Name. Click the dropdown next to **Interface** and select your public facing layer-3 interface. Click the dropdown next to **IPv4 Address** and select the public IP address you want to use for GP Portal.

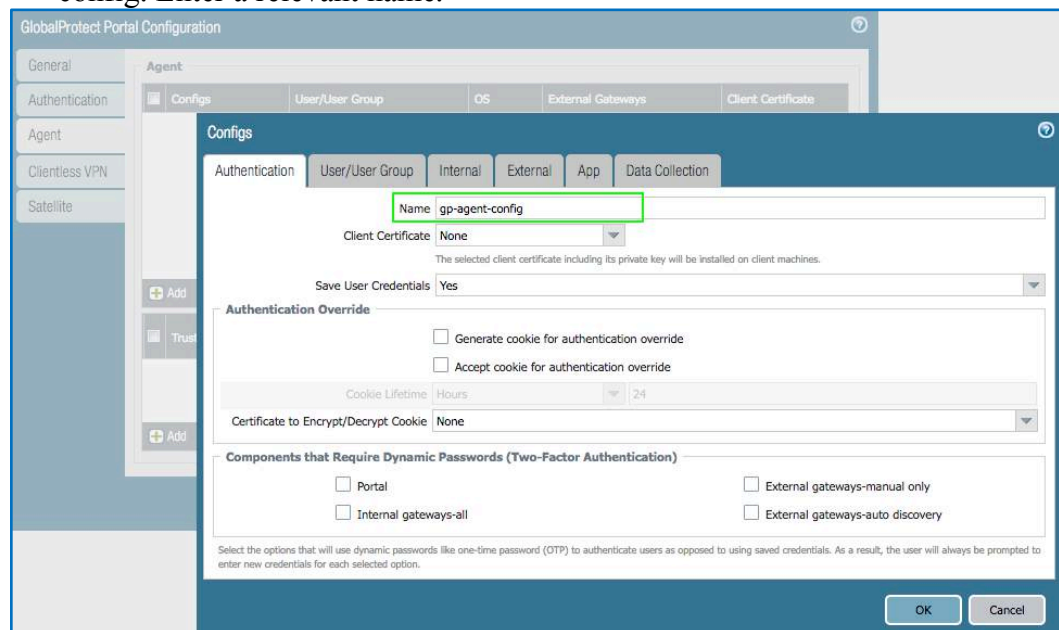
 **TIP** – A loopback interface can be used in lieu of a physical interface address – this may be useful when adding multiple GP portals using the same public-facing interface.


- iii. Click the **Authentication** tab on the left.
- iv. Click the dropdown next to **SSL/TLS Service Profile** and select the profile you created in an earlier step.
- v. Under the Client Authentication list box, click the Add button  to create a client authentication configuration.
- vi. Enter a relevant name. Under the **Authentication Profile** field, click **None** to reveal the dropdown, select the authentication profile you created in an earlier step.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

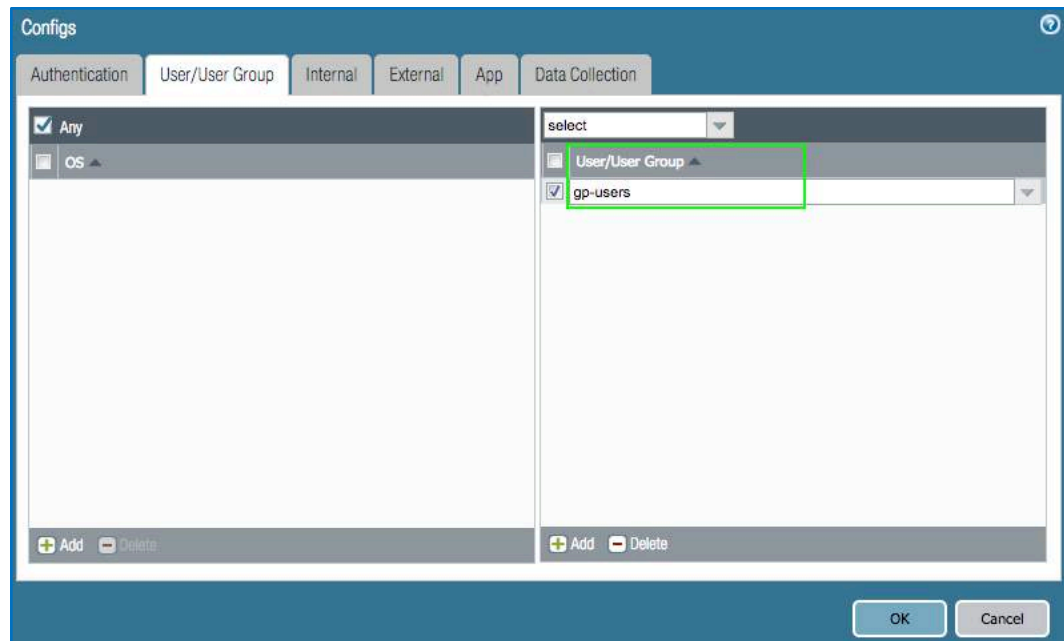




- xviii. Click the **Agent** tab on the left.
- xix. Under the Agent list box, click the Add button  to create an agent config. Enter a relevant name.



- xx. Click the **User/User Group** tab. Under the User/User Group list box, click the Add button  and manually enter the name of the *local user group* you created in an earlier step.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



- xxi. Click the **External** tab.
- xxii. Under the **External Gateways** list box, click the Add button  to add an external gateway. Enter a relevant name.
- xxiii. Next to **Address**, select the **IP** radio button.
- xxiv. Type the IP address of your GP Gateway in the **IPv4** field.
- xxv. Under the Source Region list box, click the Add button  and accept the defaults **Any** source region and **Highest** priority.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

Configs

Authentication User/User Group Internal External App Data Collection

Cutoff Time (sec) 5

External Gateways

External Gateway

Name ext-gw

Address ☐ FQDN ☒ IP

IPv4 50.63.202.9

IPv6

Source Region Any

Priority Highest

Add Delete

☐ Manual (The user can manually select this gateway)

OK Cancel

- xxvi. Click **OK** to close the External Gateway. Click the **App** tab.
- xxvii. Under **App Configurations**, next to **Connect Method**, change the selection to **On-demand (Manual user initiated connection)**.

Configs

Authentication User/User Group Internal External App Data Collection

App Configurations

Connect Method On-demand (Manual user initiated connection)

GlobalProtect App Config Refresh Interval (hours) 24 [1 - 168]

Allow User to Disable GlobalProtect App Allow

Allow User to Upgrade GlobalProtect App Allow with Prompt

Use Single Sign-on (Windows Only) Yes

Clear Single Sign-On Credentials on Logout (Windows Only) Yes

Use Default Authentication on Kerberos Authentication Failure (Windows Only) Yes

Automatic Restoration of VPN Connection Timeout (min) 30 [0 - 180]

Wait Time Between VPN Connection Restore Attempts 5 [1 - 60]

Welcome Page None

Disable GlobalProtect App

Passcode

Confirm Passcode

Max Times User Can Disable 0

Disable Timeout (min) 0

Mobile Security Manager Settings

Mobile Security Manager

Enrollment Port 443

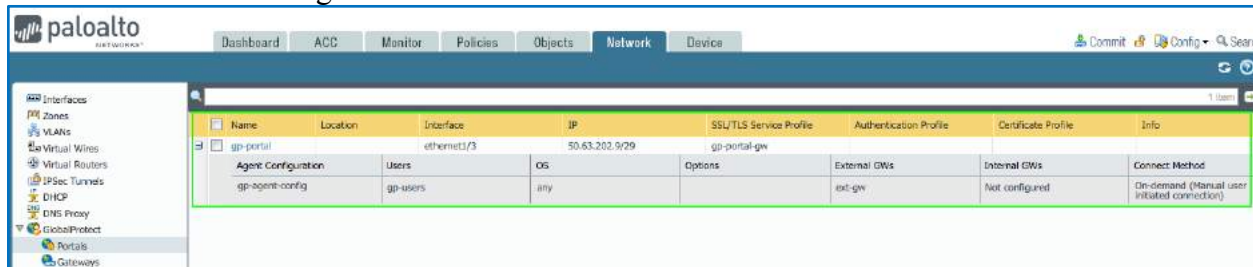
OK Cancel

**TIP** – The **Always On** GP app connection methods will facilitate more security when coupled with disabling split tunneling.

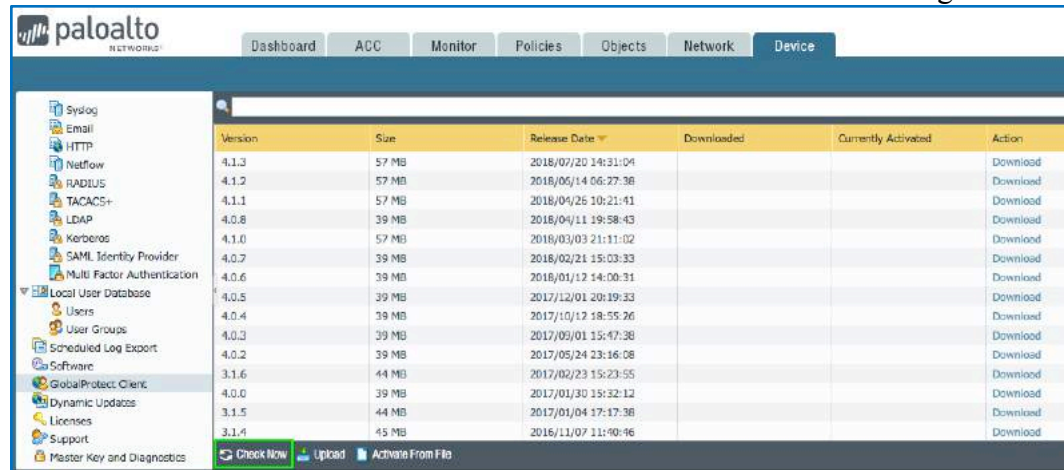
For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- xxviii. Click **OK** twice to close Configs and GlobalProtect Portal configuration windows.

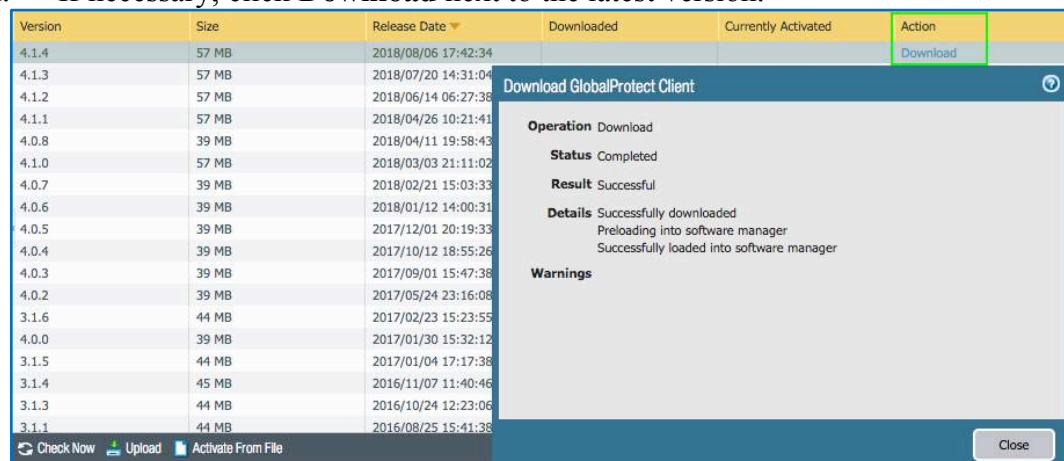
Upon expanding your GP Portals list view, your new portal should look something like this:



- d. **Host the GP Agent on the Portal** - configured in the *Device* tab under *GlobalProtect Client* in the left menu.
- i. Click **Check Now**. The firewall checks for latest version of the GP agent.



- ii. If necessary, click **Download** next to the latest version.



- iii. Click **Activate** (or Reactivate) for the GP agent that you've just downloaded.



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

Version	Size	Release Date	Downloaded	Currently Activated	Action
4.1.4	57 MB	2018/08/06 17:42:34	✓		Activate
4.1.3	57 MB	2018/07/20 14:31:04			Download
4.1.2	57 MB	2018/05/14 06:27:38			Download
4.1.1	57 MB	2018/04/26 10:21:41			Download
4.0.8	39 MB	2018/04/11 19:58:43			Download
4.1.0	57 MB	2018/03/03 21:11:02			Download
4.0.7	39 MB	2018/02/21 15:03:33			Download
4.0.6	39 MB	2018/01/12 14:00:31			Download
4.0.5	39 MB	2017/12/01 20:19:33			Download

- iv. Click **Yes**, and then click **Close** after the client package activation is completed.

paloalto						
Dashboard ACC Monitor Policies Objects Network Device						
Version	Size	Release Date	Downloaded	Currently Activated	Action	
4.1.4	57 MB	2018/08/06 17:42:34	✓	✓	Reactivate	
4.1.3	57 MB	2018/07/20 14:31:04			Download	
4.1.2	57 MB	2018/05/14 06:27:38			Download	
4.1.1	57 MB	2018/04/26 10:21:41			Download	
4.0.8	39 MB	2018/04/11 19:58:43			Download	
4.1.0	57 MB	2018/03/03 21:11:02			Download	
4.0.7	39 MB	2018/02/21 15:03:33			Download	
4.0.6	39 MB	2018/01/12 14:00:31			Download	
4.0.5	39 MB	2017/12/01 20:19:33			Download	
4.0.4	39 MB	2017/10/12 18:55:26			Download	
4.0.3	39 MB	2017/09/01 15:47:38			Download	
4.0.2	39 MB	2017/05/24 23:16:08			Download	
3.1.6	44 MB	2017/02/23 15:23:55			Download	
4.0.0	39 MB	2017/01/30 15:32:12			Download	
3.1.5	44 MB	2017/01/04 17:17:38			Download	
3.1.4	45 MB	2016/11/07 11:40:46			Download	

**\*Be sure to validate and commit your changes!**

**TIP** - For more granular control over external connectivity to the GP Portal and Gateway, consider creating two intrazone security policy rules for your outside/untrust zone, with your portal/gateway IP address as the destination: 1 rule at the top permitting only certain applications for GP (ssl, web-browsing, panos-global-protect and ipsec-esp-udp), and only from select source public IP/blocks if you so desire; and the 2<sup>nd</sup> rule would be a deny rule dropping any other connection to your portal/gateway public IP address (the assumption also is that you do **not** have an Interface Mgmt profile on your public-facing interface permitting HTTPS Mgt of the firewall). In this lab, the intrazone-default security rule accommodates both external connection with the portal/gateway, as well as internal access for GP users after they have successfully established a tunneling session with the gateway.

## 5. Download the GP Agent

### a. Purpose

Remote access clients require the GP Agent software in order to establish GP connectivity (Clientless VPN being exception to this rule, not covered in this lab).

### b. Location

[https://IP address of your GP Portal.](#)



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

c. **Download GP Agent software**

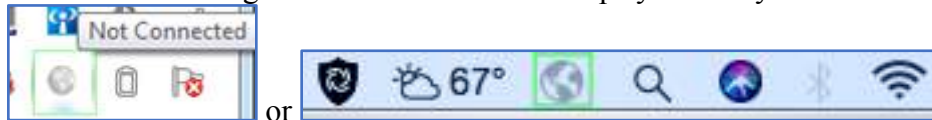
- i. On Windows or Mac client, open a web browser and https browse to the public IP address of your GP Portal. Proceed past the certificate error.



- ii. Log in using one of the local users you created in an earlier step.

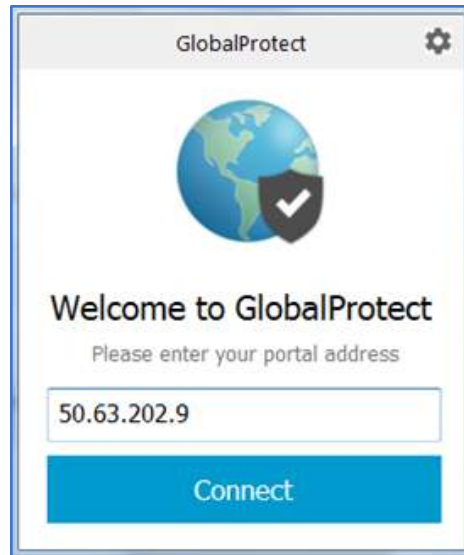



- iii. Download and install the appropriate GP agent for your OS.  
iv. Click the GP agent in the Windows desktop system tray or Mac menu bar



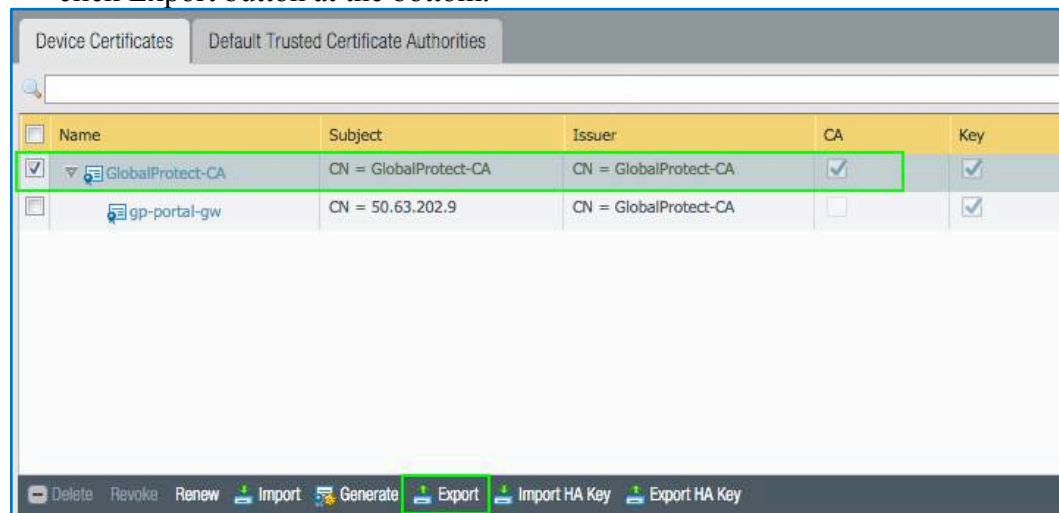
- v. Type your GP portal IP address and click **Connect**.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



 **TIP** - You can configure multiple portals via gear icon in the upper-righthand corner 

- vi. Click Continue when presented with a certificate warning (or you can choose to install the certificate on your computer).
- vii. Log in using one of the local users you created in an earlier step, and then click **Sign In**. If you have further issues with invalid/untrusted certificate error, you will need to install the CA certificate (the 1<sup>st</sup> certificate that you created in an earlier step) into the Trusted Root Certification Authorities store / Mac OS system keychain. Depending on your OS and your browser, this will likely require manually exporting the CA certificate from the firewall - on the firewall, go to Device – Certificate Mgt – Certificates. Select the CA cert and click Export button at the bottom.



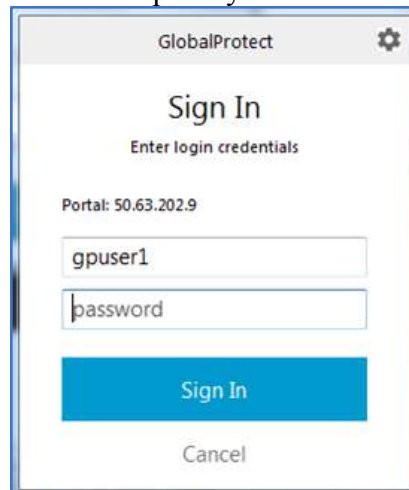
For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



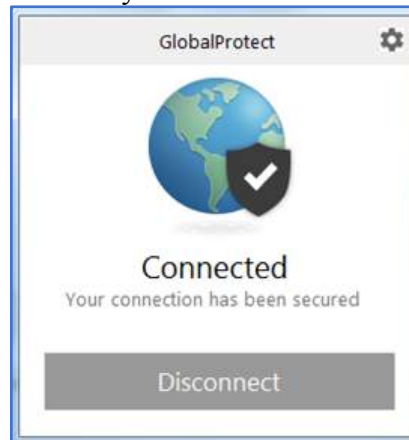
- viii. If after importing the CA certificate onto your computer, you get a certificate warning again, you may need to install the Portal/Gateway certificate on your computer. Here is how Windows Certificates.msc might display both certificates after they've been imported:

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
50.63.202.9	GlobalProtect-CA	8/9/2019	Server Authenticati...	<None>
GlobalProtect-CA	GlobalProtect-CA	8/9/2019	<All>	<None>

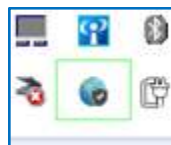
- ix. At this point you should be able to sign in...



- x. And you should connect successfully to the Gateway.



- xi. GP icon shows connected – here is Windows system tray:

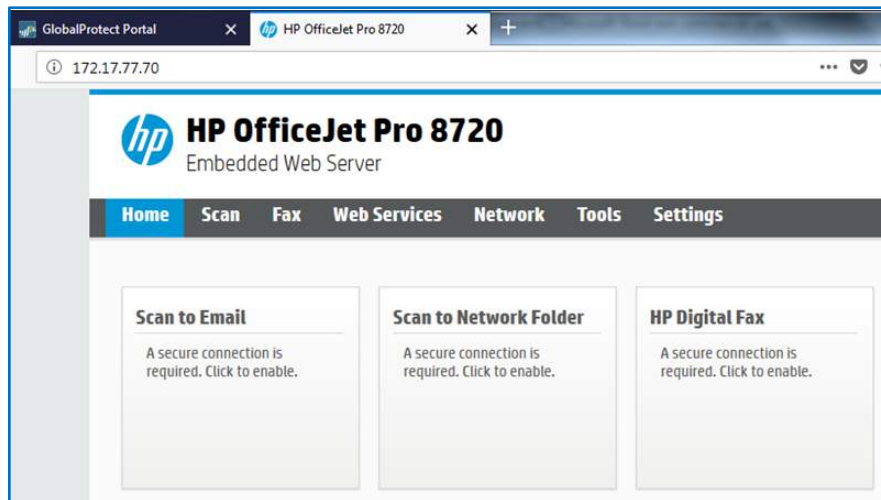


For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- xii. As general sample traffic, below we have a snip showing Windows client pinging Gateway public address and also pinging a network printer inside the lab network (on the inside/trust zone behind the firewall).

```
C:\>ping 50.63.202.9
Pinging 50.63.202.9 with 32 bytes of data:
Reply from 50.63.202.9: bytes=32 time=4ms TTL=64
Reply from 50.63.202.9: bytes=32 time=4ms TTL=64
Reply from 50.63.202.9: bytes=32 time=3ms TTL=64
Reply from 50.63.202.9: bytes=32 time=6ms TTL=64
Ping statistics for 50.63.202.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 6ms, Average = 4ms
C:\>
C:\>
C:\>ping 172.17.77.70
Pinging 172.17.77.70 with 32 bytes of data:
Reply from 172.17.77.70: bytes=32 time=4ms TTL=254
Reply from 172.17.77.70: bytes=32 time=5ms TTL=254
Reply from 172.17.77.70: bytes=32 time=52ms TTL=254
Reply from 172.17.77.70: bytes=32 time=5ms TTL=254
Ping statistics for 172.17.77.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 52ms, Average = 16ms
```

- xiii. And here we show web access to an internal network printer while connected from GP client.

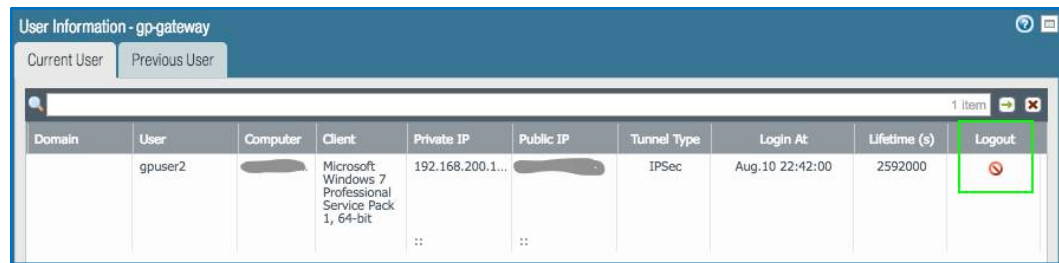


- xiv. Back over on the firewall – under **Network – GlobalProtect – Gateways –** click on **Remote Users** to see the connected users...



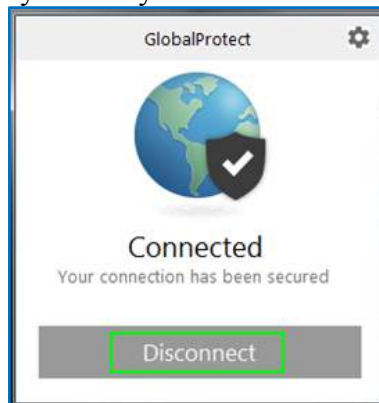
Notice various information in the columns and that you can **Logout** a user.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



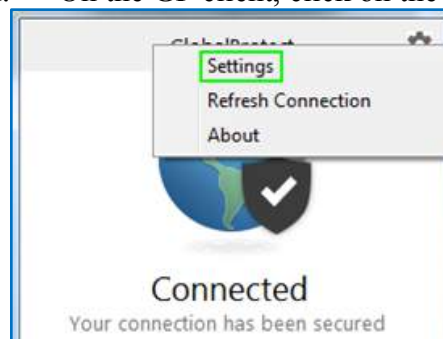
Domain	User	Computer	Client	Private IP	Public IP	Tunnel Type	Login At	Lifetime (s)	Logout
	gpuser2		Microsoft Windows 7 Professional Service Pack 1, 64-bit	192.168.200.1...		IPSec	Aug.10 22:42:00	2592000	

- xv. To disconnect GP from client side, simply click the GP icon in Windows system tray / Mac menu bar and click the **Disconnect** button.



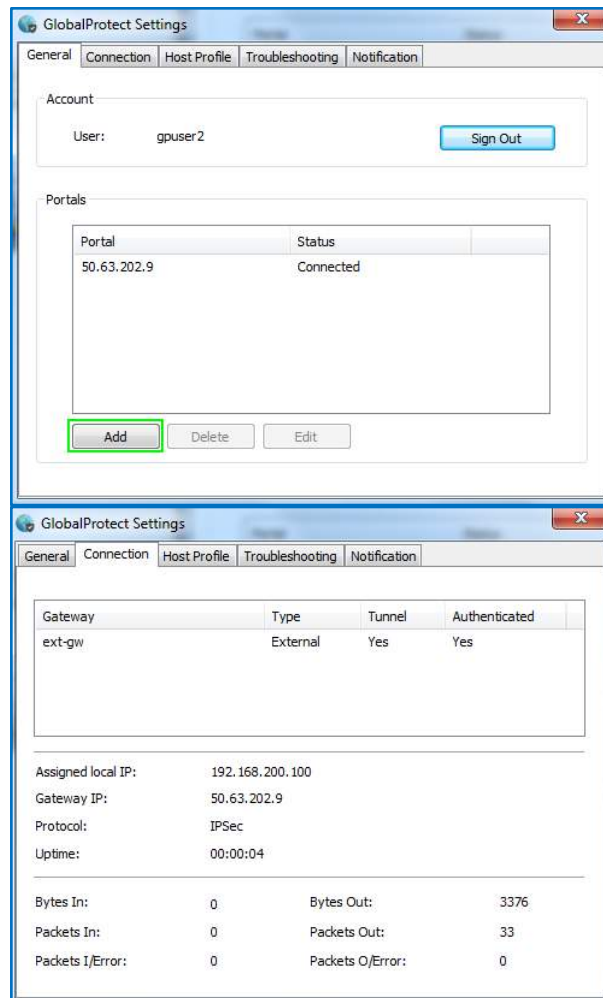
**d. Troubleshooting GlobalProtect issues**

- i. On the GP client, click on the gear icon, and then select Settings



- ii. The GP Settings window provides details about the connection including your tunneling IP address, as well as other helpful troubleshooting from the client side. The General tab is also where you can add additional portals.

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>



- iii. The Palo Alto firewall **System log** is a good place to troubleshoot GlobalProtect connection problems, related user authentication, etc. - accessible under **Monitor – Logs - System**



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

Receive Time	Type	Severity	Event	Object	Description
08/10 23:31:13	globalpr...	informational	globalprotectgateway-logout-succ	gp-gateway-N	GlobalProtect gateway user logout succeeded. User name: gpuser2, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, Reason: client logout.
08/10 23:31:13	globalpr...	informational	globalprotectgateway-config-release	gp-gateway-N	GlobalProtect gateway client configuration released. User name: gpuser2, Private IP: 192.168.200.100, Client version: 4.1.4-13, Device name: [REDACTED], Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
08/10 23:32:50	globalpr...	informational	globalprotectgateway-config-succ	gp-gateway-N	GlobalProtect gateway client configuration generated. User name: gpuser2, Private IP: 192.168.200.100, Client version: 4.1.4-13, Device name: [REDACTED], Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
08/10 23:23:49	globalpr...	informational	globalprotectgateway-regist-succ	gp-gateway-N	GlobalProtect gateway user login succeeded. Login from: [REDACTED], Source region: US, User name: gpuser2, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
08/10 23:23:49	globalpr...	informational	globalprotectgateway-auth-succ	gp-gateway-N	GlobalProtect gateway user authentication succeeded. Login from: [REDACTED], Source region: US, User name: gpuser2, Auth type: profile, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.
08/10 23:23:49	auth	informational	auth-success	gp-auth	authenticated for user 'gpuser2', auth profile 'gp-auth', vsys 'vsys1', From: [REDACTED].
08/10 23:23:48	globalpr...	informational	globalprotectportal-config-succ	gp-portal	GlobalProtect portal client configuration generated. Login from: [REDACTED], Source region: US, User name: gpuser2, Config name: gp-agent-config.
08/10 23:23:47	globalpr...	informational	globalprotectportal-auth-succ	gp-portal	GlobalProtect portal user authentication succeeded. Login from: [REDACTED], Source region: US, User name: gpuser2, Auth type: profile.
08/10 23:23:47	auth	informational	auth-success	gp-auth	authenticated for user 'gpuser2', auth profile 'gp-auth', vsys 'vsys1', From: [REDACTED].
08/10 23:23:45	globalpr...	informational	globalprotectportal-auth-fail	gp-portal	GlobalProtect portal user authentication failed. Login from: [REDACTED], Source region: US, User name: ProDev, Reason: Authentication failed: Invalid username or password, Auth type: profile.
08/10 23:23:45	auth	medium	auth-fail	gp-auth	failed authentication for user 'ProDev'. Reason: User is not in allowlist: auth profile 'gp-auth', vsys 'vsys1', From: [REDACTED].
08/10 23:20:41	globalpr...	informational	globalprotectgateway-logout-succ	gp-gateway-N	GlobalProtect gateway user logout succeeded. User name: gpuser2, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, Reason: client logout.
08/10 23:20:41	globalpr...	informational	globalprotectgateway-config-release	gp-gateway-N	GlobalProtect gateway client configuration released. User name: gpuser2, Private IP: 192.168.200.100, Client version: 4.1.4-13, Device name: [REDACTED], Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
08/10 23:14:26	globalpr...	informational	globalprotectgateway-config-succ	gp-gateway-N	GlobalProtect gateway client configuration generated. User name: gpuser2, Private IP: 192.168.200.100, Client version: 4.1.4-13, Device name: [REDACTED], Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit, VPN type: Device Level VPN.
08/10 23:14:25	globalpr...	informational	globalprotectgateway-regist-succ	gp-gateway-N	GlobalProtect gateway user login succeeded. Login from: [REDACTED], Source region: US, User name: gpuser2, Client OS version: Microsoft Windows 7 Professional Service Pack 1, 64-bit.

- iv. The Palo Alto firewall **Traffic log** is also helpful for troubleshooting – accessible under **Monitor – Logs - Traffic**

Receive Time	From Zone	Source
08/10 23:31:13	inside	192.168.200.100
08/10 23:31:12	inside	192.168.200.100

- v. To see user-id in traffic logs, enable User Identification on your inside zone (tunnel interface zone).



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

- vi. Below is a sample Traffic log snip, before and after applying user-id to the tunnel interface zone:

Receive Time	Action	Rule	From Zone	Source	Source User	Destination	To Zone
08/10 23:29:49	allow	intrazone-default	inside	192.168.200.100	gpuser2	172.17.77.70	inside
08/10 23:29:13	allow	intrazone-default	inside	192.168.200.100	gpuser2	172.17.77.70	inside
08/10 23:24:15	allow	intrazone-default	inside	192.168.200.100		172.17.77.70	inside
08/10 23:24:09	allow	intrazone-default	inside	192.168.200.100		172.17.77.70	inside

For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

## Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a few options:

- a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **[sales@sunmanagement.net](mailto:sales@sunmanagement.net)** for assistance.

- b. Reach out through the free Fuel Users Group ([www.fuelusersgroup.org](http://www.fuelusersgroup.org)) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their “Virtual Test Lab,” in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their “Virtual Test Lab” at any time)
- c. For access to live Palo Alto Networks boxes for lab practice purposes please go to:  
**<https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>**. This is a no charge service provided by Palo Alto Networks.

*If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.*

*Please direct any questions/comments/feedback on this lab exercise to:  
**[education@sunmanagement.net](mailto:education@sunmanagement.net)***

Lab Author: Jeff Wood, PCNSE, Network Security Engineer

Last Modified: August 17, 2018



For access to live Palo Alto Networks lab boxes, go to: <https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab>

## Resources

GlobalProtect Licensing:

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-overview/about-globalprotect-licenses>

GlobalProtect 8.0 Administrator's Guide:

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide>

How to Generate a Self-signed Certificate:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Generate-a-New-Self-Signed-SSL-Certificate/ta-p/53215>

Online Certificate Status Protocol (OCSP):

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management/certificate-revocation/online-certificate-status-protocol-ocsp>

