

GlobalProtect Configuration

Basic Setup

Backup Configuration (Device-Setup-Operations)

Navigate to Device->Setup->Operations

1. Save named configuration snapshot
 1. candidate config
2. Export Named Configuration
 2. Candidate Config
3. Save this somewhere you can find it. you can import this if a rollback is needed.

Alternatively, you can just verify current configuration version

 1. Load Configuration version
 2. Verify Highest number and most recent date.
 3. Roll back to this number after any changes completed.

Zones (Network-Zones)

For the most control, we need to configure a zone for our GlobalProtect. This is *optional* however **HIGHLY** recommended.

<input type="checkbox"/>	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID			Device-ID		
							ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
<input type="checkbox"/>	DMZ	layer3	ethernet1/7		<input checked="" type="checkbox"/>		<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
<input type="checkbox"/>	GP	layer3	tunnel1		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
			tunnel2									
<input type="checkbox"/>	Inside	layer3	ethernet1/1		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
			ethernet1/2									
			tunnel									
<input type="checkbox"/>	Outside	layer3	ethernet1/3		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
			ethernet1/4									

Certificates (Device-Certificate Management-Certificates)

Okay we need to generate two certificates. One is our root cert, and one will be our GlobalProtect Specific.

Root Certification Generation

Generate Certificate



Certificate Type ☒ Local ☐ SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By

☒ Certificate Authority

☐ Block Private Key Export

OCSP Responder

^ Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE
<input checked="" type="checkbox"/>	IP = "IP Address" from Subject Alternative Name (SAN) field	10.2.191.10
<div><input type="button" value="+ Add"/> <input type="button" value="- Delete"/></div>		

Generate

Cancel

GP (GlobalProtect) Certification Generation

Generate Certificate ?

Certificate Type ☒ Local ☐ SCEP

Certificate Name

Common Name
IP or FQDN to appear on the certificate

Signed By
☐ Certificate Authority
☐ Block Private Key Export

OCSP Responder

^ Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE
<input checked="" type="checkbox"/>	IP = "IP Address" from Subject Alternative Name (SAN) field	10.2.191.10

Generate

Cancel

Certificate Profile (Device-Certificate Management-Certificate Profile)

Next up we will create a certificate profile, as shown below. We're referencing our Root Cert, and leaving everything else blank

Certificate Profile
?

Name GPCert

Username Field None

User Domain

CA Certificates

<input type="checkbox"/>	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
<input type="checkbox"/>	RootCert			

+ Add
- Delete
↑ Move Up
↓ Move Down

Default OCSP URL (must start with http:// or https://)

☐ Use CRL
CRL Receive Timeout (sec) 5
☐ Use OCSP
OCSP takes precedence over CRL
OCSP Receive Timeout (sec) 5
Certificate Status Timeout (sec) 5

☐ Block session if certificate status is unknown
☐ Block session if certificate status cannot be retrieved within timeout
☐ Block session if the certificate was not issued to the authenticating device
☐ Block sessions with expired certificates

OK Cancel

SSL/TLS Service Profile (Device-Certificate Management-SSL/TLS Service Profile)

Configure this section as shown in the picture, reference the GPCert. and set the min/max versions.

SSL/TLS Service Profile
?

Name GP

Certificate gpcert2

Protocol Settings

Min Version TLSv1.0

Max Version TLSv1.2

OK Cancel

Portal Configuration

Configure as shown in the pictures below.

General

GlobalProtect Portal Configuration ?

General
Authentication
Portal Data Collectio
Agent
Clientless VPN
Satellite

NameGP1

Network Settings

Interfaceethernet1/3
IP Address TypeIPv4 Only
IPv4 Address10.2.191.10

Appearance

Portal Login Pagefactory-default
Portal Landing Pagefactory-default
App Help PageNone

Log Settings

☐ Log Successful SSL Handshake
☒ Log Unsuccessful SSL Handshake

Log ForwardingNone

OK

Cancel

Authentication

Make sure we choose the Service and Certificate profiles then add a client authentication

GlobalProtect Portal Configuration ?

General
Authentication
Portal Data Collectio
Agent
Clientless VPN
Satellite

Server Authentication

SSL/TLS Service ProfileGP

Client Authentication

	NAME	OS	AUTHENTICATION PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENT... MESSAGE	A... A... W... U... C... O... C... C...
<input checked="" type="checkbox"/>	GP1	Any	AD_Auth	<input type="checkbox"/>	Username	Password	Enter login credentials	No

+ Add
- Delete
Clone
↑ Move Up
↓ Move Down

Certificate ProfileGPCert

OK

Cancel

For this we will reference our authentication profile tied to active directory that was previously made

Client Authentication

?

Name

GP1

OS

Any

▼

Authentication Profile

AD_Auth

▼

☐

Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label

Username

Password Label

Password

Authentication Message

Enter login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate

No (User Credentials AND Client Certificate Required)

▼

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK

Cancel

Please note: The bottom box has to be set to YES in order to skip the future "device configuration" section. This will, however, make our network less secure.

Agent

You can Skip the Portal Data Collection tab for now. Here in Agent, we need to do two things:

1. Configure an Agent
2. Add the root and have it install in local root store

As you can see, you just add the trusted root ca, select RootCert and then check the box

GlobalProtect Portal Configuration
?

General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite

Agent

CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
<input checked="" type="checkbox"/>	Client-Config-1	any	any	GW1

+ Add
- Delete
Clone
Move Up
Move Down

TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE
<input type="checkbox"/>	RootCert
<input checked="" type="checkbox"/>	

+ Add
- Delete

Agent User Override Key
Confirm Agent User Override Key

OK
Cancel

Now for the agent, go ahead and add

- Name: Arbitrary, I used Client-Config-1
- Client certificate - local - pick your GPCert
- Everything else can be left alone on this tab

Configs
?

Authentication
Config Selection Criteria
Internal
External
App
HIP Data Collection

Name
Client-Config-1

Client Certificate
Local
gpcert2

The selected client certificate including its private key will be installed on client machines.

Save User Credentials
Yes

Authentication Override

☐ Generate cookie for authentication override
☐ Accept cookie for authentication override

Cookie Lifetime
Hours
24

Certificate to Encrypt/Decrypt Cookie
None

Components that Require Dynamic Passwords (Two-Factor Authentication)

☐ Portal
☐ External gateways-manual only
☐ Internal gateways-all
☐ 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

Jump to the "External" tabs and add

Cutoff Time (sec)

5

External Gateways

<input type="checkbox"/>	NAME	ADDRESS	PRIORITY RULE	MANUAL
<input checked="" type="checkbox"/>	GW1	10.2.191.10	Any (Highest)	<input type="checkbox"/>

+ Add - Delete

THIRD PARTY VPN

+ Add - Delete

OK

Cancel

Here you would put your FQDN or IP, however you want the portal reachable. I used my outside Interfaces IP of 10.2.191.10 with a source region of any.

External Gateway?

Name

GW1

Address

☐ FQDN
☒ IP

IPv4

10.2.191.10

IPv6

1 item

→ ×

<input type="checkbox"/>	SOURCE REGION	PRIORITY
<input type="checkbox"/>	Any	Highest

+ Add

- Delete

☐ Manual (The user can manually select this gateway)

OK

Cancel

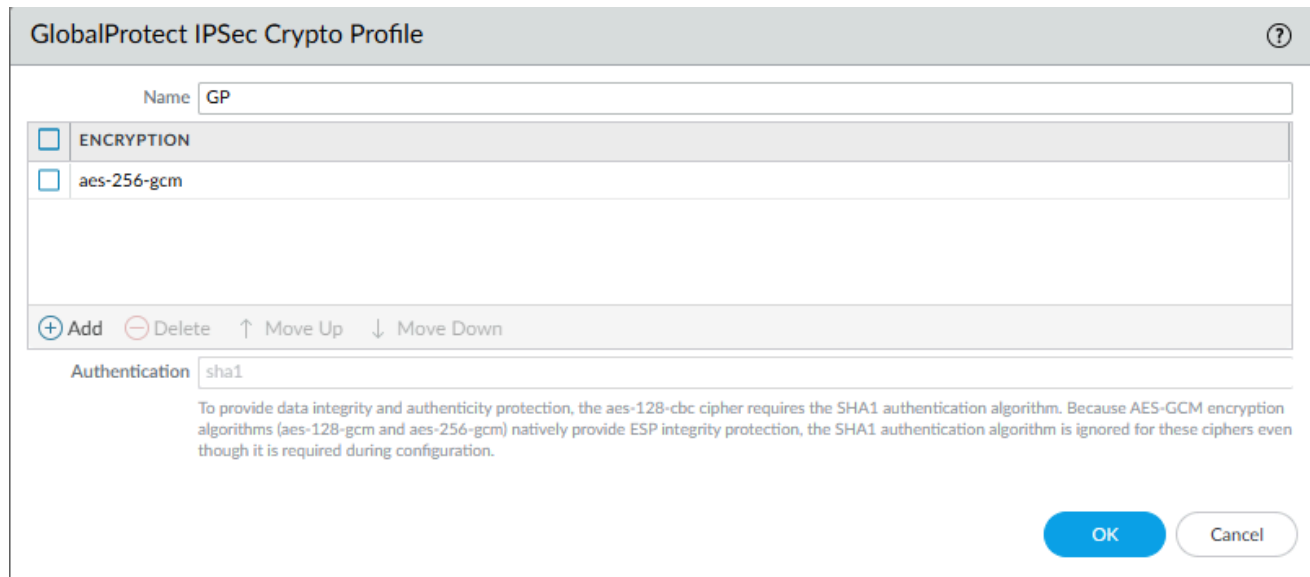
At this point you can go ahead and click okay until you reach the main page and commit. you are done configuring the portal.

Before we get started with the gateway we need to configure a few things.

IPSec Crypto Policy (network-network profiles-GlobalProtect IPSec Crypto)

- Add a new profile
- Select aes-256-gcm as this is the best option

- Name the Profile (I named it GP)



GlobalProtect IPSec Crypto Profile

Name: GP

☐ ENCRYPTION

☐ aes-256-gcm

+ Add - Delete ↑ Move Up ↓ Move Down

Authentication: sha1

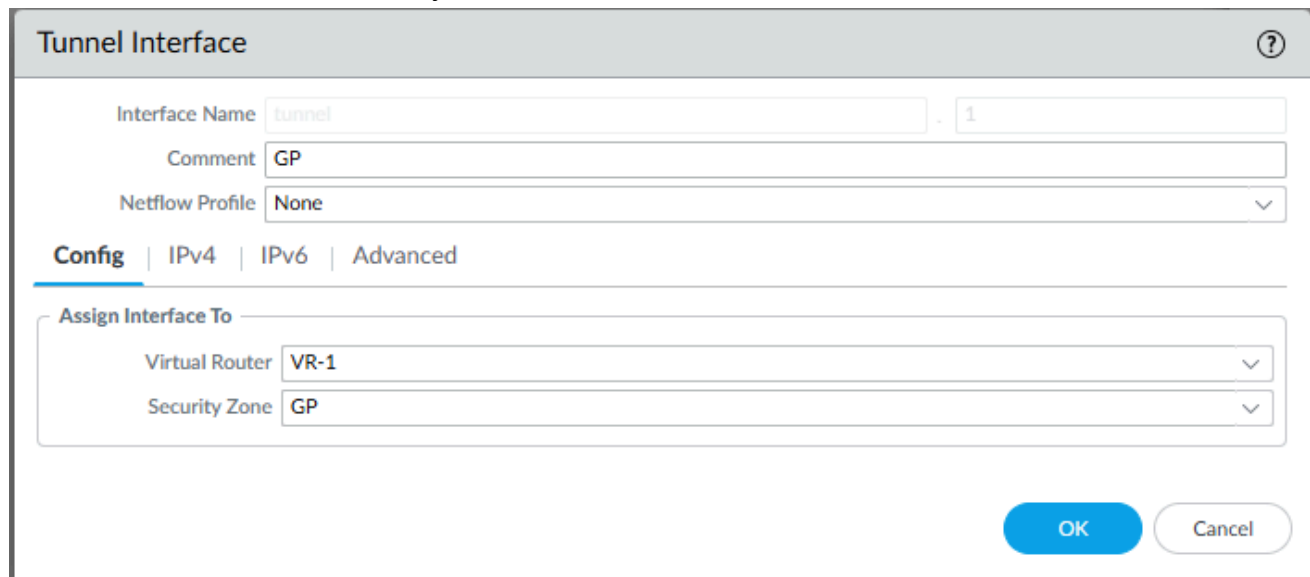
To provide data integrity and authenticity protection, the aes-128-cbc cipher requires the SHA1 authentication algorithm. Because AES-GCM encryption algorithms (aes-128-gcm and aes-256-gcm) natively provide ESP integrity protection, the SHA1 authentication algorithm is ignored for these ciphers even though it is required during configuration.

OK Cancel

Tunnel interface (Network-Interfaces-Tunnel)

We need to create two tunnel interfaces, one for the GlobalProtect base and one for the satellite. Create and name accordingly

- Assign to VR-1 virtual router
- Place both into the GP security zone



Tunnel Interface

Interface Name: tunnel . 1

Comment: GP

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: VR-1

Security Zone: GP

OK Cancel

Gateway

General

We're going to pick our interface, select ipv4 only and then use the IP on this interface, keep everything else the same.

GlobalProtect Gateway Configuration ?

General

Authentication

Agent

Satellite

Name

GP1

Network Settings

Interface

ethernet1/3

IP Address Type

IPv4 Only

IPv4 Address

10.2.191.10

Log Settings

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding

None

OK

Cancel

Authentication

We're going to once again select our SSL/TLS Service profile, our standard Certificate profile, and and setup our authentication as was done in the previous step.

GlobalProtect Gateway Configuration ?

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile

GP

Client Authentication

<input type="checkbox"/>	NAME	OS	AUTHENTICATION PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTICATION MESSAGE	ALLOW AUTHENTICATION WITH USER CREDENTIALS OR CLIENT CERTIFICATE
<input checked="" type="checkbox"/>	AD	Any	AD_Auth	<input type="checkbox"/>	Username	Password	Enter login credentials	No

+ Add

- Delete

🔄 Clone

↑ Move Up

↓ Move Down

Certificate Profile

GPCert

☒ Block login for quarantined devices

OK

Cancel

Agent

We're going to go ahead and check "tunnel mode" and choose our tunnel interface 1 (Or whichever one you created for the GlobalProtect base). Make sure we select the IPsec profile we created and enable IPsec is checked. Then move on to "Client IP Pool"

GlobalProtect Gateway Configuration

General | **Tunnel Settings** | Client Settings | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

☒ Tunnel Mode

Tunnel Interface:

Max User:

☒ Enable IPSec

GlobalProtect IPSec Crypto:

☐ Enable X-Auth Support

Group Name:

Group Password:

Confirm Group Password:

☒ Skip Auth on IKE Rekey

OK Cancel

We need to create a pool of IPs for the devices, these will be added to the firewalls routing tables but remember: *if you place them on their own network any other routers will need to add a static route or learn through dynamic routing!*

- For this example, I used some available IPs in my internal network

GlobalProtect Gateway Configuration

General | Tunnel Settings | Client Settings | **Client IP Pool** | Network Services | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

☐ IP POOL

☐ 10.2.91.37-10.2.91.45

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

OK Cancel

Finally, in the network services tab, add your primary and secondary DNS so your clients can resolve!

GlobalProtect Gateway Configuration

General | Tunnel Settings | Client Settings | Client IP Pool | **Network Services** | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

Inheritance Source:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

☐ Inherit DNS Suffixes

DNS Suffix:

OK Cancel

Satellite

Although we are not using the satellite functionality at this time, it still is required to setup here. Pick our interface we setup for the satellite (tunnel.2), configure a range of IPs to use, and keep everything else the same for now.

GlobalProtect Gateway Configuration

General | **Tunnel Settings** | Network Settings | Route Filter

Authentication

Agent

Satellite

☒ Tunnel Configuration

Tunnel Interface:

☐ Replay attack detection

☐ Copy TOS

Configuration Refresh Interval (Hours):

☐ Tunnel Monitoring

IPv4 Destination Address:

IPv6 Destination Address:

Tunnel Monitor Profile:

Crypto Profiles

IPSec Crypto Profile:

OK Cancel

GlobalProtect Gateway Configuration

General | Tunnel Settings | **Network Settings** | Route Filter

Authentication

Agent

Satellite

Inheritance Source:

[Check inheritance source status](#)

Primary DNS:

Secondary DNS:

☐ Inherit DNS Suffixes

DNS Suffix:

1 item → ×

☒ IP POOL

☒ 192.168.1.245-192.168.1.249

+ Add - Delete ↑ Move Up ↓ Move Down

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

0 items → ×

ACCESS ROUTE

Enter subnets need to be accessed by clients (e.g. 172.16.1.0/24)

+ Add - Delete

These routes will be added to the client's routing table

OK Cancel

Click OK and commit all changes. You are now ready for the PC side configuration

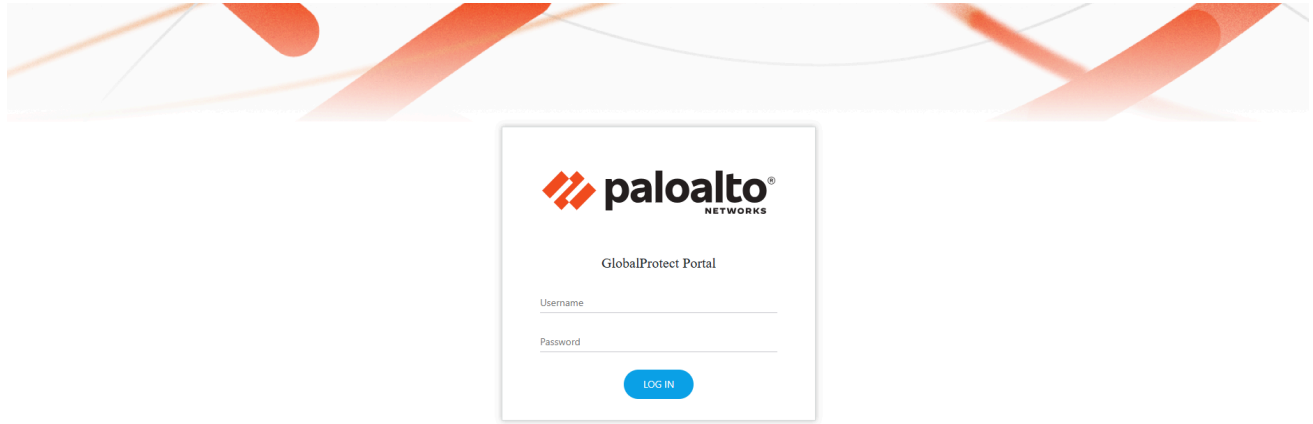
PC configuration

This section isn't needed if deploying GlobalProtect through Group policy

Due to the way we set up this deployment, upon joining the portal your PC will download the certificates once authenticated by user.

1. Navigate to the IP you set for your portal (10.2.191.10)

2. You should see the below screen



3. Login using your Active Directory Credentials, which will bring you to the below screen



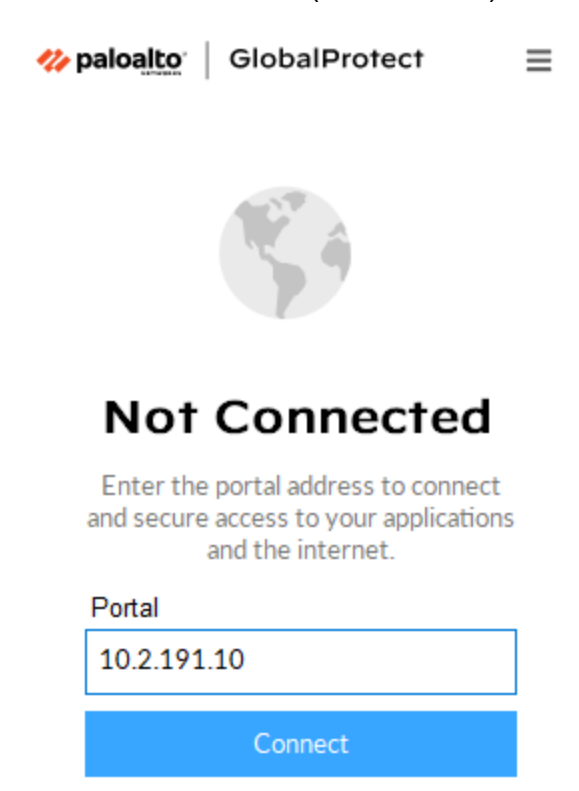
4. Download the corresponding agent to your OS

1. You do not have to change anything so just next through the installer and let it install.

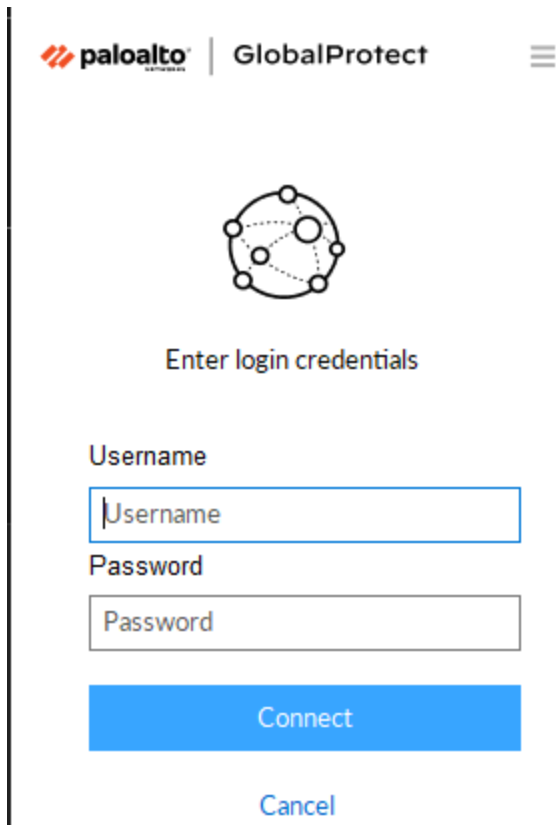
5. Click get started



6. Enter Portal address (10.2.191.10) and connect



7. It will ask for your credentials once again, enter them and hit connect.



The image shows the Palo Alto GlobalProtect login interface. At the top, the Palo Alto logo and 'GlobalProtect' text are visible. Below this is a network diagram icon. The text 'Enter login credentials' is centered. There are two input fields: 'Username' and 'Password'. Below the password field is a blue 'Connect' button and a blue 'Cancel' link.

It will now show you connected to the portal.



Verifications

1. For our first verification we can refer to the above picture. If it shows connected then we are working.

2. We can also look in the logs located at *Monitor-Logs-GlobalProtect*

RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	SOURCE REGION	HOST NAME	PUBLIC IPV4	PUBLIC IPV6	HOST ID	AUTH METHOD	ERROR
04/17 08:20:00	GP1	success	host-info	gateway-hip-report	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:20:00	GP1	success	host-info	gateway-hip-check	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:20:00	GP1	success	tunnel	gateway-tunnel-latency	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	host-info	gateway-hip-report	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	host-info	gateway-hip-check	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	tunnel	gateway-tunnel-latency	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	connected	gateway-connected	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:40	GP1	success	tunnel	gateway-setup-ipsec	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:40	GP1	success	agent-msg	gateway-agent-msg	s237.training.ast...	10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0			
04/17 08:19:35	GP1	success	configuration	gateway-getconfig	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:34	GP1	success	login	gateway-register	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300		
04/17 08:19:34	GP1	success	login	gateway-auth	calehamm	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:34	GP1	success	before-login	gateway-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	
04/17 08:19:33	GP1	success	configuration	portal-getconfig	s237.training.ast...	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:33	GP1	success	login	portal-auth	calehamm	10.0.0.0-10.255.255.255	8FQH7Y2	10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	ldap	
04/17 08:19:32	GP1	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	
04/17 08:18:52	GP1	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.8.128.41	0.0.0.0	b361539b-1785-44fe-a01b-bc892bd56300	Certificate	

We're looking specifically for the log showing "calehamm" (or your user) and "gateway auth" showing successful

3. Finally we can navigate to *ACC-Network Activity*

1. This will show us the traffic being sent over our user.