Configuring GlobalProtect

Tech Note

PAN-OS 4.1

Revision E

Contents

Overview

GlobalProtect provides security for host systems, such as laptops, that are used in the field by allowing easy and secure login from anywhere in the world. With GlobalProtect, users are protected against threats even when they are not on the enterprise network, and application and content usage is controlled on the host system to prevent leakage of data, etc. With PAN-OS release 4.1, GlobalProtect replaces NetConnect functionality. This document also covers, configuring GlobalProtect for remote access VPN replacing NetConnect

GlobalProtect Elements

There are three essential components that make up the GlobalProtect solution:

- GlobalProtect Portal: A Palo Alto Networks next-generation firewall that provides centralized control over the GlobalProtect system. Portal maintains the list of all Gateways, certificates used for authentication, and the list of categories for checking the end host.

- GlobalProtect Gateway: One or more interfaces on one or more Palo Alto Networks next-generation firewalls that provide security enforcement for traffic from the GlobalProtect Client. The Gateways can be either internal i.e. in the LAN or external, where they are deployed to be reachable via the public internet

- GlobalProtect Client: The client/Agent software on the laptop that is configured to connect to the GlobalProtect deployment.

License requirements

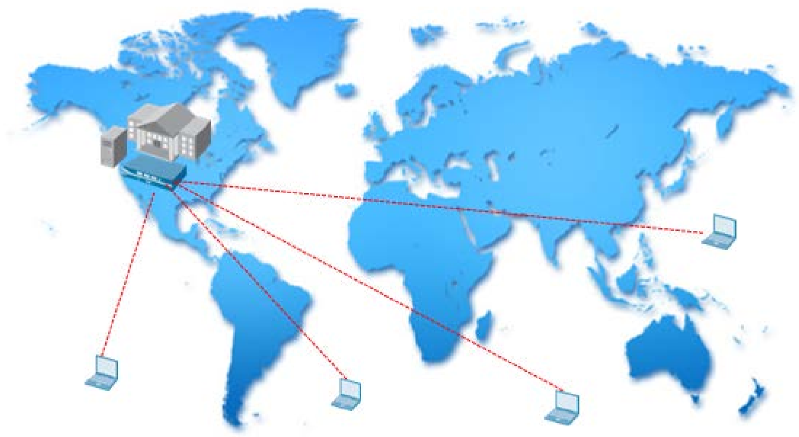
GlobalProtect portal license is one time permanent license. The gateway license is a one or three year subscription license.

1. No license is required for single portal/ gateway deployment without Host checks
2. Only a portal license is required for multiple gateway deployment without Host check
3. Portal license and gateway subscription license is required when Host check is implemented, either with single or multiple gateways

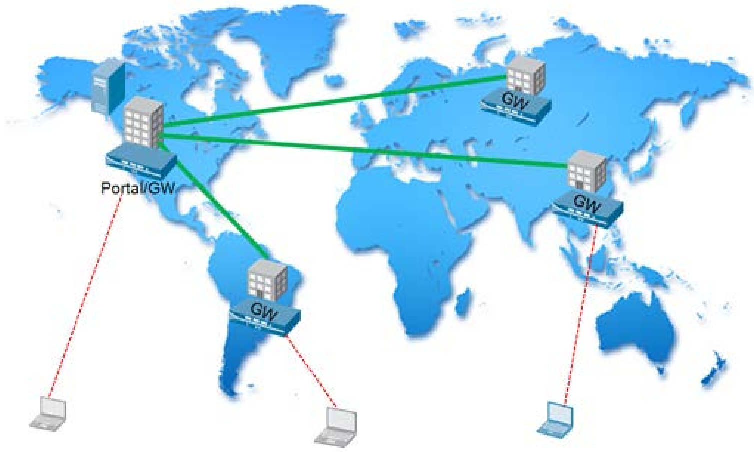
Deployment Topologies

The simplest form of deployment is a single firewall acting as both the Gateway and Portal. For larger deployments, geographically dispersed Gateways and a centralized Portal are used. This allows the Client to connect to the closest Gateway. Some of the common deployment topologies are shown below.

Single gateway for remote access VPN



Multiple Gateways



NetConnect Functionality - GlobalProtect for Remote Access VPN

This section provides configuration example of using GlobalProtect for remote access VPN. This is applicable for PAN-OS release 4.1, where NetConnect function is no longer available. Use this configuration for just remote access, with no host checks or multiple gateways, similar to NetConnect.

Note: This feature does not require both the GlobalProtect gateway and portal license.

Hardware and Software requirements

- All Palo Alto Networks firewall
- PAN-OS version 4.1
- GlobalProtect Client: Download and activate the GlobalProtect Client. GlobalProtect Client supports 32-bit XP, both 32-bit and 64-bit of Vista and Windows 7, Mac OS 10.6

Network Topology

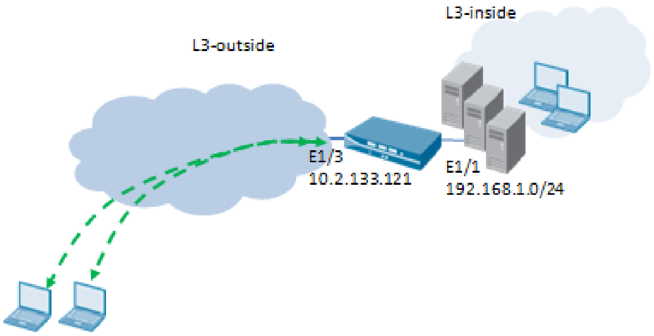
In this example, the firewall will be configured with details shown below

- Tunnel interface : Tunnel interface for VPN termination
- Authentication method: Local
- DNS Server: 10.0.0.246
- IP pool : 172.16.1.1- 172.16.1.250
- DNS suffix: mycompany.com
- Access route: 192.168.1.0/16

Interface	Comment	Zone	Virtual Router
Ethernet 1/3	Outside interface. This is IP address of the Portal and Gateway	L3-outside	default
Ethernet 1/1	Inside interface. Connects to protected resource	L3-inside	default
Tunnel	Logical interface for terminating VPN tunnel	VPN	default

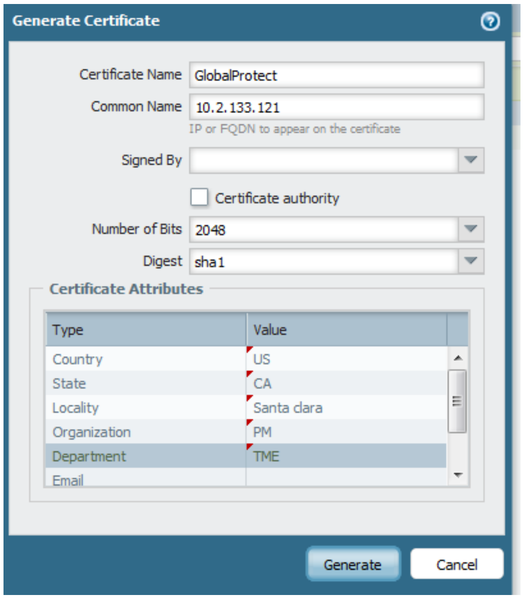
Note:

1. By binding the tunnel interface in the same zone as the interface connecting the protected resources, the remote users can access the resource without the need of security policy coming through the tunnel. For stricter policy enforcement it is recommended to assign the tunnel interface to its own zone, example VPN zone and then create policies between the VPN zone and L3-inside to securely enable access to the protected resources
2. Loopback interface can also be used as the portal and gateway interface



Step1: Create Server Certificate

Create a certificate with similar parameters as shown to be used by the Portal and Gateway. The common name must be the IP address of the FQDN of the interface where the remote users connect to.



Generate Certificate

Certificate Name: GlobalProtect

Common Name: 10.2.133.121

IP or FQDN to appear on the certificate

Signed By:

□ Certificate authority

Number of Bits: 2048

Digest: sha1

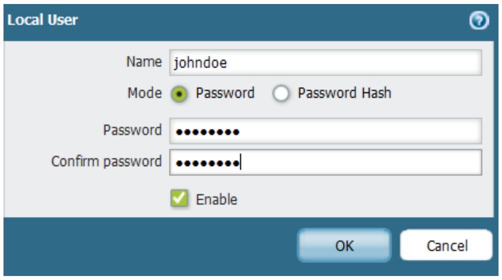
Certificate Attributes

Type	Value
Country	US
State	CA
Locality	Santa clara
Organization	PM
Department	TME
Email	

Step2: Configuring User Authentication

Identify the authentication method that will be using to authenticate GlobalProtect users. Palo Alto Networks next-generation firewalls support local database, LDAP, RADIUS or Kerberos authentication servers for authenticating users. In this example we will use the local database for authenticating users.

To create a local users navigate to **Device > Local User Database > Users** and click on add to add a new user.



Local User

Name: johndoe

Mode: ● Password ○ Password Hash

Password: ••••••••

Confirm password: ••••••••

☑ Enable

Note: To learn more about using other mechanism of user authentication refer to the section Configuring User authentication

Step3: Create a Tunnel Interface

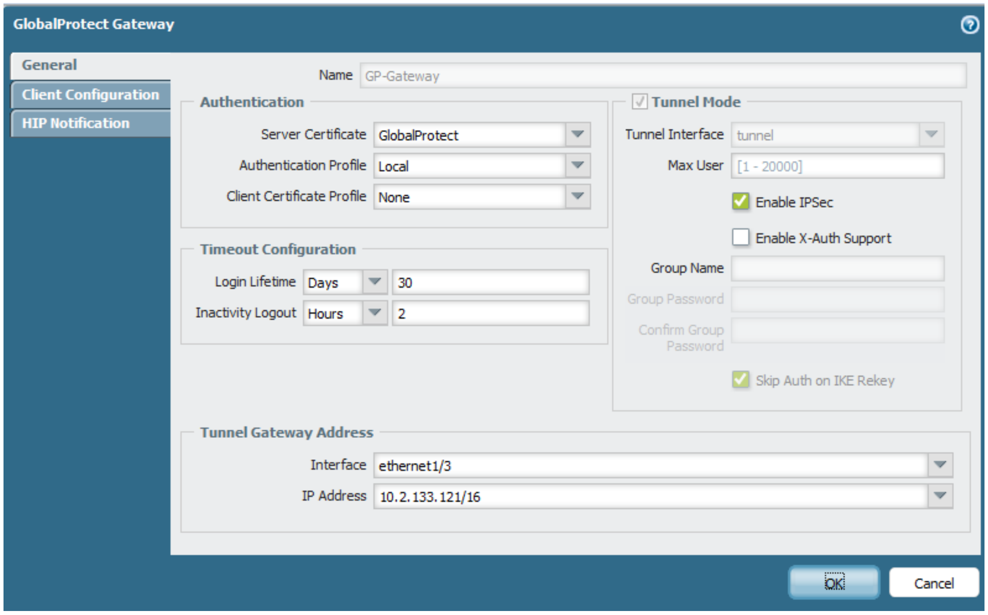
The tunnel interface is a logical interface that is only used for terminating VPN tunnels. It can be used both for site-to-site IPSec VPN and remote access VPN. There is a pre-defined tunnel interface “tunnel”. You can use either the pre-defined tunnel interface or create a separate tunnel interface. In this example we use the pre-defined tunnel interface. The tunnel interface must also be assigned to a virtual router and bound to a security zone.

Step4: Configure the Gateway

The remote access connections from users terminate on the gateway.

General Tab

Specify the gateway name and select the server certificate created in Step1
If you want the remote users to establish a secure connection using IPSec to the gateway, select "Tunnel Mode" , selecct the tunnel interface and check "Enable IPSec".
In the tunnel gateway address section, select the egress interface address from drop down. The IP address will be filled in automatically once the interface is selected.



Name: GP-Gateway

Authentication
Server Certificate: GlobalProtect
Authentication Profile: Local
Client Certificate Profile: None

Timeout Configuration
Login Lifetime: Days 30
Inactivity Logout: Hours 2

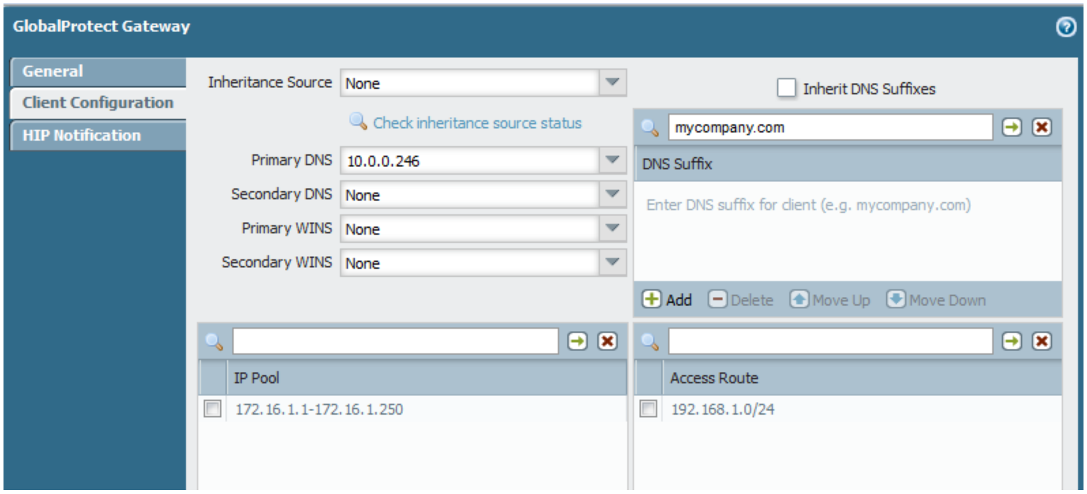
☑ Tunnel Mode
Tunnel Interface: tunnel
Max User: [1 - 20000]
☑ Enable IPSec
☐ Enable X-Auth Support
Group Name:
Group Password:
Confirm Group Password:
☑ Skip Auth on IKE Rekey

Tunnel Gateway Address
Interface: ethernet1/3
IP Address: 10.2.133.121/16

Note: Enable X-Auth Support to enable mobile devices, like Apple's iOS devices to establish IPSec tunnel to the gateway. Starting with Pan-OS release 4.1.6 , IPSec tunnels from Android devices are also supported.

Client Configuration tab

In this section, configure the IP pool , DNS server IP address, and DNS suffix that will be assigned to the client virtual adapterd upon successful connection. In the access routes specify the networks, the traffic to which will routed be through the tunnel. In this example, any traffic to subnet 192.168.1.0/24 will be encrypted and routed through the tunnel to the gateway using the virtual adapter. All other traffic is unencrypted and is routed using the physical interface of the host.



Inheritance Source: None

Primary DNS: 10.0.0.246

Secondary DNS: None

Primary WINS: None

Secondary WINS: None

☐ Inherit DNS Suffixes

mycompany.com

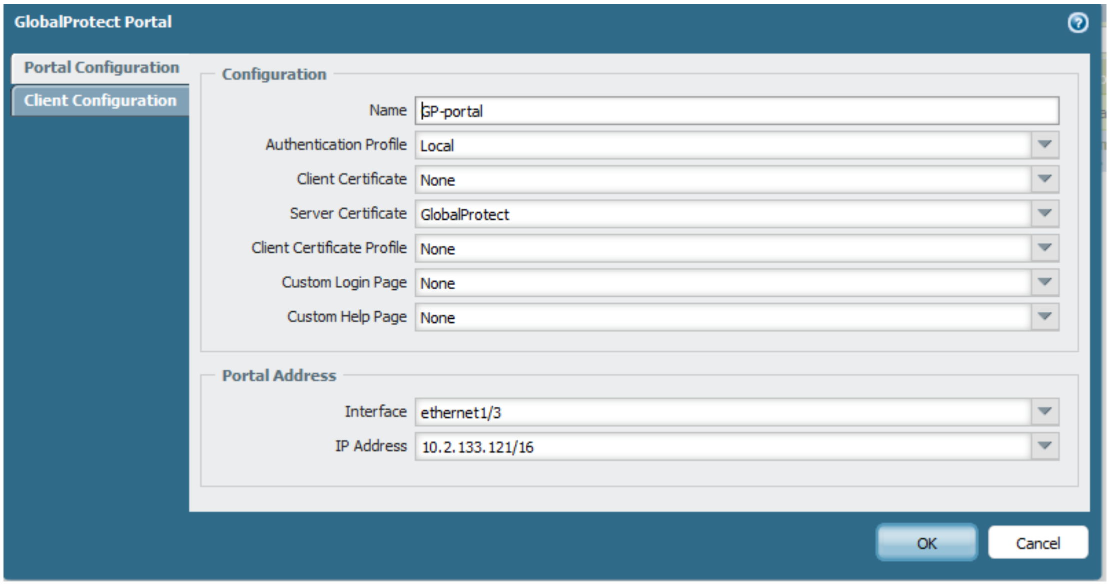
DNS Suffix
Enter DNS suffix for client (e.g. mycompany.com)

IP Pool
☐ 172.16.1.1-172.16.1.250

Access Route
☐ 192.168.1.0/24

Step5: Configure Portal

Portal configuration requires, specifying the certificate required by the gateway, authentication method used by portal, and optional client certificates.



Configuration

Name: GP-portal

Authentication Profile: Local

Client Certificate: None

Server Certificate: GlobalProtect

Client Certificate Profile: None

Custom Login Page: None

Custom Help Page: None

Portal Address

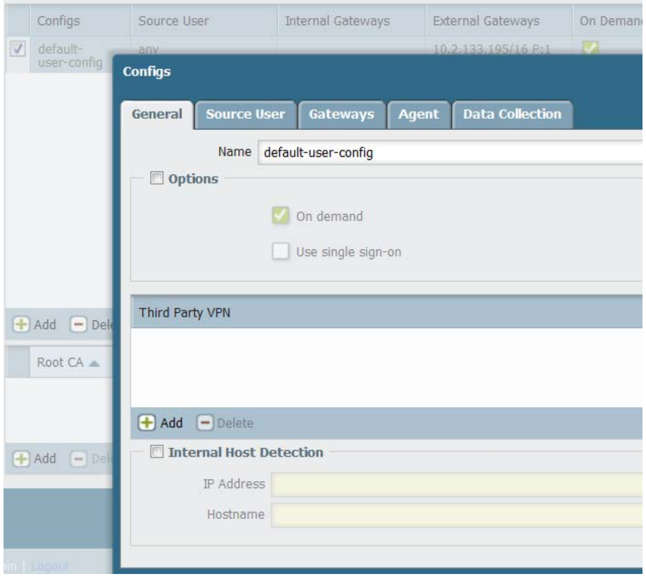
Interface: ethernet1/3

IP Address: 10.2.133.121/16

Portal Configuration
Name: Identifier for the portal
Authentication Profile: The authentication method used for authenticating the remote users.
Server Certificate: From the drop down list choose the Certificate create in Step1
Portal Address: From the drop down list, select the egress interface to which the remote users establish IPSec tunnel

Client configuration
Click on ADD to create new client configuration. The client configuration section on the portal controls the behavior of the GlobalProtect agent on the end hosts

Under the "General Tab" the "On demand" option enables the end users to activate the GlobalProtect agent when they want to connect to the gateway.



Configs	Source User	Internal Gateways	External Gateways	On Deman
☑ default-user-config	any		10.2.133.195/16 P:1	✓

Name: default-user-config

☐ Options

☑ On demand

☐ Use single sign-on

Third Party VPN

☐ Internal Host Detection

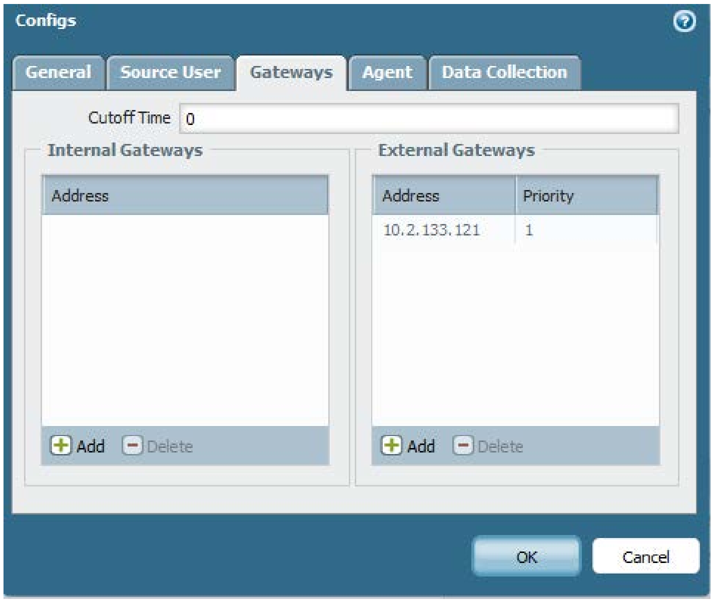
IP Address:

Hostname:

Gateways

Under the gateway section specify the IP address or FQDN of the egress interface address of the firewall where the remote VPN tunnels are established. In this example the external gateway IP address is the IP address of the ethnernet1/3 interface 10.2.133.121. The priority of the gateway is not applicable in this case, where there is only gateway (the default value is 1).

Note: In this scenario, no internal gateways need to be specified.



Cutoff Time: 0

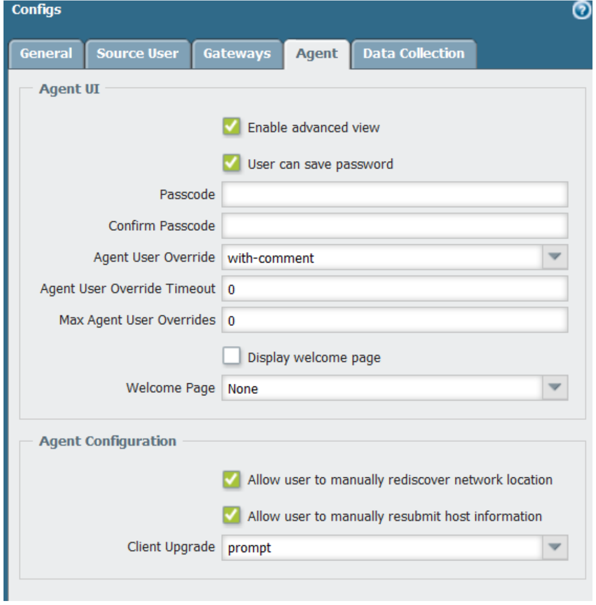
Internal Gateways

Address

External Gateways

Address	Priority
10.2.133.121	1

Agent Tab



Agent UI

☑ Enable advanced view

☑ User can save password

Passcode:

Confirm Passcode:

Agent User Override: with-comment

Agent User Override Timeout: 0

Max Agent User Overrides: 0

□ Display welcome page

Welcome Page: None

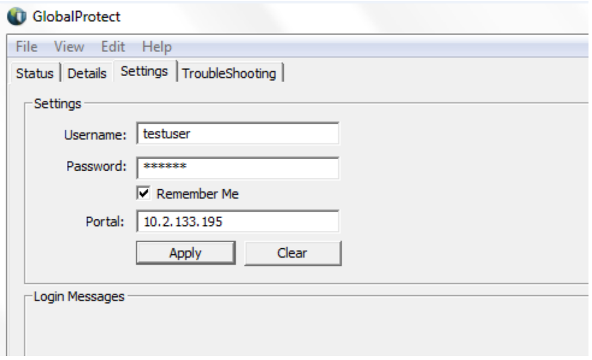
Agent Configuration

☑ Allow user to manually rediscover network location

☑ Allow user to manually resubmit host information

Client Upgrade: prompt

Enable advanced view
Allows the end users to select advanced view section of the agent which includes details, settings, and troubleshooting tabs



Settings

Username: testuser

Password: ******

☑ Remember Me

Portal: 10.2.133.195

Login Messages

Tip: It is recommended to disable Advanced View for agents to prevent users from changing settings.

User can save password: Allows the user to save the password in the GlobalProtect client
Client Upgrade: The end users will be prompted for upgrade when a new version of client is available. The "transparent" option will automatically download the newer version of agent when available without prompting the user for upgrade

Step 6: Download and Activate the GlobalProtect Client

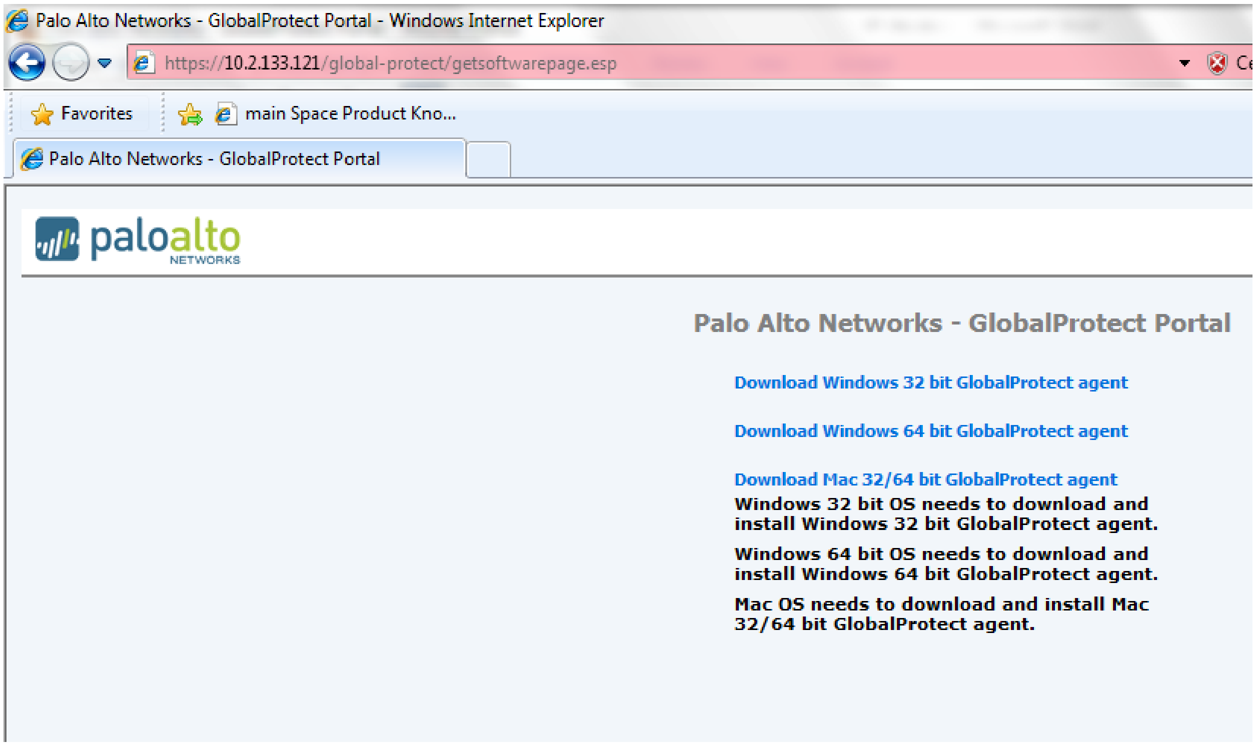
Before testing connectivity, you must download and activate the GlobalProtect client. This is done by navigating to Device > GlobalProtect Client. When a new version of the client becomes available, you can download and activate the new client for the remote users.

Note: Admin rights to the client machine are required for the first install of GlobalProtect client. Once the client is installed, subsequent client upgrades do not require admin rights.

Tip: If you set the client upgrade to transparent as described in the section above, when new client is activated, it will be downloaded to the client machines and the client upgraded automatically with users intervention.

Client connection

If the GlobalProtect client is not installed on the end host, the client msi file required for installation can be downloaded directly from the firewall. To download the client msi file, browse to the address portal/gateway. In this example the address 10.2.133.121 is used.


Palo Alto Networks - GlobalProtect Portal - Windows Internet Explorer
https://10.2.133.121/global-protect/getsoftwarepage.esp
Favorites
main Space Product Kno...
Palo Alto Networks - GlobalProtect Portal
paloalto NETWORKS

Palo Alto Networks - GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

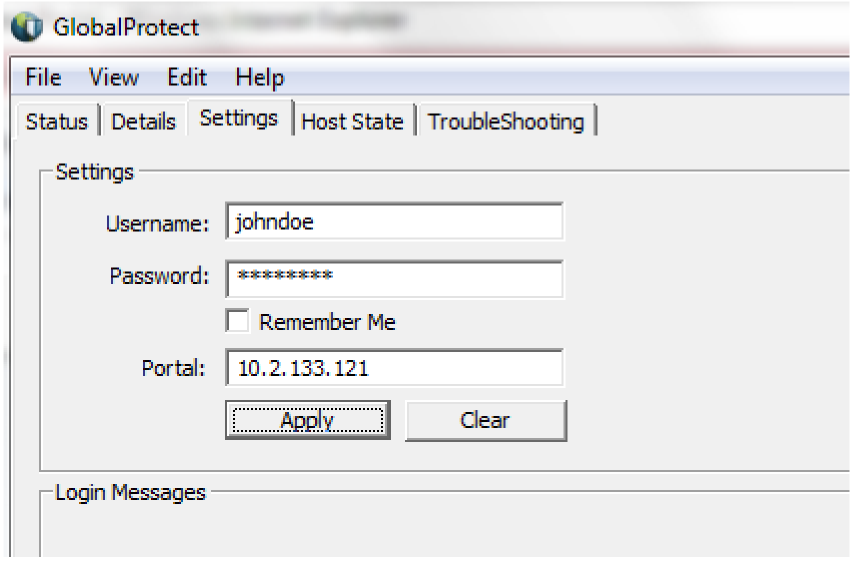
Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.

Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.

Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

Adminstrator privileges are required to install the GlobalProtect client for the first time. To distribute the client to multiple hosts, refer to the section Distributing GlobalProtect Client

Configure the client to connect to the gateway. Click on apply to connect



Settings

Username: johndoe

Password: *********

□ Remember Me

Portal: 10.2.133.121

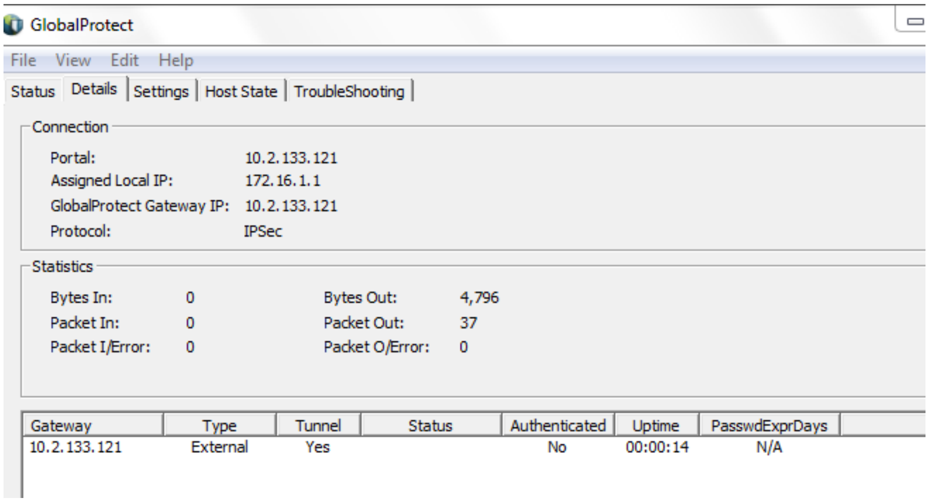
Login Messages

Note: If the portal has FQDN associated with the IP address, enter the hostname without the “ https:” in the portal section.

Verification

You can view the connection state on the client machine, by viewing the GlobalProtect Client setting tab.

Note: In order to view the settings tab, enable advanced view must be checked on the portal.



Connection

Portal: 10.2.133.121
Assigned Local IP: 172.16.1.1
GlobalProtect Gateway IP: 10.2.133.121
Protocol: IPSec

Statistics

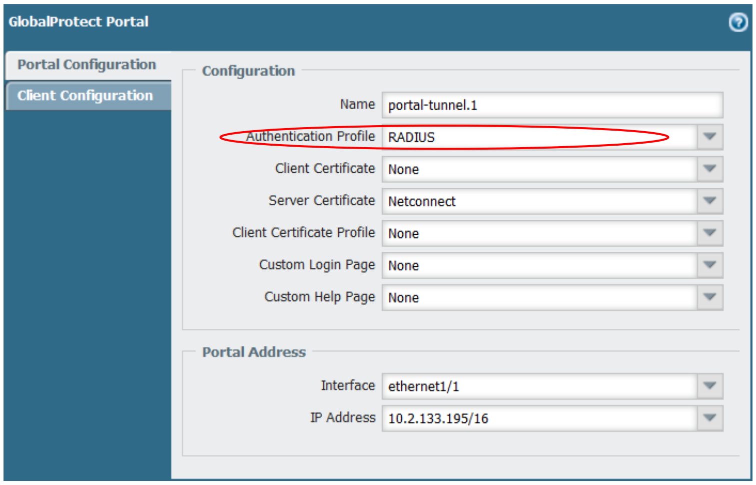
Bytes In:	0	Bytes Out:	4,796
Packet In:	0	Packet Out:	37
Packet I/Error:	0	Packet O/Error:	0

Gateway	Type	Tunnel	Status	Authenticated	Uptime	PasswdExprDays
10.2.133.121	External	Yes		No	00:00:14	N/A

OTP Considerations

The GlobalProtect agent will authenticate to the portal and the gateway before establishing the connection. This is different from the NetConnect behavior where the clients authenticate once to the NetConnect gateway. When using OTP (One Time Password) for authentication, the users will be prompted to enter the password twice, once each for the portal and gateway in order to establish the tunnel.

If you prefer that the end users input the password only once, but still use OTP as an authentication method, you can configure the portal to use a different authentication method such as RADIUS and have the gateway use OTP for authentication. On the GlobalProtect agent, configure the username and password used to authenticate against the portal. Upon the first connect, the agent will send this credential to authenticate against the portal, and then prompt for a new password to connect to the gateway. The configuration snap shot of both the portal and gateway for such scenario is shown below.



GlobalProtect Portal

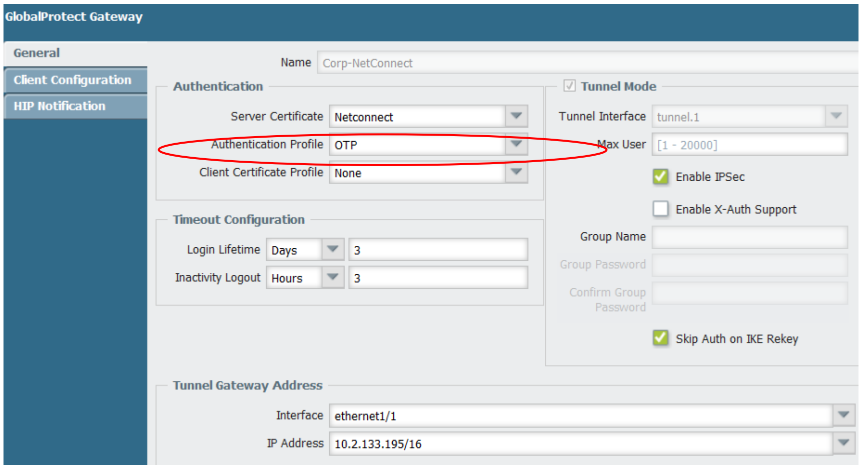
Portal Configuration
Client Configuration

Configuration

Name portal-tunnel.1
Authentication Profile RADIUS
Client Certificate None
Server Certificate Netconnect
Client Certificate Profile None
Custom Login Page None
Custom Help Page None

Portal Address

Interface ethernet1/1
IP Address 10.2.133.195/16



GlobalProtect Gateway

General
Client Configuration
HIP Notification

Name Corp-NetConnect

Authentication

Server Certificate Netconnect
Authentication Profile OTP
Client Certificate Profile None

Timeout Configuration

Login Lifetime Days 3
Inactivity Logout Hours 3

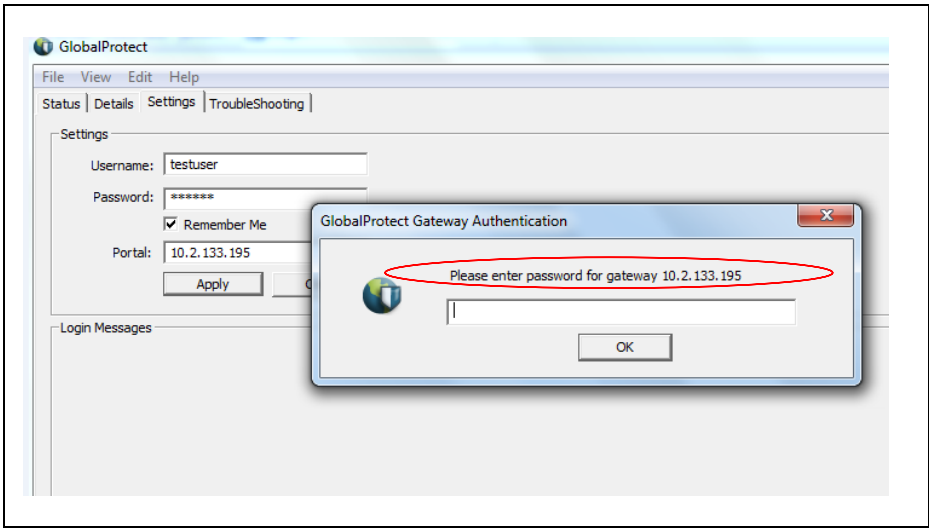
☑ Tunnel Mode

Tunnel Interface tunnel.1
Max User [1 - 20000]
☑ Enable IPSec
☐ Enable X-Auth Support
Group Name
Group Password
Confirm Group Password
☑ Skip Auth on IKE Rekey

Tunnel Gateway Address

Interface ethernet1/1
IP Address 10.2.133.195/16

The end user will be prompted for authenticating to gateway after connecting to the portal as shown in the following screenshot:


GlobalProtect
File View Edit Help
Status Details Settings TroubleShooting
Settings
Apply
Login Messages
GlobalProtect Gateway Authentication
OK

Username: testuser

Password: ******

☑ Remember Me

Portal: 10.2.133.195

Please enter password for gateway 10.2.133.195

Verification

Viewing the active flow

```
admin@PA-5060-2> show global-protect-gateway flow

total tunnels configured:                             1
filter - type GlobalProtect-Gateway, state any

total GlobalProtect-Gateway tunnel shown:             1

id     name                  local-i/f         local-ip         tunnel-i/f
--------------------------------------------------------------------------------
------------------
8      GP-Gateway            ethernet1/3       10.2.133.121     tunnel
```

```
admin@PA-5060-2> show global-protect-gateway flow tunnel-id 8

tunnel  GP-Gateway
        id:                  8
        type:                GlobalProtect-Gateway
        local ip:            10.2.133.121
        inner interface:     tunnel           outer interface:  ethernet1/3
        ssl cert:            GlobalProtect
        active users:        1

assigned-ip      remote-ip       encapsulation
-----------------------------------------------------------------------------
172.16.1.1       10.20.1.193     IPSec SPI 7DB25D3E (context 3)
```

Viewing the gateway configuration

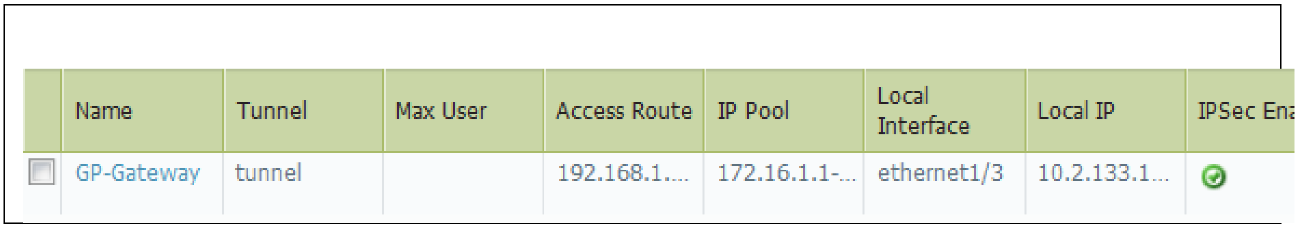
```
admin@PA-5060-2> show global-protect-gateway gateway name GP-Gateway

        GlobalProtect Name   : GP-Gateway
        Tunnel ID            : 8
        tunnel-interface     : tunnel
        encap-interface      : ethernet1/3
        inheritance-from     :
        Local Address        : 10.2.133.121
        SSL server port      : 443
        IPSec encap          : yes
        tunnel negotiation   : ssl
        HTTP redirect        : no
        UDP port             : 4501
        Max users            : 0
        IP pool ranges       : 172.16.1.1 - 172.16.1.20;
        DNS servers          : 10.0.0.247
                             : 0.0.0.0
        WINS servers         : 0.0.0.0
                             : 0.0.0.0
        Access routes        : 192.168.1.0/24;
        VSYS                 : vsys1 (id 1)
        SSL Server Cert      : GlobalProtect
        Auth Profile         : Local
        Client Cert Profile  :
        Lifetime             : 2592000 seconds
        Idle timeout         : 7200 seconds
```

Viewing the connected users

```
show global-protect-gateway current-user user
OR
show user ip-user-mapping type GP all
```

From Network > GlobalProtect > Gateway choose “More users info”.



	Name	Tunnel	Max User	Access Route	IP Pool	Local Interface	Local IP	IPSec Ena
☐	GP-Gateway	tunnel		192.168.1....	172.16.1.1-...	ethernet1/3	10.2.133.1...	✓

Configuring GlobalProtect with Multiple Gateways and Host Checks

Note: This requires purchasing GlobalProtect Portal license and Gateway subscription license.

Sequence of steps

This section covers the sequence of steps when an end host connects to the GlobalProtect system for the first time.

1. User makes an SSL connection to the Portal and authenticates.
2. Upon successful authentication, the user is prompted to download the Client software. The Client files for both 32bit and 64bit OS are available.
3. The downloaded Client is installed and configured with username/password and the IP address or FQDN of the Portal to connect to.
4. After a successful authentication, portal will send client, the configuration and the client certificate The client configuration will contain the following:
   a) The gateway list (both internal and external)
   b) (Optional) The DNS name/IP mapping that GlobalProtect Client uses to determine if the PC is inside or outside the office. This is used to determine if the Client must connect to an internal or external Gateway.
   c) Trusted CAs Client software should use to verify the gateways belong to the same organization.
   d) Host information data collection instructions that Client software should report, e.g. OS version, AV version, disk encryption version, specific registry key/value, etc.
   e) Base64 embedded client certificate that allows client to authenticate itself when connecting to gateways.
   f) Third-Party VPN Clients that should be allowed to run.
   g) Client users override policy.
   h) Portal Client software version. This is to allow the Client software to determine if a different version is available.
5. At this point, the Client will obtain the host information, and find the closest Gateway to connect to.
6. If the client determines that the user is inside the network and the gateway is the internet firewall, then the Client can connect to multiple internal Gateways, authenticate, update the host information profile (HIP) and have access through the Gateways which may be using HIP-augmented policies.
7. If the Client determines that the user is outside the internal network, then the Client will find the closest external Gateway, authenticate, establish a SSL VPN tunnel, and then provide the HIP.
8. The gateway provides notifications as configured back to the Client for user notification.
9. The gateway enforces the security policy based on user, application, content and the HIP submitted from the Client.

The following list of items is required to configure GlobalProtect:

1. IP address of the Authentication server and type of authentication method
2. IP address for Portal and Gateway
3. Access to CA server to generate certificate.

4. Licenses- License for GlobalProtect Portal and Gateway is required. If there are multiple Gateways managed by the Portal, a license for each Gateway is required

Note: Step 3 is not required if you are using the Palo Alto Networks next-generation firewall as the CA server.

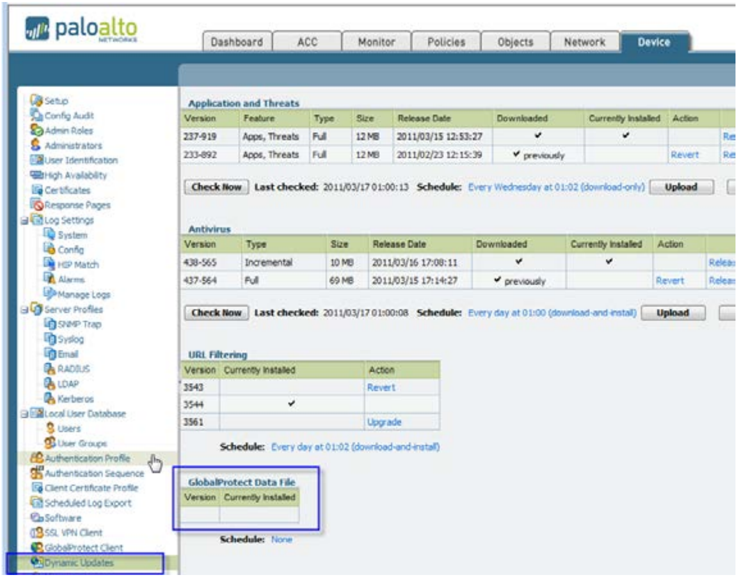
Note: For external deployments, if the portal and gateway are using private address, these IP addresses must be mapped to a public IP address using NAT.

Software Requirements

- PAN-OS version 4.1
- GlobalProtect Client: Download and activate the GlobalProtect Client. GlobalProtect Client supports 32-bit XP, both 32-bit and 64-bit of Vista and Windows 7, Mac OS 10.6 and 10.7
- Latest Application and Threats, Antivirus is required and the GlobalProtect data file

Note

- Configure schedule for GlobalProtect Data File (Device>Updates). This is required to download the OPSWAT data file.
- IOS and MAC OS support requires PAN-OS 4.1.



Application and Threats

Version	Feature	Type	Size	Release Date	Downloaded	Currently Installed	Action	
237-919	Apps, Threats	Full	12 MB	2011/03/15 12:53:27	✓	✓		Re
233-892	Apps, Threats	Full	12 MB	2011/02/23 12:15:39	✓ previously		Revert	Re

Check Now **Last checked:** 2011/03/17 01:00:13 **Schedule:** Every Wednesday at 01:02 (download-only) Upload

Antivirus

Version	Type	Size	Release Date	Downloaded	Currently Installed	Action	
438-565	Incremental	10 MB	2011/03/16 17:08:11	✓	✓		Relea
437-564	Full	69 MB	2011/03/15 17:14:27	✓ previously		Revert	Relea

Check Now **Last checked:** 2011/03/17 01:00:08 **Schedule:** Every day at 01:00 (download-and-install) Upload

URL Filtering

Version	Currently Installed	Action
3543		Revert
3544	✓	
3561		Upgrade

Schedule: Every day at 01:02 (download-and-install)

GlobalProtect Data File

Version	Currently Installed

Schedule: None

Configuration Steps

The following items are required to configure GlobalProtect. Configure the items listed in the following order:

1. Certificates
2. User Authentication
3. Gateway Configuration
4. Portal Configuration

Certificates

GlobalProtect uses certificates to authenticate the portal, gateway and clients. All certificates must be signed by the same CA.

The following certificates are required:

- CA certificate: Used to sign the gateway and client certificate.
- Gateway Certificate- Used to establish a secure tunnel between the GlobalProtect client and gateway.
- Client certificate-Used to establish a secure tunnel with the gateway and authenticate the client.

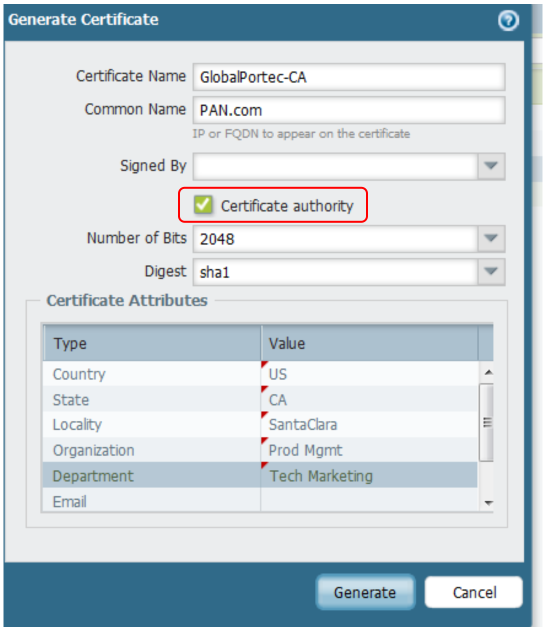
As of PAN-OS release 4.0, the Palo Alto Networks next-generation firewall itself can act as the CA server. In this example the firewall is configured as CA server and this certificate to sign Gateway and Client certificates.

Note: Certificate names must not have spaces between words.

Generating CA Certificate

Navigate to Device > Certificate > Generate

To generate a certificate and make it as the CA server certificate, check the box "certificate authority". This certificate must be used to sign the certificates used by the GlobalProtect gateway and the clients.



Generate Certificate

Certificate Name: GlobalPortec-CA

Common Name: PAN.com

IP or FQDN to appear on the certificate

Signed By:

☑ Certificate authority

Number of Bits: 2048

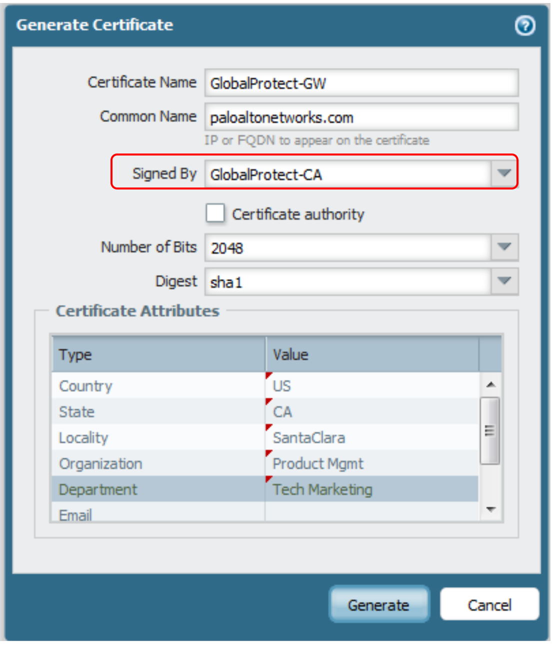
Digest: sha1

Certificate Attributes

Type	Value
Country	US
State	CA
Locality	SantaClara
Organization	Prod Mgmt
Department	Tech Marketing
Email	

Generating a Gateway certificate

This certificate is used by the GlobalProtect gateway to authenticate the clients. Use the Certificate Authority certificate generated earlier to sign this certificate. This is done by selecting the CA certificate generated earlier from the "signed by" drop down menu as shown below.



Certificate Name: GlobalProtect-GW

Common Name: paloaltonetworks.com

IP or FQDN to appear on the certificate

Signed By: GlobalProtect-CA

□ Certificate authority

Number of Bits: 2048

Digest: sha1

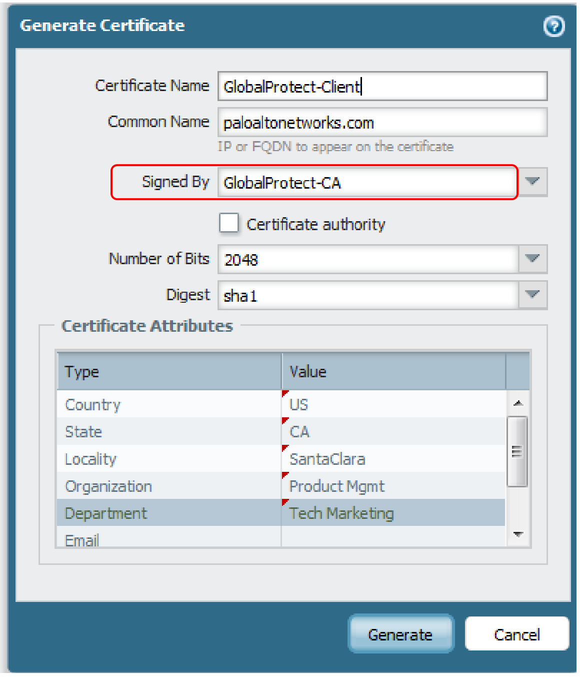
Certificate Attributes

Type	Value
Country	US
State	CA
Locality	SantaClara
Organization	Product Mgmt
Department	Tech Marketing
Email	

Note: Use the IP address of the interface or FDQN that maps to the IP in the common name field to avoid certificate errors.

Generating a Client Certificate

This Client certificate is used by the GlobalProtect clients to authenticate the GlobalProtect gateways. Please note, usage of client certificates is not necessary for authentication, but if used they do provide an elevated level of security. Using the client certificates also necessitates the distribution of these client certificates to all hosts that utilize the GlobalProtect client.



Certificate Name: GlobalProtect-Client

Common Name: paloaltonetworks.com

IP or FQDN to appear on the certificate

Signed By: GlobalProtect-CA

□ Certificate authority

Number of Bits: 2048

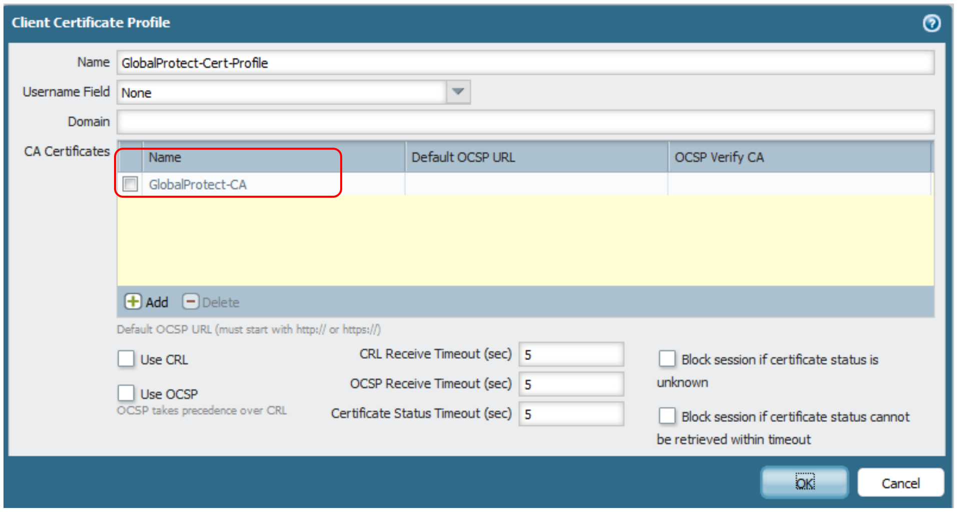
Digest: sha1

Certificate Attributes

Type	Value
Country	US
State	CA
Locality	SantaClara
Organization	Product Mgmt
Department	Tech Marketing
Email	

Creating a Client Certificate Profile

The client certificate profile is used to verify the certificates of every involved party. This specifies the CA server certificate that was used to sign the Gateway and the client certificate.
To create a profile, navigate to **Device > client certificate profile,** add the CA certificate generated earlier. This is the same certificate used to sign the Gateway and client certificate.



Client Certificate Profile

Name: GlobalProtect-Cert-Profile
Username Field: None
Domain:
CA Certificates:

	Name	Default OCSP URL	OCSP Verify CA
□	GlobalProtect-CA		

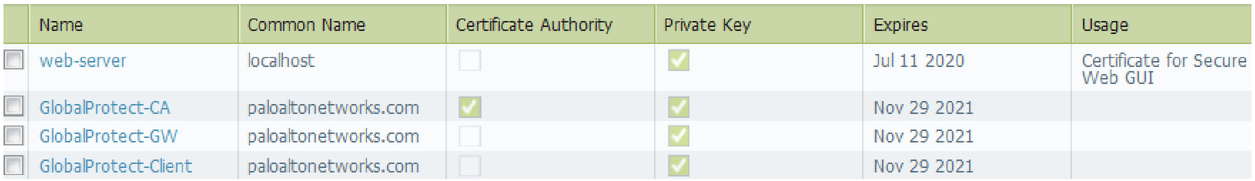
Default OCSP URL (must start with http:// or https://)

□ Use CRL
□ Use OCSP
OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5
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

The screen shot below shows the list of the certificates configured on the device. This is available from **Device > Certificates.**



	Name	Common Name	Certificate Authority	Private Key	Expires	Usage
□	web-server	localhost	□	☑	Jul 11 2020	Certificate for Secure Web GUI
□	GlobalProtect-CA	paloaltonetworks.com	☑	☑	Nov 29 2021	
□	GlobalProtect-GW	paloaltonetworks.com	□	☑	Nov 29 2021	
□	GlobalProtect-Client	paloaltonetworks.com	□	☑	Nov 29 2021	

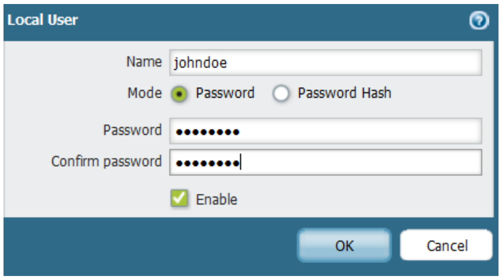
Configuring User Authentication

Identify the authentication method that you will be using to authenticate GlobalProtect users. Palo Alto Networks next-generation firewalls support the following authentication methods:

1. Local
2. LDAP
3. RADIUS
4. Kerberos

Local Database

To create a local users navigate to **Device>Local User Database>Users** and click on add to add a new user.



Name johndoe

Mode ● Password ○ Password Hash

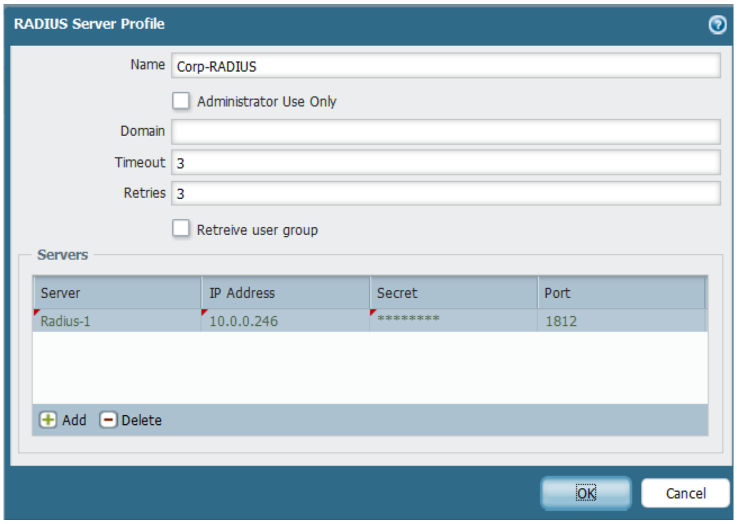
Password ••••••••

Confirm password ••••••••

☑ Enable

RADIUS

Navigate to ***Device > Server Profiles*** Specify the RADIUS server IP address, port and the shared secret.



Name Corp-RADIUS

□ Administrator Use Only

Domain

Timeout 3

Retries 3

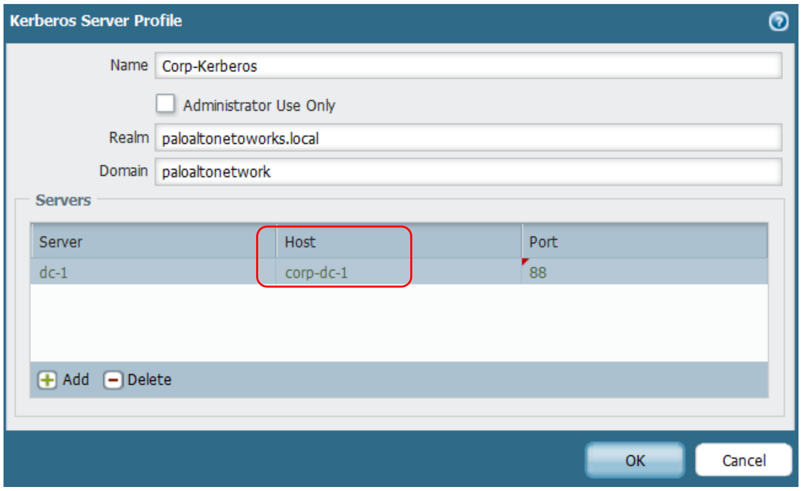
□ Retreive user group

Servers

Server	IP Address	Secret	Port
Radius-1	10.0.0.246	********	1812

Kerberos

Kerberos server profile has a realm (for hostname), a domain (NetBIOS style), FQDNs and optional port that represent the KDC (Key Distribution Center) for the domain. The realm represents the hostname part of account principle name i.e. login name. For example the user account name johndoe@paloaltonetworks.local has realm 'paloaltonetworks.local'. Domain is provided to allow the ability to use usernames in NetBIOS format in allow list in the format domainname\username.



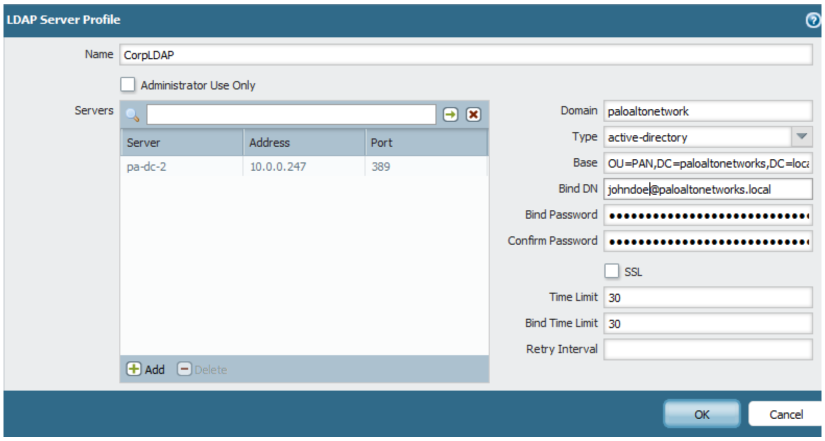
Name	Corp-Kerberos
	□ Administrator Use Only
Realm	paloaltonetoworks.local
Domain	paloaltonetwork

Servers

Server	Host	Port
dc-1	corp-dc-1	88

LDAP

Specify the IP address and the port number of the LDAP server, domain name, type of the server (active directory, e-directory, sun) and the base DN (the location in the LDAP hierarchy where the server must begin to search).



Name	CorpLDAP
	□ Administrator Use Only

Servers

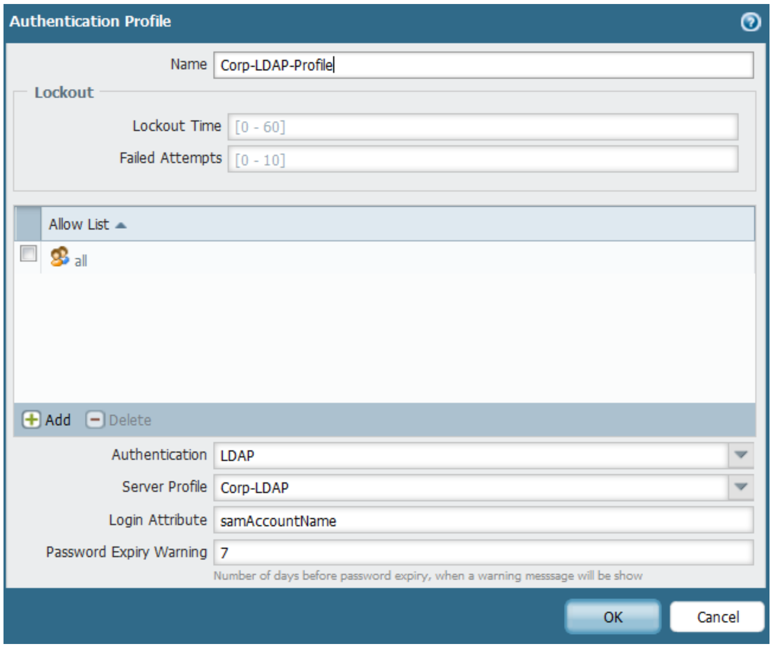
Server	Address	Port
pa-dc-2	10.0.0.247	389

Domain	paloaltonetwork
Type	active-directory
Base	OU=PAN,DC=paloaltonetworks,DC=loca
Bind DN	johndoe@paloaltonetworks.local
Bind Password	••••••••••••••••••••••••••••
Confirm Password	••••••••••••••••••••••••••••
	□ SSL
Time Limit	30
Bind Time Limit	30
Retry Interval	

Authentication Profile

The authentication profile refers to the authentication method configured in the previous step. The authentication profile is then used to associate the authentication method in the GlobalProtect Portal configuration. An example of using the LDAP database is shown below. Authentication profile using LDAP requires the “Login Attribute” field.

Note: The authentication profile name must not have any spaces between words.



Name: Corp-LDAP-Profile

Lockout Time: [0 - 60]

Failed Attempts: [0 - 10]

Allow List
□ all

Authentication: LDAP

Server Profile: Corp-LDAP

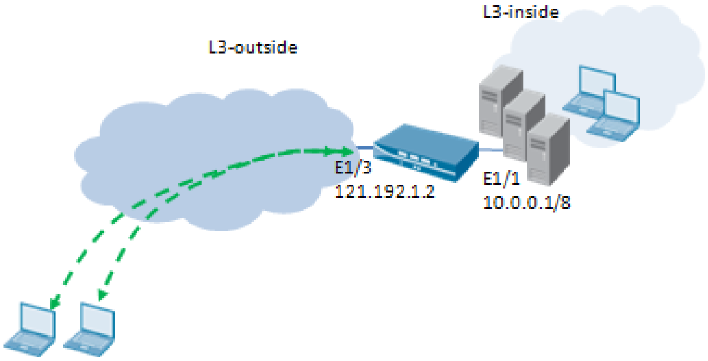
Login Attribute: samAccountName

Password Expiry Warning: 7

Number of days before password expiry, when a warning messsage will be show

Configuring the Gateway

The GlobalProtect Gateway provides the endpoint for the Client's connection. Once the client is connected, it sends all traffic through the Gateway. The Gateway(s) can be either external gateways or internal Gateways. External gateways require a tunnel. Internal gateways do not require tunnel. External gateways also support split tunnel. This is not recommended if you want to extend firewall policy with application control and visibility to all traffic from the users. The gateway(s) receive HIP profiles and allow enforcing a policy on it. In this configuration example we will refer to the following topology:



The interface and zone binding on the firewall are summarized below

Interface	Zone	Comment
Ethernet1/3	L3- outside	Global Protect Portal and Gateway interface
Ethernet1/1	L3-inside	Internal network
Tunnel.1	L3-GP	Global Protect Tunnel termination zone/interface

To configure the Gateway navigate to ***Network* > *GlobalProtect* > *Gateways.***

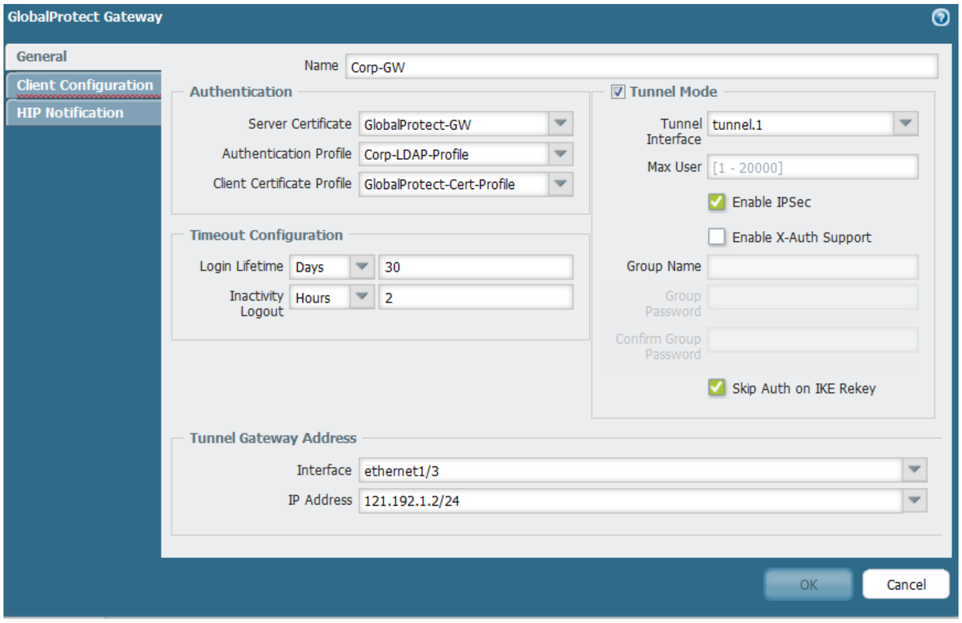
In this example we configure an external gateway. A tunnel interface is required when configuring external Gateway. The IPSec tunnel from the remote users is terminated on this tunnel interface.

Tip:

- When using external gateway, it is recommended to configure the tunnel interface in its own zone. This provides the ability to enforce a different security policy on the traffic from the remote users that are connected using GlobalProtect tunnel.
- In order to identify users, "Enable User Identification' must be checked on the zone where the tunnel interface is bound.
- In order to identify user IP address with internal gateways, the GlobalProtect client must not be configured to use to on demand mode. This is defined under *GP Portal configuration* > *options*.

Note:

1. When tunnel is used between the client and the gateway, the IP to user mapping will capture the IP address of the client virtual adapter.
2. With internal gateways, the IP to user mapping will capture the IP address of the client physical adapter.



Name: Corp-GW

Authentication
Server Certificate: GlobalProtect-GW
Authentication Profile: Corp-LDAP-Profile
Client Certificate Profile: GlobalProtect-Cert-Profile

Timeout Configuration
Login Lifetime: Days 30
Inactivity Logout: Hours 2

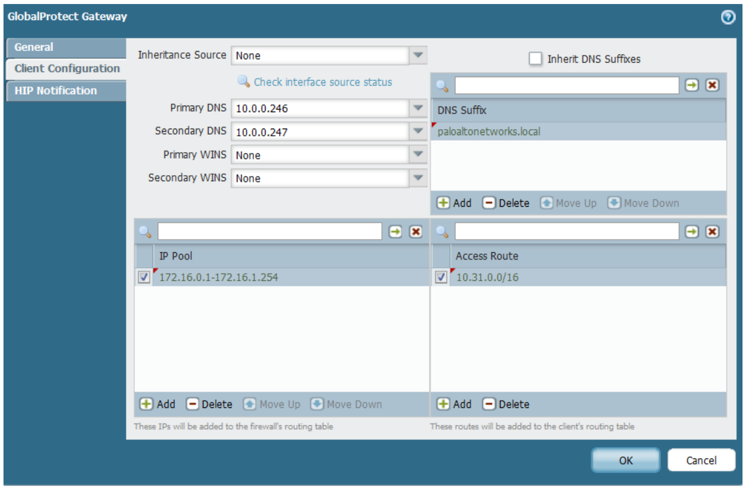
☑ Tunnel Mode
Tunnel Interface: tunnel.1
Max User: [1 - 20000]
☑ Enable IPSec
□ Enable X-Auth Support
Group Name:
Group Password:
Confirm Group Password:
☑ Skip Auth on IKE Rekey

Tunnel Gateway Address
Interface: ethernet1/3
IP Address: 121.192.1.2/24

<u>**General Tab:**</u>

Name: Enter the name of the GlobalProtect gateway.
Authentication: Choose the gateway certificate, client certificate profile and the user authentication profile.
Tunnel mode: Check this option if this is an external Gateway, and then select a tunnel interface. You can limit the number of users that can connect to the Gateway by specifying a number in the "max users" column.
Timeout Configuration: Specify the lifetime of the tunnel.
Tunnel Gateway Address: Select the interface that will be used as the gateway.

Client configuration tab:



Inheritance Source: None

□ Inherit DNS Suffixes

Primary DNS: 10.0.0.246

Secondary DNS: 10.0.0.247

Primary WINS: None

Secondary WINS: None

DNS Suffix
paloaltonetworks.local

	IP Pool
☑	172.16.0.1-172.16.1.254

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

	Access Route
☑	10.31.0.0/16

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

The client configuration is required only when using external gateway or connecting to internal gateway in tunnel mode. If tunnel mode is disabled, this section will be grayed out. When the client connects to the gateway using a tunnel, a virtual adapter is created and the networking configuration defined in the client configuration will be assigned to this client virtual adapter. Specify the DNS, WINS and DNS suffix to be used by the Client. Also specify the pool from which an IP addresses will be assigned to the client.

Note: If the client's physical adapters IP address overlaps with the IP pool defined on the gateway, the client will not get an IP address from the gateway. In this case, you will need to change the IP pool range, or define a second range of IP addresses.

Access routes

By default all traffic from the client will be sent to the gateway. Access routes, allow you to define networks that will be accessible by the client through the tunnel. This is also known as split tunneling.

Inheritance source

This is used when one of the firewall interfaces is configured as DHCP client, and you want the parameters like DNS server IP, WINS server IP and DNS suffix obtained by the DHCP client interface to be used by the GlobalProtect clients. From the "inheritance source" drop down select the DHCP client interface from which the DNS, WINS and DNS suffixes can be inherited.

Portal Configuration

To configure the Portal navigate to ***Network > GlobalProtect > Portal.***

Portal Configuration

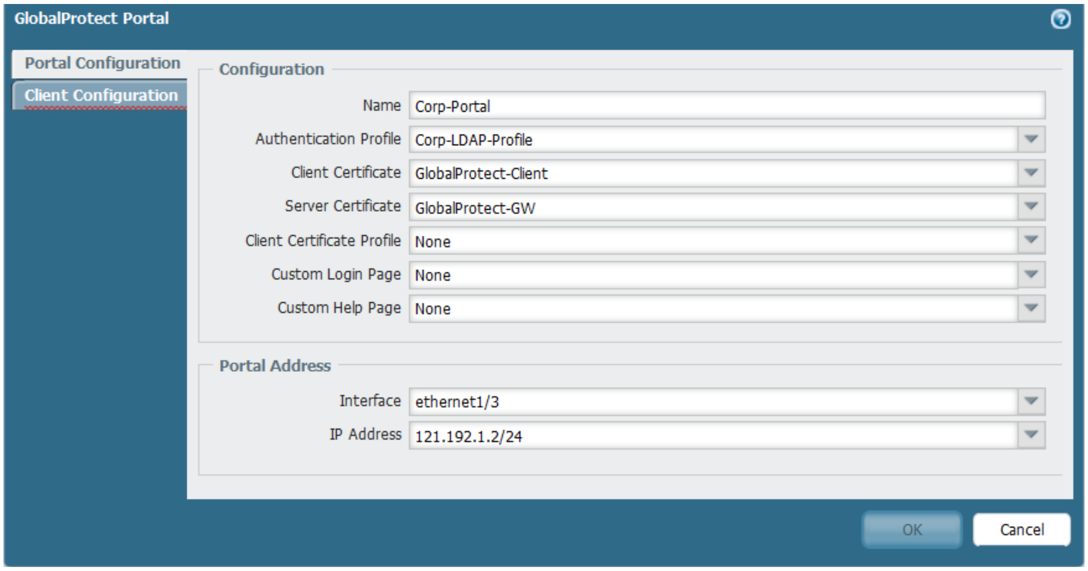
The authentication profile is used to authenticate users when the first browse to the Portal address to authenticate and downloads the GlobalProtect Client. The client and server certificate is used to authenticate the Client and the Portal. The certificates are sent to the Client when it first connects to Portal.

Portal IP address

From the interface drop down list choose the interface that will be used as the GlobalProtect Portal and specify the IP address of the interface. Referring to the topology we use in this example, Portal interface is loopback.1 with IP address of 192.168.50.57.

Note:

- If the firewall is deployed in active-active HA, the floating IP address can be used as the Portal IP address. In such deployment, select "floating IP address" as the choice
- PAN-OS version 4.1 supports both the Portal and Gateway using the same interface and IP address



Configuration

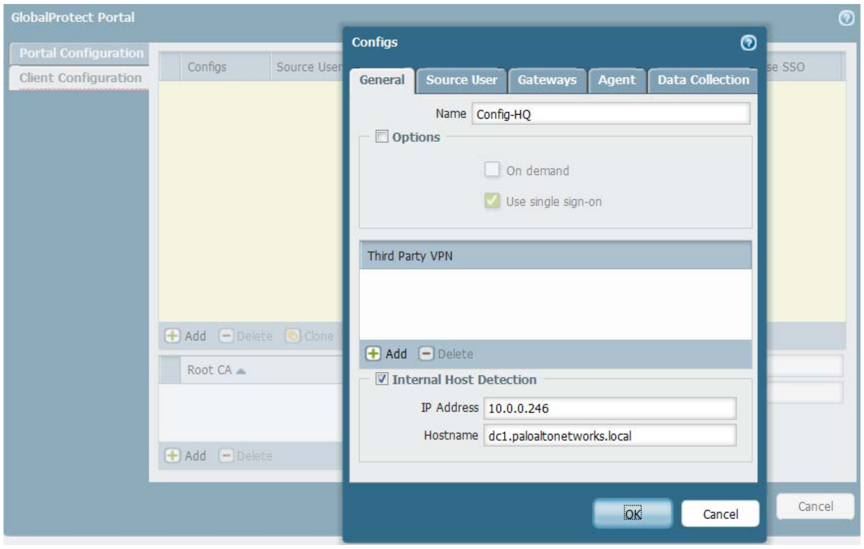
Name: Corp-Portal
Authentication Profile: Corp-LDAP-Profile
Client Certificate: GlobalProtect-Client
Server Certificate: GlobalProtect-GW
Client Certificate Profile: None
Custom Login Page: None
Custom Help Page: None

Portal Address

Interface: ethernet1/3
IP Address: 121.192.1.2/24

Client Configuration General Tab

This section defines the parameters that will determine the GlobalProtect client behavior. Click "Add" to create a new client configuration and give it a name.



Name: Config-HQ

□ Options

□ On demand

☑ Use single sign-on

☑ Internal Host Detection

IP Address: 10.0.0.246
Hostname: dc1.paloaltonetworks.local

Options

The client can be configured to connect On-demand or use Single-Sign-On to connect to the portal and the gateway.

On-demand Mode
With this setting GlobalProtect client will not automatically connect to the gateway. Instead the user will have to manually connect to the gateway by clicking to connect on the client icon.

Single-Sign-On
The client will use the windows credentials of the user to authenticate to the GlobalProtect portal. This method is completely transparent to the end users. Single-sign-on can be completely tied to AD authentication. Windows Vista and Windows 7 leverages Microsoft Credential Provider and Windows XP leverages GINA chaining and "secure attention sequence".

Third party VPN
This is used to exempt traffic from other third party VPN adapter from being sent to the GlobalProtect Gateway. If the host that has the GlobalProtect client running also has other remote access VPN software installed (Juniper Network Connect for example), you can use this option to exempt the traffic from the Juniper Network Connect adapter to be sent across the GlobalProtect tunnel. The following third party VPN adapters are supported:

- Palo Alto NetConnect
- Juniper Networks Network Connect virtual adapter
- Cisco Systems VPN adapter

If no virtual adapters are selected, all traffic from the host will be routed via the GlobalProtect Gateway.

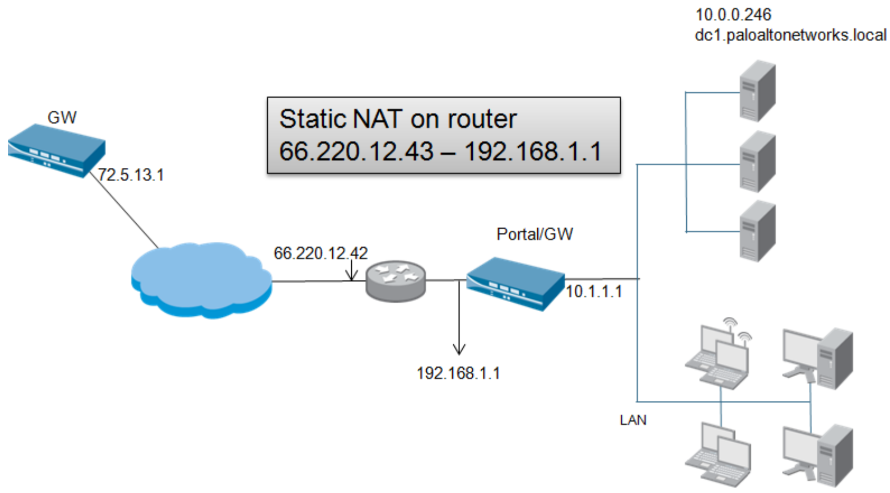
Internal Host Detection
This option is used to determine whether the host is inside or outside of the corporate network. Once this is determined, the client will connect to the corresponding Gateway.
If "Internal Host Detection" is enabled, the DNS name entered specifies a hostname that can only be reached from internal network and its IP address. The client performs a reverse lookup on the IP address and if it receives the expected hostname as a response, it will attempt to connect to the gateways in the internal gateway list. If no response is received, the client will attempt to connect to the external gateways in the external gateway list.
If the "internal-host-detection" feature is not configured, the GlobalProtect client will check for internal gateways first, if none are found, it will search for external gateways.
In this example, internal host detection is configured as follows- IP address 10.0.0.246 with host name dc1.paloaltonetworks.local. It is important to note that the IP address and host name should not be reachable on the public network.

Source User
The GlobalProtect portal allows for configuration based on users and user group. This allows different set of users or groups to have a dedicated set of gateways and client settings to be passed on. If there are multiple configurations, they are processed top down until a user or group is matched in order to apply the settings.

Gateways
This section is used to define the list of internal and external gateways that portal manages. A cut off time can be defined to limit the amount of time clients wait to get a response from the gateways.
External gateways can be assigned priorities. The priority is a numeric value between 1 and 5, with 1 being the highest priority and 5 the lowest. The client also considers the latency along with priority before connecting to a gateway.

Note: The GlobalProtect client may not always connect to the highest priority gateway if the latency is high compared to the other gateways.

The sample topology that follows is used to illustrate the configurations used to configure internal and external gateway.



IP address	Comment
66.220.12.43	Portal
66.220.12.43	External Gateway
72.5.13.1	External Gateway
10.1.1.1	Internal Gateway

Gateway selection algorithm

Case1

Let us assume the following Gateways with priorities as the response time as follows:

Gateway name	Priority	Response time
Gateway-1	1	80 ms
Gateway-2	2	25 ms
Gateway-3	3	50 ms

The average response time in this case is 51 milliseconds. In this case, the Client will connect to Gateway-2, because the response time is less than the average response time of the three Gateways. Gateway-1, even though has higher priority has a response time, higher than the average response time of 51 millisecond.

Case2

Let us assume the following Gateways with priorities as the response time as follows:

Gateway name	Priority	Response time
Gateway-1	1	30 ms
Gateway-2	2	25 ms
Gateway-3	3	50 ms

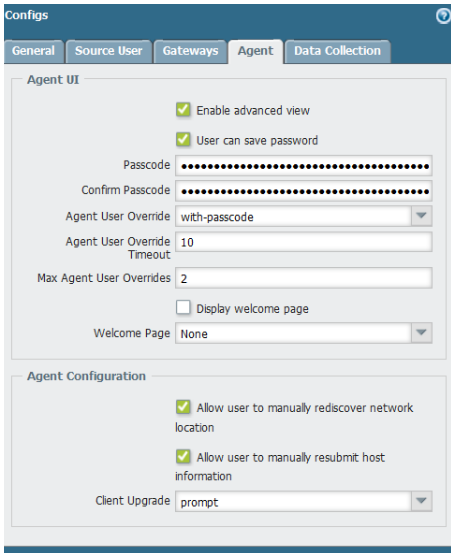
The average response time in this case is 35 milliseconds. Even though Gateway-2 has the lowest response time, the Client will connect to Gateway-1, because its response time is less than the average, and has the highest priority.

Note:

- The Client will connect to only one External Gateway.
- If there are multiple internal gateways, the client will send the host state report to all the internal gateways in the list. All traffic from the client will traverse the through gateway as determined by the network configuration.

Agent

This section defines the client's look and feel from the users point of view, and the ability to disable client.



Agent UI

☑ Enable advanced view

☑ User can save password

Passcode: ••

Confirm Passcode: ••

Agent User Override: with-passcode

Agent User Override Timeout: 10

Max Agent User Overrides: 2

□ Display welcome page

Welcome Page: None

Agent Configuration

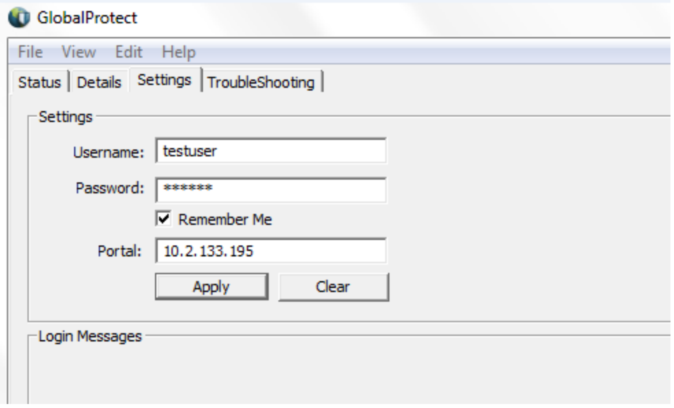
☑ Allow user to manually rediscover network location

☑ Allow user to manually resubmit host information

Client Upgrade: prompt

Enable advanced view

Allows the end users to select advanced view section of the agent which includes details, settings, and troubleshooting tabs.



Settings

Username: testuser

Password: ******

☑ Remember Me

Portal: 10.2.133.195

Tip: It is recommended to disable Advanced View for Clients, this will prevent users from changing settings and prevent users from viewing what HIP objects are being matched on the Gateway

Note: Refer to the section HIP objects and profiles for more information on HIP

User can save password:

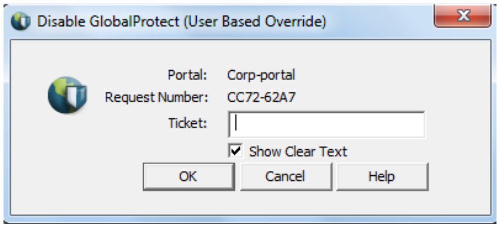
Allows the user to save password on the GlobalProtect client

Agent override with comment

Users will be prompted to enter a comment when the disable

Agent override with password
Users will be prompted to enter a password to disable the Client. All users use the same password to disable the Client.

Agent override with ticket
This option enables a challenge-response mechanism to authorize disabling GlobalProtect on the client side. When this option is selected, the user is prompted with a challenge when disabling GlobalProtect. The challenge is then communicated to the firewall administrator out-of-band, and the administrator can validate the challenge through the firewall management interface. The firewall produces a response that is read back to the user who can then disable GlobalProtect by entering the response in GlobalProtect.
When a user tries to disable the client, the client generates a request number and prompts for ticket as shown in the following screen shot:

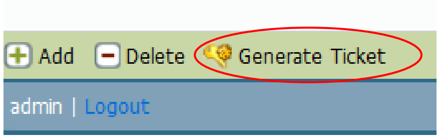

Disable GlobalProtect (User Based Override)

Portal: Corp-portal
Request Number: CC72-62A7
Ticket:
☑ Show Clear Text

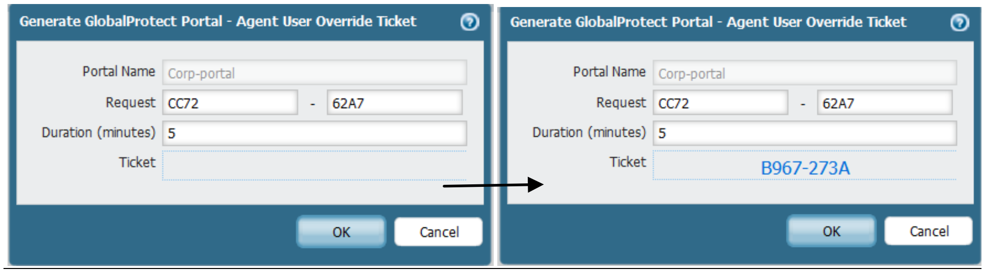
The user will then give the request number to the firewall administrator offline in order to get a ticket that can be used to disable the Client.

The process for generating the ticket is listed below.

- From the Portal configuration screen (*Network* > *GlobalProtect Portal*), click on Generate ticket.



- Enter the request number provided by user. The request number is case sensitive.
- Specify the duration the ticket is valid and click on OK. The maximum value is 65535.
- This generates ticket. This ticket is then communicated to the user to disable the client


Generate GlobalProtect Portal - Agent User Override Ticket

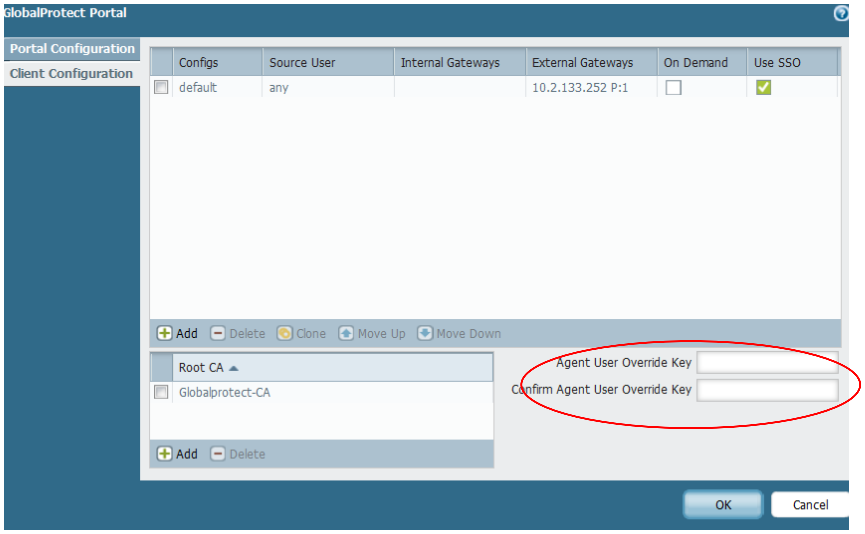
Portal Name: Corp-portal
Request: CC72 - 62A7
Duration (minutes): 5
Ticket:

Generate GlobalProtect Portal - Agent User Override Ticket

Portal Name: Corp-portal
Request: CC72 - 62A7
Duration (minutes): 5
Ticket: B967-273A

Note: It is not required to commit the configuration after generating the ticket

Agent user override key (optional)
To secure the client user override ticket, you can specify a "Agent user override key" under the client configuration section of the portal. This key is used to validate the client when user tries to disable using ticket.



	Configs	Source User	Internal Gateways	External Gateways	On Demand	Use SSO
□	default	any		10.2.133.252 P:1	□	☑

	Root CA ▲
□	Globalprotect-CA

Agent User Override Key

Confirm Agent User Override Key

Agent User Override Timeout

This is the amount of time; the client can remain disconnected before connecting to a gateway. A value of '0" means, agent can remain disconnected for infinite amount of time. The maximum value is 65535 minutes.

Max Agent User Overrides

Specify the maximum number of times a user can disable the client before a successful connection to a firewall is required.

Client Upgrade

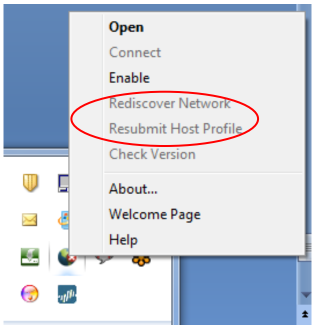
This setting defines the client upgrade behavior. The two options available are prompt, and transparent.
Prompt: The end users will be prompted for upgrade when new version of client is available.
Transparent: This setting will automatically download the newer version of Client when available without prompting the user for upgrade.

Allow user to manually rediscover network location

Select this check box to allow the user to manually trigger network rediscovery on the client.

Allow user to manually resubmit host information

Select this check box to allow the user to manually trigger resubmission of the latest HIP client.



Root CA

Specify the Root CA that the GlobalProtect Client will trust when connecting to a Gateway. If a gateway presents a certificate to the client that hasn't been issued by one of the listed CAs, the client will reject the handshake and terminate the connection.

Host Information Objects and Profiles

HIP objects

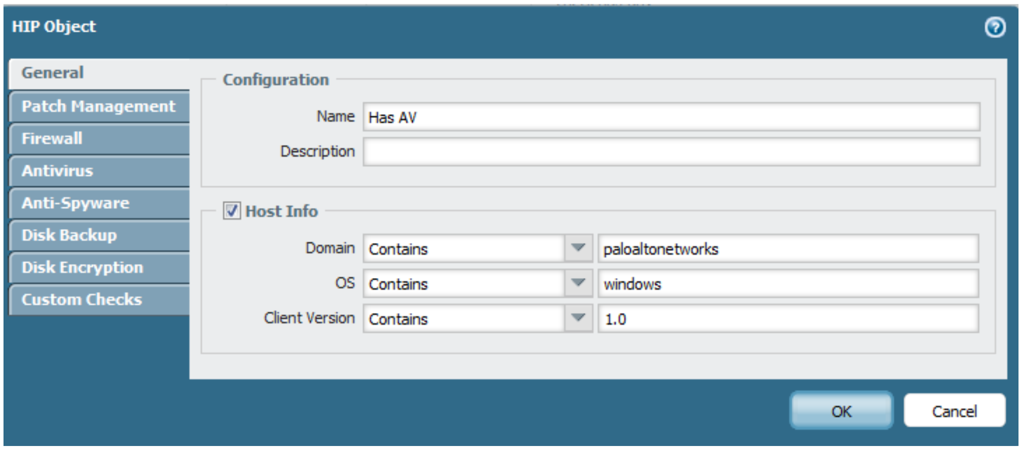
The GlobalProtect client gathers information about the end host, which is then reported back to the gateway. This is referred to as HIP Objects. HIP object definition, is used to match on the categories sent by the GlobalProtect client to the gateway. The GlobalProtect gateway then uses the information received from the client to generate HIP report about the host.
The Client can be configured to check the end host for the following predefined categories:

- Host Info
  - Match on the version of Windows that is running on the end host, GlobalProtect Client version and the domain of the host.
- Anti-virus
  - Check for AV vendor, product version, real time protection, and last scan time.
- Anti-spyware
  - Check for AV vendor, product version, real time protection, and last scan time.
- Disk backup
  - Check for disk backup software, time since last backup.
- Disk encryption
  - Checks for data encryption software and the location of the data on the end host provide as the directory path. It allows to check if the data is fully or partially encrypted.
- Firewall
  - Check for firewall vendor, product version and if the firewall is on or off.
- Patch management
  - Checks for missing patches, list of vendors.
- Custom Checks
  - Check for certain processes and registry keys on the end host.

HIP object definition, is used to match on the categories sent by the GlobalProtect Client to the Gateway. The GlobalProtect Gateway then uses the information received from the Client to generate HIP report about the host.

The following example shows the HIP objects to check for antivirus and host information:

Object > GlobalProtect > HIP object > Add



Configuration

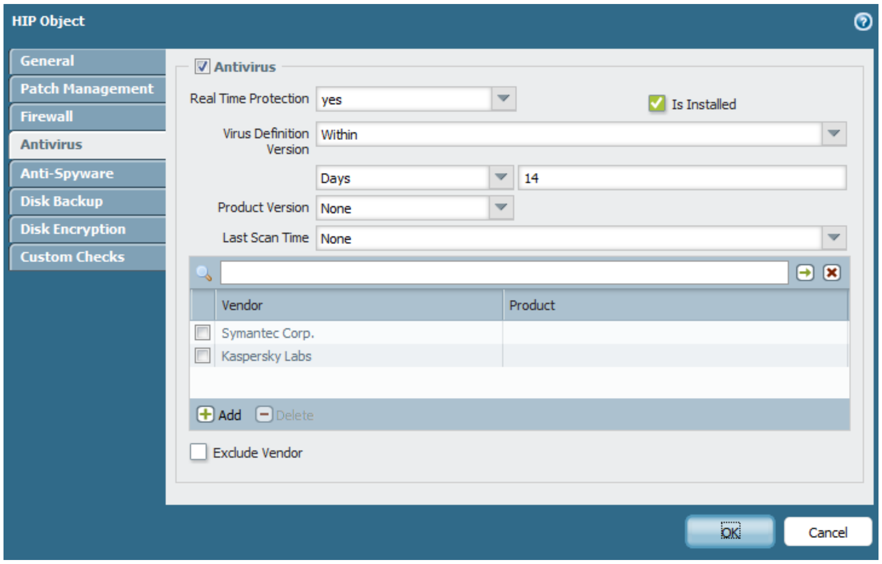
Name: Has AV

Description:

☑ Host Info

Domain	Contains	paloaltonetworks
OS	Contains	windows
Client Version	Contains	1.0

The host info section in the General tab provides for matching information on the end host such as the domain name, the operating system version and the GlobalProtect client version.



☑ Antivirus

Real Time Protection: yes

☑ Is Installed

Virus Definition Version: Within

Days: 14

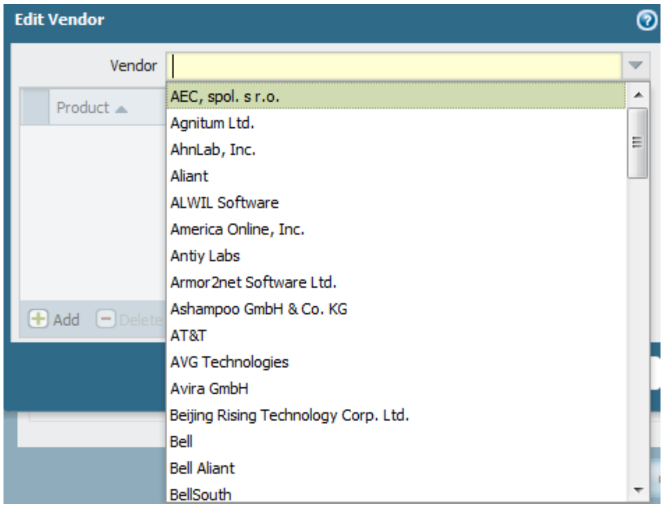
Product Version: None

Last Scan Time: None

	Vendor	Product
□	Symantec Corp.	
□	Kaspersky Labs	

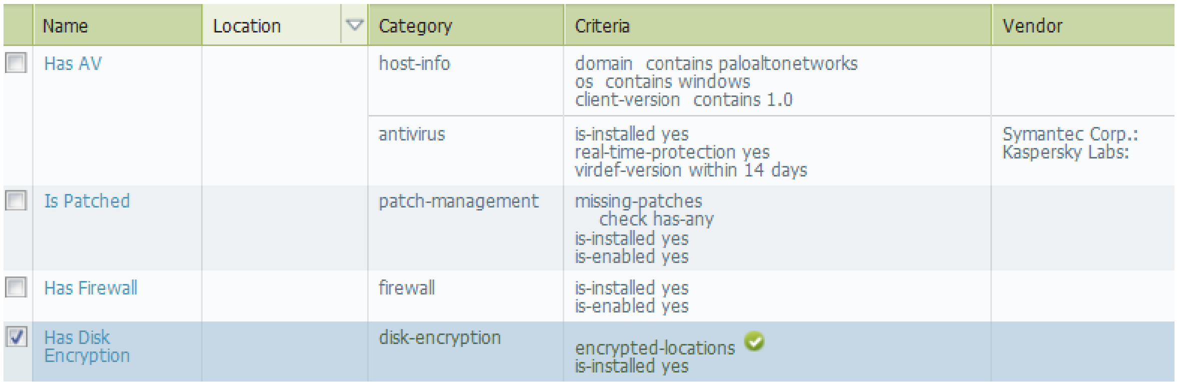
□ Exclude Vendor

Click on add to list the available vendors. If you know the name of the vendor you can also type the first few characters of name in the vendor list to auto complete.



You can also view all the defined HIP objects by navigating to **Objects > GlobalProtect > HIP object**. An example of the configured HIP objects is shown below. The location column displays the name of the VSYS where the object is defined

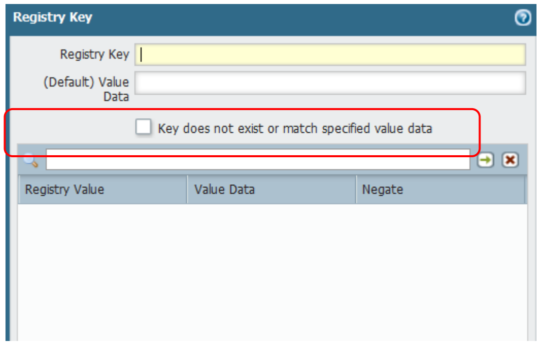
Object > GlobalProtect > HIP object



	Name	Location	Category	Criteria	Vendor
☐	Has AV		host-info	domain contains paloaltonetworks os contains windows client-version contains 1.0	
			antivirus	is-installed yes real-time-protection yes virdef-version within 14 days	Symantec Corp.: Kaspersky Labs:
☐	Is Patched		patch-management	missing-patches check has-any is-installed yes is-enabled yes	
☐	Has Firewall		firewall	is-installed yes is-enabled yes	
☑	Has Disk Encryption		disk-encryption	encrypted-locations ✓ is-installed yes	

HIP objects checking registry keys

You can also configure HIP objects to match on specific registry keys. For example, to check if a given machine is a member of a company domain you can match the registry key HKEY_Local_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain



Registry Key

Registry Key:

(Default) Value Data:

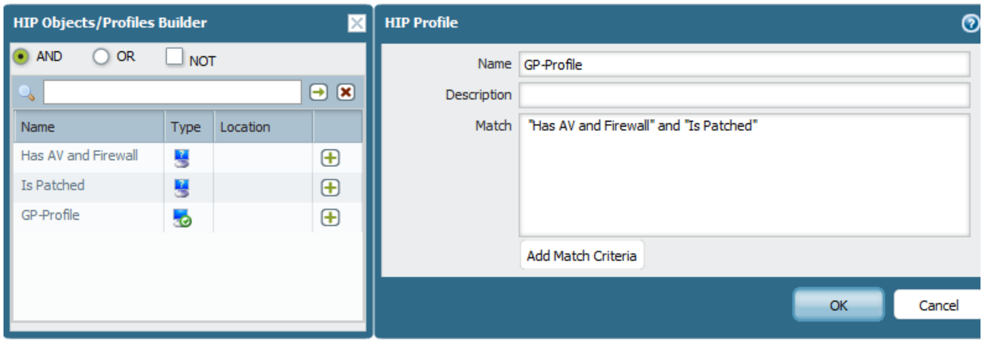
☐ Key does not exist or match specified value data

Registry Value	Value Data	Negate

The option "key does not exist or match specified value data" is negating the value i.e. not match the specified registry entry value.

HIP profiles

A HIP Profiles defines an evaluation of a set of collected HIP objects with combined logic such that when evaluated, the result will either be true or false. HIP profile is referred to as a match condition in the security policy configured on the gateway. To configure a HIP profile navigate to *Object* > *GlobalProtect* > *HIP profile*.



HIP Objects/Profiles Builder

● AND ○ OR ☐ NOT

Name	Type	Location
Has AV and Firewall		
Is Patched		
GP-Profile		

HIP Profile

Name: GP-Profile

Description:

Match: "Has AV and Firewall" and "Is Patched"

Configure HIP profile a name, Click on **Add match criteria** to add the HIP objects to the profile. The list of the available HIP objects will be displayed in a new pop-up window. The HIP profile can be configured to use the Boolean AND/OR/NOT operation to match all or any one of the HIP objects. Choose the operator

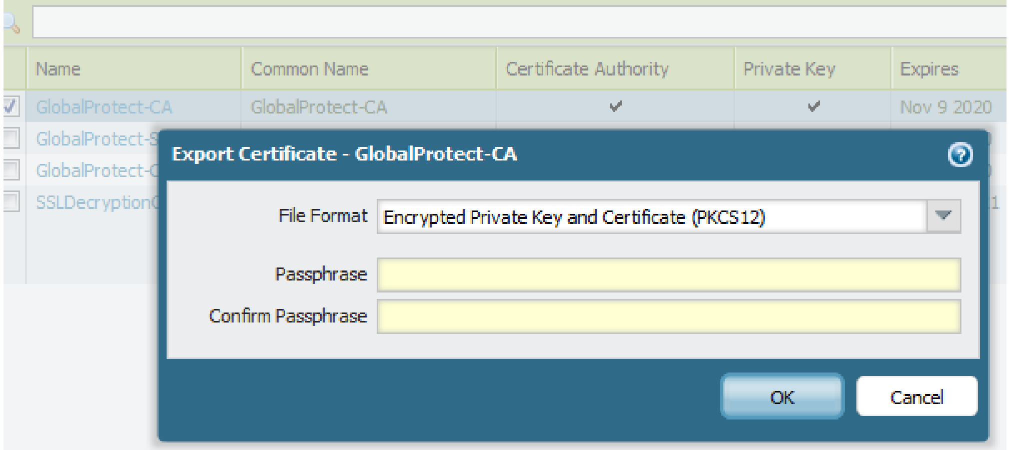
from the top of the HIP objects screen and click on the "+" sign next to the object to add the object to the HIP profile. The HIP profiles are used in the security policy as a match condition to either allow or deny traffic.
Table below shows sample security policies and HIP profiles used in conjunction to allow or deny traffic.

Source Zone	Dst Zone	Src IP	Dst IP	HIP profile	Action
Accounting	DMZ	Account-net	Account-Servers	Disk Encryption	Allow
Accounting	DMZ	Account-net	Account-Servers	No-HIP	deny
Any	Internet	Any	Any	Has AV and Has FW	Allow

First rule requires disk encryption enabled to access accounting servers. The follow up rule, denies access to accounting server is the host does not have Disk Encryption. The third rule requires both host anti-virus and firewall to be enabled for the users to access the internet.

Configuring multiple GlobalProtect Gateways

When deploying multiple Gateways, each one of the Gateway must have its own Gateway certificate signed by the same certificate authority. This requires that the certificate of the CA server and the key be imported to each one of the Gateway and use this certificate to sign the Gateway and the client certificates. For the ease deployment, you can use the same Gateway and client certificate across multiple Gateways. This is accomplished by first exporting the certificates from one device and later importing these certificates to all other Gateways. In the example we export the following certificates- CA server cert, GlobalProtect Gateway cert and Client cert. From ***Device>Certificate*** select the CA server certificate and click on export. Enter passphrase, save it to local computer. Repeat the same steps for Gateway and client certificates



	Name	Common Name	Certificate Authority	Private Key	Expires
☑	GlobalProtect-CA	GlobalProtect-CA	✓	✓	Nov 9 2020
□	GlobalProtect-S				
□	GlobalProtect-C				
□	SSLDecryption				

Export Certificate - GlobalProtect-CA

File Format: Encrypted Private Key and Certificate (PKCS12)

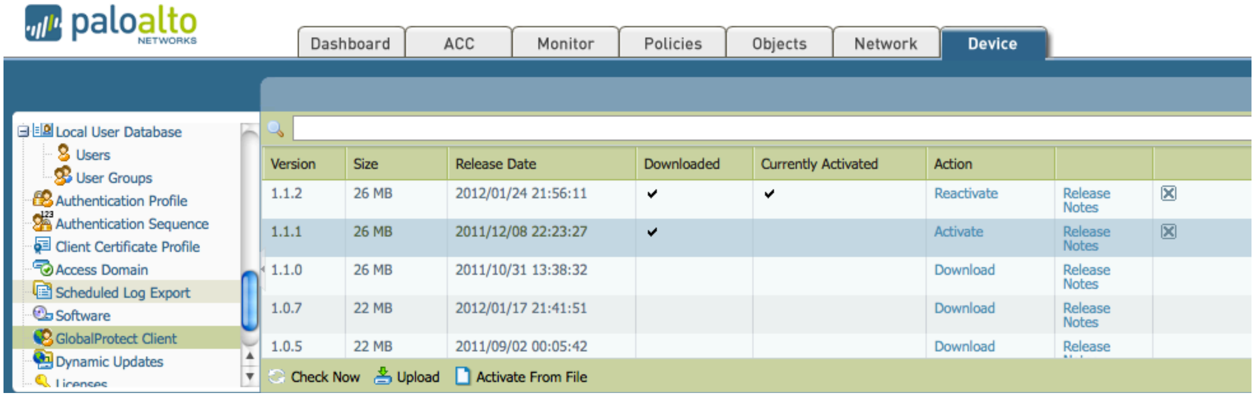
Passphrase:

Confirm Passphrase:

After login into the second firewall that will be used as the gateway, select **Device > Certificate** click on **Import** to import all the three certificates. Follow the steps in the Configuring Gateway to complete the configuration.

Download and Activate the GlobalProtect Client on the Firewall

There are several versions of the GlobalProtect Clients available, so the firewall must know which version to use. To select the GlobalProtect version, go to **Device > GlobalProtect Client** click **Check Now** (bottom left) to get the latest list of GlobalProtect Clients. Click **Download** on the version of client you wish to use. After the download has completed, click **Activate**.



Version	Size	Release Date	Downloaded	Currently Activated	Action		
1.1.2	26 MB	2012/01/24 21:56:11	✓	✓	Reactivate	Release Notes	☒
1.1.1	26 MB	2011/12/08 22:23:27	✓		Activate	Release Notes	☒
1.1.0	26 MB	2011/10/31 13:38:32			Download	Release Notes	
1.0.7	22 MB	2012/01/17 21:41:51			Download	Release Notes	
1.0.5	22 MB	2011/09/02 00:05:42			Download	Release	

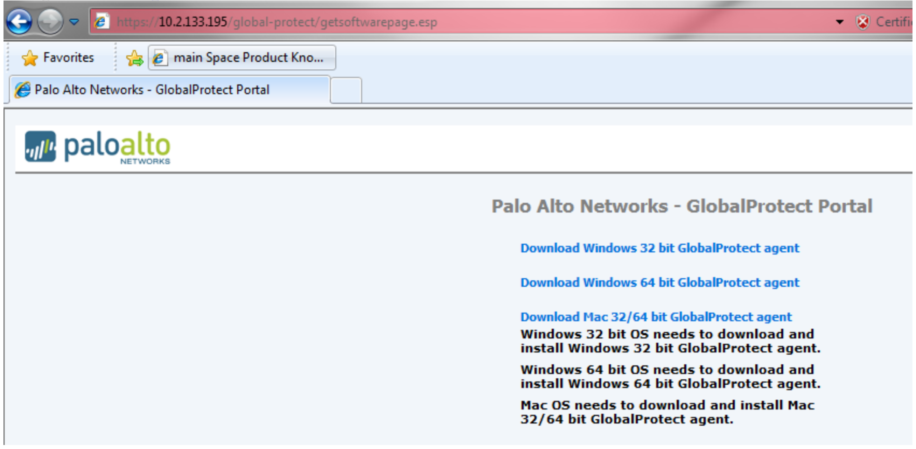
Note:

1. If you fail to complete this step, any attempt to download the client from the firewall will result in a download of errors.txt. In this case, errors.txt indicates there is no file found on the firewall.
2. In a HA cluster you should enable the same version of client on both cluster members.

Distributing GlobalProtect Client

In Active Directory environments, GlobalProtect Client can also be distributed to end users, using active directory group policy. AD Group policies allows administrators to modify Windows host computer settings and software automatically. Refer to the article at http://support.microsoft.com/kb/816102 for more information on how to use Group Policy to automatically distribute programs to Host computers or users.

The GlobalProtect agent msi file can be downloaded directly from the portal by browsing to the address of the portal https://<hostname or IP address>


https://10.2.133.195/global-protect/getsoftwarepage.esp
Certifi
Favorites
main Space Product Kno...
Palo Alto Networks - GlobalProtect Portal
paloalto NETWORKS

Palo Alto Networks - GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.

Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.

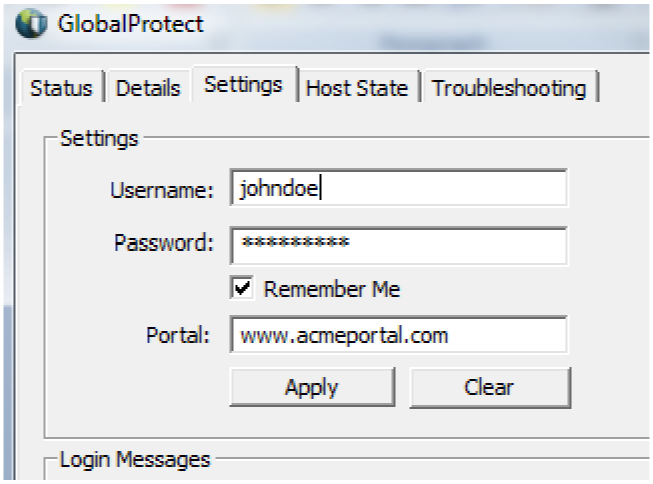
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

Note: Administrator privilege is required for installing the GlobalProtect client for the first time. Subsequent upgrades do not require administrator privileges.

Establishing connection

Connection to the GlobalProtect system can be accomplished in two ways.

After installing the Client, it must be configured to connect to the GlobalProtect Portal. Provide the IP address/FQDN of the Portal and user credentials to connect to the portal.



Settings

Username: johndoe

Password: **********

☑ Remember Me

Portal: www.acmeportal.com

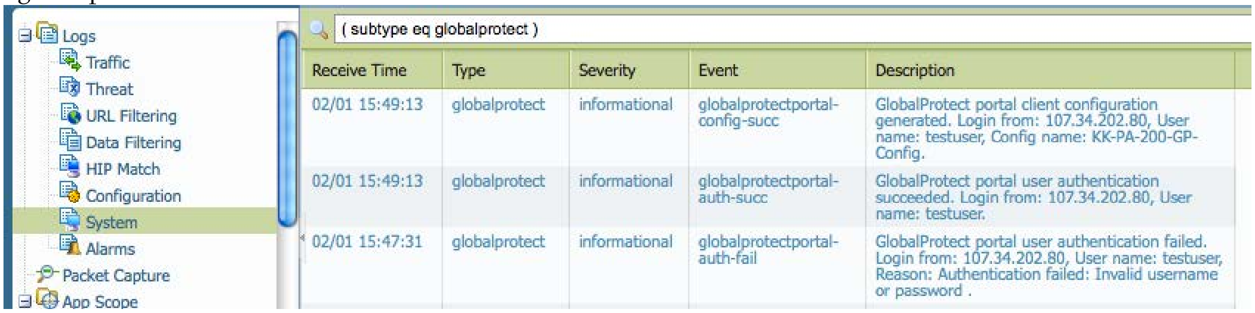
The sequence of the steps for the Client to connect to the Gateway is as follows:

- The client contacts the portal and retrieves the list of gateways among other configuration.
- The client then checks whether it is on the internal network or external network by performing the reverse DNS lookup.
- If the client determines it is on external network, it contacts all gateways in the list and establishes a SSL handshake to measure the response time of each gateway
- Client establishes then connection to gateway with fastest response or highest priority and submits HIP report

GlobalProtect will first check for the "LastUrl" entry under HKEY_CURRENT_USER\Software\Palo Alto Networks\GlobalProtect\Settings. If that is not present or empty, it will additionally check for the presence of a "Portal" entry under HKEY_LOCAL_MACHINE\Software\Palo Alto Networks\GlobalProtect\PanSetup. For mass deployments, you can also deploy a registry key "Portal" under HKEY_LOCAL_MACHINE\Software\Palo Alto Networks\GlobalProtect\PanSetup with the portal hostname in it. In that case, a newly installed client will always connect to the portal configured in this entry. It is important to know for mass deployments is also that GlobalProtect client will always try to use SSO credentials on its first connection when no username or password has been defined yet. By combining the SSO feature together with deploying the "Portal" registry entry, you can accomplish seamless user experience. In this case, GlobalProtect client will connect to the pre-defined portal with the SSO credentials captured from the system.

Logging and reporting

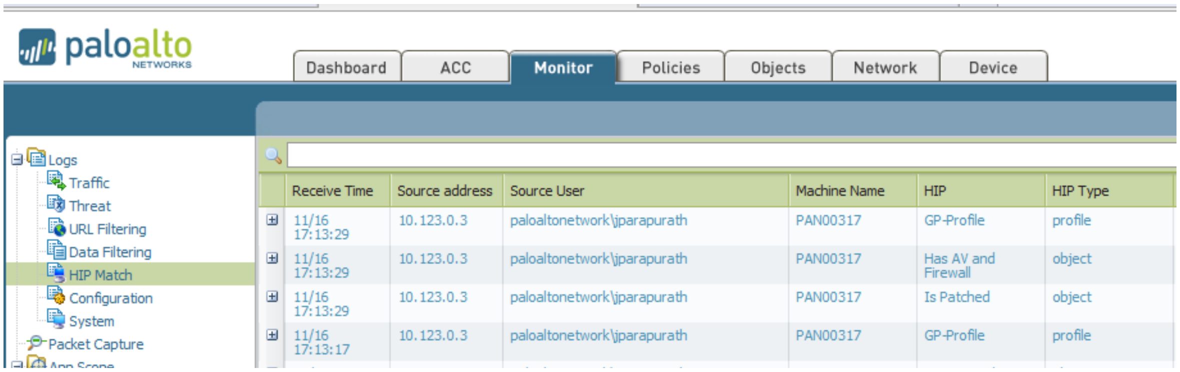
Logging of the GlobalProtect Client connection, user login and login failure error messages are available at **Monitor > System**. System logs provide information about user activity. Filter on the subtype “globalprotect”.



(subtype eq globalprotect)

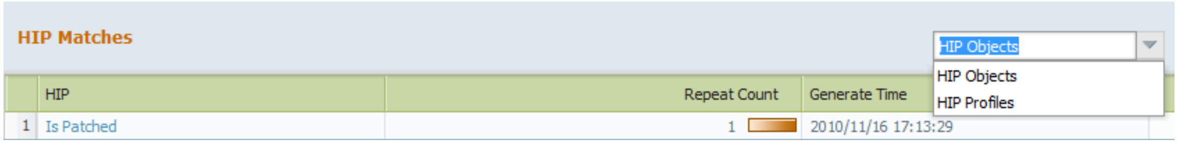
Receive Time	Type	Severity	Event	Description
02/01 15:49:13	globalprotect	informational	globalprotectportal-config-succ	GlobalProtect portal client configuration generated. Login from: 107.34.202.80, User name: testuser, Config name: KK-PA-200-GP-Config.
02/01 15:49:13	globalprotect	informational	globalprotectportal-auth-succ	GlobalProtect portal user authentication succeeded. Login from: 107.34.202.80, User name: testuser.
02/01 15:47:31	globalprotect	informational	globalprotectportal-auth-fail	GlobalProtect portal user authentication failed. Login from: 107.34.202.80, User name: testuser, Reason: Authentication failed: Invalid username or password .

Additionally, the GlobalProtect Client sends HIP logs to the Gateway that it connects to. The logs can be viewed under the HIP match section of the Monitor tab.



Receive Time	Source address	Source User	Machine Name	HIP	HIP Type
11/16 17:13:29	10.123.0.3	paloaltonetwork\jparapurath	PAN00317	GP-Profile	profile
11/16 17:13:29	10.123.0.3	paloaltonetwork\jparapurath	PAN00317	Has AV and Firewall	object
11/16 17:13:29	10.123.0.3	paloaltonetwork\jparapurath	PAN00317	Is Patched	object
11/16 17:13:17	10.123.0.3	paloaltonetwork\jparapurath	PAN00317	GP-Profile	profile

ACC provides reports for HIP objects and profiles

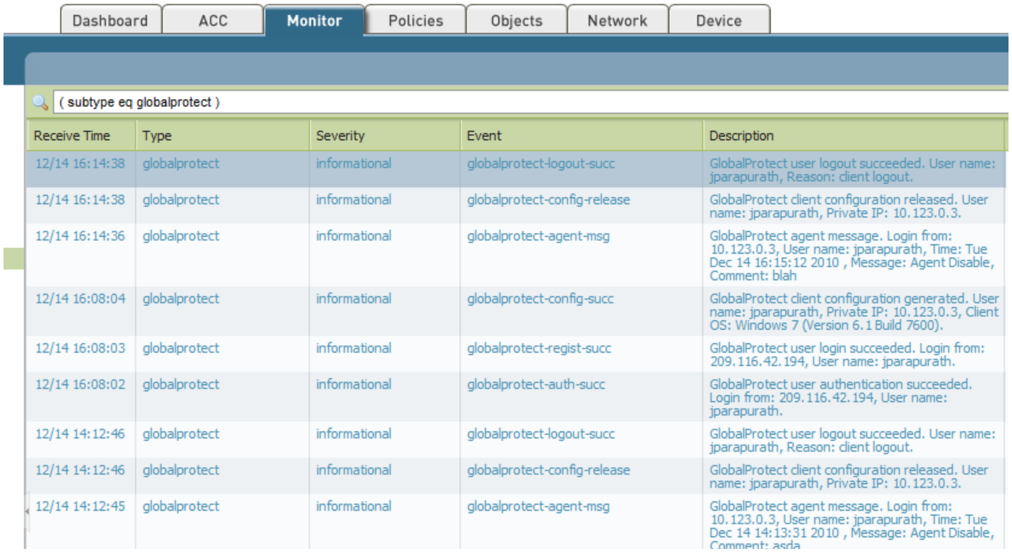


HIP Matches

HIP Objects

	HIP	Repeat Count	Generate Time
1	Is Patched	1	2010/11/16 17:13:29

System logs provide information about user activity. Filter on the subtype “globalprotect”.



(subtype eq globalprotect)

Receive Time	Type	Severity	Event	Description
12/14 16:14:38	globalprotect	informational	globalprotect-logout-succ	GlobalProtect user logout succeeded. User name: jparapurath, Reason: client logout.
12/14 16:14:38	globalprotect	informational	globalprotect-config-release	GlobalProtect client configuration released. User name: jparapurath, Private IP: 10.123.0.3.
12/14 16:14:36	globalprotect	informational	globalprotect-agent-msg	GlobalProtect agent message. Login from: 10.123.0.3, User name: jparapurath, Time: Tue Dec 14 16:15:12 2010 , Message: Agent Disable, Comment: blah
12/14 16:08:04	globalprotect	informational	globalprotect-config-succ	GlobalProtect client configuration generated. User name: jparapurath, Private IP: 10.123.0.3, Client OS: Windows 7 (Version 6.1 Build 7600).
12/14 16:08:03	globalprotect	informational	globalprotect-regist-succ	GlobalProtect user login succeeded. Login from: 209.116.42.194, User name: jparapurath.
12/14 16:08:02	globalprotect	informational	globalprotect-auth-succ	GlobalProtect user authentication succeeded. Login from: 209.116.42.194, User name: jparapurath.
12/14 14:12:46	globalprotect	informational	globalprotect-logout-succ	GlobalProtect user logout succeeded. User name: jparapurath, Reason: client logout.
12/14 14:12:46	globalprotect	informational	globalprotect-config-release	GlobalProtect client configuration released. User name: jparapurath, Private IP: 10.123.0.3.
12/14 14:12:45	globalprotect	informational	globalprotect-agent-msg	GlobalProtect agent message. Login from: 10.123.0.3, User name: jparapurath, Time: Tue Dec 14 14:13:31 2010 , Message: Agent Disable, Comment: asda

High Availability

Redundancy of the portal and gateway require the firewall deployed in the HA cluster. Separate licenses are required for each the devices in the cluster. When using Active-active cluster, the floating IP address must be used as the gateway and the portal IP address. The HIP reports are synchronized between devices in HA.

- When no HA is deployed, If a portal fails, the existing users will still be able to connect to gateway using cached configuration. All connection attempts from first time users connecting to GlobalProtect will fail, since they need to authenticate to the portal first.
- If a Gateway fails, GlobalProtect client will try and establish connection to other available gateway.

Scaling

The maximum number of simultaneous users that can connect to GlobalProtect system is dependent on the VPN capacity, i.e. SSL or IPSec connections of the firewall. For large scale deployments, it is recommended to have a firewall dedicated to function as portal. As previously mentioned the portal is only used to provide the first time authentication to GlobalProtect users and push the configuration changes. The gateway is the device that provides secure connection to the protected resources. The clients establish a tunnel to the gateway.

Troubleshooting

View the active Gateway flow from the CLI:

```
admin@LAB> show global-protect-gateway flow

total tunnels configured:                               1
filter - type GlobalProtect-Gateway, state any

total GlobalProtect-Gateway tunnel shown:               1

id    name                 local-i/f         local-ip        tunnel-i/f
-------------------------------------------------------------------------------------------
2     Corp-NetConnect      ethernet1/1       10.2.133.195    tunnel.1
```

```
admin@LAB> show global-protect-gateway flow tunnel-id 2

tunnel  Corp-NetConnect
        id:                 2
        type:               GlobalProtect-Gateway
        local ip:           10.2.133.195
        inner interface:    tunnel.1         outer interface:  ethernet1/1
        ssl cert:           Netconnect
        active users:       1

assigned-ip      remote-ip       encapsulation
-----------------------------------------------------------------------------------------------
172.16.0.1       10.20.0.240     IPSec SPI 448772F2 (context 3)
```

View the Gateway configuration from the CLI:

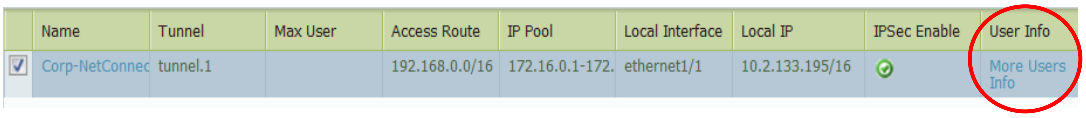
```
admin@LAB> show global-protect-gateway gateway name Corp-NetConnect

        GlobalProtect Name   : Corp-NetConnect
        Tunnel ID            : 2
        tunnel-interface     : tunnel.1
        encap-interface      : ethernet1/1
        inheritance-from     :
        Local Address        : 10.2.133.195
        SSL server port      : 443
        IPSec encap          : yes
        tunnel negotiation   : ssl
        HTTP redirect        : no
        UDP port             : 4501
        Max users            : 0
        IP pool ranges       : 172.16.0.1 - 172.16.1.254;
        DNS servers          : 4.2.2.2
                             : 0.0.0.0
        WINS servers         : 0.0.0.0
                             : 0.0.0.0
        DNS suffix           : mycompany.com
        Access routes        : 192.168.0.0/16;
        VSYS                 : vsys1 (id 1)
        SSL Server Cert      : Netconnect
        Auth Profile         : RADIUS
        Client Cert Profile  :
        Lifetime             : 259200 seconds
        Idle timeout         : 10800 seconds
```

To view the users connected:

```
show global-protect-gateway current-user
show user ip-user-mapping type GP
```

or from the Web interface navigate to: ***Network>GlobalProtect>Gateway*** *and click “****More Users Info****”:*



	Name	Tunnel	Max User	Access Route	IP Pool	Local Interface	Local IP	IPSec Enable	User Info
☑	Corp-NetConnec	tunnel.1		192.168.0.0/16	172.16.0.1-172.	ethernet1/1	10.2.133.195/16	✓	More Users Info

To view the tunnels established:

```
      show global-protect-Gateway flow
      show global-protect-Gateway flow tunnel-id <value>
      debug global-protect Portal interval n
```

Where n is the number of seconds for the interval in which the Client creates the HIP report. It can be between 60-86400 seconds, meaning one minute to 24 hours

To troubleshoot HIP related issues

```
debug user-id on debug
debug user-id set hip all
```

Logs will be in useridd.log in mp-log. This can be viewed by the command **"tail mp-log useridd.log"**

Show the current state of the HIP cache in management plane

```
debug user-id dump hip-profile-database

debug user-id dump hip-report <computer/ip/user>
```

GP Client logs

In the event the Client crashed, Client logs can be collected from Start ->All Programs ->Palo Alto networks ->GlobalProtect -> PanGPsupport

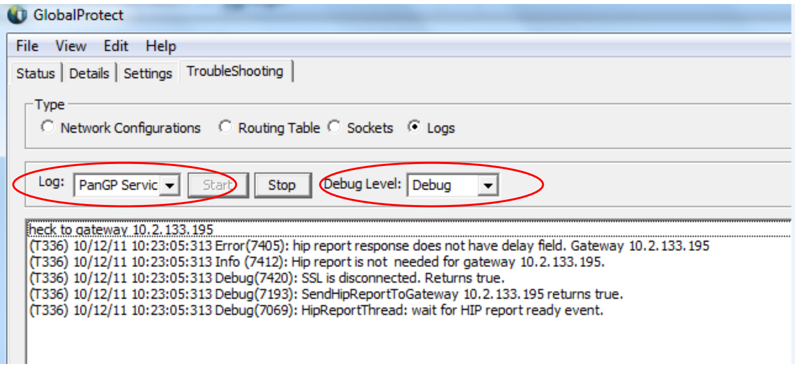
Firewall

- Authentication failures
  - o Verify the users can authenticate by browsing to the IP address of the portal and authenticating to it
  - o View the authentication logs on the firewall in real time using the following command- **tail follow yes mp-log authd.log**
- GlobalProtect specific logs can be viewed on the firewall System logs by filtering on (subtype eq globalprotect)

Agent

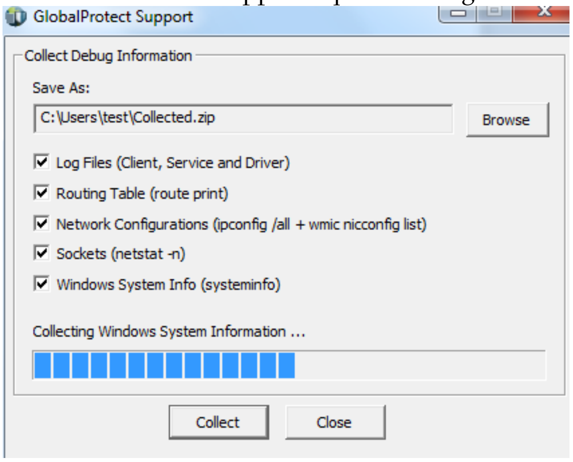
If the agent fails to connect, you can view the debug logs on the agent as shown below. The advanced view on the agent must be enabled to view the troubleshooting tab of the agent.

Set the log to PanGPService and Debug level to debug. You can see authentication failed messages and connectivity failure messages


GlobalProtect
File View Edit Help
Status | Details | Settings | TroubleShooting
Type
○ Network Configurations ○ Routing Table ○ Sockets ● Logs
Log: PanGP Servic
Start
Stop
Debug Level: Debug

```
heck to gateway 10.2.133.195
(T336) 10/12/11 10:23:05:313 Error(7405): hip report response does not have delay field. Gateway 10.2.133.195
(T336) 10/12/11 10:23:05:313 Info (7412): Hip report is not  needed for gateway 10.2.133.195.
(T336) 10/12/11 10:23:05:313 Debug(7420): SSL is disconnected. Returns true.
(T336) 10/12/11 10:23:05:313 Debug(7193): SendHipReportToGateway 10.2.133.195 returns true.
(T336) 10/12/11 10:23:05:313 Debug(7069): HipReportThread: wait for HIP report ready event.
```

To collect the tech support equivalent logs from the agent, select File>Collect Log and click on collect logs



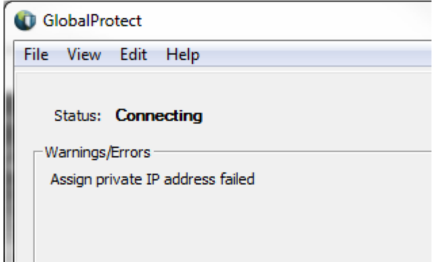
Save As: C:\Users\test\Collected.zip

☑ Log Files (Client, Service and Driver)
☑ Routing Table (route print)
☑ Network Configurations (ipconfig /all + wmic nicconfig list)
☑ Sockets (netstat -n)
☑ Windows System Info (systeminfo)

Collecting Windows System Information ...

Address allocation failure

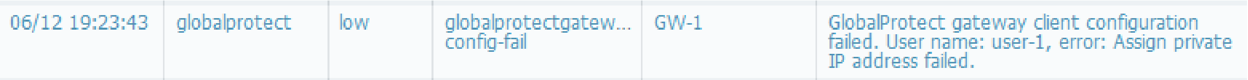
If the client physical adapter IP address overlaps with IP pool created on the gateway, the client will not be assigned an IP address. The screen shot below show the error message on the client and the corresponding log from firewall.



Status: **Connecting**

Warnings/Errors

Assign private IP address failed



06/12 19:23:43	globalprotect	low	globalprotectgatew... config-fail	GW-1	GlobalProtect gateway client configuration failed. User name: user-1, error: Assign private IP address failed.

This issue can be resolved by configuring a second IP pool that does not overlap with the client subnet

Revision History

Date	Revision	Comment
5/21/2012	E	A new item was added in the troubleshooting section "Troubleshooting Client IP Address Allocations Errors ". Updated information on the "Internal host detection" option. If this is off, GlobalProtect clients will search for internal gateways and if none are found, will search for external gateways. Minor document formatting updates.
05/09/2012	D	The following was added in the tips section on page 5. In order to identify user IP address with internal gateways, the GlobalProtect client must not be configured to use to on demand mode. This is defined under *GP Portal configuration* > *options*.
02/29/2012	C	Updated to include GlobalProtect usage as NetConnect.
02/28/2012	B	Updated sections on HA and gateways.
02/04/2012	A	First published draft with 4.1.