Configuring GlobalProtect

Tech Note

PAN-OS 4.1

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.

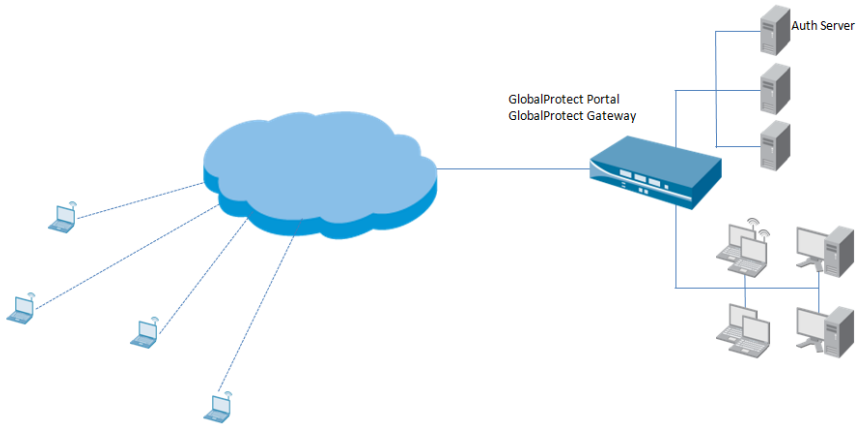
GlobalProtect elements

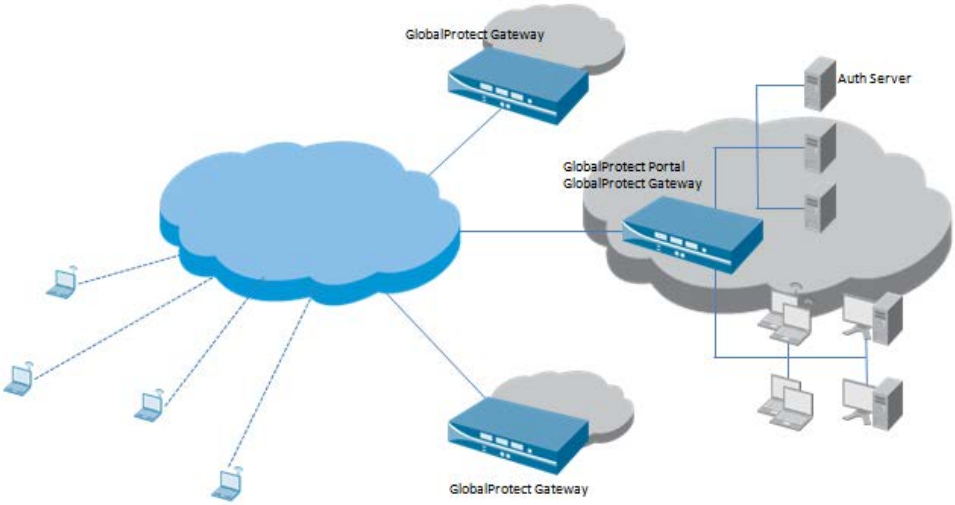
There are three essential components that make up the GlobalProtect solution:

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

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 is used. This allows the Client to connect to the closest Gateway. Some of the common deployment topologies are shown below.





Sequence of steps

This section covers the sequence of steps when an end host connects to the GlobalProtect system

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 to the Client. 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 security policy based on user, application, content and the HIP submitted from the Client.

Configuration check list

The following list of items is required for configuring GlobalProtect

- IP address of the Authentication server and type of authentication method
- IP address for Portal and Gateway

Access to CA server to generate certificate.
Note: This step is not required if you are using the Palo Alto Networks next-generation firewall as the CA server
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

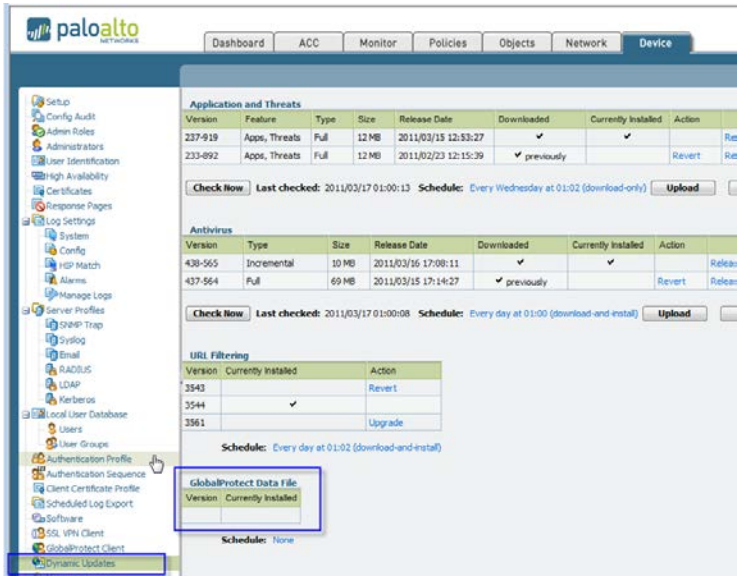
Note: For external deployments, if the Portal and Gateway are using private address, these IP addresses must be mapped to a public IP address

Software requirements

- PAN-OS version 4.0 or later
- 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
- Latest Application and Threats, Antivirus is required and 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



Hardware requirements

The PA-200, PA-500, PA-2000 series, PA-4000 Series and PA-5000 series of firewalls support GlobalProtect

Configuration steps

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

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, so that the Gateways can verify the end hosts are legitimate

The following certificates are required

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

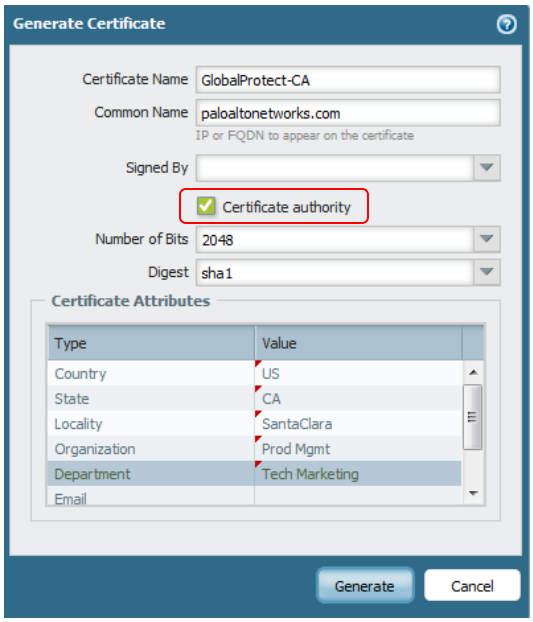
With PAN-OS release 4.0, the PaloAlto Networks next-generation firewall itself can act the CA server. In this example the firewall is configured as CA server and this certificate to sign Gateway and Client certificates.

Note: Certificate names must not spaces between words

Generating CA certificate

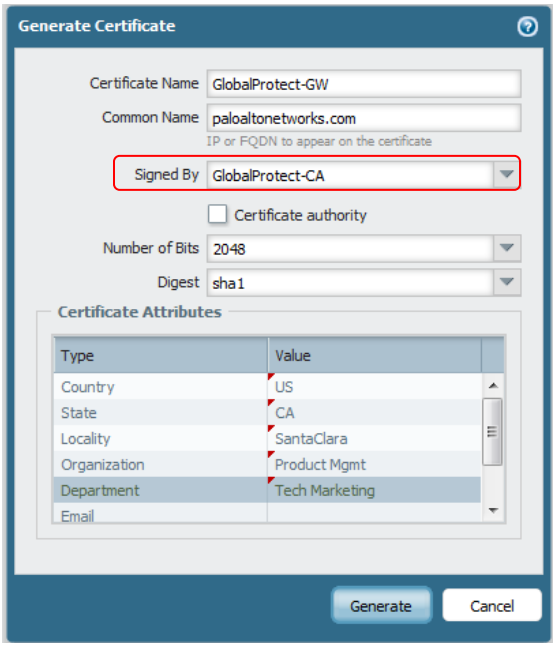
Navigate to Device>certificate>generate

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



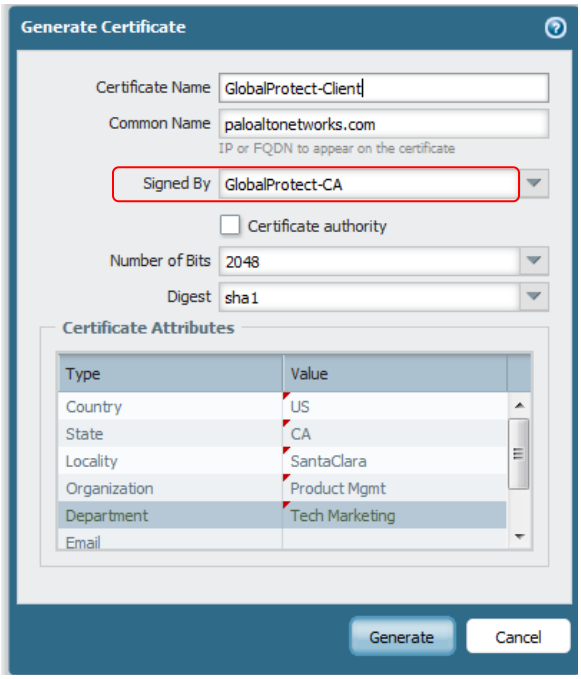
Generating a Gateway certificate

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.



Generating a Client certificate

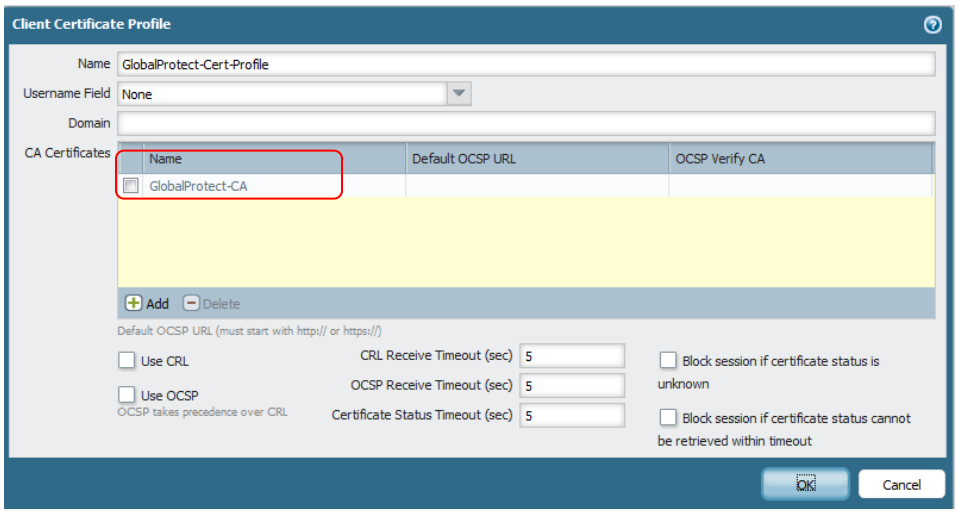
This Client certificate is used by the GlobalProtect Clients to authenticate the GlobalProtect Gateways. This certificate must also be signed by the same certificate authority. Please note, usage of Client certificates is not necessary, but if used they do provide an elevated level of security. Using the Client certificates also necessitates the distribution of these Client certificates to all hosts which utilize the GlobalProtect Client.



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 same certificate used to sign the Gateway and client certificate



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

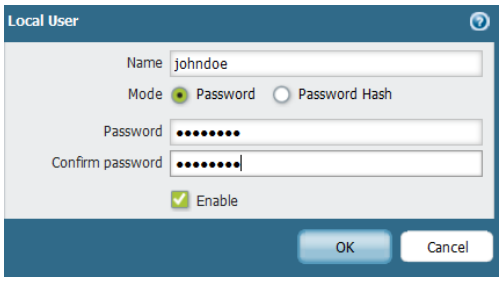
Name	Common Name	Certificate Authority	Private Key	Expires	Usage
web-server	localhost		✓	Jul 11 2020	Certificate for Secure Web GUI
GlobalProtect-CA	paloaltonetworks.com	✓	✓	Nov 29 2021	
GlobalProtect-GW	paloaltonetworks.com		✓	Nov 29 2021	
GlobalProtect-Client	paloaltonetworks.com		✓	Nov 29 2021	

Configuring User authentication

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

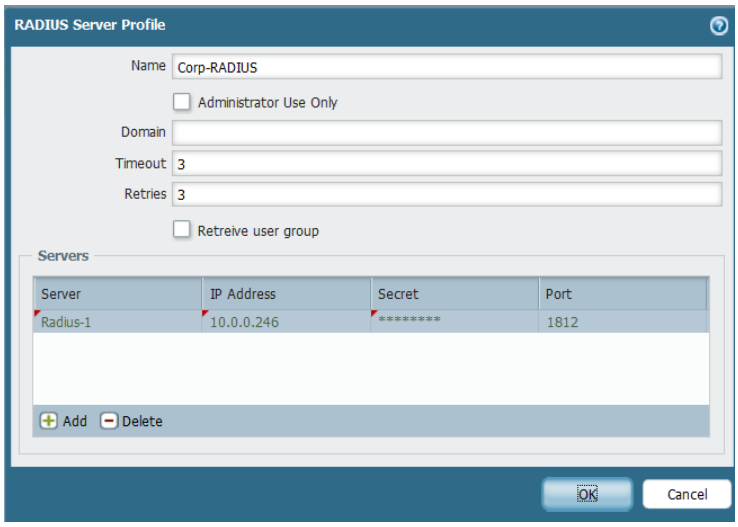
Local Database

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



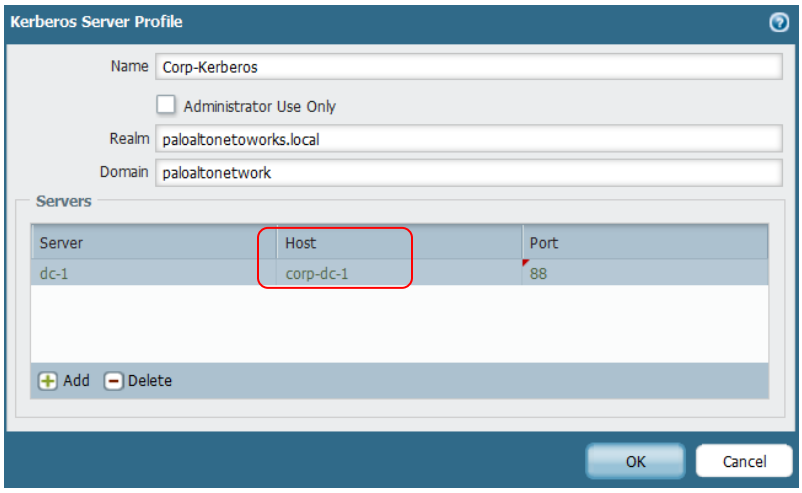
RADIUS

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



Kerberos

Kerberos server profile has a realm (for hostname), a domain (NetBIOS style), FQDNs and optional port that represent the KDCs 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 for by allowing usernames in NetBIOS format in allow list domainname\username).

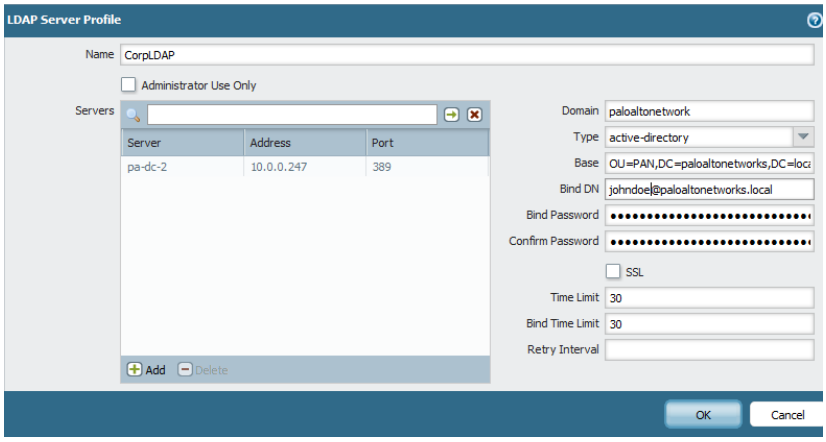


Note: The host entry should be FQDN and not the IP address

LDAP

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

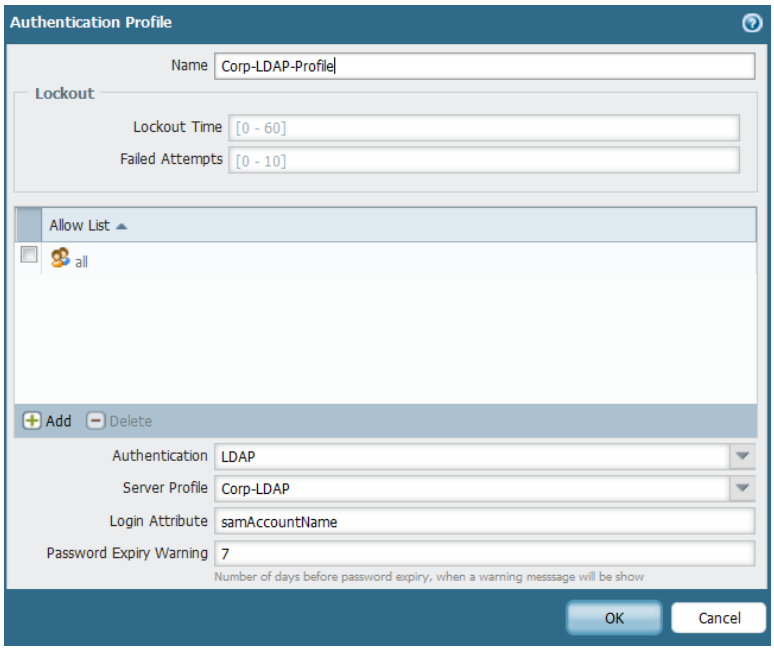
search).



Authentication profile

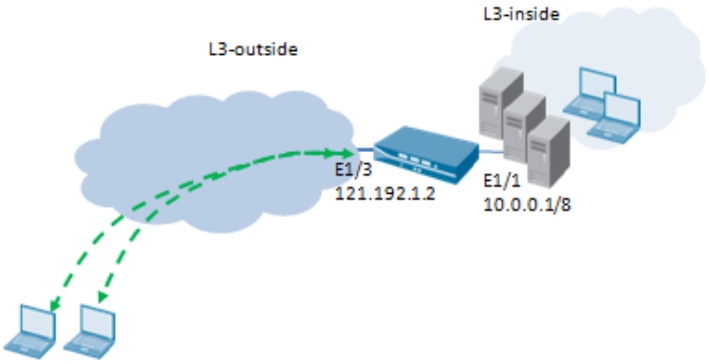
The authentication profile refers to the authentication method configured in the previous step. The authentication profile is then used to associate the authentication method in the GlobalProtect Portal configuration. An example of using the LDAP database is shown below. Authentication profile using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

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



Configuring 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, but can be configured to use tunnel. Forcing the internal Gateway to use tunnel will provide the Firewall with the user to IP mapping. Gateways support split tunnel. This is not recommended if you want to extend firewall policy with application control and visibility to all mobile users. The Gateway(s) receive HIP profiles and allow enforcing policy on it. For this configuration example we will refer the topology below



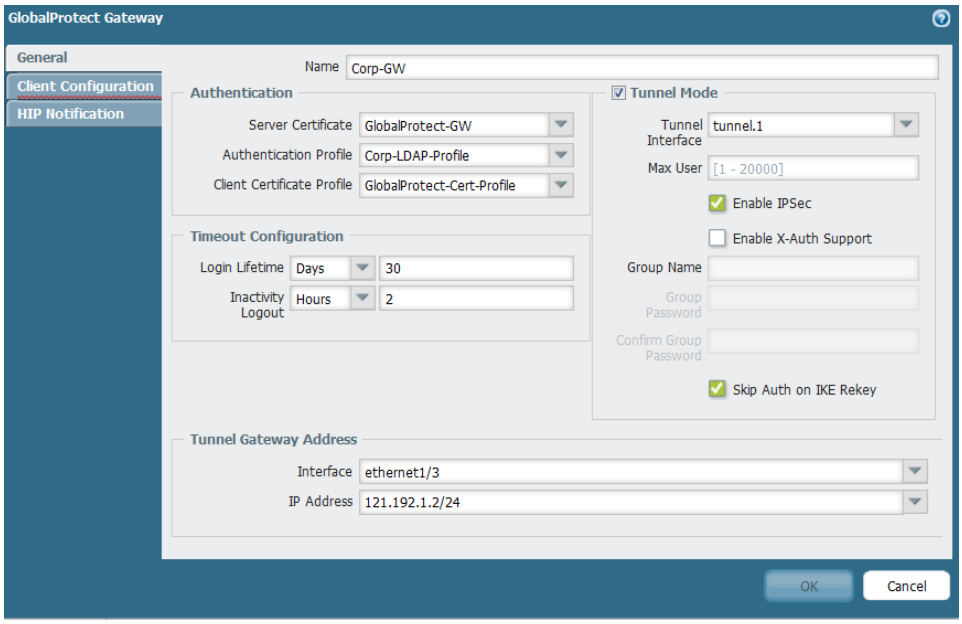
The interface and zone binding on the firewall are summarized below

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 to Gateway navigate ***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:

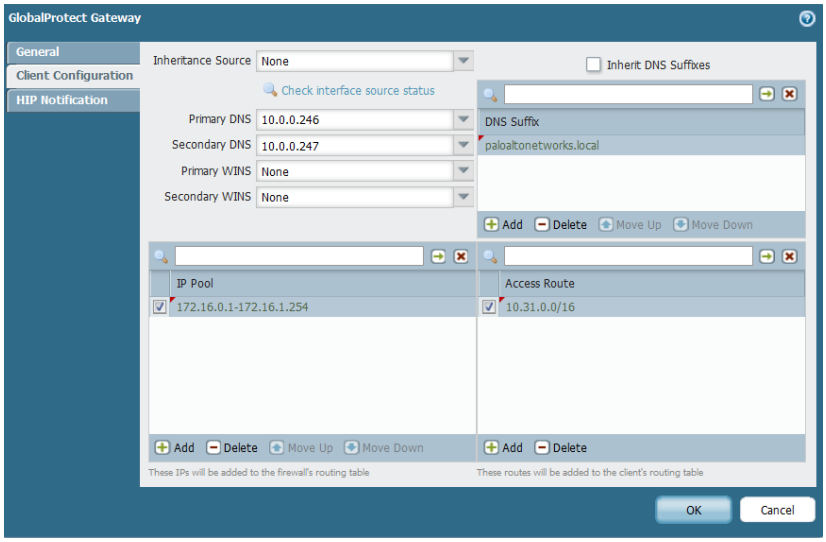
- When using external Gateway, it is recommended to configure the tunnel interface in its own zone. This provides the ability to enforce a different security policy on the traffic from the remote users which are connected using GlobalProtect tunnel.
- In order to identify users, enable 'User Identification' on the zone in which the tunnel interface is bound



General Tab:

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 choose 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:



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

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, also known as split tunneling.

Inheritance source: This specifies 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

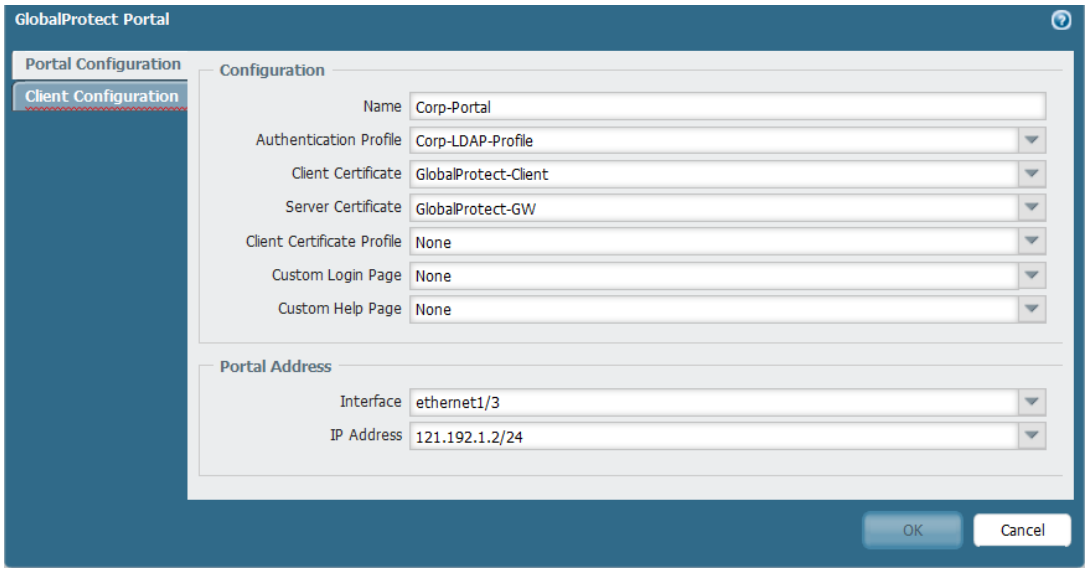
Note: If the firewall is deployed in active-active HA, the floating IP address can be used as the Portal IP address. In such deployment, select "floating IP address" as the choice

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

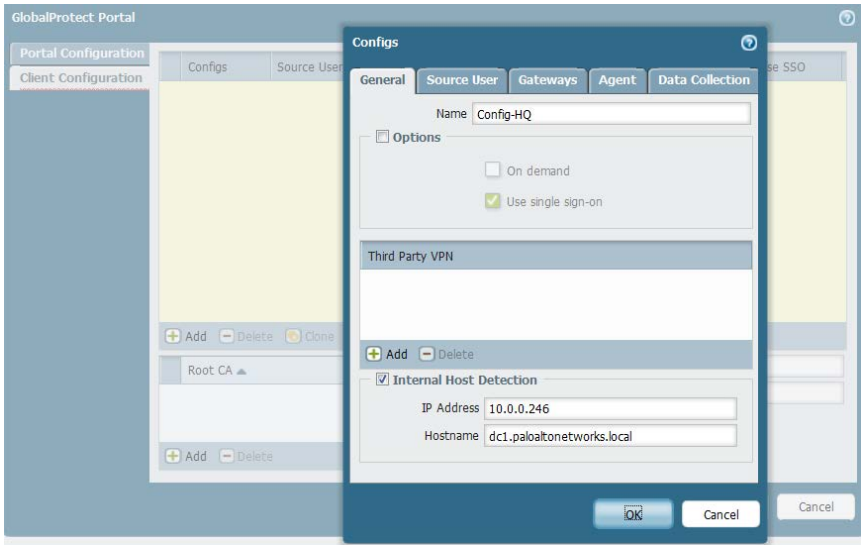
Portal Configuration:
The authentication profile is used to authenticate users when they first browse to the Portal address to authenticate and download the GlobalProtect Client. The Client and server certificate are used to authenticate the Client and the Portal. The certificates are sent to the Client 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



Client configuration general tab:
This section defines the parameters that will determine the GlobalProtect Client behavior. Click on "ADD" to create a new Client configuration and give it a name



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 to be being sent to the GlobalProtect Gateway. If the host that has GlobalProtect Client running also has other remote access VPN software installed, for example Juniper Network Connect, you can use this option to exempt the traffic from 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.

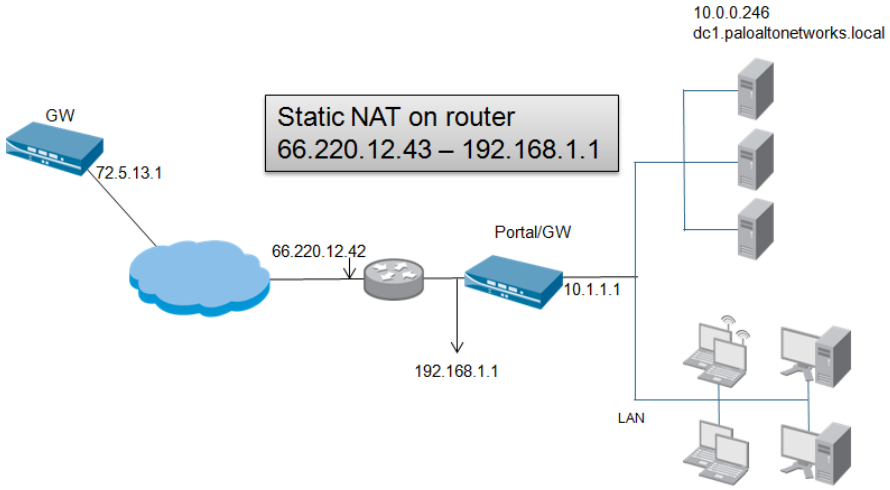
Internal Host Detection: This helps Client determine whether the host is inside or outside the corporate network and then connect to the corresponding Gateway. The DNS name specifies a hostname that only can be reached from internal network and its IP address. The Client performs a reverse lookup on the IP address and if it receives the expected hostname as a response, it will attempt connecting to the Gateways in the internal list. If no response is received that Client will attempt to connect to the external Gateways in the external list
If no "internal-host-detection" configuration is provided, Client always connectes to the 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 are not reachable on the public network.

Source User
GlobalProtect Portal allows for configuration based on users and user group. This allows different set of users or groups to have their 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.

Gateway
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. 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 shown below 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 shown below

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:

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

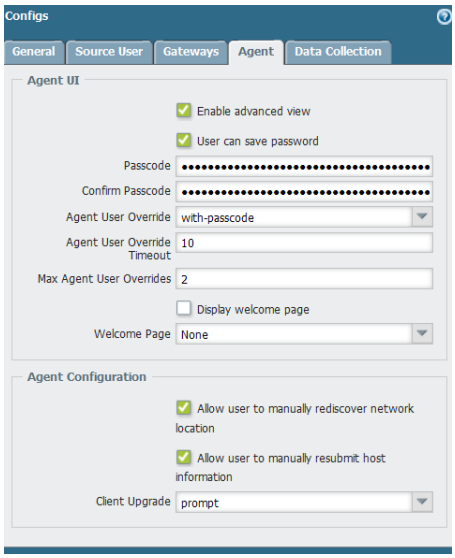
The average response time in this case is 35 milliseconds. Even though Gateway-2 has the lowest response time, the Client will connect to Gateway-1, because its response time is less than the average, and has the highest priority.

Note:

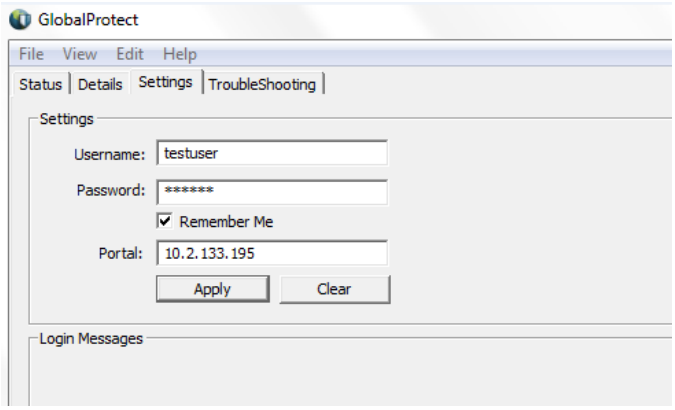
- The Client will connect to only one External Gateway
- If there are multiple internal Gateways, Client will send the host state report to all the internal Gateways in the list. All traffic from the Client will traverse the through Gateway determined the network configuration.

Client

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



Enabled Advanced View: Allows the end users to select advanced view section of the Client as shown below



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

Client/Agent override with comment

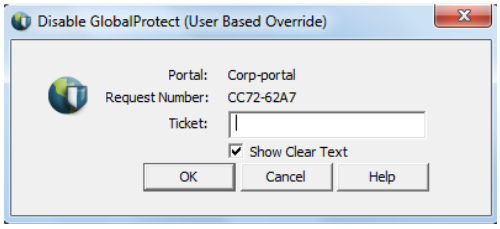
Users will be prompted to enter a comment when the disable

Client/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.

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 screen shot below

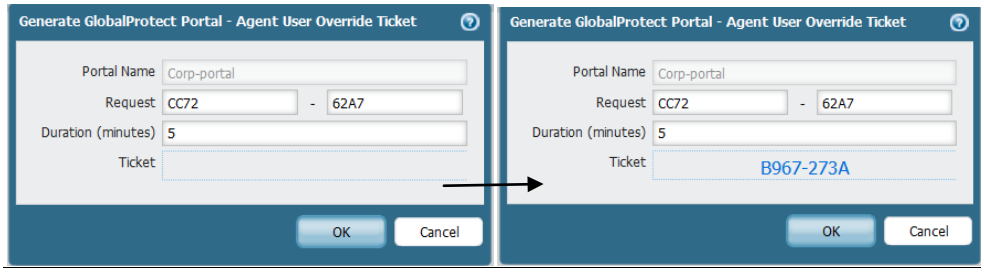


The user will then give the request number to the firewall administrator offline in order to get a ticket that can be used to disable the Client.

The process for generating the ticket is listed below.

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

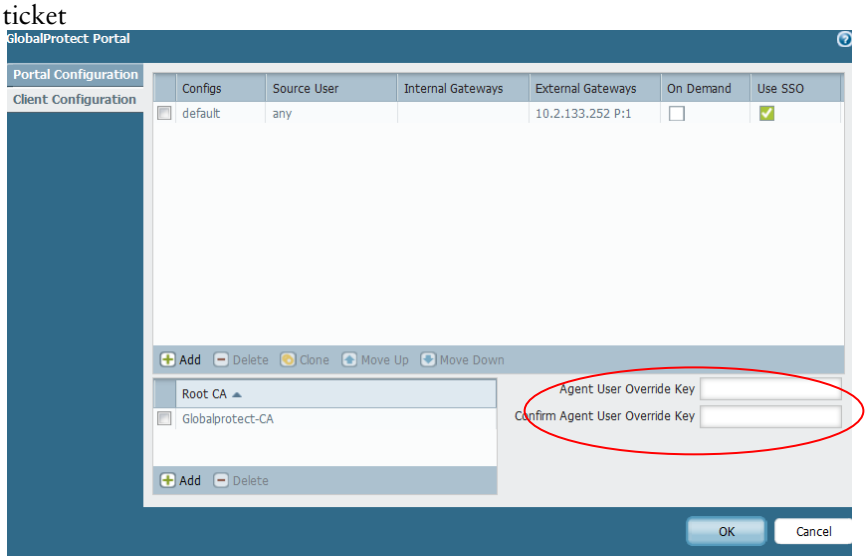
- Enter the request number provided by user. The request number is case sensitive.
- Specify the lifetime the ticket is valid and be used to disabled the Client and click on OK. The maximum value is 65535
- This generates ticket. This ticket is used by the user to disable the Client



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

Agent/Client user override key (optional)

To secure the Client User override ticket, you can specify a Client 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



Agent User Override Timeout—The amount of time, the Client/Agent 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/Agent before a successful connection to a firewall is required.

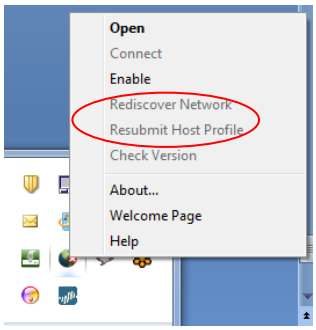
Client Upgrade: This setting defines the Client/Agent upgrade behavior. The two options available are prompt, and transparent.

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/Agent

Allow user to manually resubmit host information—Select this check box to allow the user to manually trigger resubmission of the latest HIP Client/Agent



Root CA
Specify the Root CA or issuing certificates 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

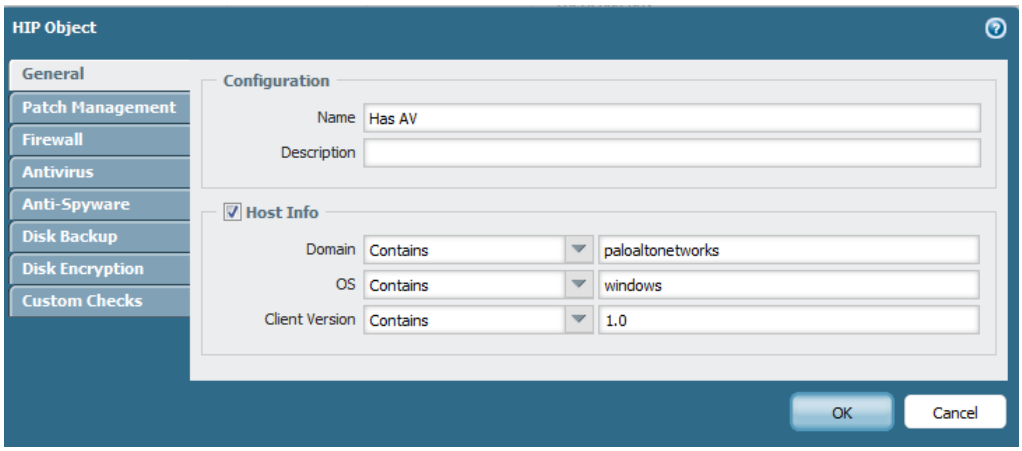
The GlobalProtect Client gathers information about the end host, which is then reported back to the Gateway. This is referred to as HIP Objects. HIP object definition, is used to match on the categories sent by the GlobalProtect Client to the Gateway. The GlobalProtect Gateway then uses the information 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

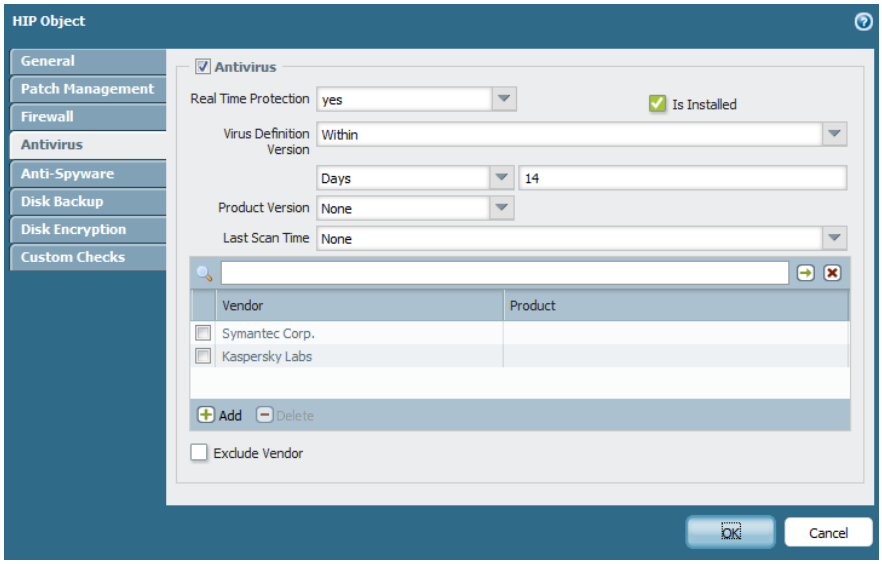
HIP object definition, is used to match on the categories sent by the GlobalProtect Client to the Gateway. The GlobalProtect Gateway then uses the information received from the Client to generate HIP report about the host.

In the example below shows HIP objects to check for antivirus and host information

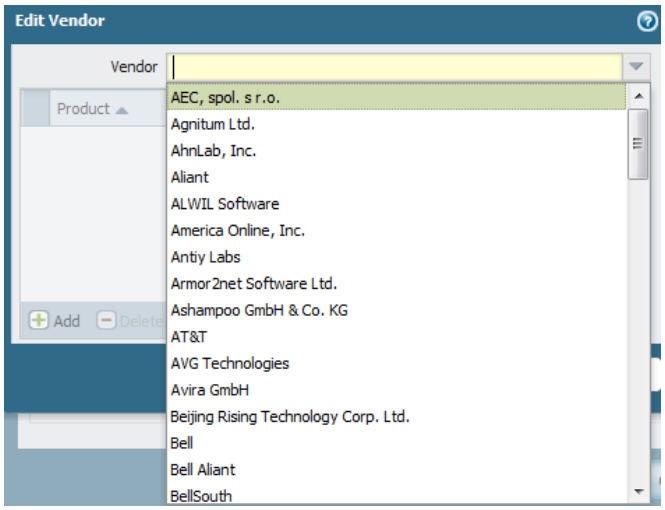
Object>GlobalProtect > HIP object>Add



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



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



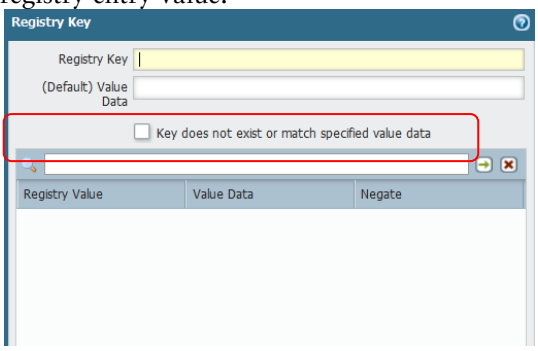
You can view all the defined HIP objects by navigating to **Objects>GlobalProtect>HIP object**. An example of the configured HIP objects is shown below. The location column displays the name of the VSYS where the object is defined

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	

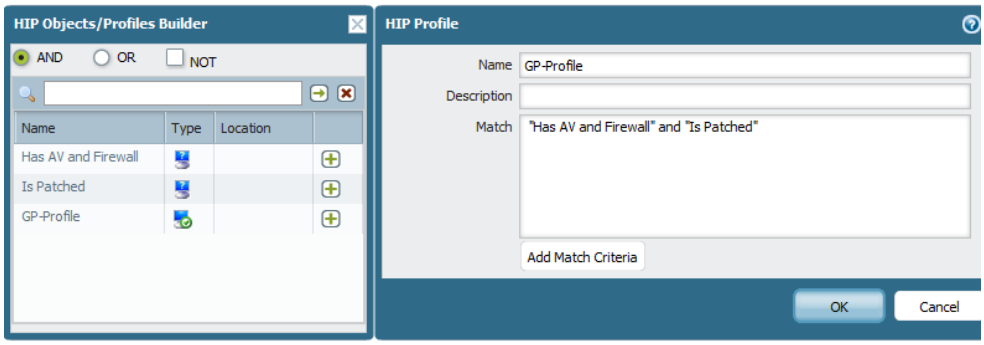
HIP objects checking registry keys

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, combined logic such that when evaluated, the result will either be true or false. HIP profile is referred as match condition in the security policy configured on the Gateway. To configure a HIP profile navigate to *Object>GlobalProtect > HIP profile*



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.

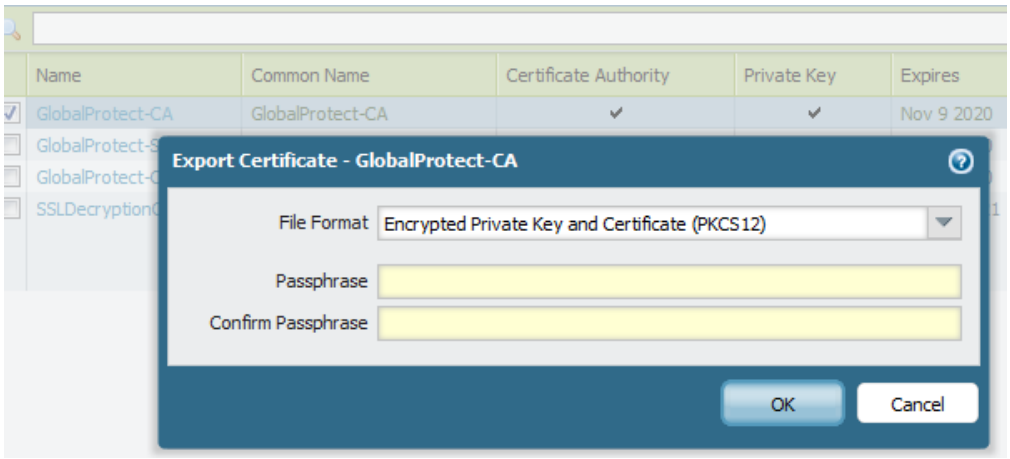
Table below shows sample security policies and HIP profiles used in conjunction to allow or deny traffic

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 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 AV and FW to be present for user to access the internet.

Configuring multiple GlobalProtect Gateways

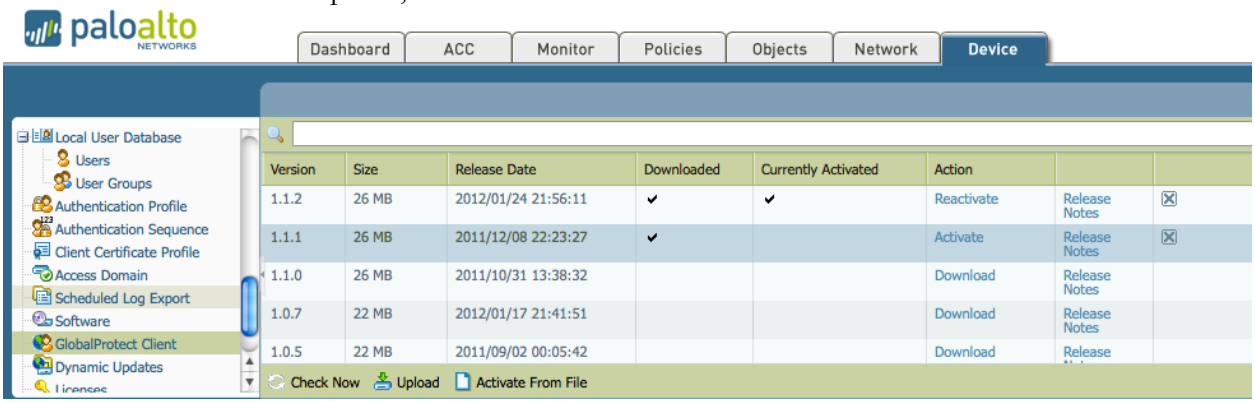
When deploying multiple Gateways, each one of the Gateway must have its own Gateway certificate signed by the same certificate authority. This requires that the certificate of the CA server and the key be imported to each one of the Gateway and use this certificate to sign the Gateway and the client 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



Log into the second firewall that will be used as the Gateway, from **Device > Certificate** click on **Import** to import all the three certificates. Follow the steps in the Configuring Gateway (above) to complete the configuration.

Download and Activate the GlobalProtect Client on the Firewall

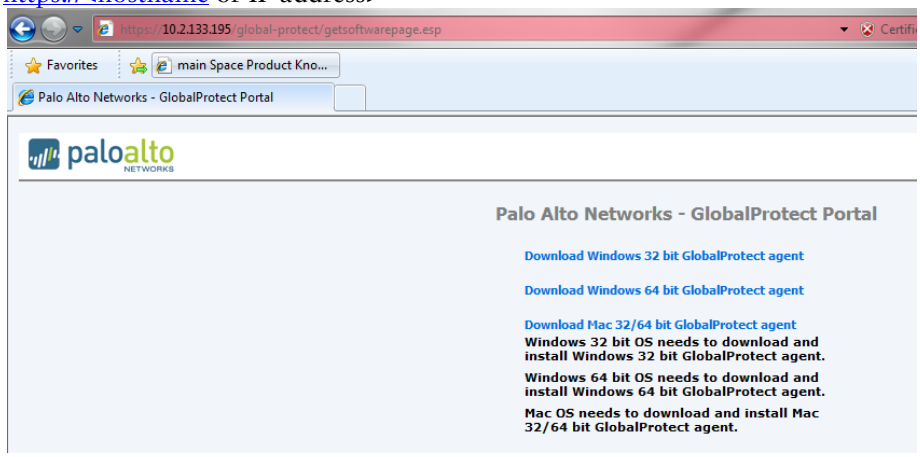
There are several versions of the GlobalProtect Clients available, so the Firewall must know which version to use. To select the GlobalProtect version, go to **Device > GlobalProtect Client** click **Check Now** (bottom left) to get the latest list of GlobalProtect Clients. Click **Download** on the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



Note: 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.

Distributing GlobalProtect Client

In Active Directory environments, GlobalProtect Client can also be distributed to end users, using AD group policy. AD Group Policy 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 by browsing to the address of the Portal https://<hostname or IP address>

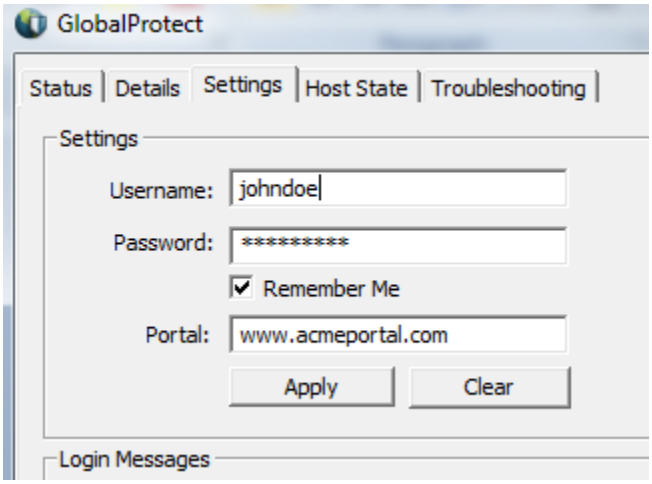


Note: Administrator privilege is required for installing the GlobalProtect Client/Agent for the first time. Subsequent upgrades do not require administrator privileges.

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



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

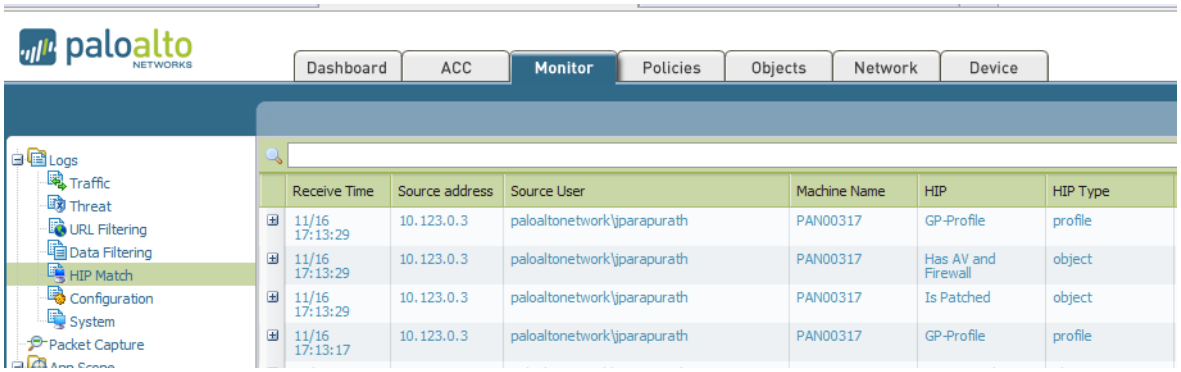
- The Client contacts the Portal and retrieves the list of Gateways among other configuration.
- The Client then checks whether it is on the internal network or external network by performing the reverse DNS lookup.
- If the Client determines it is on external network, it contacts all Gateways in the list and establishes a SSL handshake.
- Client establishes connection to Gateway with fastest response 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 your Portal hostname in it. In that case, a newly installed GP Client will always connect to the Portal configured in this entry. It is important to know for mass deployments is also that GP will always try to use SSO credentials on its first connection when no username or password has been defined yet. So if you combine the SSO feature together with deploying the "Portal" registry entry, you should get a completely seamless user experience. In that case, GP 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**

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



ACC provides reports for HIP objects and profiles

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

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. 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:

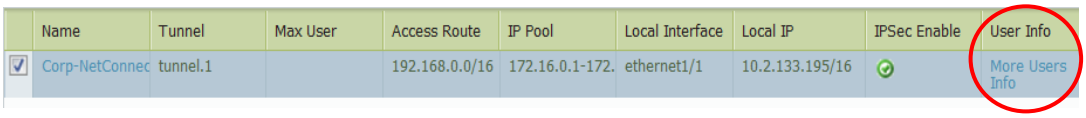
```
admin@LAB> show global-protect-gateway gateway name Corp-NetConnect

        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**":*



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 device-server dump hip-profile-database - This command shows the current active GP users and their HIP profiles

debug device-server dump hip-report computer <computer name> user <username> ip <address>
This command shows the raw XML version of the hip-report received by the Gateway

Debug device-server set hip (all\|basic\|detail\|ha) - This command enables debug trace in device server about hip report processing. The output is in devsrv.log

GP Client logs

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

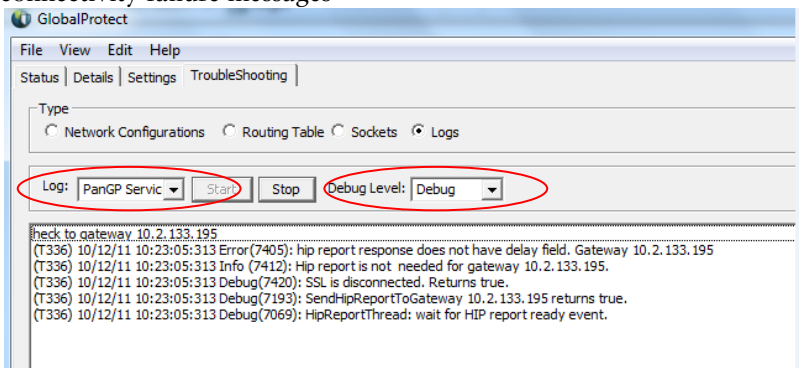
Firewall

- Authentication failures
  - Verify the users can authenticate by browsing to the IP address of the portal and authenticating to it
  - 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)

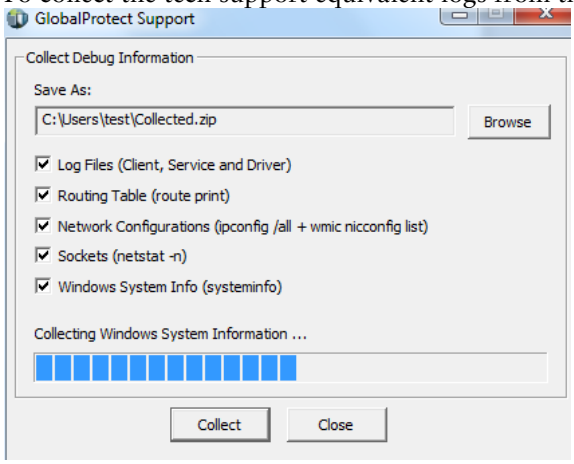
Agent

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



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



Revision History

Date	Revision	Comment
02/04/2012	1.1	First published draft with 4.1
02/28/2012	1.2	Updated sections on HA and gateways