SECURING ENDPOINTS WITH GLOBALPROTECT

EXTEND PREVENTION TO REMOTE USERS

- GlobalProtect overview
- Preparing the firewall for GlobalProtect
- Configuration: GlobalProtect Portal
- Configuration: GlobalProtect Gateway
- Configuration: GlobalProtect agents
- Monitoring GlobalProtect connections

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

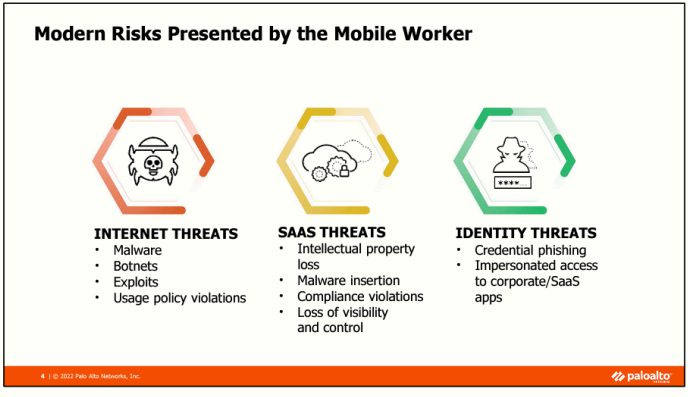
After you complete this module,
you should be able to:

- Describe the three major components of GlobalProtect
- Configure the client and server certificates to authenticate the agent and the portal
- Configure a GlobalProtect Portal
- Configure a GlobalProtect internal and external gateway
- Configure a GlobalProtect client

After you complete this module, you should be able to:

- Describe the three major components of GlobalProtect
- Configure the client and server certificates to authenticate the agent and the portal
- Configure a GlobalProtect Portal
- Configure a GlobalProtect internal and external gateway
- Configure a GlobalProtect client

This section provides a high-level introduction to GlobalProtect.

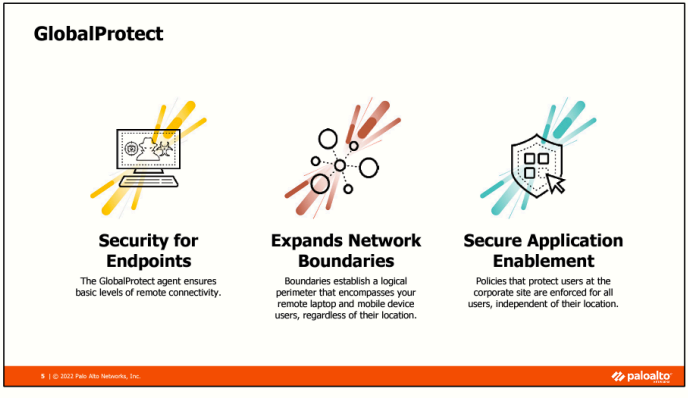


Whether checking email from home or updating corporate documents from an airport or coffee shop, the majority of today's employees work outside physical corporate boundaries. This mobile workforce increases productivity and flexibility while simultaneously introducing significant security risks. Every time users leave the building with their laptops or smartphones; they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network.

Most attacks start by exploiting a user in order to compromise an endpoint. An endpoint that is operating outside of the network perimeter is exposed to a greater amount of risk. If these endpoints are exploited, and then the user returns to the organization, it gives the attacker the ability to conduct lateral movement operations by directing the attack from a command-and-control server.

A second area where there is risk is the use of SaaS applications. With SaaS applications, the risk is not just from users leaving the perimeter boundaries; risk comes from the applications as well. With both the user and the SaaS application outside of the perimeter, the organization has no ability to stop threats such as the use of unsanctioned apps and the movement of data. Data is moving into areas where the organization cannot control it, and the applications being used are typically outside of the organization's control as well.

Credential theft is a multistage issue—and a big problem. A stolen credential allows the attacker to impersonate a legitimate user, thus allowing them to bypass many of the controls that are designed to stop an intruder. The first stage is the theft of the credential itself, such as tricking the user to visit a phishing site or delivering malware to the user that steals keystrokes. The second stage is the use of the stolen credential to gain network access to the organization or to access SaaS applications.



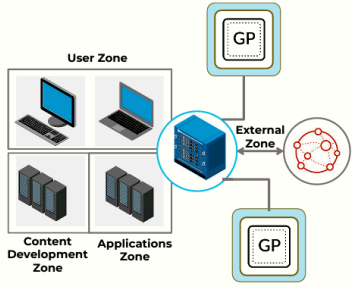
GlobalProtect network security for endpoints builds on familiar mobile security technology: the remote-access VPN. The GlobalProtect agent ensures basic levels of remote connectivity. From this base, GlobalProtect builds more advanced features that transform mobile security.

GlobalProtect expands the boundaries of the physical network while effectively establishing a logical perimeter that encompasses your remote laptop and mobile device users, regardless of their location. When a remote user logs in to the device, GlobalProtect automatically determines the closest gateway available to the roaming device and establishes a secure connection using strong authentication. Laptops and mobile devices stay always connected to the corporate network and are protected as if they never left the corporate campus.

GlobalProtect solves the security challenges introduced by roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located. As a result, the operational challenges associated with creating and managing separate policies for corporate firewalls and remote users are eliminated. GlobalProtect provides policy criteria of applications, users, and content.

Zero Trust Principles with GlobalProtect

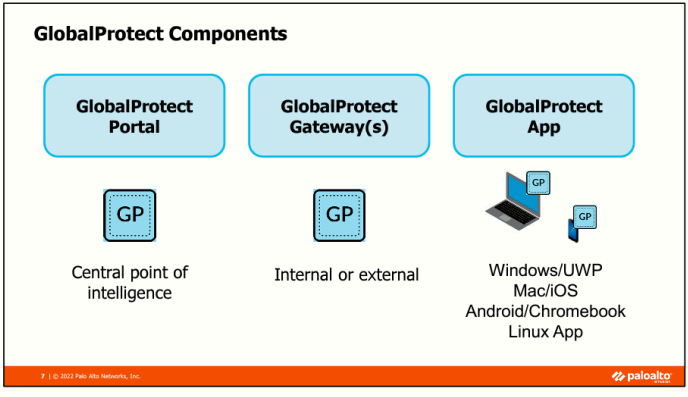
- Extend next-generation firewall protection to endpoints
- Apply quarantine restrictions
- Policies allow or restrict network access



6 | © 2022 Palo Alto Networks, Inc.

Not all users need access to all assets inside your corporate network. Security teams are adopting Zero Trust principles to segment their networks and enforce precise controls for access to internal resources. GlobalProtect provides the fastest, most authoritative user identification for the platform, enabling you to write precise policies that allow or restrict access based on business need. Furthermore, GlobalProtect provides host information that establishes device compliance criteria associated with Security policies. These measures allow you to take preventive steps to secure your internal networks, adopt Zero Trust network controls, and reduce the risk of attack.

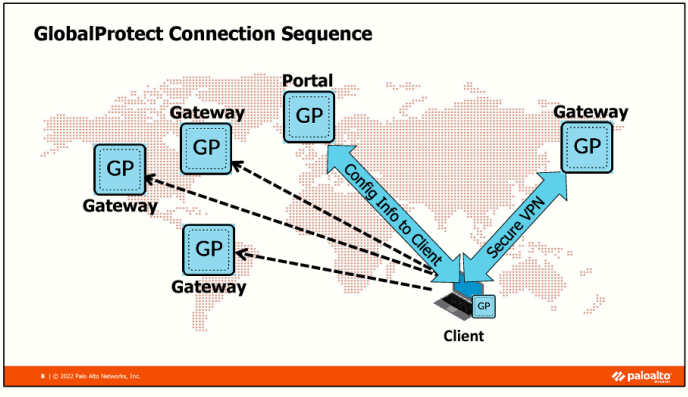
In addition, GlobalProtect enables you to quarantine compromised devices by using an endpoint's immutable characteristics. This will allow administrators to restrict network access as well as prevent the compromised endpoint from infecting other users and devices. Quarantine restrictions can apply whether the compromised device is external or on the internal network.



GlobalProtect provides a complete infrastructure for managing your mobile workforce to enable secure access for all your users, regardless of what endpoints they are using or where they are located. At the most basic level, you can use GlobalProtect as a replacement for the traditional VPN gateway, eliminating the complexity and headaches of administering a standalone, third-party VPN gateway.

GlobalProtect deployment has three major components:

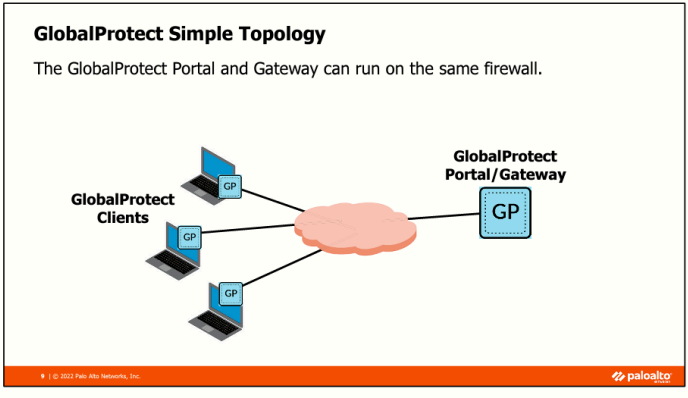
- **GlobalProtect Portal**: Provides the management functions for your GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about what gateways are available as well as any client certificates that may be required to connect to the GlobalProtect Gateway(s). In addition, the portal controls the behavior and distribution of the GlobalProtect app software.
- **GlobalProtect Gateway**: Provides security enforcement for traffic from GlobalProtect apps. Additionally, if the Host Information Profiles (HIP) feature is enabled, the gateway generates a HIP report from the raw host data the apps submit and can use this information in policy enforcement. You can configure different types of gateways to provide security enforcement or VPN access for your remote users, or to apply a Security policy for access to internal resources.
- **GlobalProtect App**: Runs on endpoints and enables access to your network resources through the portals and gateways that you have deployed. The GlobalProtect app for Windows and macOS endpoints is deployed from the GlobalProtect Portal. The GlobalProtect app for mobile endpoints (iOS, Android, and Windows UWP) is available through the official store for the endpoint—the Apple App Store for iOS, Google Play for Android, and the Microsoft Store for Windows UWP.



The GlobalConnect connection sequence is as follows:

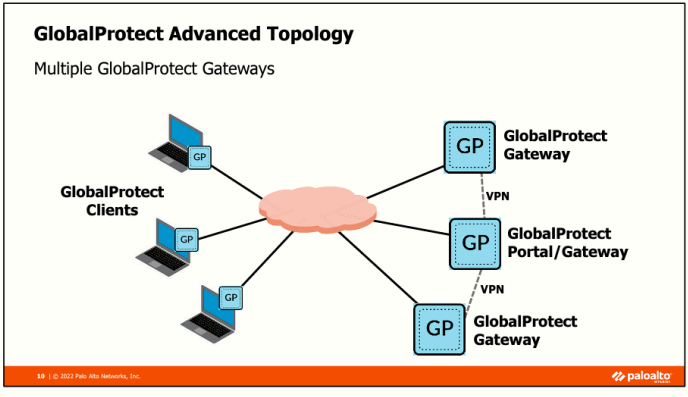
1. The GlobalProtect client on the local system connects to the GlobalProtect Portal for authentication.
2. After authorization is confirmed, the portal sends the client configuration and a list of GlobalProtect Gateways.
3. The client connects to the best gateway (based on SSL response time and local priority) to respond to its connection request.

The client communicates with portals and gateways. There is no direct communication among gateways or between gateways and portals. After the client is installed and enabled, the client contacts the portal when setting up a connection. Any time the client contacts the portal, the portal authenticates the connections.



A GlobalProtect implementation requires at least one portal and one gateway:

- The portal and gateway can be configured on the same firewall.
- In the simplest configuration, a single firewall is configured to serve gateway and portal services from the same IP address, which provides end users with VPN access to the internal networks with a minimum of configuration.
- If the gateway and portal share an IP address, only one certificate is needed for the firewall.

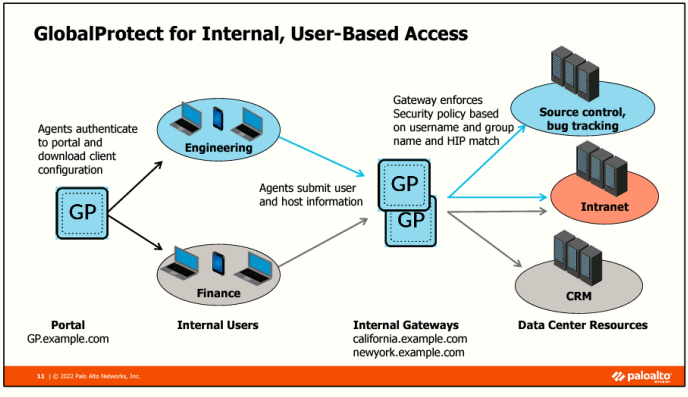


For larger environments, GlobalProtect can be configured with multiple gateways:

- Additional gateways can be used to provide access to multiple protected networks. They also can be used to provide redundancy and performance improvements for end users.
- GlobalProtect clients connect directly to a gateway (from a list provided by the portal). By default, the chosen gateway is the one that responds fastest to the connection request.
- To ensure consistent access, multiple gateways often require the networks to be connected to each other by VPN so that the end user has access to the same data, regardless of which gateway they connect to.

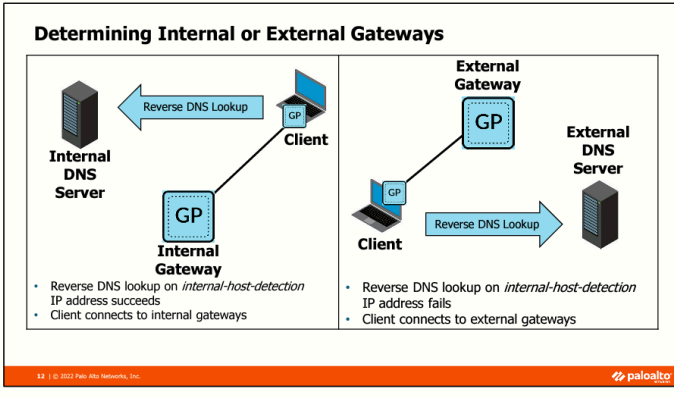
Although there can be only one portal, the portal is not a single point of failure: If the firewall that hosts the portal is not reachable, then the clients will use their cached configuration to connect to the gateways.

The only limitation of this scenario is a down portal. If the portal is down, you cannot install a new client or distribute configuration changes to existing clients. To resolve this issue, either re-establish the connection to the portal or redirect clients to a standby portal configured on another firewall. The redirection can be executed by a change in the DNS record of the portal.



An internal gateway is an interface on the internal network that is configured as a GlobalProtect Gateway. When used in conjunction with User-ID and HIP checks, an internal gateway can be used to provide a secure, accurate method of identifying and controlling traffic based on user or device state. Internal gateways are useful in sensitive environments where authenticated access to critical resources is required.

In this example, internal gateways are used to enforce group-based policies that allow users in the Engineering group access to the internal source control and bug tracking databases and allow users in the Finance group to the CRM applications. All authenticated users have access to internal web resources. HIP Profiles configured on the gateway also check each host to ensure compliance with internal maintenance requirements, such as whether the latest security patches and antivirus definitions are installed, whether disk encryption is enabled, or whether the required software is installed.



An internal gateway is an interface on the internal network that is configured as a GlobalProtect Gateway and applies Security policies for internal resource access. An external gateway resides outside of the corporate network and provides security enforcement and VPN access for your remote users.

The portal can provide an IP address and DNS hostname as part of the information passed to the client, which the client can use to determine whether it is inside or outside the corporate network:

- The agent performs a reverse lookup on the IP address. If it receives the expected hostname as a response, the agent assumes it is on an internal network and connects to the gateways in the internal list.
- If no response is received for the lookup, the client connects to the gateways in the external list. If an internal host detection hostname and address pair is not provided, the client connection attempts to connect to the internal gateways first, then to the external gateways.

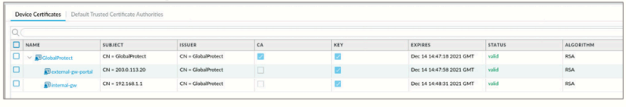
The DNS hostname and IP address must correspond to a device whose name can be resolved only by an internal name server.

This section provides an overview of preparing the firewall for GlobalProtect.

GlobalProtect Certificates

- Certificate authority (CA) certificate (optional)
- GlobalProtect Portal certificate
- GlobalProtect Gateway certificate
- GlobalProtect client certificate (optional)

Device > Certificate Management > Certificates



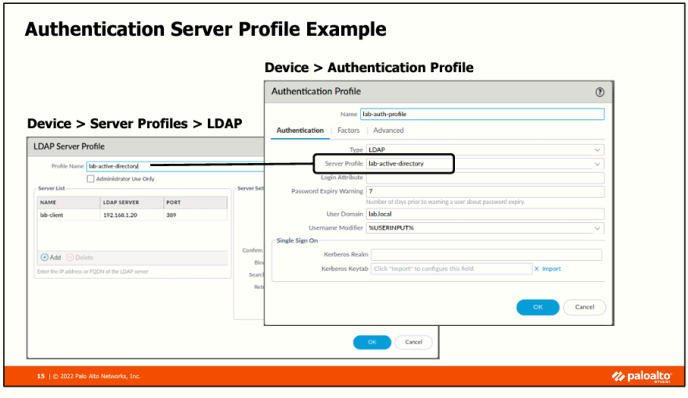
Connectivity between all parts of the GlobalProtect infrastructure is authenticated using SSL certificates. The portal can act as a certificate authority (CA) for the system (using a self-signed or imported subordinate issuing a CA certificate within the portal), or customers can generate certificates using their own CAs. The portal, gateways, and agents must use certificates signed by the same CA. Prior to transferring any information, the client verifies that the gateway is using a server certificate signed by the appropriate CA. You can configure the gateway to verify that the client has a client certificate signed by the appropriate CA.

If third parties that might not trust a self-signed CA are to be granted remote access, a certificate issued by a public CA should be used for the portal.

The portal includes the CA's public certificate and the needed client certificate and key in the configuration bundle that is sent to the client. GlobalProtect Gateways use the client certificate to authenticate and identify the client.

Support is provided for the portal to export the necessary server certificate and key for the gateways. If an external CA is used, support is provided to import the CA certificate, server certificate, and key for portals and gateways, or with a client certificate and key for clients.

Portals and gateways do not communicate directly, so gateway certificates must be imported manually onto those firewalls.

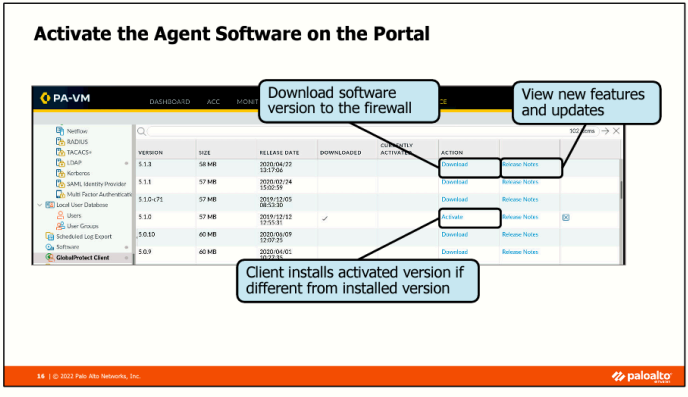


GlobalProtect relies on the same system of Server Profiles and Authentication Profiles as PAN-OS software does with administration authentication or User-ID:

1. Create the Authentication Server Profile. The example uses an LDAP configuration.
2. Attach the Authentication Server Profile to an Authentication Profile.

Before you can configure a firewall to authenticate against an existing LDAP server, ensure that the LDAP Server Profile contains the server's name, IP address, port, and proper server settings.

After the Server Profile is created, create the Authentication Profile. In this example, we set the authentication **Type** to **LDAP** and selected the **Server Profile** to **lab-active-directory**.



Before you deploy the GlobalProtect app for your end users, you should download the new app installation package to the firewall that is hosting your portal, and then activate the software for download to the apps connecting to the portal. This deployment method is available for all non-mobile app versions.

The GlobalProtect client page lists the available GlobalProtect releases, and you can download and activate the agent version you wish to support. When the agent connects to the portal, the firewall checks the version and installs the currently *activated* version if it is different from the version that is on the client system.

Only the portal provides client information to end users, so this software must be maintained only on the portal firewall.

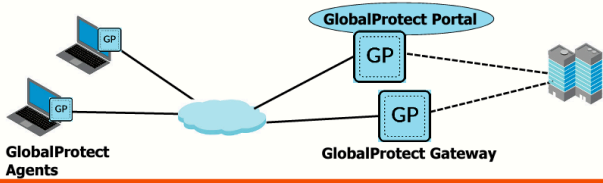
After you have downloaded the GlobalProtect client, you must activate it. You can only have one activated version of the GlobalProtect client.

If the firewall does not have internet access, you can download the GlobalProtect App software package from the Palo Alto Networks software updates support site using an internet-connected computer. Then, manually upload the app to the firewall.

This section provides an overview of configuring the GlobalProtect Portal.

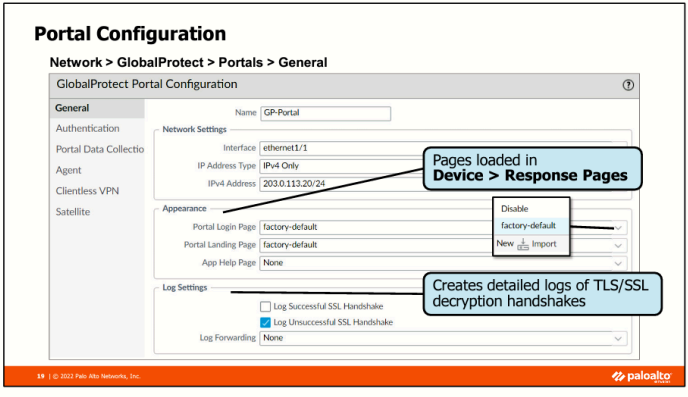
GlobalProtect Portal

- Authenticates users initiating connections to GlobalProtect
- Can create and store custom client configurations
- Maintains lists of internal and external gateways
- Manages CA certificates for client validations of gateways



Most configuration for GlobalProtect happens on the portal. The portal is responsible for coordinating communications and interaction between all other GlobalProtect components.

GlobalProtect administrators can set the level of control that end users have over their connections, from a fully locked-down configuration to one where users are allowed to select which gateway they connect to.



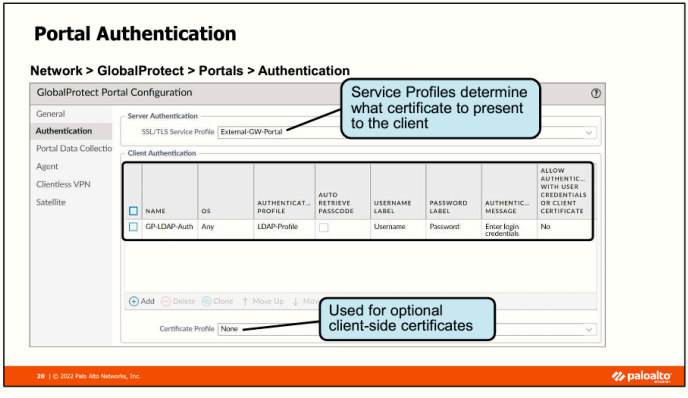
Use the portal configuration window to manage the portal's configuration. A Layer 3-capable interface is needed to host the portal functionality.

The options on the **General**, **Authentication**, and **Satellite** tabs are similar between gateways and portals.

The **Agent** tab options are different. The **Clientless VPN** tab is available only for the portal.

The portal agent configurations pertain specifically to the agents that will be hosted on the portal. When you configure a GlobalProtect Portal, you can disable access to the portal login page from a web browser. This action prevents public access to the portal login page and unauthorized attempts to authenticate to the GlobalProtect Portal from a browser. Enablement of this option does not affect access of the GlobalProtect agents or GlobalProtect apps to the portal. The GlobalProtect agents and apps continue to authenticate and connect to the portal to receive their respective configuration updates.

You can log successful and unsuccessful TLS/SSL decryption handshakes. By default, only unsuccessful handshakes are logged. You can forward decryption logs to Log Collectors, other storage devices, and specific administrators.
Any environment that requires customized login and help pages for GlobalProtect can be configured in **Device > Response Pages**.

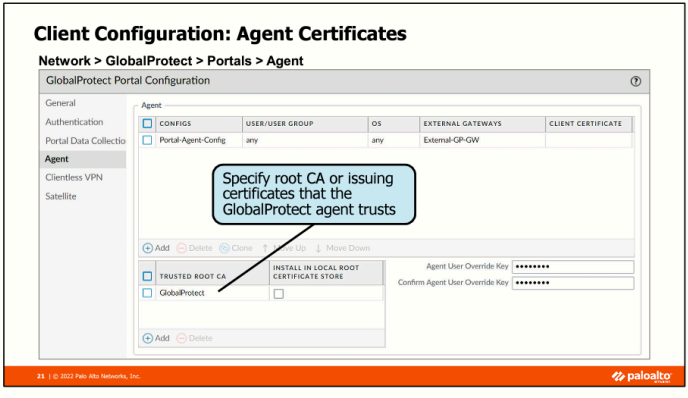


The **Authentication** tab is used to configure how agents will authenticate when they connect to the portal. The authentication configuration specifies which certificates and authentication method will be used in securing the GlobalProtect Portal and agent communication.

Use the **SSL/TLS Service Profile** to configure which certificate the portal presents to the GlobalProtect client software to verify the portal's identity.

Use the **Certificate Profile** to configure which certificate the portal should use to verify agent certificates, if agent certificates were configured.

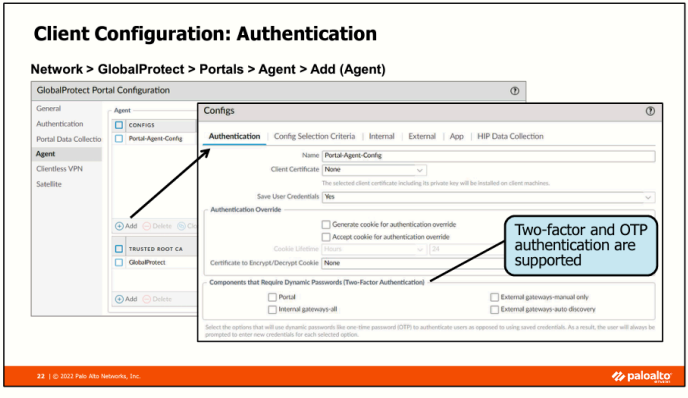
The **Client Authentication** section enables you to configure the method the portal will use to authenticate the agent. Agents running different operating systems can be configured to use different authentication methods. While you configure this section, you can configure an **Authentication Message**. This customizable message will be presented to end users when they attempt to log in to GlobalProtect. The authentication message can be used to tell them which credentials should be used for logging in to your gateways. It can be up to 50 characters in length.



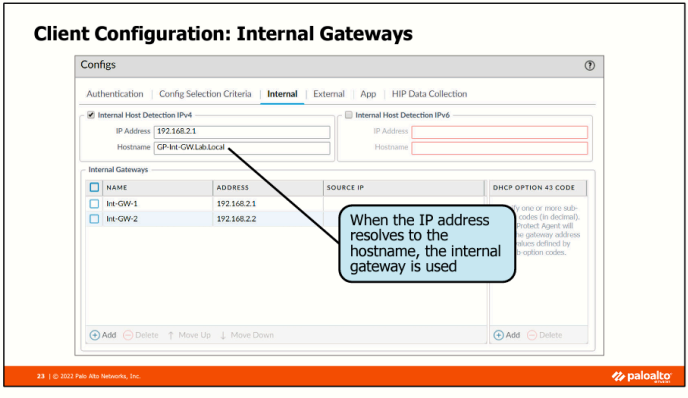
You can specify that the portal automatically deploys trusted root CA certificates and intermediate certificates. If the endpoints do not trust the server certificates that the GlobalProtect Gateways and GlobalProtect Mobile Security Manager are using, the endpoints will use these certificates to establish HTTPS connections to the gateways or Mobile Security Manager. The portal pushes the certificates you specify to the client along with the client configuration.

To add a trusted root CA certificate, **Add** an existing certificate or **Import** a new certificate. To transparently install the trusted root CA certificates that are required for SSL Forward Proxy decryption in the certificate store on the client, select **Install in Local Root Certificate Store**.

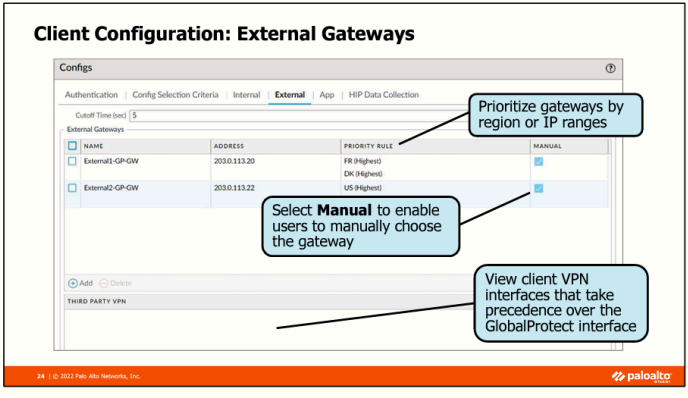
If the portal or gateway presents a certificate that has not been signed or issued by the same CA that issued the trusted root CA, the GlobalProtect app cannot establish a connection with the portal or gateway.



You can customize GlobalProtect connections for different users by creating multiple client configuration profiles. For example, you can configure the portal to handle connections from internal employee desktops and field personnel devices with different behavior for the two groups of users. However, if some remote users are using non-standard devices (such as iPads), additional functionality will be needed that traditional laptops do not require.



Use the **Internal** tab to configure the list of available internal gateways. You may also use this tab to configure the IP address and hostname that agents will use for internal gateway host detection. If an agent does a DNS reverse lookup on the listed **IP Address**, then the internal DNS server should return the listed **Hostname**.



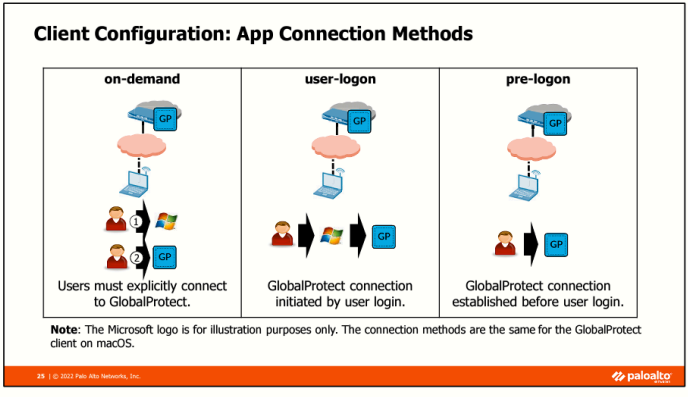
Use the **External** tab to configure the list of external gateways sent to the agent. For external gateways, the client contacts all the gateways and establishes a tunnel with the best gateway based on SSL response time and priority value. Priority can be further defined by region.

After the client is connected to a gateway, all client traffic is sent through the gateway.

Select a gateway's **Manual** check box if you want to permit users to manually choose to connect to that gateway. With this check box selected, the GlobalProtect agent presents the user the option to manually select that gateway. When the client connects to a new gateway, any existing tunnel will be disconnected, and a new tunnel will be established.

Gateways configured as **Manual** are not used during the automatic gateway selection process. The **(Manual only)** value can be viewed in the **Priority Rule** column.

The **Third Party VPN** section enables you to define a list of client VPN interfaces that will take precedence over the GlobalProtect interface. This section is designed for interoperability between GlobalProtect and other VPN clients. If there were no client VPN interfaces list, GlobalProtect might clash with routes presented by other clients.

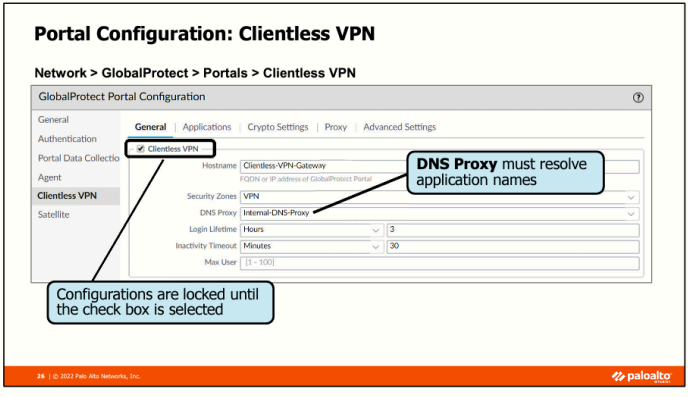


GlobalProtect supports three methods for client connections:

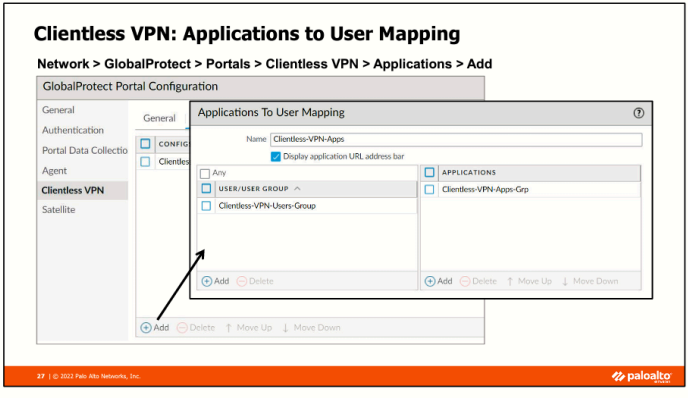
- **on-demand**: With this option, the user must explicitly initiate the connection.
- **user-logon**: This option automatically establishes a GlobalProtect client connection after the user logs in to their computer. If the use of single sign-on (or SSO) is selected, the agent uses the Windows credentials of the user to authenticate to the GlobalProtect Portal in a process that is completely transparent to end users. This method requires the Authentication Profile to use the same verification service as the login process (e.g., Active Directory or RADIUS).
- **pre-logon**: This option preserves pre-login and post-login services provided by a corporate infrastructure regardless of where the user machine is located. GlobalProtect establishes a connection, even if the user is not logged in to their computer. This practice means that a company can create a "logical network" that maintains the security and management features normally achieved by a physical network (e.g., Active Directory group policy enforcement). Tunnel selection and establishment happens before user login, based on machine certificates deployed outside of GlobalProtect.

For deployments using User-ID technology, pre-login conditions are marked with the user identifier of pre-login rather than a distinct user. After a user logs in to the client, the user information is changed to that username.

Note: Internal gateways support only always-on connection methods (user-logon or pre-logon). Select the agent connection method by navigating to **Network > GlobalProtect > Portals > Agent**. Either select an existing portal or create a new portal and configure your method from the **App** tab.



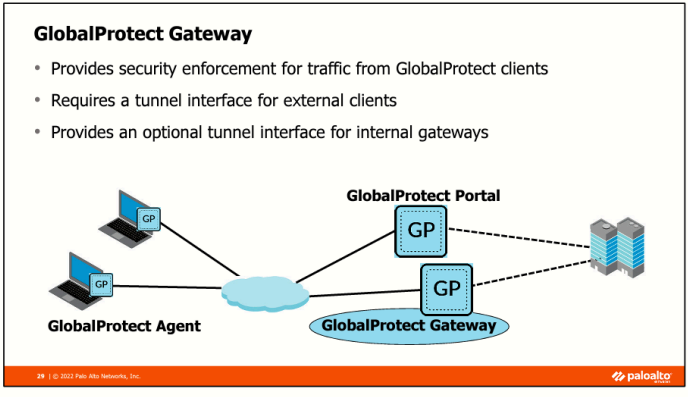
When you configure a clientless VPN, remote users can log in to the GlobalProtect Portal using a web browser and then launch the web applications you publish for the user. You can allow users to access a set of applications that you make available to them, or allow them to access additional corporate applications.



Applications can be published to users or to user groups for ease of use with clientless VPNs. However, access to those applications still is controlled through independent Security policy rules. Rules that allow the application traffic to flow for these remote users must be put in place before the clientless VPN applications can work.

Note: You must configure group mapping (**Device > User Identification > Group Mapping Settings**) before you can select the groups.

This section provides an overview of configuring the GlobalProtect Gateway.



The GlobalProtect Gateway provides the endpoint for the agent's connection.

If tunnel mode is enabled, the client will send all traffic through the connected gateway:

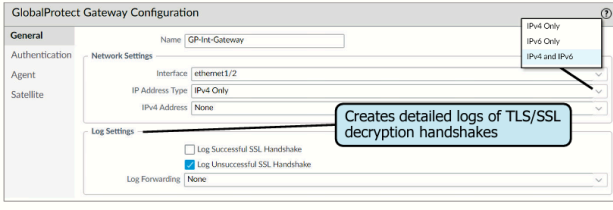
- External gateways require a tunnel.
- Internal gateways do not require a tunnel, but they can be configured to use one.

GlobalProtect Gateways support split tunneling. Although split tunneling is available, this feature is not recommended for extending the firewall policy with application control and visibility to all mobile users. Gateways enforce the policy based on the HIP Profiles they receive.

Gateway: General Tab

The **General** tab enables you to configure the settings that are common across both types of gateways.

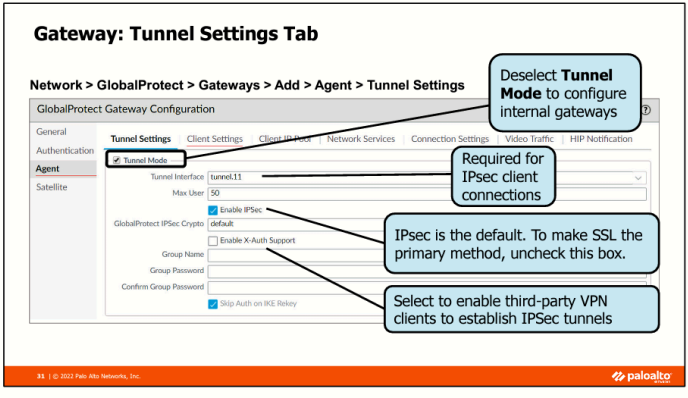
Network > GlobalProtect > Gateways > Add > General



Use the **General** tab to define the gateway interface to which the apps can connect and to specify how the gateway authenticates endpoints. **Network Settings** enables you to select the Layer 3-capable interface on the firewall that is visible to the client devices.
The **IP Address Type** can be **IPv4 Only** (IPv4 traffic only), **IPv6 Only** (IPv6 traffic only), or **IPv4 and IPv6**. Use **IPv4 and IPv6** if your network supports dual-stack configurations, where IPv4 and IPv6 run at the same time.

The IP address must be compatible with the IP address type (e.g., 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6). If you choose **IPv4 and IPv6**, enter the appropriate address type for each.

The options on the **General**, **Authentication**, and **Satellite** tabs are similar between gateways and portals. **Agent** tab options, however, are different. **Agent** tab configuration options pertain to the connection between the agents and the gateway.



Use the **Tunnel Settings** tab to configure the tunnel settings that enable the app to establish a VPN tunnel with the gateway. If you are configuring an internal gateway, these settings are optional.

For gateways that require a tunnel connection, select **Tunnel Mode**:

- Select a **Tunnel Interface** from the pull-down list to attach the interface to this gateway.
- Tunnel mode defaults to SSL, but it can be configured for IPSec.
- If IPsec is not available, the gateway will default back to SSL.

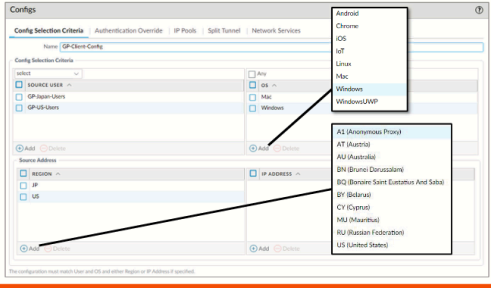
Timeout configurations can be set if the gateway is running tunnel mode. User timeouts can be specified so that inactive connections are automatically closed.

Select the **Enable X-Auth Support** option to enable Extended Authentication (X-Auth) support in the GlobalProtect Gateway when IPSec is enabled. With X-Auth support, third-party IPSec VPN clients that support X-Auth (such as the IPSec VPN client on Apple iOS and Android devices and the VPNC client on Linux) can establish a VPN tunnel with the GlobalProtect Gateway. The X-Auth option provides remote access from the VPN client to a specific GlobalProtect Gateway.

Selecting X-Auth support enables the **Group Name** and **Group Password** options. You can use the **Group Name** and **Group Password** fields instead of certificates to authenticate third-party VPN clients.

Gateway: Config Selection Criteria Tab

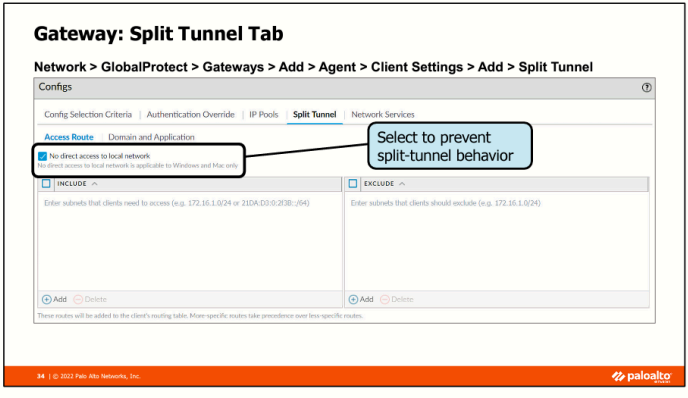
Network > GlobalProtect > Gateways > Add > Agent > Client Settings > Add > Config Selection Criteria



You can deploy tunnel configurations for multiple user locations from a single GlobalProtect Gateway. Users can receive an associated tunnel configuration that contains specific authentication overrides, IP pools, split tunnel, and DNS settings based on the location from which they are connecting.
The **Config Selection Criteria** tab indicates the criteria that users must match against when connecting to a GlobalProtect Gateway. Selection criteria can include a specific user or user group, operating system of the client workstation, country, or IP address. If a user matches all the selection criteria configured on the **Config Selection Criteria** tab, then the gateway deploys the client settings configuration to the GlobalProtect user.

A gateway configured in tunnel mode functions as a DHCP server to connected clients. IP addresses and other networking information are passed to the client for use during the VPN connection.

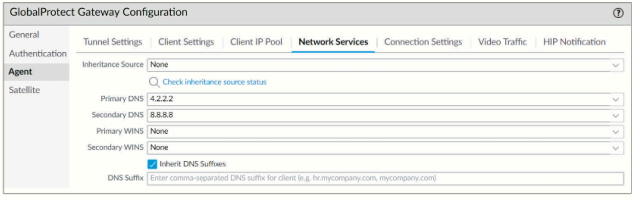
The **IP Pools** options are available only if you have enabled tunnel mode and defined a tunnel interface on the **Tunnel Settings** tab (**Network > Interfaces > Tunnel**). Add a range of IPv4 or IPv6 addresses to assign to remote users. After establishing the tunnel, the GlobalProtect Gateway allocates IP addresses in this range to all endpoints that connect through that tunnel.



If you do not include or exclude routes, every request is routed through the VPN tunnel (without a split tunnel). You can include or exclude specific destination IP subnet traffic from being sent over the VPN tunnel. The routes that you send through the VPN tunnel can be defined as the routes you include in the tunnel, routes that you exclude from the tunnel, or both. To configure split tunneling to ensure that all traffic (including local subnet traffic) goes through the VPN tunnel for inspection and policy enforcement, select the **No direct access to local network** option.

Gateway: Enable Network Services

Network > GlobalProtect > Gateways > Add > Agent > Network Services



The **Network Services** tab enables you to configure DNS settings that are assigned to the virtual network adapter on the client system when the GlobalProtect app establishes a tunnel with the gateway.

In the **Inheritance Source** field, select a source to propagate the DNS server and other settings from the selected DHCP client or PPPoE client interface into the GlobalProtect app's configuration. With this setting, all client network configuration, such as DNS servers and WINS servers, will be inherited from the configuration of the interface selected in the **Inheritance Source** field.

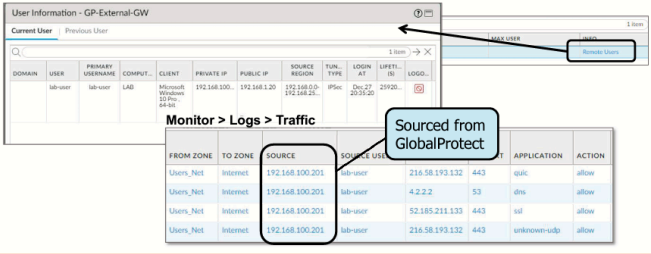
Click the **Check inheritance source status** link to display the server settings that are currently assigned to the client interfaces.

Note: Options in the **Network Services** tab are available only if you have enabled tunnel mode and defined a tunnel interface on the **Tunnel Settings** tab.

GlobalProtect and User-ID

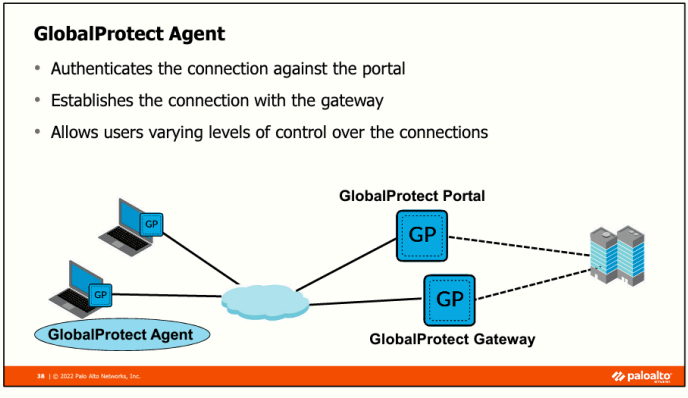
GlobalProtect can be used as a source of user mapping for User-ID technology

Network > GlobalProtect > Gateways > Remote Users (info)

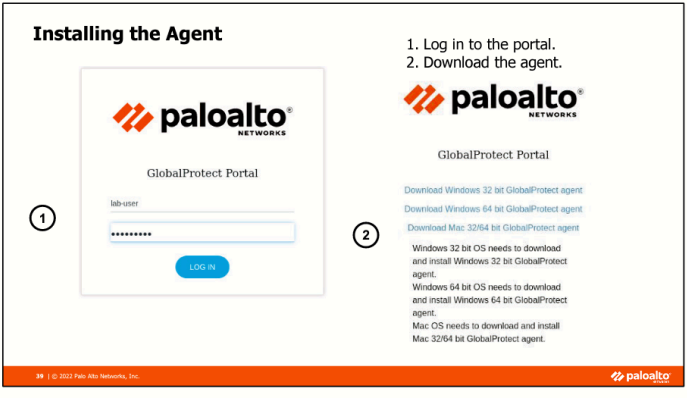


For mobile or roaming users, the GlobalProtect agent provides user mapping information to the firewall directly. In this case, every GlobalProtect user has an agent or app running that requires the user to enter login credentials for VPN access to the firewall. This login information then is added to the User-ID user mapping table on the firewall for visibility and user-based Security policy enforcement. Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. This solution is best in sensitive environments where you must be certain that only specific users are allowed access to an application or service.

This section provides an overview of configuring GlobalProtect agents.



The GlobalProtect agent software runs on end user systems. After a GlobalProtect user connects to the portal and is authenticated by the portal, the portal sends the agent configuration to the app, based on the settings you define. If you have different roles for users or groups that need specific configurations, you can create a separate agent configuration for each user type or user group. The portal uses the operating system of the endpoint and the username or group name to determine which agent configuration to deploy. The software is available both in agent form (for Windows and macOS systems) and in app form (for mobile devices).

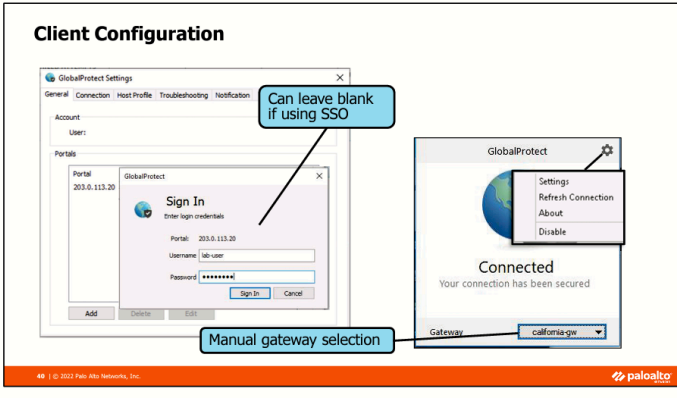


The GlobalProtect agent must be installed before a connection can be established.

Users can download the software manually by opening an SSL connection to the portal and authenticating with a username and password. After the user is authenticated, the user is prompted to download the agent software and must choose the appropriate version for their platform.

After the agent is installed, the user might have to configure the client software, depending on how the GlobalProtect administrator has configured the environment. End users can be granted varying levels of control over their local agents. The agent needs at least the FQDN or the IP address of the portal to initiate the connection process. If GlobalProtect is not configured for SSO, a username and password also are needed.

For mobile devices that cannot use the standard agent (such as an iPad), GlobalProtect supports the use of selected third-party VPN clients on a mobile device.



As the GlobalProtect administrator, you can make GlobalProtect completely transparent to end users, which restricts them from control over their connection. The interfaces shown in this section will vary based on the specific permissions granted to the users when the portal is configured.

Devices that require manual configuration must supply their login information in the **General** tab of the agent.

The username and password must match the Authentication Profile set on the portal. If the session is configured for SSO, the **Username** and **Password** fields can be left blank.

After the login information is set, the user can connect to GlobalProtect by right-clicking the icon in the system tray or launching **GlobalProtect Client**. Only actions that users are permitted to run will be displayed to them.

By default, the agent automatically discovers gateways. Gateways can be marked as **manual** to enable users to establish a connection with specific gateways. Any rediscovery event reverts the agent to Auto Discovery mode.

This section provides an overview of monitoring GlobalProtect connections.

GlobalProtect Log

- Starting with PAN-OS 9.1, GlobalProtect now has its own log:
  - GlobalProtect log entries also are integrated into the Unified log.

Monitor > Logs > GlobalProtect

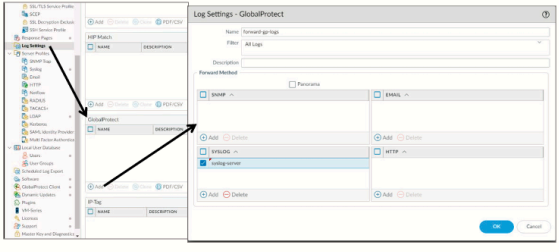
RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	REGION	HOST NAME	PUBLIC IPV4	PUBLIC IPV6
12/27 20:45:27	GP-External-GW	success	login	gateway-register	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 20:45:37	GP-External-GW	success	login	gateway-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 20:45:37	GP-Portal	success	login	portal-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 20:35:20	GP-External-GW	success	login	gateway-register	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 20:35:20	GP-External-GW	success	login	gateway-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 20:35:19	GP-Portal	success	login	portal-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 00:39:11	GP-External-GW	success	login	gateway-register	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 00:39:11	GP-External-GW	success	login	gateway-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 00:38:55	GP-Portal	success	login	portal-auth	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0
12/27 00:37:42	GP-External-GW	success	login	gateway-register	lab-user	192.168.0.0-192.168.255.255	LAB	192.168.1.20	0:0:0:0

Starting with PAN-OS 9.1, GlobalProtect log entries no longer are written to the firewall's System log.
GlobalProtect log entries now are written to a separate GlobalProtect log.
The portal and gateway firewalls maintain information about the connections in the GlobalProtect log. Any interaction between the client and the other components will be logged on the device that handles the interaction.
Use this new log location to monitor or troubleshoot GlobalProtect operation.
GlobalProtect log entries also are added to the Unified log.

GlobalProtect Log Forwarding

GlobalProtect log entries can be forwarded to an external log service.

Device > Log Settings

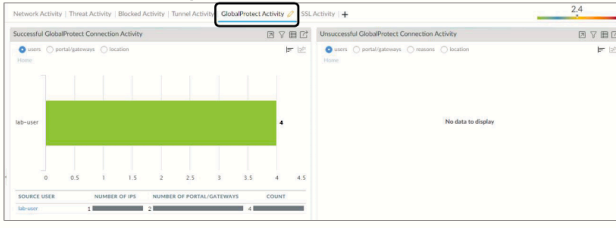


Because there is a separate GlobalProtect log starting with PAN-0S 9.1, the log forwarding configuration page at **Device > Log Settings** also has been updated to include the option to forward GlobalProtect log entries to an external log destination. Here, we show that **GlobalProtect** log entries will be forwarded to an external syslog service.

GlobalProtect Activity in the ACC

Visualize successful and unsuccessful GlobalProtect connection information

ACC > GlobalProtect Activity



Starting with PAN-OS 9.1, GlobalProtect also has a new **GlobalProtect Activity** tab on the ACC. This new tab displays an overview of user activity in your GlobalProtect deployment. Information includes the number of users, the number of times each user connected, the gateways to which each user connected, the number of connection failures with a failure reason, a summary of authentication methods and GlobalProtect app versions used, and the number of endpoints that are quarantined.

Use the **Successful GlobalProtect Connection Activity** widget to view and visualize successful user attempts to connect to your GlobalProtect deployment. You can view which users have connected to which portals and gateways, and in which locations.

To visualize and help troubleshoot any unsuccessful user connection attempts, use the **Unsuccessful GlobalProtect Connection Activity** widget. You can view which users have not been able to connect to which portals and gateways, and in which locations. Notice that this widget includes a **reasons** filter that enables you to see why a user could not connect to GlobalProtect.

Use the **GlobalProtect Deployment Activity** widget to view and visualize GlobalProtect deployment information. You can view how many users are using different authentication methods (such as LDAP), how many clients are using which GlobalProtect app version, or how many clients are using which operating systems.

The ACC also features a **GlobalProtect Quarantine Activity** widget to view a summary of devices that have been quarantined. You can use the toggle at the top of the chart to view the quarantined devices by the actions that caused GlobalProtect to quarantine the device, the reason GlobalProtect quarantined the device, and the location of the quarantined devices.

Module Summary

Now that you have completed this module, you should be able to:

- Describe the three major components of GlobalProtect
- Configure the client and server certificates to authenticate the agent and the portal
- Configure a GlobalProtect Portal
- Configure a GlobalProtect internal and external gateway
- Configure a GlobalProtect client

Now that you have completed this module, you should be able to perform the tasks listed.

Review Questions

1. Which operation is used by a GlobalProtect client to determine whether it should connect to an internal or external gateway?
    a. reverse DNS lookup
    b. user selection during agent startup
    c. IP address of the client system
    d. GlobalProtect agent starting in online or offline mode
2. The GlobalProtect agent is available in which two formats? (Choose two.)
    a. dmg
    b. exe
    c. msi
    d. pkg
3. True or false? If a GlobalProtect agent fails to establish an IPsec connection, the connection type will fall back to SSL-VPN.
    a. true
    b. false
4. Which GlobalProtect component provides the management functions for the GlobalProtect infrastructure?
    a. agent
    b. internal gateway
    c. external gateway
    d. portal
5. In which GlobalProtect user connection method must users explicitly connect to GlobalProtect?
    a. user-logon (always on)
    b. pre-logon (always on)
    c. on-demand
    d. pre-logon, then on-demand

Answers to Review Questions

1. a
2. c, d
3. a (true)
4. d
5. c