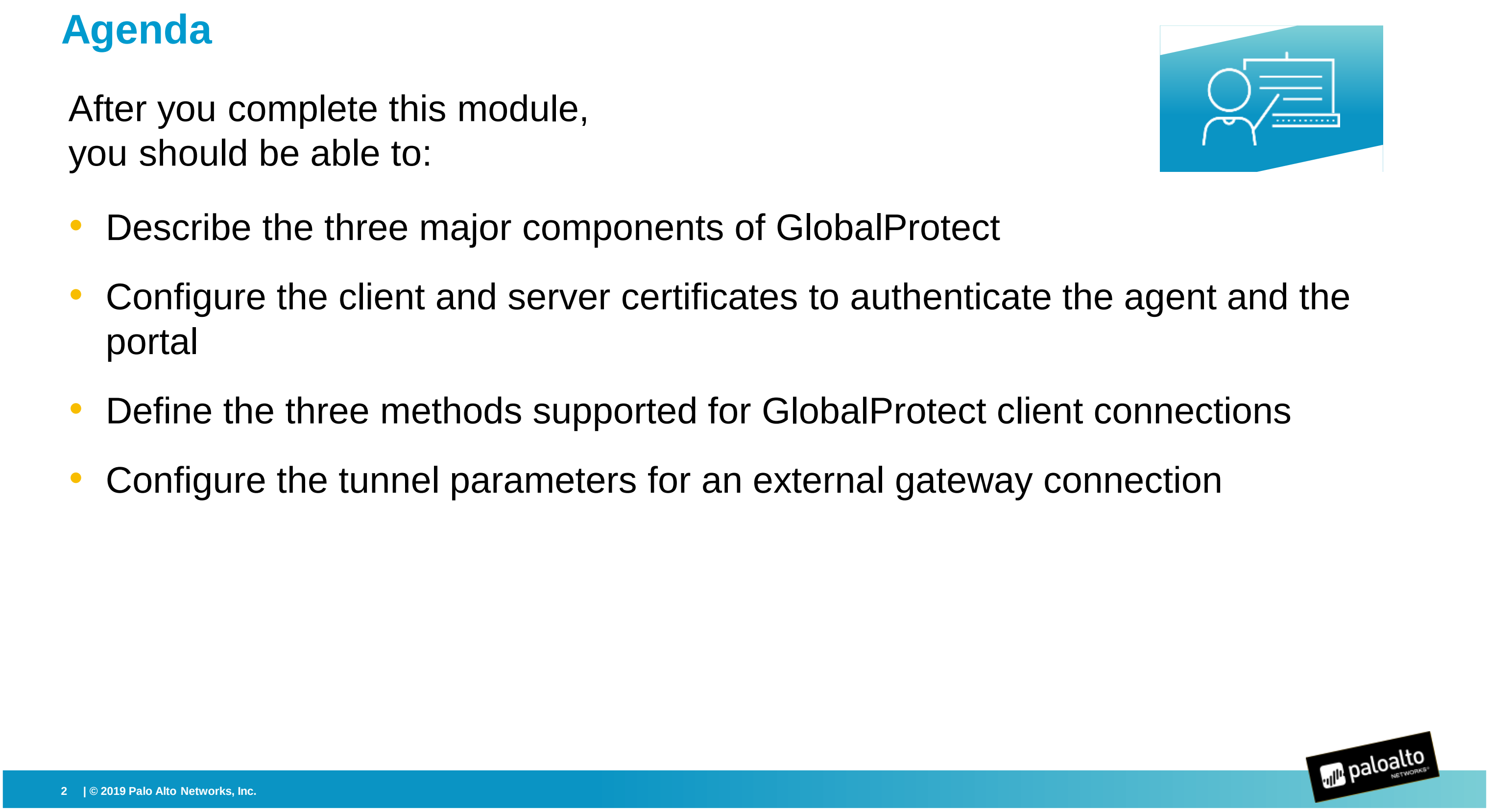
GLOBALPROTECT

GP

EDU-210 Version A
PAN-OS® 9.0

EXTEND PREVENTION TO REMOTE USERS

- GlobalProtect overview
- Preparing the firewall for GlobalProtect
- Configuration: GlobalProtect portal
- Configuration: GlobalProtect gateway
- Configuration: GlobalProtect agents



Agenda

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
- Define the three methods supported for GlobalProtect client connections
- Configure the tunnel parameters for an external gateway connection

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
- Define the three methods supported for GlobalProtect client connections
- Configure the tunnel parameters for an external gateway connection

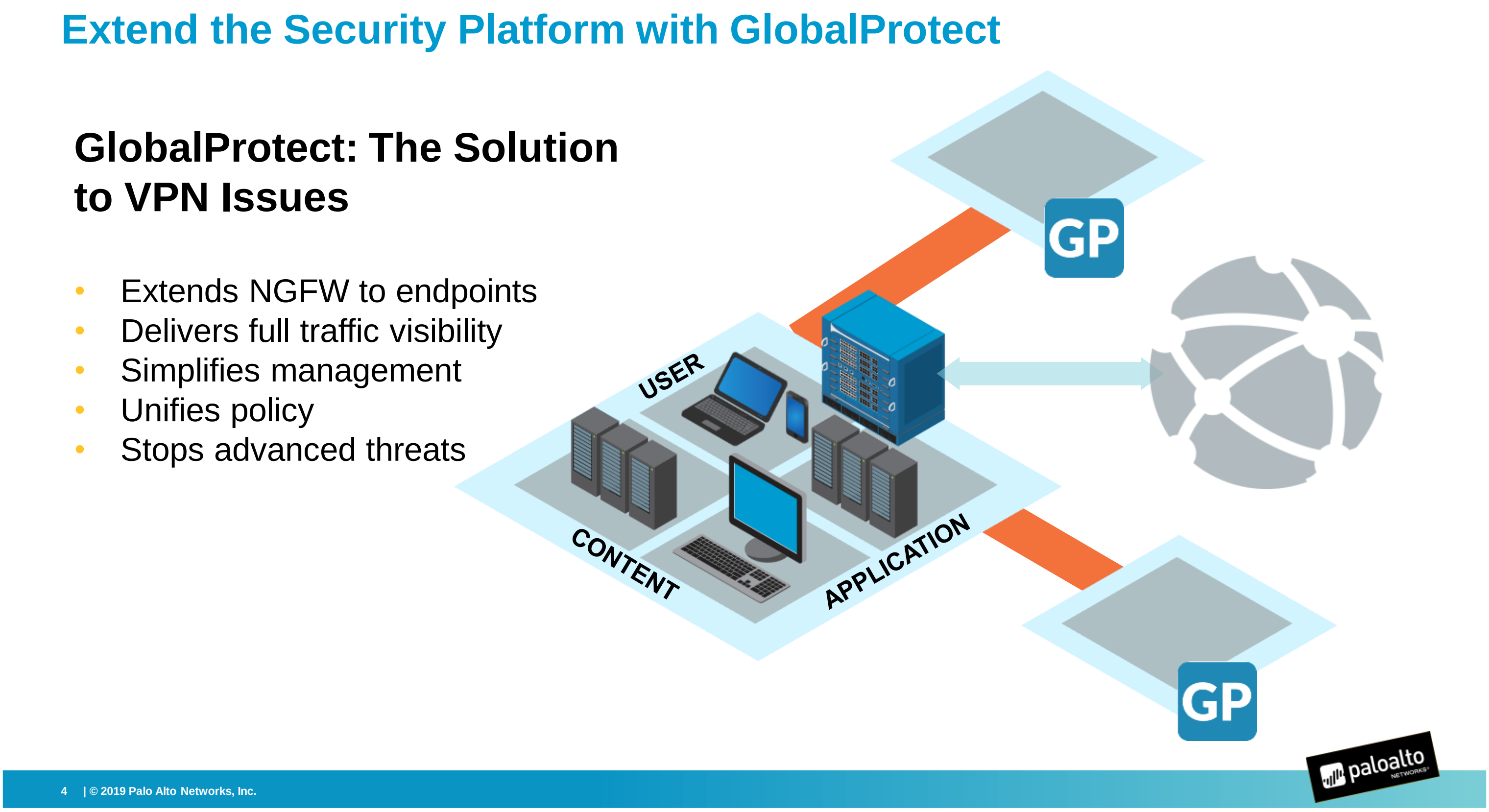
GlobalProtect overview

Preparing the firewall for GlobalProtect

Configuration: GlobalProtect portal

Configuration: GlobalProtect gateway

Configuration: GlobalProtect agents



Extend the Security Platform with GlobalProtect

GlobalProtect: The Solution to VPN Issues

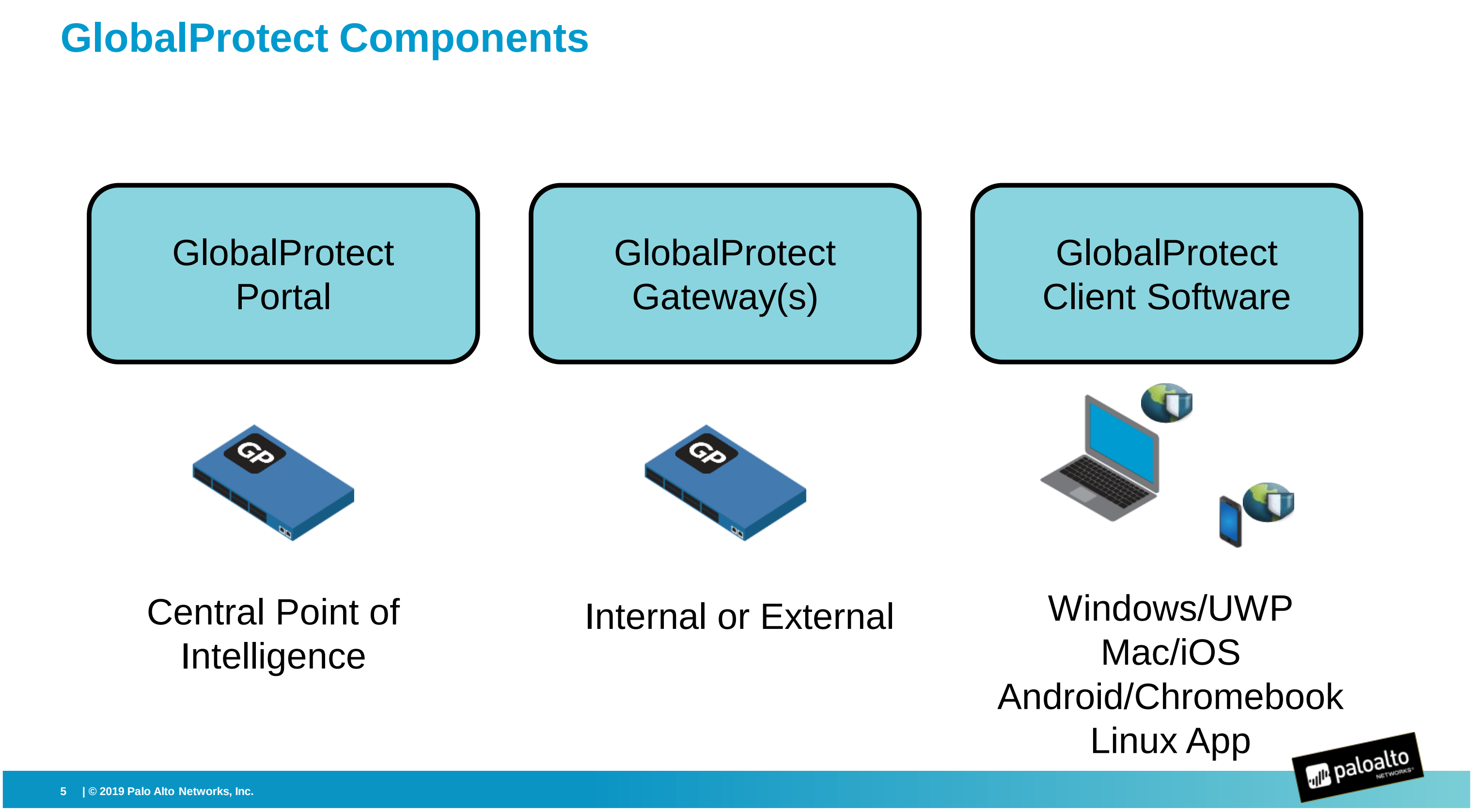
- Extends NGFW to endpoints
- Delivers full traffic visibility
- Simplifies management
- Unifies policy
- Stops advanced threats

4 | © 2019 Palo Alto Networks, Inc.

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. Laptop and mobile devices stay connected to the corporate network at all times, and are protected as if they never left the corporate campus.

GlobalProtect ensures that the same secure application enablement policies that protect users at the corporate site are enforced for all users, independent of their location. 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.



GlobalProtect Components

GlobalProtect Portal

GlobalProtect Gateway(s)

GlobalProtect Client Software

Central Point of Intelligence

Internal or External

Windows/UWP
Mac/iOS
Android/Chromebook
Linux App

5 | © 2019 Palo Alto Networks, Inc.

GlobalProtect deployment has three major components:

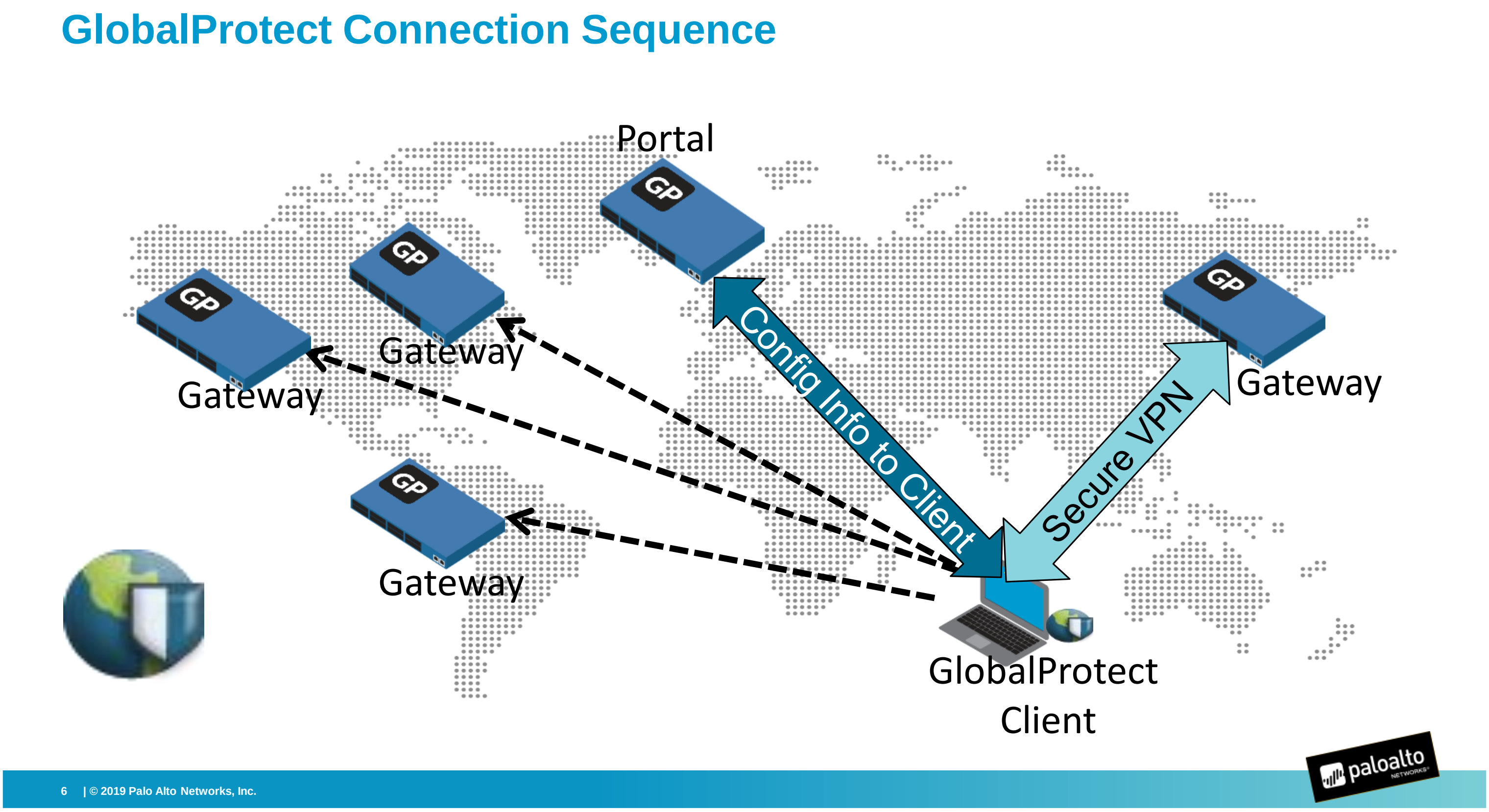
- **GlobalProtect Portal**: Provides the management functions for your GlobalProtect infrastructure. Every client connecting to the GlobalProtect network receives configuration information from the portal.
- **GlobalProtect Gateways**: Provide security enforcement for traffic from GlobalProtect agents and apps:
  - External gateways provide security enforcement and VPN access for remote users.
  - Internal gateways apply Security policy for access to internal resources.
- **GlobalProtect client software**: Runs on end-user systems and enables access to network resources via the deployed GlobalProtect portals and gateways.

The installer will be in .MSI (Windows) or .PKG (Mac) format.

GlobalProtect also has install agents for Android, Chromebook devices, iOS, and Universal Windows Platform, or UWP. The iOS version is available through the Apple App Store. The Android version is available through Google Play.

The GlobalProtect app for Linux extends User-ID and Security policy enforcement to users on Linux endpoints. The Linux app provides a command line interface and functions as an SSL or IPsec VPN client. It supports common GlobalProtect features and authentication methods, including client certificate authentication, server certificate validation, authentication cookies, and two-factor authentication.

The GlobalProtect app for Linux is available for installation using .deb, .rpm, or .tar packages and can be installed on CentOS 7.0 and later, Red Hat Enterprise 7.0 and later, or Ubuntu 14.04 and later.



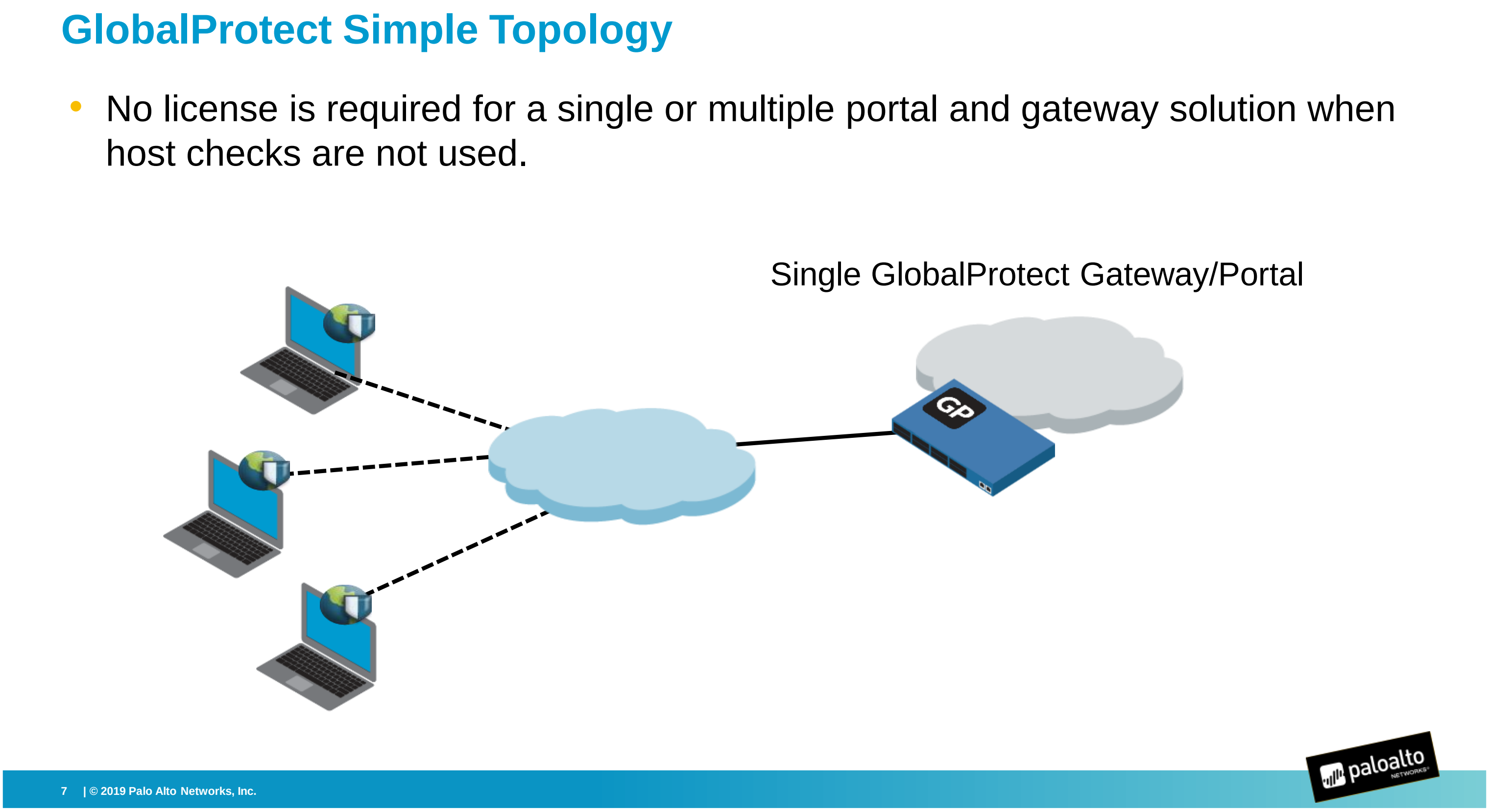
GlobalProtect Connection Sequence

6 | © 2019 Palo Alto Networks, Inc.

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 configurations 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, it contacts the portal when setting up a connection. Any time the client contacts the portal, the portal authenticates the connections.



GlobalProtect Simple Topology

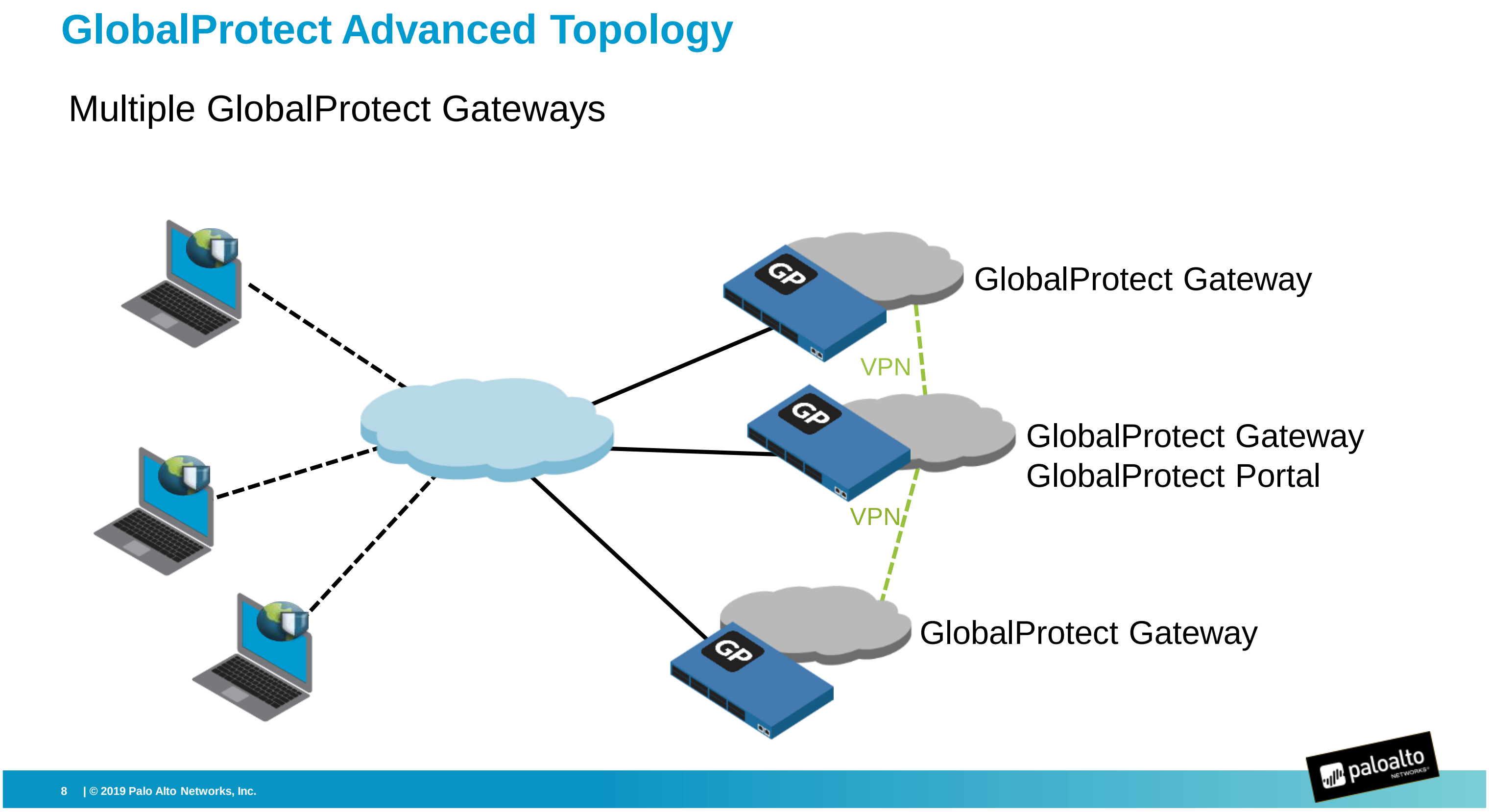
- No license is required for a single or multiple portal and gateway solution when host checks are not used.

Single GlobalProtect Gateway/Portal

7 | © 2019 Palo Alto Networks, Inc.

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.



GlobalProtect Advanced Topology

Multiple GlobalProtect Gateways

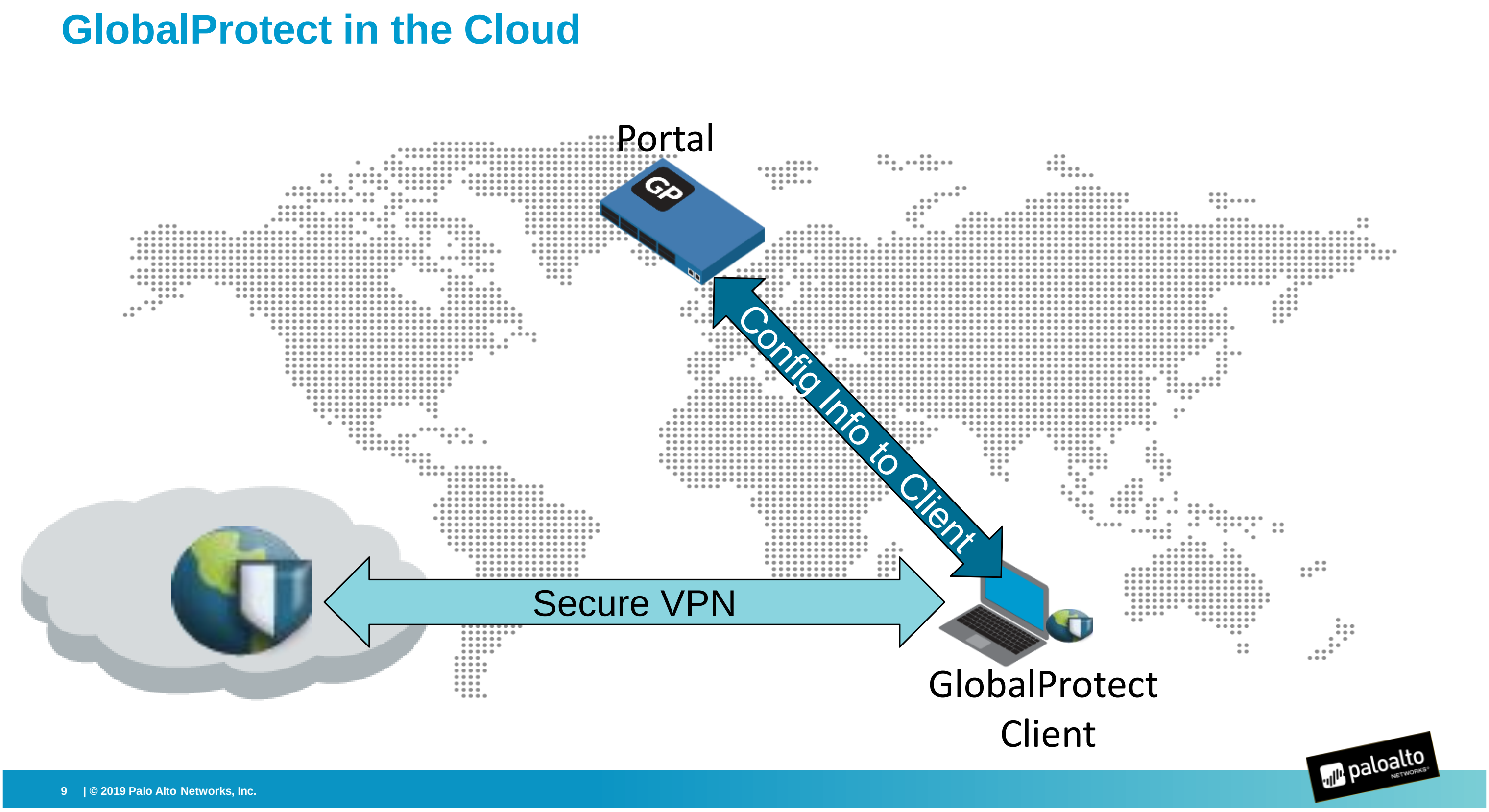
8 | © 2019 Palo Alto Networks, Inc.

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 always 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.

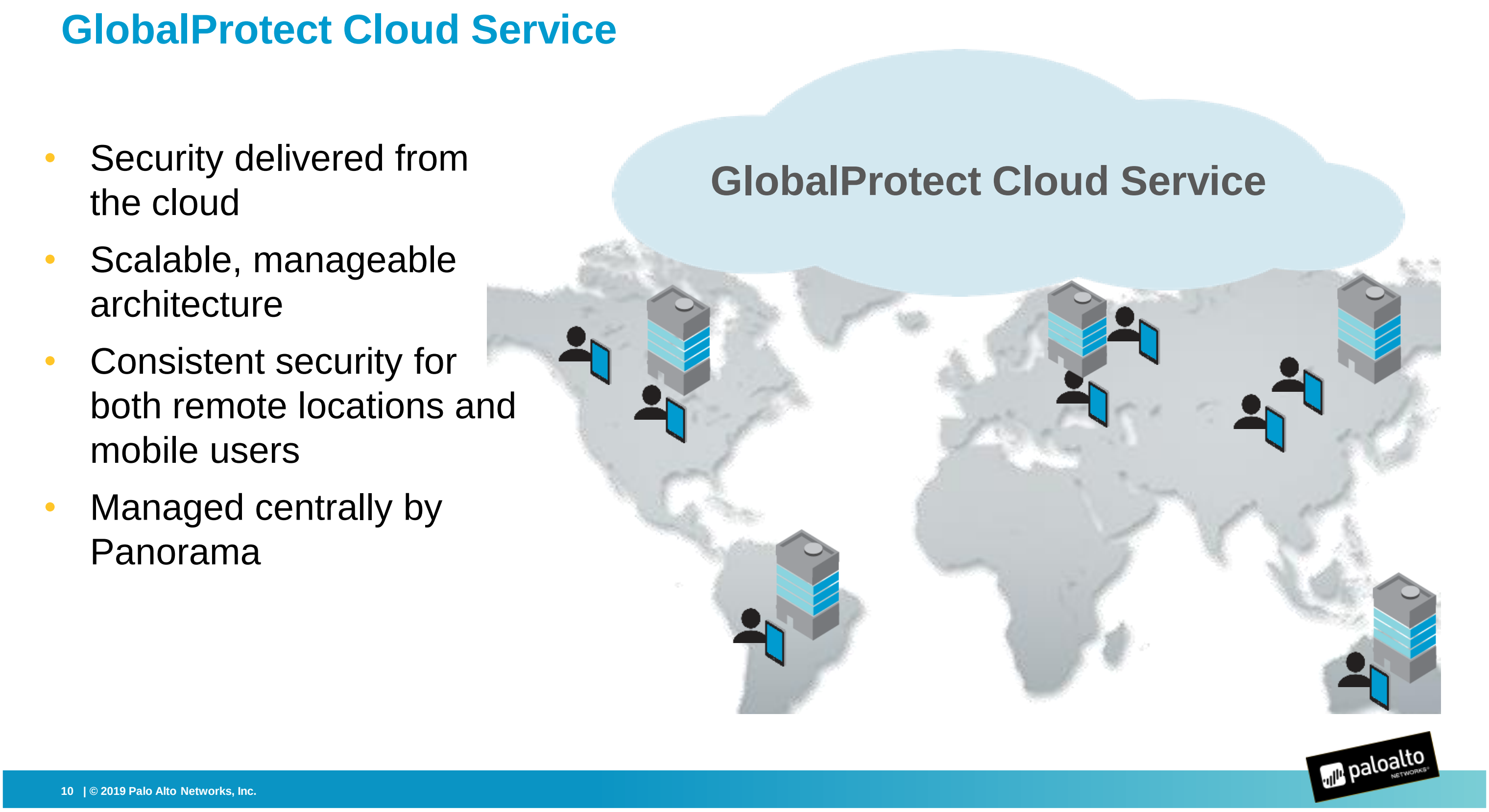
The only limitation of this scenario is a down portal, in which case you cannot install a new client, nor can configuration changes be distributed to existing clients. To resolve this issue, either re-establish connection to the portal or redirect clients to a standby portal configured on another firewall. The redirection can be executed by a change in the DNS record of the portal.



GlobalProtect in the Cloud

9 | © 2019 Palo Alto Networks, Inc.

The scalability and global presence of the AWS computing infrastructure, combined with the VM-Series firewalls and GlobalProtect mobile security, enable you to extend your corporate Security policy to your remote users and mobile devices, regardless of their location. GlobalProtect establishes a secure connection to protect the user from internet threats and enforces application-based access control policies. The platform provides full protection, regardless of whether the user or network needs access to the internet, data center, or SaaS applications.



GlobalProtect Cloud Service

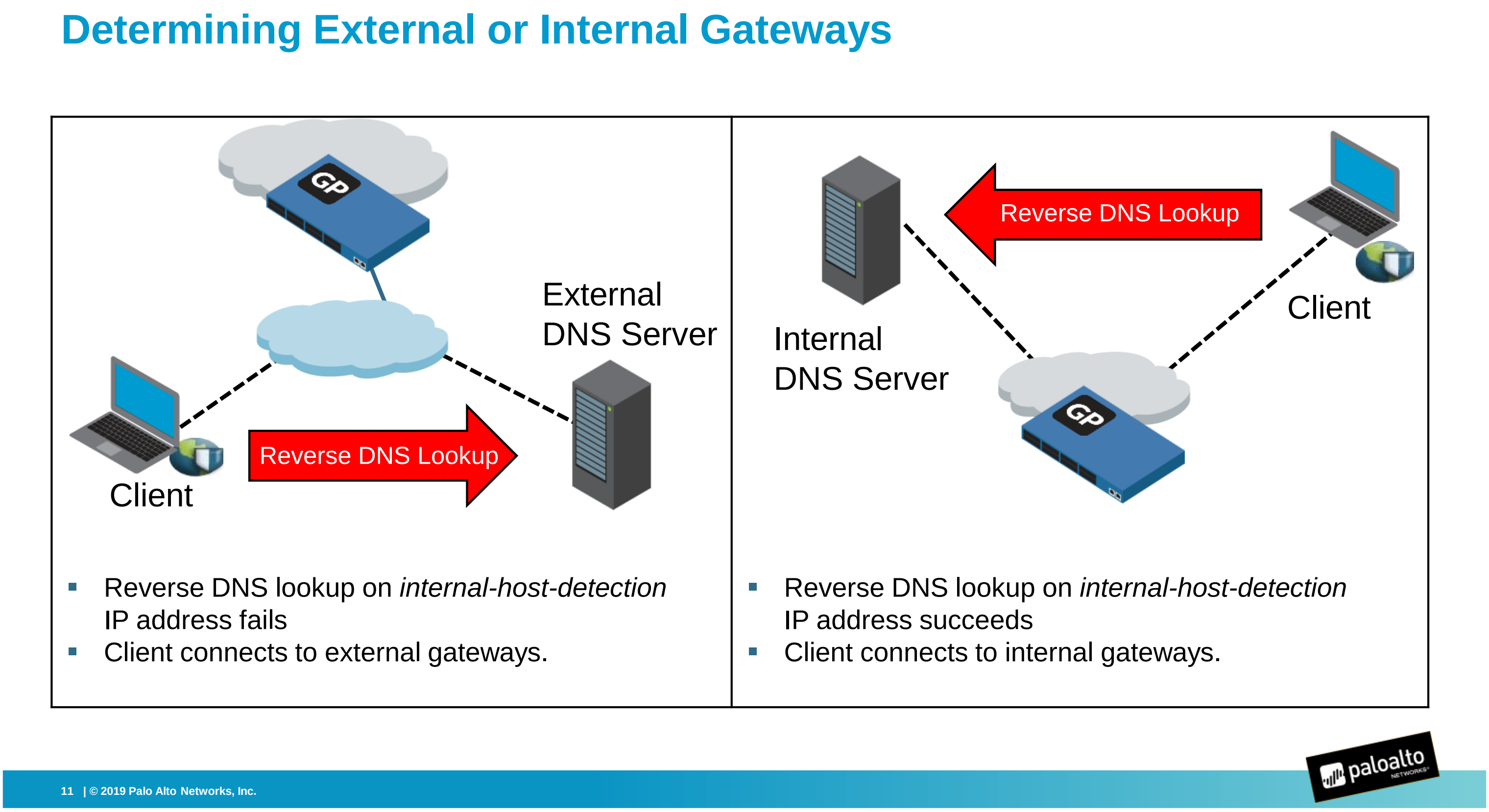
- Security delivered from the cloud
- Scalable, manageable architecture
- Consistent security for both remote locations and mobile users
- Managed centrally by Panorama

GlobalProtect Cloud Service

10 | © 2019 Palo Alto Networks, Inc.

GlobalProtect cloud service reduces the burden associated with securing your remote networks and mobile users by leveraging a cloud-based security infrastructure managed by Palo Alto Networks. GlobalProtect cloud service is security delivered from the cloud. It provides you with a scalable and manageable architecture. Administrators centrally manage GlobalProtect cloud services using Panorama to onboard sites, manage policies, and query logs for monitoring and reporting capabilities.

GlobalProtect cloud service enables you to automatically scale your services based on the growth of your headquarters, remote networks, and mobile users. Subscriptions for Threat Prevention, URL Filtering, and WildFire® are included. AutoFocus contextual threat intelligence and Aperture SaaS security can be deployed to complement GlobalProtect cloud service.



Determining External or Internal Gateways

External DNS Server

Client

Reverse DNS Lookup

- Reverse DNS lookup on *internal-host-detection* IP address fails
- Client connects to external gateways.

Internal DNS Server

Client

Reverse DNS Lookup

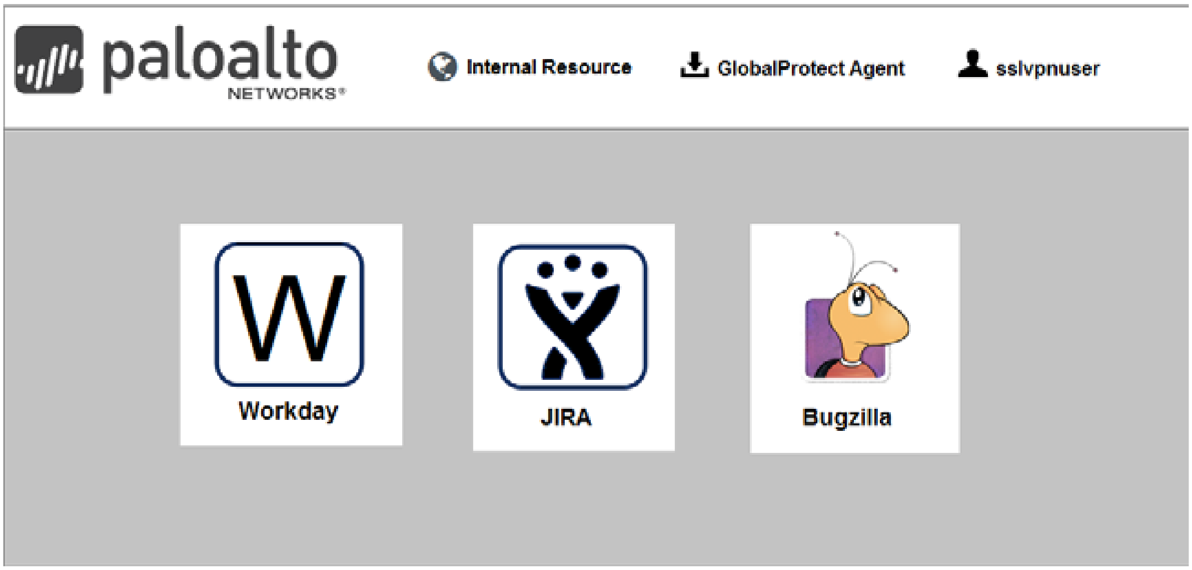
- Reverse DNS lookup on *internal-host-detection* IP address succeeds
- Client connects to internal gateways.

11 | © 2019 Palo Alto Networks, Inc.

The portal may provide an IP address and DNS hostname as part of the information passed to the client to determine whether the host is inside or outside the corporate network:

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

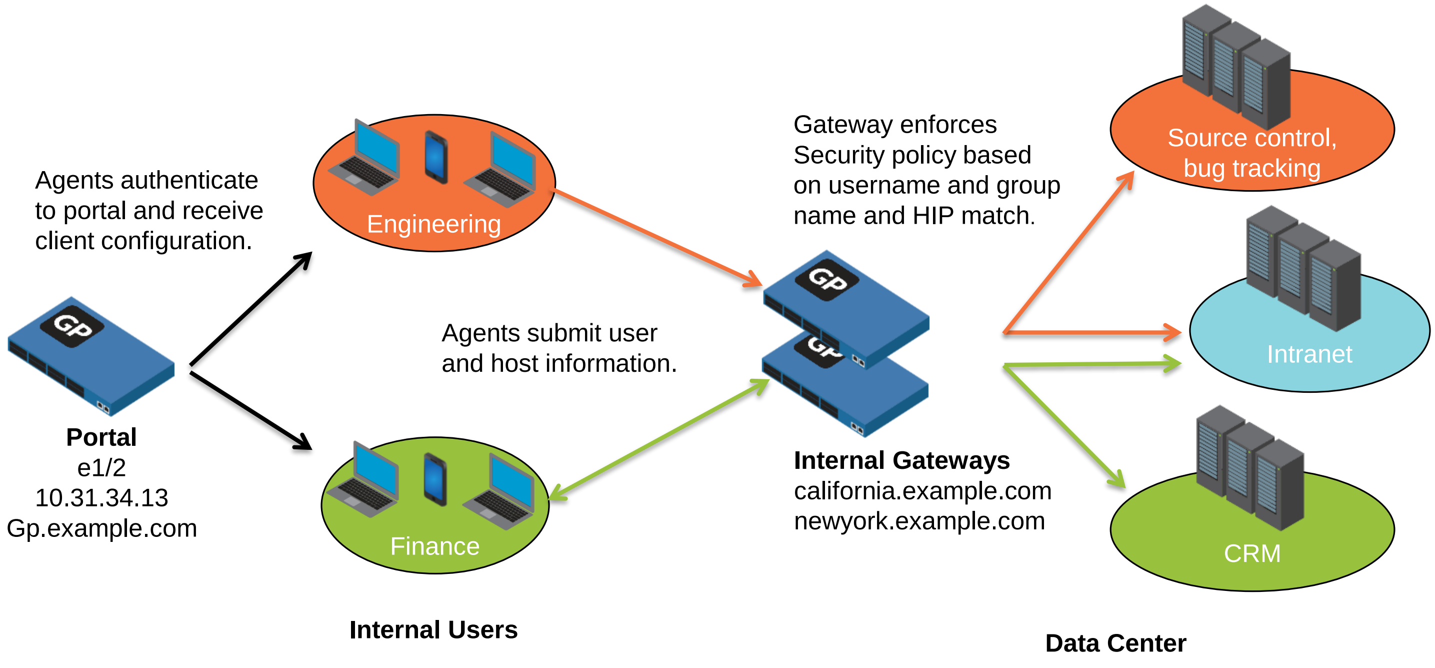
Clientless VPN



GlobalProtect clientless VPN provides secure remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies. Your remote users have the advantage of secure access from SSL-enabled web browsers without installing the GlobalProtect client software. Remote users can log in to the GlobalProtect portal using a web browser and launch the web applications you publish for the user. Based on users or user groups, you can allow users to access a set of applications that you make available to them, or allow them to access additional corporate applications. The remote user who logs in to the portal will see a published applications page with a list of web applications they can launch.

When you configure GlobalProtect clientless VPN, you need to configure Security policies to allow traffic from GlobalProtect clients to the security zone associated with the GlobalProtect portal that hosts the published applications landing page. Security policies also will need to be configured to allow user-based traffic from the GlobalProtect portal zone to the security zone where the published application servers are hosted. The Security policies you define control which users have permission to use each published application.

GlobalProtect for Internal User-Based Access



Agents authenticate to portal and receive client configuration.

Agents submit user and host information.

Gateway enforces Security policy based on username and group name and HIP match.

Portal
e1/2
10.31.34.13
Gp.example.com

Internal Gateways
california.example.com
newyork.example.com

Internal Users

Data Center

An internal gateway that is used in conjunction with User-ID technology can be used to provide a secure, accurate method of identifying and controlling traffic by user. 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 databases, and 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.

GlobalProtect overview

Preparing the firewall for GlobalProtect

Configuration: GlobalProtect portal

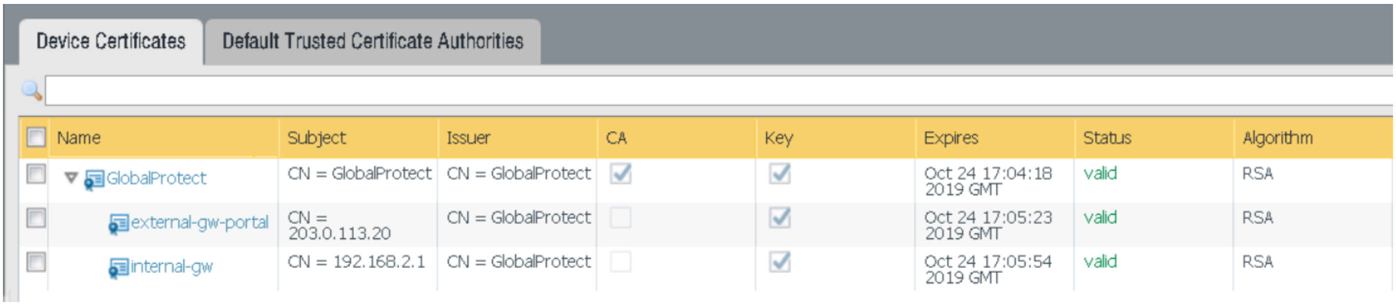
Configuration: GlobalProtect gateway

Configuration: GlobalProtect agents

GlobalProtect Certificates

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

Device > Certificate Management > Certificates



□	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm
□	GlobalProtect	CN = GlobalProtect	CN = GlobalProtect	☑	☑	Oct 24 17:04:18 2019 GMT	valid	RSA
□	external-gw-portal	CN = 203.0.113.20	CN = GlobalProtect	□	☑	Oct 24 17:05:23 2019 GMT	valid	RSA
□	internal-gw	CN = 192.168.2.1	CN = GlobalProtect	□	☑	Oct 24 17:05:54 2019 GMT	valid	RSA

Connectivity between all parts of the GlobalProtect infrastructure is authenticated using SSL certificates. The portal can act as a 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. The gateway also verifies that the client has a client certificate signed by the appropriate CA.

If third parties who may 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.

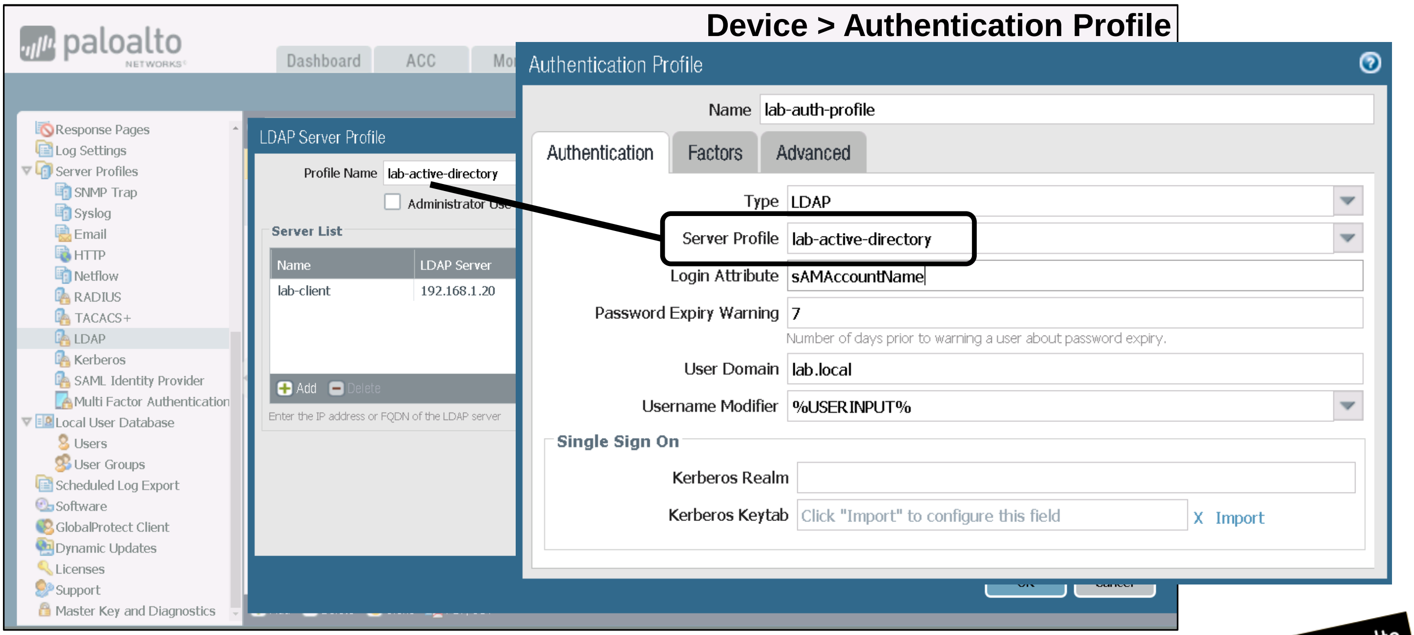
The portal includes the public certificate of the CA and the needed client certificate and key as part of the configuration bundle that is sent to the client. GlobalProtect gateways use the client certificate to authenticate and identify the client.

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 along with a server certificate and key for the portals and gateways, and with a client certificate and key for the clients.

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

Authentication Server Profile Example

Device > Server Profiles > LDAP > Add



Device > Authentication Profile

LDAP Server Profile

Profile Name: lab-active-directory

☐ Administrator Use

Server List

Name	LDAP Server
lab-client	192.168.1.20

Add Delete

Enter the IP address or FQDN of the LDAP server

Authentication Profile

Name: lab-auth-profile

Authentication | Factors | Advanced

Type: LDAP

Server Profile: lab-active-directory

Login Attribute: sAMAccountName

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain: lab.local

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field X Import

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

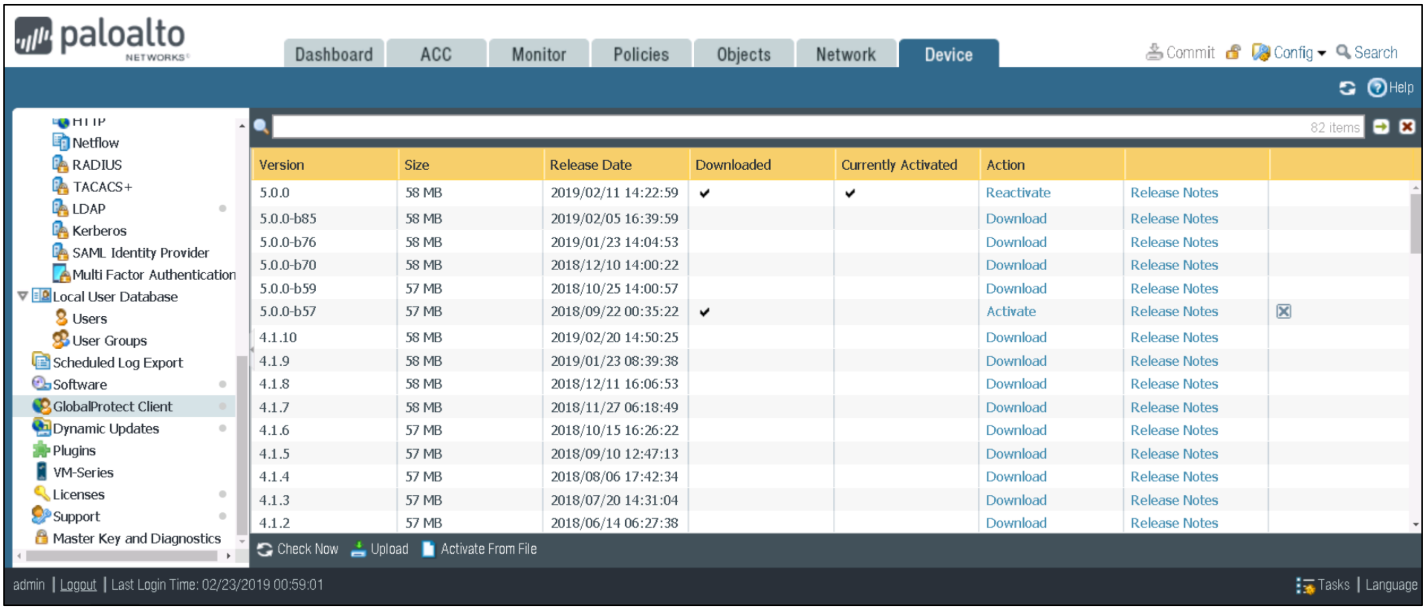
1. Create the Authentication Server Profile. The example uses an LDAP configuration.
2. Attach to an Authentication Profile.

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

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

Agent Software on the Portal

Device > GlobalProtect Client



Version	Size	Release Date	Downloaded	Currently Activated	Action		
5.0.0	58 MB	2019/02/11 14:22:59	✓	✓	Reactivate	Release Notes	
5.0.0-b85	58 MB	2019/02/05 16:39:59			Download	Release Notes	
5.0.0-b76	58 MB	2019/01/23 14:04:53			Download	Release Notes	
5.0.0-b70	58 MB	2018/12/10 14:00:22			Download	Release Notes	
5.0.0-b59	57 MB	2018/10/25 14:00:57			Download	Release Notes	
5.0.0-b57	57 MB	2018/09/22 00:35:22	✓		Activate	Release Notes	☒
4.1.10	58 MB	2019/02/20 14:50:25			Download	Release Notes	
4.1.9	58 MB	2019/01/23 08:39:38			Download	Release Notes	
4.1.8	58 MB	2018/12/11 16:06:53			Download	Release Notes	
4.1.7	58 MB	2018/11/27 06:18:49			Download	Release Notes	
4.1.6	57 MB	2018/10/15 16:26:22			Download	Release Notes	
4.1.5	57 MB	2018/09/10 12:47:13			Download	Release Notes	
4.1.4	57 MB	2018/08/06 17:42:34			Download	Release Notes	
4.1.3	57 MB	2018/07/20 14:31:04			Download	Release Notes	
4.1.2	57 MB	2018/06/14 06:27:38			Download	Release Notes	

admin | Logout | Last Login Time: 02/23/2019 00:59:01

The GlobalProtect client page lists the available GlobalProtect releases. 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.

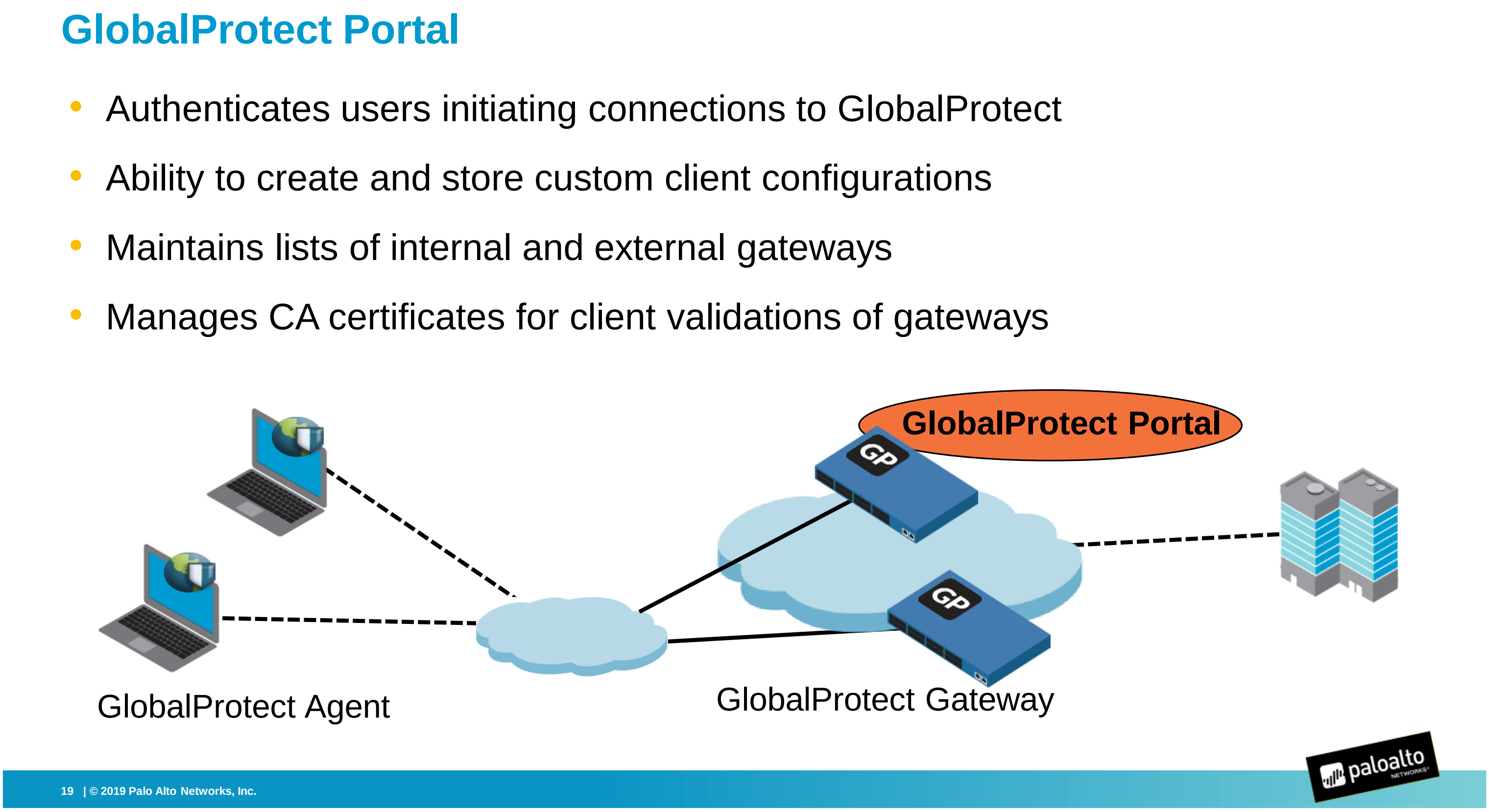
GlobalProtect overview

Preparing the firewall for GlobalProtect

Configuration: GlobalProtect portal

Configuration: GlobalProtect gateway

Configuration: GlobalProtect agents



GlobalProtect Portal

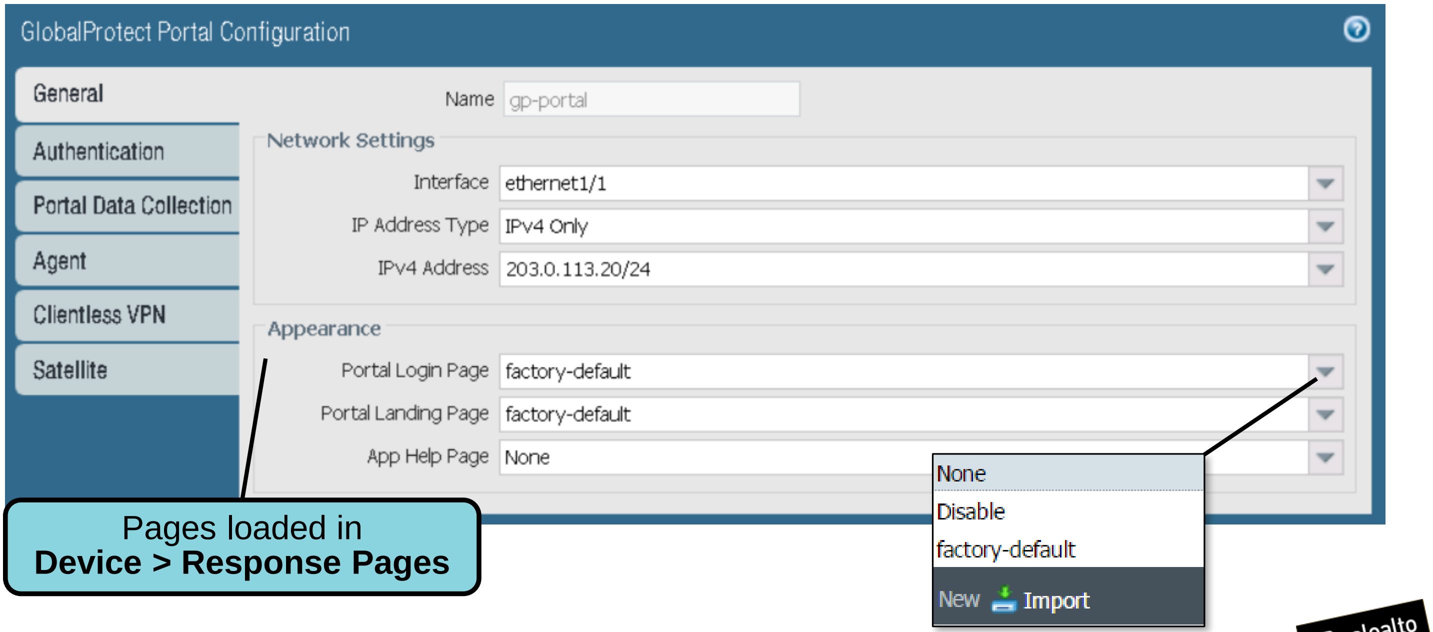
- Authenticates users initiating connections to GlobalProtect
- Ability to create and store custom client configurations
- Maintains lists of internal and external gateways
- Manages CA certificates for client validations of gateways

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.

Portal Configuration

Network > GlobalProtect > Portals > General



GlobalProtect Portal Configuration

Name: gp-portal

Network Settings

- Interface: ethernet1/1
- IP Address Type: IPv4 Only
- IPv4 Address: 203.0.113.20/24

Appearance

- Portal Login Page: factory-default
- Portal Landing Page: factory-default
- App Help Page: None

Pages loaded in **Device > Response Pages**

The **Portal Configuration** window manages the way that the portal itself is configured. A Layer 3-capable interface is needed to host the portal functionality.

Any environment that requires customized login and help pages for GlobalProtect can be configured in **Device** > **Response Pages**.

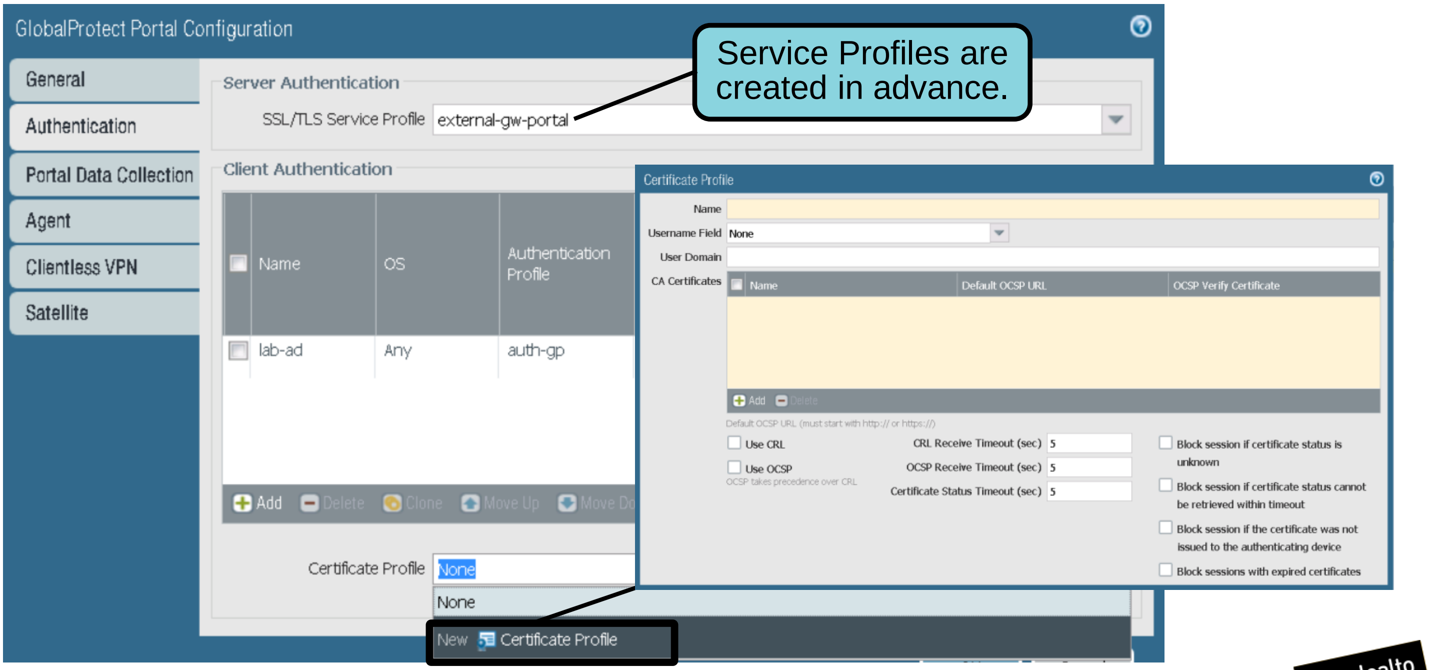
When you configure a GlobalProtect Portal, you can disable access to the portal login page from a web browser. This action prevents public access to the portal login page and unauthorized attempts to authenticate to the GlobalProtect Portal from a browser. Enablement of this option does not affect access 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.

General, **Authentication**, and **Satellite** options are similar between gateways and portals. **Agent** options, however, are different. **Clientless VPN** options are available only from the portal.

The portal agent configurations pertain specifically to the agents that will be hosted on the portal.

Portal Authentication

Network > GlobalProtect > Portals > Authentication



Service Profiles are created in advance.

GlobalProtect Portal Configuration

Server Authentication

SSL/TLS Service Profile: external-gw-portal

Client Authentication

□	Name	OS	Authentication Profile
□	lab-ad	Any	auth-gp

Certificate Profile: None

Certificate Profile

Name:

Username Field: None

User Domain:

CA Certificates

□	Name	Default OCSP URL	OCSP Verify Certificate

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

□ Use CRL

□ Use OCSP

OCSP takes precedence over CRL

CRL Receive Timeout (sec): 5

OCSP Receive Timeout (sec): 5

Certificate Status Timeout (sec): 5

□ Block session if certificate status is unknown

□ Block session if certificate status cannot be retrieved within timeout

□ Block session if the certificate was not issued to the authenticating device

□ Block sessions with expired certificates

SSL/TLS Service Profile
The Authentication Profile is used to authenticate users when they first browse to the portal address to authenticate and download the GlobalProtect agent. This profile object specifies which certificates and protocols will be used in securing the GlobalProtect Portal traffic.

Certificate Profile
The client and server certificates are used to authenticate the agent and the portal, for mutual identity validation. The certificates are sent to the agent when it first connects to the portal.

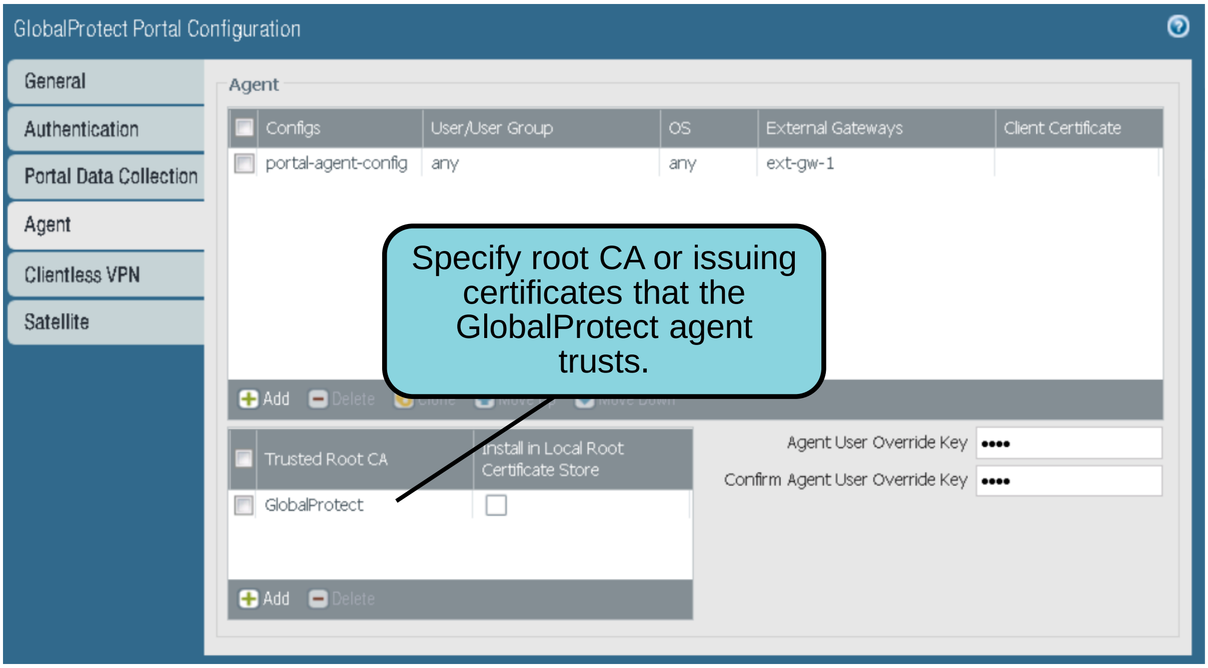
Configure connection security by selecting the appropriate certificates and Authentication Profile object.

Authentication Profile
Choose an Authentication Profile or sequence from the drop-down list to authenticate access to the gateway.

Authentication Message
This customizable message space will be presented to end users. It can be used to tell them which credentials should be used for logging in to this gateway. It can be up to 50 characters in length.

Client Configuration: Agent Certificates

Network > GlobalProtect > Portals > Agent



Agent

☐ Configs	User/User Group	OS	External Gateways	Client Certificate
☐ portal-agent-config	any	any	ext-gw-1	

☐ Trusted Root CA	Install in Local Root Certificate Store
☐ GlobalProtect	☐

Agent User Override Key ••••

Confirm Agent User Override Key ••••

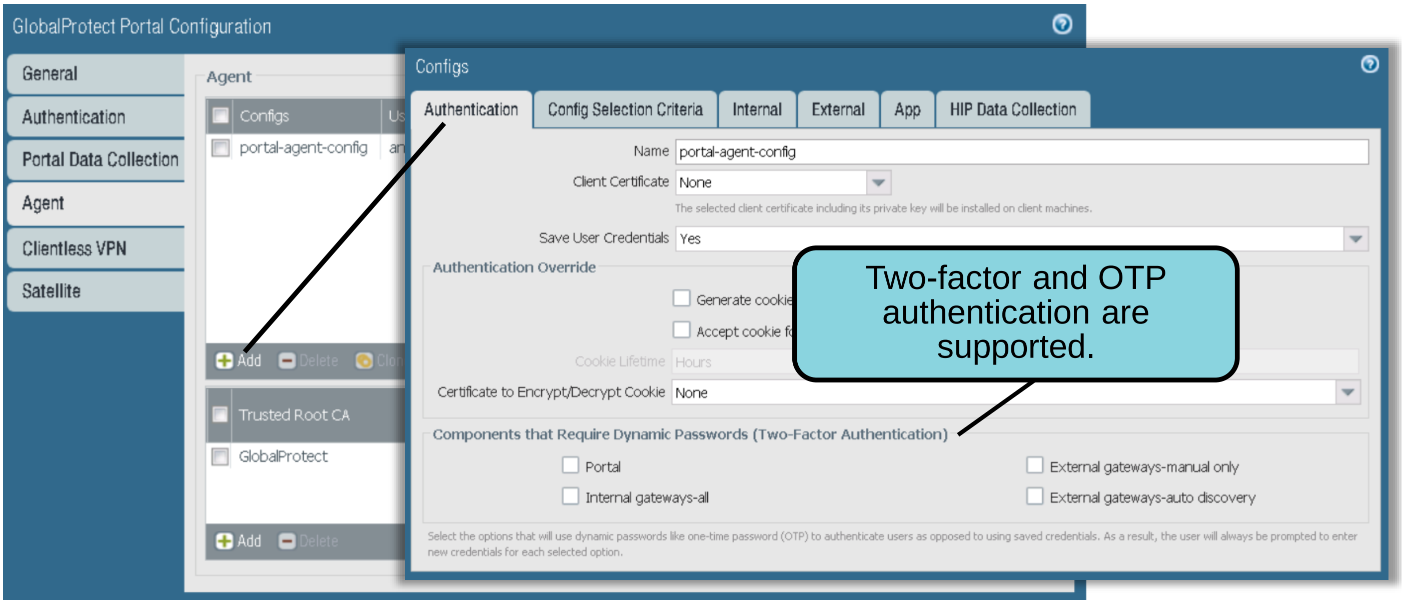
Specify root CA or issuing certificates that the GlobalProtect agent trusts.

You must specify the root CA or issuing certificates that the GlobalProtect agent will trust when connecting to a gateway.

If a gateway presents a certificate to the agent that was not issued by one of the listed CAs, the agent rejects the handshake and terminates the connection.

Client Configurations: Authentication

Network > GlobalProtect > Portals > Agent > Add (Agent)



Name: portal-agent-config

Client Certificate: None

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

Save User Credentials: Yes

Authentication Override

□ Generate cookie

□ Accept cookie f

Cookie Lifetime: Hours

Certificate to Encrypt/Decrypt Cookie: None

Components that Require Dynamic Passwords (Two-Factor Authentication)

□ Portal

□ External gateways-manual only

□ Internal gateways-all

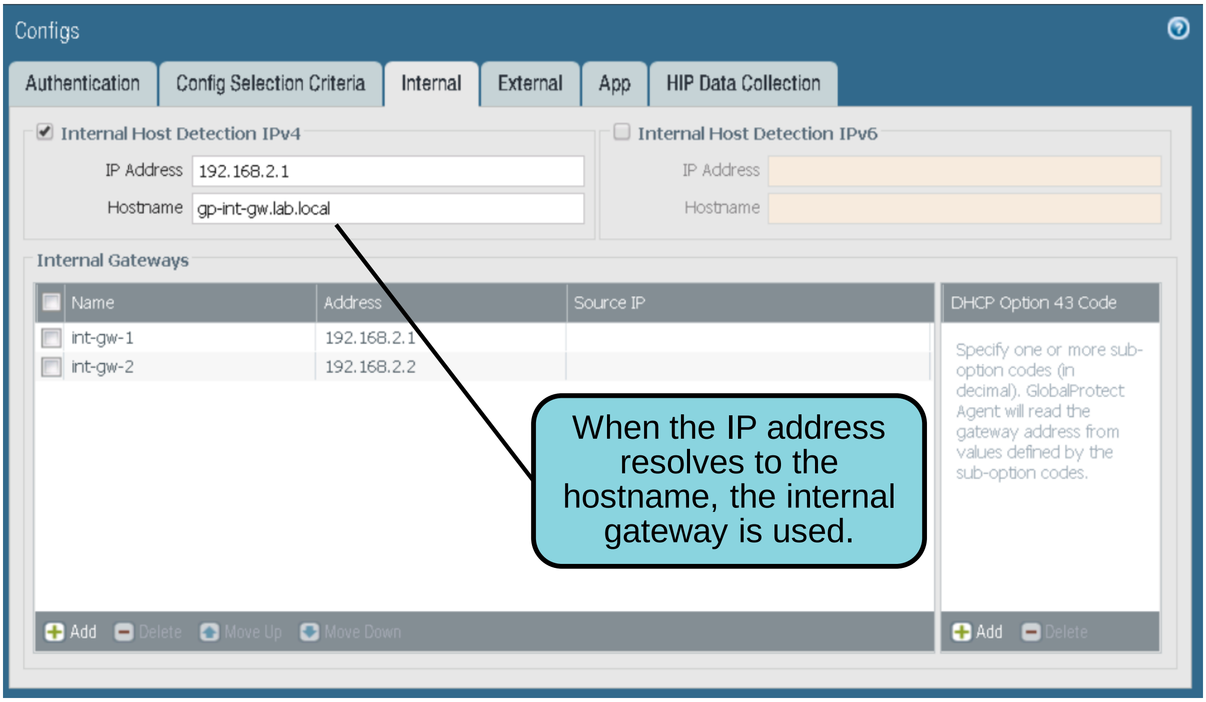
□ External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

Two-factor and OTP authentication are supported.

You can customize the 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. However, you want different behavior for the two groups of users. If some remote users are using nonstandard devices (such as iPads), additional functionality will be needed that traditional laptops do not require.

Client Configuration: Internal Gateways



☑ Internal Host Detection IPv4

IP Address: 192.168.2.1

Hostname: gp-int-gw.lab.local

☐ Internal Host Detection IPv6

IP Address:

Hostname:

Internal Gateways

☐	Name	Address	Source IP
☐	int-gw-1	192.168.2.1	
☐	int-gw-2	192.168.2.2	

DHCP Option 43 Code

Specify one or more sub-option codes (in decimal). GlobalProtect Agent will read the gateway address from values defined by the sub-option codes.

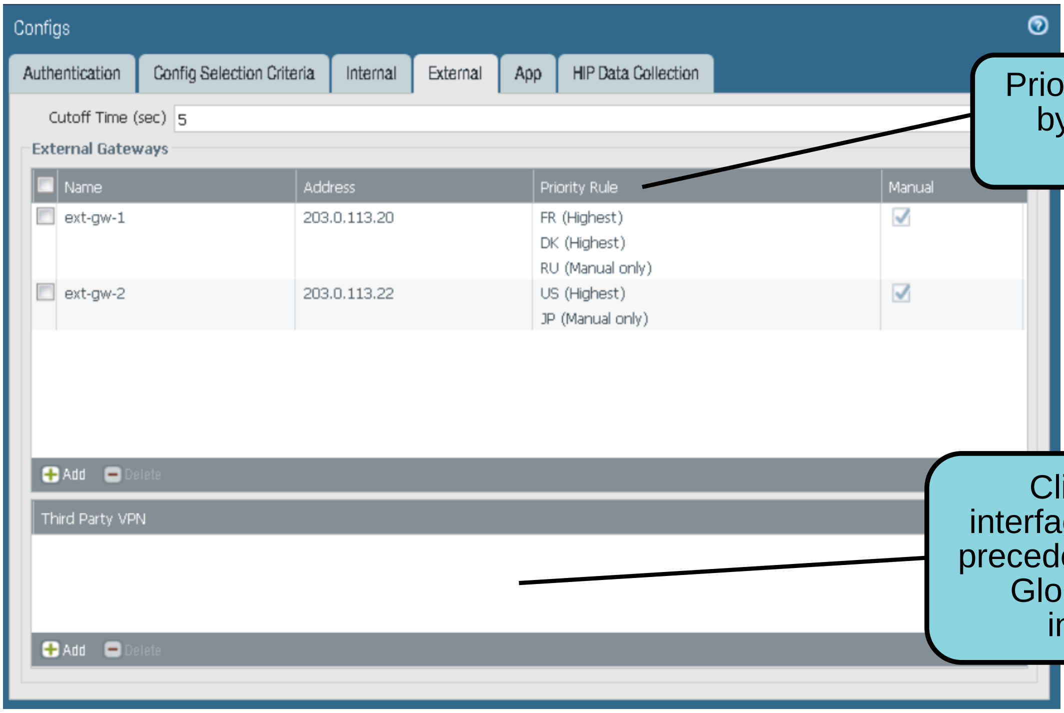
When the IP address resolves to the hostname, the internal gateway is used.

24 | © 2019 Palo Alto Networks, Inc.

The **Internal** tab stores the lists of internal gateways that are provided to clients. Clients can connect only to gateways that are defined here within the portal.

Clients authenticate and provide HIP reports to all internal gateways, which allows the HIP report information to be used by all internal gateways for policy. If the internal gateways are created with tunnel interfaces, all traffic from the client will be routed through the internal gateway that responds first.

Client Configuration: External Gateways



Cutoff Time (sec): 5

External Gateways

□	Name	Address	Priority Rule	Manual
□	ext-gw-1	203.0.113.20	FR (Highest) DK (Highest) RU (Manual only)	☑
□	ext-gw-2	203.0.113.22	US (Highest) JP (Manual only)	☑

Prioritize gateways by region or IP ranges.

Client VPN interfaces that take precedence over the GlobalProtect interface

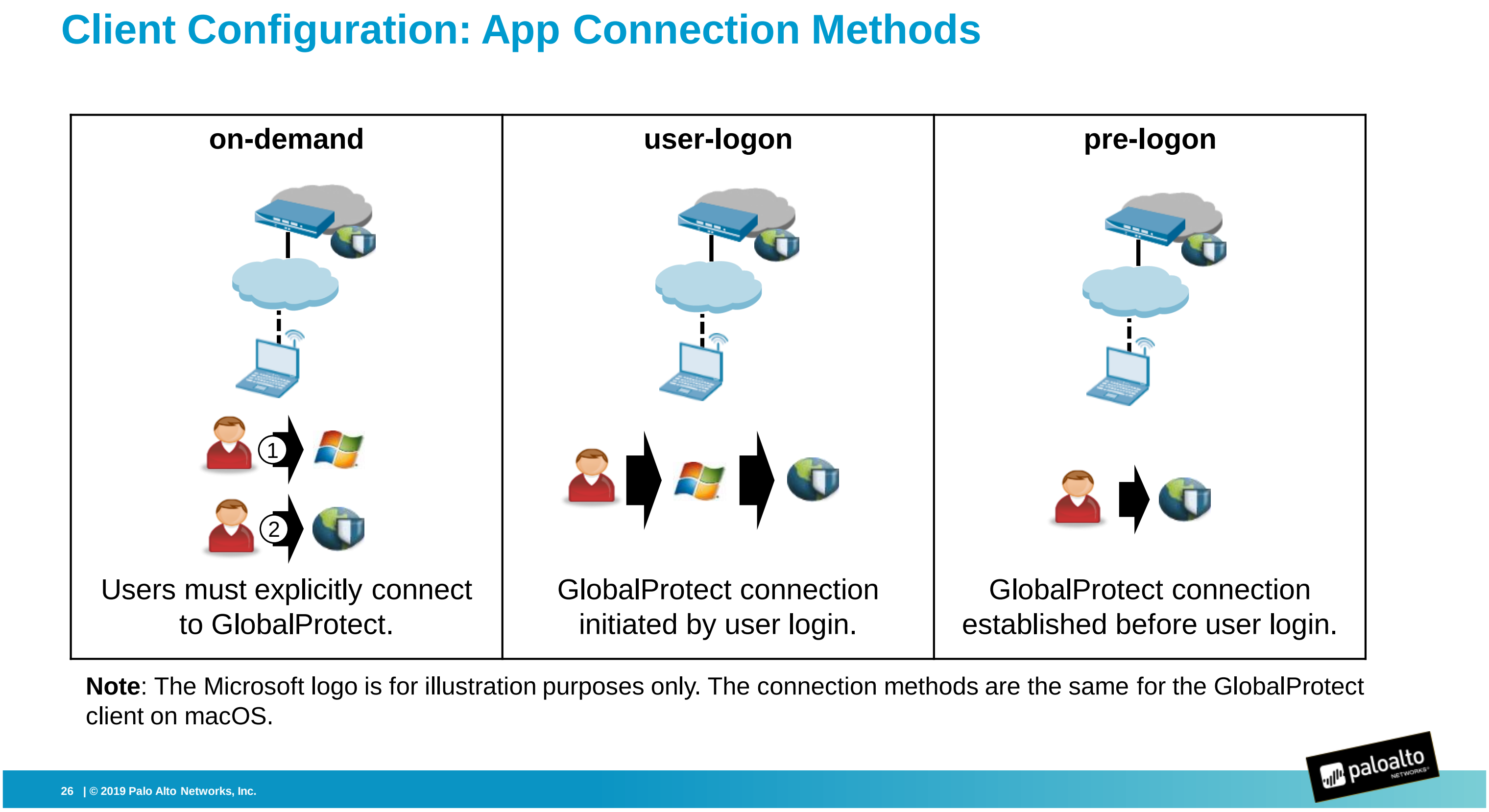
For external gateways, the client contacts all of the gateways and establishes a tunnel with the best firewall based on SSL response time and priority value. Priority can be further defined by region.

All traffic is sent through this 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 only** are not used during the automatic gateway selection process. The **Manual only** setting can be viewed in the **Priority Rule** column.

The **Third Party VPN** section allows 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. Without client VPN interfaces list, GlobalProtect may clash with routes presented by other clients.



Client Configuration: App Connection Methods

on-demand	user-logon	pre-logon
Users must explicitly connect to GlobalProtect.	GlobalProtect connection initiated by user login.	GlobalProtect connection established before user login.

Note: The Microsoft logo is for illustration purposes only. The connection methods are the same for the GlobalProtect client on macOS.

26 | © 2019 Palo Alto Networks, Inc.

GlobalProtect supports three methods for client connections:

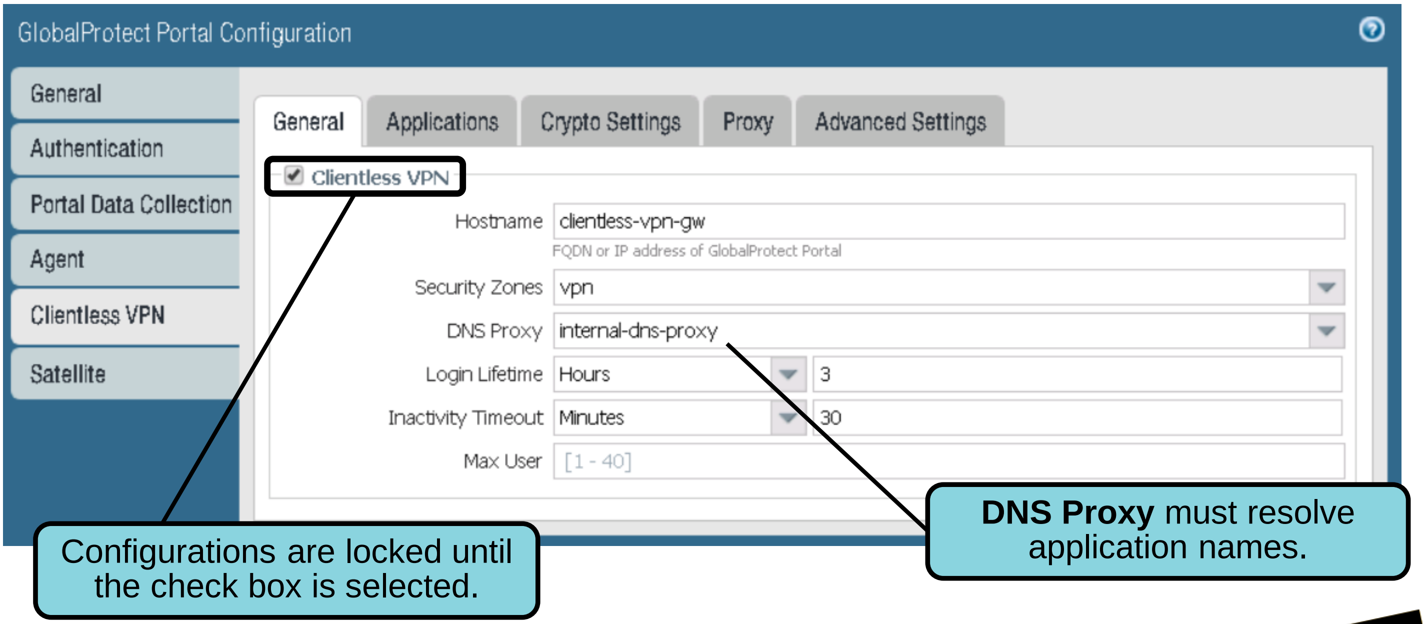
- on-demand: Allows users to establish a connection on demand. With this option, the user must explicitly initiate the connection.
- user-logon: Automatically establishes a GlobalProtect client connection after the user logs in to their computer. If the use of single sign-on, or SSO, is selected, the agent uses the Windows credentials of the user to authenticate to the GlobalProtect Portal in a process that is completely transparent to the 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: 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). The agent connection method is selected 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.

Portal Configuration: Clientless VPN

Network > GlobalProtect > Portals > Clientless VPN



☑ Clientless VPN

Hostname: clientless-vpn-gw

FQDN or IP address of GlobalProtect Portal

Security Zones: vpn

DNS Proxy: internal-dns-proxy

Login Lifetime: Hours 3

Inactivity Timeout: Minutes 30

Max User: [1 - 40]

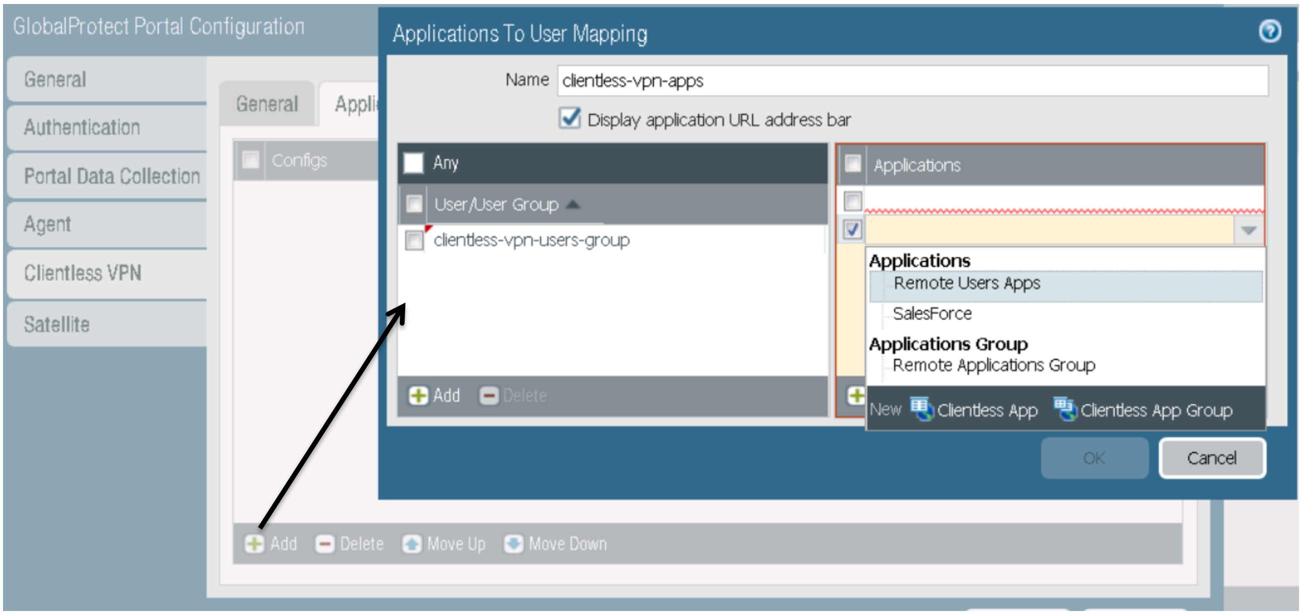
Configurations are locked until the check box is selected.

DNS Proxy must resolve application names.

When you configure clientless VPN, remote users can log in to the GlobalProtect Portal using a web browser and can 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.

Clientless VPN: Applications to User Mapping

Network > GlobalProtect > Portals > Clientless VPN > Application > Add



Applications To User Mapping

Name: clientless-vpn-apps

☑ Display application URL address bar

□ Any

User/User Group: clientless-vpn-users-group

Applications:

- Applications
  - Remote Users Apps
  - SalesForce
- Applications Group
  - Remote Applications Group

Applications can be published to users or to user groups for ease of use with clientless VPN. However, access to those application 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.

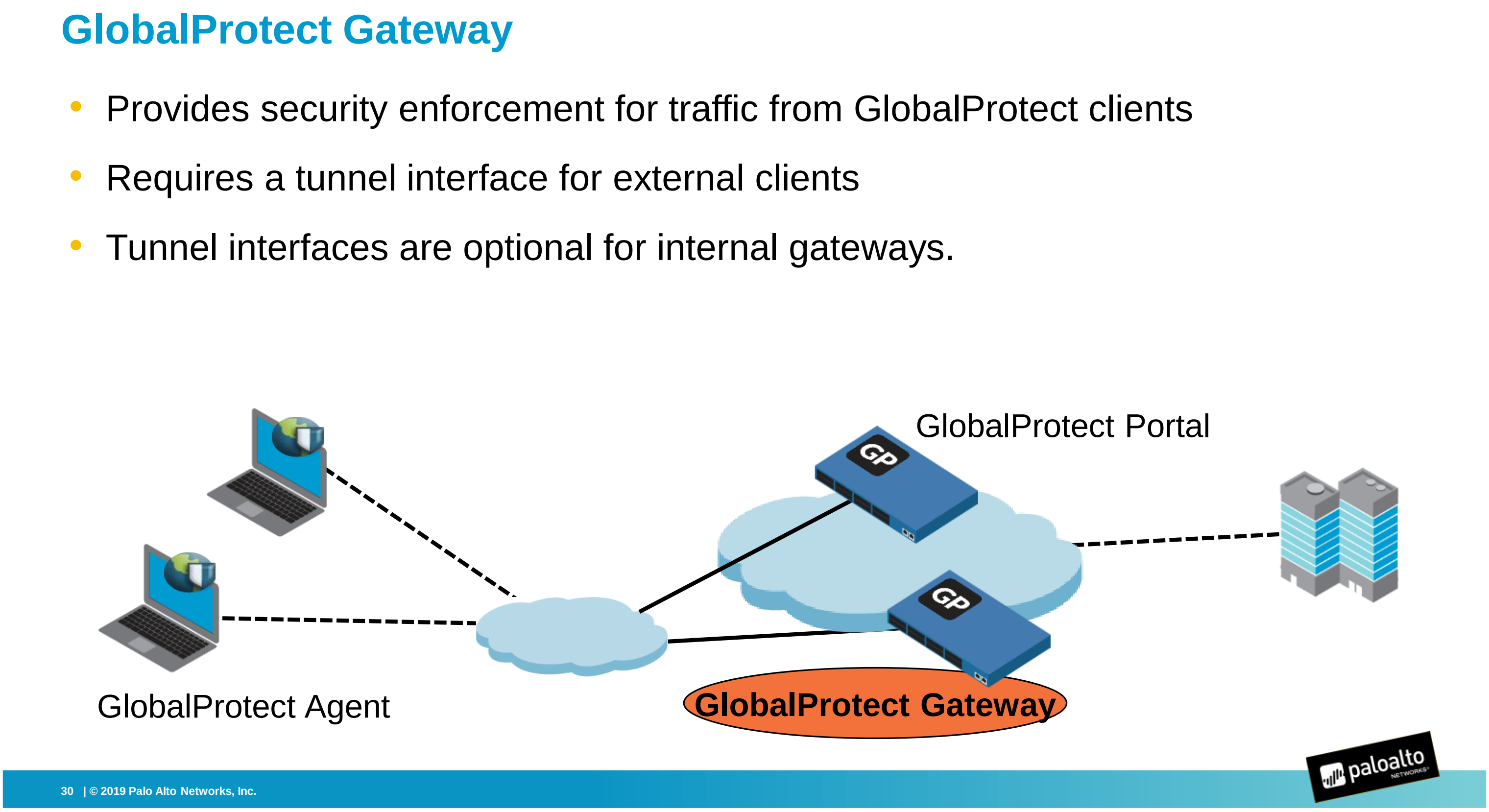
GlobalProtect overview

Preparing the firewall for GlobalProtect

Configuration: GlobalProtect portal

Configuration: GlobalProtect gateway

Configuration: GlobalProtect agents



GlobalProtect Gateway

- Provides security enforcement for traffic from GlobalProtect clients
- Requires a tunnel interface for external clients
- Tunnel interfaces are optional for internal gateways.

30 | © 2019 Palo Alto Networks, Inc.

The GlobalProtect gateway provides the endpoint for the agent’s connection.

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

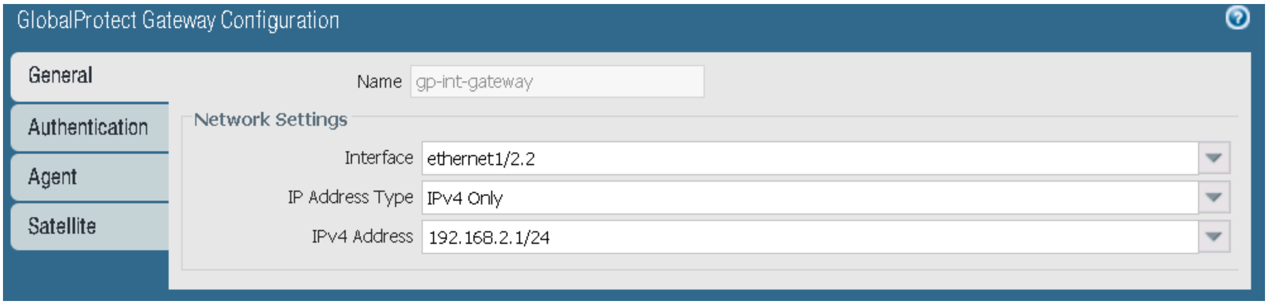
- External gateways require a tunnel.
- Internal gateways do not require a tunnel, but can be configured to use one.

Gateways support split tunneling, though this feature is not recommended for extending the firewall policy with application control and visibility to all mobile users. Gateways enforce the policy that is based on the HIP Profiles that are received.

Gateway: General Tab

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

Network > GlobalProtect > Gateways > Add > General



GlobalProtect Gateway Configuration

Name gp-int-gateway

Network Settings

Interface ethernet1/2.2

IP Address Type IPv4 Only

IPv4 Address 192.168.2.1/24

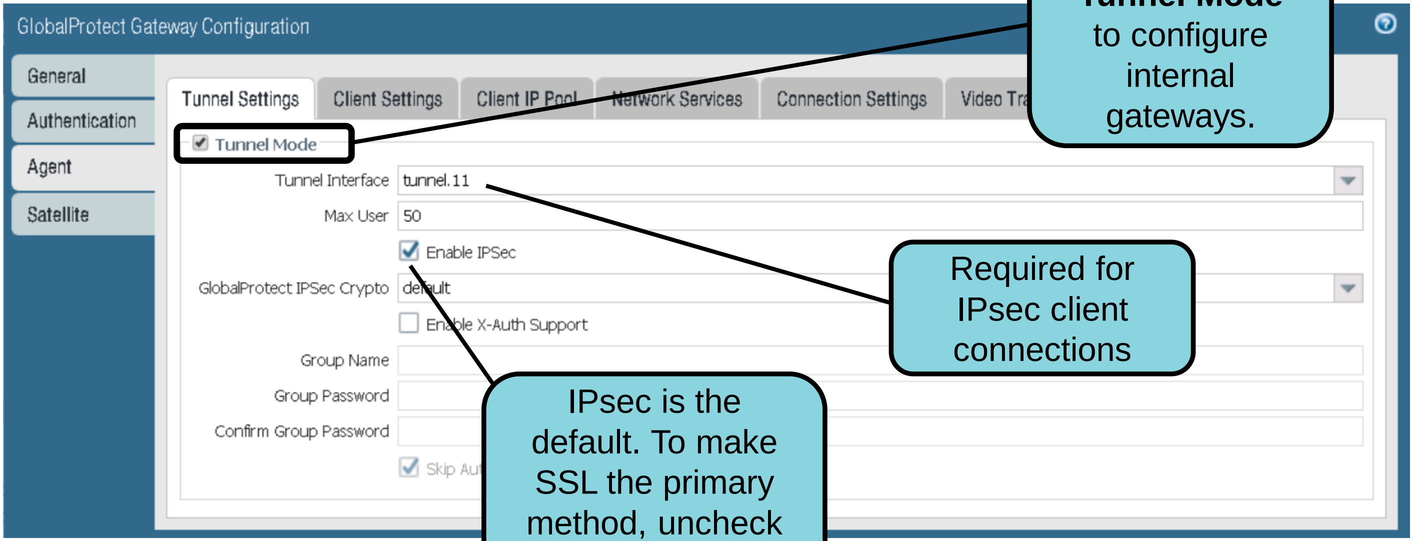
Select the Layer 3-capable interface on the firewall that is visible to the client devices. The **IPv4 Address** field will accept only an IP address and netmask assigned to the selected interface.

General, **Authentication**, and **Satellite** options are similar between gateways and portals. **Agent** options, however, are different.

The Gateway Agent configuration pertains to the connection between the agents and the gateway.

Gateway: Tunnel Settings Tab

Network > GlobalProtect > Gateways > Add > Agent > Tunnel Settings



GlobalProtect Gateway Configuration

☑ Tunnel Mode

Tunnel Interface: tunnel.11

Max User: 50

☑ Enable IPSec

GlobalProtect IPSec Crypto: default

☐ Enable X-Auth Support

Group Name:

Group Password:

Confirm Group Password:

☑ Skip Au

Deselect the **Tunnel Mode** to configure internal gateways.

Required for IPsec client connections

IPsec is the default. To make SSL the primary method, uncheck this box.

Use the **Tunnel Settings** tab to configure the tunnel parameters and enable tunneling. The tunnel parameters are required if you are setting up an external gateway. If you are configuring an internal gateway, they are optional.

For gateways that require a tunnel connection, go to the **Tunnel Settings** tab and 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 can be configured for IPsec.
- If IPsec is not available, the gateway will default back to SSL.

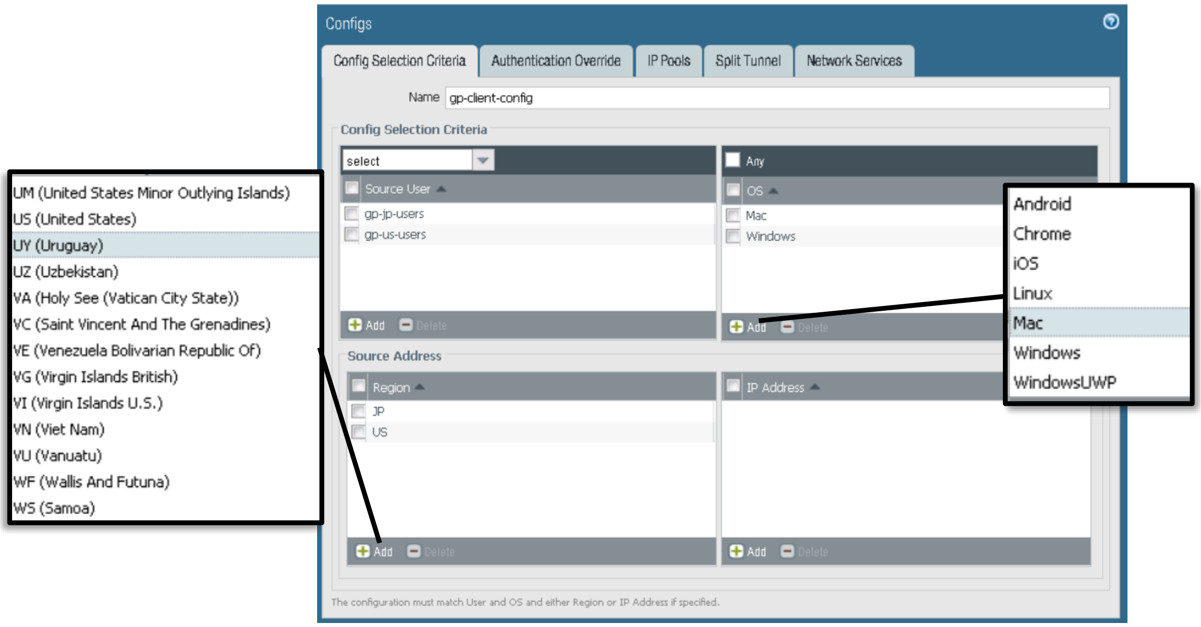
Timeout configurations can be set whether or not the gateway is running Tunnel mode. User timeouts can be specified so that inactive connections automatically are closed.

The **Enable X-Auth Support** option is needed to allow third-party VPN clients to establish IPsec tunnels to the gateway.

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



Name gp-client-config

Config Selection Criteria

□ Source User	□ OS
□ gp-jp-users	□ Mac
□ gp-us-users	□ Windows

Source Address

□ Region	□ IP Address
□ JP	
□ US	

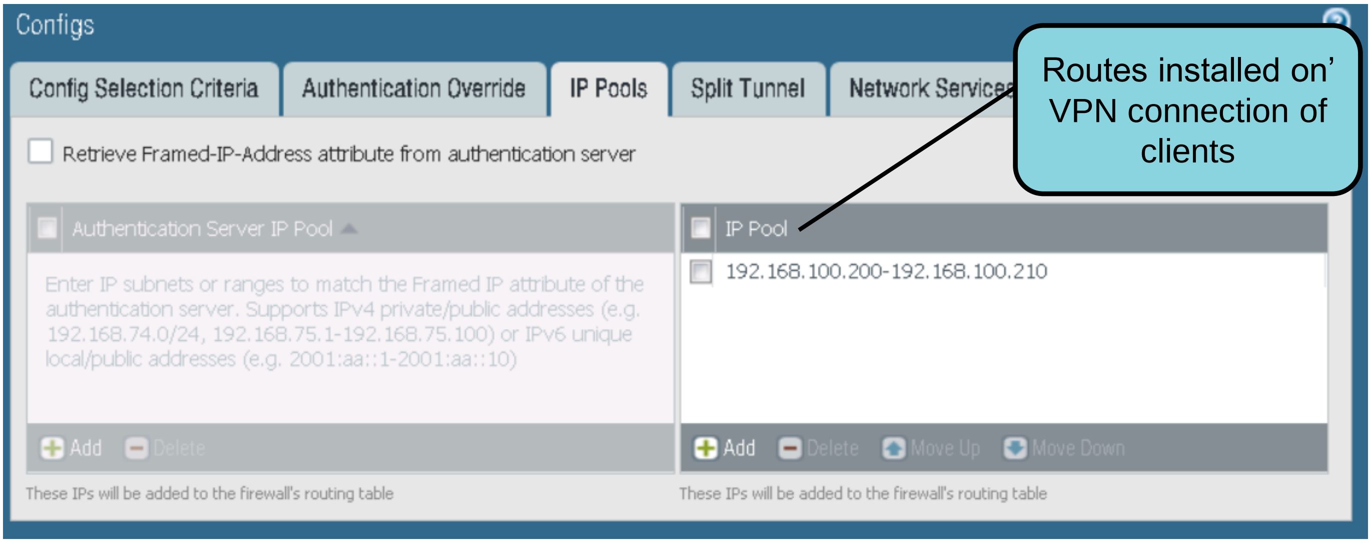
The configuration must match User and OS and either Region or IP Address if specified.

With the release of PAN-OS 9.0, 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 of the selection criteria configured on the **Config Selection Criteria** tab, then the gateway deploys the client settings configuration to the GlobalProtect user.

Gateway: IP Pools Tab

Network > GlobalProtect > Gateways > Add > Agent > Client Settings > Add > IP Pools



□ Retrieve Framed-IP-Address attribute from authentication server

□ Authentication Server IP Pool

Enter IP subnets or ranges to match the Framed IP attribute of the authentication server. Supports IPv4 private/public addresses (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) or IPv6 unique local/public addresses (e.g. 2001:aa::1-2001:aa::10)

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

□ IP Pool

□ 192.168.100.200-192.168.100.210

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

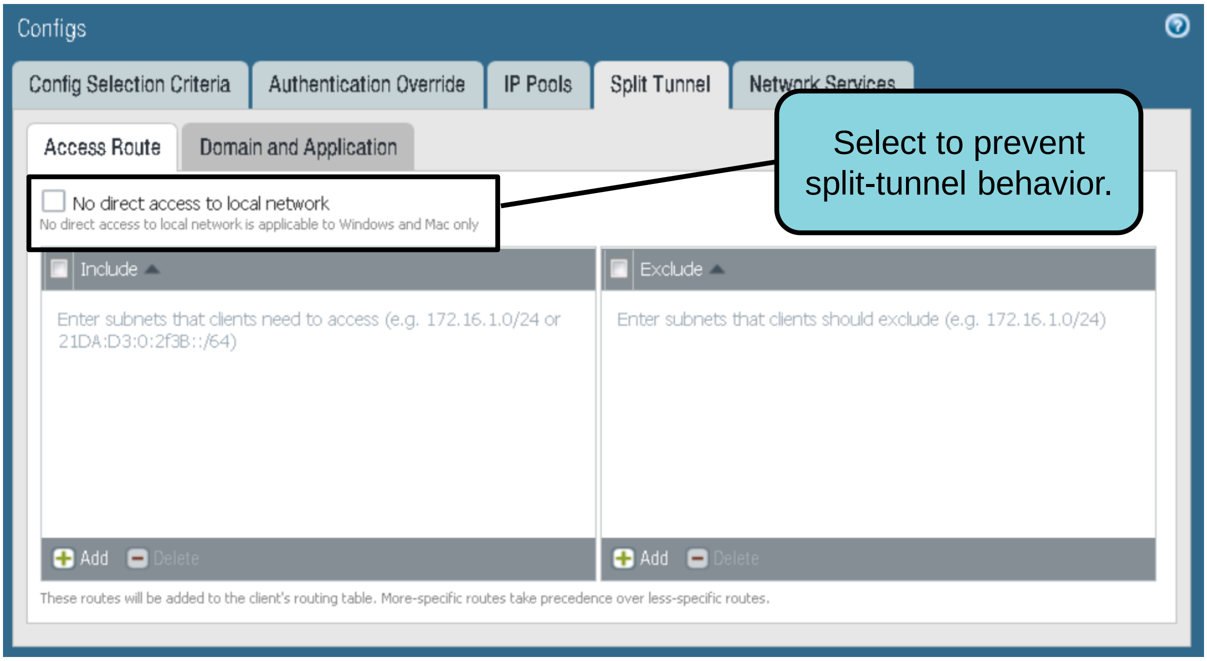
Routes installed on’ VPN connection of clients

A gateway configured in Tunnel mode functions as a DHCP server to connected clients. IP addresses and other networking 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**). The network settings defined here are assigned to the virtual network adapter on the client system when an agent establishes a tunnel with the gateway. The contents of the tab are unavailable otherwise.

Gateway: Split Tunnel Tab

Network > GlobalProtect > Gateways > Add > Agent > Client Settings > Add > Split Tunnel



□ No direct access to local network

No direct access to local network is applicable to Windows and Mac only

Enter subnets that clients need to access (e.g. 172.16.1.0/24 or 21DA:D3:0:2f3B::/64)

Enter subnets that clients should exclude (e.g. 172.16.1.0/24)

These routes will be added to the client's routing table. More-specific routes take precedence over less-specific routes.

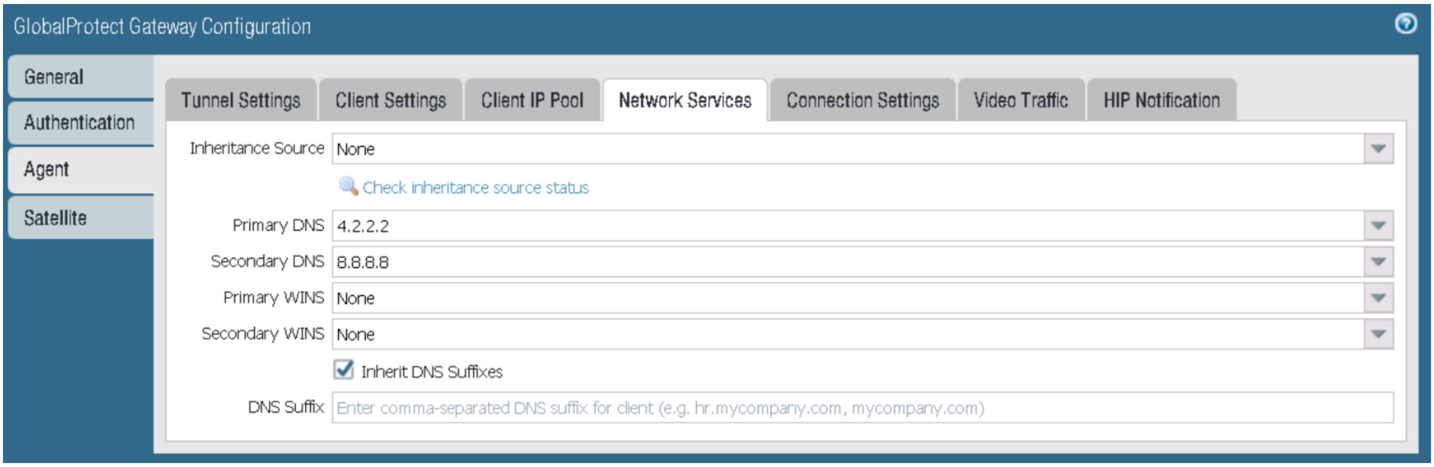
Select to prevent split-tunnel behavior.

Split-tunneling also is supported. To enable split-tunneling, enter the multiple network addresses. The gateway is assigning the IP address for the connection, so it can map the IP address to the user for User-ID functionality.

An administrator can disable local subnet access at the GlobalProtect gateway. When local subnet access is disabled, any requests to the local subnet are routed through the tunnel after the GlobalProtect tunnel is established.

Gateway: Enable Network Services

Network > GlobalProtect > Gateways > Agent > Network Services



Inheritance Source: None

Primary DNS: 4.2.2.2

Secondary DNS: 8.8.8.8

Primary WINS: None

Secondary WINS: None

☑ Inherit DNS Suffixes

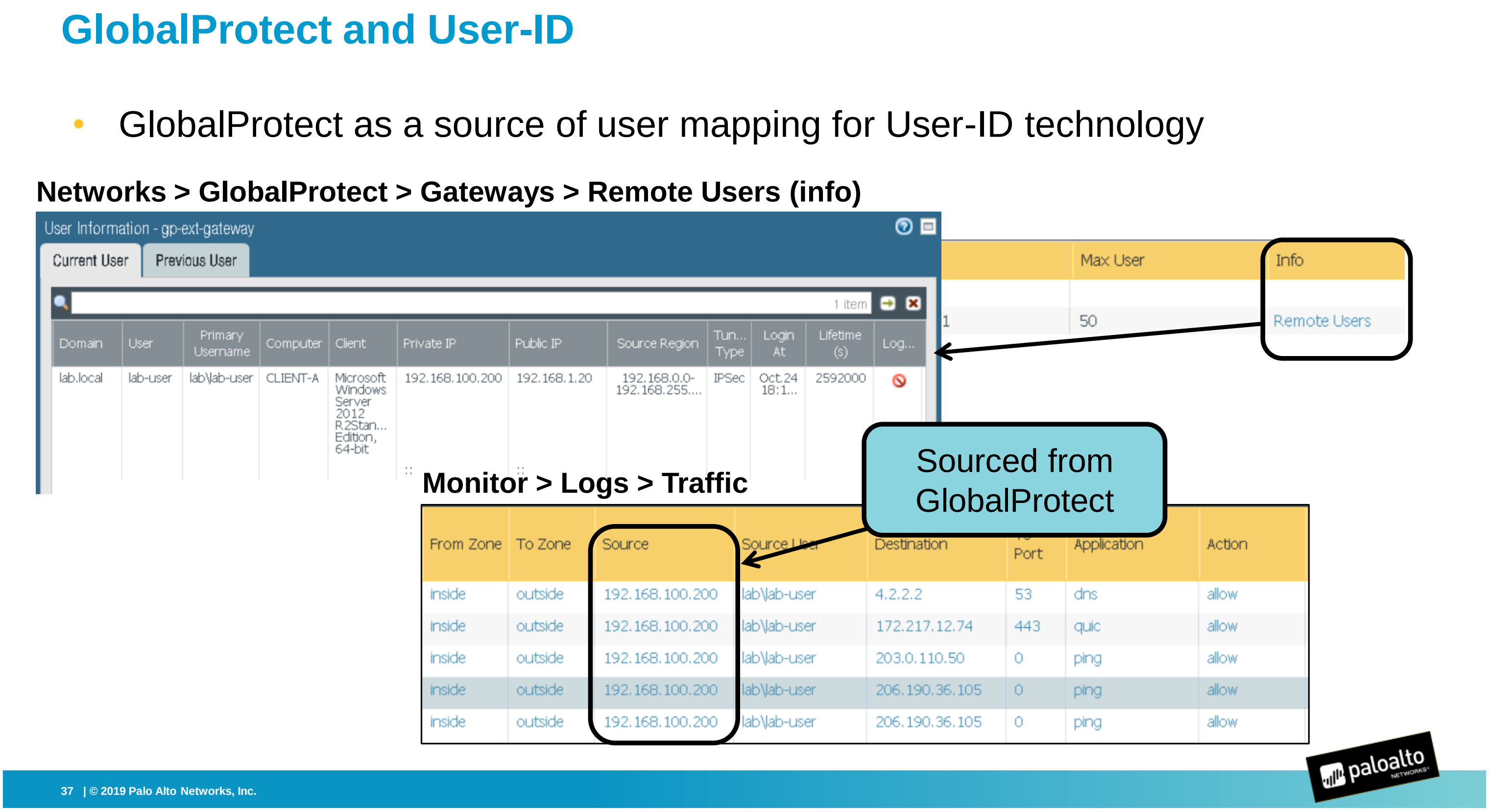
DNS Suffix: Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)

The **Network Services** tab allows you to configure DNS settings that are assigned to the virtual network adapter on the client system when an agent 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 agent's configuration. With this setting, all client network configuration, such as DNS servers and WINS servers, is 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 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 as a source of user mapping for User-ID technology

Networks > GlobalProtect > Gateways > Remote Users (info)

User Information - gp-ext-gateway

Domain	User	Primary Username	Computer	Client	Private IP	Public IP	Source Region	Tun... Type	Login At	Lifetime (s)	Log...
lab.local	lab-user	lab\lab-user	CLIENT-A	Microsoft Windows Server 2012 R2Stan... Edition, 64-bit	192.168.100.200	192.168.1.20	192.168.0.0-192.168.255....	IPSec	Oct.24 18:1...	2592000	🚫

	Max User	Info
1	50	Remote Users

Monitor > Logs > Traffic

From Zone	To Zone	Source	Source User	Destination	Port	Application	Action
inside	outside	192.168.100.200	lab\lab-user	4.2.2.2	53	dns	allow
inside	outside	192.168.100.200	lab\lab-user	172.217.12.74	443	quic	allow
inside	outside	192.168.100.200	lab\lab-user	203.0.110.50	0	ping	allow
inside	outside	192.168.100.200	lab\lab-user	206.190.36.105	0	ping	allow
inside	outside	192.168.100.200	lab\lab-user	206.190.36.105	0	ping	allow

Sourced from GlobalProtect

37 | © 2019 Palo Alto Networks, Inc.

For mobile or roaming users, the GlobalProtect client provides the user mapping information to the firewall directly. In this case, every GlobalProtect user has an agent or app running on the client 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.

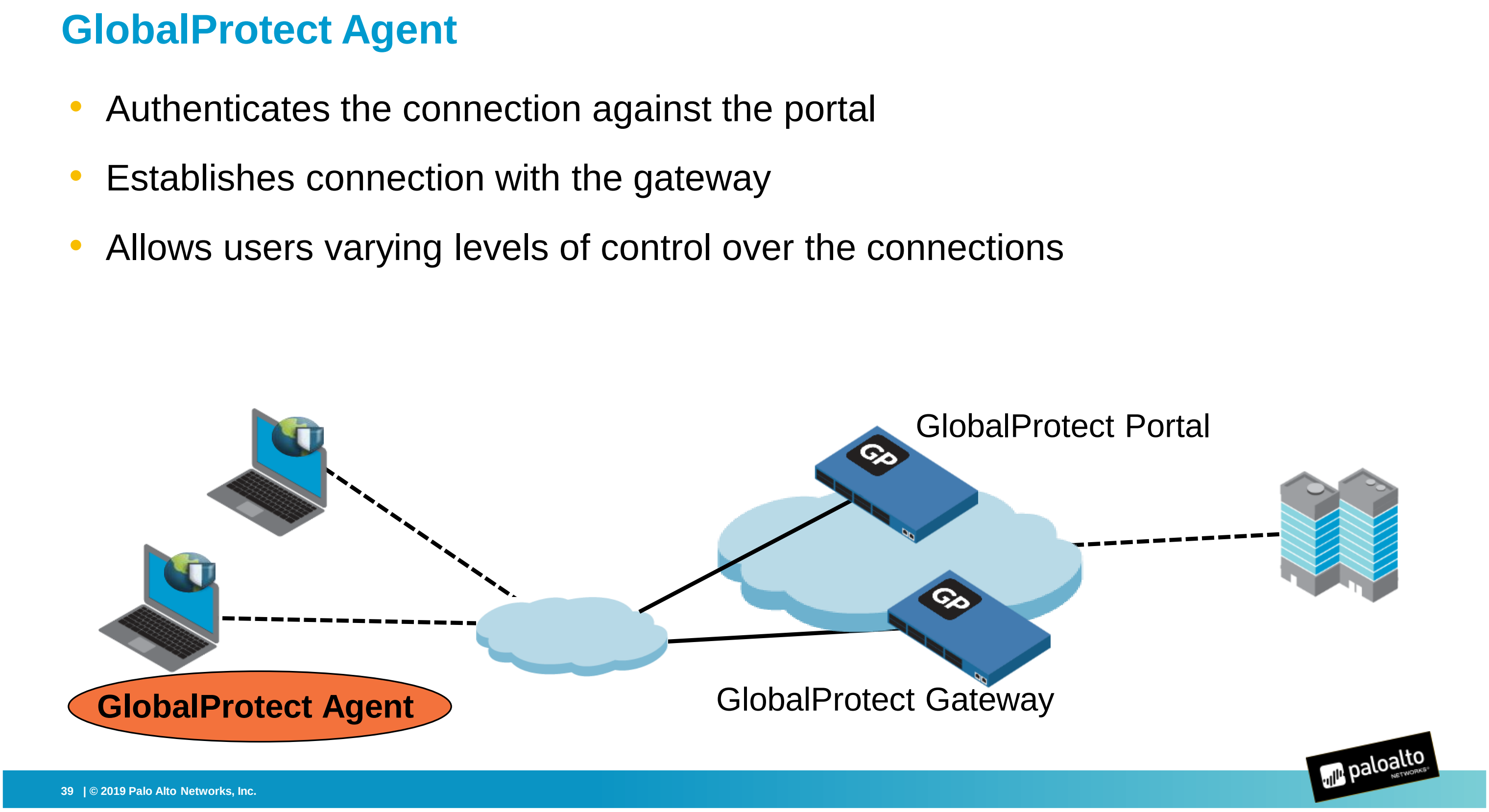
GlobalProtect overview

Preparing the firewall for GlobalProtect

Configuration: GlobalProtect portal

Configuration: GlobalProtect gateway

Configuration: GlobalProtect agents



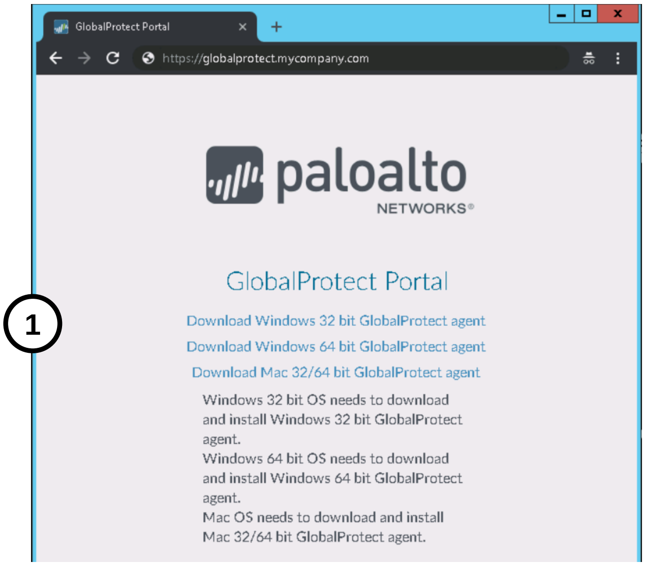
GlobalProtect Agent

- Authenticates the connection against the portal
- Establishes connection with the gateway
- Allows users varying levels of control over the connections

The GlobalProtect client software runs on end user systems and enables access to your network resources via the GlobalProtect portals and gateways you have deployed. The software is available both in Agent form (for Windows and macOS systems) and in App form (for mobile devices).

Installing the Agent

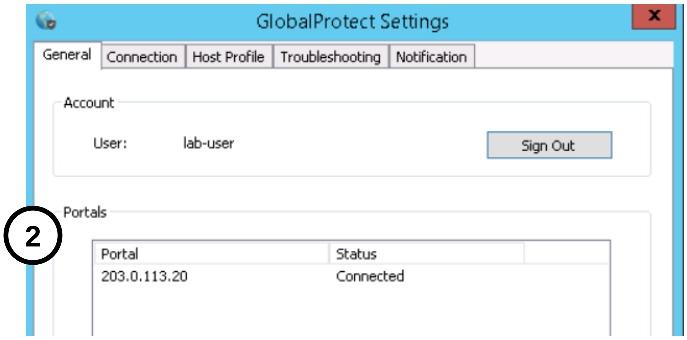
1. Download the software.
2. Configure the agent.



GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent
Download Windows 64 bit GlobalProtect agent
Download Mac 32/64 bit GlobalProtect agent

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



GlobalProtect Settings

Account

User: lab-user

Portals

Portal	Status
203.0.113.20	Connected

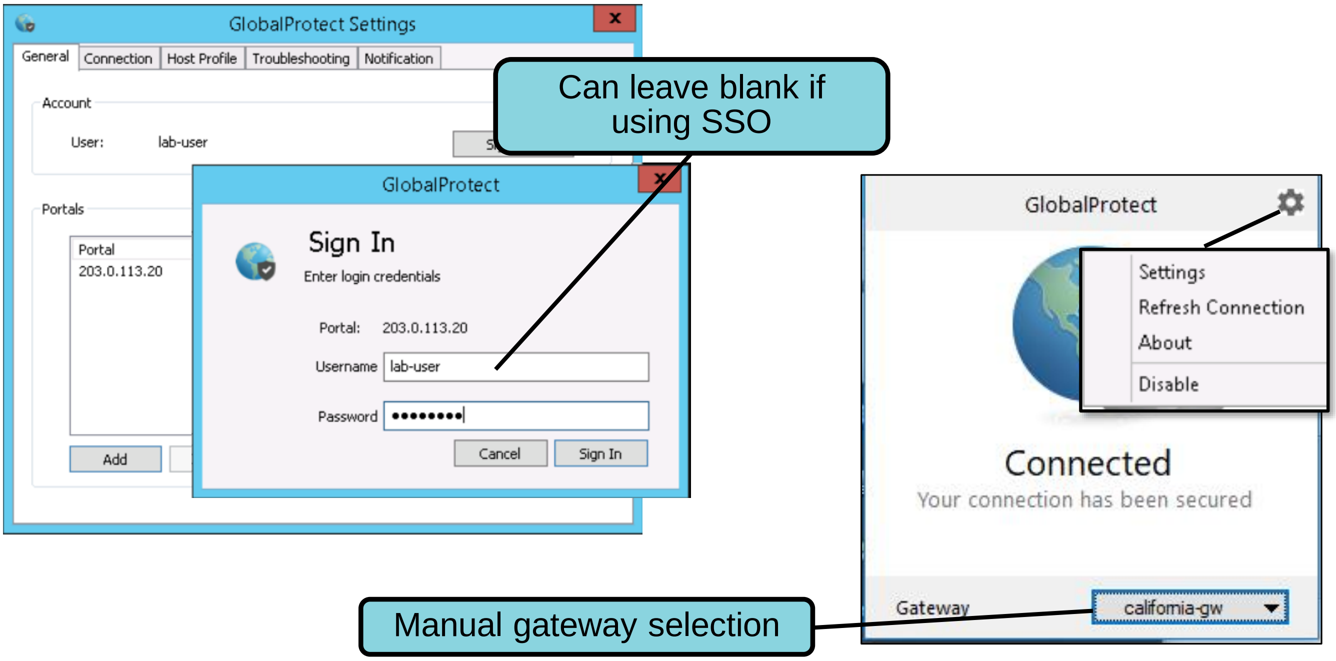
The GlobalProtect agent must be installed before a connection can be established.

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

Client Configuration



GlobalProtect Settings

Account

User: lab-user

Portals

Portal
203.0.113.20

GlobalProtect

Sign In

Enter login credentials

Portal: 203.0.113.20

Username: lab-user

Password: ••••••••

Can leave blank if using SSO

GlobalProtect

Connected

Your connection has been secured

Gateway: california-gw

Manual gateway selection

As the GlobalProtect administrator, you can make GlobalProtect completely transparent to the end users, which allows them no control over their connections. The interfaces shown in this section will vary based on the specific permissions granted to the users when the portal is configured.

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

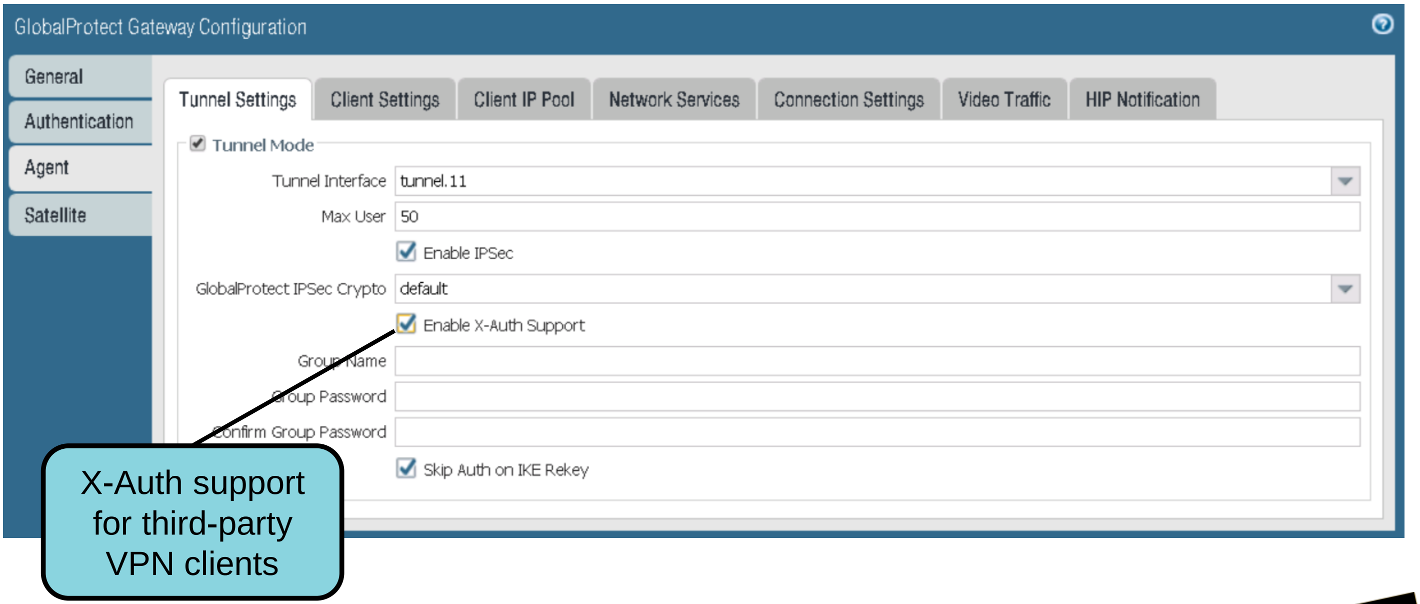
The username and password must match the Authentication Profile set on the portal. If the session is configured for SSO, the **Username** and **Password** fields can be left blank.

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 client automatically discovers the gateways. Gateways can be marked as **manual** to allow users to establish a connection with specific networks. Any rediscovery event reverts the agent to Auto Discovery mode.

X-Auth Configuration

Network > GlobalProtect > Gateways > <select_gateway> > Agent > Tunnel Settings



☑ Tunnel Mode

Tunnel Interface: tunnel.11

Max User: 50

☑ Enable IPSec

GlobalProtect IPSec Crypto: default

☑ Enable X-Auth Support

Group Name

Group Password

Confirm Group Password

☑ Skip Auth on IKE Rekey

X-Auth support for third-party VPN clients

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. Because X-Auth access provides limited GlobalProtect functionality, consider using the GlobalProtect app for simplified access to the full security feature set that GlobalProtect provides on iOS and Android devices.

Selection of X-Auth support activates the **Group Name** and **Group Password** fields.

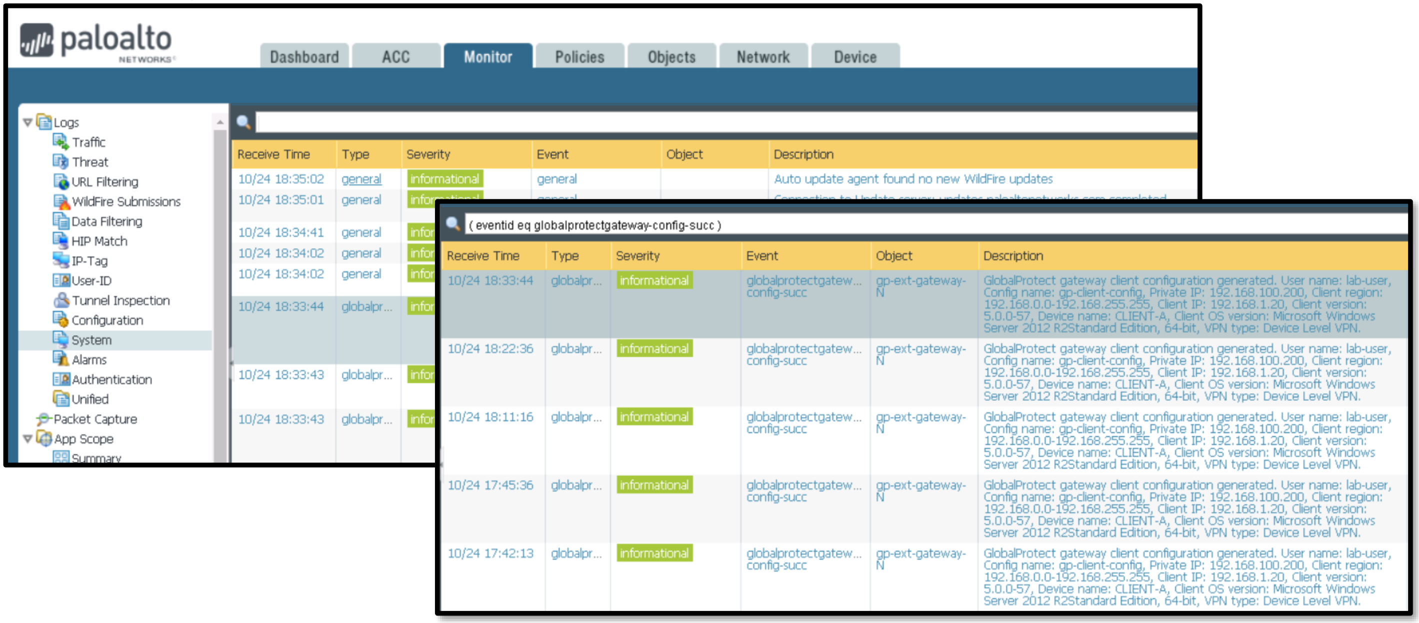
If the group name and group password are specified, the first authentication phase requires both parties to use this credential to authenticate. The second phase requires a valid username and password, which are verified through the Authentication Profile configured in the **Authentication** tab.

If no group name and group password are defined, the first authentication phase is based on a valid certificate presented by the third-party VPN client. This certificate then is validated through the Certificate Profile configured in the **Authentication** tab.

By default, the user is not required to re-authenticate when the key used to establish the IPsec tunnel expires. To require the user to re-authenticate, clear the **Skip Auth on IKE Rekey** option.

System Log

Monitor > Logs > System



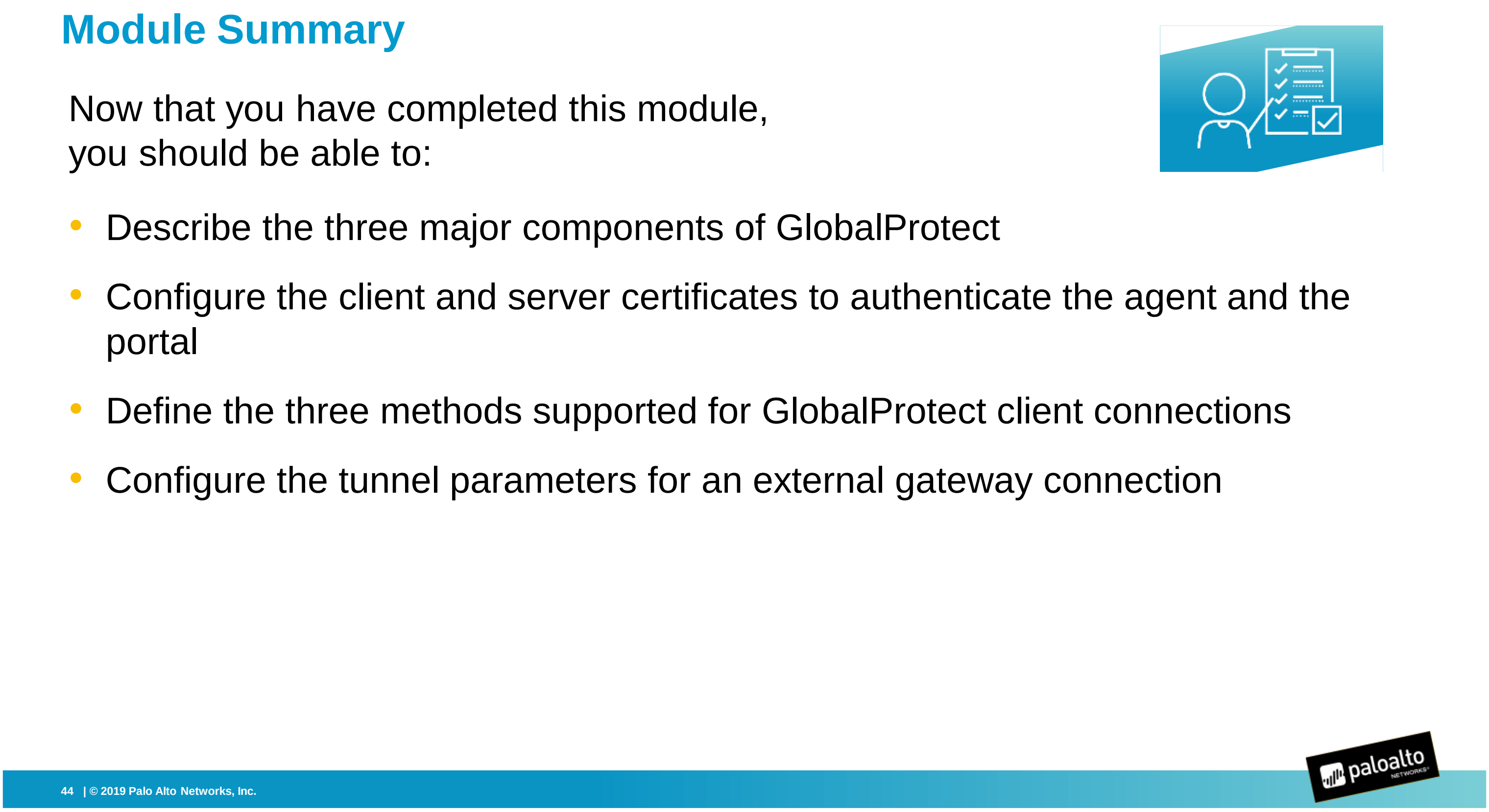
Receive Time	Type	Severity	Event	Object	Description
10/24 18:35:02	general	informational	general		Auto update agent found no new WildFire updates
10/24 18:35:01	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed
10/24 18:34:41	general	infor			
10/24 18:34:02	general	infor			
10/24 18:34:02	general	infor			
10/24 18:33:44	globalpr...	infor			
10/24 18:33:43	globalpr...	infor			
10/24 18:33:43	globalpr...	infor			

(eventid eq globalprotectgateway-config-succ)

Receive Time	Type	Severity	Event	Object	Description
10/24 18:33:44	globalpr...	informational	globalprotectgatew... config-succ	gp-ext-gateway-N	GlobalProtect gateway client configuration generated. User name: lab-user, Config name: gp-client-config, Private IP: 192.168.100.200, Client region: 192.168.0.0-192.168.255.255, Client IP: 192.168.1.20, Client version: 5.0.0-57, Device name: CLIENT-A, Client OS version: Microsoft Windows Server 2012 R2Standard Edition, 64-bit, VPN type: Device Level VPN.
10/24 18:22:36	globalpr...	informational	globalprotectgatew... config-succ	gp-ext-gateway-N	GlobalProtect gateway client configuration generated. User name: lab-user, Config name: gp-client-config, Private IP: 192.168.100.200, Client region: 192.168.0.0-192.168.255.255, Client IP: 192.168.1.20, Client version: 5.0.0-57, Device name: CLIENT-A, Client OS version: Microsoft Windows Server 2012 R2Standard Edition, 64-bit, VPN type: Device Level VPN.
10/24 18:11:16	globalpr...	informational	globalprotectgatew... config-succ	gp-ext-gateway-N	GlobalProtect gateway client configuration generated. User name: lab-user, Config name: gp-client-config, Private IP: 192.168.100.200, Client region: 192.168.0.0-192.168.255.255, Client IP: 192.168.1.20, Client version: 5.0.0-57, Device name: CLIENT-A, Client OS version: Microsoft Windows Server 2012 R2Standard Edition, 64-bit, VPN type: Device Level VPN.
10/24 17:45:36	globalpr...	informational	globalprotectgatew... config-succ	gp-ext-gateway-N	GlobalProtect gateway client configuration generated. User name: lab-user, Config name: gp-client-config, Private IP: 192.168.100.200, Client region: 192.168.0.0-192.168.255.255, Client IP: 192.168.1.20, Client version: 5.0.0-57, Device name: CLIENT-A, Client OS version: Microsoft Windows Server 2012 R2Standard Edition, 64-bit, VPN type: Device Level VPN.
10/24 17:42:13	globalpr...	informational	globalprotectgatew... config-succ	gp-ext-gateway-N	GlobalProtect gateway client configuration generated. User name: lab-user, Config name: gp-client-config, Private IP: 192.168.100.200, Client region: 192.168.0.0-192.168.255.255, Client IP: 192.168.1.20, Client version: 5.0.0-57, Device name: CLIENT-A, Client OS version: Microsoft Windows Server 2012 R2Standard Edition, 64-bit, VPN type: Device Level VPN.

The portal and gateway firewalls maintain information about the connections in the System log. Any interaction between the client and the other components is logged on the device that handles the interaction.

Use the search string `(subtype eq globalprotect)` to filter for GlobalProtect entries. **Note:** This filter alone does not display the authentication events.



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
- Define the three methods supported for GlobalProtect client connections
- Configure the tunnel parameters for an external gateway connection

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

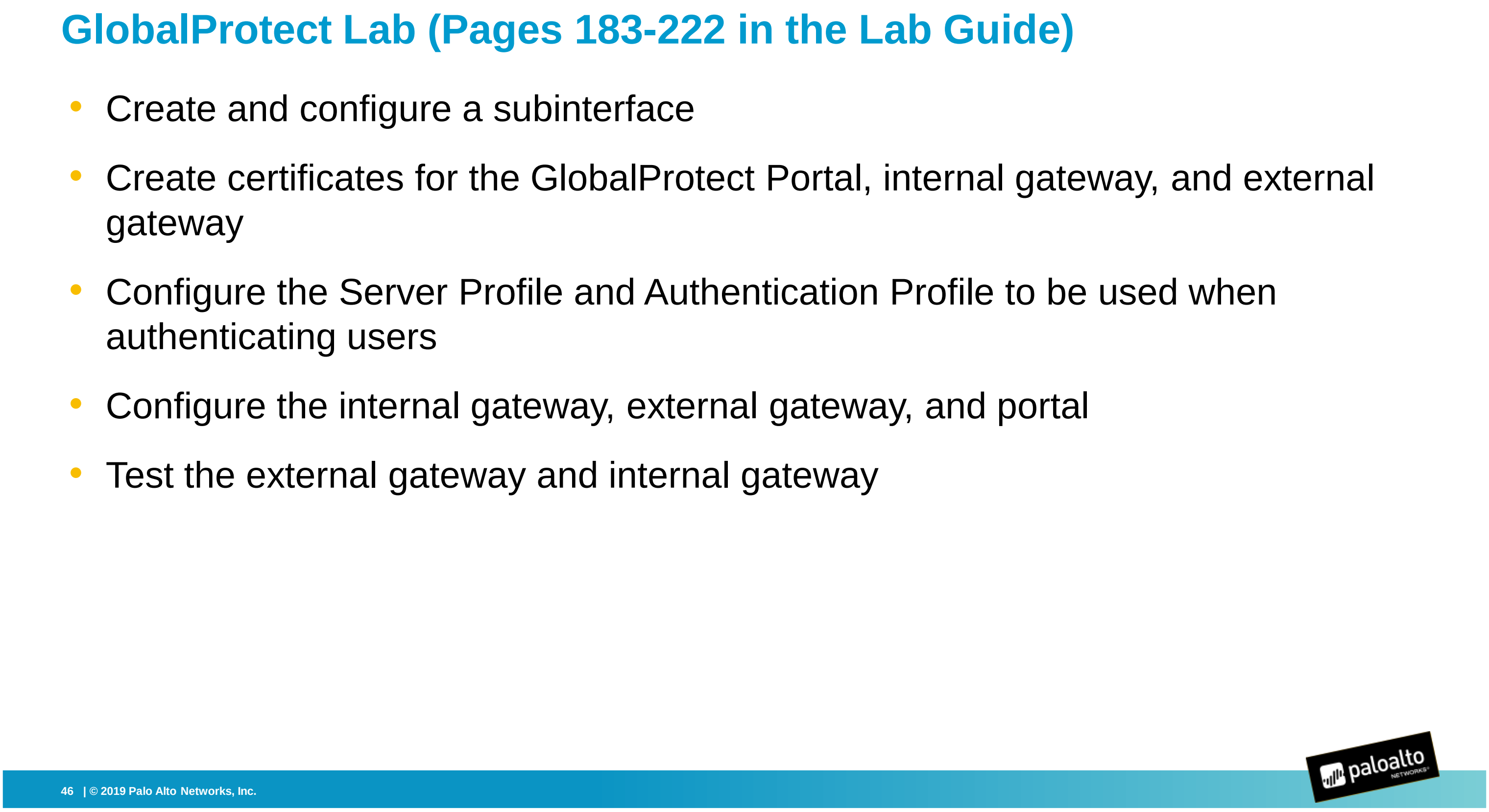
- Describe the three major components of GlobalProtect
- Configure the client and server certificates to authenticate the agent and the portal
- Define the three methods supported for GlobalProtect client connections
- Configure the tunnel parameters for an external gateway connection

Questions?

45 | © 2019 Palo Alto Networks, Inc.

Review Questions

1. The GlobalProtect client will connect to either an internal gateway or an external gateway based on its location (inside or outside of the corporate network). This location determination is based on the result of which option?
    a. reverse DNS lookup
    b. user selection during agent startup
    c. IP address of the client system
    d. whether the user starts the client in online or offline mode
2. The GlobalProtect client 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 three statements are true regarding a GlobalProtect Gateway? (Choose three.)
    a. Provides security enforcement for traffic from GlobalProtect clients.
    b. Requires a tunnel interface for external clients.
    c. Tunnel interfaces are optional for internal gateways.
    d. Authenticates users against a Server Profile.
5. For which type of functionality can a GlobalProtect Gateway map IP addresses to the user?
    a. App-ID
    b. Content-ID
    c. User-ID



GlobalProtect Lab (Pages 183-222 in the Lab Guide)

- Create and configure a subinterface
- Create certificates for the GlobalProtect Portal, internal gateway, and external gateway
- Configure the Server Profile and Authentication Profile to be used when authenticating users
- Configure the internal gateway, external gateway, and portal
- Test the external gateway and internal gateway

PROTECTION. DELIVERED.

Answers to Review Questions

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

This page intentionally left blank