# PALO ALTO NETWORKS - EDU-210

# Lab 10: GlobalProtect

**Document Version: 2020-06-26**

Due to the length of this lab, it is recommended that you allow yourself a 1-hour reservation, at minimum, to complete this lab.

# Contents



## Introduction

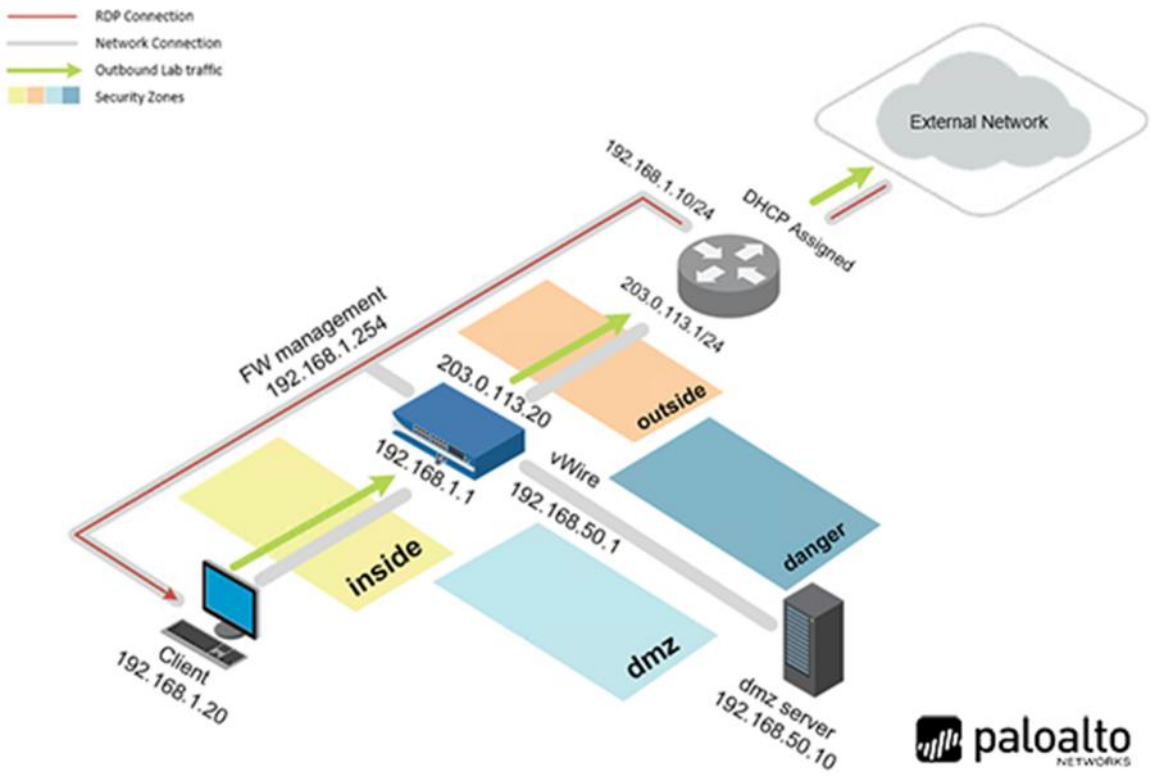
Secure communication with the corporate network is very important, especially when employees are traveling. We have decided to deploy Palo Alto Networks GlobalProtect™ features in our environment. This will allow us to do SSL VPN back to the corporate environment, as well as User-id and enforce our corporate policies on remote employees and partners.

## Objectives

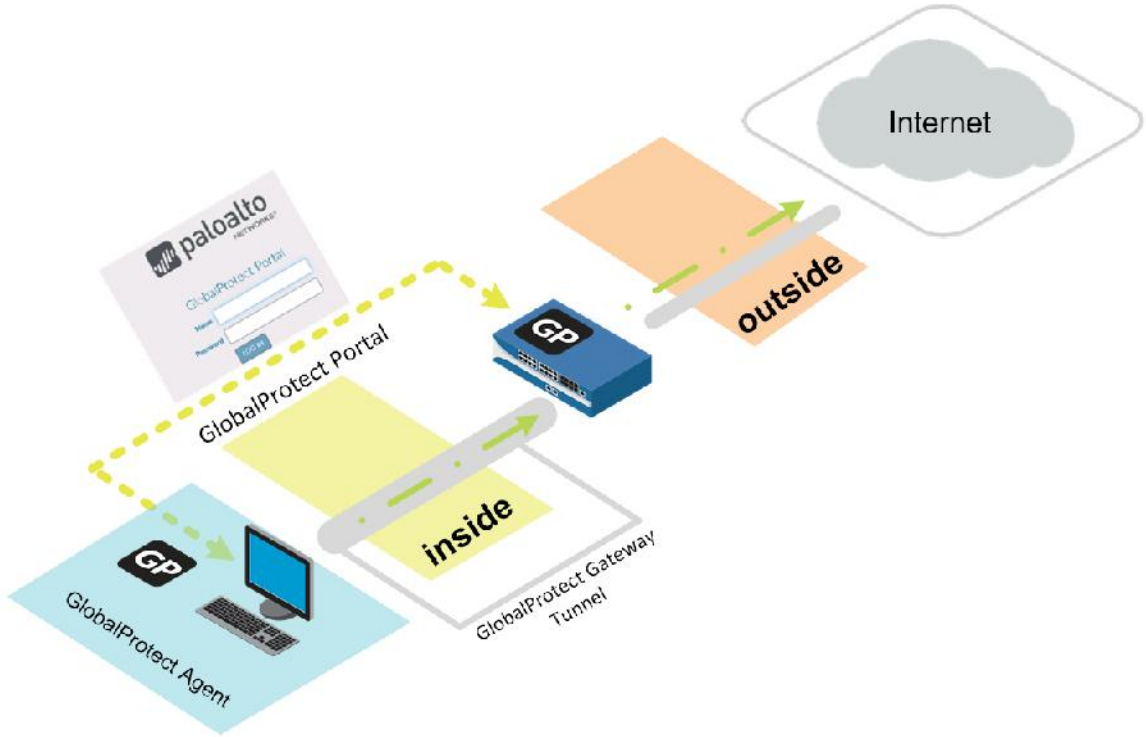
- Create and configure a subinterface
- Create certificates for the GlobalProtect portal, internal gateway, and external gateway
- Attach certificates to an SSL-TLS Service Profile
- Configure the Server Profile and Authentication Profile to be used when authenticating users
- Create and configure the tunnel interface to be used with the external gateway
- Configure the internal gateway, external gateway, and portal
- Host the GlobalProtect agent on the portal for download
- Create a No-NAT policy rule to ensure that portal traffic is not subjected to network address translation
- Test the external gateway and internal gateway

## Lab Topology




## Theoretical Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| Virtual Machine | IP Address | Account (if needed) | Password (if needed) |
|---|---|---|---|
| **Client** | 192.168.1.20 | `lab-user` | `Train1ng$` |
| **Firewall** | 192.168.1.254 | `admin` | `Train1ng$` |

# 10 GlobalProtect

## 10.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.

> To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as **`lab-user`** using the password **`Train1ng$`**.

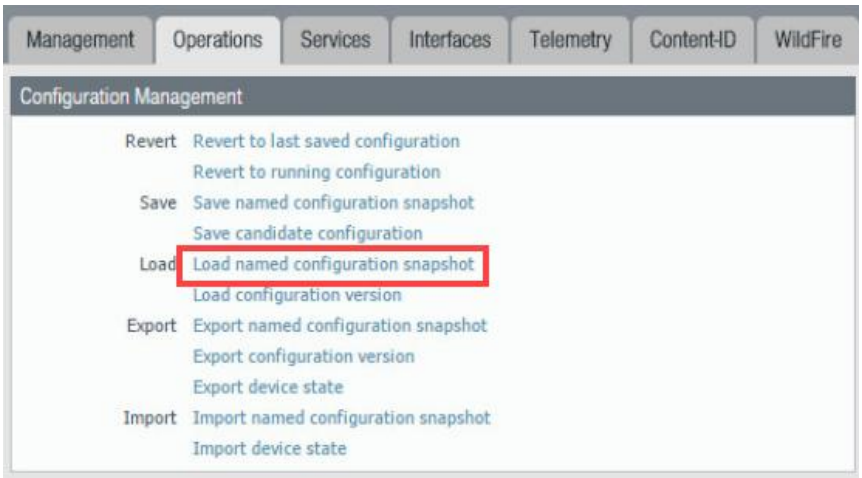

3. Launch the **Chromium Web Browser** and connect to **`https://192.168.1.254.`**
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

| Parameter | Value |
|---|---|
| Name | **`admin`** |
| Password | **`Train1ng$`** |

6. In the web interface, select **Device > Setup > Operations**.

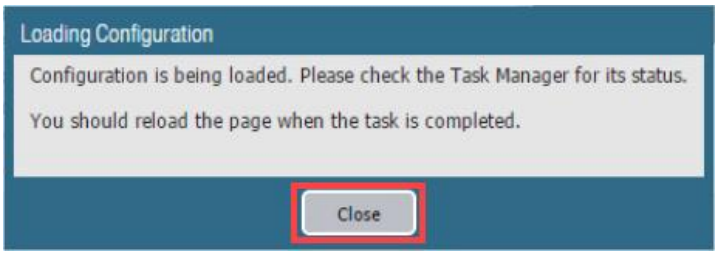

  

7. Click **Load named configuration snapshot**:



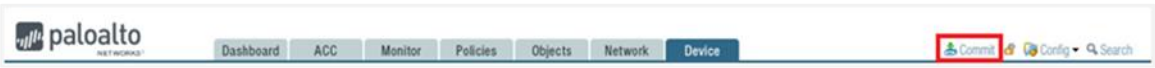

8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-10.xml**. Click **OK**.


9. Click **Close**.



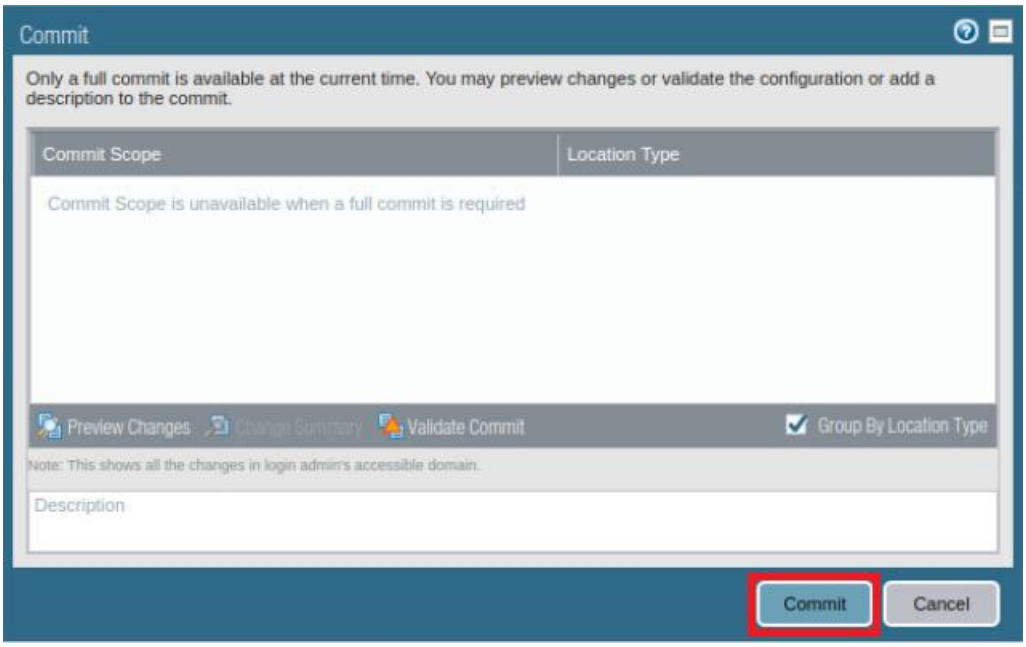

The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

10. Click the **Commit** link at the top-right of the web interface.

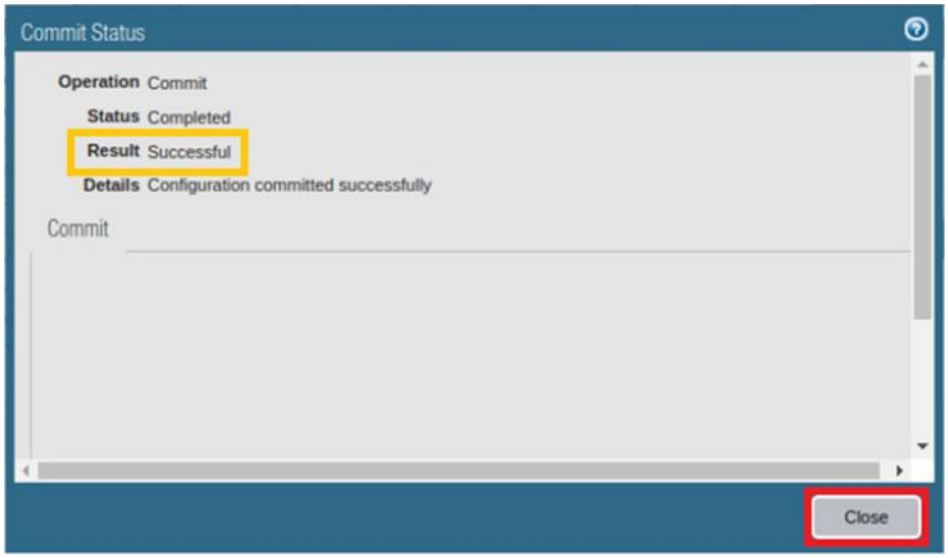


11. Click **Commit** and wait until the commit process is complete.




12. Once completed successfully, click **Close** to continue.




A warning might appear about EDL lab-dns-sinkhole and url-block-list being used without any valid entries. It can be safely ignored.

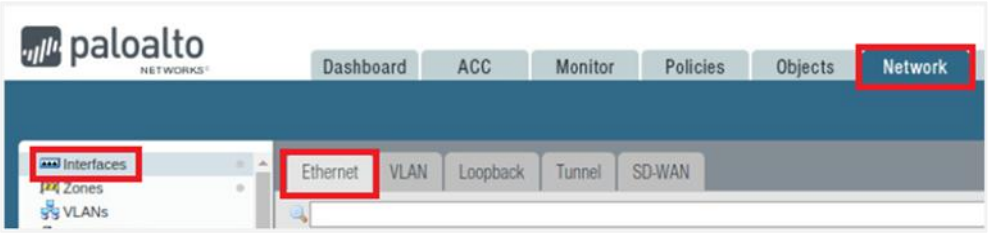
13. Leave the firewall web interface open to continue with the next task.

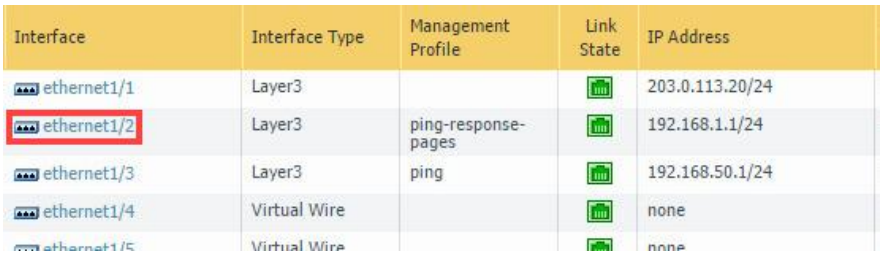
## 10.1 Configure a Subinterface

By default, VLAN tags are required for subinterfaces. However, untagged interfaces can be used to isolate traffic via zones on the same physical interface.

1. In the web interface, navigate to **Network > Interfaces > Ethernet**.

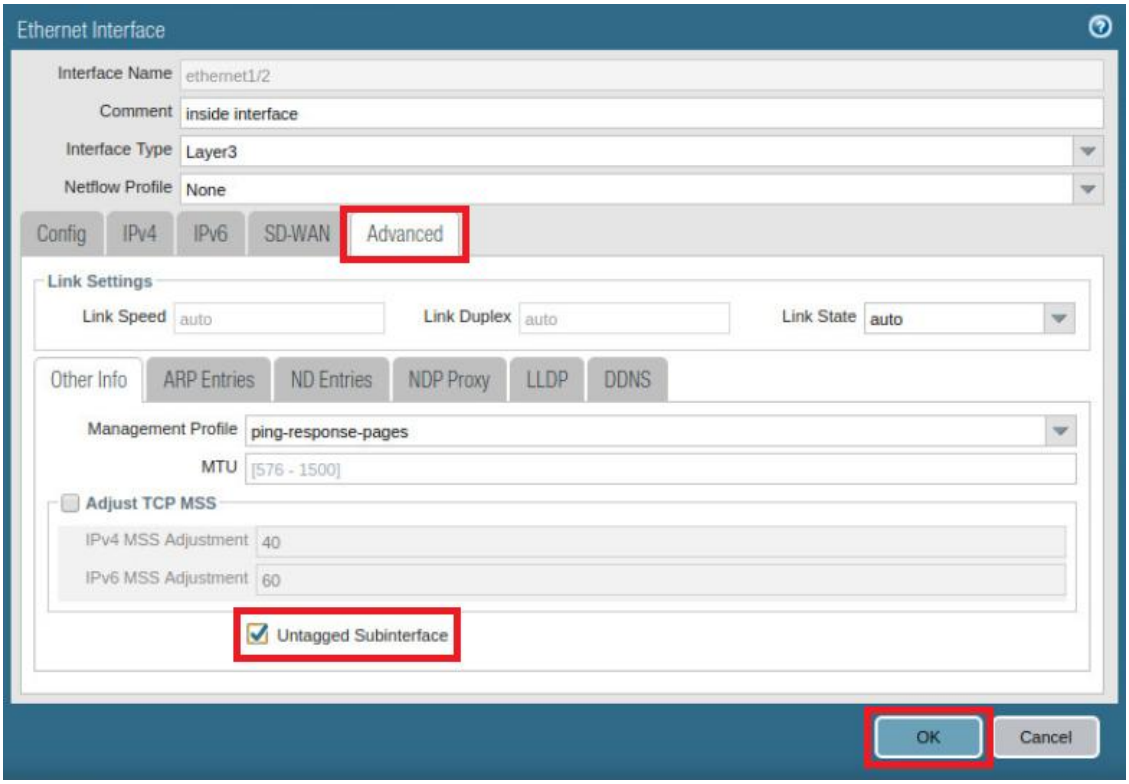



2. Click on **ethernet1/2** from the list.



| Interface | Interface Type | Management Profile | Link State | IP Address |
|---|---|---|---|---|
| ethernet1/1 | Layer3 | | | 203.0.113.20/24 |
| ethernet1/2 | Layer3 | ping-response-pages | | 192.168.1.1/24 |
| ethernet1/3 | Layer3 | ping | | 192.168.50.1/24 |
| ethernet1/4 | Virtual Wire | | | none |
| ethernet1/5 | Virtual Wire | | | none |

3. In the *Ethernet Interface* window, click the **Advanced** tab, then check the **Untagged Subinterface** checkbox and click **OK**.

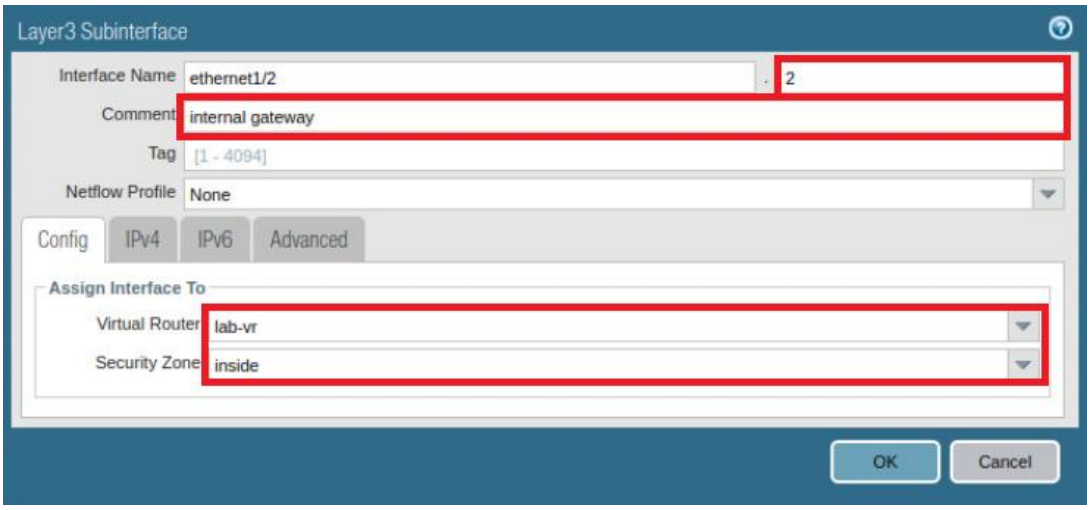


4. Verify that **ethernet1/2** is still selected and click **Add Subinterface**.


5. In the *Layer3 Subinterface* window, configure the following.

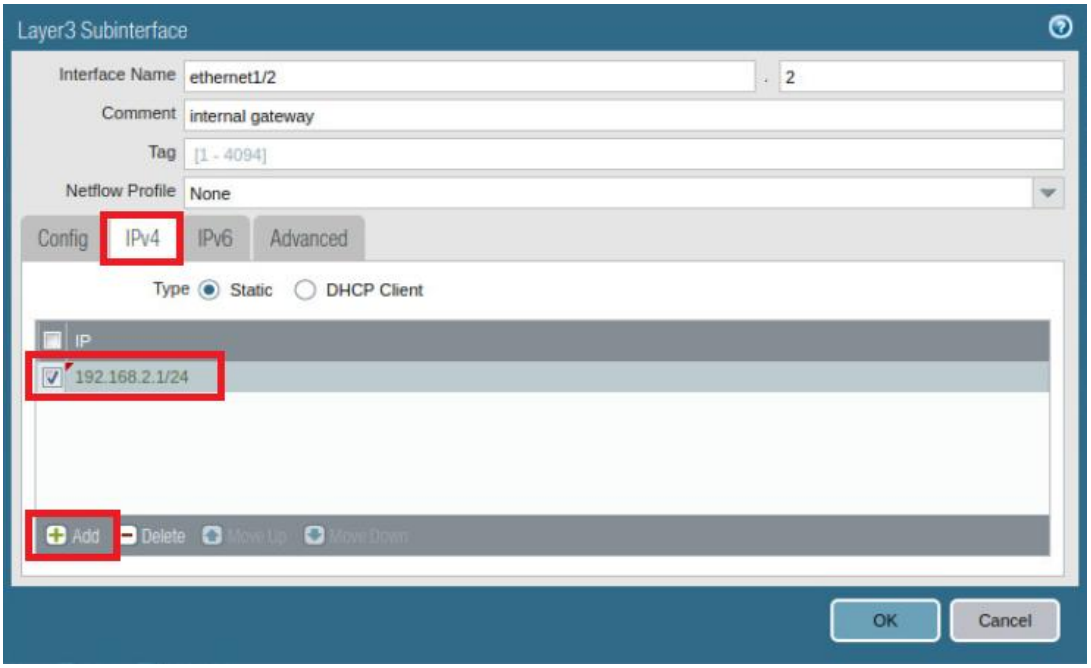
| Parameter | Value |
|---|---|
| Interface Name | Type `2` in the second text field so that it reads *ethernet1/2.2* |
| Comment | Type `internal gateway` |
| Virtual Router | Select **lab-vr** from the dropdown list |
| Security Zone | Select **inside** from the dropdown list |



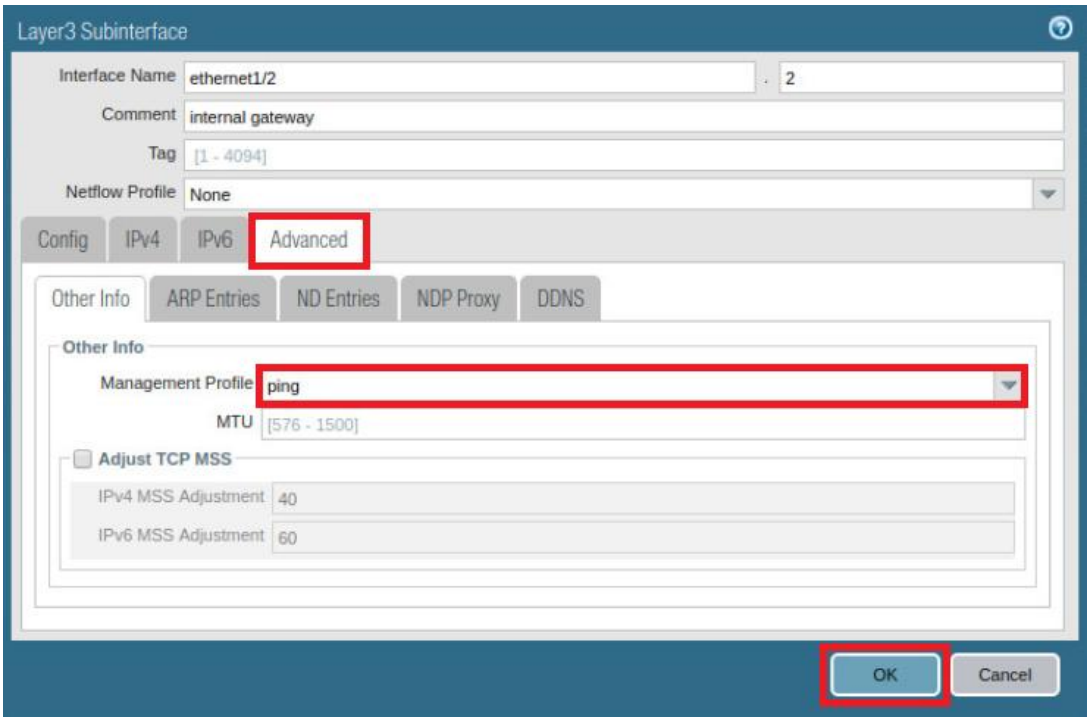

  

6. In the *Layer3 Subinterface* window, click the **IPv4** tab and configure the following:

| Parameter | Value |
|---|---|
| Interface Name | Click **Add** and type **192.168.2.1/24** |




7. In the *Layer3 Subinterface* window, click the **Advanced** tab, select **ping** for the *Management Profile* and then click **OK**.



Addition of a management profile is not a requirement for *GlobalProtect* but can make troubleshooting easier if you need to verify that the IP address on the subinterface is available.

8. Verify that your new configuration looks like the following.

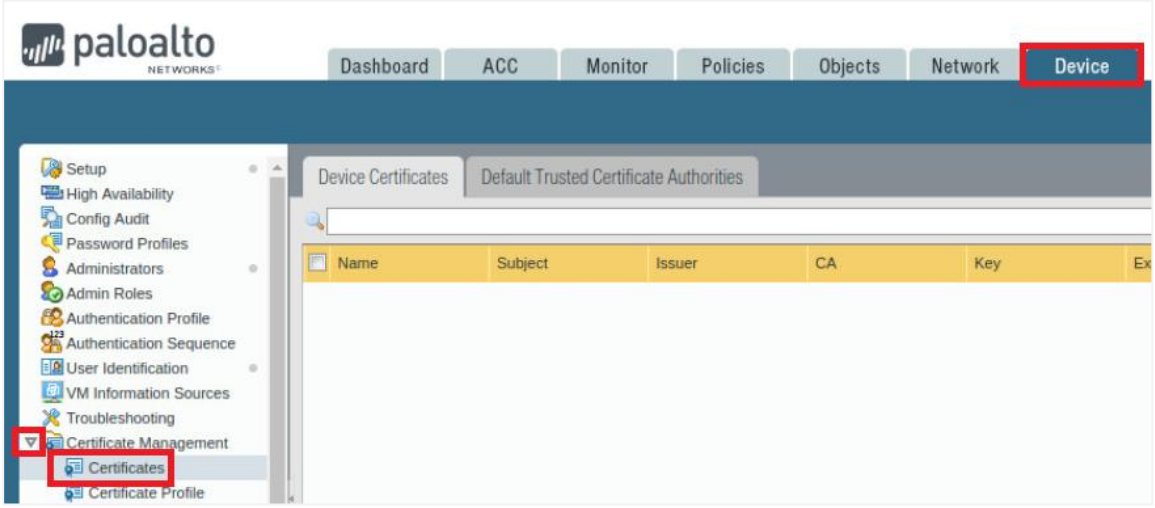
| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router | Tag | VLAN / Virtual-Wire | Security Zone |
|---|---|---|---|---|---|---|---|---|
| ethernet1/1 | Layer3 | | | 203.0.113.20/24 | lab-vr | Untagged | none | outside |
| ethernet1/2 | Layer3 | ping-response-pages | | 192.168.1.1/24 | lab-vr | Untagged | none | inside |
| ethernet1/2.2 | Layer3 | ping | | 192.168.2.1/24 | lab-vr | Untagged | none | inside |
| ethernet1/3 | Layer3 | ping | | 192.168.50.1/24 | lab-vr | Untagged | none | dmz |

9. Leave the firewall web interface open to continue with the next task

## 10.2 Generate Self-Signed Certificates

GlobalProtect needs three certificates, one each for the portal, external gateway, and internal gateway. These certificates are typically signed by a common CA certificate. This lab creates a CA certificate and internal gateway certificate but combines the Portal and External Gateway certificates because these GlobalProtect functions are combined on the same IP address.

1. In the web interface, select **Device > Certificate Management > Certificates**.

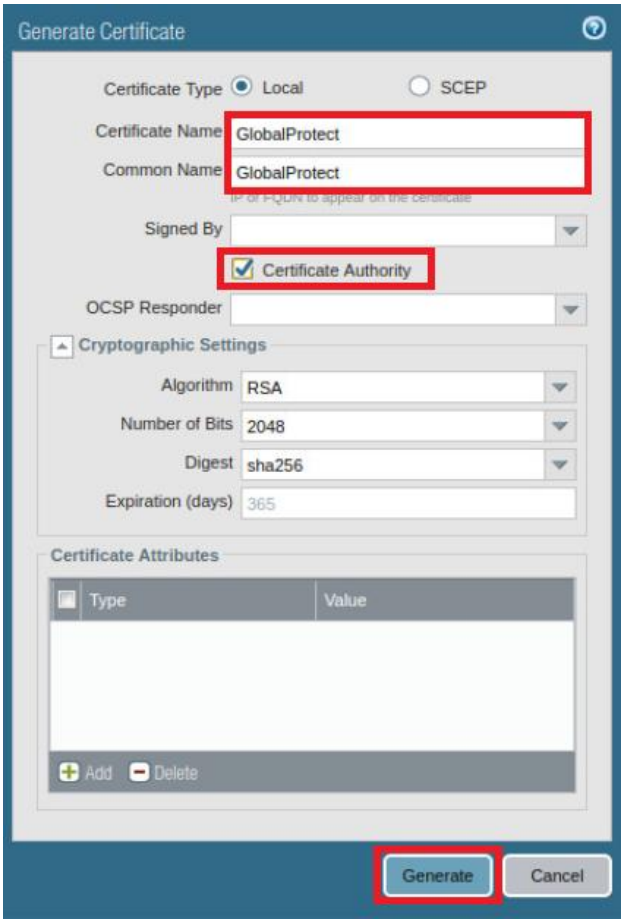



2. Click **Generate** to create a certificate.

3. In the *Generate Certificate* window, fill out the form using the information below and then click **Generate**.

| Parameter | Value |
|---|---|
| Certificate Name | Type `GlobalProtect` |
| Common Name | Type `GlobalProtect` |
| Signed By | Leave blank |
| Certificate Authority | Select the checkbox |



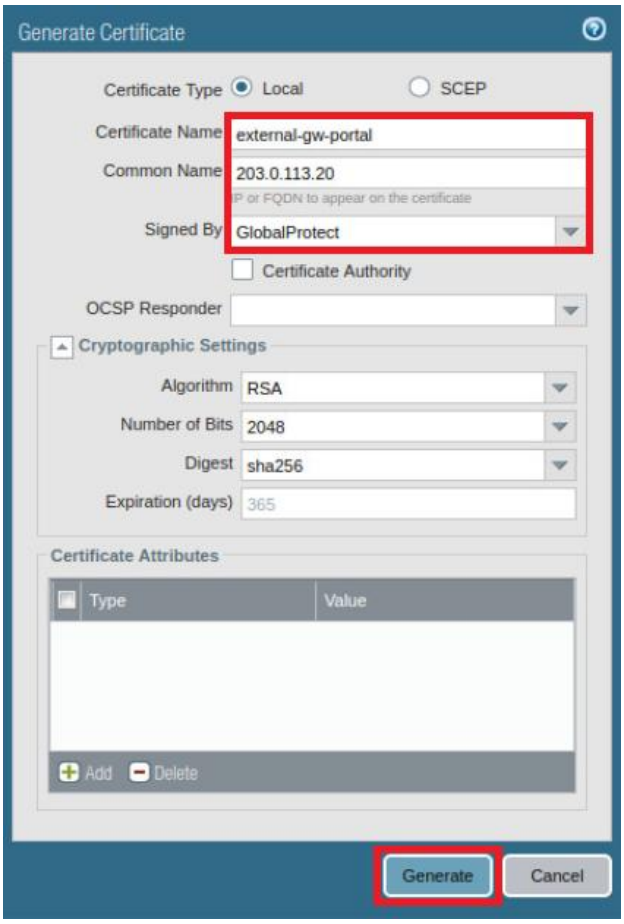

This certificate will be used to sign the external and internal gateway certificates.

4. Click **OK** to dismiss the successful status window.

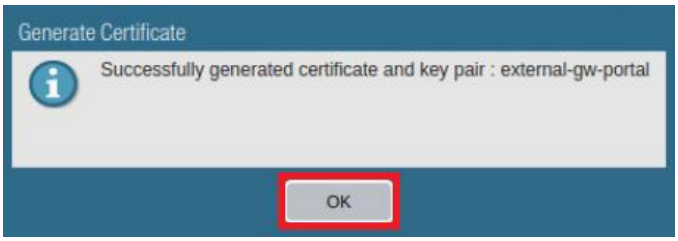

  

5. Click **Generate** to create another certificate using the following data, then click **Generate**.

| Parameter | Value |
|---|---|
| Certificate Name | Type `external-gw-portal` |
| Common Name | Type `203.0.113.20` |
| Signed By | Select **GlobalProtect** from the dropdown list |



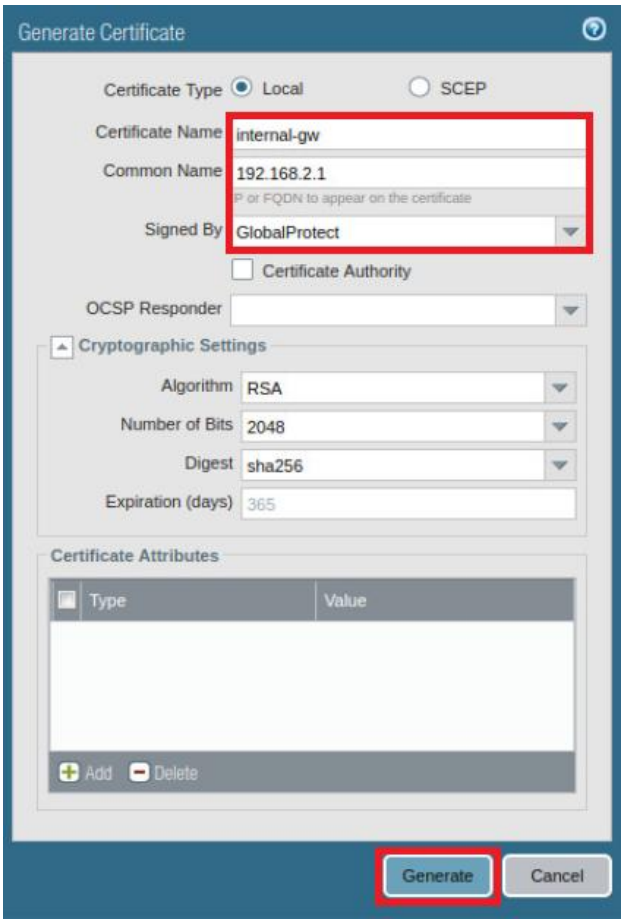

6. Click **OK** to dismiss the successful status window.



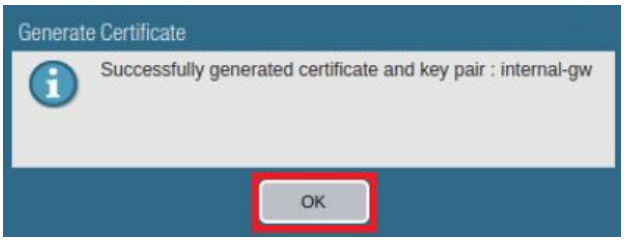

  

7. Click **Generate** once more to create another certificate using the following data and then click **Generate**.

| Parameter | Value |
|---|---|
| Certificate Name | Type `internal-gw` |
| Common Name | Type `192.168.2.1` |
| Signed By | Select **GlobalProtect** from the dropdown list |




8. Click **OK** to dismiss the successful status window.



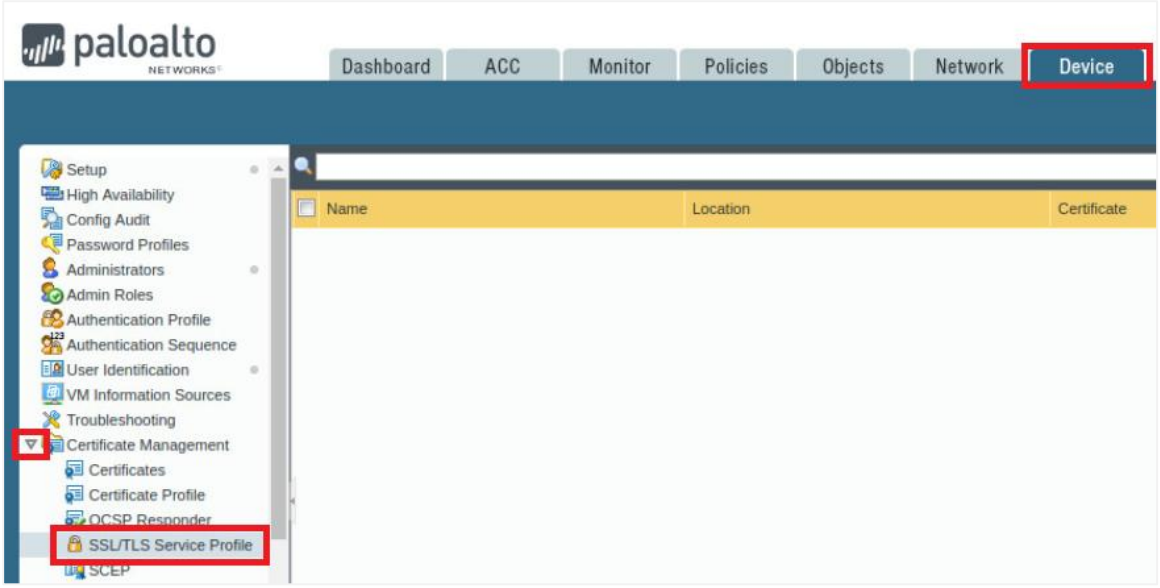
9. Verify that your configuration looks like the following.

| Name | Subject | Issuer | CA | Key |
|---|---|---|---|---|
| GlobalProtect | CN = GlobalProtect | CN = GlobalProtect | ✓ | ✓ |
| external-gw-portal | CN = 203.0.113.20 | CN = GlobalProtect | | ✓ |
| internal-gw | CN = 192.168.2.1 | CN = GlobalProtect | | ✓ |

10. Leave the firewall web interface open to continue with the next task.

## 10.3 Configure the SSL-TLS Service Profile

1. In the web interface, navigate to **Device > Certificate Management > SSL/TLS Service Profile**.

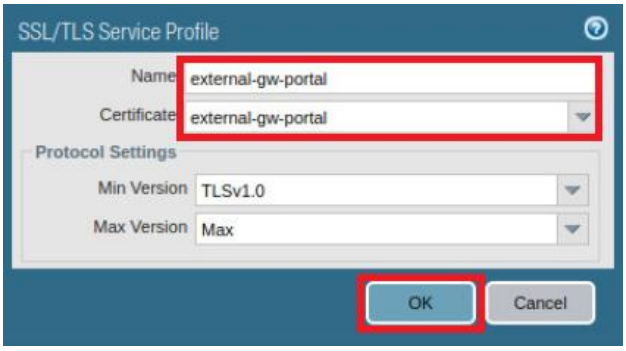



2. Click **Add** to create an *SSL/TLS Service Profile*.

3. In the *SSL/TLS Service Profile* window, fill the form with the following data and then click **OK**.

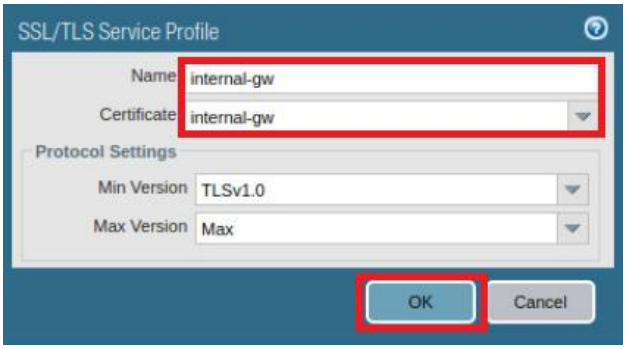
| Parameter | Value |
|---|---|
| Name | Type `external-gw-portal` |
| Certificate | Select **external-gw-portal** from the dropdown list |




This *SSL-TLS Service Profile* defines the certificate to present to the *GlobalProtect* client agent when the agent initially connects to the *GlobalProtect* portal. The firewall will present this same certificate when the agent software connects to an external gateway.

4. Click **Add** to create another *SSL/TLS Service Profile*. Fill the form with the following data and then click **OK**.

| Parameter | Value |
|---|---|
| Name | Type `internal-gw` |
| Certificate | Select **internal-gw** from the dropdown list |




This *SSL-TLS Service Profile* defines the certificate to present to the *GlobalProtect* client agent when the agent connects to an internal *GlobalProtect* gateway.

5. Verify that your configuration looks like the following.

| Name | Location | Certificate | Protocol Versions |
|---|---|---|---|
| external-gw-portal | | external-gw-portal | Min Version: TLSv1.0<br>Max Version: Max |
| internal-gw | | internal-gw | Min Version: TLSv1.0<br>Max Version: Max |

These entries instruct the firewall to use the appropriate certification when communicating with the *GlobalProtect* agent software. We have one certificate to use when the client connects to the portal or to an external gateway; and a second certificate to use when the client connects to an internal gateway.

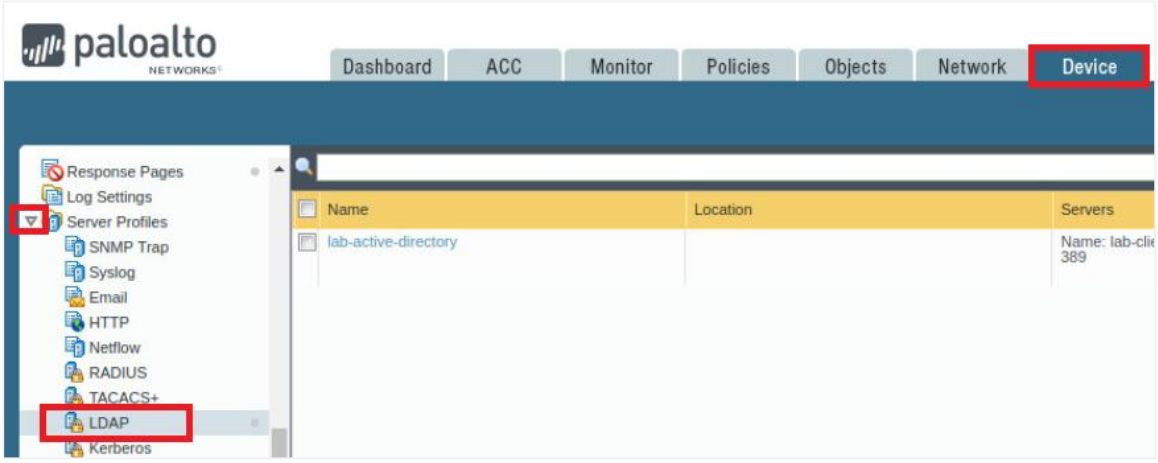
6. Leave the firewall web interface open to continue with the next task.

## 10.4 Configure the LDAP Server Profile

In this task, you define the server that the firewall will use to authenticate users when they invoke the *GlobalProtect* agent software. When the software agent connects to the portal, the firewall must authenticate the user. Separately, when the software agent connects to a gateway to establish a VPN, the firewall must authenticate the user.

1. In the web interface, navigate to **Device > Server Profiles > LDAP**.




2. Click on **lab-active-directory** to open the *LDAP Server Profile*.


3. In the *LDAP Server Profile* window, verify the following information.

| Parameter | Value |
|---|---|
| Name | `lab-active-directory` |

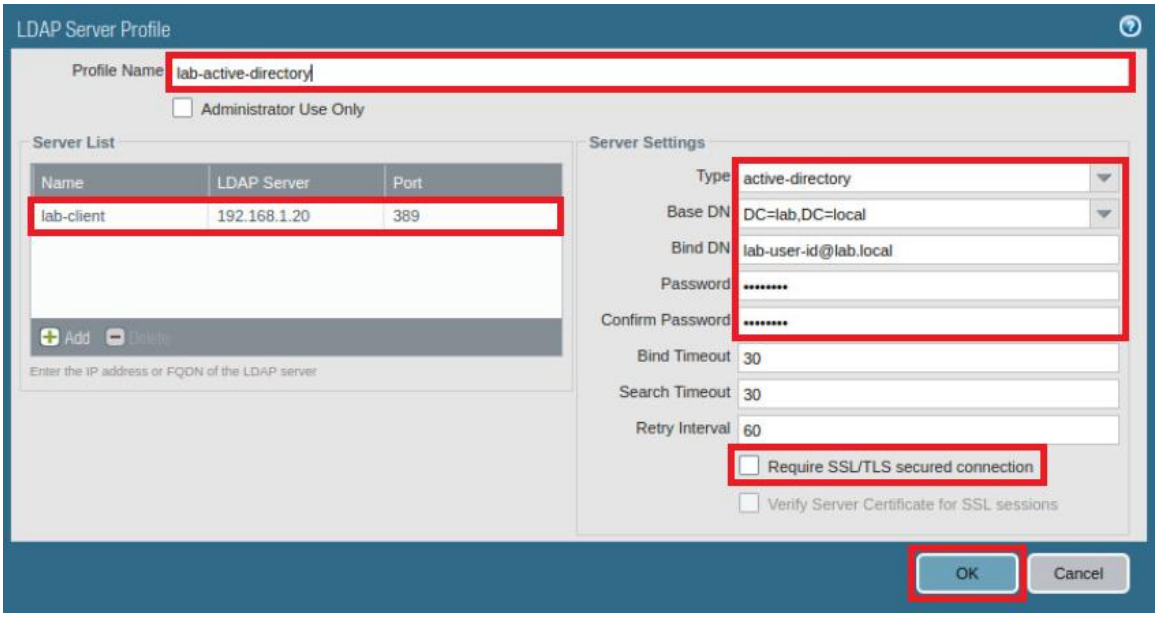
4. In the *LDAP Server Profile* window, locate the **Server List** pane and verify the following.

| Parameter | Value |
|---|---|
| Name | **lab-client** |
| LDAP Server | **192.168.1.20** |
| Port | **389** |

5. In the *LDAP Server Profile* window, locate the **Server Settings** pane and verify the following. Re-enter the password as shown to ensure it is correct. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Type | `active-directory` |
| Base DN | `DC=lab,DC=local` |
| Bind DN | `lab-user-id@lab.local` |
| Password | `Pal0Alt0` |
| Require SSL/TLS secured connection | Deselect the checkbox |



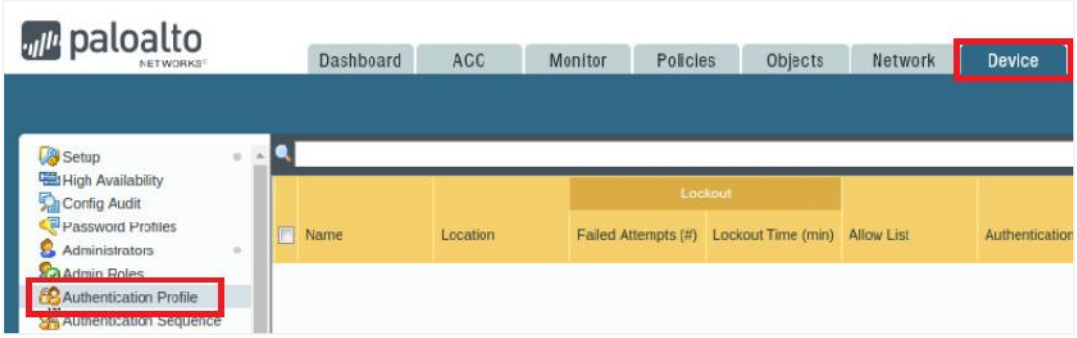

6. Leave the firewall web interface open to continue with the next task.

## 10.5 Configure the Authentication Profile

In this task, you will configure an *Authentication Profile* that contains the *LDAP Server Profile*. You will reference this profile to tell the firewall how to authenticate users accessing the *GlobalProtect* portal or the gateway.

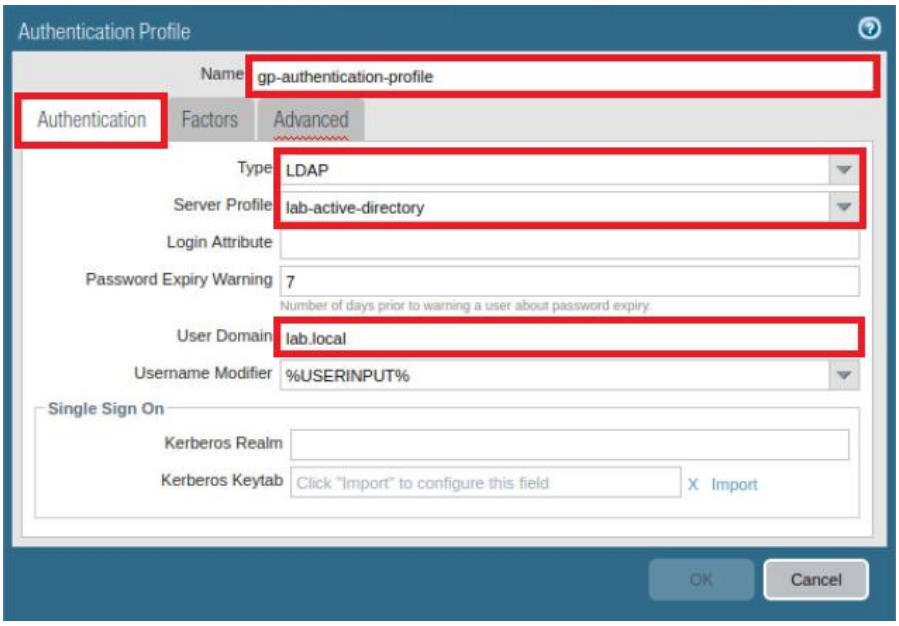
1. In the web interface, navigate to **Device > Authentication Profile**.




2. Click **Add** to create a new *Authentication Profile*.


3. In the *Authentication Profile* window, while on the *Authentication* tab, configure the following.

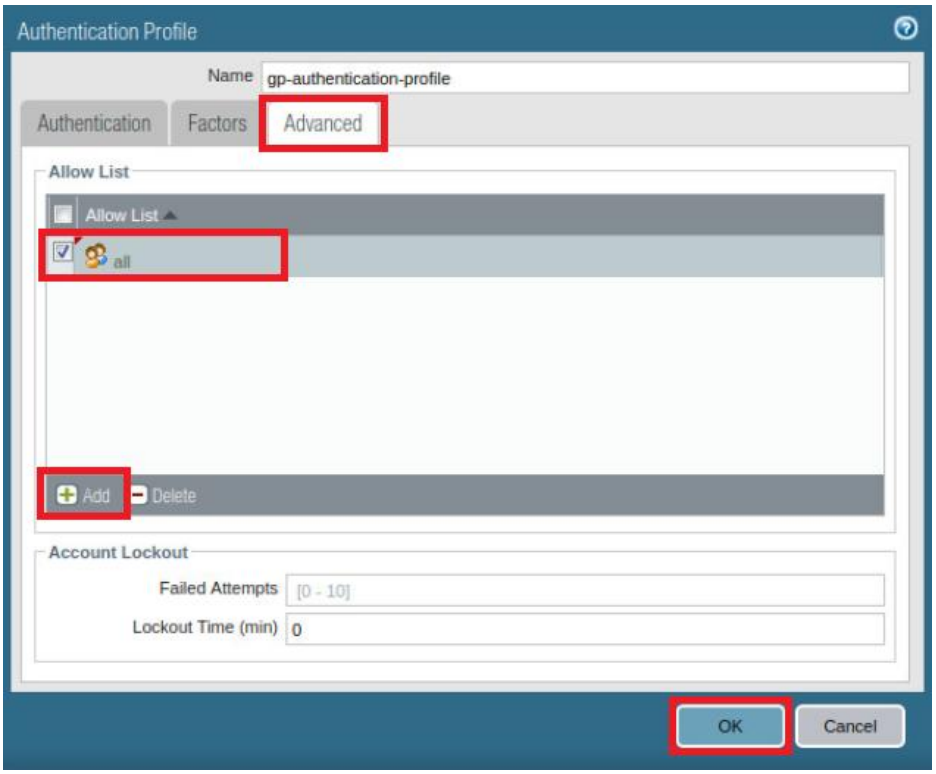
| Parameter | Value |
|---|---|
| Name | Type `gp-authentication-profile` |
| Type | Select **LDAP** from the dropdown list |
| Server Profile | Select **lab-active-directory** from the dropdown list |
| User Domain | Type `lab.local` |



4. In the *Authentication Profile* window, click the **Advanced** tab and configure the following, then click **OK**.

| Parameter | Value |
|---|---|
| Allow List | Click **Add** and select **all** |




5. Leave the firewall web interface open to continue with the next task.

## 10.6 Configure the Tunnel Interface

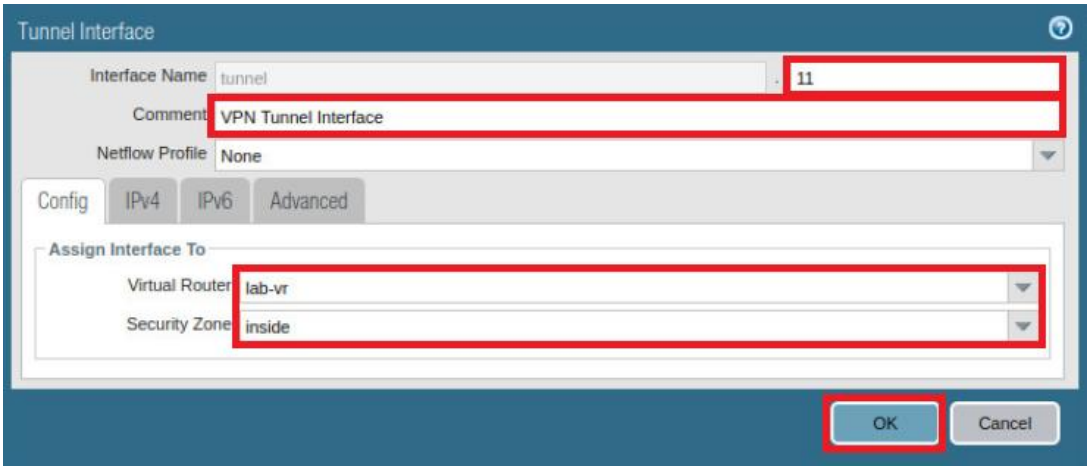
The *GlobalProtect* client agent software uses a VPN tunnel when it establishes a secure connection to the gateway, and the firewall uses a logical tunnel for encrypting and decrypting traffic with the client.

1. In the web interface, navigate to **Network > Interfaces > Tunnel**.


2. Click **Add** to create a new tunnel interface.


3. In the *Tunnel Interface* window, configure the following and then click **OK**.

| Parameter | Value |
|---|---|
| Interface Name | Type `11` in the second text field |
| Comment | Type `VPN Tunnel Interface` |
| Virtual Router | Select **lab-vr** from the dropdown list |
| Security Zone | Select **inside** from the dropdown list |




> The logical tunnel interface is connected to a virtual router and assigned to a security zone just as are other interfaces

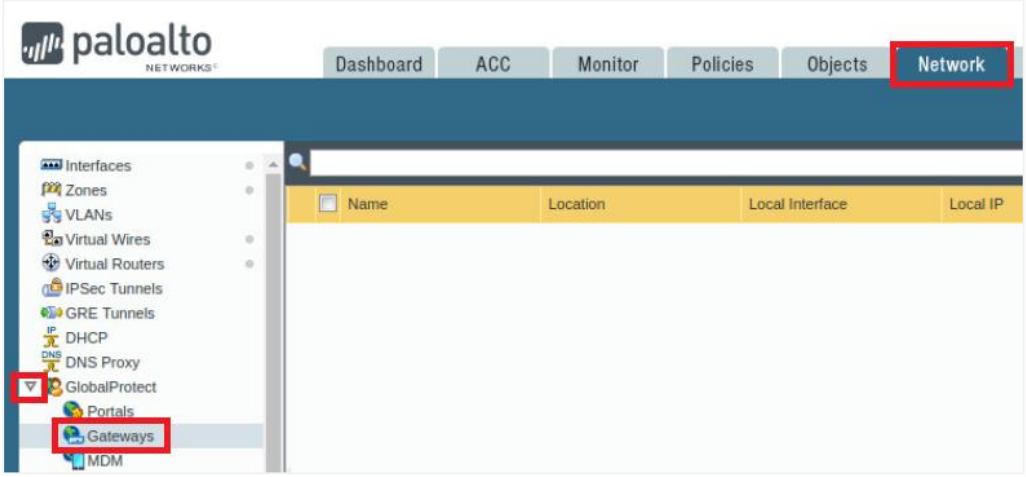
4. Leave the firewall web interface open to continue with the next task.

## 10.7 Configure the Internal Gateway

Internal gateways can be used for User-ID deployment and host information profile (HIP) enforcement. They also can be used to encrypt traffic from the client to sensitive internal resources through a VPN gateway.

1. In the web interface, navigate to **Network > GlobalProtect > Gateways**.




2. Click **Add** to create a gateway.

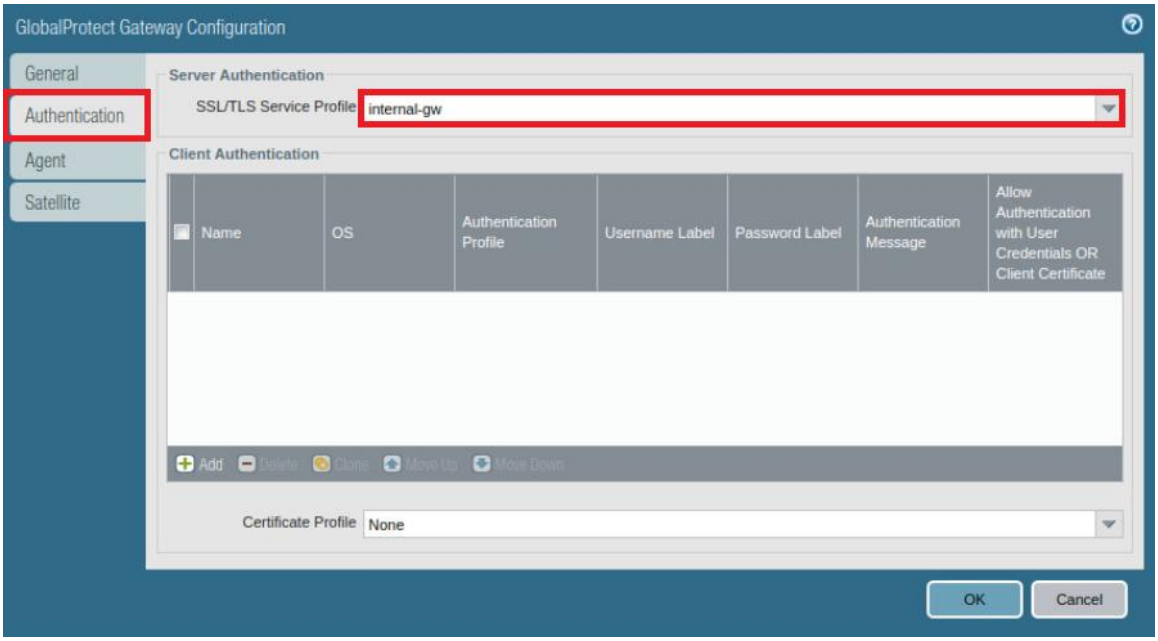

3. In the *GlobalProtect Gateway Configuration* window, while on the *General* tab, configure the following.

| Parameter | Value |
|---|---|
| Name | Type `gp-int-gateway` |
| Interface | Select **ethernet1/2.2** from the dropdown list |
| IPv4 Address | Select **192.168.2.1/24** from the dropdown list |

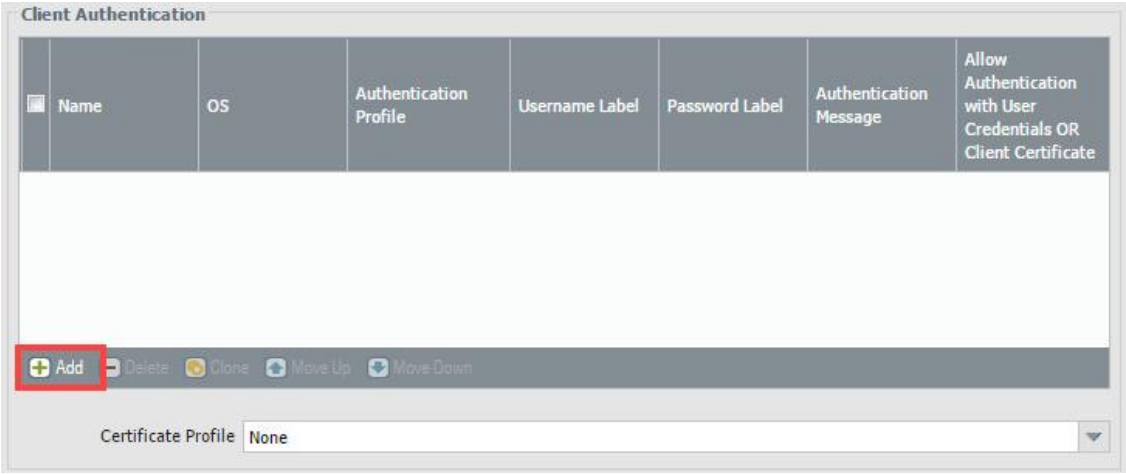

  

4. In the *GlobalProtect Gateway Configuration* window, click on the **Authentication** tab and configure the following.

| Parameter | Value |
|---|---|
| SSL/TLS Service Profile | Select **internal-gw** from the dropdown list |



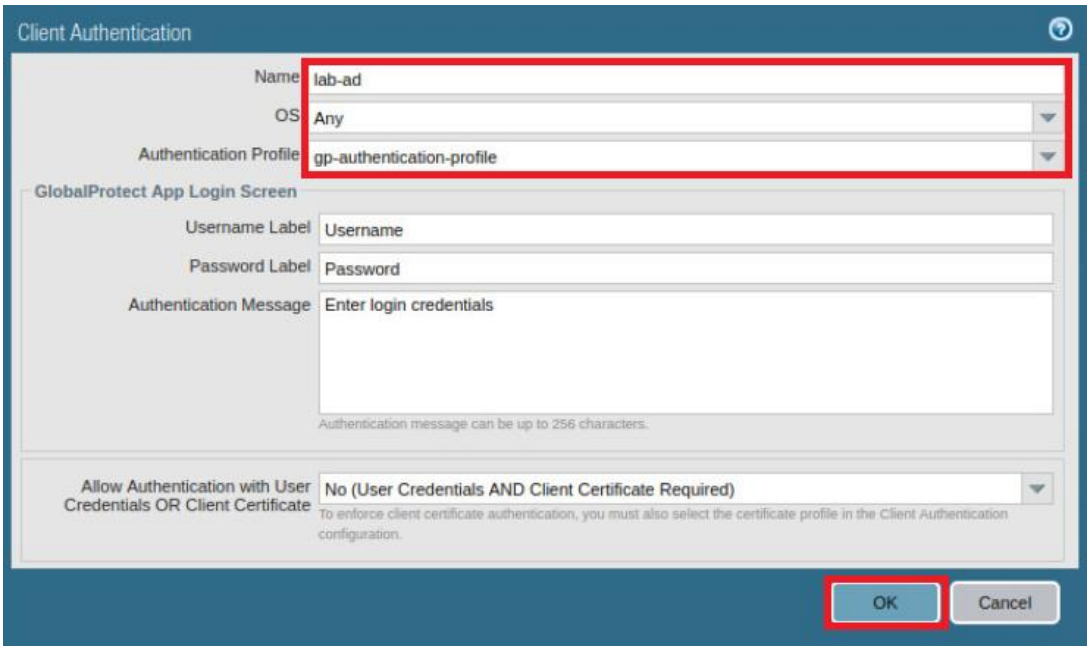

5. Locate the **Client Authentication** pane and click **Add**.



6. In the *Client Authentication* window, configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Name | Type `lab-ad` |
| OS | Verify that **Any** is selected |
| Authentication Profile | Select **gp-authentication-profile** from the dropdown list |




This area lets you configure different authentication methods for different sets of users based on the operating system in use for the *GlobalProtect* client agent software.

7. Back on the *GlobalProtect Gateway Configuration* window, click **OK**.
8. Leave the firewall web interface open to continue with the next task.

## 10.8 Configure the External Gateway

In this task, you will create the external *GlobalProtect* gateway.

1. Click **Add** to create a second gateway.

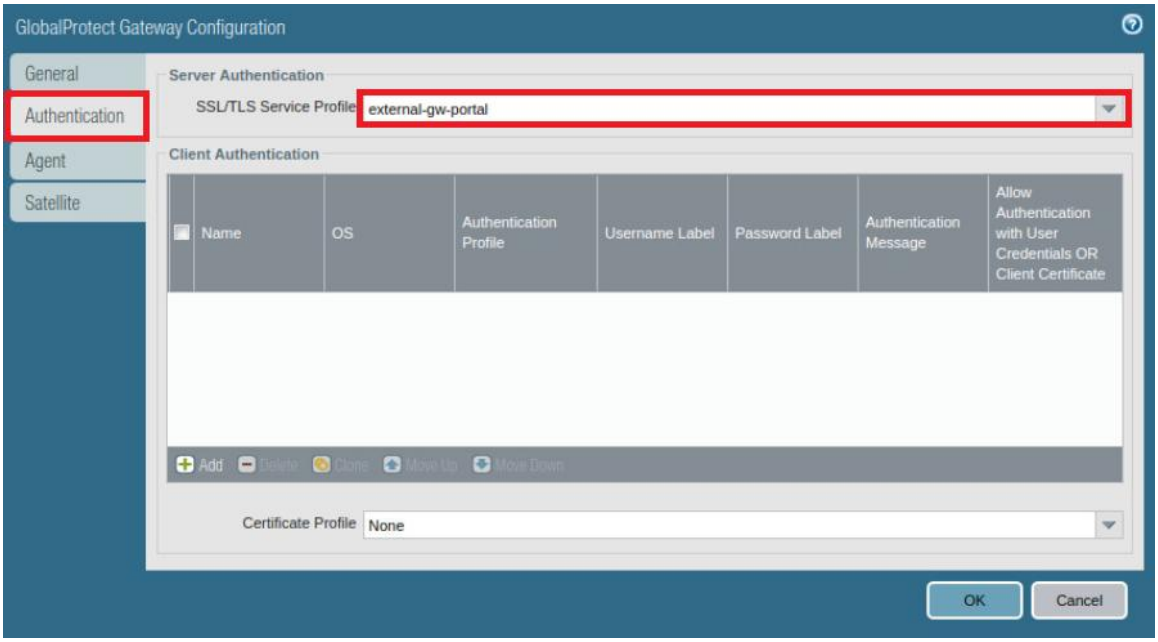

2. In the *GlobalProtect Gateway Configuration* window, while on the *General* tab, configure the following.

| Parameter | Value |
|---|---|
| Name | Type `gp-ext-gateway` |
| Interface | Select **ethernet1/1** from the dropdown list |
| IPv4 Address | Select **203.0.113.20/24** from the dropdown list |


3. In the *GlobalProtect Gateway Configuration* window, click on the **Authentication** tab and configure the following.

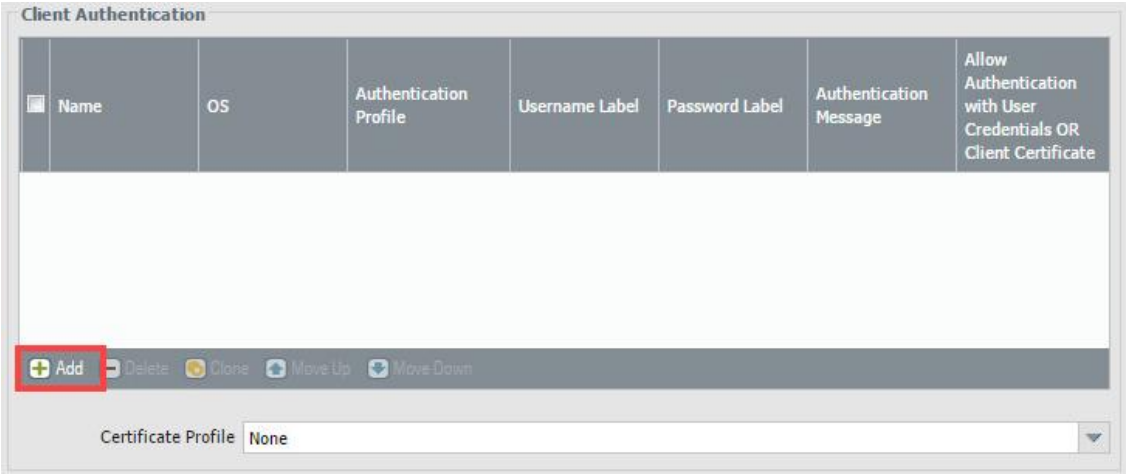
| Parameter | Value |
|---|---|
| SSL/TLS Service Profile | Select **external-gw-portal** from the dropdown list |




This section defines the certificates to present to the client when it connects to the gateway. Remember that we created a single *SSL/TLS Service Profile* for the portal and for the external gateway.

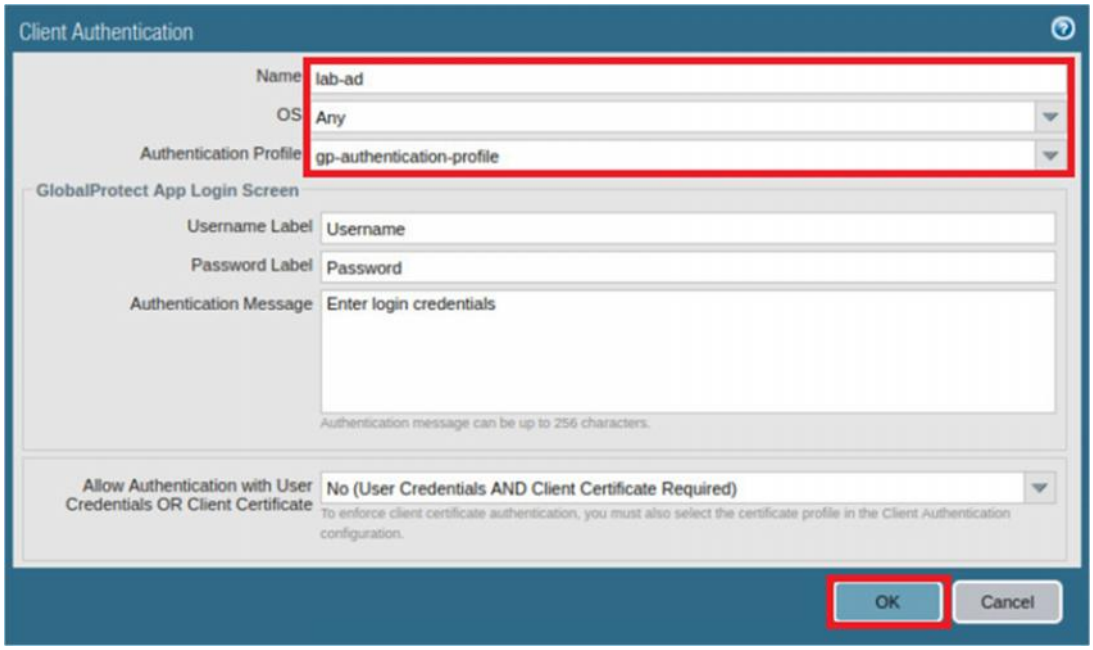
4. Locate the **Client Authentication** pane and click **Add**.



5. In the *Client Authentication* window, configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Name | Type `lab-ad` |
| OS | Verify that **Any** is selected |
| Authentication Profile | Select **gp-authentication-profile** from the dropdown list |

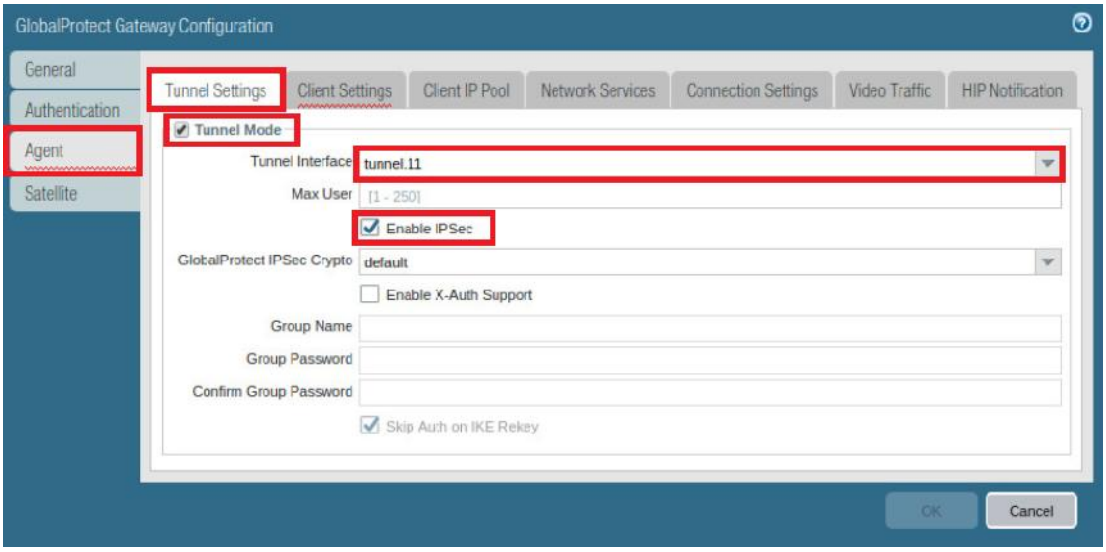



This section allows you to select different authentication methods (*Authentication Profiles*) based on the operating system of client hosts.

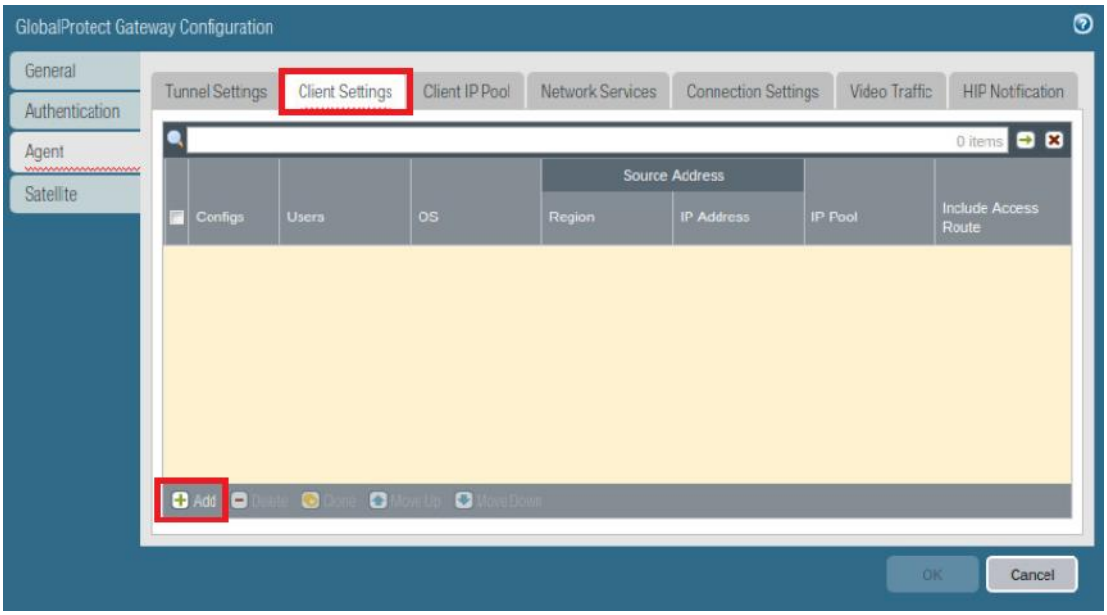
6. In the *GlobalProtect Gateway Configuration* window, click the **Agent** tab and the **Tunnel Settings** subtab configure the following.

| Parameter | Value |
|---|---|
| Tunnel Mode | Select the checkbox |
| Tunnel Interface | Select **tunnel.11** from the dropdown list |
| Enable IPSec | Verify that the **Enable IPSec** checkbox is selected |

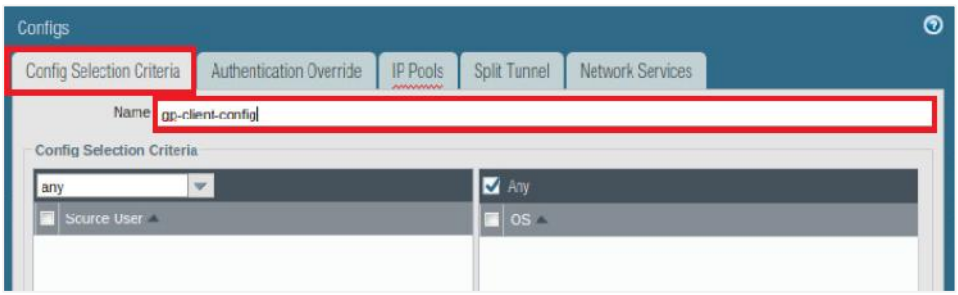
  




7. In the *GlobalProtect Gateway Configuration* window, click the **Client Settings** subtab, then click **Add**.




8. In the *Configs* window, under the **Config Selection Criteria** tab, type **`gp-client-config`** in the *Name* text field.



After a client has been authenticated to establish a VPN with a gateway, these settings define which IP address and other network elements the *GlobalProtect* client adapter will use.

9. Click the **IP Pools** tab and configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| IP Pool | Click **Add** and type `192.168.100.200-192.168.100.210` |


The firewall will assign an IP address to each *GlobalProtect* client from this range of addresses.

10. Back on the *GlobalProtect Gateway Configuration* window, click the **Network Services** subtab to configure the following and then click **OK**.

| Parameter | Value |
|---|---|
| Primary DNS | Type `4.2.2.2` |
| Secondary DNS | Type `8.8.8.8` |


The servers used in the lab are public, but in many cases the DNS servers that are assigned to the *GlobalProtect* client adapter will be private, internal DNS hosts. This setting will allow the client to resolve internal hostnames while connected to the VPN.

11. Verify that your configuration looks like the following:

| | Name | Location | Local Interface | Local IP | Tunnel |
|---|---|---|---|---|---|
| ⊞ | gp-int-gateway | | ethernet1/2.2 | 192.168.2.1/24 | |
| ⊞ ☑ | gp-ext-gateway | | ethernet1/1 | 203.0.113.20/24 | tunnel.11 |

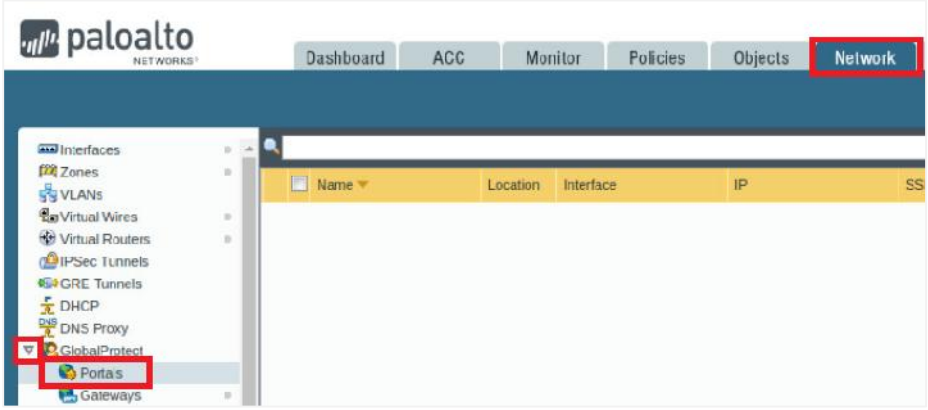
12. Leave the firewall web interface open to continue with the next task.

## 10.9 Configure the Portal

The *GlobalProtect* portal provides the management functions for the *GlobalProtect* infrastructure. Every endpoint that participates in the *GlobalProtect* network receives its configuration from the portal, including information about the available *GlobalProtect* gateways and any optional client certificates that might be necessary for the client to connect to a gateway.

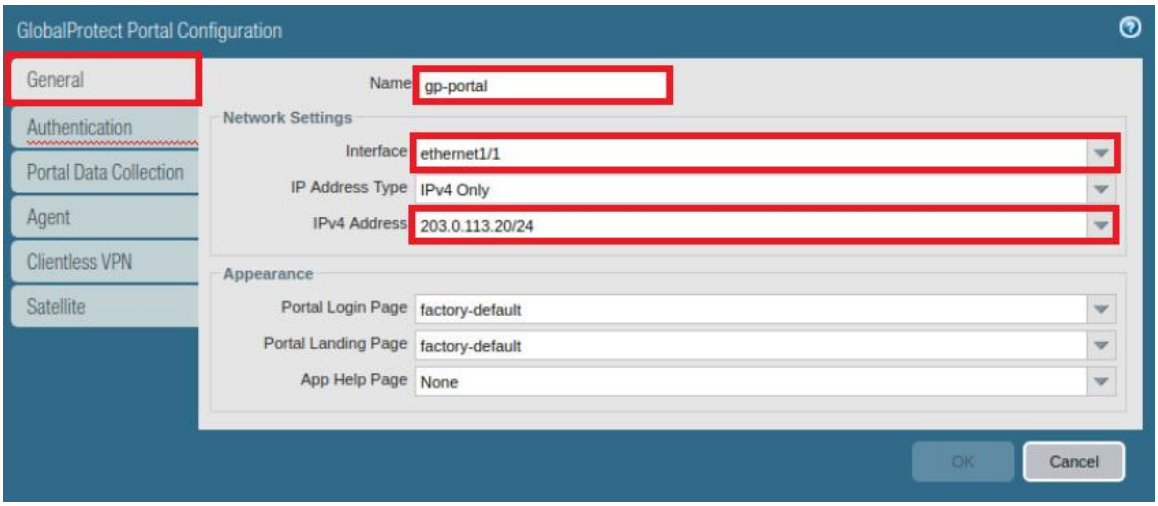
1. In the web interface, select **Network > GlobalProtect > Portals**.




2. Click **Add** to create a new portal.


3. In the *GlobalProtect Portal Configuration* window, while on the **General** tab, configure the following.

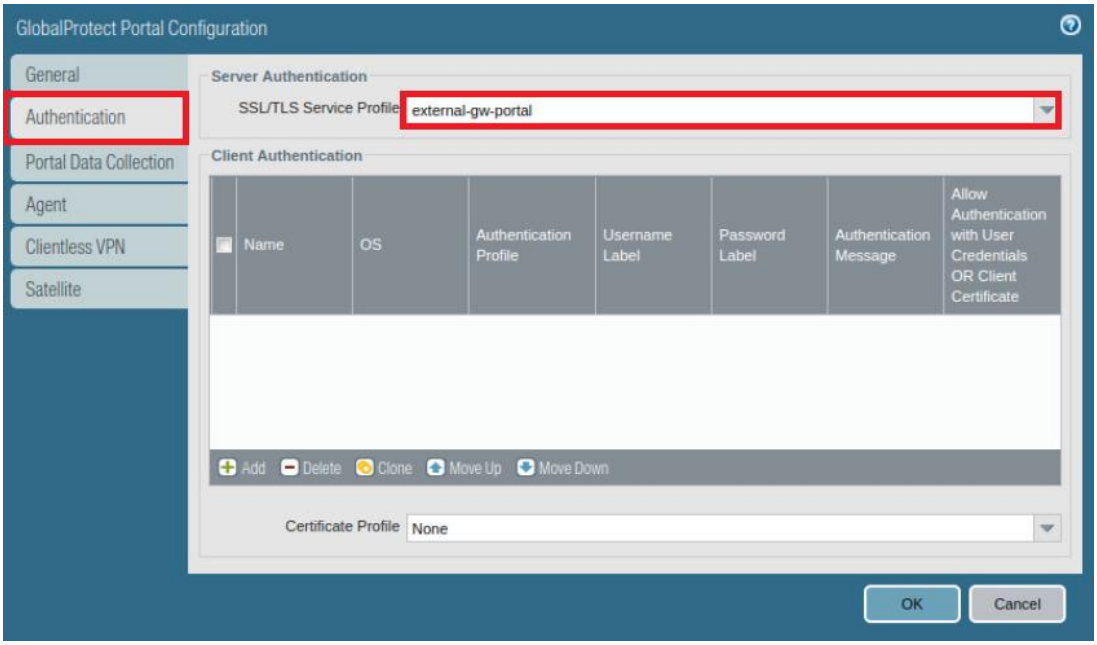
| Parameter | Value |
|---|---|
| Name | Type `gp-portal` |
| Interface | Select **ethernet1/1** from the dropdown list |
| IPv4 Address | Select **203.0.113.20/24** from the dropdown list |



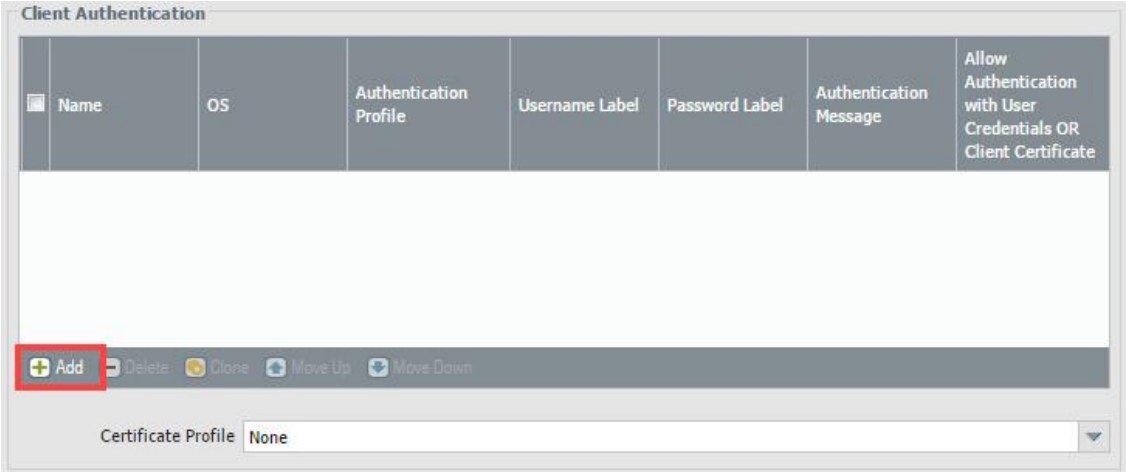

  

4. In the *GlobalProtect Portal Configuration* window, click the **Authentication** tab and configure the following.

| Parameter | Value |
|---|---|
| SSL/TLS Service Profile | Select **external-gw-portal** from the dropdown list |



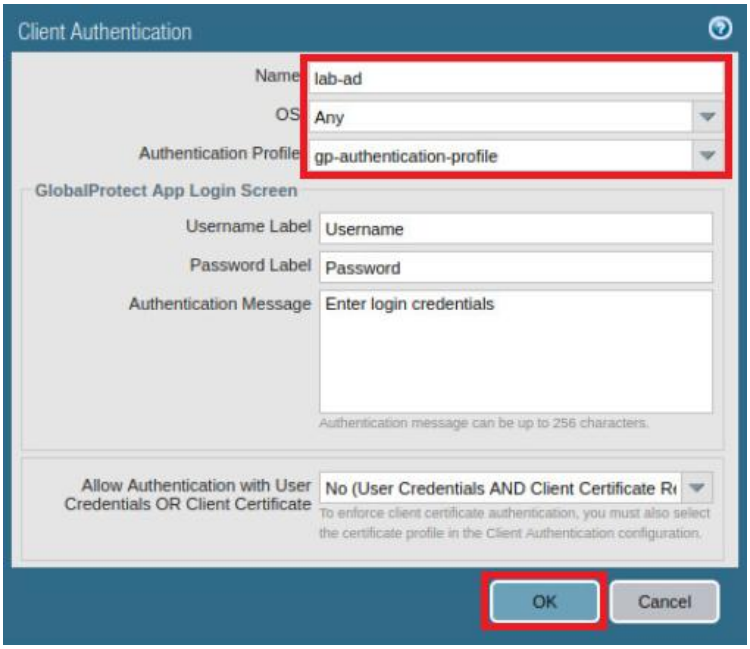

5. Locate the **Client Authentication** pane and click **Add**.




6. In the *Client Authentication* window, configure the following. Once finished, click **OK**.

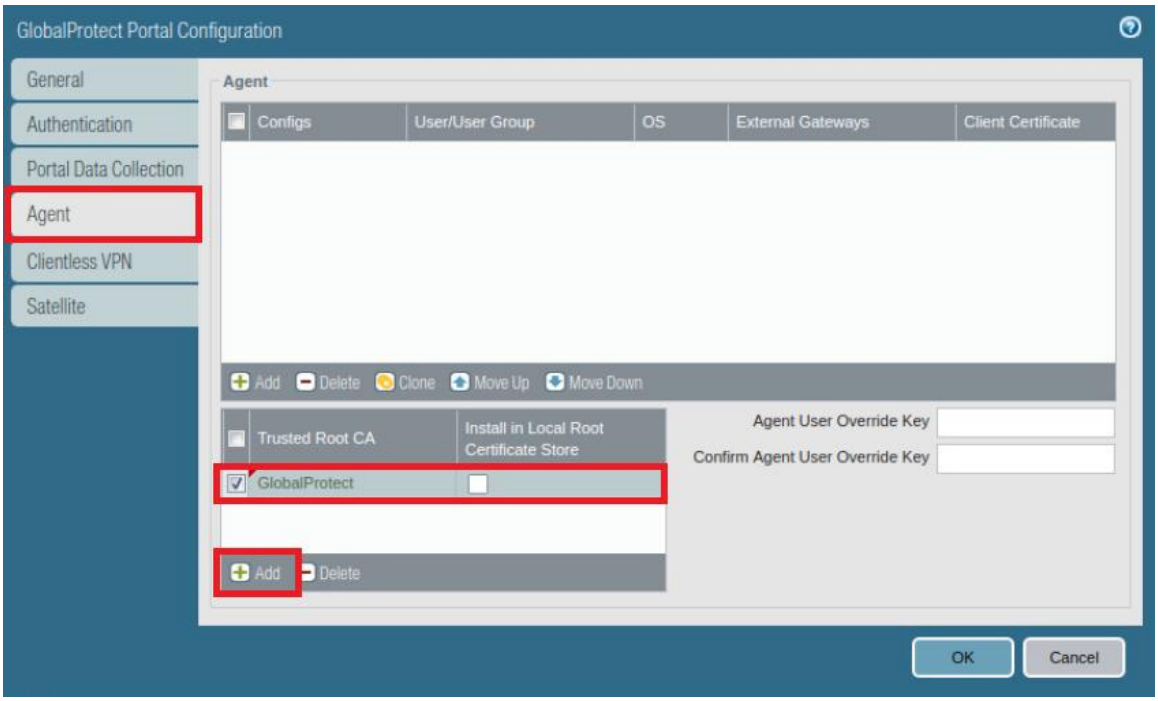
| Parameter | Value |
|---|---|
| Name | Type **`lab-ad`** |
| OS | Verify that **Any** is selected |
| Authentication Profile | Select **gp-authentication-profile** from the dropdown list |




In this section, the portal is being configured to authenticate users against the *auth-gp* profile that contains our LDAP server.

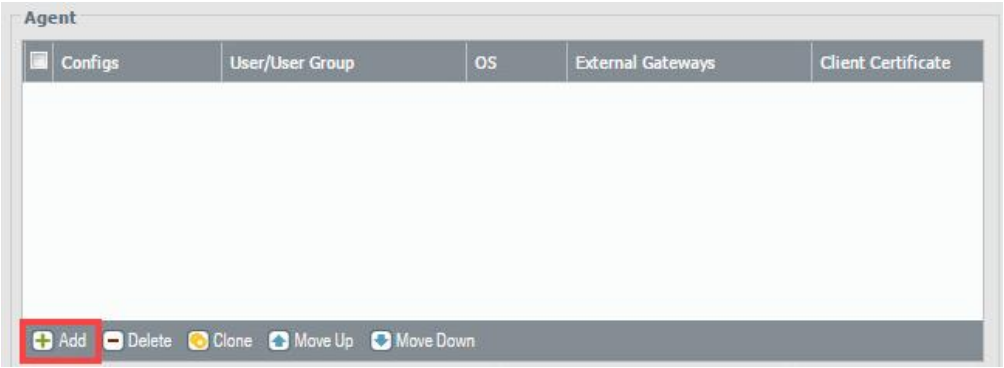
7. In the *GlobalProtect Gateway Configuration* window, click the **Agent** tab.
8. Locate the *Trusted Root CA* pane and click **Add**. Select the **GlobalProtect** certificate from the dropdown list.



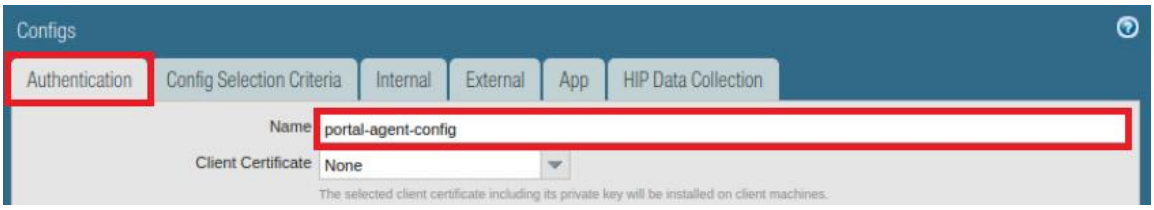

  

This is the certificate we used to sign the portal certificate and the gateway certificate. By placing it in this section, we can push this signing certificate down to the client's trusted certificate store through the *GlobalProtect* connection. This CA is at the top of the chain of trust, so the client host will trust any certificate signed by this one, including the portal and gateway certificates.

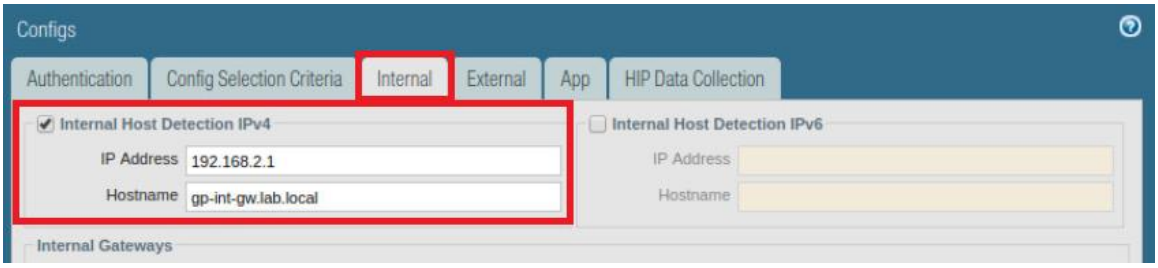
9. Locate the *Agent* list box and click **Add** to open the *Configs* window.




10. In the *Configs* window, while on the **Authentication** tab, type **`portal-agent-config`** in the *Name* text field.

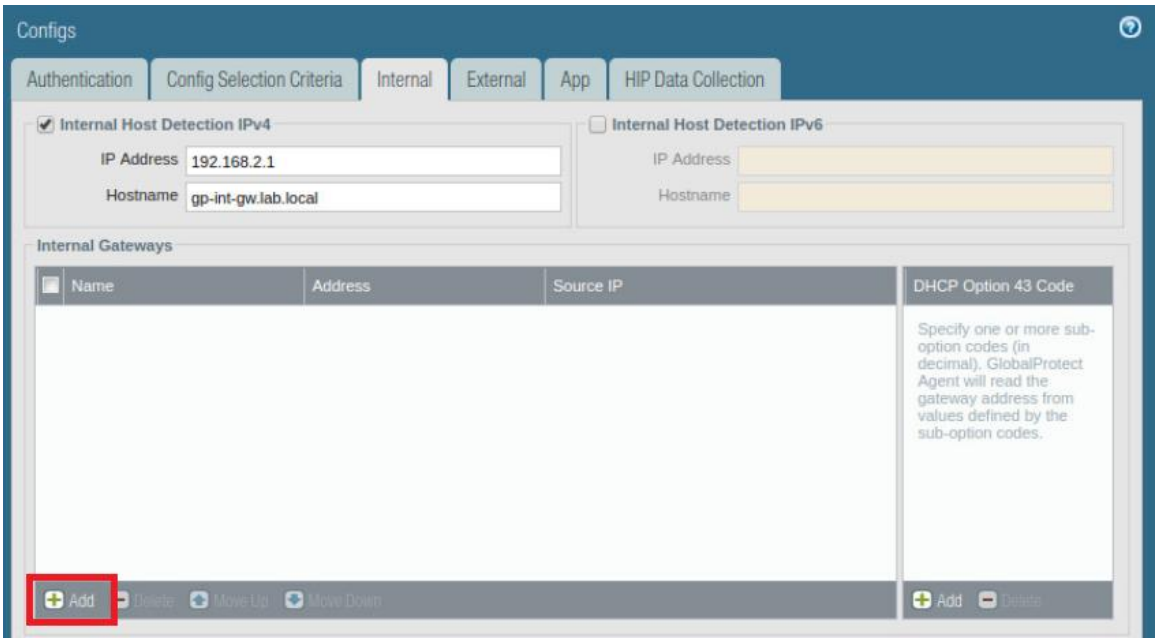



11. Click the **Internal** tab and select the **Internal Host Detection IPv4** checkbox. Type **`192.168.2.1`** in the *IP Address* field and then type **`gp-int-gw.lab.local`** in the *Hostname* text field.



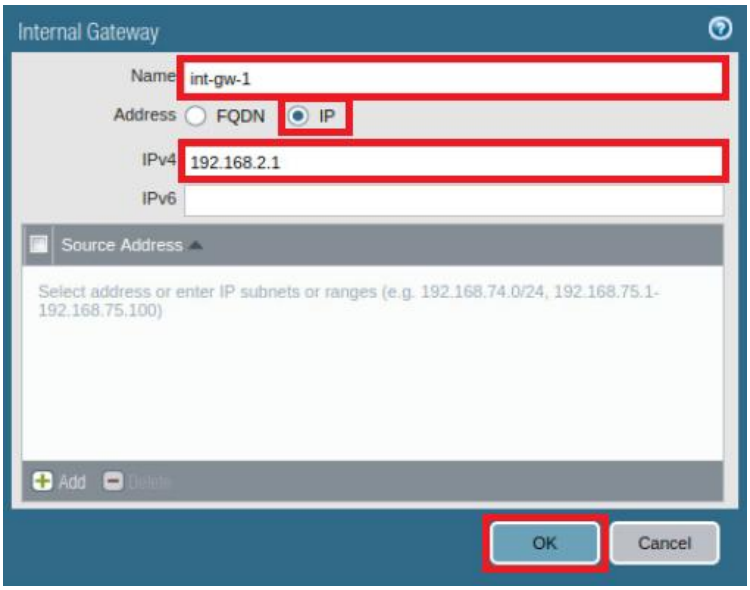

  

12. Locate the *Internal Gateways* pane and click **Add**.



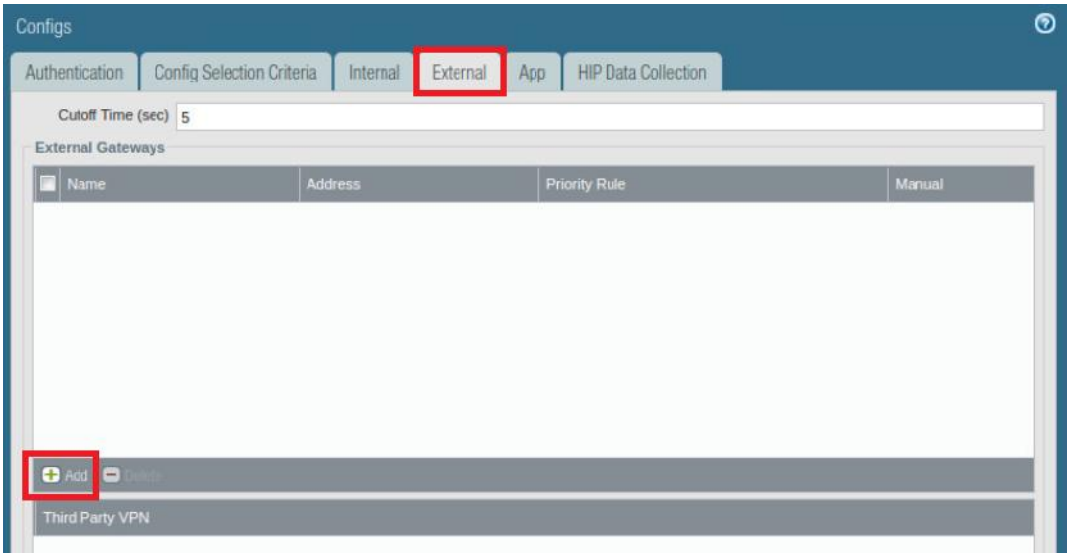

13. In the *Internal Gateway* window, configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Name | Type `int-gw-1` |
| Address | Select the **IP** radio button |
| IPv4 | Type `192.168.2.1` |



14. Back on the *Configs* window, click the **External** tab, locate the **External Gateways** list box and click **Add**.



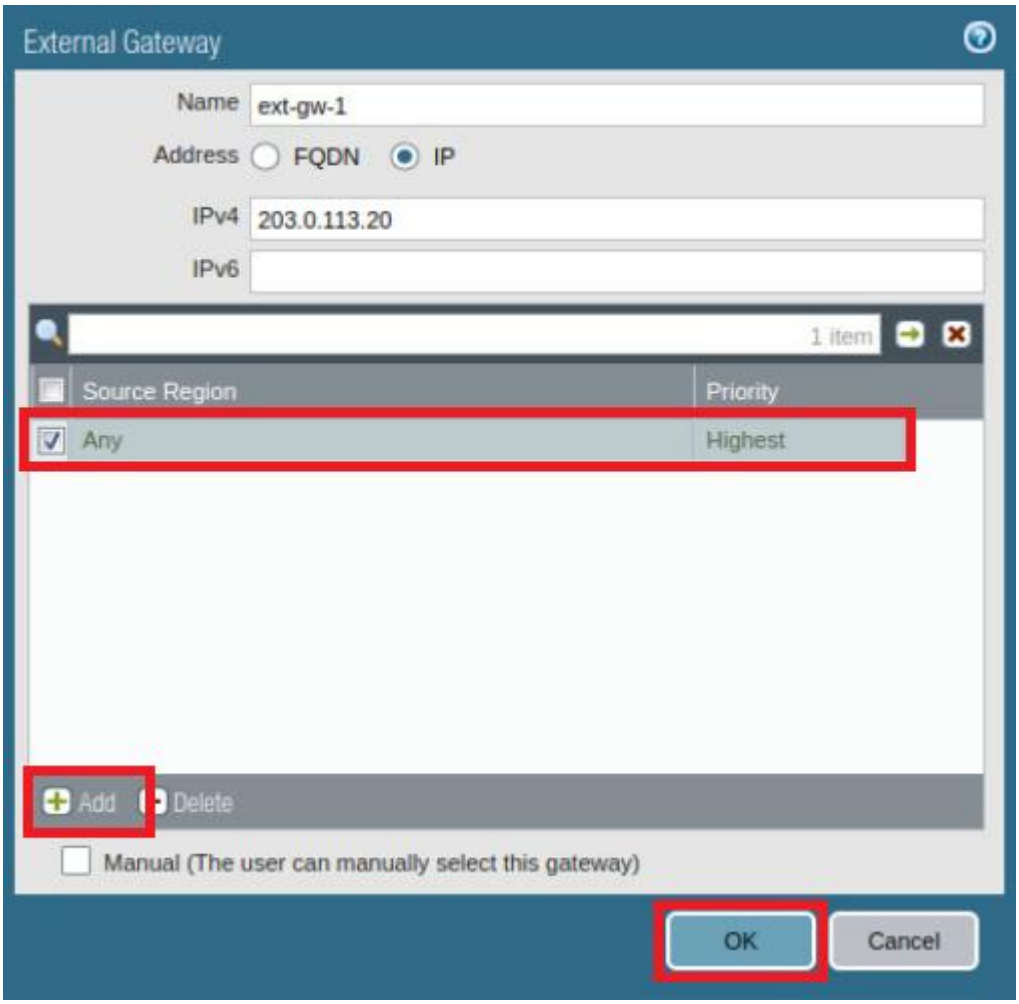

15. In the *External Gateway* window, configure the following.

| Parameter | Value |
|---|---|
| Name | Type **`ext-gw-1`** |
| Address | Select the **IP** radio button |
| IPv4 | Type **`203.0.113.20`** |


16. In the *External Gateway* window, locate the *Source Region* pane and click **Add** to configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Source Region | Select **Any** from the dropdown list |
| Priority | Verify that **Highest** is selected |




The *Source Region* options allow you to prioritize that the external gateway that a client connects to be based on the geographic assignment of a client's IP address. We have only a single external gateway, so we are setting *Source Region* to *Any* so that all clients connect to this gateway, regardless of their IP address.

17. Click **OK** to close the *Configs* window.
18. Click **OK** again to close the *GlobalProtect Portal Configuration* window.
19. A new *GlobalProtect* gateway should appear in the web interface. Click the **plus icon** to expand the entry view and verify that your configuration looks like the following.

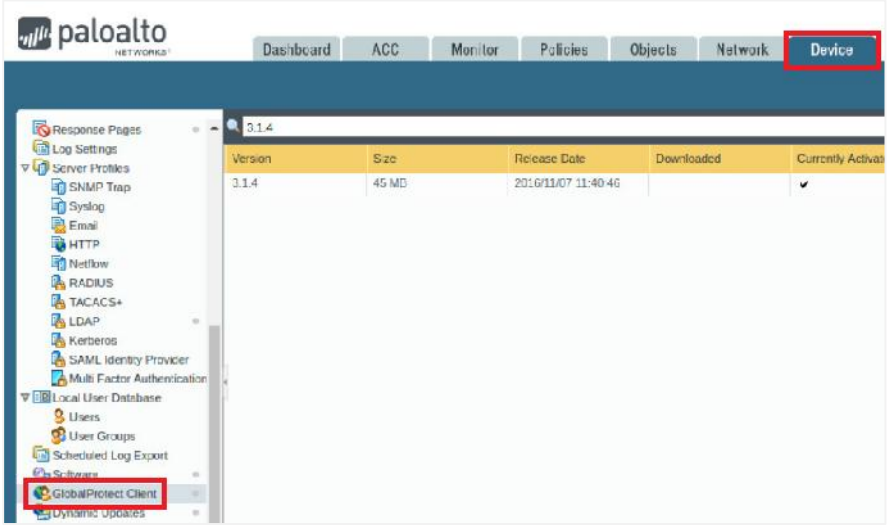

20. Leave the firewall web interface open to continue with the next task.

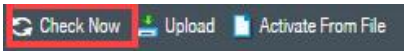
## 10.10 Host the GlobalProtect Agent on the Portal

To make the progress of obtaining and installing the *GlobalProtect* agent software easier for users, you will download a specific version and activate it on the portal. Activation of the *GlobalProtect* agent software allows users to connect to a webpage on the portal and download the appropriate version of the client software for their host operating system.

1. In the web interface, select **Device > GlobalProtect Client**.




2. Click **Check Now** located near the bottom of the page.



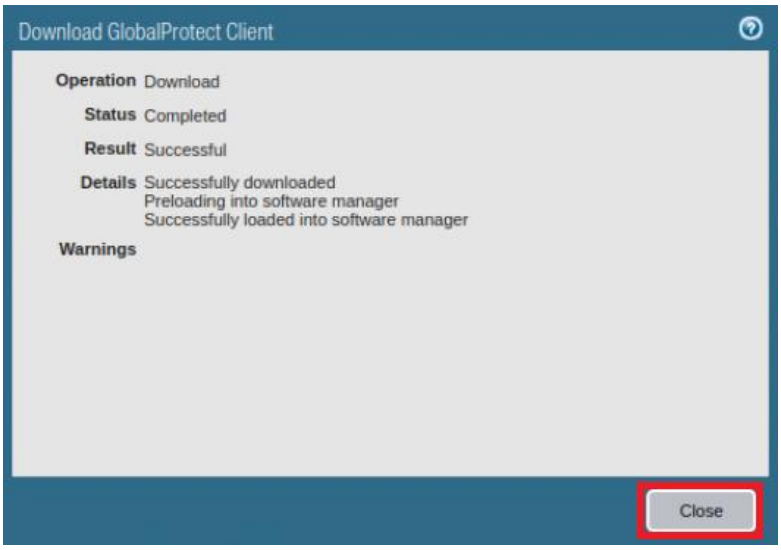

3. Notice the *Palo Alto Networks* firewall checks for the latest version of the *GlobalProtect* agent. Clear any existing filters and locate version **5.0.0**. Click **Download** underneath the *Action* column.

| Version | Size | Release Date | Downloaded | Currently Activated | Action |
|---|---|---|---|---|---|
| 5.1.1 | 57 MB | 2020/02/24 15:02:59 | | | Download |
| 5.1.0 | 57 MB | 2019/12/12 12:55:31 | | | Download |
| 5.0.8 | 59 MB | 2020/01/30 15:04:01 | | | Download |
| 5.0.7 | 59 MB | 2019/12/19 07:17:51 | | | Download |
| 5.0.6 | 59 MB | 2019/12/05 11:25:24 | | | Download |
| 5.0.5 | 59 MB | 2019/10/14 10:40:12 | | | Download |
| 5.0.4 | 59 MB | 2019/08/15 16:20:49 | | | Download |
| 5.0.3 | 59 MB | 2019/07/03 13:57:07 | | | Download |
| 5.0.2 | 59 MB | 2019/05/07 11:07:02 | | | Download |
| 5.0.1 | 59 MB | 2019/03/11 16:23:18 | | | Download |
| 5.0.0 | 58 MB | 2019/02/11 14:22:59 | | | Download |
| 4.1.13 | 59 MB | 2019/10/14 14:33:51 | | | Download |

After a new version of the *GlobalProtect* client software is released, you can download it through this interface and activate it. Any users currently running an older version of the *GlobalProtect* software will be upgraded to the new version when they connect to the portal.

4. Once the download completes, click **Close**.

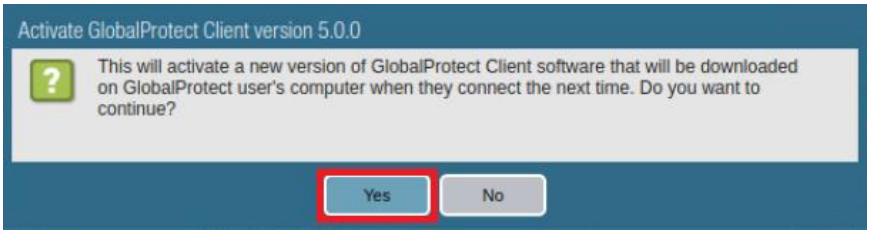



5. Click **Activate** in the *Action* column for the **5.0.0** version.

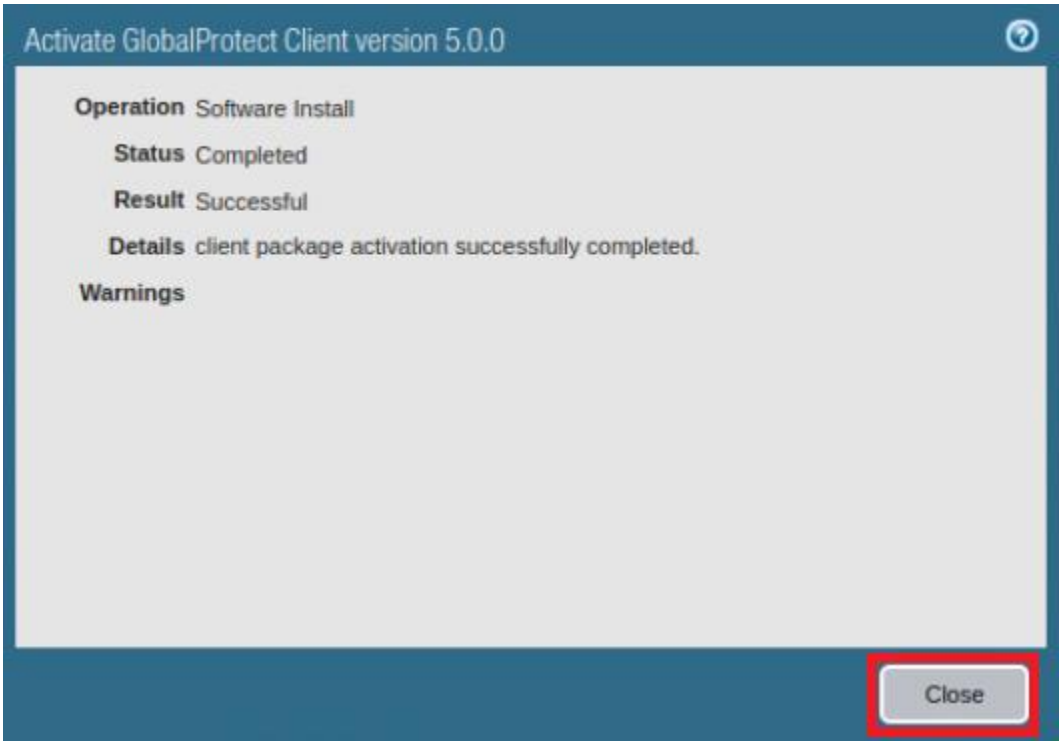
| Version | Size | Release Date | Downloaded | Currently Activated | Action |
|---|---|---|---|---|---|
| 5.1.1 | 57 MB | 2020/02/24 15:02:59 | | | Download |
| 5.1.0 | 57 MB | 2019/12/12 12:55:31 | | | Download |
| 5.0.8 | 59 MB | 2020/01/30 15:04:01 | | | Download |
| 5.0.7 | 59 MB | 2019/12/19 07:17:51 | | | Download |
| 5.0.6 | 59 MB | 2019/12/05 11:25:24 | | | Download |
| 5.0.5 | 59 MB | 2019/10/14 10:40:12 | | | Download |
| 5.0.4 | 59 MB | 2019/08/15 16:20:49 | | | Download |
| 5.0.3 | 59 MB | 2019/07/03 13:57:07 | | | Download |
| 5.0.2 | 59 MB | 2019/05/07 11:07:02 | | | Download |
| 5.0.1 | 59 MB | 2019/03/11 16:23:18 | | | Download |
| 5.0.0 | 58 MB | 2019/02/11 14:22:59 | ✔ | | Activate |
| 4.1.13 | 59 MB | 2019/10/14 14:33:51 | | | Download |

6. When prompted, click **Yes** to close the *Activate GlobalProtect Client version* message.




7. After successful completion, click **Close**.




8. Leave the firewall web interface open to continue with the next task.

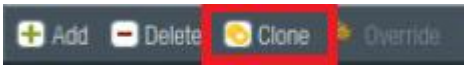
  

## 10.11 Create Security Policy Rule

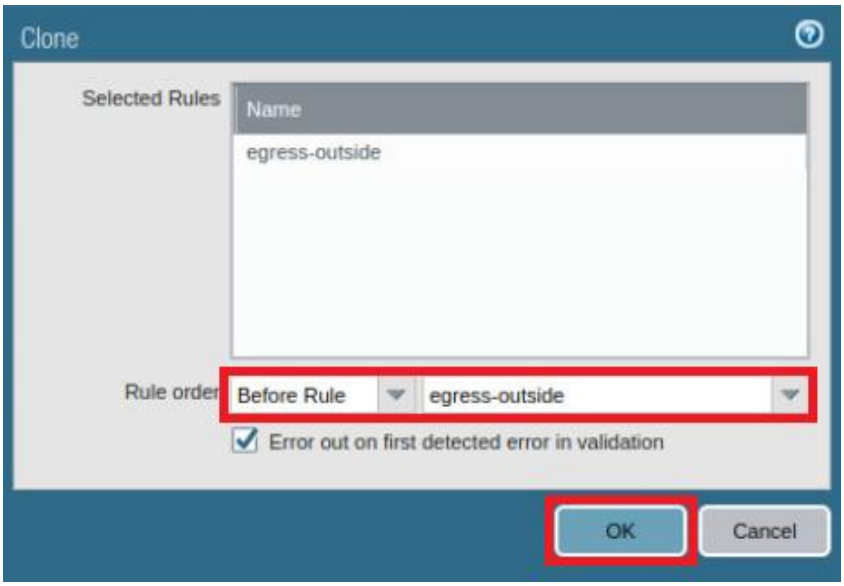
1. In the web interface, navigate to **Policies > Security**.


2. Click on the **egress-outside** Security Policy Rule without opening it.


3. Click **Clone** to create a copy of the *egress-outside* Security Policy Rule.




4. In the *Clone* window, select **Before Rule** for *egress-outside* and click **OK**.



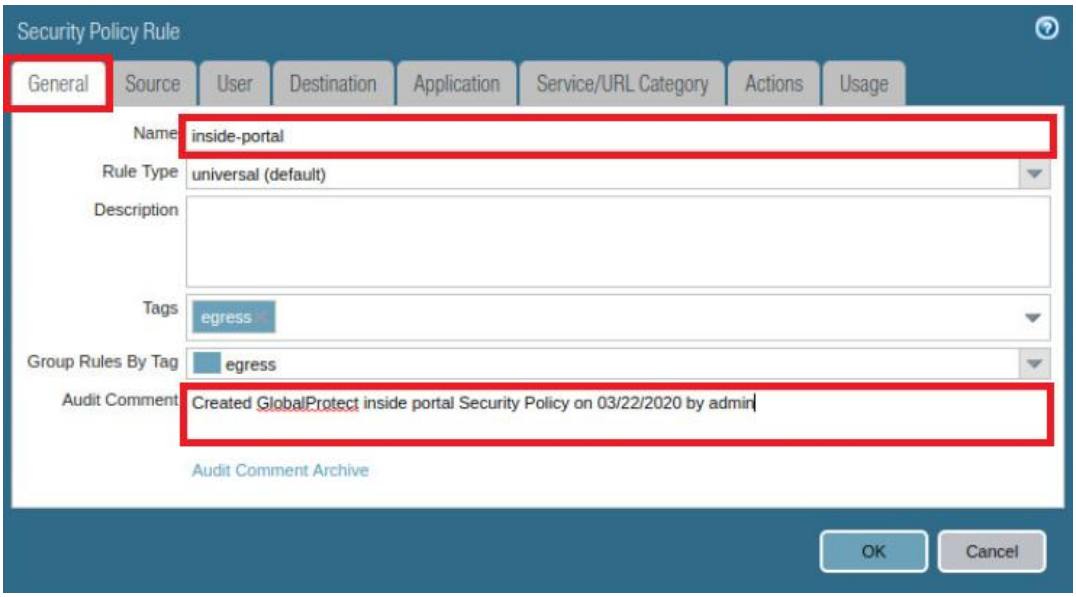

  

5. Click on the **egress-outside-1** Security Policy Rule.

| | Name | Tags | Type | Zone | Address |
|---|---|---|---|---|---|
| 1 | internal-inside-dmz | internal | universal | inside | any |
| 2 | egress-outside-1 | egress | universal | inside | any |
| 3 | egress-outside | egress | universal | inside | any |
| 4 | egress-outside-cont... | egress | universal | inside | any |
| 5 | danger-simulated-tra... | none | universal | danger | any |
| 6 | intrazone-default | none | intrazone | any | any |
| 7 | interzone-default | none | interzone | any | any |

6. In the *Security Policy Rule* window, while on the *General* tab, configure the following.

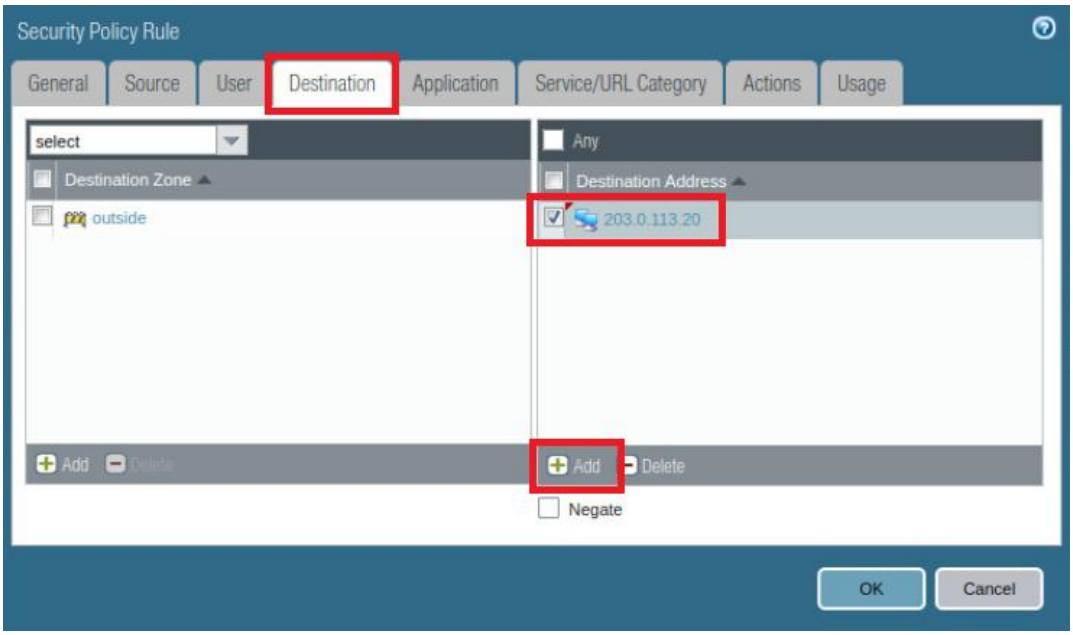
| Parameter | Value |
|---|---|
| Name | Rename the policy to `inside-portal` |
| Audit Comment | Type `Created GlobalProtect inside portal Security Policy on <date> by admin` |



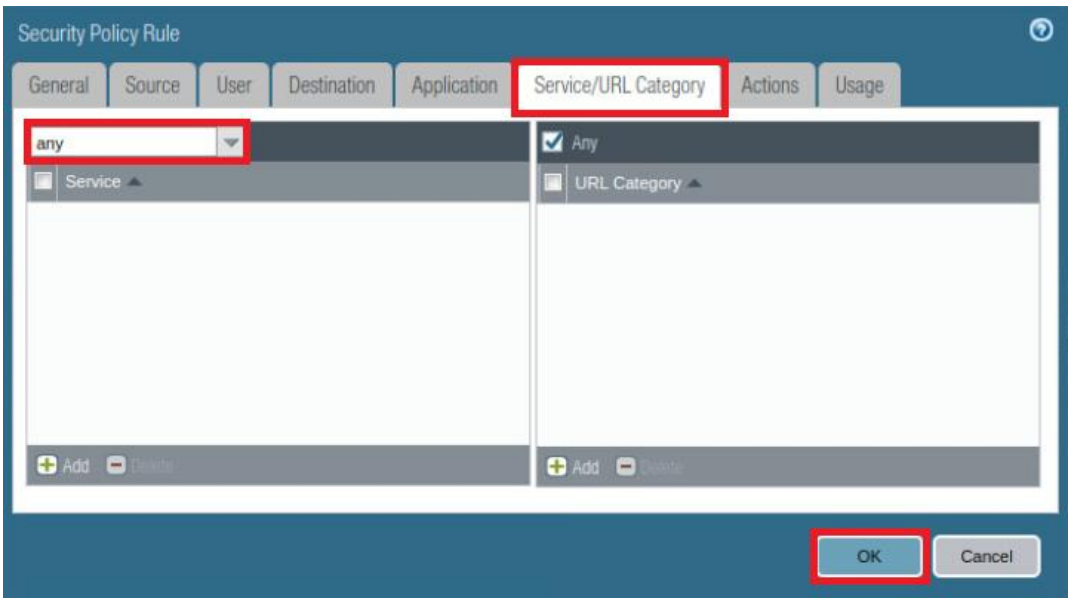
7. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

| Parameter | Value |
|---|---|
| Destination Address | Click **Add** and type `203.0.113.20` |




8. In the *Security Policy Rule* window, click the **Service/URL Category** tab and configure the following. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Service | Select **Any** from the dropdown list |



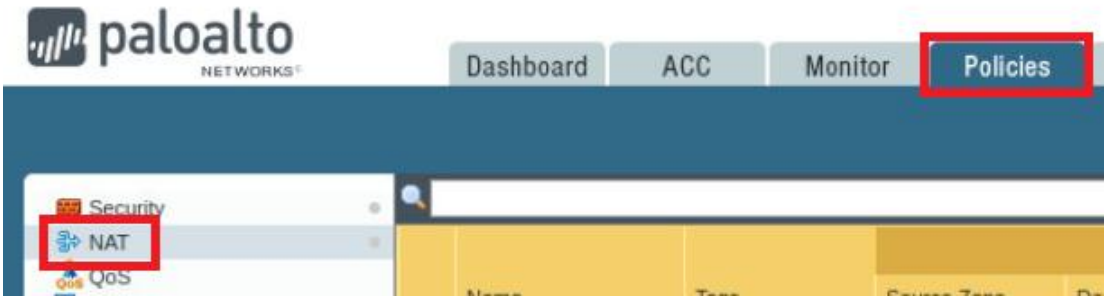

9. Leave the firewall web interface open to continue with the next task.

## 10.12 Create a No-NAT Rule

All traffic from the inside zone to the outside zone uses source NAT. In this task, you will create a new NAT policy rule so that internal requests for the *GlobalProtect* portal (203.0.113.20) will not get their address translated by the *source-egress-outside* rule. The new NAT policy rule must be matched before the *source-egress-outside* rule, so you will place it at the top of the NAT policy.

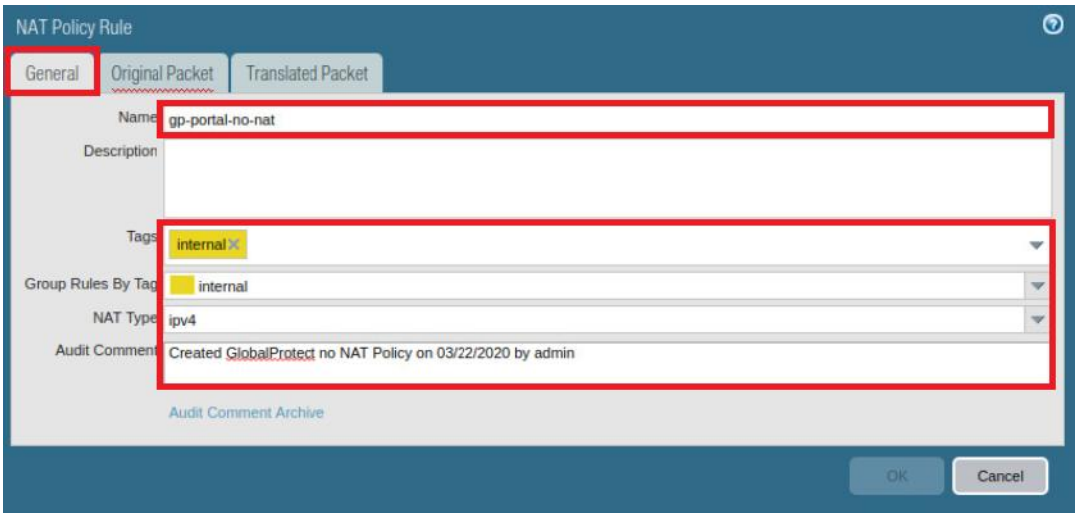
1. In the web interface, navigate to **Policies > NAT**.




2. Click **Add** to create a new source NAT policy rule.


3. In the *NAT Policy Rule* window, while on the *General* tab, configure the following.

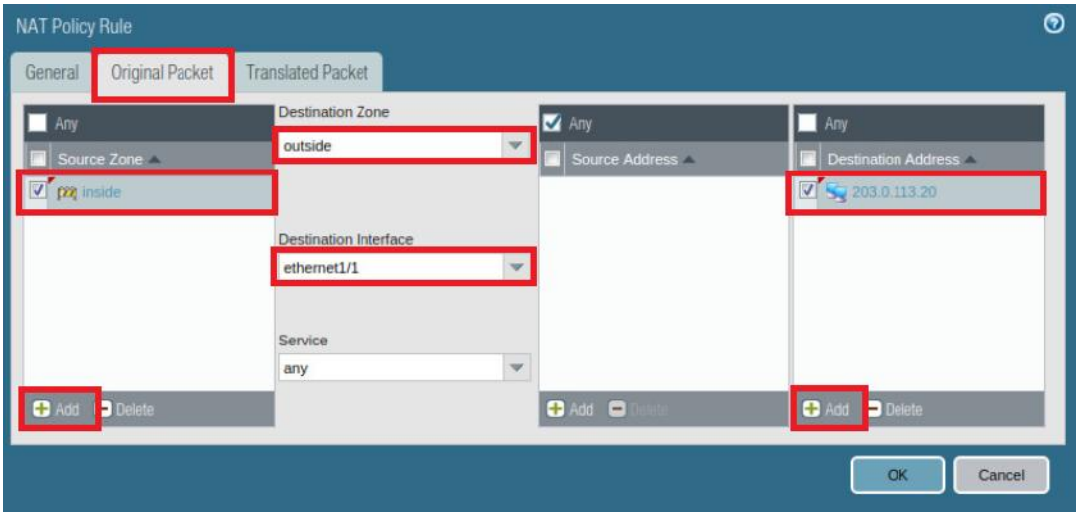
| Parameter | Value |
|---|---|
| Name | Type `gp-portal-no-nat` |
| Tags | Select **internal** from the dropdown list |
| Group Rules By Tag | Select **internal** from the dropdown list |
| NAT Type | Verify that **ipv4** is selected |
| Audit Comment | Type `Created GlobalProtect no NAT Policy on <date> by admin` |



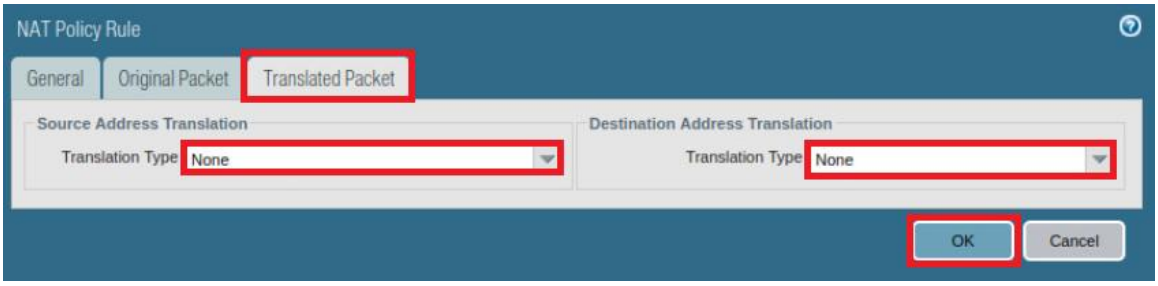

  

4. In the *NAT Policy Rule* window, click the **Original Packet** tab and configure the following.

| Parameter | Value |
|---|---|
| Source Zone | Click **Add** and select **inside** from the dropdown list |
| Destination Zone | Select **outside** from the dropdown list |
| Destination Interface | Select **ethernet1/1** from the dropdown list |
| Destination Address | Click **Add** and type **`203.0.113.20`** |



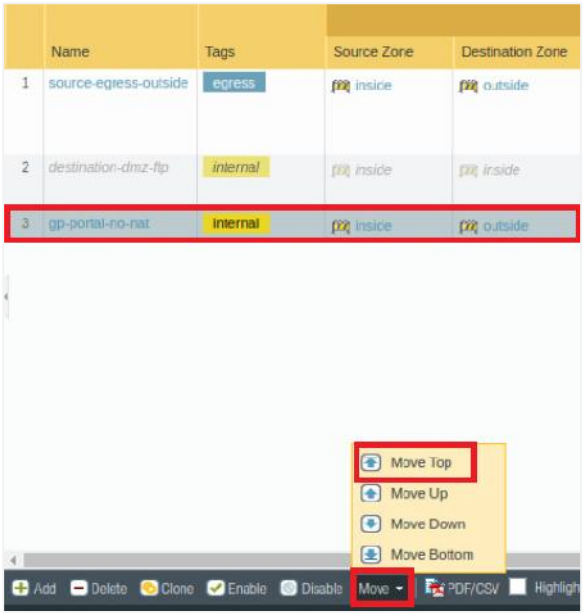

5. In the *NAT Policy Rule* window, click the **Translated Packet** tab and verify that the *Translation Type* for *Source Address Translation* and *Destination Address Translation* are set to **None**. Once finished, click **OK**.




This rule instructs the firewall to not perform network address translation of any kind for traffic from the inside zone that has a destination address of *203.0.113.20* in the outside zone, which is the IP address of the *GlobalProtect* portal and of the external gateway.

6. Select, but do not open the **gp-portal-no-nat** NAT policy rule. Click **Move** and select **Move Top**.




Traffic that is not destined for the portal IP address (*203.0.113.20*) will be translated by the *source-egress-outside* rule.

7. **Commit** all changes.

A warning might appear about IPv6 not being enabled on the tunnel interface. It can be safely ignored.

## 10.13 Download the GlobalProtect Agent

1. Open a new tab in **Chromium Web Browser** and browse to `https://203.0.113.20`.


2. If a certificate warning appears, click through the *Certificate Warning*.
3. Once the webpage loads, log in with the following.

| Parameter | Value |
|---|---|
| Username | `lab-user` |
| Password | `Pa10Alt0` |


4. If you were using a Windows or Mac client, you would download the *GlobalProtect agent* from there. Since the lab is using a Linux client, go ahead and close the browser tab and proceed to the next step.

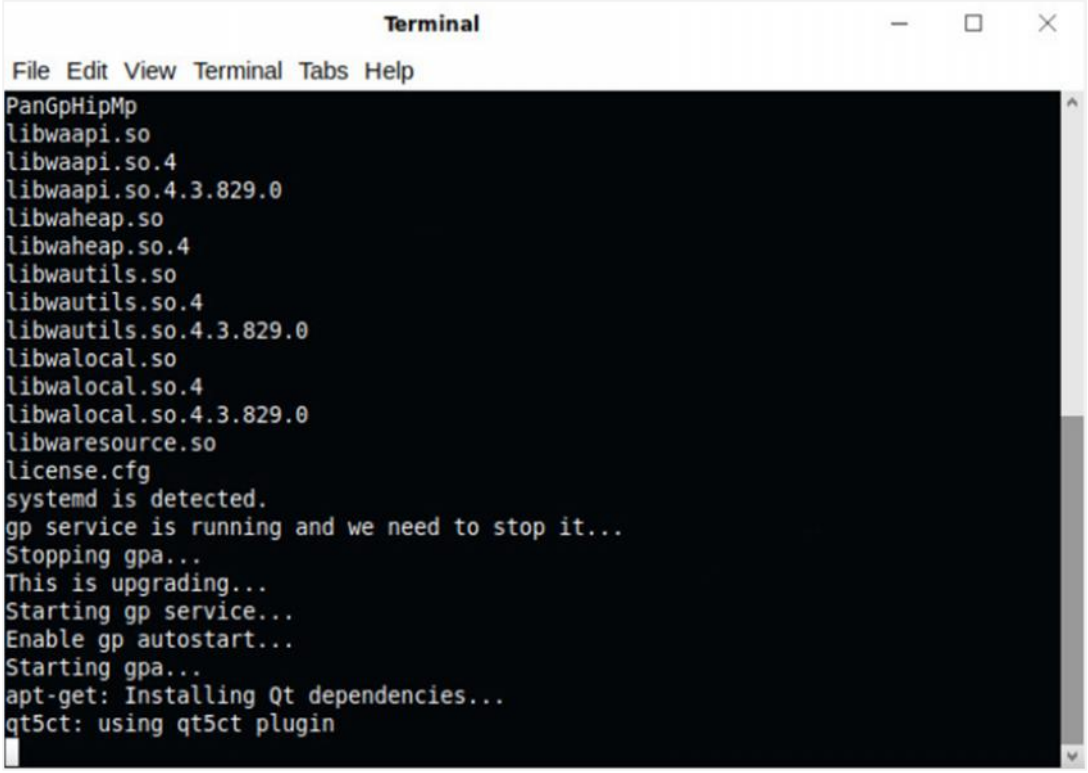
5. On the Client desktop, double-click the **lab** 

folder.
6. Double-click the **scripts** folder.
7. Double-click the **globalprotect.sh** 

to launch *GlobalProtect* agent 0installation.
8. When prompted, enter **`Train1ng$`** as the password.

```
[sudo] password for lab-user: *********
```

9. Leave the *Terminal* window running in the background.



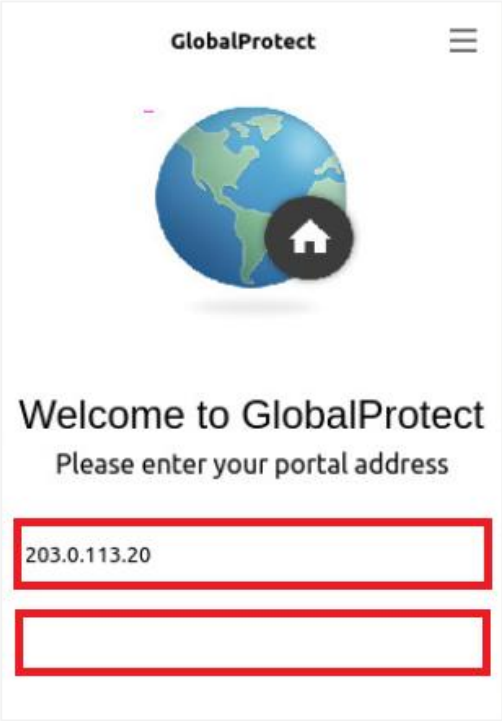

10. Proceed to the next task.

## 10.14 Connect to the External Gateway

1. 1. Notice that a *Welcome to GlobalProtect* window appears. If not, click on the **GlobalProtect** agent icon in the Client system tray.

2. In the *Welcome to GlobalProtect* box, type **`203.0.113.20`** as the portal address, followed by clicking on **Connect**.

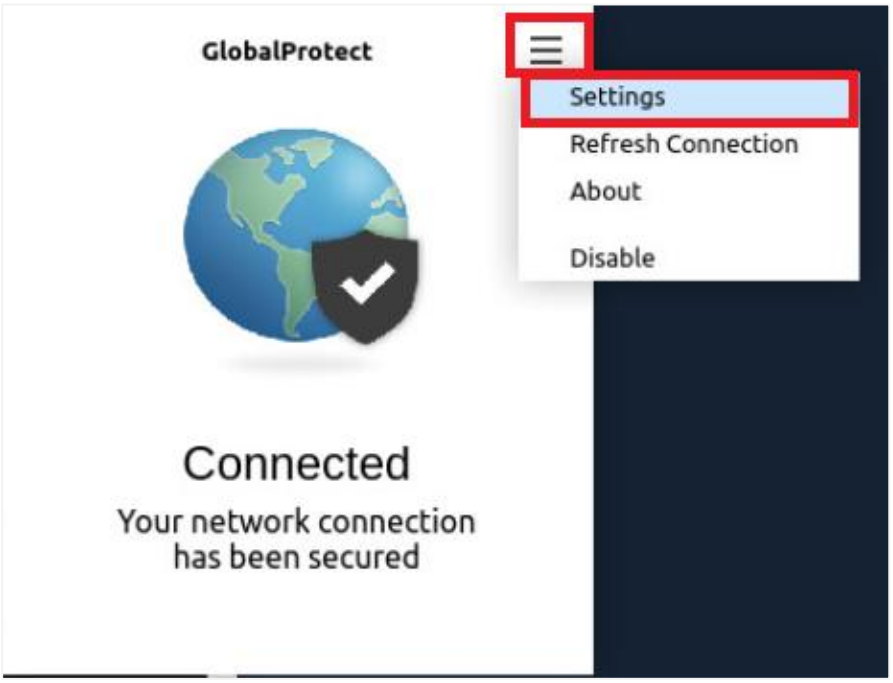



3. After a couple of seconds, notice a *GlobalProtect* message may appear, concerning the certificate. Click **Yes** to connect.

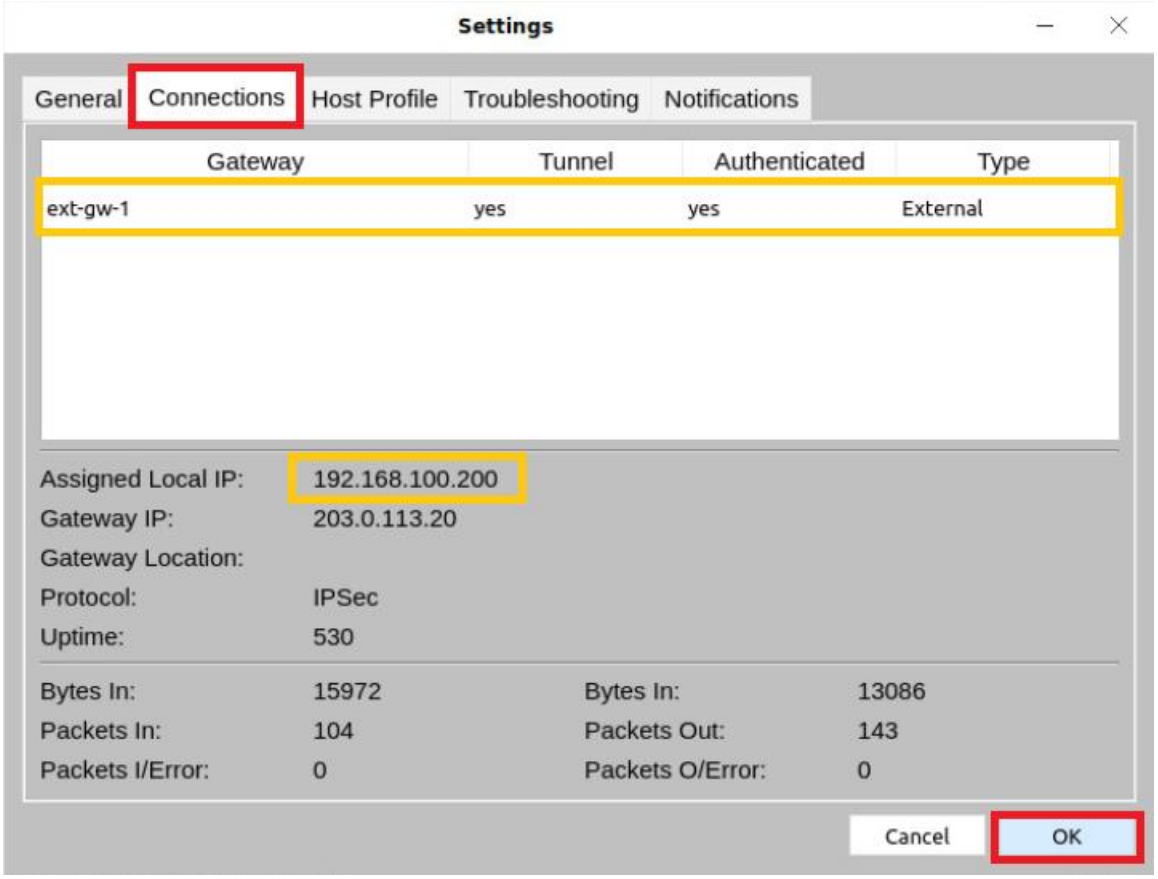
4. Notice the *GlobalProtect* login screen should appear. Log in as `lab-user` with `Pa10Alt0` as the password. Click **Sign In**.


5. After about a minute, the *GlobalProtect* windows should say *Connected*. Once it does, click the **Menu** icon in the top-right corner and then select **Settings** from the dropdown list.



6. In the *Settings* window, click the **Connections** tab; once finished, click **OK** to close.



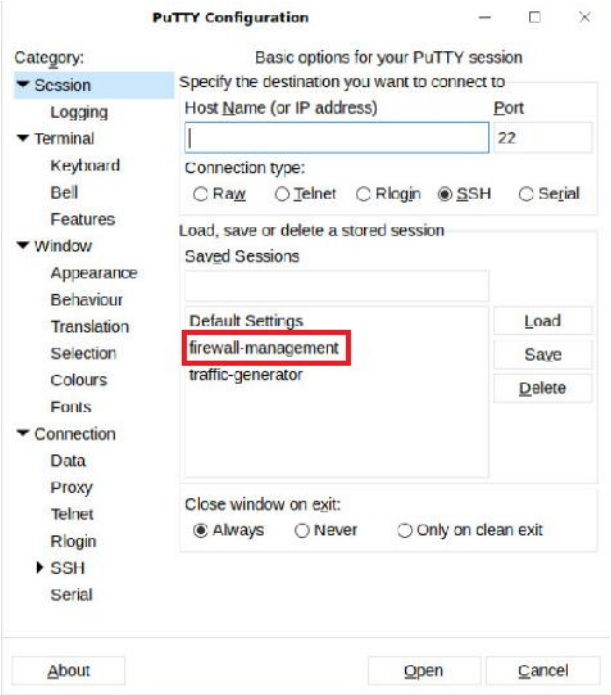

Notice the gateway listed as 203.0.113.20, the gateway type is *External*, and a tunnel is established. Also notice that the IP assigned is the first in the IP pool specified on the external gateway.

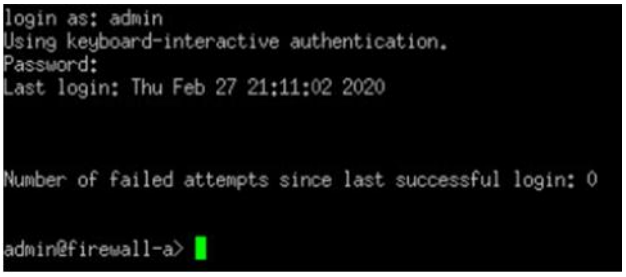
## 10.15 View User-ID Information

1. On the Client desktop, open **PuTTY** 

and double-click **firewall-management**.

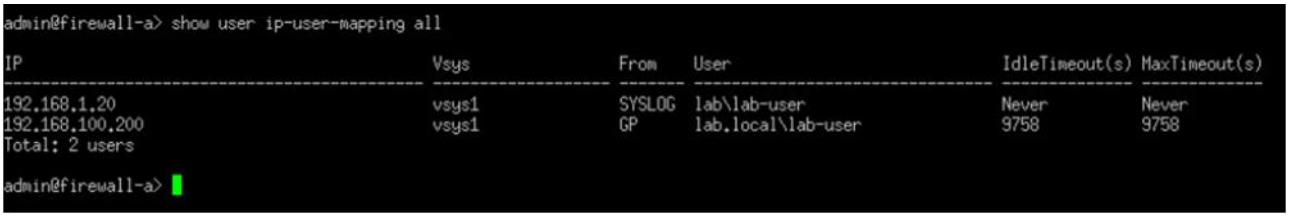



2. Log in to the firewall using the username **admin** and password **Train1ng$**.




3. At the prompt, enter the command below.

```
admin@firewall-a> show user ip-user-mapping all
```



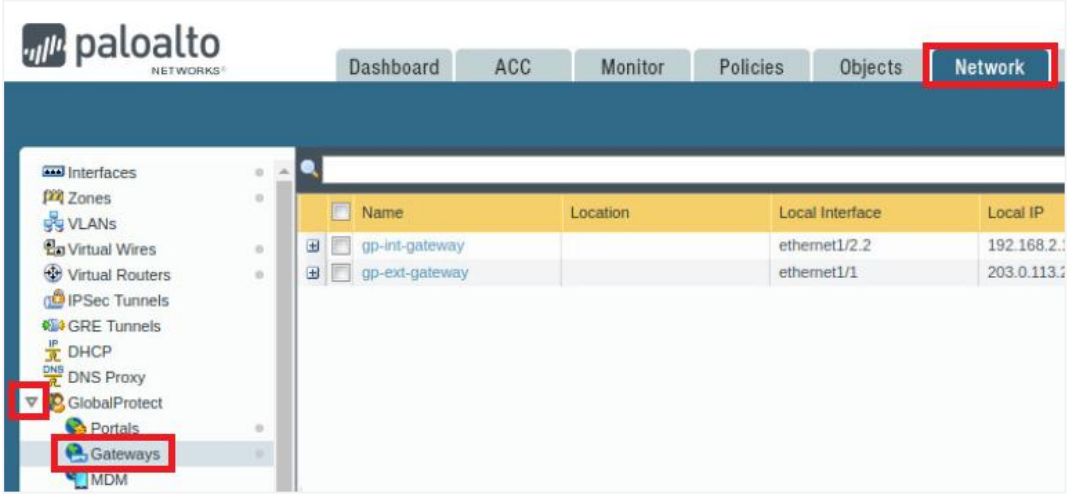

  

The IP addresses for lab-user have been updated to include the tunnel IP address. Notice the From column lists *GP* (*GlobalProtect*). *GlobalProtect* is one of the ways that you can provide username and IP address mappings to the firewall for User-ID. For more information about User-ID, see the User-ID lab.

4. Type **`exit`** to close the *PuTTY* session.

## 10.16 Disconnect the Connected User

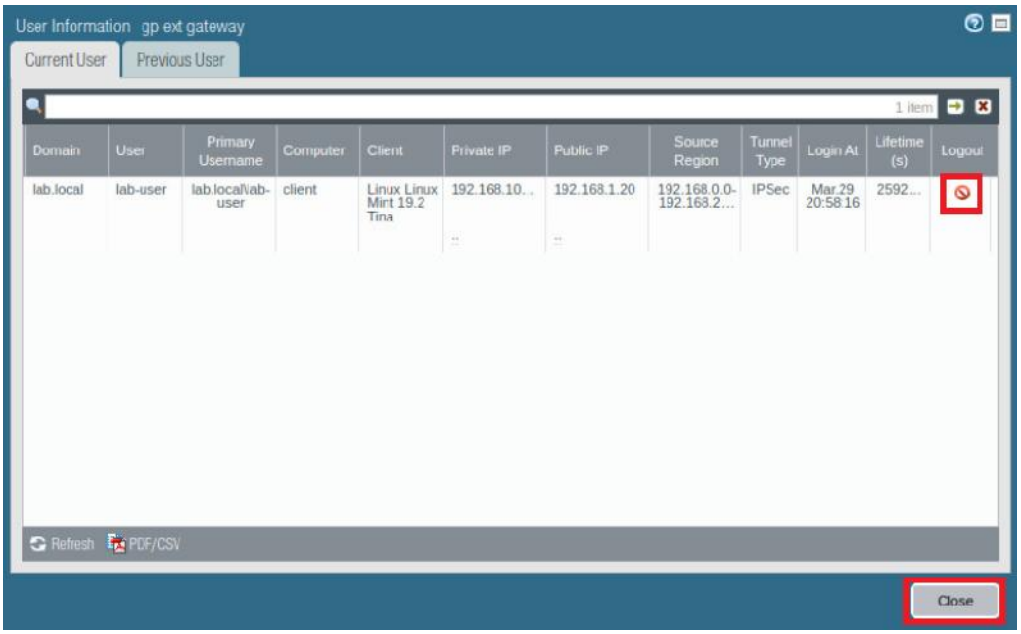
1. Change focus to the firewall's web interface and navigate to **Network > GlobalProtect > Gateways**.




2. Click **Remote Users** to the far-right of the *gp-ext-gateway* underneath the *Info* column.

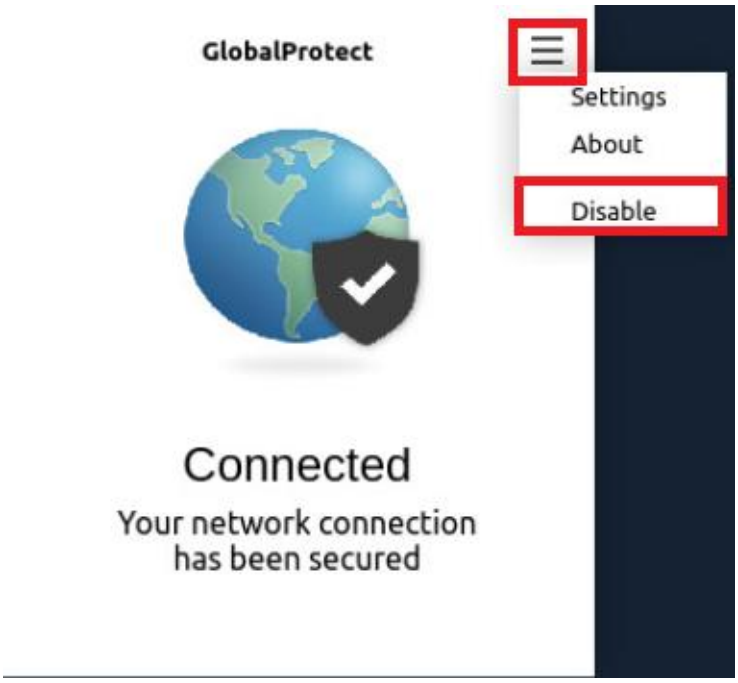

  

3. In the *User Information - gp-ext-gateway* window, while on the *Current User* tab, click the icon in the **Logout** column to disconnect the *lab-user*. Notice that the *lab-user* then disappears from the list. Click **Close**.




4. Click on the **GlobalProtect** agent icon in the Client system tray.


5. Click the **Menu** icon in the top-right corner and select **Disable** from the dropdown list.



## 10.17 Configure DNS Proxy

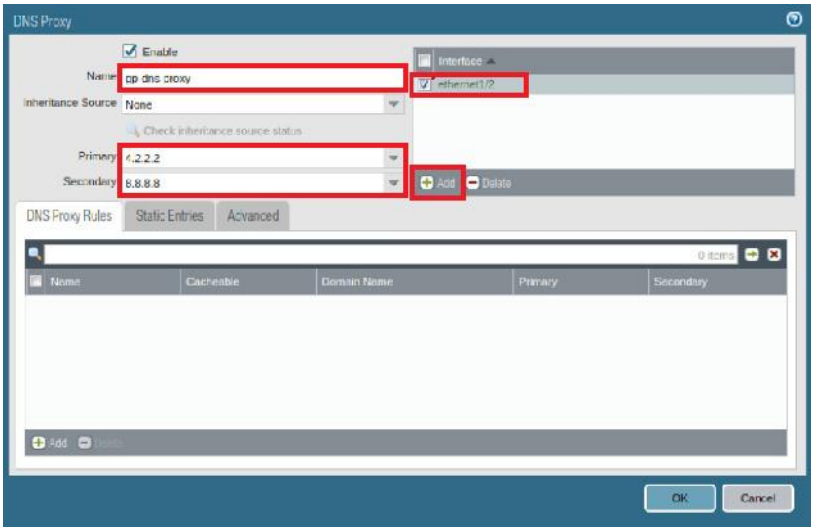
DNS servers resolve a hostname to an IP address and vice versa. When you configure the firewall as a DNS proxy, the firewall acts as an intermediary between the DNS clients and DNS servers, and as a DNS server by resolving queries from its DNS cache or forwarding queries to other DNS servers. Configuration of the firewall to be a DNS proxy is required so that *GlobalProtect* internal host detection works correctly.

1. In the web interface, select **Network > DNS Proxy**.


2. Click **Add** to create a new DNS proxy.


3. In the *DNS Proxy* window, configure the following parameters.

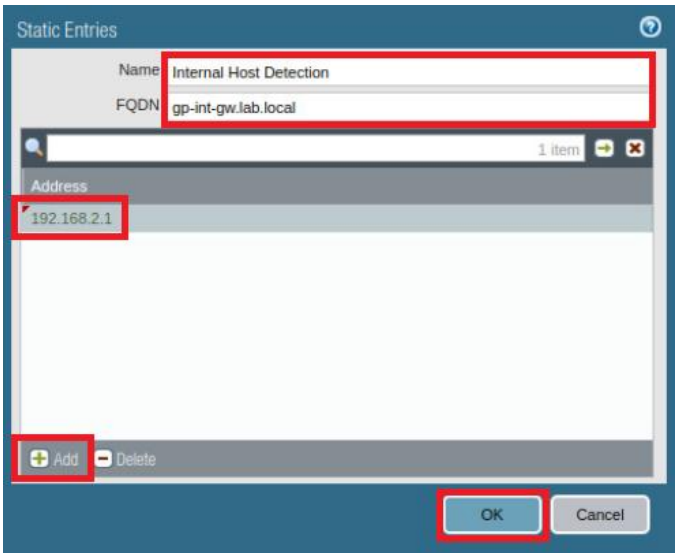
| Parameter | Value |
|---|---|
| Name | Type **gp-dns-proxy** |
| Interface | Click **Add** and select **ethernet1/2** from the dropdown list |
| Primary | Type **4.2.2.2** |
| Secondary | Type **8.8.8.8** |



4. In the *DNS Proxy* window, click on the **Static Entries** tab. Click **Add** to create a new static entry using the information below. Once finished, click **OK**.

| Parameter | Value |
|---|---|
| Name | Type `Internal Host Detection` |
| FQDN | Type `gp-int-gw.lab.local` |
| Address | Click **Add** and type `192.168.2.1` |

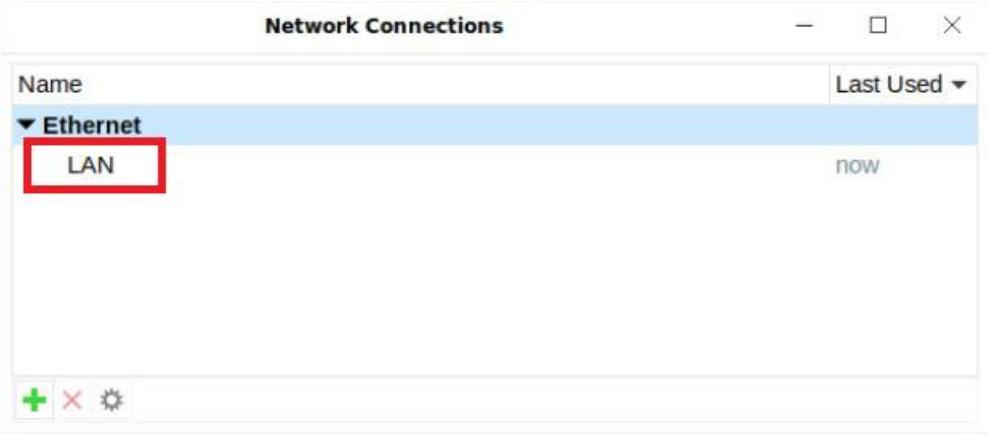



5. Back on the *DNS Proxy* window, click **OK**.
6. **Commit** all changes.
7. Click on the **Connections** icon in the Client system tray.

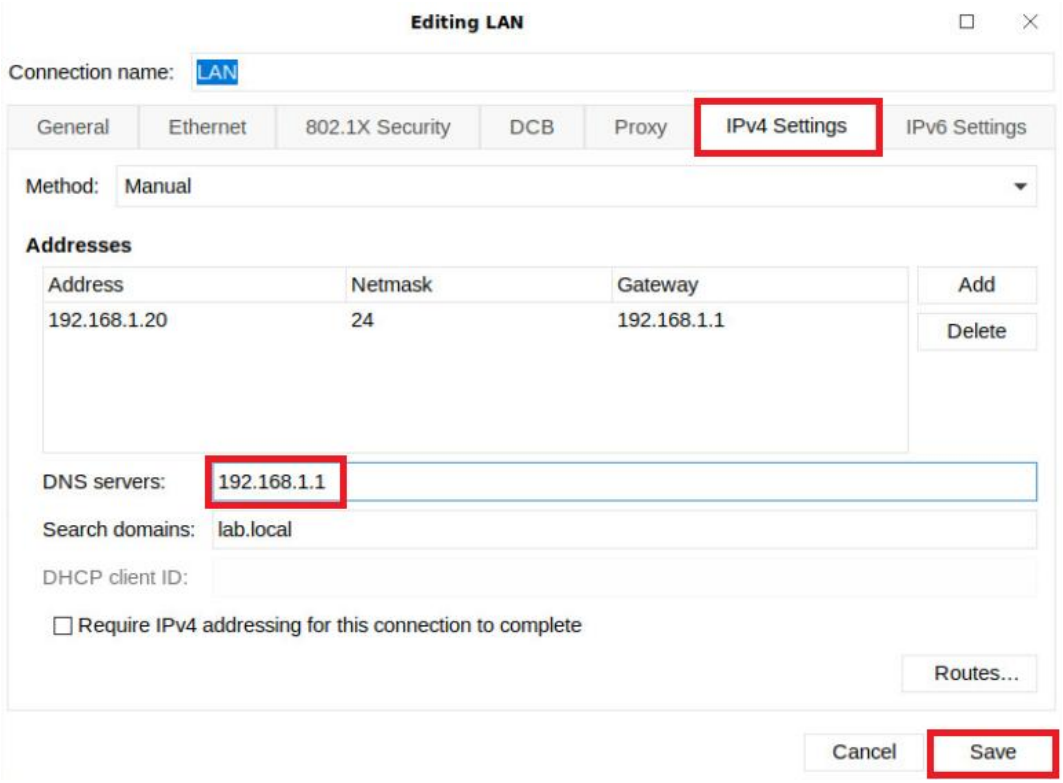

8. Click **Edit Connections…**.

9. Double-click the **LAN** in the *Network* Connections window.

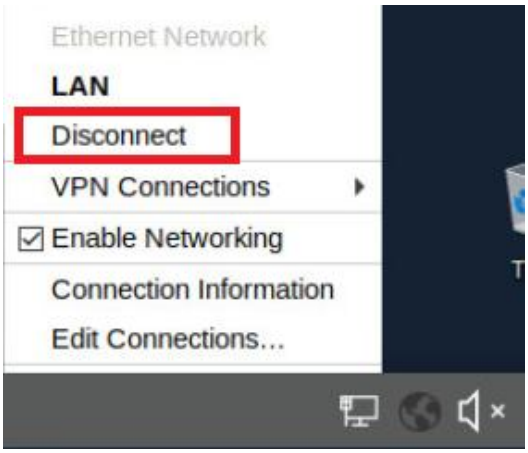



10. In the *Editing Lan* window, click the **IPv4 Settings** tab and enter **192.168.1.1** in the *DNS servers:* box and click **Save**.



11. Click on the **Connections** icon in the Client system tray and click **Disconnect**.



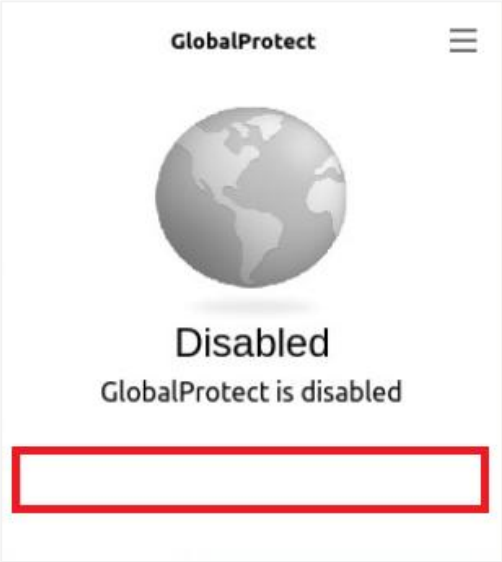

12. Click on the **Connections** icon again and click **LAN**.

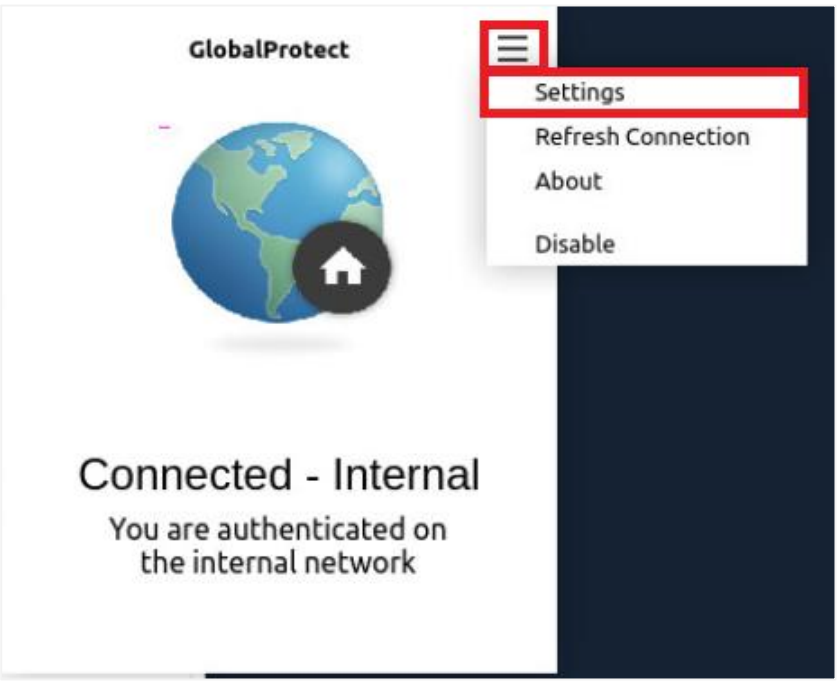
## 10.18 Connect to the Internal Gateway

1. Click on the **GlobalProtect** agent icon in the Client system tray.

2. Notice the *GlobalProtect* window appears. Click on **Enable**.

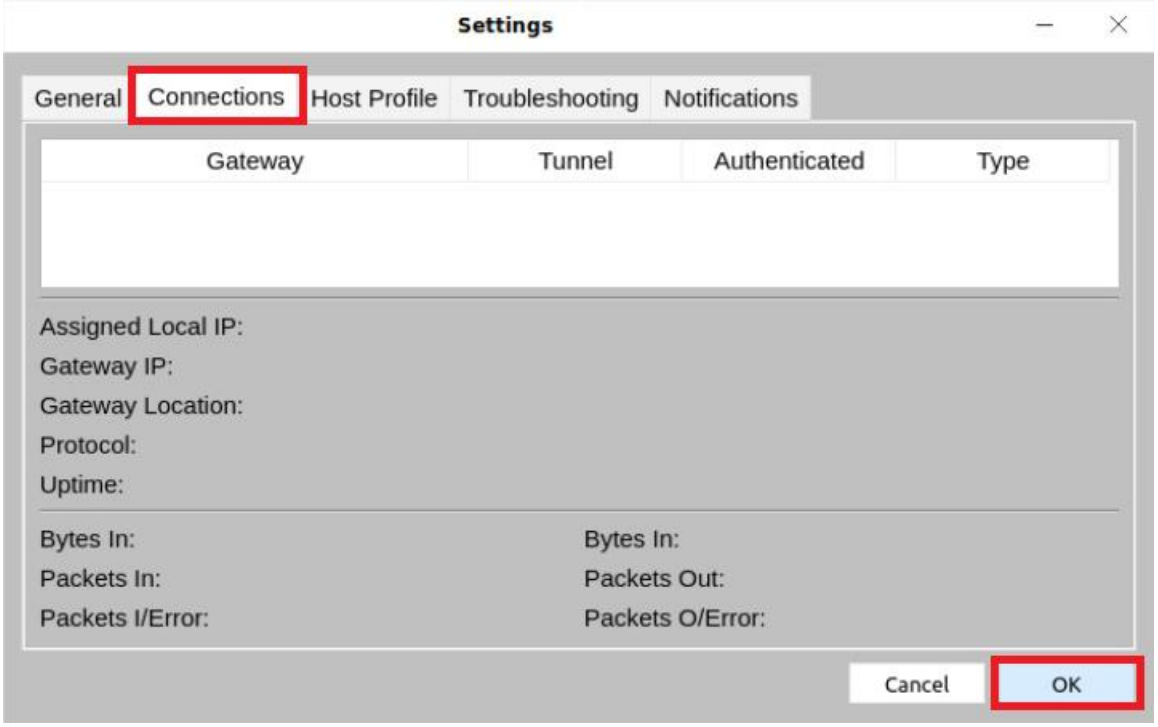



3. Notice after a moment that the status updates to *Connected - Internal*. Click the **Menu** icon in the top-right corner and then select **Settings** from the dropdown list.



4. In the *Settings* window, click the **Connection** tab. Notice that there is nothing populated. Click **OK** when finished.




5. Close the **Settings** window.
6. Click on the **GlobalProtect** agent icon once more in the Client system tray.

7. Click the **gear icon** in the top-right corner and select **Disable** from the dropdown list.


8. The lab is now complete; you may end the reservation.