CLOUD SECURITY FUNDAMENTALS V2

Lab 05: Configuring HIP for GlobalProtect

Document Version: 2022-12-22

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Configuring HIP for Global Protect. 6
1.0 Load Lab Configuration 6
1.1 Download the GlobalProtect Agent 10
1.2 Create a HIP Object 14
1.3 Create a HIP Profile 16
1.4 Modify Security Policy to Add HIP Profile 17
1.5 Modify GlobalProtect Gateway to Add a HIP Notification and Commit 18
1.6 Configure and Connect the GlobalProtect Agent for Network Access 22
1.7 View the GlobalProtect HIP Matches Logs 27

Introduction

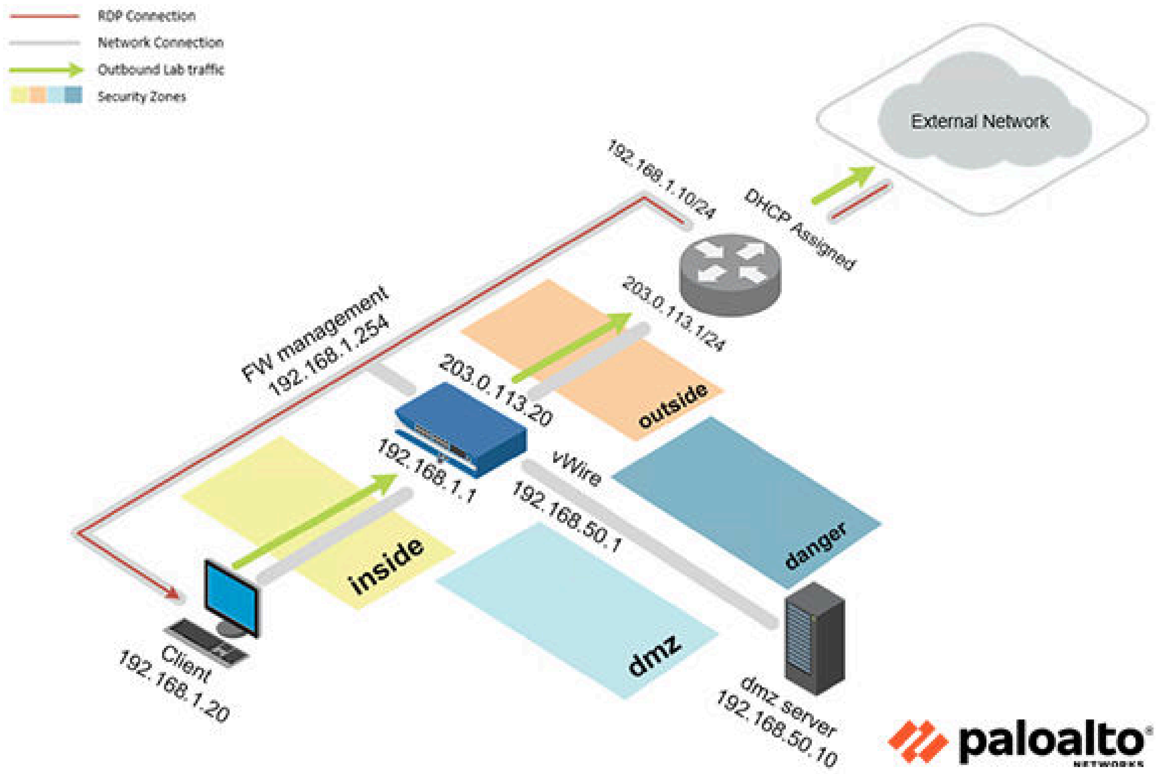
In this lab, you will install GlobalProtect^{TM} while utilizing a HIP Object within a HIP Profile. Using HIP profiles for policy enforcement enables a granular security approach that will ensure the remote host that client machines accessing the network are properly maintained and adhering to the security policies in place.

Objective

In this lab, you will perform the following tasks:

- Install the GlobalProtect Agent
- Create a HIP Object
- Create a HIP Profile
- Modify Security Policy to Add HIP Profile
- Modify GlobalProtect Gateway to Add a HIP Notification and Commit
- Configure and Connect the GlobalProtect Agent for Network Access
- Reconnect the GlobalProtect Agent for Network Access

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.

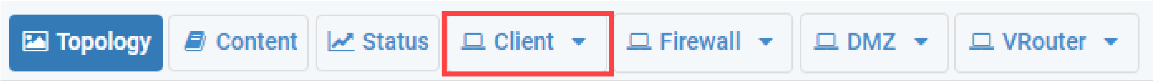
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Configuring HIP for Global Protect.

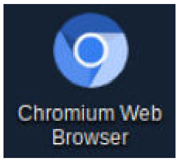
1.0 Load Lab Configuration

In this section, you will load the *Firewall* configuration file.

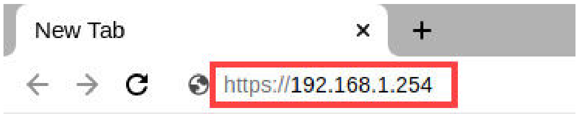
1. Click on the **Client** tab to access the *Client* machine.



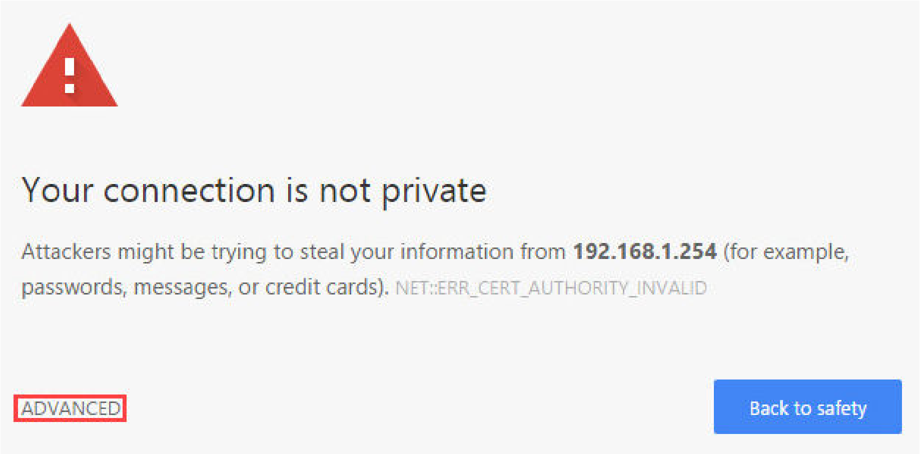
2. Log in to the Client machine as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



4. In the *Chromium address* field, type `https://192.168.1.254` and press **Enter**.



5. You will see a "*Your connection is not private"* message. Click on the **Advanced** link.

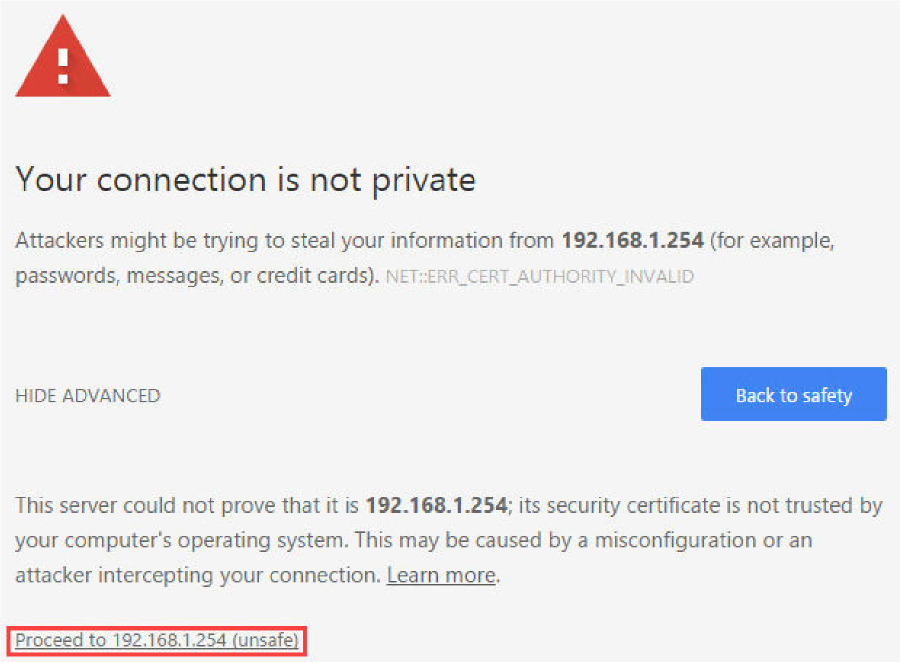


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

6. Click on **Proceed to 192.168.1.254 (unsafe)**.

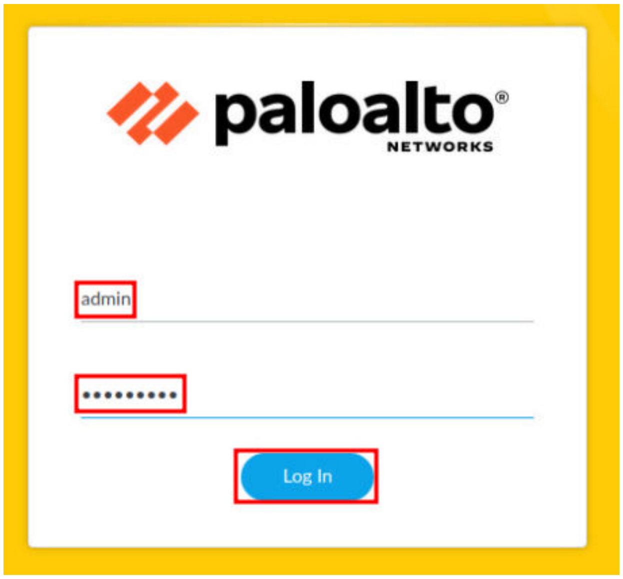


Your connection is not private

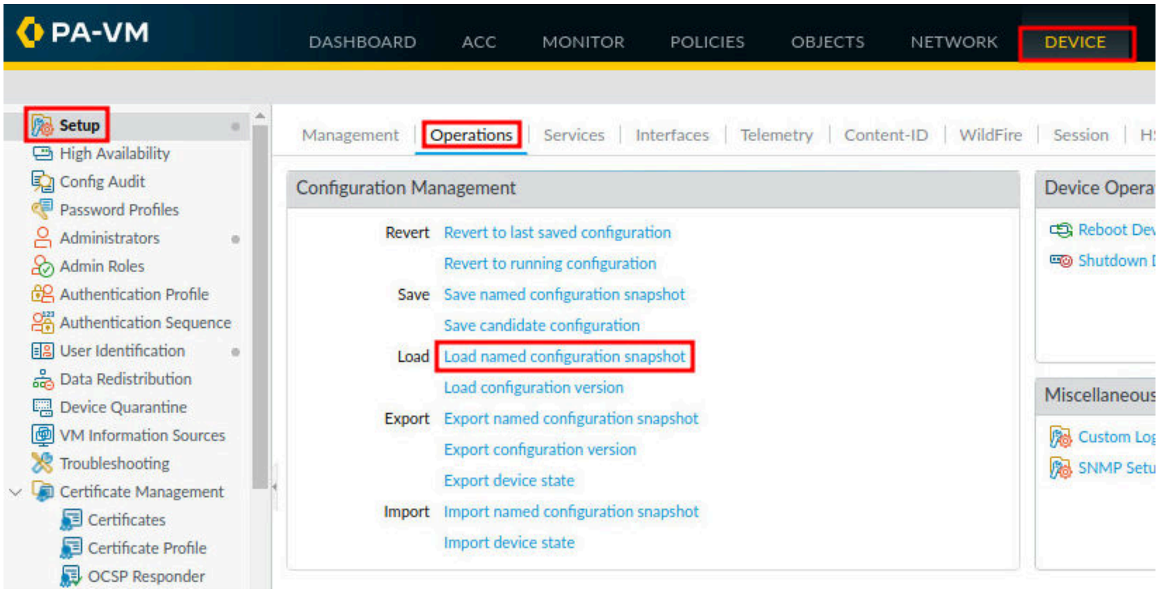
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

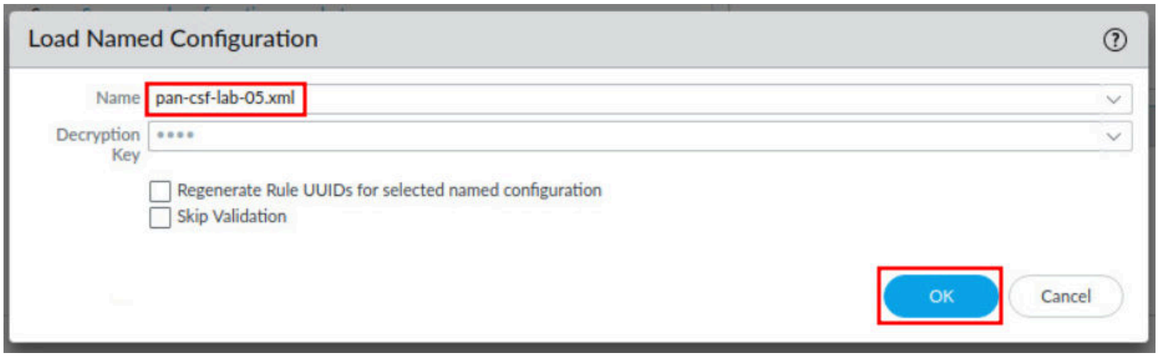
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



8. Navigate to **Device > Setup > Operations > Load named configuration snapshot**.



9. In the *Load Named Configuration* window, select **pan-csf-lab-05.xml** from the *Name* dropdown box and click **OK**.


Load Named Configuration

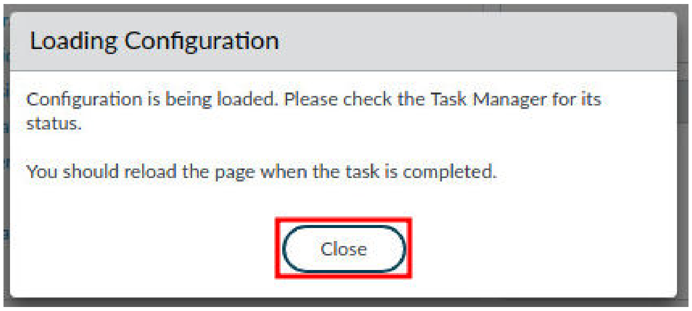
Name: pan-csf-lab-05.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

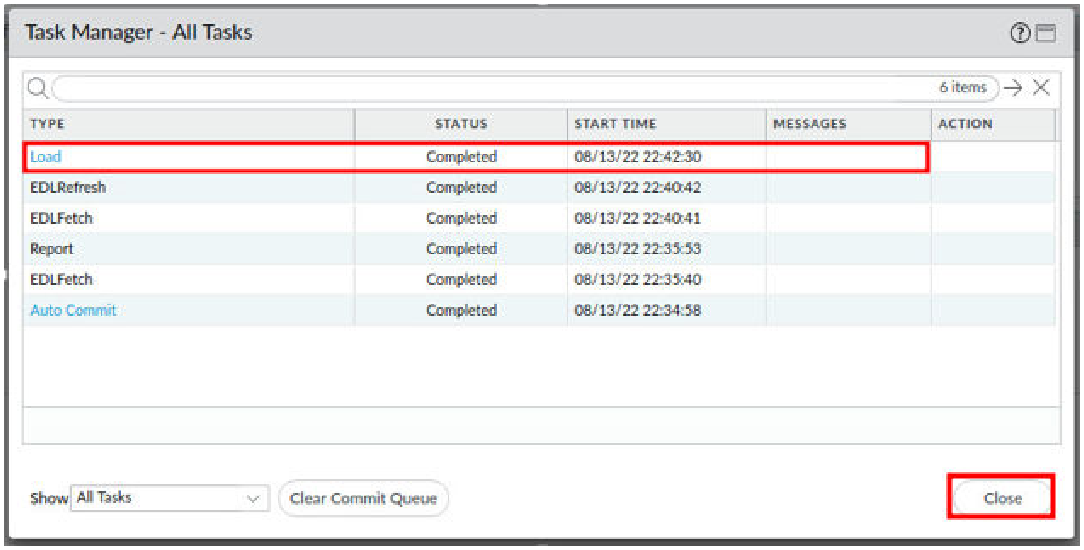
10. A message will confirm the configuration has loaded. Click **Close** to continue.


Loading Configuration

Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**

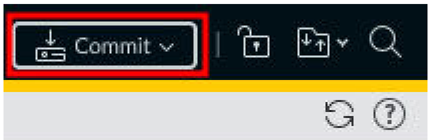


Task Manager - All Tasks

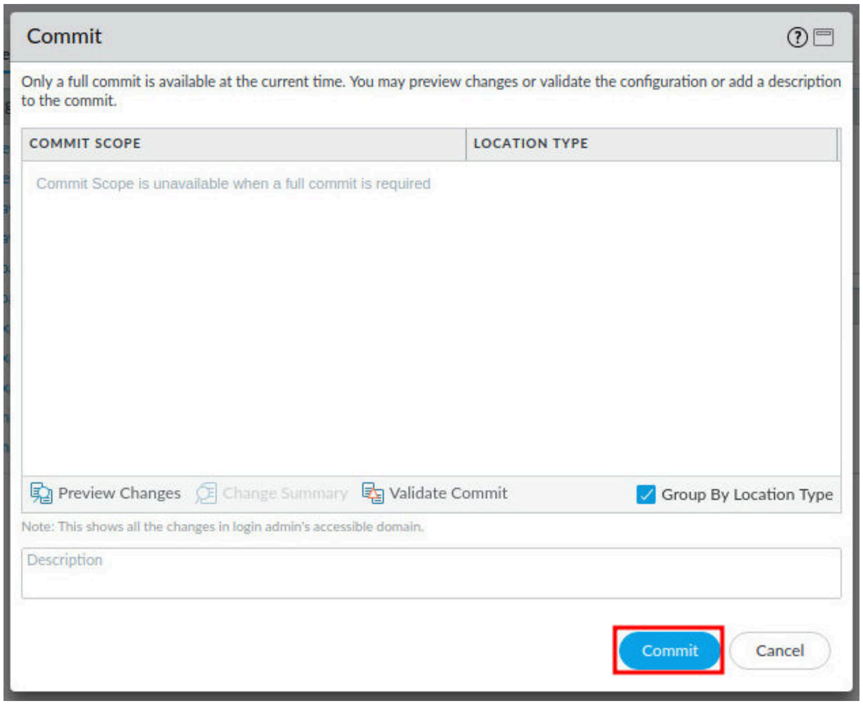
6 items

TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

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



13. In the *Commit* window, click **Commit** to proceed with committing the changes.



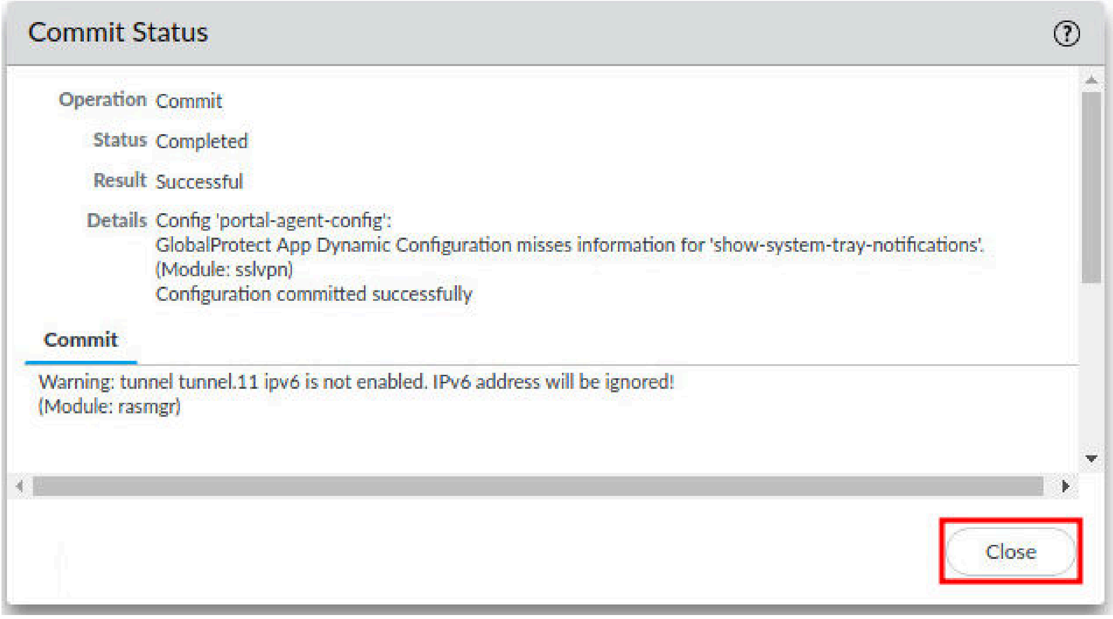
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

14. When the commit operation successfully completes, click **Close** to continue.



Commit Status

Operation Commit

Status Completed

Result Successful

Details Config 'portal-agent-config':
GlobalProtect App Dynamic Configuration misses information for 'show-system-tray-notifications'.
(Module: sslvpn)
Configuration committed successfully

Commit

Warning: tunnel tunnel.11 ipv6 is not enabled. IPv6 address will be ignored!
(Module: rasmgr)

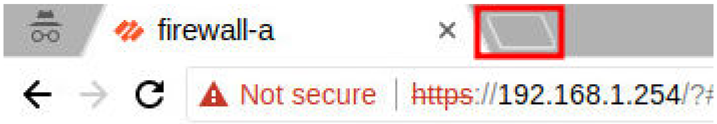
The **Warnings** displayed are normal. IPv6 has not been enabled for this lab and therefore this warning can be ignored.

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

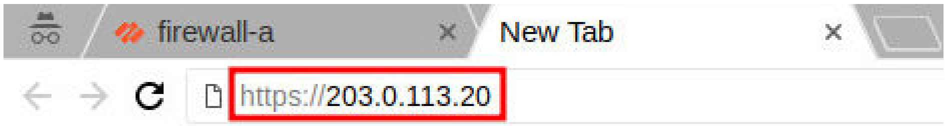
1.1 Download the GlobalProtect Agent

In this section, you will step through the normal process of downloading the *GlobalProtect Agent*. The *GlobalProtect* agent is an application that is installed on a client system to support *GlobalProtect* connections with portals and gateways. You will then install the *GlobalProtect Agent* using a custom script.

1. Click on the **New tab** button.

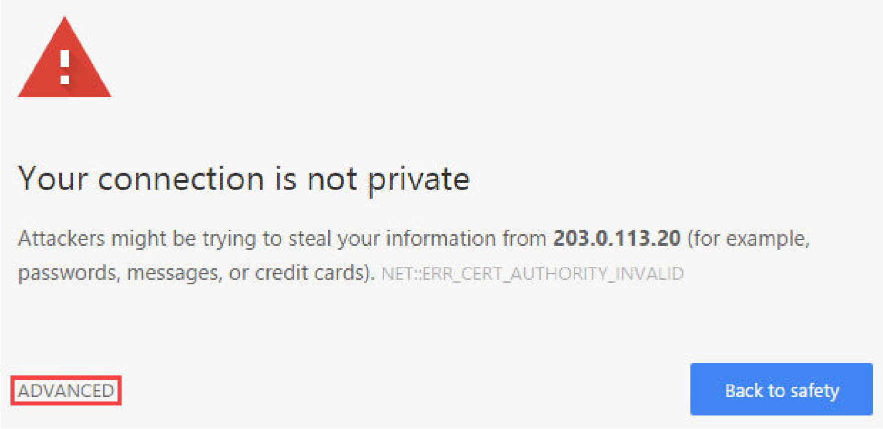


2. In the address bar, type `https://203.0.113.20` and click **Enter**.



https://203.0.113.20

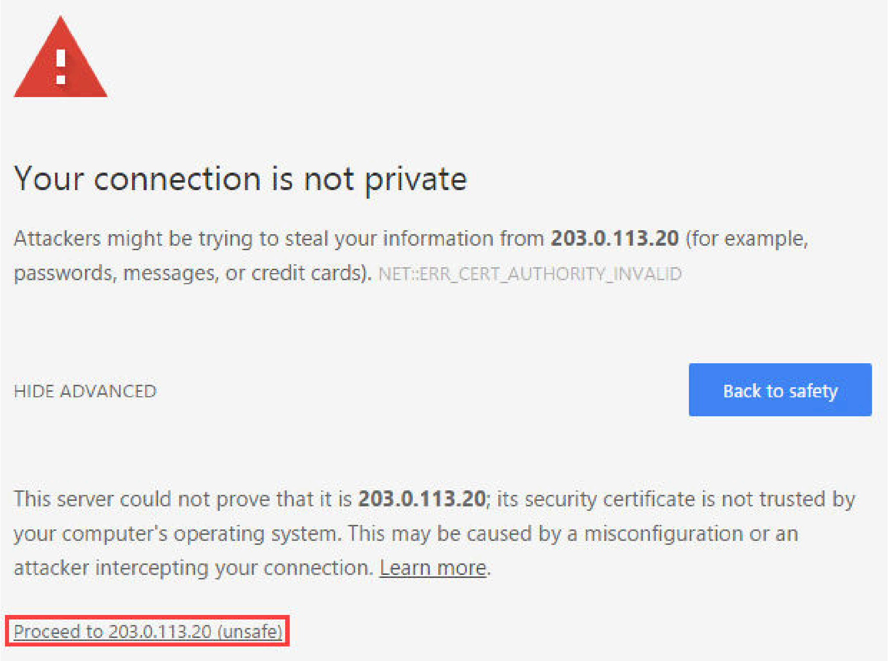
3. You will see a "*Your connection is not private*" message. Click on the **Advanced** link.



Your connection is not private

Attackers might be trying to steal your information from **203.0.113.20** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

4. Click on **Proceed to 203.0.113.20 (unsafe)**.



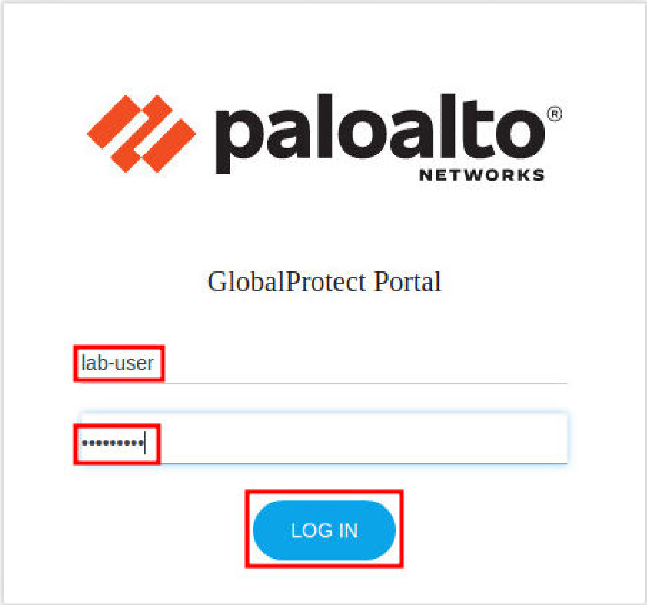
Your connection is not private

Attackers might be trying to steal your information from **203.0.113.20** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

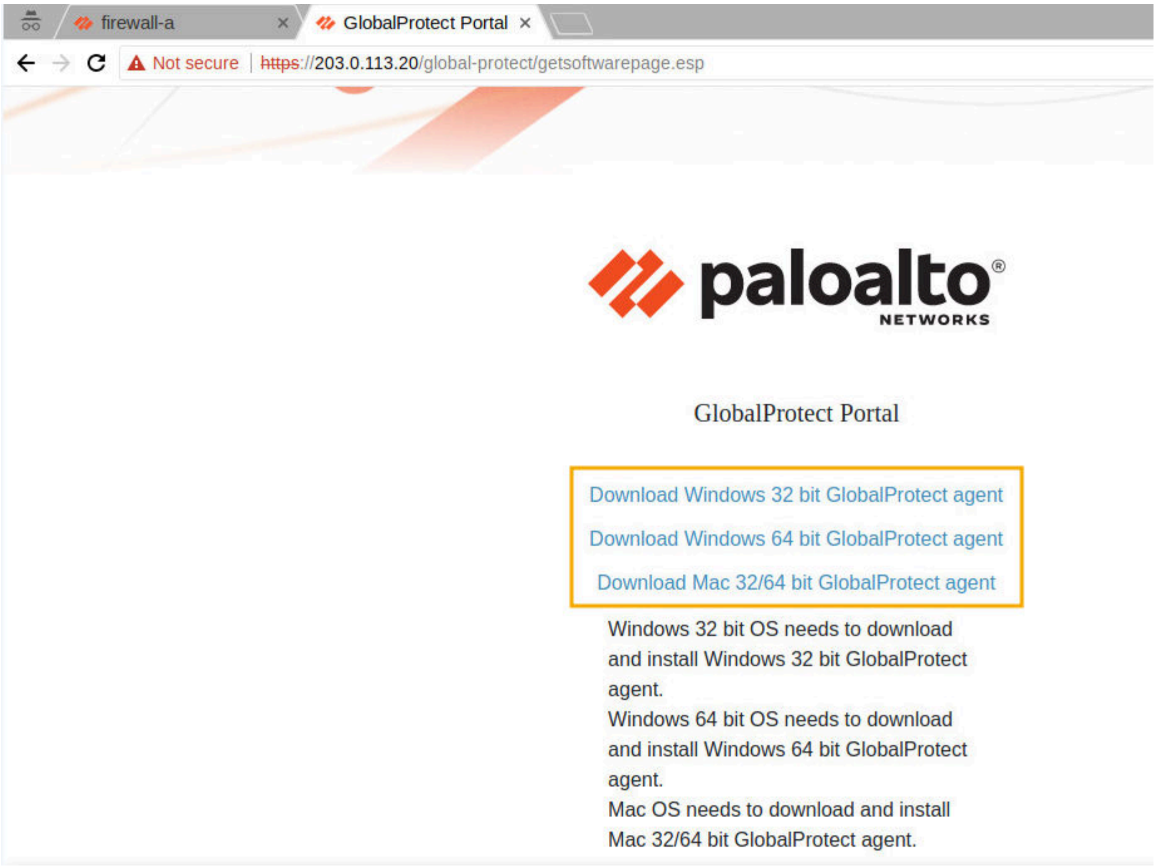
This server could not prove that it is **203.0.113.20**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to 203.0.113.20 (unsafe)

5. In the *GlobalProtect Portal* login screen, type `lab-user` for the *Name* field. Then, type `Pal0Alt0!` for the *Password* field. Next, click the **Log In** button.

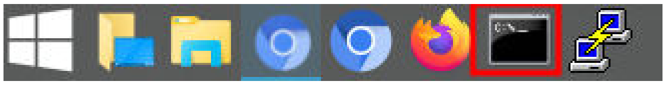


6. Notice the download options available in the *GlobalProtect Portal* download screen.


firewall-a
GlobalProtect Portal
Not secure
https://203.0.113.20/global-protect/getsoftwarepage.esp
paloalto NETWORKS
GlobalProtect Portal
Download Windows 32 bit GlobalProtect agent
Download Windows 64 bit GlobalProtect agent
Download Mac 32/64 bit GlobalProtect agent

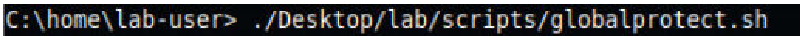
Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

7. Since the *Client* in the lab environment is running on a Linux OS, a custom script will be used instead to install the *GlobalProtect* agent. Open a new **terminal** window.



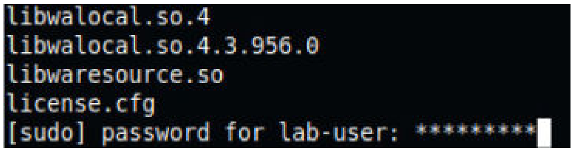
8. In the terminal window, type the command below, followed by pressing the **Enter** key.

```
C:\home\lab-user> ./Desktop/lab/scripts/globalprotect.sh
```



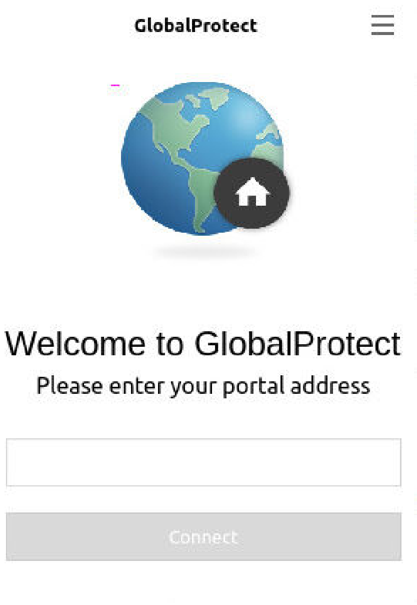
```
C:\home\lab-user> ./Desktop/lab/scripts/globalprotect.sh
```

9. When prompted for a password, enter `Pal0Alt0!`.



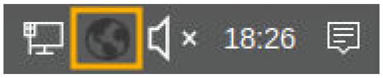
```
libwalocal.so.4
libwalocal.so.4.3.956.0
libwaresource.so
license.cfg
[sudo] password for lab-user: *********
```

10. Notice that the *GlobalProtect* window appears and is now installed. Also notice the GlobalProtect icon in the notification area at the bottom left.



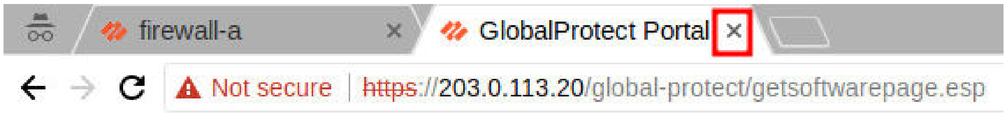
Welcome to GlobalProtect

Please enter your portal address



Note that if the GlobalProtect window has a problem, you may close the **terminal** window and run the script to install the agent again.

11. Navigate back to the web browser and close the second tab.



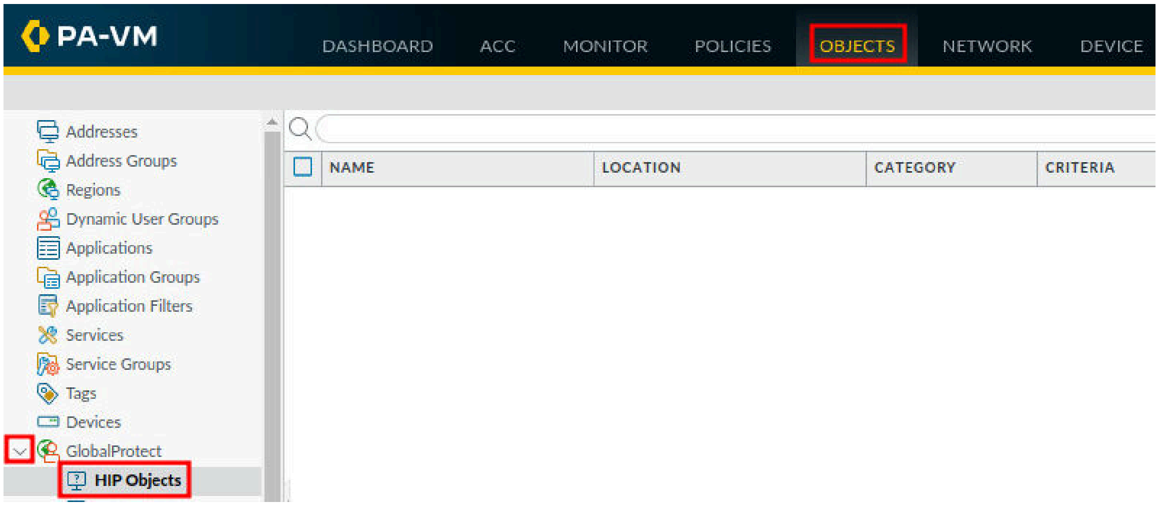
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

12. Leave the web browser open to continue with the next task.

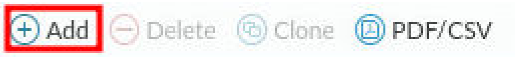
1.2 Create a HIP Object

In this section, you will create a *Host Information Profile* (*HIP*) object. *HIP Objects* provide matching criteria for filtering the raw data reported by an agent or application to enforce policy. *HIP Objects* are building blocks that allow administrators to create the *HIP Profiles* used in *Security Policies*.

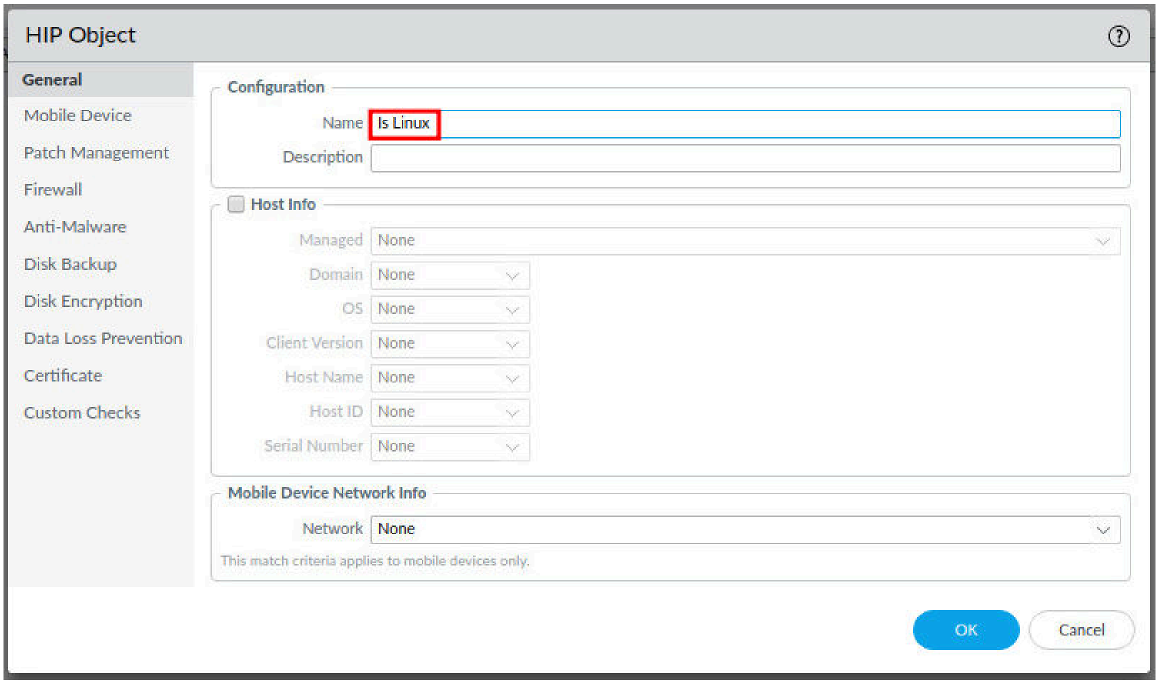
1. In the firewall web interface, navigate to **Objects > GlobalProtect > HIP Objects**.



2. Click **Add** to add a new *HIP Object*.

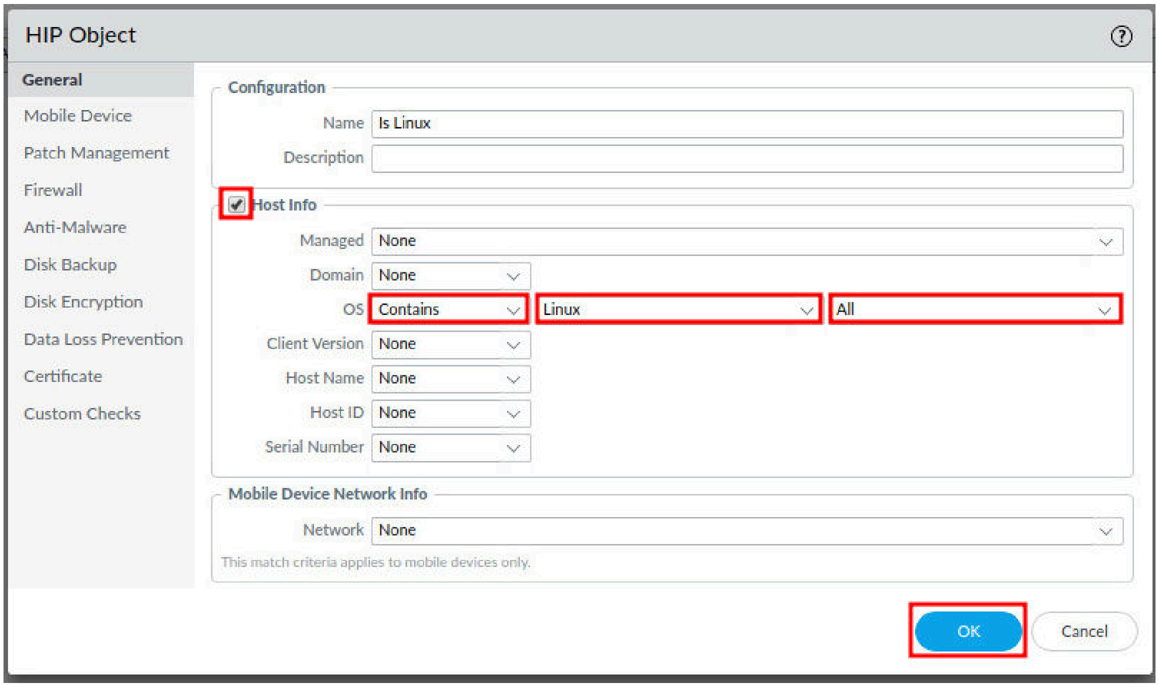


3. In the *HIP Object* window, type `Is Linux` in the *Name* field.



Name: Is Linux
Description:
□ Host Info
Managed: None
Domain: None
OS: None
Client Version: None
Host Name: None
Host ID: None
Serial Number: None
Network: None
This match criteria applies to mobile devices only.

4. In the *HIP Object* window, while on the *General* tab, check the checkbox for **Host Info** and then select **Contains** from the first dropdown menu for *OS,* followed by selecting **Linux** and then **All** for the remaining dropdown menus. Click **OK** once finished. You may need to adjust the window if the *GlobalProtect* window is still showing.



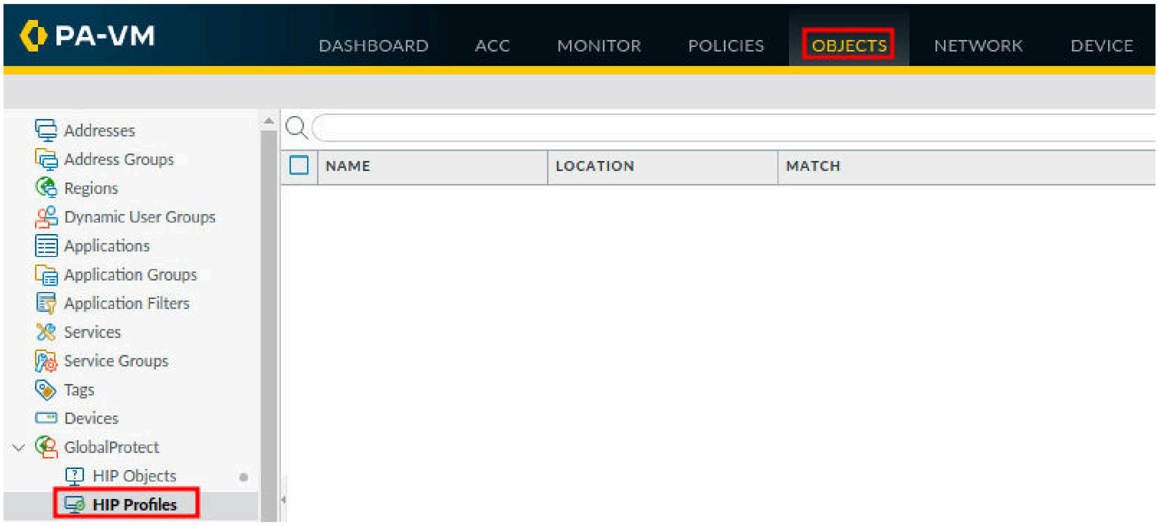
Name: Is Linux
Description:
☑ Host Info
Managed: None
Domain: None
OS: Contains | Linux | All
Client Version: None
Host Name: None
Host ID: None
Serial Number: None
Network: None
This match criteria applies to mobile devices only.

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

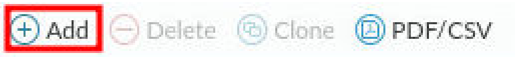
1.3 Create a HIP Profile

In this section, you will create a *HIP Profile* that will be combined with the *HIP Object* that you created. *HIP Profiles* allow administrators to collect information about the security status of the end device that will be connecting to the network via *GlobalProtect*.

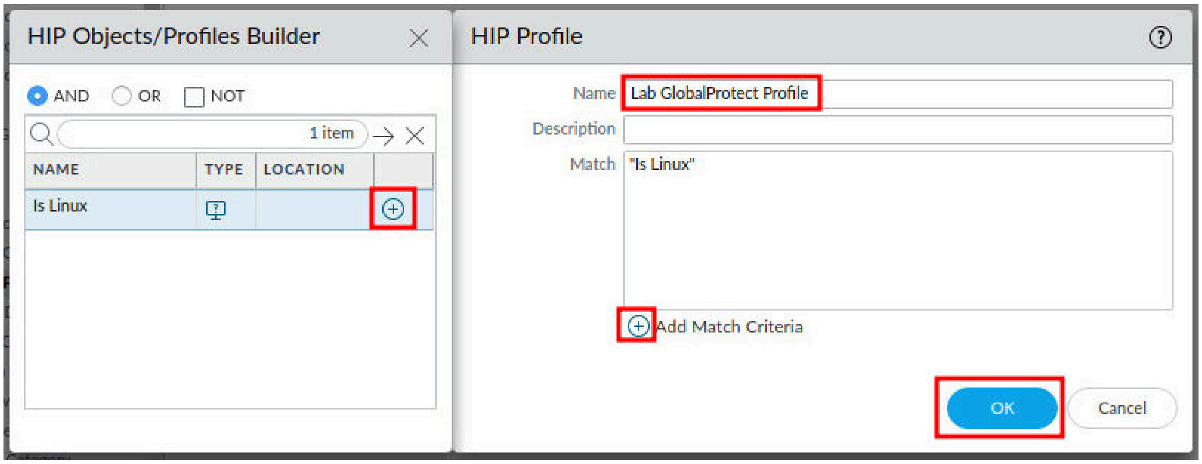
1. In the firewall web interface, navigate to **Objects > GlobalProtect > HIP Profiles**.



2. Click **Add** to add a new *HIP Profile*.



3. In the *HIP Profile* window, type `Lab GlobalProtect Profile` for the *Name* field. Then, click **Add Match Criteria**. Next, in the *HIP Objects/Profiles Builder* window, click the **+** icon to add **Is Linux** to the *Match* field of the *HIP Profile*. Finally, click the **OK** button.



Is Linux

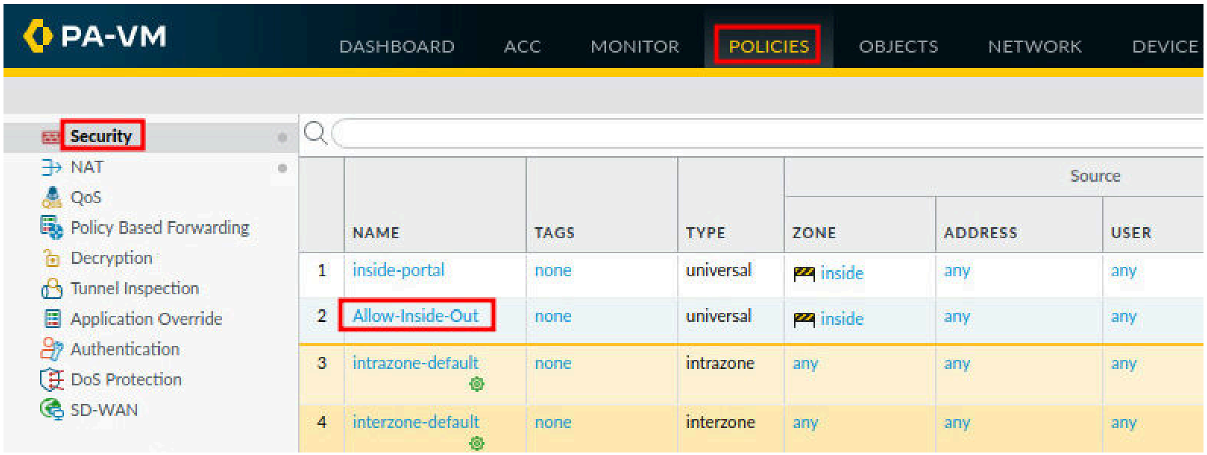
Name: Lab GlobalProtect Profile
Description:
Match: "Is Linux"

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

1.4 Modify Security Policy to Add HIP Profile

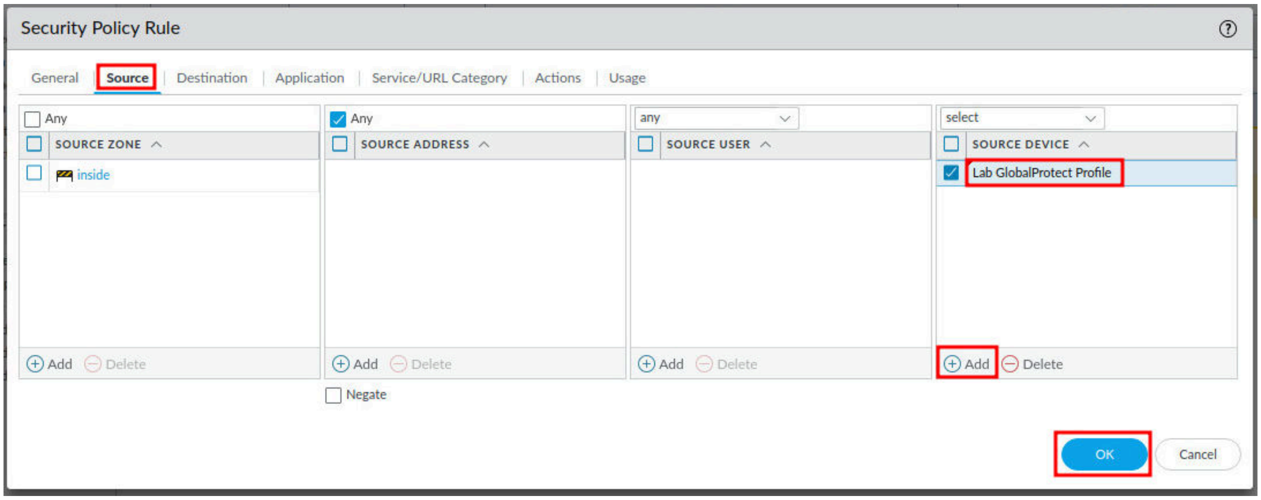
In this section, you will modify the *Allow-Inside-Out* Security Policy to add the *Lab GlobalProtect Profile* HIP Profile you created earlier.

1. In the firewall web interface, navigate to **Policies > Security > Allow-Inside-Out**.



				Source		
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	inside-portal	none	universal	inside	any	any
2	Allow-Inside-Out	none	universal	inside	any	any
3	intrazone-default	none	intrazone	any	any	any
4	interzone-default	none	interzone	any	any	any

2. In the *Security Policy Rule* window, click the **Source** tab. Then, click **Add** in the *Source Device* section. Next, select **Lab GlobalProtect Profile** from the dropdown. Finally, click the **OK** button.



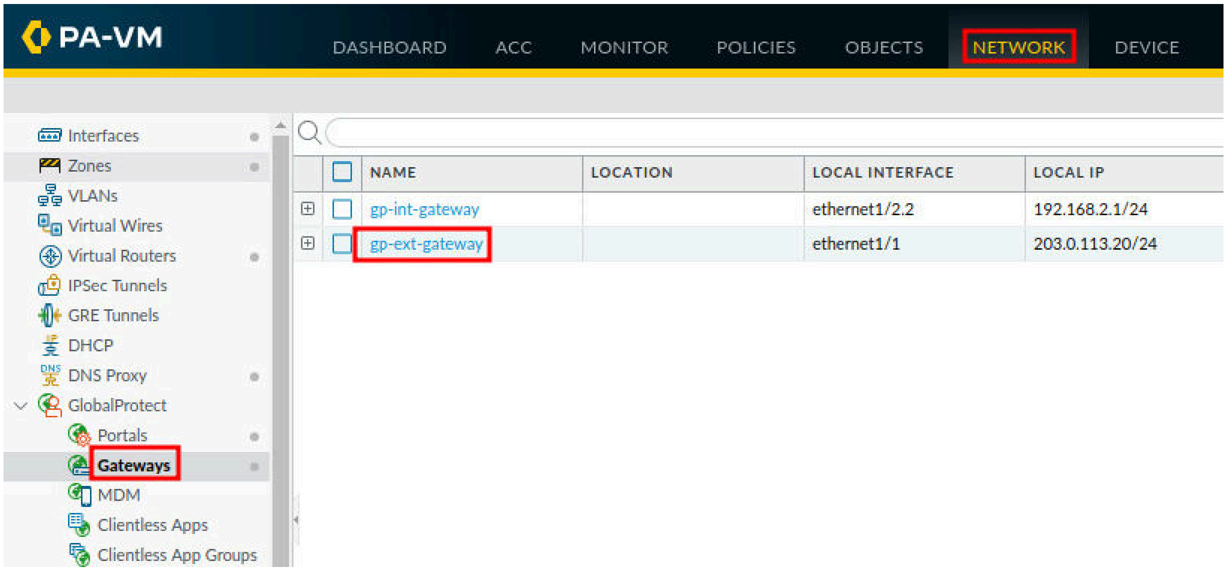
SOURCE ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DEVICE
□ inside			☑ Lab GlobalProtect Profile

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

1.5 Modify GlobalProtect Gateway to Add a HIP Notification and Commit

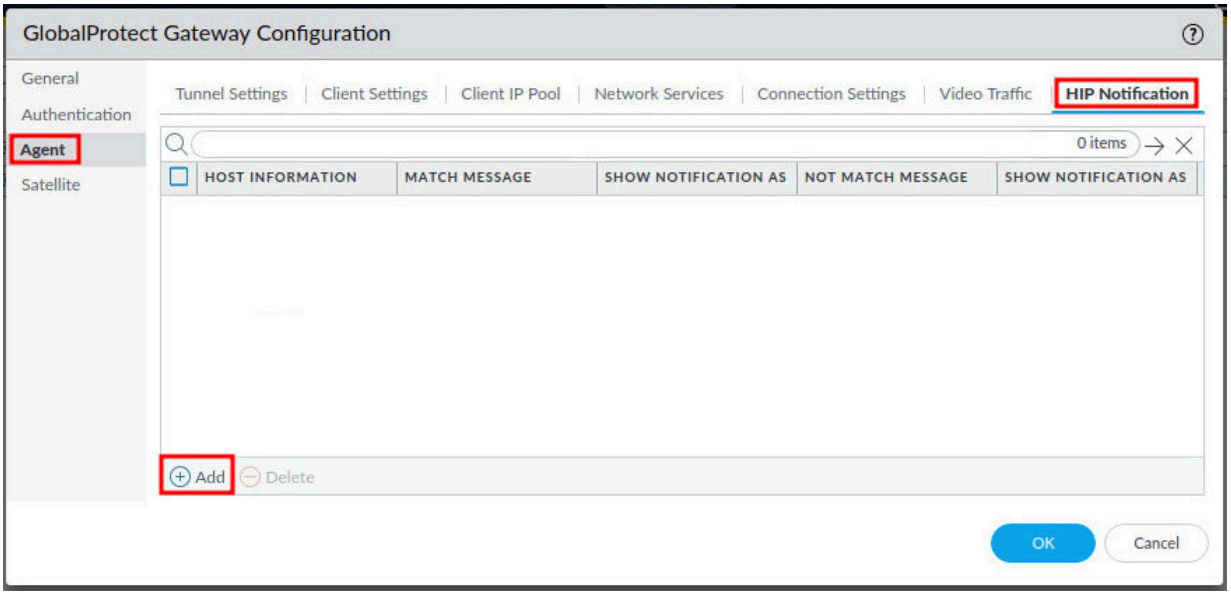
In this section, you will modify the *gp-ext-gateway* gateway to create a *HIP Notification*. *HIP Notification* messages are what a client machine sees when a security rule, with a Host Information Profile enabled, is enforced. Then, you will commit your changes to the Firewall.

1. In the firewall web interface, navigate to **Network > GlobalProtect > Gateways > gp-ext-gateway**.

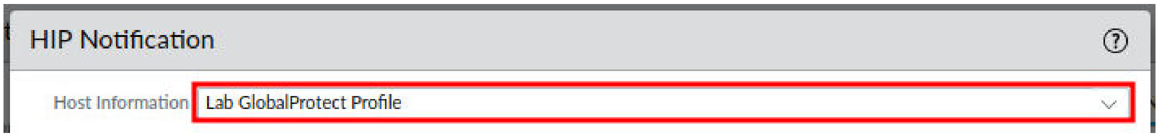


NAME	LOCATION	LOCAL INTERFACE	LOCAL IP
gp-int-gateway		ethernet1/2.2	192.168.2.1/24
gp-ext-gateway		ethernet1/1	203.0.113.20/24

2. In the *GlobalProtect Gateway Configuration* window, click the **Agent** tab on the left. Then, click the **HIP Notification** tab in the upper-right. Next, click the **Add** button.



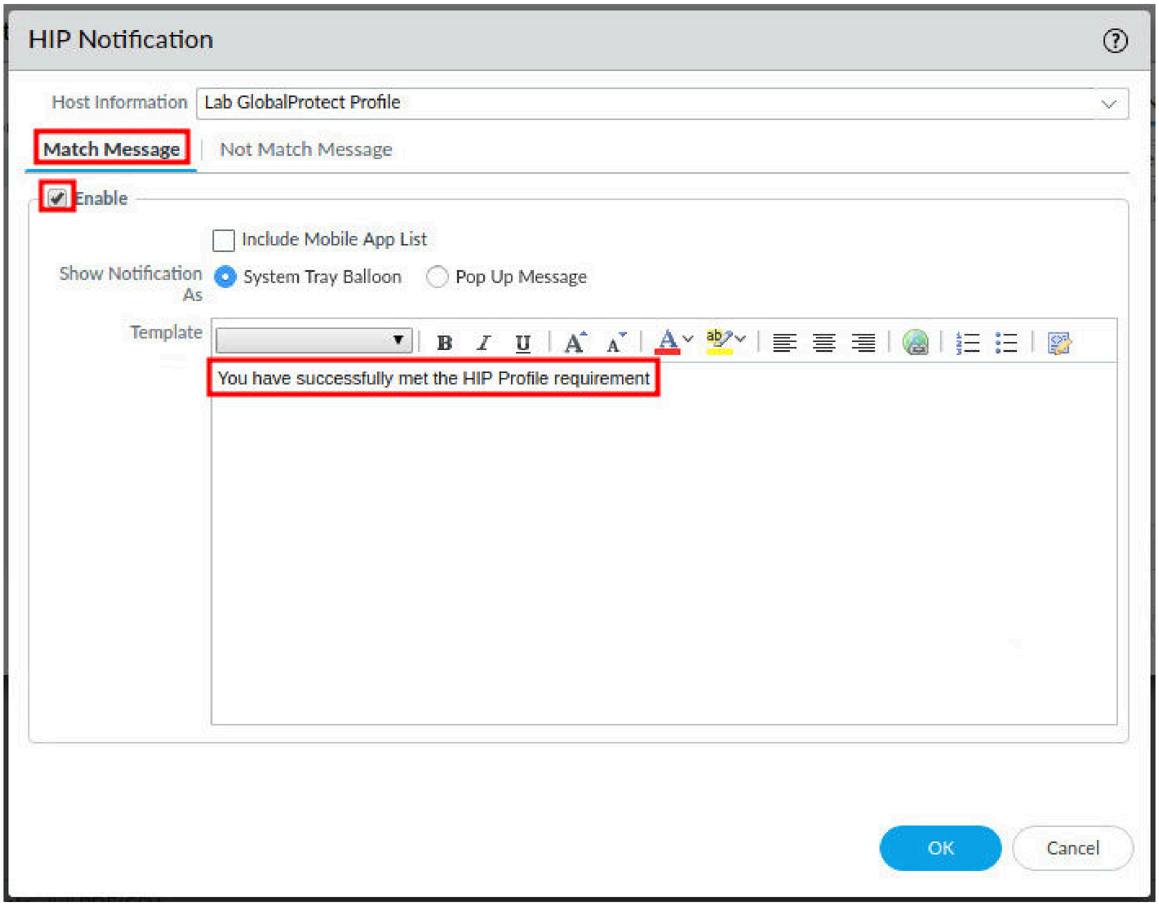
3. In the *HIP Notification* window, select **Lab GlobalProtect Profile** from the *Host Information* dropdown.



HIP Notification

Host Information: Lab GlobalProtect Profile

4. In the *HIP Notification* window, click on the **Match Message** tab. Then, click the **Enable** checkbox. Next, type `You have successfully met the HIP Profile requirement`.



HIP Notification

Host Information: Lab GlobalProtect Profile

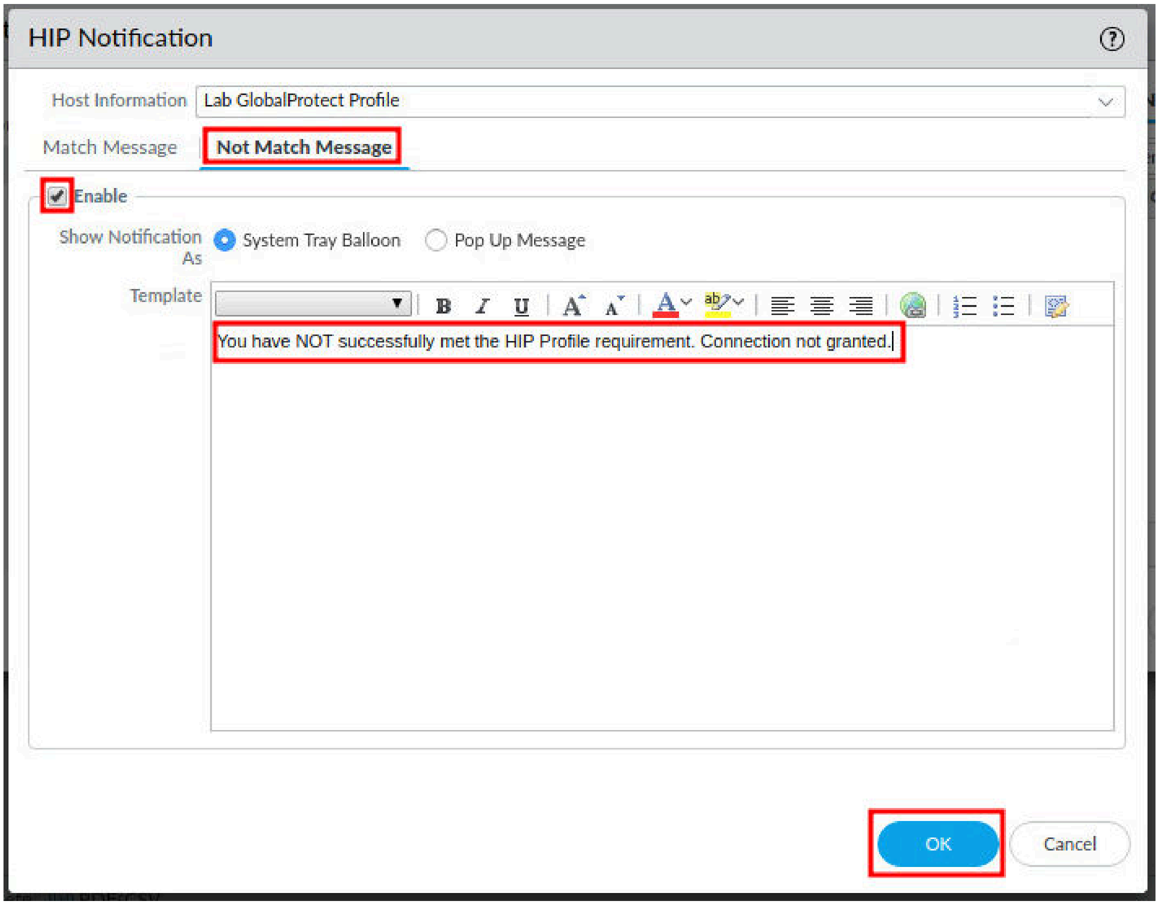
☑ Enable

□ Include Mobile App List

Show Notification As: ● System Tray Balloon ○ Pop Up Message

Template: You have successfully met the HIP Profile requirement

5. In the *HIP Notification* window, click on the **Not Match Message** tab. Then, click the **Enable** checkbox. Next, type `You have NOT successfully met the HIP Profile requirement. Connection not granted`**.** Finally, click the **OK** button.



HIP Notification

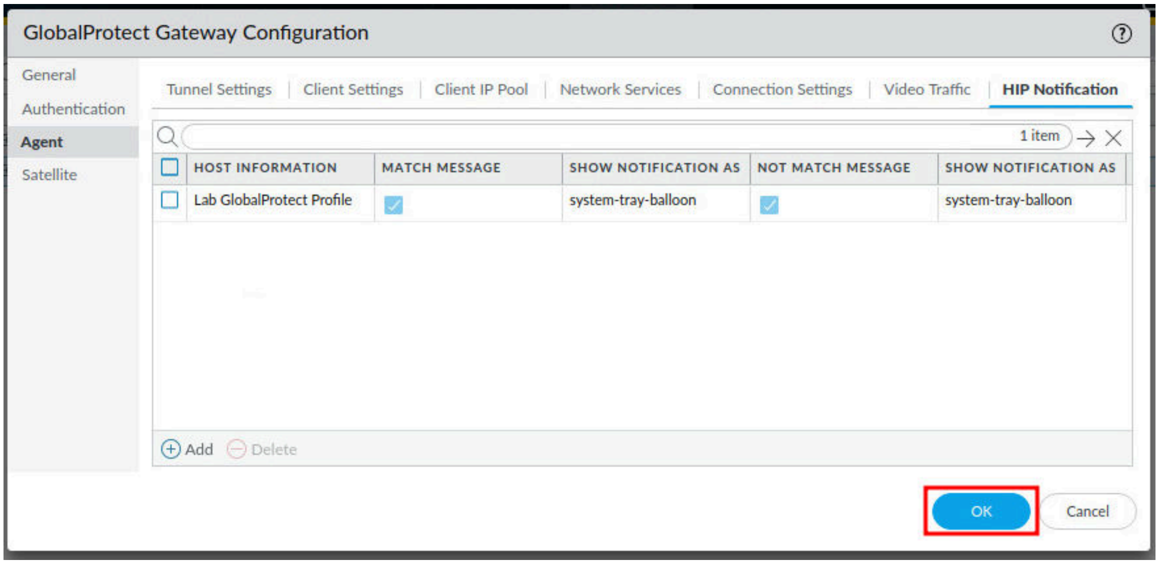
Host Information: Lab GlobalProtect Profile

☑ Enable

Show Notification As: ● System Tray Balloon ○ Pop Up Message

Template: You have NOT successfully met the HIP Profile requirement. Connection not granted.

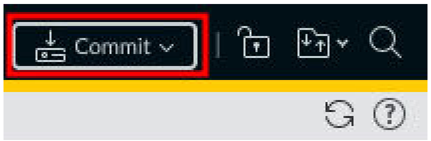
6. Back on the *GlobalProtect Gateway Configuration* window, verify the information and click the **OK** button.



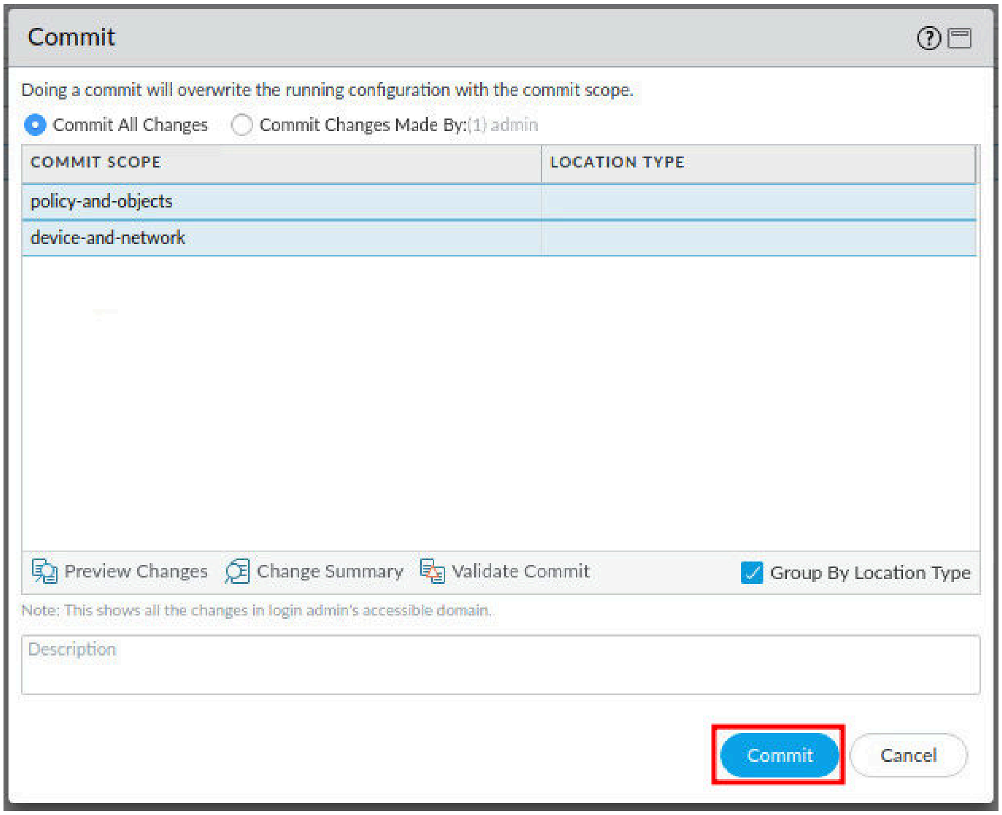
GlobalProtect Gateway Configuration

HOST INFORMATION	MATCH MESSAGE	SHOW NOTIFICATION AS	NOT MATCH MESSAGE	SHOW NOTIFICATION AS
Lab GlobalProtect Profile	✓	system-tray-balloon	✓	system-tray-balloon

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



8. In the *Commit* window, click **Commit** to proceed with committing the changes.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
device-and-network	

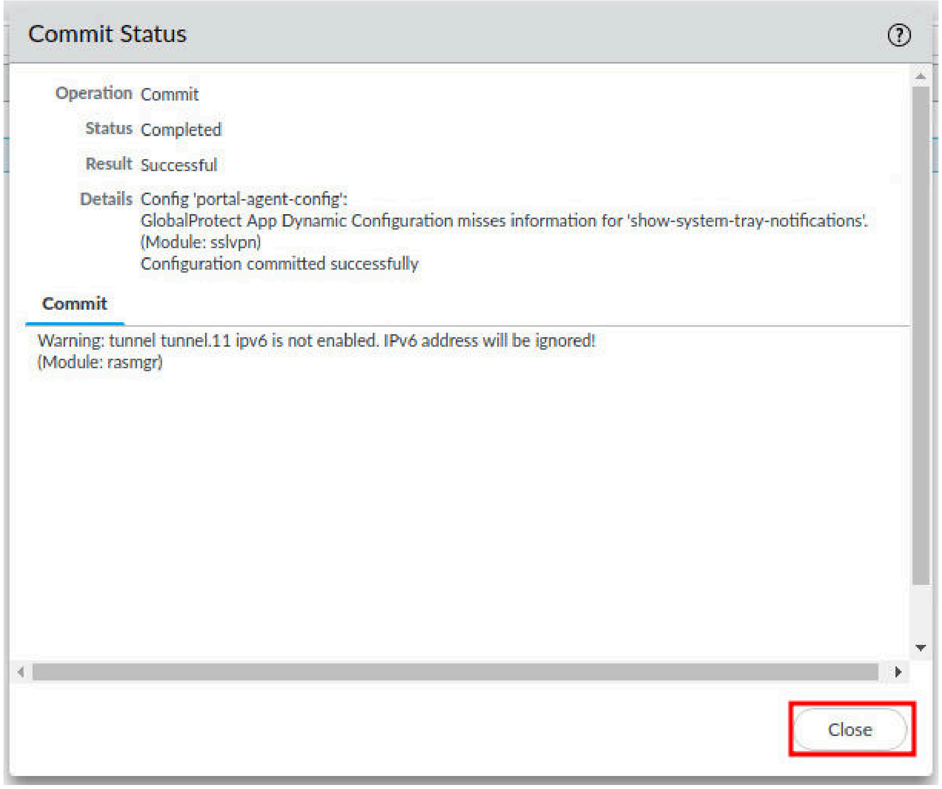
Preview Changes Change Summary Validate Commit ☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit Cancel

9. When the commit operation successfully completes, click **Close** to continue.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Config 'portal-agent-config':
GlobalProtect App Dynamic Configuration misses information for 'show-system-tray-notifications'.
(Module: sslvpn)
Configuration committed successfully

Commit

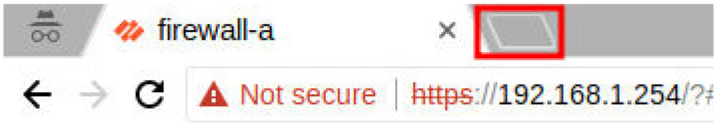
Warning: tunnel tunnel.11 ipv6 is not enabled. IPv6 address will be ignored!
(Module: rasmgr)

The **Warnings** displayed are normal. IPv6 has not been enabled for this lab and therefore this warning can be ignored.

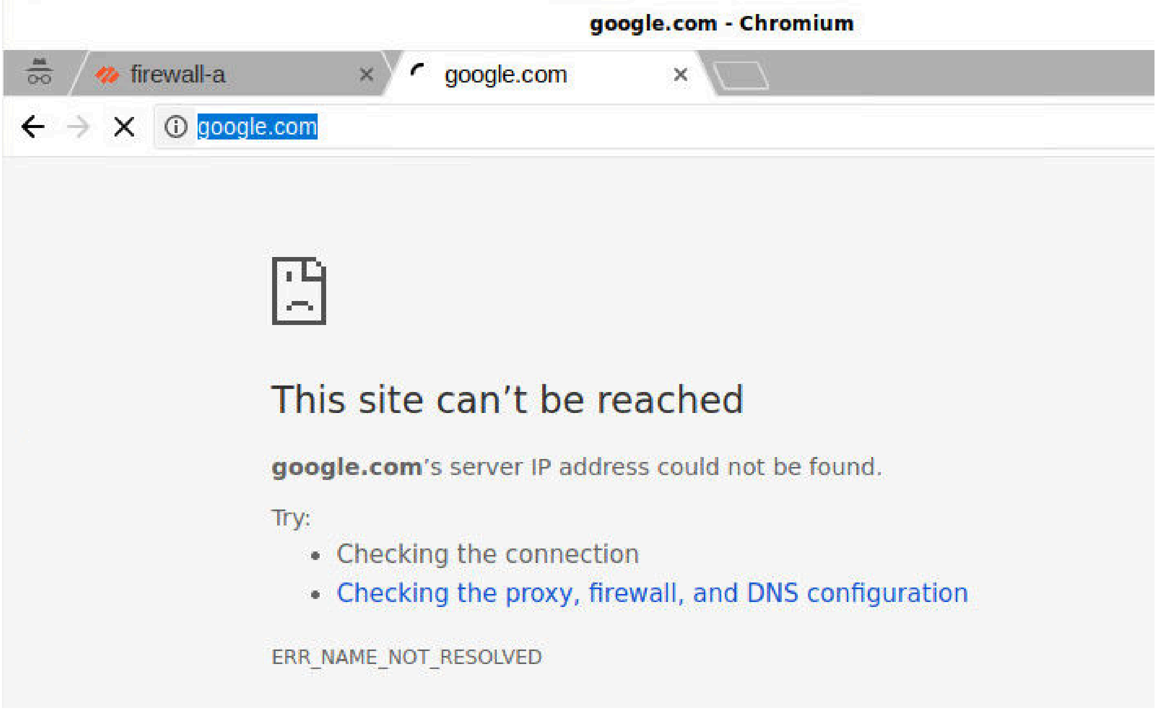
1.6 Configure and Connect the GlobalProtect Agent for Network Access

In this section, you will configure and connect the *GlobalProtect Agent* to allow Internet access via the *HIP Policy* you created.

1. Click on the **New tab** button.



2. In the address bar, type `http://google.com` and press **Enter**.



This site can’t be reached

google.com’s server IP address could not be found.

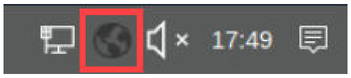
Try:

- Checking the connection
- Checking the proxy, firewall, and DNS configuration

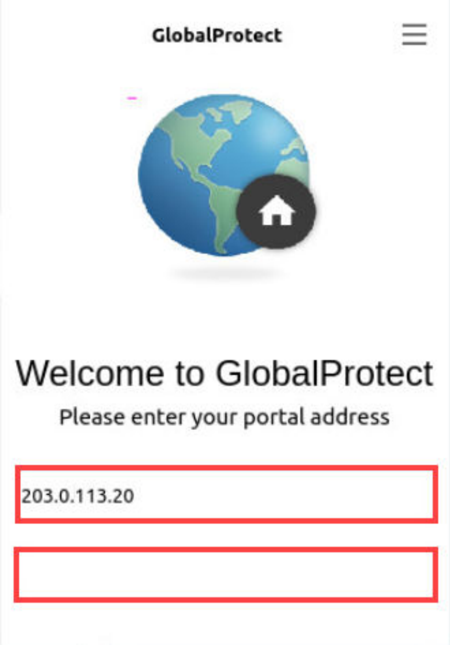
ERR_NAME_NOT_RESOLVED

Notice you get a *This page can’t be displayed* error message. The *Security Policy* you enabled blocks all traffic from the inside zone to the outside zone until a *GlobalProtect* connection is made.

3. On the taskbar, In the lower-right corner, click on the **GlobalProtect Agent** icon.



4. In the *GlobalProtect* window, type `203.0.113.20` as the portal address, followed by clicking on **Connect** (notice the *Connect* button may be hard to read. The red box below highlights the area for **Connect**.)

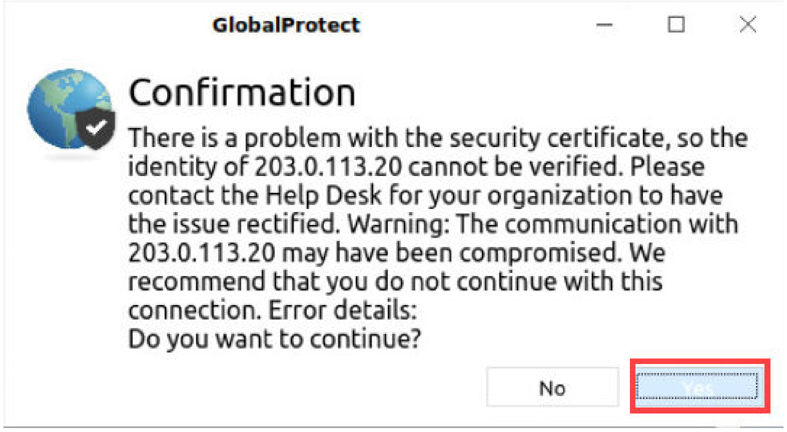


Welcome to GlobalProtect

Please enter your portal address

203.0.113.20

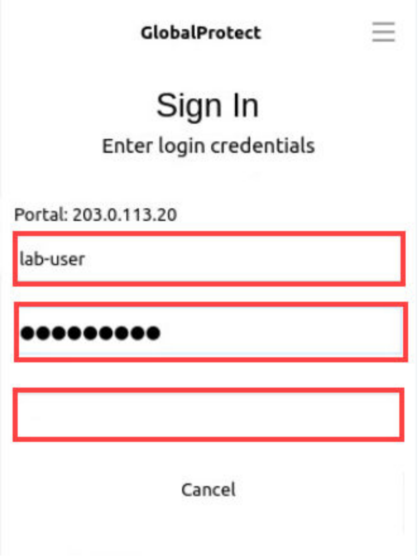
5. After a couple of seconds, notice a *GlobalProtect* message may appear about the certificate. Click **Yes** to connect.



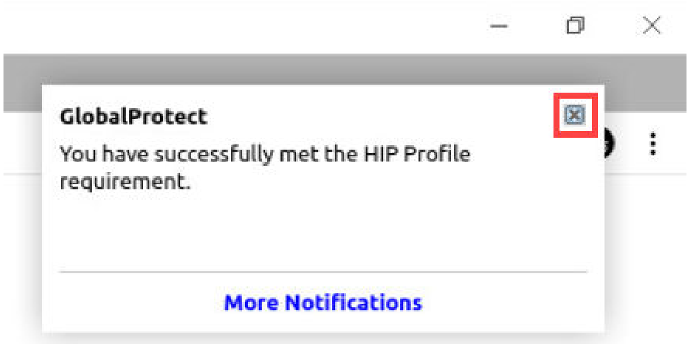
Confirmation

There is a problem with the security certificate, so the identity of 203.0.113.20 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified. Warning: The communication with 203.0.113.20 may have been compromised. We recommend that you do not continue with this connection. Error details:
Do you want to continue?

6. Notice the *GlobalProtect* login screen should appear. Log in as `lab-user` with `Pal0Alt0!` as the password. Click **Sign In** (notice the *Sign In* button may be difficult to read. The red box below highlights the area for **Sign In.**)



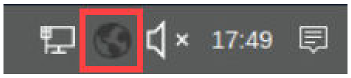
7. After about a minute, the GlobalProtect agent should successfully connect. Notice a *GlobalProtect Notification* window appears. Click the **X** in the upper-right to dismiss the message.


GlobalProtect

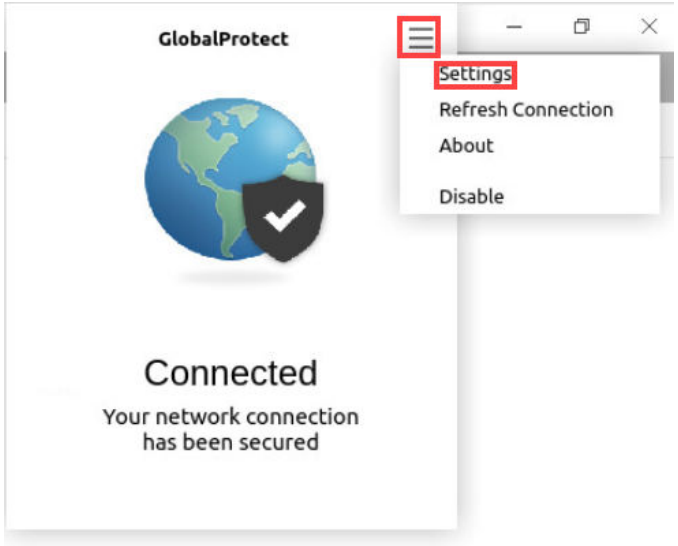
You have successfully met the HIP Profile requirement.

Notice the message matches the *Match HIP* notification you created earlier.

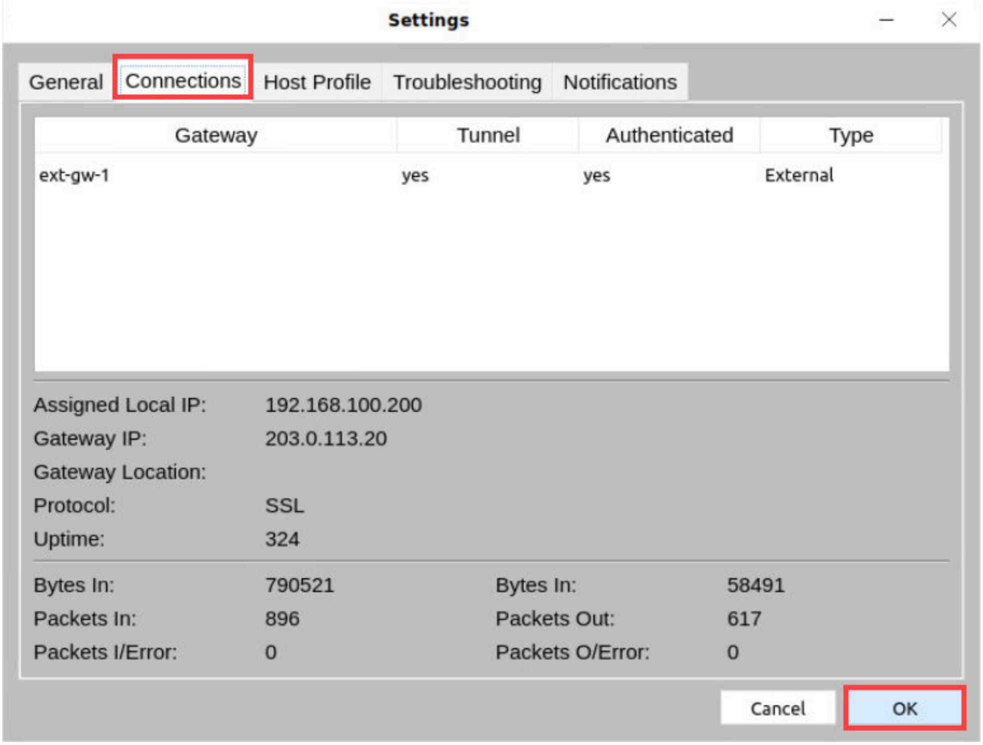
8. Once connected, click on the **GlobalProtect Agent** icon in the taskbar.



9. In the *GlobalProtect* window, click on the **Menu** icon in the top-right corner and select **Settings**.



10. In the *Settings* window, click on the **Connections** tab and notice the information available here, such as *Assigned Local IP* and *Gateway IP*. When finished reviewing, click **OK**.



Gateway	Tunnel	Authenticated	Type
ext-gw-1	yes	yes	External

Assigned Local IP: 192.168.100.200
Gateway IP: 203.0.113.20
Gateway Location:
Protocol: SSL
Uptime: 324

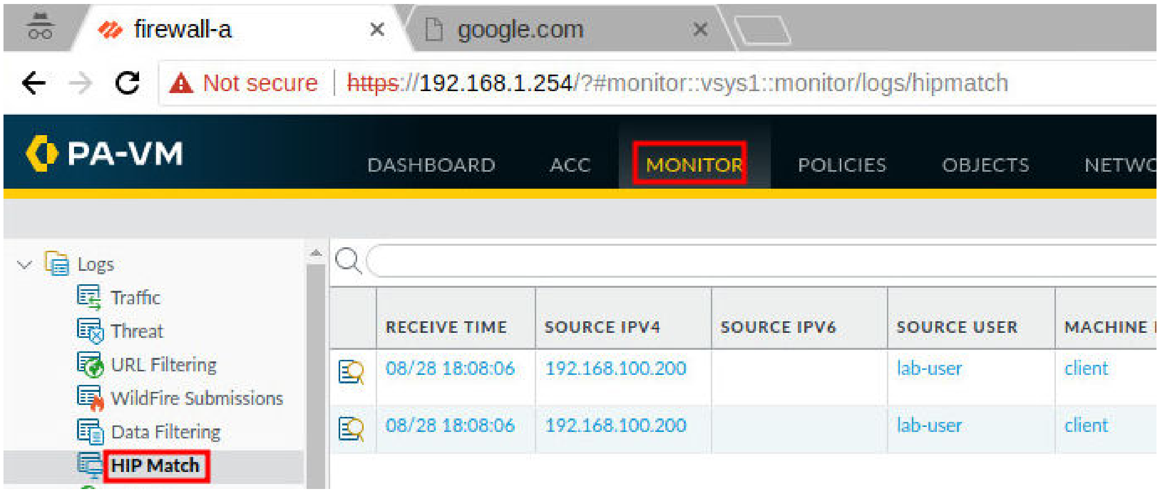
Bytes In:	790521	Bytes In:	58491
Packets In:	896	Packets Out:	617
Packets I/Error:	0	Packets O/Error:	0

Notice the gateway is 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. Additionally, the protocol listed may be IPSec instead of SSL.

1.7 View the GlobalProtect HIP Matches Logs

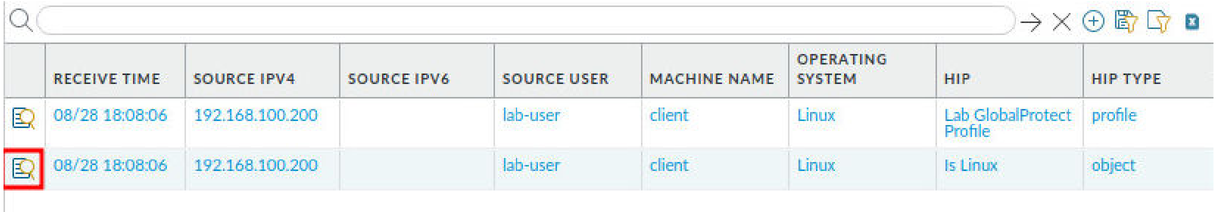
In this section, you will verify the *GlobalProtect HIP* matches by viewing the log information.

1. Change focus back to the firewall web interface and navigate to **Monitor > Logs > Hip Match**.



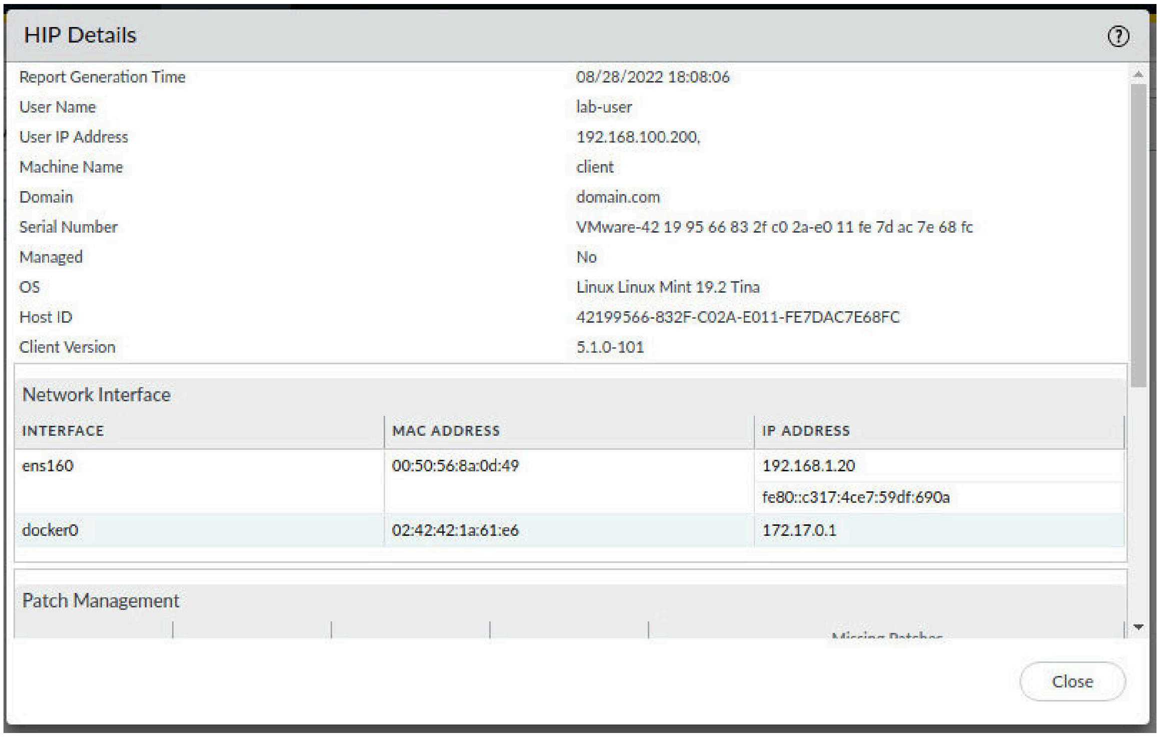
	RECEIVE TIME	SOURCE IPV4	SOURCE IPV6	SOURCE USER	MACHINE
	08/28 18:08:06	192.168.100.200		lab-user	client
	08/28 18:08:06	192.168.100.200		lab-user	client

2. Click on the **magnifying glass** icon for the *HIP Object* entry.



	RECEIVE TIME	SOURCE IPV4	SOURCE IPV6	SOURCE USER	MACHINE NAME	OPERATING SYSTEM	HIP	HIP TYPE
	08/28 18:08:06	192.168.100.200		lab-user	client	Linux	Lab GlobalProtect Profile	profile
	08/28 18:08:06	192.168.100.200		lab-user	client	Linux	Is Linux	object

3. In the *Log Details* window, notice all the information recorded about the client after a successful *GlobalProtect* connection has been established.



HIP Details

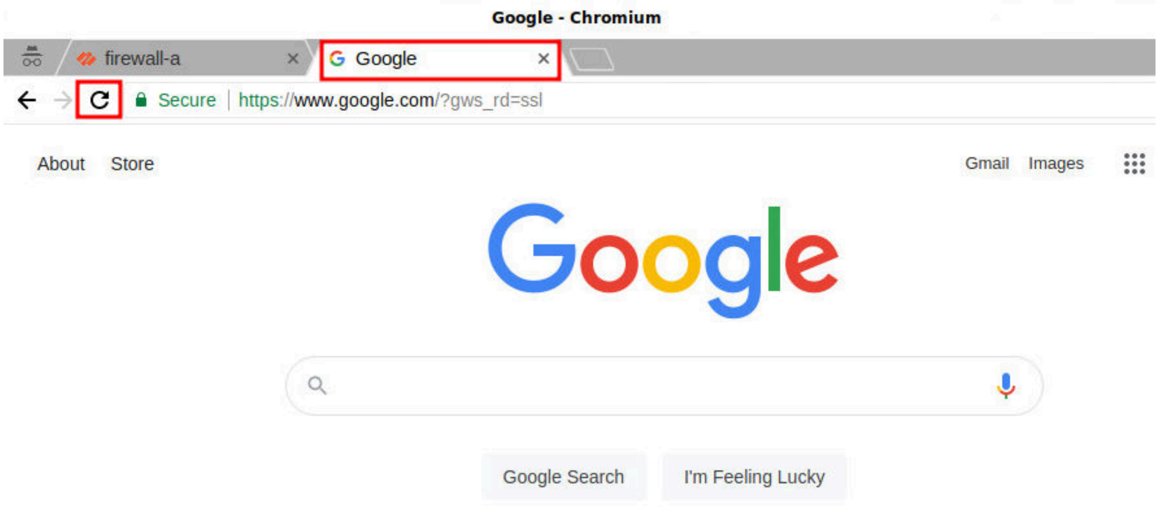
Report Generation Time	08/28/2022 18:08:06
User Name	lab-user
User IP Address	192.168.100.200,
Machine Name	client
Domain	domain.com
Serial Number	VMware-42 19 95 66 83 2f c0 2a-e0 11 fe 7d ac 7e 68 fc
Managed	No
OS	Linux Linux Mint 19.2 Tina
Host ID	42199566-832F-C02A-E011-FE7DAC7E68FC
Client Version	5.1.0-101

Network Interface

INTERFACE	MAC ADDRESS	IP ADDRESS
ens160	00:50:56:8a:0d:49	192.168.1.20 fe80::c317:4ce7:59df:690a
docker0	02:42:42:1a:61:e6	172.17.0.1

Patch Management

4. Navigate back to the tab that you tried to access Google with. Click **Reload** and notice google.com now loads due to Global Protect being properly configured and logged in.



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