Overview

Today's security teams must protect their data against modern threats while also providing security for users to:

- 1. Use the internet
- 2. Access applications in the data center
- 3. Access applications in the public cloud or SaaS

Palo Alto Networks **GlobalProtect** (GP) network security for endpoints builds upon 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... The GlobalProtect solution:

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









GlobalProtect has 3 main components:

- 1. GlobalProtect Portal central point of intelligence provides management functions for your GlobalProtect infrastructure
- 2. GlobalProtect Gateway(s) internal or external provides security enforcement for traffic from GlobalProtect agents/apps
- 3. GlobalProtect Clients Windows/UWP, Mac/iOS, Android/Chromebook, Linux

TIP – A GlobalProtect implementation requires at least one portal and one gateway.

- \checkmark The portal and gateway can be configured on the same firewall.
- ✓ In the simplest configuration, a single firewall is configured to serve portal and gateway services from the same IP address, which provides end users with VPN access to the internal networks with a minimum of configuration.
- ✓ If the portal and gateway share an IP address, only one certificate is needed for the firewall.
- ✓ The portal can act as a certificate authority (CA) for the system (using a self-signed or imported subordinate issuing a CA certificate within the portal), or customers can generate certificates using their own CAs. The portal, gateways, and agents must use certificates signed by the same CA.

There are some things you can do with GlobalProtect that do not require additional licensing, and there are some advanced GP features that require a GP subscription. The table below shows which features require the subscription.

Subscription Required?	Feature
No	Single, external gateway (Windows and Mac)
No	Single or multiple internal gateways
No	Multiple external gateways
Yes	HIP Checks
Yes	Mobile app for iOS endpoints, Android endpoints, Chromebooks, and Windows 10 UWP endpoints
Yes	IPv6 support
Yes	Linux agent
Yes	Clientless VPN

Objective

In this lab, we will learn how to implement GlobalProtect for secure remote access, using a single portal / single gateway, a self-signed certificate and local users.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab
Single GlobalProtect Gateway/Portal



<u>Tools</u>

- ✓ Palo Alto firewall
- ✓ Windows or Mac computer with Internet access

Target Devices

One or more of the following devices may be used as a GlobalProtect Portal or Gateway:

- ✓ Palo Alto hardware appliance firewall
- ✓ Palo Alto VM-series firewall

Lab Setup

Our lab setup consists of a Palo Alto firewall running PANOS 8.0.11-h1 and 2 remote access clients (1 Windows, 1 Mac) connected outside of the lab firewall (not on an inside zone). It is assumed that the Palo Alto firewall is already deployed on the network and the initial setup has been accomplished, including a layer-3 interface configured with a static public IP address. It is also assumed that the intrazone-default security rule is in effect, permitting all intra-zone traffic.







Lab Configuration Steps

1. Prepare the firewall for GlobalProtect - Certificates

a. Purpose

GlobalProtect needs multiple certificates, one for the portal and one for each gateway. These certificates are typically signed by a common CA certificate. In this lab we will combine the portal and gateway certificates because these GP functions are combined on the same IP address.

b. Location

Certificates are configured in the *Device* tab under *Certificate Management* - *Certificates* in the left menu and the *Device Certificates* subtab.



c. Create CA certificate and GP portal/gateway certificate

- i. Click the Generate button Generate at the bottom to create a CA certificate.
- ii. Enter a relevant Certificate Name and Common Name, leave Signed By blank, and select the Certificate Authority checkbox.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Certificate Name GlobalProtect-CA Common Name GlobalProtect-CA IP or FQDN to appear on the certificate Signed By Certificate Authority OCSP Responder Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Value	Certificate Type	Local SCEP	
Common Name GlobalProtect-CA IP or FQDN to appear on the certificate Signed By Certificate Authority OCSP Responder Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Value	Certificate Name	GlobalProtect-CA	
IP or FQDN to appear on the certificate Signed By ✓ Certificate Authority OCSP Responder ▲ Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365	Common Name	GlobalProtect-CA	
Signed By Certificate Authority OCSP Responder Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Value Value	1	P or FQDN to appear on the certificate	
Certificate Authority OCSP Responde Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Type Value	Signed By		1
OCSP Responder Cryptographic Settings Algorithm RSA Algorithm RSA Digest sha256 Expiration (days) Certificate Attributes Value Value	[Certificate Authority	
Cryptographic Settings Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Value Value	OCSP Responder		-
Algorithm RSA Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Value Value	- Cryptographic Set	tings	
Number of Bits 2048 Digest sha256 Expiration (days) 365 Certificate Attributes Type Value	Algorithm	RSA	v
Digest sha256 Expiration (days) 365 Certificate Attributes Type Value	Number of Bits	2048	-
Expiration (days) 365 Certificate Attributes Type Value	Digest	sha256	~
Certificate Attributes Type Value	Everytics (days)	265	
Type Value	Expiration (60)57		
Type Value	Certificate Attributes		
	Type	Value	
	🕂 Add 😑 Delete		
🛟 Add 🗖 Delete			
🛨 Add 🗖 Delete			
Add Delete			

- iii. Click the Generate button
- iv. Click **OK** to dismiss the successful status window.
- v. Click the Generate button at the bottom to create another certificate (for GP Portal and Gateway).
- vi. Enter a relevant Certificate Name. Use your firewall outside IP address for the Common Name. Click the dropdown next to Signed By and select the CA certificate that you created in the previous step. Leave the Certificate Authority checkbox unchecked.







Generate Certificate		
Certificate Type	Local SCEP	
Certificate Name	gp-portal-gw	
Common Name	50.63.202.9	
1	P or FQDN to appear on the certificate	
Signed By	GlobalProtect-CA	
1	Certificate Authority	
OCSP Responder		-
Cryptographic Set	ttings	
Algorithm	RSA	v
Number of Bits	2048	~
Digest	sha256	-
Expiration (days)	365	
Certificate Attributes		
Type	Value	
		10
🕂 Add 🖃 Delete		
	200	
	Generate	Cance
	Constants	

viii. Click **OK** to dismiss the successful status window. Your 2 certificates should look something like this in the list of device certificates:

Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm
🗸 🔄 GlobalProtect-CA	CN = GlobalProtect-CA	CN = GlobalProtect-CA	7	1	Aug 9 15:38:33 2019 GMT	valid	RSA
ggp-portal-gw	CN = 50.63.202.9	CN = GlobalProtect-CA			Aug 9 15:53:43 2019 GMT	valid	RSA

TIP – In a live production environment, as a Certificate Authority, the firewall would need to respond to revocation queries. Not covered in this lab, an OCSP Responder is configured in Device – Certificate Mgt – OCSP Responder (a reference URL is provided at the end of the lab).









For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

d. Associate the GP certificate with an SSL-TLS Service Profile - configured in the *Device* tab under *Certificate Management – SSL/TLS Service Profile* in the left menu.

paloalto	Dashboard ACC	Manitor Policies Objects Network	Device	
Setup Figh Availability Sa Config Audit	Name	Location	Certificate	Protocol Versions
Password Profiles S Administrators Admin Roles Authentication Brofile				
Authentication Sequence				
Certificate Management				
SSL/TLS Service Profile				
B SSL Decryption Exclusion Response Pages				

- i. Click the Add button Add at the bottom to create an SSL/TLS Service Profile.
- ii. Enter a relevant Name. Click the dropdown next to Certificate and select the GP certificate that you created in the previous step.

Certificate	pp-portal-gw	-
Protocol Settings		
Min Version	TLSv1.0	*
Max Version	Max	*

iii. Click **OK** to save the setting

2. Configure GlobalProtect User Authentication

a. Purpose

To authenticate users for access to corporate networks... In a production enterprise environment, it's recommended to configure LDAP authentication, preferably coupled with Multi-Factor Authentication. This lab uses local users.

b. Location

Local users are configured in the *Device* tab under *Local User Database – Users* in the left menu.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
	in the second second			<u>un</u>				
Setup High Availability Config Audit Rassword Profiles Administrators	Name	_					Location	
Admin Roles Authentication Profile Authentication Sequence User Identification VM Information Sources								
Certificate Management Certificates Certificate Profile CCSP Responder								
SSL/TLS Service Profile SSL/TLS Service Profile SCEP SSL Decryption Exclusion Response Pages								
E Log Settings ✓ ⑦ Server Profiles ③ SNMP Trap ③ Syslog								
Email RetTIP 아Netflow 옵션 RADIUS								
IACACS+ IA LDAP IA Kerberos 욕 SAML Identity Provider								
Multi Factor Authentication								

c. Create Local Users

- i. Click the Add button at the bottom to create a local user.
- ii. Populate the user name and password fields, and click OK.

Name	gpuser1
Mode	Password Password Hash
Password	
Confirm Password	
	Z Enable

- iii. Repeat this step and create a 2nd local user.
- d. Create a Local User Group configured in the *Device* tab under *Local User Database User Groups* in the left menu.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

aloalto	Dashboard ACC	Monitor Policies Objects	Network Device	
Setup High Availability	Name		Location	Local Users
Password Profiles Administrators Admin Roles Authentication Profile				
Authentication Sequence				
Gertificate Management Gertificates Gertificate Profile				
SSL/TLS Service Profile SSL/TLS Service Profile SSL/TLS Service Profile SSL				
Response Pages				
SIMP Trap Syslog				
Netflow				
Contractors Contractors Contractors				
SAML Identity Provider				
Users User Groups Checkled Log Export				

- i. Click the Add button Add at the bottom to create a local user group.
- ii. Enter a relevant group name.
- iii. Click the Add button Add and select a user that you created in the previous step (twice).

Local User Group		0
Name	gp-users	
All Local Users	User 🔺	
	gpuser1	
	gpuser2	
	🗣 Add 🛛 🗖 Delete	
	Child Channe	_
	ок с	ancel

iv. Click **OK** to save the setting. Your new local user group should look something like this in the list of user groups:

Name	Location 🔺	Local Users
gp-users		gpuser1
		gpuser2

e. Associate the Local User Group with an Authentication Profile - configured in the *Device* tab under *Authentication Profile* in the left menu.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

paloalto		Dashboard	ACC	Monitor	Poli cies	Objects N	letwork	Device			
Setup High Availability	•			_		ncknait			_		
Scorfig Audit Ressword Profiles		Name	Location		Failed Attempts (#)	Lockout Time (m	n) Allow	/ List	Authentication	Server Profile	Authentication Factors
Admin Roles											
Authentication Sequence User Identification VM Information Sources											

i. Click the Add button Add at the bottom to create an authentication profile.
ii. Enter a relevant Name. Click the dropdown next to Type and select Local

Name gp-auth	
Authentiaction Factors Advanced	
Authentication Factors Advanced	
Type Local Database User Domain	~
Username Modifier %USERINPUT%	-
Single Sign On Kerberos Realm	
Kerberos Keytab Click "Import" to configure this field X Import	

- iii. Click the **Advanced** tab.
- iv. Click the Add button and select the local user group that you created in the previous step.

Rising Technologies 🤎

	Name	gp-auth		
uthentication	Factors	Advanced		
Allow List				
Allow List	*			
gp-users				
S all				
Sigp-use	rs			
gpuser	1			
Upuser.	2			
Add De	alete cout			
Add De	slete cout Failed Attemp	s 0	_	
Add De Account Lock	elete cout Failed Attemp out Time (mir	s 0) 0		
Add De Account Lock	elete cout Failed Attemp out Time (mir	s 0) 0	ОК	Cano
Add De Add Count Lock	elete cout Failed Attemp out Time (mir	s 0) 0	OK	Canc





For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

v. Click **OK** to save the setting. Your new authentication profile should look something like this in the list of authentication profiles:

Name	Location	Failed Attempts (#)	Lockout Time (min)	Allow List	Authentication	Server Profile	Authentication Factors
gp-auth		0 (default)	0 (default)	S gp-users	Local		

3. Configure an External GlobalProtect Gateway and Tunnel Interface

a. Purpose

External GP Gateways provide security enforcement and VPN access for remote users. The gateway requires a tunnel interface for external clients.

b. Location

Tunnel interfaces are configured in the *Network* tab under *Interfaces* in the left menu and the *Tunnel* subtab.

	Dashboard	ACC Mor	nitor Policies	Objects Network	Device	
Interfaces Zones VLANs	Ethernet VLAN	Loopback Tuni	nel			
Virtual Wires Virtual Routers Difference IPSec Tunnels DHCP	Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features
♥ Conserved Conserved ♥ Conserved ♥ Cons						16

c. Create Tunnel Interface

- i. Click the Add button Add at the bottom to create a tunnel interface.
- ii. The read-only Interface Name is set to *tunnel*. In the adjacent field, enter a numeric suffix (1-9,999) to identify the interface.

Interface Name tunnel . 100 Comment Netflow Profile None Config IPv4 IPv6 Advanced	-
Comment Netflow Profile None Config IPv4 IPv6 Advanced	~
Netflow Profile None Config IPv4 IPv6 Advanced	~
Config IPv4 IPv6 Advanced	
Acrise Interface To	
Assign Interface 10	
Virtual Router default-vr	-
Security Zone inside	*







11

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

- iii. Under the **Config** tab, click the dropdown next to **Virtual Router** and select your default router.
- iv. Click the dropdown next to Security Zone and select your inside/trust zone.
- v. Click **OK** to save the setting. Your new tunnel interface should look something like this in the list of tunnel interfaces:

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features
tunnel.100		none	default-vr	inside	

TIP - For more granular control over GP client access into the internal network, create an independent zone for GP-VPN, just note that an additional security rule will be needed to permit traffic flow between the GP-VPN zone and your primary inside/trust zone.

d. Configure the External Gateway - configured in the *Network* tab under *GlobalProtect – Gateways* in the left menu.

paloalto	Dashboard AC	C Monitor Policies	Objects Network Devic	e	
Interfaces M Zones VLANs	Name	Location	Local Interface	Local IP	Tunnel
Virtual Wires Virtual Routers Image Contents EDHCP DHCP DHC					
ClobalProtect Portals Gateways					

- i. Click the Add button Add at the bottom to create a GP Gateway configuration.
- ii. Enter a relevant Name. Click the dropdown next to **Interface** and select your public facing layer-3 interface. Click the dropdown next to **IPv4 Address** and select the public IP address you want to use for GP Gateway.

way Configuration		(
Name]p-gateway	
Interface	ethernet1/3	~
IP Address Type	IPv4 Only	v
IPv4 Address	50.63.202.9/29	¥
		Dis Cancel
	Name Configuration Name Configuration Network Settings Interface IP Address Type IPv4 Address	Name gp-gateway Network Settings ethernet1/3 Interface ethernet1/3 IP Address Type IPv4 Only IPv4 Address 50.63.202.9/29

TIP – A loopback interface can be used in lieu of a physical interface address – this may be useful when adding multiple GP gateways using the same public-facing interface.

- iii. Click the Authentication tab on the left.
- iv. Click the dropdown next to **SSL/TLS Service Profile** and select the profile you created in an earlier step.







- v. Under the Client Authentication list box, click the Add button **G** Add to create a client authentication configuration.
- vi. Enter a relevant name. Under the **Authentication Profile** field, click **None** to reveal the dropdown, select the authentication profile you created in an earlier step.

eneral	Server Authentication				
uthentication	SSL/TLS Service P	rofile gp-portal-gw			
gent	Client Authenticatio	n			
atellite	Name	OS	Authentication Profile	Authentication Message	
accounter.	period a second s				
	♥ gp-local	Any	^r gp-auth	Enter login credentials	
	gp-local	Any	rgp-auth	Enter login credentials	
	gp-local	Any	gp-auth Down	Enter login credentials	

- vii. Click the Agent tab on the left.
- viii. Under the **Tunnel Settings** subtab, select the **Tunnel Mode** checkbox.
- ix. Click the dropdown next to **Tunnel Interface** and select the tunnel interface you created in an earlier step.
 - x. Verify that the Enable IPSec checkbox is selected.

General	Tunnel Cettings	Pattings Oligat Cattings Natural Convision UID Matiliastics	
Authentication	Tunnel Settings	Settings Client Settings Network Services HiP Notification	
Agont	Tunnel Mode		
Ayeni	Tunnel Interface	tunnel.100	~
Satellite	Max User	[1 - 250]	
		C Enable IPSec	
	GlobalProtect IPSec Crypto	default	*
		Enable X-Auth Support	
	Group Name		
	Group Password		
	Confirm Group Password		
		Skip Auth on IKE Rekey	

- xi. Click the **Client Settings** subtab, click the Add button **Add** to create a client settings configuration.
- xii. Under the Authentication Override tab, enter a relevant name.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

General	Tunnel Cottingo	Timon & Cottingo	Cotting	an Natural Consist	uiD Matifiaat	tion	
Authentication	runner oeunigs	Cheni	Semu	gs iverwork aervice	is mir wonnea	DOLI	
Agent	٩		_			0 items 😁 🙁	
	Configs						
Satemte	Configs	3					nindlik
		,					
	Auther	ntication Override User/U	ser Gro	up IP Pools Sp	lit Tunnel		
		Name gp-client-config					
	Auti	hentication Override					
			Ē	Generate cookie for	authentication over	rride	
			E	Accept cookie for au	thentication overrid	le	
		Cookie Life	etime	Hours	- 24		
	c	Certificate to Encrypt/Decrypt C	ookie	None			*
	🖶 Add						

xiii. Click the User/User Group tab. Under the Source User list box, click the Add button Add and manually enter the name of the *local user group* you created in an earlier step.

Configs	0
Authentication Override User/User Group IP Pools Split To	Innel
select	🗸 Any
Source User	os 🔺
gp-users	
and a second	
Add Delete	🛨 Add 🖨 Delete
	OK Cancel

xiv. Click the **IP Pools** tab. Under **IP Pool**, click the Add button and enter an available IP range for your GP clients.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Authentication Override	User/User Group	IP Pools	Split Tunnel				
Retrieve Framed-IP-Add	dress attribute from au	thentication s	erver				
Authentication Server	IP Pool			IP Pool			
Enter IP subnets or range 192.168.75.1-192.168.75 the authentication server	s (e.g. 192.168.74.0/ .100) to match the Fra	24, imed IP attrib	ute of	192.168.200	.100-192.168.200.	110	
🖶 Add 🛛 🖨 Decte			÷	Add 😑 Dele	te 💽 Move Up 🕻	Move Down	
These IPs will be added to the fin	ewall's routing table		These	IPs will be adde	d to the firewall's routi	ng table	

TIP – Split Tunneling can be disabled in order to route all remote user traffic through the GP connection, thereby facilitating content-id* scanning for mobile users (*additional licensing required).

xv. Click **OK** to close out the Configs window. The GP Gateway configuration window should still be open on the Client Settings subtab.

GlobalProtect Gate	eway Configuration					
General	Tunnel Cattingo Tim	Client	Cottingo	Natural Continen	LID Notification	
Authentication	Tunner Seturigs	sour aerrings Chenr	Settings	INELWORK SERVICES	The Notification	
Agent	•	2 2	122	22		1 item 🔿 🗙
Satellite	gp-client-config	Jser/User Group gp-users	OS any	IP Pool 192.168.200.100-	192.168.200.110	Include Access Route
	🕂 Add 📼 Delete 💿	Clone 💽 Move Up 💽 N	love Down			
						OK

xvi. Click the Network Services subtab. Enter public DNS server IP addresses in the Primary DNS and Secondary DNS fields.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

General	T						
Authentication	Tunnel Settings	meout Settings Client Settings Network Se	rvices HIP Notification				
A	Inheritance Source	one					
Agent		Check inheritance source status					
Satellite	Primary DNS	8.8.8					
	Secondary DNS	2.2.2					
	Primary WINS	one					
	Secondary WINS	None					
		Inherit DNS Suffixes					
	DNS Suffix	nter comma-separated DNS suffix for client (e.g. hr.r	nycompany.com, mycompany.com)				

TIP – To resolve internal domains, enter private DNS server addresses.
 TIP – If configuring Internal GP Gateway, the firewall would also need to be configured as a DNS Proxy.

xvii. Click **OK** to close the GP Gateway configuration window.

Upon expanding your GP Gateways list view, your new gateway should look something like this:

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device			📥 Commit 🧃 🖟
Interfaces	٩.	Name	Location		Local Interface	Local IP		Tunnel		Max User	Info
STS VLANS	3 [gp-gateway			ethemet1/3			bunnel.	100		Remote Users
Virtual Routers		Agent Configu	ration	Users			05		IP Pool	Authentication IP Pool	Access Route
PSec Tunnels		gp-client-confi	g	go-us	ers		алу		192.168.200.100-192.158.200.11	j	
Cobal Proxy Gobal Protect Fortals											

*This may be a good point to pause, to validate and commit your changes.

4. Configure GlobalProtect Portal

a. Purpose

The GP Portal provides the management functions for the GP infrastructure. Every endpoint that participates in the GP network receives its configuration from the portal.

b. Location

GlobalProtect Portals are configured in the *Network* tab under *GlobalProtect* – *Portals* in the left menu.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

paloalto	Dashboard	ACC Monitor	Policies Objects	Network Device	1		🏝 Con
(11) Interfaces (11) Zones 양 VLM's 영 Vinual Nines 양 Vinual Routers 대 IPSec Turnel's 중 CHCP	Name	Location	Interface	đ	SSL/TLS Service Profile	Authentication Profile	Certificate Profile
DNS Proxy ClobalProtect Portals Control Documents Documents							

c. Configure the Portal

- i. Click the Add button ^{G Add} at the bottom to create a GP Portal configuration.
- ii. Enter a relevant Name. Click the dropdown next to **Interface** and select your public facing layer-3 interface. Click the dropdown next to **IPv4 Address** and select the public IP address you want to use for GP Portal.

		0
Name	gp-portal	
Network Settings		
Interface	thernet1/3	~
IP Address Type	Pv4 Only	v
IPv4 Address	0.63.202.9/29	-
Appearance		
Portal Login Page	lone	v
Portal Landing Page	lone	~
App Help Page	lone	~
	OK	Cancel
	Name Network Settings Interface IP Address Type I IPv4 Address Appearance Portal Login Page App Help Page I	Name gp-portal Network Settings ethernet1/3 IP Address Type IPv4 Only IPv4 Address 50.63.202.9/29 Appearance Portal Login Page None None None None None None None Non

TIP – A loopback interface can be used in lieu of a physical interface address – this may be useful when adding multiple GP portals using the same public-facing interface.

- iii. Click the Authentication tab on the left.
- iv. Click the dropdown next to **SSL/TLS Service Profile** and select the profile you created in an earlier step.
- v. Under the Client Authentication list box, click the Add button ^{G Add} to create a client authentication configuration.
- vi. Enter a relevant name. Under the **Authentication Profile** field, click **None** to reveal the dropdown, select the authentication profile you created in an earlier step.







17

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

ieneral	Server Authentication							
uthentication	SSL/TLS Service Prot	SSL/TLS Service Profile gp-portal-gw						
igent	Client Authentication							
No and a second	Name	OS	Authentication Profile	Authentication Message				
IIEDHESS VPN								
atellite	gp-local	Any	gp-auth	Enter login credentials				
atellite	gp-local	Any Sone 💽 Move Up 💽 Move	gp-auth	Enter login credentials				

xviii.

Click the **Agent** tab on the left.

xix. Under the Agent list box, click the Add button • to create an agent config. Enter a relevant name.

GlobalProtect Por	tal Configuration				0	
General	Agent					
Authentication	🔲 Configs	User/User Group	os	External Gateways	Client Certificate	
Agent	Config	gs				0
Clientless VPN	Auth	entication User/User Group	Internal Ext	ternal App Data Colle	ction	
Satellite		Nar	me gp-agent-config			ļ.
		Client Certifica	ate None	v		
	P 4//	Save User Credenti	als Yes	ertricate including its private key wil	t be installed on client machines.	
	- Au	thentication Override				
	Trust		Generate coo	okie for authentication override	2	
			Accept cooki Hours	e for authentication override		
	-	ertificate to Encrypt/Decrypt Cook	ie None			~
	- Co	mponents that Require Dynam	mic Passwords (Tv	wo-Factor Authentication)		
		Portal			External gateways-manual only	
		Internal gat	teways-all		External gateways-auto discovery	
	Selec	t the options that will use dynamic passw new credentials for each selected option	vords like one-time passv I.	word (OTP) to authenticate users as (opposed to using saved credentials. As a result, the user will always be p	rompted to
					ОК	Cancel

xx. Click the User/User Group tab. Under the User/User Group list box, click the Add button Add and manually enter the name of the *local user group* you created in an earlier step.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Configs	0
Authentication User/User Group Internal External App	Data Collection
🖾 Any	select 👻
🔲 OS 🔺	User/User Group
	gp-users
🗣 Add 💭 Delete	🕄 Add 🗖 Delete
	OK Cancel

- xxi. Click the **External** tab.
- xxii. Under the **External Gateways** list box, click the Add button ^{Add} to add an external gateway. Enter a relevant name.
- xxiii. Next to Address, select the IP radio button.
- xxiv. Type the IP address of your GP Gateway in the IPv4 field.
- xxv. Under the Source Region list box, click the Add button and accept the defaults **Any** source region and **Highest** priority.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Addreshication	User/User Group	Internal	External	Арр	Data Collec	tion		
Cutoff Time	(sec) 5							
External Gate	iways							
External Ga	teway					0		
	Name ext-gw							
	Address 🔘 FQDN 🚺	• IP						
	IPv4 50.63.202.9							
	IPv6							
<u></u>					1 item	→ ×		
Source	Region			Priorit	y			
Any				nigne	st			
						- 1		
						- 1		
						- 1		
e Add	1 Delate							
🕀 Add 🗧) Datete	ally calact this	atousv			_		
Add C) Dolete al (The user can manu	ally <mark>select t</mark> his	gateway)				ОК	G
€ Add C) Dollar al (The user can manu	ally select this	gateway)	OK	Ca	ncel	ок	Ca

Under App Configurations, next to Connect Method, change the selection to On-demand (Manual user initiated connection).

Ann Configur	ations				Walsons Dr.	Nese	11
Connect Metho	od	On-demand (M initiated conne	lanual user ction)	Disable Glob	alProtect App	None	
GlobalProtect /	App Config Refresh	24 [1 - 168]			Passcode		
Allow User to I GlobalProtect /	Disable App	Allow		Co Max Times U	onfirm Passcode	0	
Allow User to U GlobalProtect /	Upgrade App	Allow with Pro	mpt	Disable	le Timeout (min)	0	
Use Single Sign Only)	n-on (Windows	Yes		Mobile Secur	rity Manager Sel	ttings	
Clear Single Si on Logout (Wi	gn-On Credentials ndows Only)	Yes		Mobile	Security Manager		
Use Default Au Kerberos Autho (Windows Only	uthentication on entication Failure y)	Yes			Enrollment Port	443	7
Automatic Res Connection Tin	toration of VPN meout (min)	30 [0 - 180]					
Wait Time Bet Connection Re	ween VPN store Attempts	5 [1 - 60]					

TIP – The **Always On** GP app connection methods will facilitate more security when coupled with disabling split tunneling.







xxviii. Click **OK** twice to close Configs and GlobalProtect Portal configuration windows.

Upon expanding your GP Portals list view, your new portal should look something like this:

ALCONG.	-	Jashbuard	Nou	manitor	r oneisis obje		LIGVICO		jur de	S (
Interfaces	•	_	_							1. Steen
Zones		Name	Location	Interfac	ue .	IP	SSL/TLS Service Profile	Authentication Profile	Certificate Profile	Info
Es virtual Wires	3 🗆	gp-portal		etherne	:11/3	50.63.202.9/29	gp-portal-gw			
Virtual Routers		Agent Config.	uration	Users	05		Options	External GWs	Internal GWs	Connect Method
DHCP		gp-agent-coni	fig	gp-users	any			ext-gw	Not configured	On-demand (Manual user initiated connection)
7 🖏 GiobalProtect										
Rortals										
Gateways										

- d. Host the GP Agent on the Portal configured in the *Device* tab under *GlobalProtect Client* in the left menu.
 - i. Click Check Now. The firewall checks for latest version of the GP agent.

NETWORKS.	Dashooard	AGC Monik	Poncies Objects	Network	ce	
T Syslog	۹.					
Email	Version	Size	Release Date 🕶	Downloaded	Currently Activated	Action
Netflow	4.1.3	57 MB	2018/07/20 14:31:04			Download
B RADIUS	4.1.2	57 MB	2018/05/14 06:27:38			Download
TACAC5+	4.1.1	57 MB	2018/04/25 10:21:41			Download
LDAP	4.0.8	39 MB	2018/04/11 19:58:43			Download
Kerberos	4.1.0	57 MB	2018/03/03 21:11:02			Download
SAML Identity Provider	4.0.7	39 MB	2018/02/21 15:03:33			Download
Aulti Factor Authentication	4.0.6	39 MB	2018/01/12 14:00:31			Downlog
Local User Database	4.0.5	39 MB	2017/12/01 20:19:33			Downioa
S Users	4.0.4	39 MB	2017/10/12 18:55:26			Downlos
🥵 User Groups	4.0.3	39 MB	2017/09/01 15:47:38			Downlos
Scheduled Log Export	4.0.2	39 MB	2017/05/24 23:16:08			Downlos
Software	316	44 MB	2017/02/23 15:23:55			Downlog
GobalProtect Client	4.0.0	39 MB	2017/01/30 15:32:12			Downloa
Dynamic Updates	3.1.5	44 MB	2017/01/04 17:17:38			Downloa
S Licenses	214	d5 MB	2016/11/07 11:40:46			Downlos

ii. If necessary, click **Download** next to the latest version.

Version	Size	Release Date 💌	Downloaded	Currently Activated	Action	
4.1.4	57 MB	2018/08/06 17:42:34			Download	
4.1.3	57 MB	2018/07/20 14:31:04				
4.1.2	57 MB	2018/06/14 06:27:38	whicad GlobalProtect Ci	ient		U
4.1.1	57 MB	2018/04/26 10:21:41	Operation Download			
4.0.8	39 MB	2018/04/11 19:58:43	operation bownload			
4.1.0	57 MB	2018/03/03 21:11:02	Status Completed			
4.0.7	39 MB	2018/02/21 15:03:33	Result Successful			
4.0.6	39 MB	2018/01/12 14:00:31	Details Successfully			
4.0.5	39 MB	2017/12/01 20:19:33	Preloading in			
4.0.4	39 MB	2017/10/12 18:55:26	Successfully I			
4.0.3	39 MB	2017/09/01 15:47:38	Warnings			
4.0.2	39 MB	2017/05/24 23:16:08				
3.1.6	44 MB	2017/02/23 15:23:55				
4.0.0	39 MB	2017/01/30 15:32:12				
3.1.5	44 MB	2017/01/04 17:17:38				
3.1.4	45 MB	2016/11/07 11:40:46				
3.1.3	44 MB	2016/10/24 12:23:06				
3.1.1	44 MB	2016/08/25 15:41:38				

iii. Click Activate (or Reactivate) for the GP agent that you've just downloaded.







Version	Size	Release Date 🐨	Downloaded	Currently Activated	Action		
4.1.4	57 MB	2018/08/06 17:42:34	¥		Activate		
4.1.3	57 MB	2018 Activate GlobalPr	8 Activate Global Protect Client version 4.1.4				
4.1.2	57 MB	2018	OLECT OREITE VEISION 4.1.	•			
4.1.1	57 MB	2018 👩 This wi	This will activate a new version of GlobalProtect Client software that will be do on GlobalProtect user's computer when they connect the next time. Do you w				
4.0.8	39 MB	2018 0n Glot					
4.1.0	57 MB	2018 Continu	er				
4.0.7	39 MB	2018					
4.0.6	39 MB	2018		Yes No			
4.0.5	39 MB	2017					

iv. Click **Yes**, and then click **Close** after the client package activation is completed.

	Dashboard	ACC Monito	or Policies Objects	Network De	vice	
Log Settings	۹.					
Server Profiles	Version	Size	Release Date 🖛	Downloaded	Currently Activated	Action
SNMP Trap	414	57 M8	2018/08/05 17:42:34	-		Reactivate
Email	413	57 MB	2018/07/20 14:31:04	1.22		Download
HTTP	4.1.2	57 MB	2018/06/14 06:27:38			Download
Nethow	4.1.1	57 MB	2018/04/25 10:21:41			Download
RADIUS	4.0.8	39 MB	2018/04/11 19:58:43			Download
A TACACS+	4.1.0	57 MB	2018/03/03 21:11:02			Download
LDAP	4.0.7	39 MB	2018/02/21 15:03:33			Download
Kerberos	4.0.6	39 MB	2018/01/12 14:00:31			Download
SAML Identity Provider	4.0.5	39 MB	2017/12/01 20:19:33			Download
Multi Factor Autoentication	4.0.4	39 MB	2017/10/12 18:55:26			Download
Rener Street	4.0.3	39 MB	2017/09/01 15:47:38			Download
S User Groups	4.0.2	39 MB	2017/05/24 23:16:08			Download
Scheduled Log Export	3.1.6	44 MB	2017/02/23 15:23:55			Downkiad
Software	4.0.0	39 MB	2017/01/30 15:32:12			Download
ClobalProtect Client	3.1.5	44 MB	2017/01/04 17:17:38			Download
Dynamic Updates	3.1.4	45 MB	2016/11/07 11:40:46			Download

*Be sure to validate and commit your changes!

TIP - For more granular control over external connectivity to the GP Portal and Gateway, consider creating two intrazone security policy rules for your outside/untrust zone, with your portal/gateway IP address as the destination: 1 rule at the top permitting only certain applications for GP (ssl, web-browsing, panos-global-protect and ipsec-esp-udp), and only from select source public IP/blocks if you so desire; and the 2nd rule would be a deny rule dropping any other connection to your portal/gateway public IP address (the assumption also is that you do **not** have an Interface Mgmt profile on your public-facing interface permitting HTTPS Mgt of the firewall). In this lab, the intrazone-default security rule accommodates both external connection with the portal/gateway, as well as internal access for GP users after they have successfully established a tunneling session with the gateway.

5. Download the GP Agent

a. Purpose

Remote access clients require the GP Agent software in order to establish GP connectivity (Clientless VPN being exception to this rule, not covered in this lab).

b. Location

https://IP address of your GP Portal.







For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

- c. Download GP Agent software
 - i. On Windows or Mac client, open a web browser and https browse to the public IP address of your GP Portal. Proceed past the certificate error.

	paloalto	
	GlobalProtect Portal Name Password LOG IN	
ii.	Log in using one of the loc paloalto	cal users you created in an earlier step.
	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.	
iii. iv.	Download and install the a Click the GP agent in the Not Connected or or	uppropriate GP agent for your OS. Windows desktop system tray or Mac menu bar











STIP - You can configure multiple portals via gear icon in the upper-righthand corner

- vi. Click Continue when presented with a certificate warning (or you can choose to install the certificate on your computer).
- vii. Log in using one of the local users you created in an earlier step, and then click Sign In. If you have further issues with invalid/untrusted certificate error, you will need to install the CA certificate (the 1st certificate that you created in an earlier step) into the Trusted Root Certification Authorities store / Mac OS system keychain. Depending on your OS and your browser, this will likely require manually exporting the CA certificate from the firewall on the firewall, go to Device Certificate Mgt Certificates. Select the CA cert and click Export button at the bottom.

Device	Certificates Default Tr	usted Certificate Authorities			
4					
Nam	e	Subject	Issuer	CA	Key
V v .	GlobalProtect-CA	CN = GlobalProtect-CA	CN = GlobalProtect-CA	Z	2
	🔄 gp-portal-gw	CN = 50.63.202.9	CN = GlobalProtect-CA		
😑 Delete	e Revoka Renew 🛃 Imp	ort 😹 Generate 🛃 Export 🛃 Im	nport HA Key 🚢 Export HA Key		







\$

File Format	Base64 Encoded Certificate (PEM)	
	Export private key	
Passphrase		
Confirm Passphrase		

viii. If after importing the CA certificate onto your computer, you get a certificate warning again, you may need to install the Portal/Gateway certificate on your computer. Here is how Windows Certificates.msc might display both certificates after they've been imported:

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
50.63.202.9	GlobalProtect-CA	8/9/2019	Server Authenticati	<none></none>
GlobalProtect-CA	GlobalProtect-CA	8/9/2019	<all></all>	<none></none>

ix. At this point you should be able to sign in...

GlobalProtect	\$
Sign In	
Enter login credentials	
Portal: 50.63.202.9	
gpuser1	
password	
Sign In	
Cancel	

x. And you should connect successfully to the Gateway.









25

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

xii. As general sample traffic, below we have a snip showing Windows client pinging Gateway public address and also pinging a network printer inside the lab network (on the inside/trust zone behind the firewall).

C:\>ping 50.63.202.9
Pinging 50.63.202.9 with 32 bytes of data:
Reply from 50.63.202.9: bytes=32 time=4ms TTL=64
Reply from 50.63.202.9: bytes=32 time=4ms TTL=64
Keply from 50.63.202.7: Dytes=32 time=3ms IIL=64
Neply from 50.65.202.7. Dytes-52 time-oms 116-64
Ping statistics for 50.63.202.9:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 6ms, Average = 4ms
C:>>
C:\>
C:\>ping 172.17.77.70
Pinging 172.17.77.70 with 32 bytes of data: Deply from 172.17.77.70 bytes -22 time-4me TTL-254
Reply from 172.17.77.70. Jyles-32 time=5ms 110-234 Reply from 172 17 77 70: butes=32 time=5ms TTL=254
Renly from 172.17.77.70: hytes=32 time=52ms TTL=254
Reply from 172.17.77.70: bytes=32 time=5ms TTL=254
Ping statistics for 172.17.77.70:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Minimum = 4ms Maximum = 52ms Quenage = 16ms
HITTHUM - THS, HAXIMUM - JAMS, HVERAGE - TUMS

xiii. And here we show web access to an internal network printer while connected from GP client.

77 70					~				
7.70								6	1
	HP Of	ffice ed Web	Jet P Server	ro 87	720				
lome	Scan	Fax	Web Se	rvices	Network	Tools	Settings		
Scan to	Email			Scan to	Network Fol	der	HP Digital Fax		
A secure connection is required. Click to enable.				A secure connection is required. Click to enable.			A secure connection is required. Click to enable.		
	iome Scan to A secur required	tome Scan Scan to Email A secure connection required. Click to e	Image: Non-Workshop Content Image: Non-Workshop Content None Scan Fax Scan to Email A secure connection is required. Click to enable.	HP OfficeJet P Embedded Web Server tome Scan Scan Fax Web Server	HP OfficeJet Pro 87 Embedded Web Server Iome Scan Scan Fax Web Services Scan to Email A secure connection is required. Click to enable.	Scan Fax Web Services Network Scan to Email A secure connection is required. Click to enable. A secure connection is required. Click to enable.	Image: Scan Fax Web Services Network Tools Scan To Email A secure connection is required. Click to enable.	Scan Fax Web Services Network Tools Settings Scan to Email Asecure connection is required. Click to enable. HP Digital Fax A secure connection is required. Click to enable.	Scan Fax Web Services Network Tools Settings Scan to Email Asecure connection is required. Click to enable. Asecure connection is required. Click to enable. HP Digital Fax

xiv. Back over on the firewall – under Network – GlobalProtect – Gateways – click on Remote Users to see the connected users...

paloalto	1	Dashboard	ACC	Monitor Policies	s Objects	Network Device		🕹 Controlt 🧉 🤤 Conf
III Interfaces	•							
VLANS.	E	Name	Location	Local Interface	Local IP	Tonnei	Max User	Info
CarWitbal Wires Wirpul Routers CarBibles Turnels CarBibles Turnels CarBibles CarBibles Portab CarBibles	æ ["	1 OD-CATCHOY		ethemeti/3		tunnel 100		Remote Lison

Notice various information in the columns and that you can Logout a user.







For access to live Palo Alto Networks lab boxes, go to: <u>https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab</u>

Current User	Previous User								
Domain	User	Computer	Client	Private IP	Public IP	Tunnel Type	Login At	Lifetime (s)	item 🤿
	gpuser2		Microsoft Windows 7 Professional Service Pack	192.168.200.1		IPSec	Aug.10 22:42:00	2592000	0

xv. To disconnect GP from client side, simply click the GP icon in Windows system tray / Mac menu bar and click the **Disconnect** button.



d. Troubleshooting GlobalProtect issues

i. On the GP client, click on the gear icon, and then select Settings



ii. The GP Settings window provides details about the connection including your tunneling IP address, as well as other helpful troubleshooting from the client side. The General tab is also where you can add additional portals.







neral	Connection	Host Profile	Troubleshootin	g Notification	
Acco	int				
ı	Jser: g	jpuser2			Sign Out
Porta	ls				
Ĩ	Portal		Statu	5	
	50.63.202.9		Conne	ected	
	Add	Delete	Edit		
E	Add	beece	- George		
loba	Protect Satt	inar			
iloba	IProtect Setti	ings			No.
Globa neral	IProtect Setti Connection	ings Host Profile	Troubleshooting	g Notification	No.
Globa neral Gatew	IProtect Setti Connection	ings Host Profile	Troubleshootin	g Notification	Authenticated
Globa neral Gatew ext-gv	IProtect Setti Connection	ings Host Profile	Troubleshootin Type External	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv	IProtect Setti Connection	ings Host Profile	Troubleshootin Type External	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv	IProtect Setti Connection	ings Host Profile	Troubleshootin Type External	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv	IProtect Setti Connection	ings Host Profile	Troubleshootin Type External	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv essigne atewa	IProtect Setti Connection	ings Host Profile 192. 50.6	Troubleshootin Type External	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv ssigne atewa rotocc	IProtect Setti Connection way w ed local IP: et local IP: et local IP:	ings Host Profile 192 50.6 JPSe	Troubleshootin Type External .168.200.100 .3.202.9	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv ssigne satewa rotocc	IProtect Setti Connection vay w ed local IP: sy IP: sy IP: s:	ings Host Profile 192: 50.6 IPSe 00:0	Troubleshootin Type External 168.200.100 53.202.9 sc 10:04	g Notification Tunnel Yes	Authenticated Yes
Globa neral Gatew ext-gv Assigne Satewa Protoco	IProtect Setti Connection vay w ed local IP: by IP: bl: : :	ings Host Profile 192. 50.6 IPSe 00:0	Troubleshootin Type External 168.200.100 33.202.9 sc 10:04 Byt	g Notification Tunnel Yes	Authenticated Yes 3376
Globa neral Gatew ext-gu Assigne Satewa Protoco Jptime: Bytes In Bytes In	IProtect Setti Connection vay w ed local IP: by IP: bl: : : :	ings Host Profile 192. 50.6 IPSe 00:0 0	Troubleshootin Type External 168.200.100 33.202.9 sc 10:04 Byth Pac	9 Notification Tunnel Yes es Out: kets Out:	Authenticated Yes 3376 33

- iii.
- . The Palo Alto firewall **System log** is a good place to troubleshoot GlobalProtect connection problems, related user authentication, etc. accessible under **Monitor – Logs - System**







paloalto Dashboard ACC Monitor Policies Objects Network Device V CLOGS (subtype eq auth) or (subtype eq globalprotect) and (receive_time leq '2018/08/10 23:32:00') Traffic Threat Receive Time Type Severity Event Object Description inform B URL Filtering 08/10 23:31:13 globalpr... globalprotectgateway-logout-succ GlobalProtect gateway user logout succeeded. User name: gpuser2, Client OS version: Micros Windows 7 Professional Service Pack 1, 64-bit, WildFire Submissions Reason: client logout. Data Filtering 08/10 23:31:13 globalpr... Inform HIP Match gp-gateway-N ct gateway client co ctgatewayglobalprotec config-releas eased. User name: gpuser2, Private IP: 2.168.200.100, Client version: 4.1.4-13, vice name: Client Version: Client OS version: crosoft Windows 7 Professional Service Pack 1 -bit, VPN type: Device Level VPN. 💷 User-ID S Tunnel Inspection Configuration System globalpr... 08/10 23:23:50 globalprotectga config-succ way- gp-gateway-N Alarms 92,168,20 4.1.4-13 Authentication ervice Pa Professional vice Level VP Unified P-Packet Capture 08/10 23:23:49 globalpr... gp-gatev globalprotectgateway-regist-succ App Scope Client OS version: Micro al Service Pack 1, 64-bit 88 Summary 08/10 23:23:49 globalpr... globalprotectgateway- gp-gateway-auth-succ Change Monitor Threat Monitor user2, AL dicrosoft 🚯 Threat Map Network Monitor 08/10 23:23:49 auth auth-success gp-auth R Traffic Map Session Browser 08/10 23:23:48 olobalor... gp-portal nt configurati globalprotectportal-config-succ GlobalProtect portal cli gion: US, User Botnet PDF Reports Manage PDF Summary 08/10 23:23:47 globalpr... gp-portal GlobalProtect portal Sa User Activity Report US, Us gpuser2. Auth type SaaS Application Usage Report Groups 08/10 23:23:47 auth auth-success gp-auth le 'gr Email Scheduler 08/10 23:23:45 globalpr... globalprotectportal-auth-fail gp-portal authentication fail Manage Custom Reports Source region: US, Authentication password, Auth type e: ProDev, Reason: Aut valid username or pass III Reports 08/10 23:23:45 auth auth-fail entication for user 'ProDev'. R gp-auth failed authority profile 'gp-auth', User is not in allowlist, auth vsys 'vsys1', From: 08/10 23:20:41 globalpr... globalprotectgateway-logout-succ qp-gateway-N ect gat ay user logout su , Client OS versio version: Micros Pack 1, 64-bit, nt logout. 08/10 23:20:41 globalpr... Inform qp-gateway-N tect gateway client globalprotect config-releas r name: gpus 100, Client ver vice Pack 1 bit, VPN type: Device Level VPN 08/10 23:14:26 globalpr... informational globalprotectgateway- gp-gateway-N config-succ ay client config Private IF 4.1.4-13. venal Service Pac VPN. Windows 7 Professio N type: Device Level obalProtect gateway user login succeeded. gin from: Control Source region: US, ser name: gpuser2, Client OS version: Micros indows 7 Professional Service Pack 1, 64-bit 08/10 23:14:25 globalpr... globalprotectgateway-regist-succ

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

iv. The Palo Alto firewall **Traffic log** is also helpful for troubleshooting – accessible under **Monitor – Logs - Traffic**

paloalto	1	Dashboard	ACC	Monitor	Policies	Objects
▼ @Loos	q (a	ddr.src in 192.16	8.200.100)			
Traffic		Receive Tim	e From	n Zone S	ource	
WildFire Submissions	Þ	08/10 23:31	:13 insid	e 1	92.168.200.100	
Data Filtering	P	08/10 23:31	:12 insid	le 1	92.168.200.100	

v. To see user-id in traffic logs, enable User Identification on your inside zone (tunnel interface zone).







29

For access to live Palo Alto Networks lab boxes, go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab

Name	inside		User Identification ACL		
Log Setting	None		Enable User Identification		
Туре	Layer3	-	🗐 Include List 🔺		
Interfaces ethernet1/2 tunnel.100			Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24		
			Add Delete Users from these addresses/subnets will be identified. Exclude List		
Add 🖨 Delete			Select an address or address group or type in your own address. Ex: 192,168.1.20 or 192,168.1.0/24		
Zone Protection					
Zone Protection Zone Protection Profile	None	*	+ Adt Delete		

vi. Below is a sample Traffic log snip, before and after applying user-id to the tunnel interface zone:

Receive Time	Action	Rule	From Zone	Source	Source User	Destination	To Zone
08/10 23:29:49	allow	intrazone-default	inside	192.168.200.100	gpuser2	172.17.77.70	inside
08/10 23:29:13	allow	intrazone-default	inside	192.168.200.100	gpuser2	172.17.77.70	inside
08/10 23:24:15	allow	intrazone-default	inside	192.168.200.100		172,17,77,70	inside
08/10 23:24:09	allow	intrazone-default	inside	192.168.200.100		172.17.77.70	inside







30

Next Steps

If you want to test this on your own and do not have access to a lab environment to do so, you have a few options:

a. Contact your Sun Management Account Rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

If you are unsure who your Account Rep is or do not have one yet, you can reach out to **sales@sunmanagement.net** for assistance.

- **b.** Reach out through the free Fuel Users Group (www.fuelusersgroup.org) which at the time this lab is being written is offering limited free access to a virtual lab environment, which they refer to as their "Virtual Test Lab," in which you can practice the steps outlined above. (Note: The Fuel Users Group may alter or discontinue offering their "Virtual Test Lab" at any time)
- c. For access to live Palo Alto Networks boxes for lab practice purposes please go to: https://www.paloaltonetworks.com/services/education/cybersecurity-skills-practice-lab. This is a no charge service provided by Palo Alto Networks.

If you feel Sun Management brings value to you and your organization with these labs, please keep us in mind for other network and network security related requirements. We are here to help you. Thank you for your business.

Please direct any questions/comments/feedback on this lab exercise to: education@sunmanagement.net

Lab Author: Jeff Wood, PCNSE, Network Security Engineer

Last Modified: August 17, 2018







Resources

GlobalProtect Licensing:

https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-overview/about-globalprotect-licenses

GlobalProtect 8.0 Administrator's Guide: <u>https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide</u>

How to Generate a Self-signed Certificate: <u>https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Generate-a-New-Self-Signed-SSL-Certificate/ta-p/53215</u>

Online Certificate Status Protocol (OCSP): <u>https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/certificate-management/certificate-revocation/online-certificate-status-protocol-ocsp</u>





