paloalto® NETWORKS in

Google Cloud Platform

Using Terraform to Deploy a Simple GlobalProtect Infrastructure in GCP

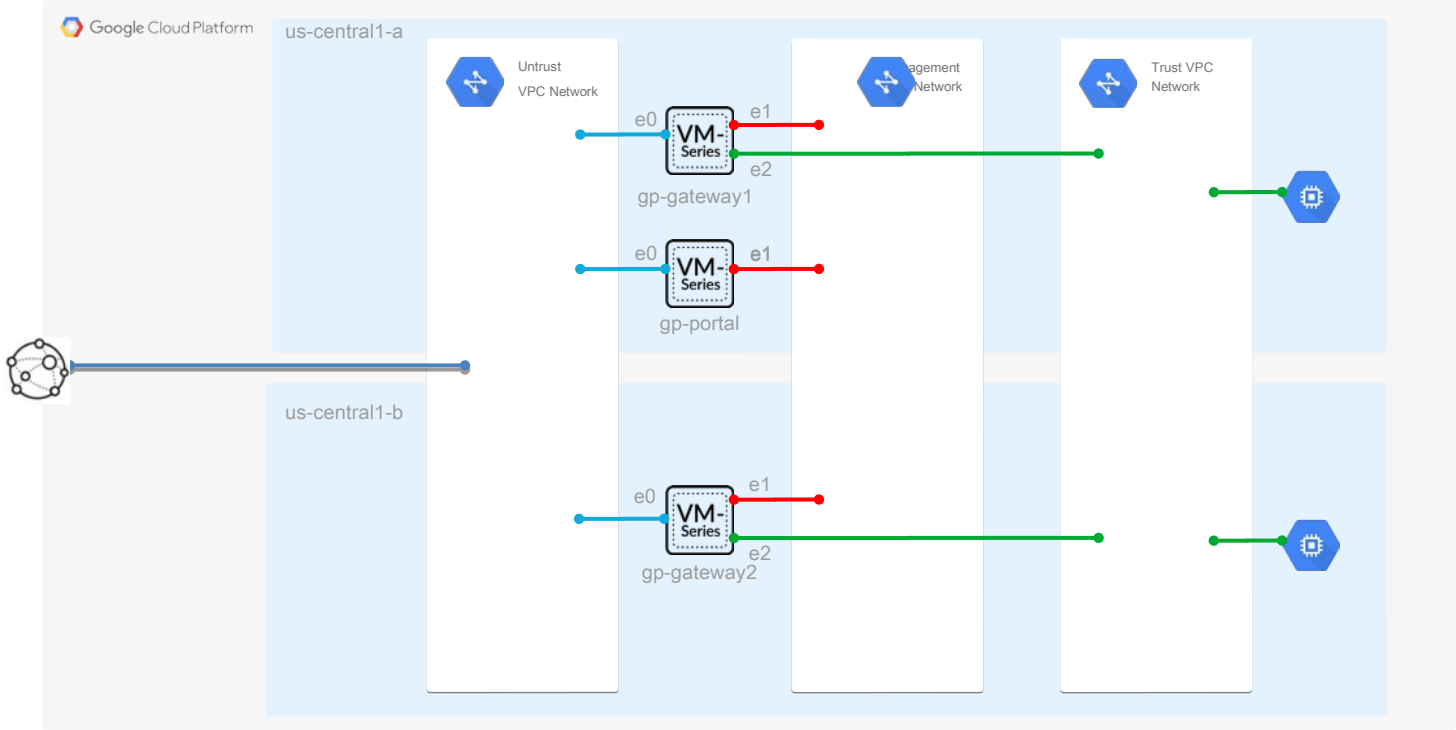
Patrick Glynn – Public Cloud CE

April 2020

Customers are increasingly looking to the public cloud to provide scalable, flexible, on-demand infrastructure to support business-critical processes as well as disaster recovery on demand. The ability to establish scalable, secure connectivity to these environment is a critical element of enabling remote users.

Here, we demonstrate a simple GlobalProtect deployment consisting of a portal and two gateways in separate zones. Terraform is used to facilitate rapid, consistent deployment and bootstrapping is used to create pre-configured portals/gateways which reduces the post-deployment configuration steps required to get the solution up and running.

This is the infrastructure that will be built. A single GlobalProtect portal will be deployed to us-central1-a, two gateways to us-central1-a and us-central1-b, and two test Ubuntu hosts.



Notes:

- The portal is displayed to us-central1-a and gateways are deployed to us-central1-a and us-central1-b. Alternate regions are supported by editing the tfvars file prior to deployment. The template will automatically pick the first two zones in the region.

- Two sample users have been created in the local database for testing purposes. Refer to published documentation for additional authentication options.

- The template creates a project with a unique ID and may be used as a stand-alone project or enabled as a host project for use with Shared VPC architectures.

- The template creates an entire sample deployment, including: a project, VPC networks, subnets, routes, GCP firewall rules, the GlobalProtect infrastructure, and two test ubuntu servers.

- A self-signed CA certificate is used for this example. For production use, a CA certificate signed by a corporate or public PKI is best practice.

Step 1: Navigate to the the GP-NoAutoscale directory and edit the file terraform.tfvars to suit requirements.

```
Billing_Account = "<GCP Billing Account>"

Base_Project_Name = "<Base Project Name>"

Public_Key_Path = "~/.ssh/id_rsa.pub"

#FW_PanOS = "byol-904"                  # Uncomment for PAN-OS 9.0.4 - BYOL
FW_PanOS  = "bundle1-904"               # Uncomment for PAN-OS 9.0.4 - PAYG Bundle 1
#FW_PanOS = "bundle2-904"               # Uncomment for PAN-OS 9.0.4 - PAYG Bundle 2

FW_Machine_Type = "<FW Machine Size>"

FW_Image   = "https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/global/images/

GCP_Region = "<GCP Region>"

Management_Subnet_CIDR = "10.0.0.0/24"

Untrust_Subnet_CIDR = "10.0.1.0/24"

Trust_Subnet_CIDR = "10.0.2.0/24"
```

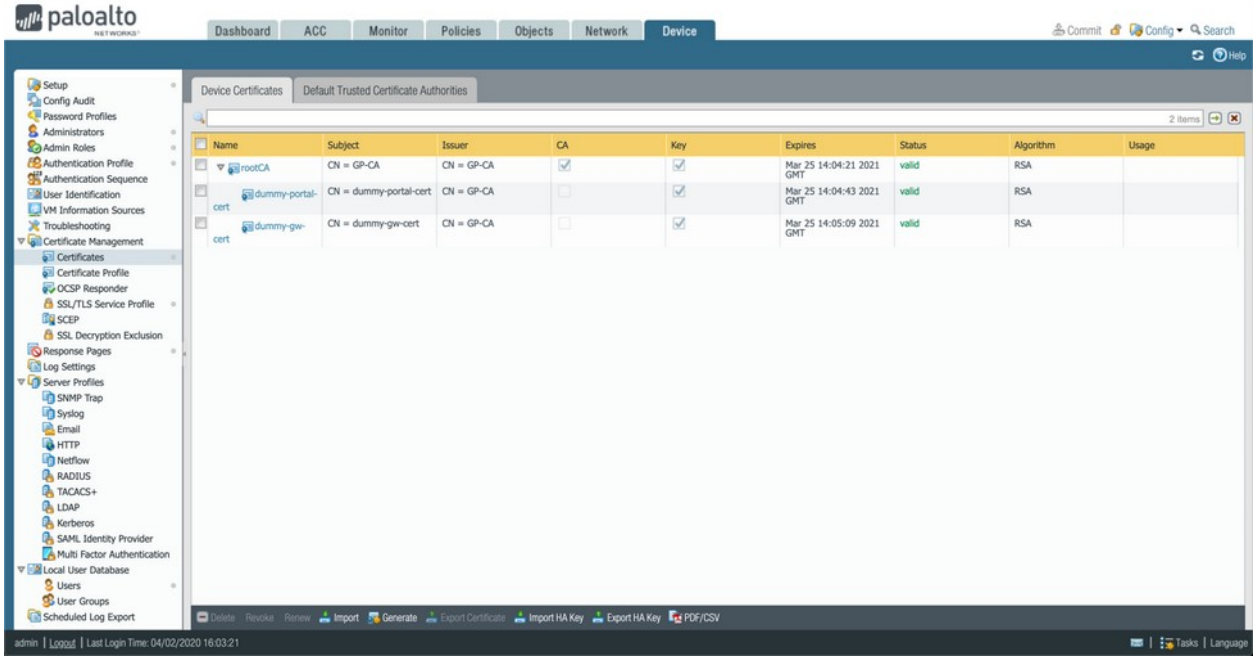
Step 2: Authenticate to GCP.

```
bash-4.3# gcloud auth login
Go to the following link in your browser:

    https://accounts.google.com/o/oauth2/auth?code_challenge=uBJkH8p4pyeB1NZtFzfI8hxjKr5qm9FAZX8tdAfO
lRY&prompt=select_account&code_challenge_method=S256&access_type=offline&redirect_uri=urn%3Aietf%3Awg
%3Aoauth%3A2.0%3Aoob&response_type=code&client_id=32555940559.apps.googleusercontent.com&scope=openid
+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fc
loud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.
com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth


Enter verification code: 4/yQEQnp4mkB6jZC2wFi_ryxYj95q5jsMZTYzbILct9SDXvaXCpNxqGoI

You are now logged in as [ptglynn@cloudy.business].
Your current project is [adv-peering-2fw-2spoke-common]. You can change this setting by running:
  $ gcloud config set project PROJECT_ID


Updates are available for some Cloud SDK components. To install them,
please run:
  $ gcloud components update

bash-4.3#
```

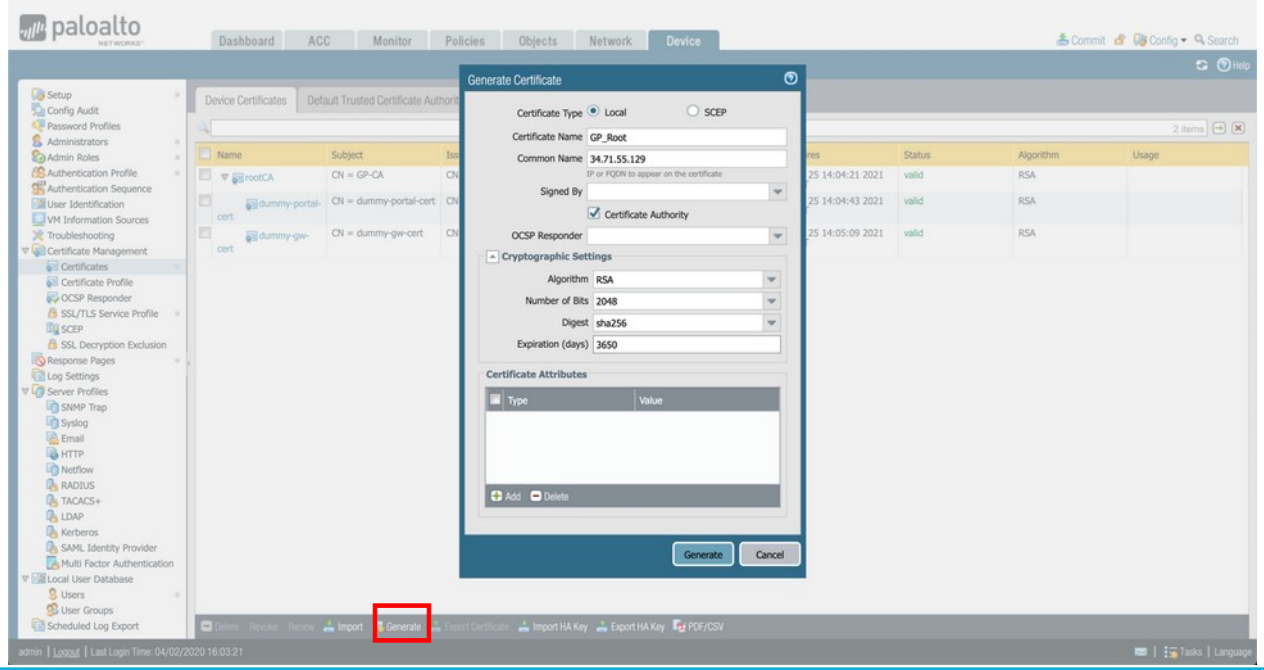
Step 3: Apply the Terraform template to the environment. This process will take several minutes to complete as bootstrapping is used to perform the initial configuration of the portal/gateways. Once done, the output will include the management/untrust IP addresses of the portal/gateways as well as the private IP addresses of the test servers.

```
google_storage_bucket_object.portal_software: Refreshing state... [id=portal-55d9-software/null.txt]
google_storage_bucket_object.portal_license: Refreshing state... [id=portal-55d9-license/null.txt]
google_storage_bucket_object.portal_content: Refreshing state... [id=portal-55d9-content/null.txt]
google_compute_instance.server1: Refreshing state... [id=projects/782961236101/zones/us-central1-a/in
stances/server1]
google_compute_instance.server2: Refreshing state... [id=projects/782961236101/zones/us-central1-b/in
stances/server2]
google_compute_instance.gateway2: Refreshing state... [id=projects/782961236101/zones/us-central1-b/i
nstances/gp-gateway2]
google_compute_instance.gateway1: Refreshing state... [id=projects/782961236101/zones/us-central1-a/i
nstances/gp-gateway1]
google_compute_instance.portal: Refreshing state... [id=projects/782961236101/zones/us-central1-a/ins
tances/gp-portal]

Apply complete! Resources: 0 added, 0 changed, 0 destroyed.

Outputs:

Gateway1-Management-IP = 104.197.113.130
Gateway1-Untrust-IP = 35.184.52.74
Gateway2-Management-IP = 35.226.146.146
Gateway2-Untrust-IP = 104.154.69.217
Portal-Management-IP = 34.71.55.129
Portal-Untrust-IP = 35.223.117.106
Server1-IP = 10.0.2.5
Server2-IP = 10.0.2.4
bash-4.3#
```

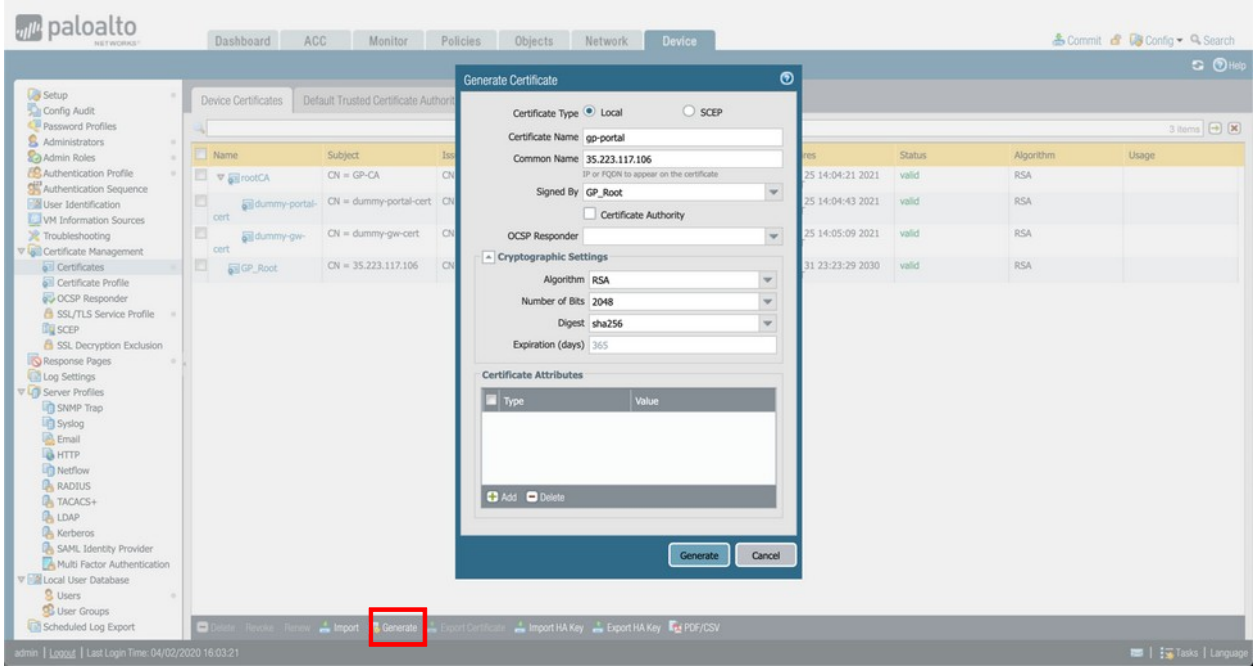
Step 4: Login to the portal (admin/Pal0ALt0@123) and navigate to the Device Tab > Certificates. Dummy certs have been added as placeholders and need to be replaced.



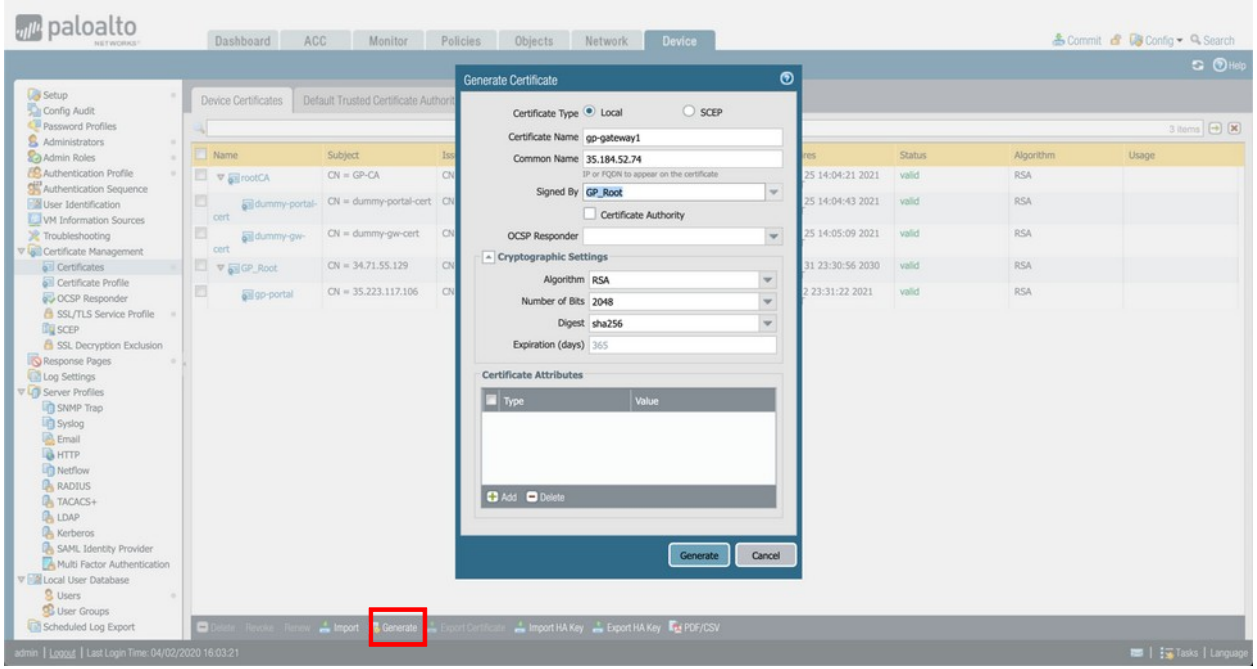
Step 5: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “GP_Root”), the public IP of the **management** interface of the portal, and optionally, set a longer expiration time. Tick the “Certificate Authority” box and then click “Generate”. This is the root CA certificate that will sign all other certificates.



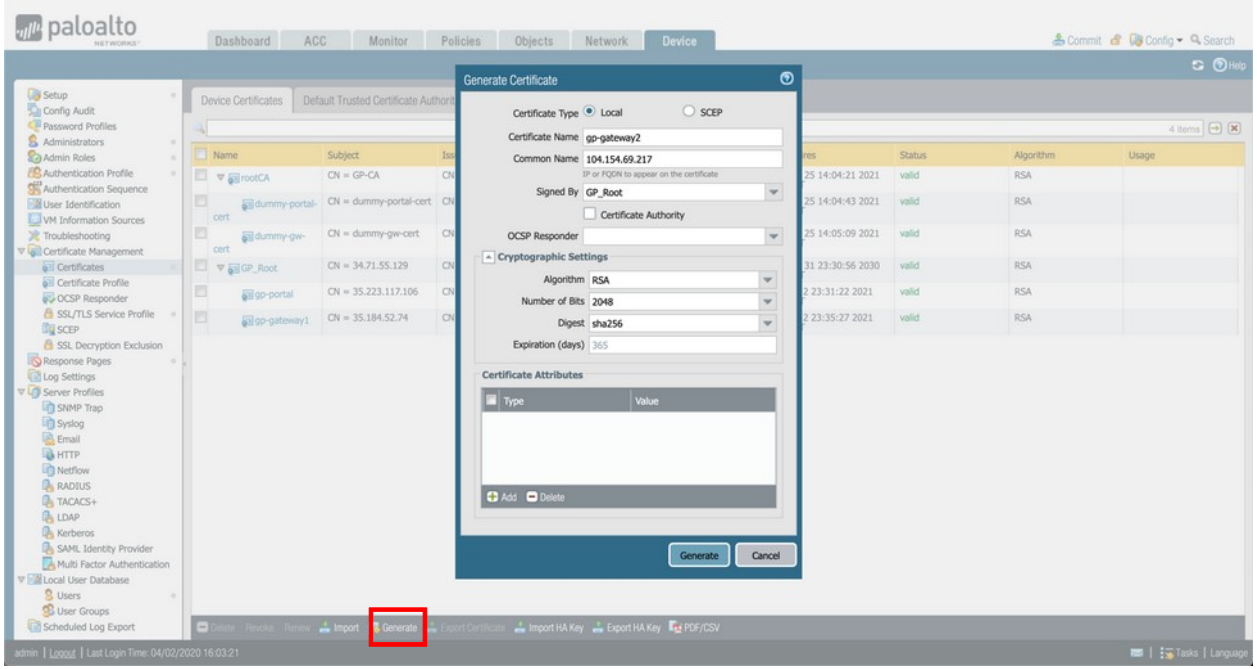
Step 6: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-portal”), the public IP of the **untrust** interface of the portal. Select the recently-created root certificate from the “Signed By’ drop-down and then click “Generate”. This is the certificate for the portal interface.



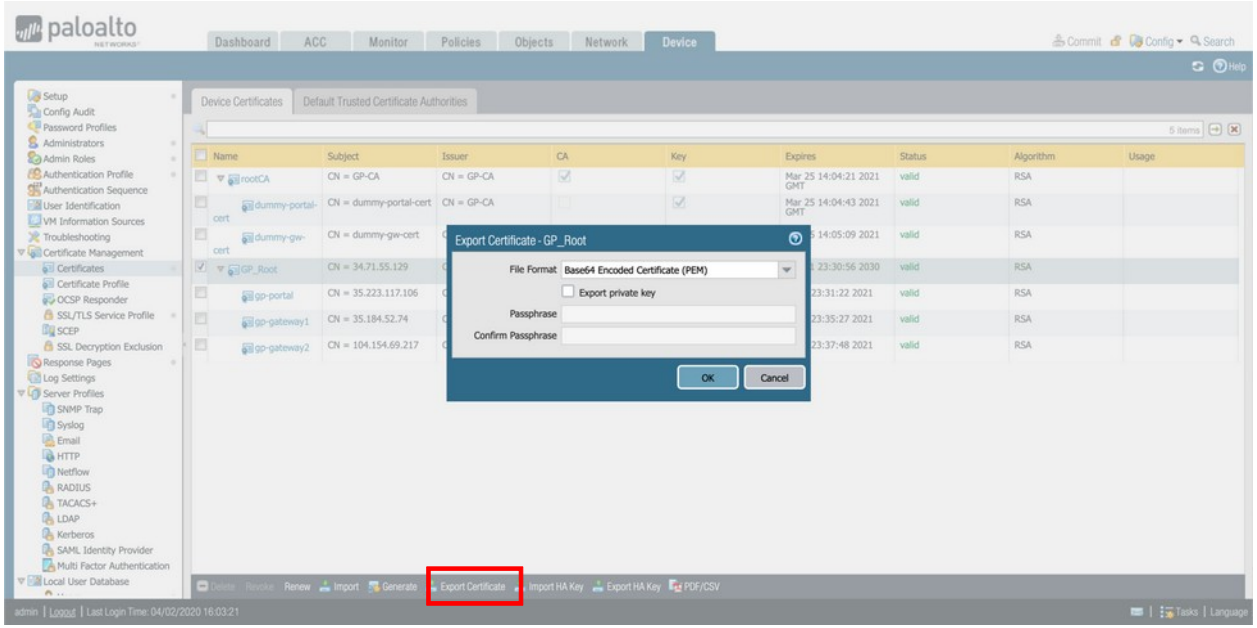
Step 7: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-gateway1”), the public IP of the **untrust** interface of the first gateway. Select the recently-created root certificate from the “Signed By’ drop-down and then click “Generate”. This is the certificate for the first gateway interface.



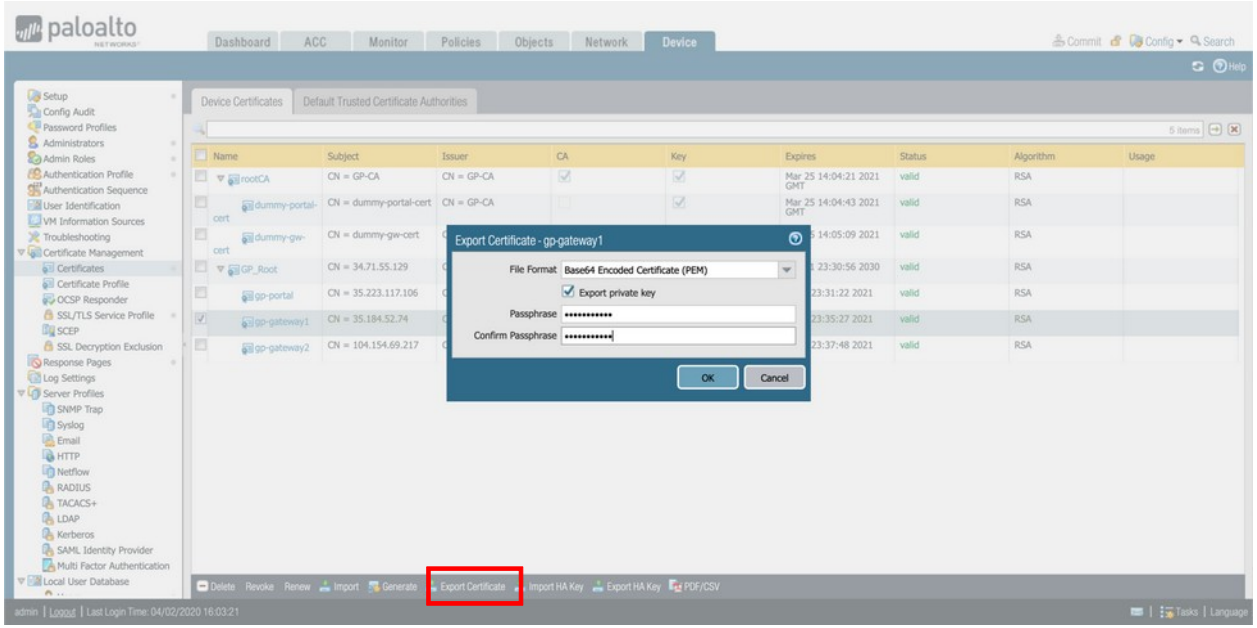
Step 8: Click “Generate” at the bottom of the page and specify a descriptive name (e.g. “gp-gateway2”), the public IP of the **untrust** interface of the second gateway. Select the recently-created root certificate from the “Signed By’ drop-down and then click “Generate”. This is the certificate for the second gateway interface.



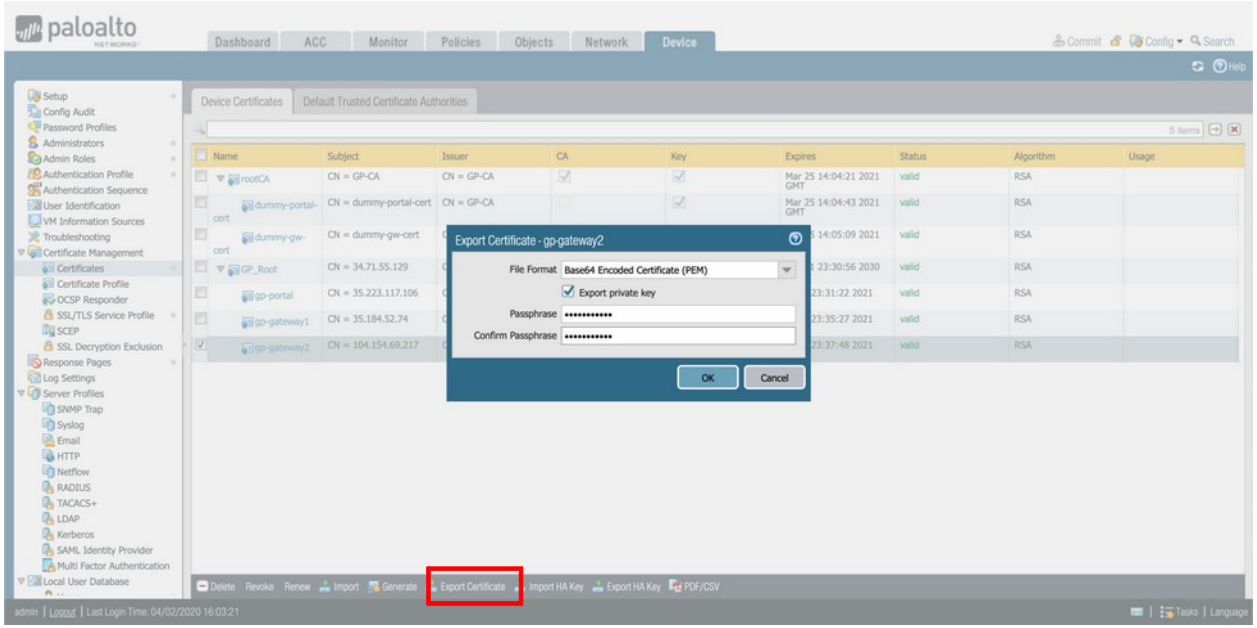
Step 9: Select the root certificate (GP_Root in this example), and click “Export Certificate”. Save the certificate to a known location. This certificate must be imported into all of the gateways although the associated private key is not required.



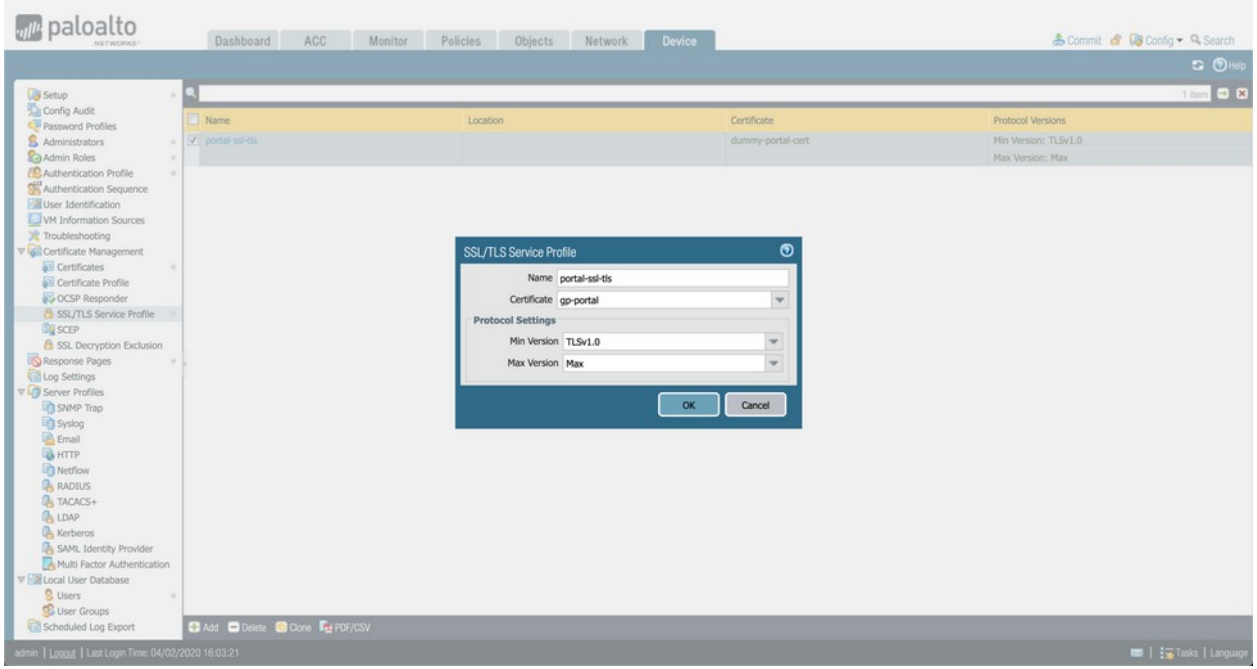
Step 10: Select the first gateway certificate (gp-gateway1 in this example), tick “Export Private Key”, specify a password, and click “OK”. Save the certificate to a known location. This certificate will be imported into the first gateway.



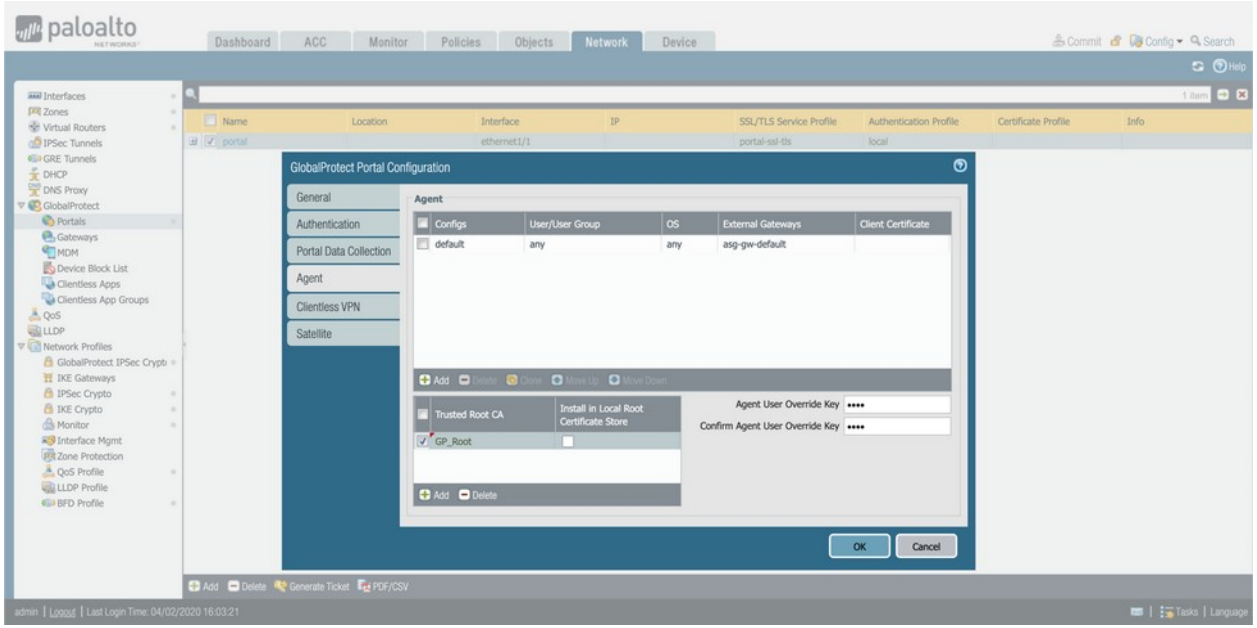
Step 11: Select the second gateway certificate (gp-gateway2 in this example), tick “Export Private Key”, specify a password, and click “OK”. Save the certificate to a known location. This certificate will be imported into the second gateway.



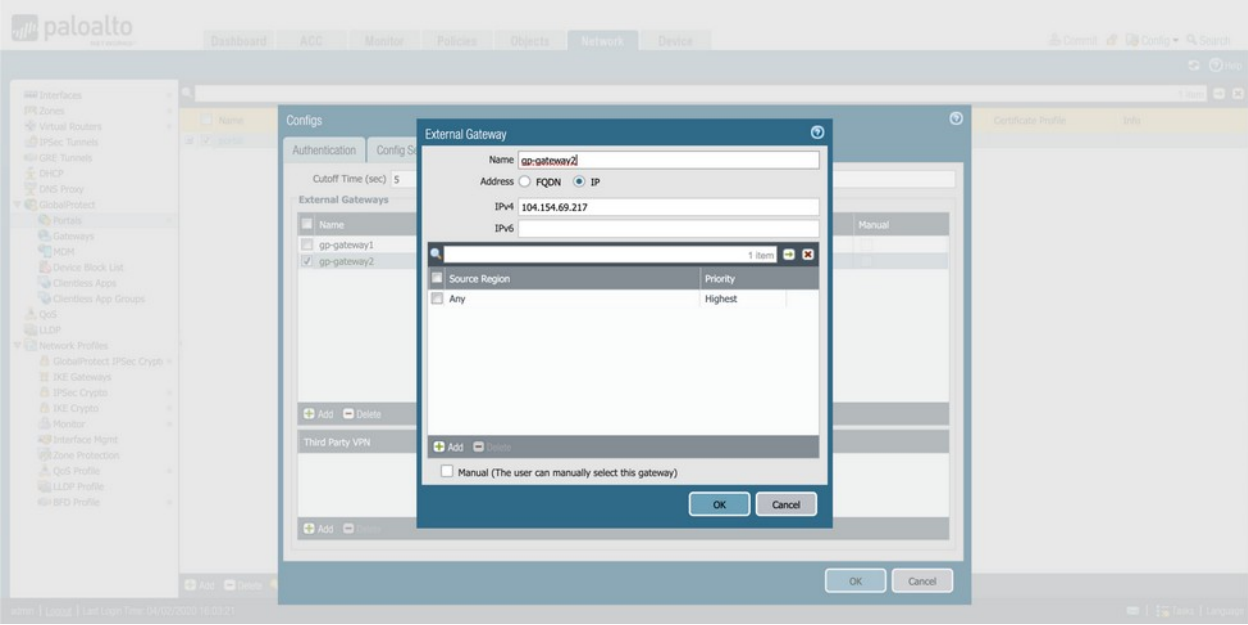
Step 12: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “portal-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-portal in this example).



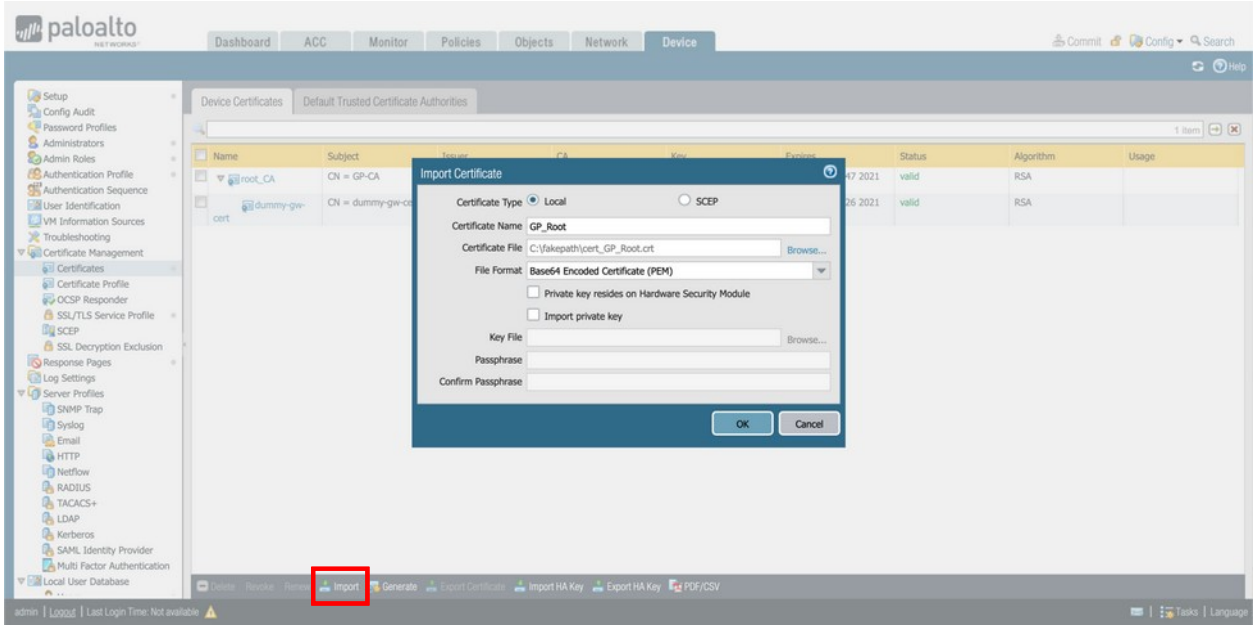
Step 12: Navigate to the Network **Tab > GlobalProtect > Portals** and click on “portal”. Click on the **Agent** tab. Update the “Trusted Root CA” to the recently created one. Click on “default”.



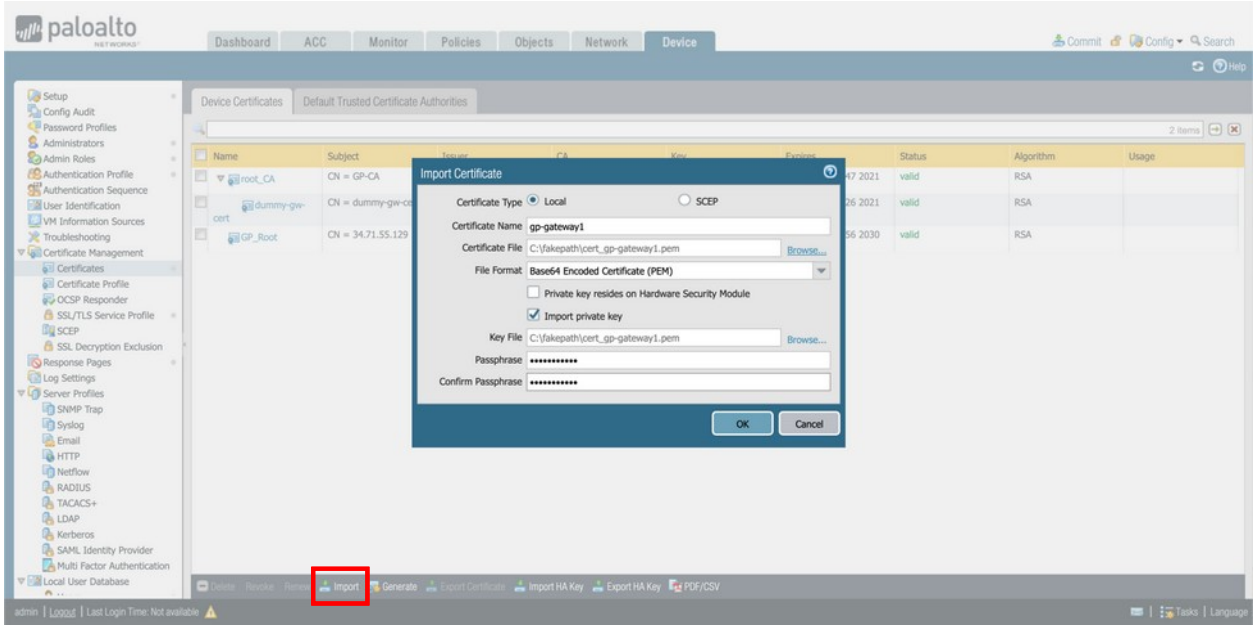
Step 12: Click on the **External** tab, delete the existing external gateway and add the IP addresses of the two new gateways, specifying them by IP address. Commit the changes when done.



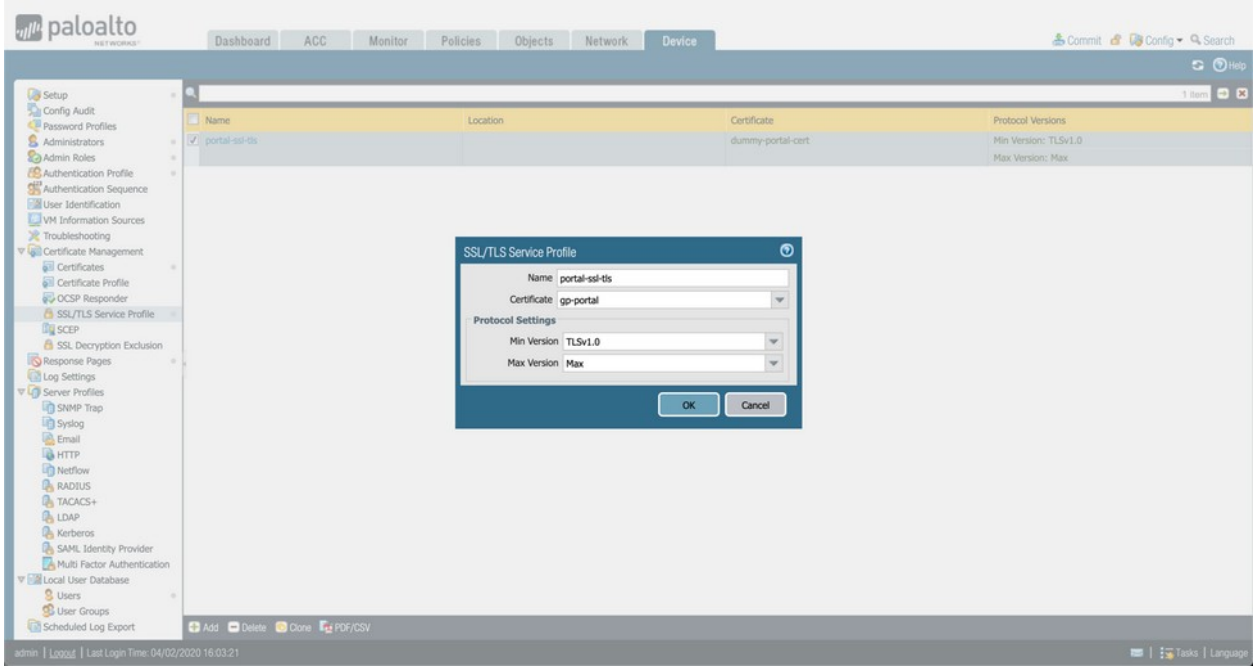
Step 13: Login to the first gateway (admin/Pal0ALt0@123) and navigate to the Device Tab > Certificates. Click “Import”. Provide a name for the certificate (e.g. GP_Root), and browse to the locaiton of the exported root certificate. Click “OK”.



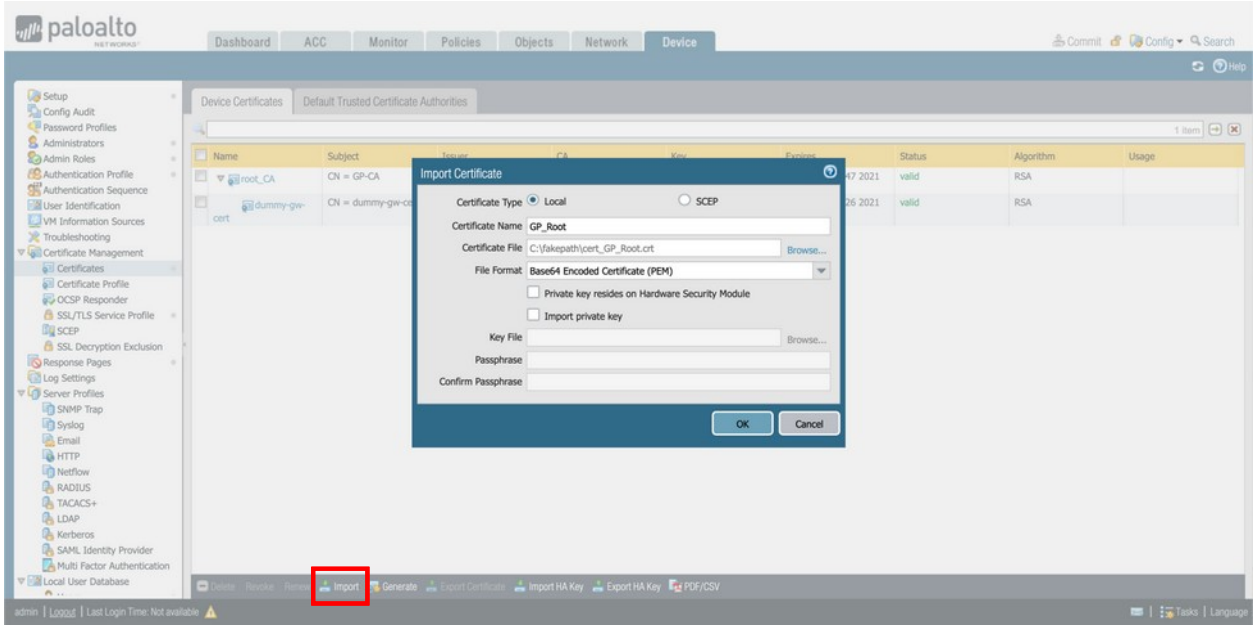
Step 14: Click “Import”. Provide a name for the certificate (e.g. gp-gateway1), and browse to the location of the exported certificate for the first gateway. Tick “Import private key”, browse to the location of the exported certificate for the first gateway, and input the password used to secure the certificate. Click “OK”.



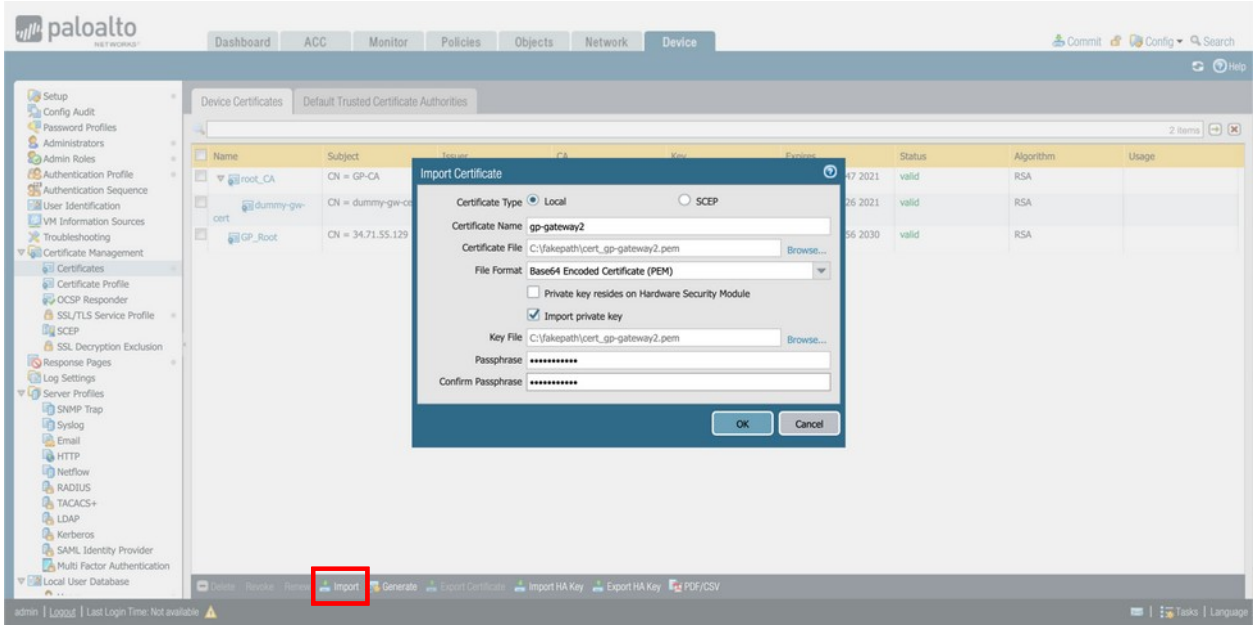
Step 15: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “gateway-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-gateway1 in this example). Commit all changes.



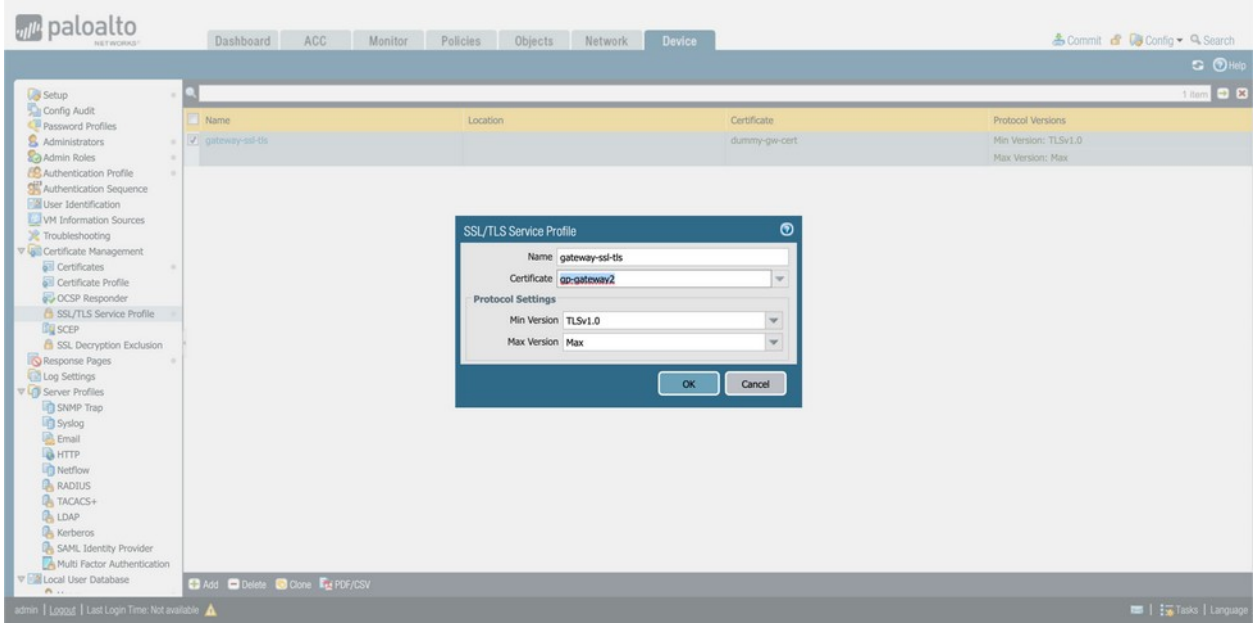
Step 16: Login to the second gateway (admin/Pal0ALt0@123) and navigate to the Device Tab > Certificates. Click “Import”. Provide a name for the certificate (e.g. GP_Root), and browse to the locaiton of the exported root certificate. Click “OK”.



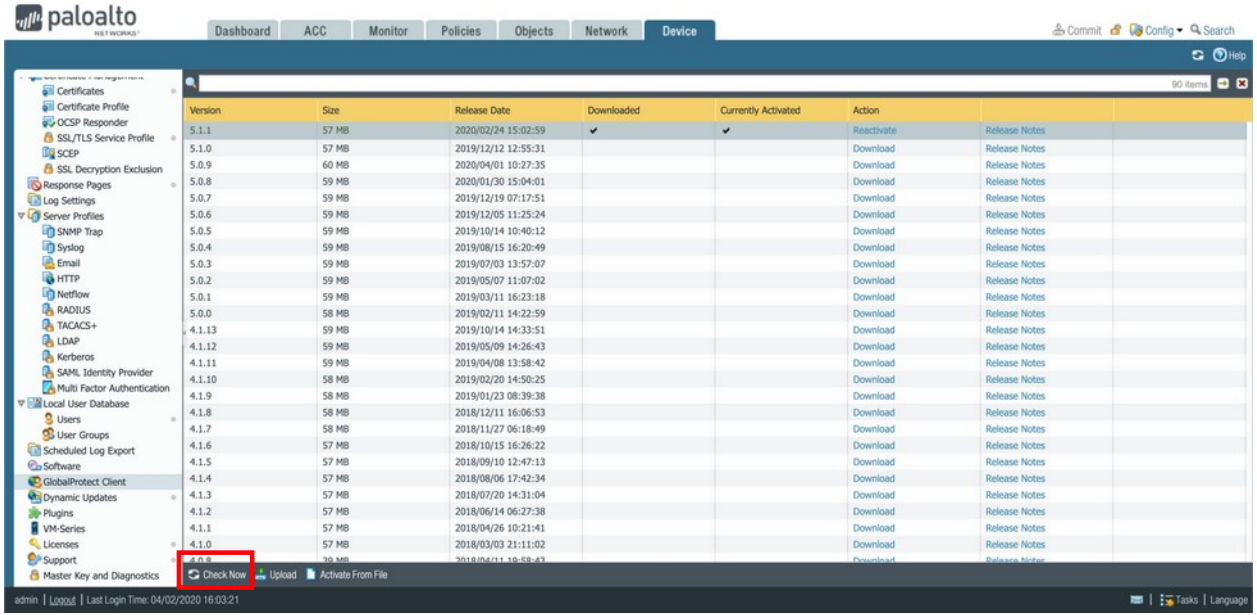
Step 17: Click “Import”. Provide a name for the certificate (e.g. gp-gateway2), and browse to the location of the exported certificate for the second gateway. Tick “Import private key”, browse to the location of the exported certificate for the first gateway, and input the password used to secure the certificate. Click “OK”.



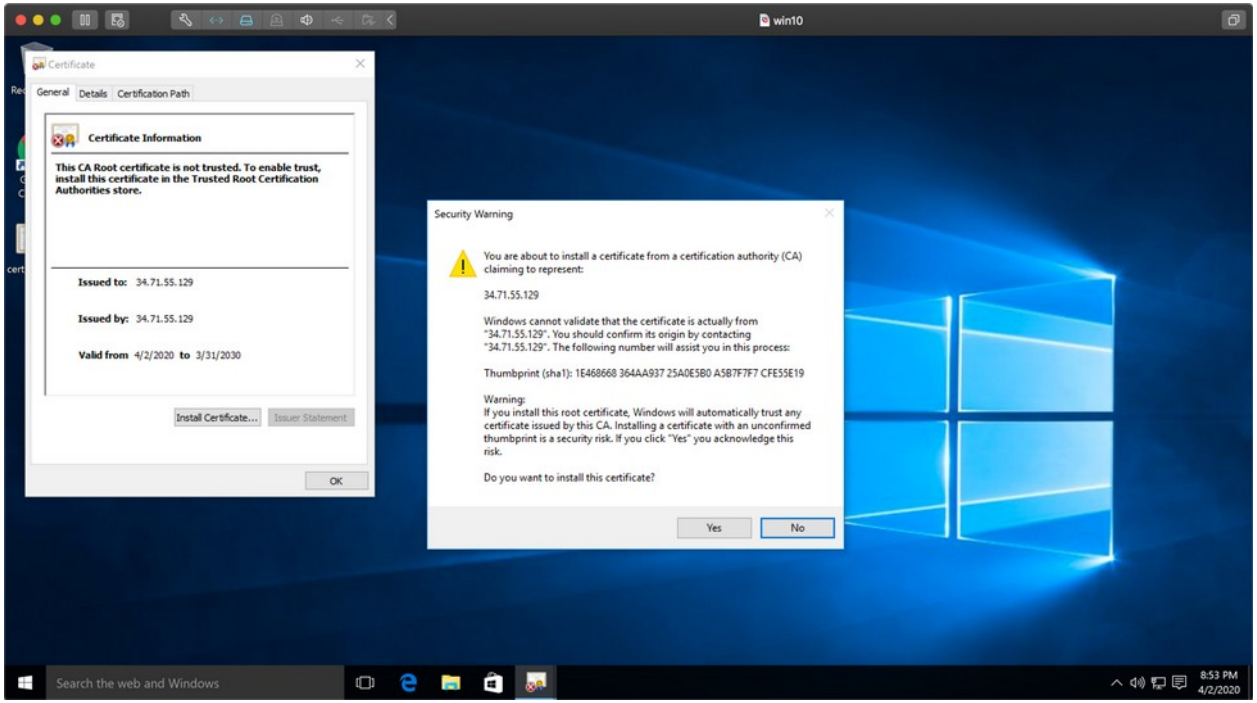
Step 18: Navigate to the **Device Tab > SSL/TLS Service Profile** and click on “gateway-ssl-tls”. Click the Certificate drop-down and select the new portal certificate (gp-gateway2 in this example). Commit all changes.



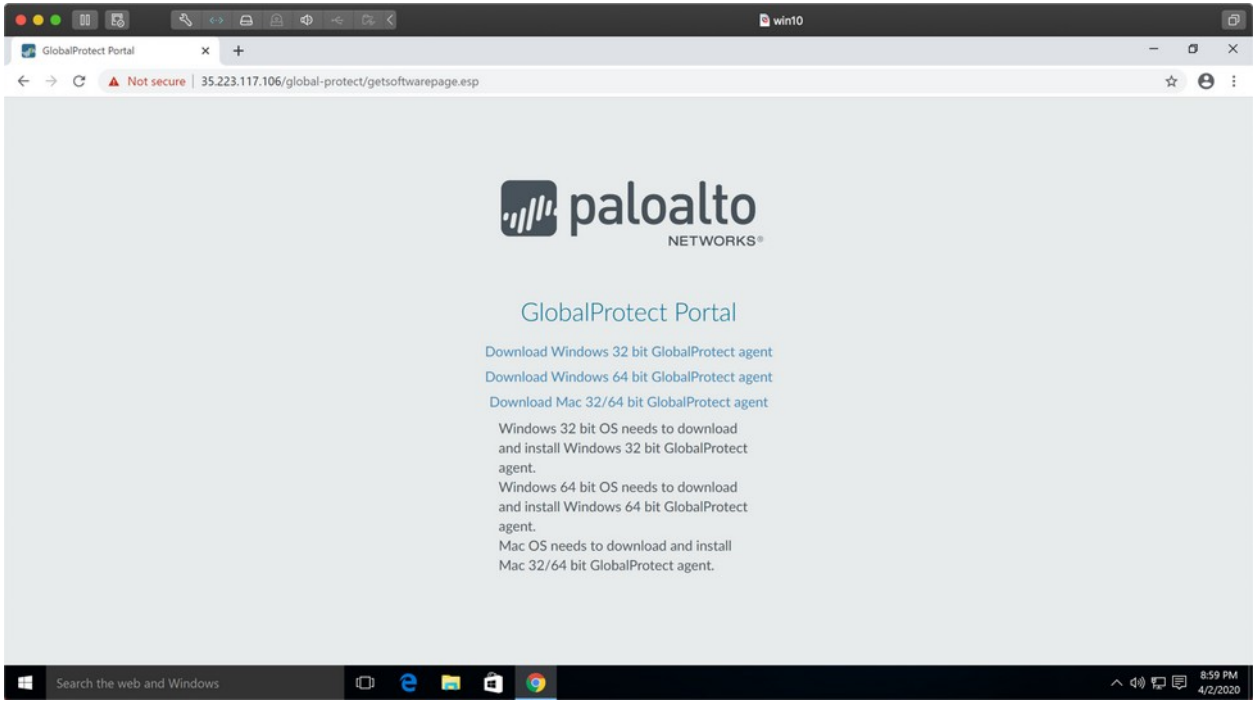
Step 19: Login to the portal and Navigate to the **Device Tab > GlobalProtect Client** and click on “Check Now”. Download and then activate the desired client version. If you see the error “The device is not found or not registered, please try after some time”, acknowledge the error and click “Check Now” again.



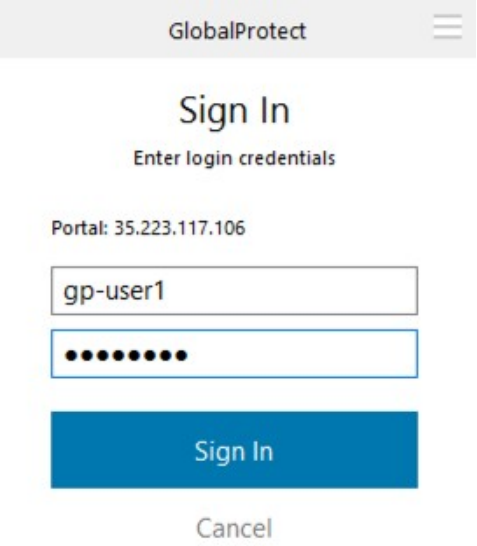
Step 20: Copy the exported CA certificate to the test machine and import it as a trusted CA certificate. This is required to ensure that the client trusts the certificates presented by the portal and gateways.



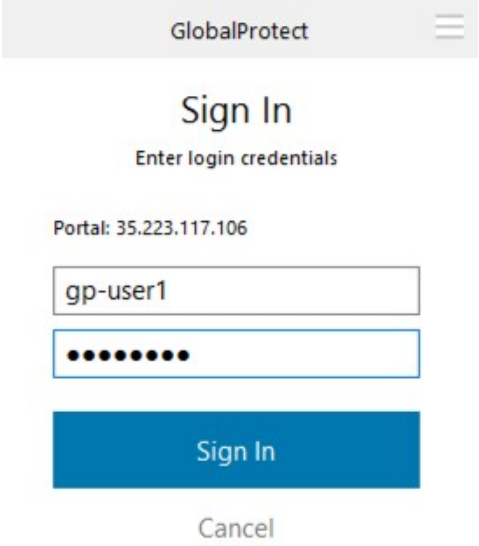
Step 21: Login to the portal using one of the two pre-created GlobalProtect users (gp-user1/paloalto) or (gp-user2/paloalto). Once authenticated, download and install the relevant client software.



Step 22: Enter one of the ample username/password combinations and click “Sign In”.



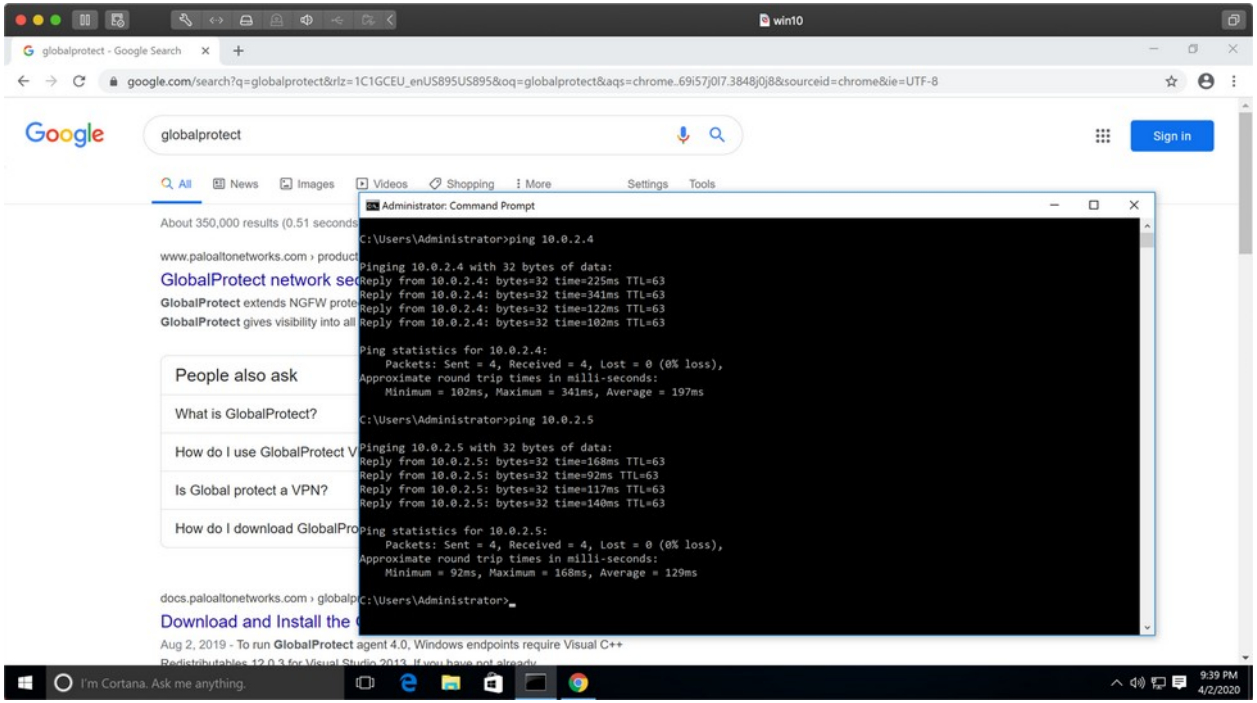
Step 23: Enter one of the ample username/password combinations and click “Sign In”.



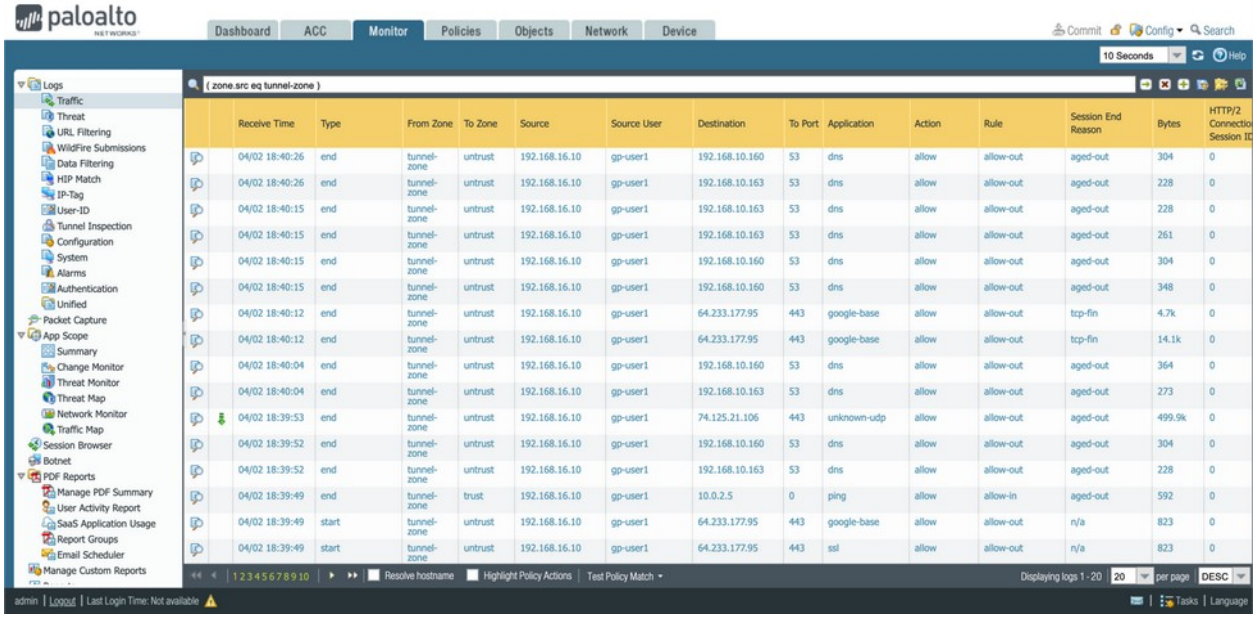
The client will reflect a successful connection.

The client will reflect a successful connection.

The Firewall policy allows internet traffic outbound as well as in to the trusted subnet.



The traffic logs will show the relevant logs in addition to user attribution.



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connectio Session ID
04/02 18:40:26	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
04/02 18:40:26	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	261	0
04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
04/02 18:40:15	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	348	0
04/02 18:40:12	end	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	tcp-fin	4.7k	0
04/02 18:40:12	end	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	tcp-fin	14.1k	0
04/02 18:40:04	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	364	0
04/02 18:40:04	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	273	0
04/02 18:39:53	end	tunnel-zone	untrust	192.168.16.10	gp-user1	74.125.21.106	443	unknown-udp	allow	allow-out	aged-out	499.9k	0
04/02 18:39:52	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.160	53	dns	allow	allow-out	aged-out	304	0
04/02 18:39:52	end	tunnel-zone	untrust	192.168.16.10	gp-user1	192.168.10.163	53	dns	allow	allow-out	aged-out	228	0
04/02 18:39:49	end	tunnel-zone	trust	192.168.16.10	gp-user1	10.0.2.5	0	ping	allow	allow-in	aged-out	592	0
04/02 18:39:49	start	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	google-base	allow	allow-out	n/a	823	0
04/02 18:39:49	start	tunnel-zone	untrust	192.168.16.10	gp-user1	64.233.177.95	443	ssl	allow	allow-out	n/a	823	0