VM-Series for GCP

GCP Template

Deployment Guide

Deploys an External Load Balancer multiple VM-Series NGFW Internal Load Balancers and Web Servers. This deployment model is commonly referred to as a Load Balancer Sandwich.

https://www.paloaltonetworks.com

Last Update: May 2016

Table of Contents

Version History

Version number	Comments
1.0	Initial Draft

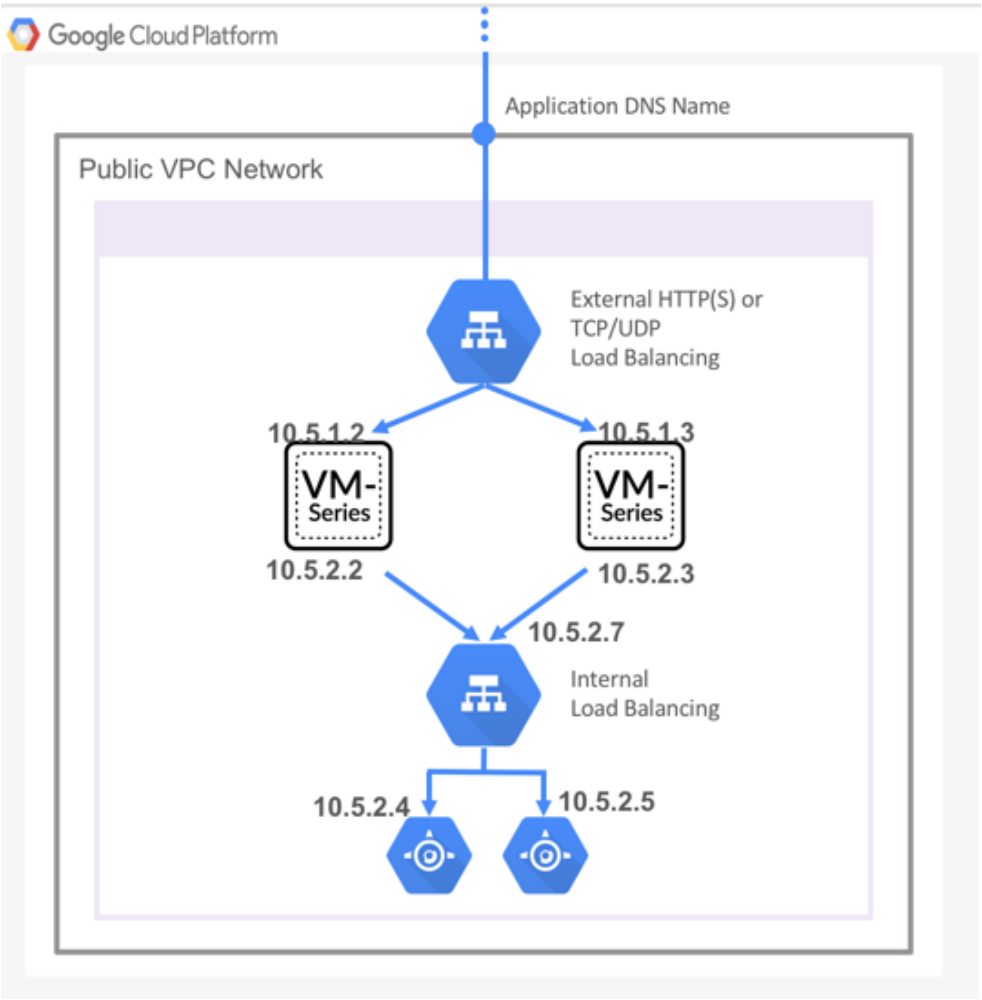
1. About Templates

GCP Templates, are files that can deploy, configure, and launch GCP resources such as VPC networks & subnets, security groups, firewall rules, route tables, load balancers, and more. These templates are used for ease of deployment and are key to any cloud deployment model.

For more information on Templates refer to Google's documentation

https://cloud.google.com/compute/docs/instance-templates/

This document will explain how to deploy a template that launches everything that is shown below in the diagram. This includes, multiple apache web server, multiple VM-Series firewall and the subnets, an HTTP ELB, and a TCP ILB. In addition, the template performs a native bootstrapping feature on the VM-Series firewall that allows for additional configuration of the VM-Series firewall (such as routes, security policies, management interface swap, etc.) Once the template has been deployed, the network topology will align with the following diagram:



2. Support Policy

This template is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself.

Unless explicitly tagged, all projects or work posted in our GitHub repository (at https://github.com/PaloAltoNetworks/googlecloud) or sites other than our official Downloads page on https://support.paloaltonetworks.com are provided under the best effort policy.

3. Instances used

When using this template the following machine types are used:

Instances	Machine Types
Apache Web Servers	n1-standard-1
VM Series Firewall	n1-standard-4

Note: There are costs associated with each machine type launched, please refer to the Google instance pricing page https://cloud.google.com/compute/pricing

4. Prerequisites

Here are the prerequisites required to successfully launch this template:

- A GCP account
- Access to the Google Cloud SDK

4.1 Create GCP account

If you do not have a GCP account already, go to https://cloud.google.com/free/ and create an account.

4.2 Install the Google Cloud SDK

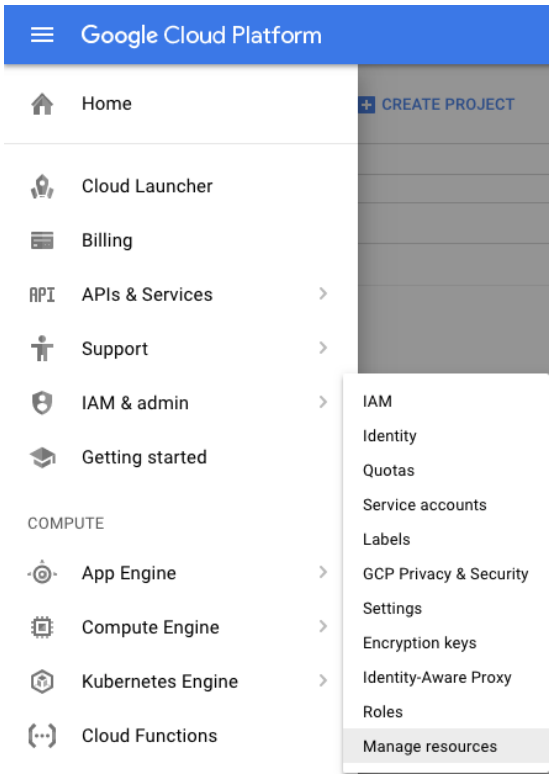
Template installations in GCP are performed from the CLI. Install the SDK/CLI by selecting the relevant platform from the following link and following the installation instructions:

https://cloud.google.com/sdk/

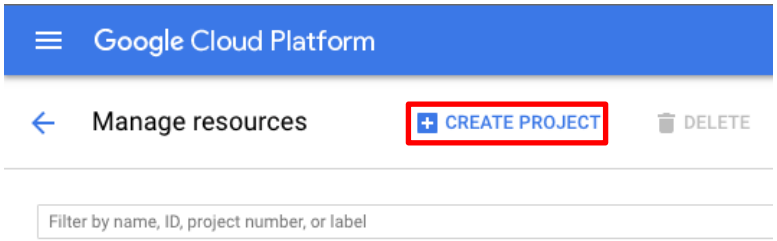
4.3 Accept the EULA (If Required)

4.4 Create a Project

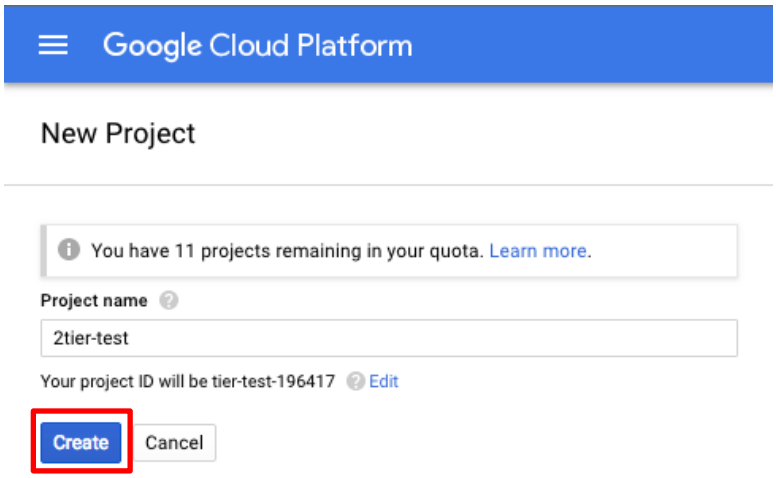
All GCP resources are deployed to a GCP Project. A GCP Project is an organizational boundary that separates users, resources, billing information, etc. A GCP Project is similar to an AWS VPC or an Azure Resource Group. By default, GCP will create a Project upon creation of an account. If that is not the case or to manually create a dedicated project, use the drop-down on the left and select **IAM & admin > Manage Resources**:



Click **Create Project**:



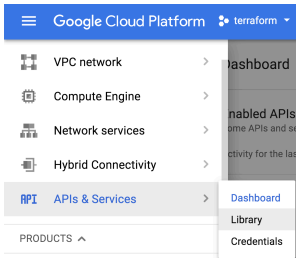
Specify a name for the project and click **Create**:



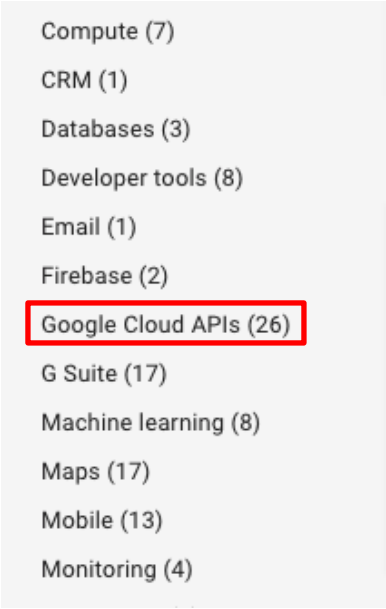
Note: GCP Project creation will take a few minutes.

4.5 Enable the API

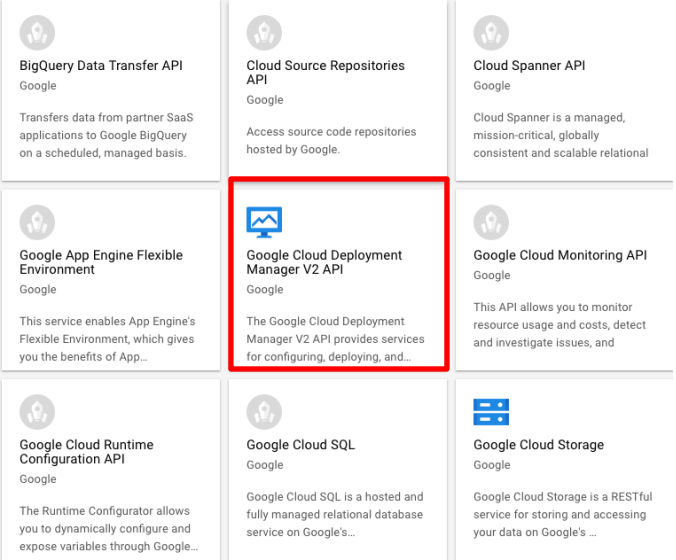
Deploying a template requires the API be enable on the project. Navigate to **APIs & Services > Library**:



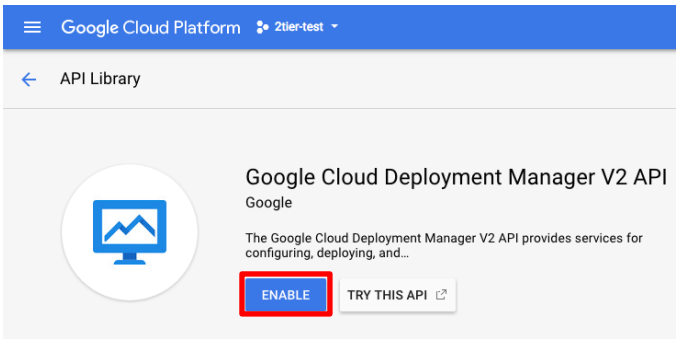
Select Google Cloud APIs on the left-hand-side:



Select Google **Cloud Deployment Manager V2 API**:



Select **Enable**:

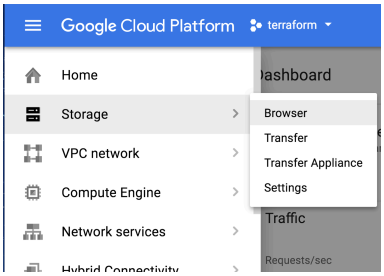


Note: Enabling the API for the project will take a few minutes to complete.

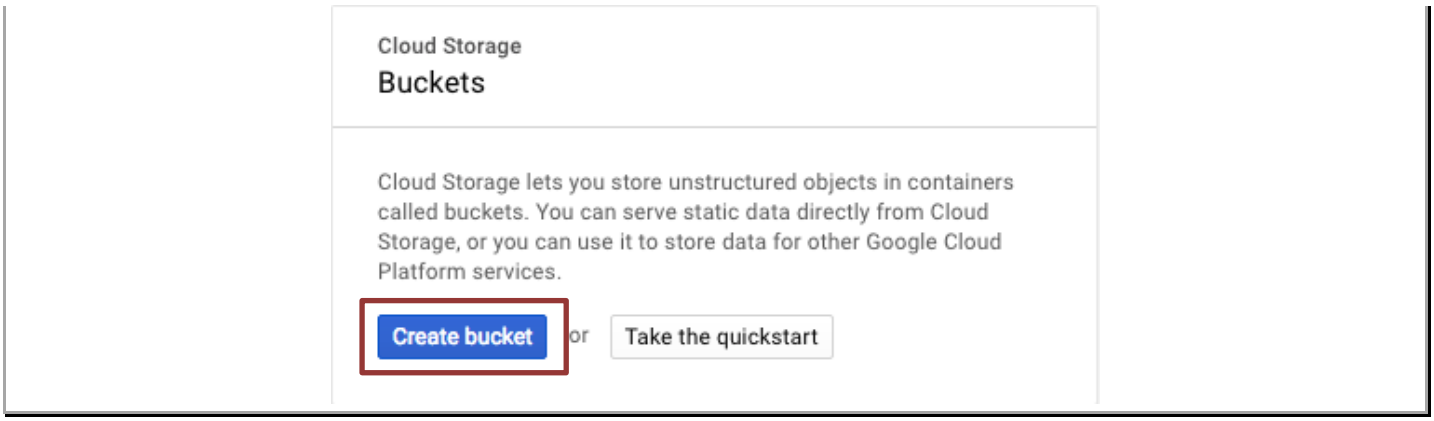
4.6 Create a Bootstrap Bucket

Bootstrapping is a feature of the VM-Series firewall that allows you to load a pre-defined configuration into the firewall during boot-up. This ensures that the firewall is configured and ready at initial boot-up, thereby removing the need for manual configuration. The bootstrapping feature also enables automating deployment of the VM-Series firewall.

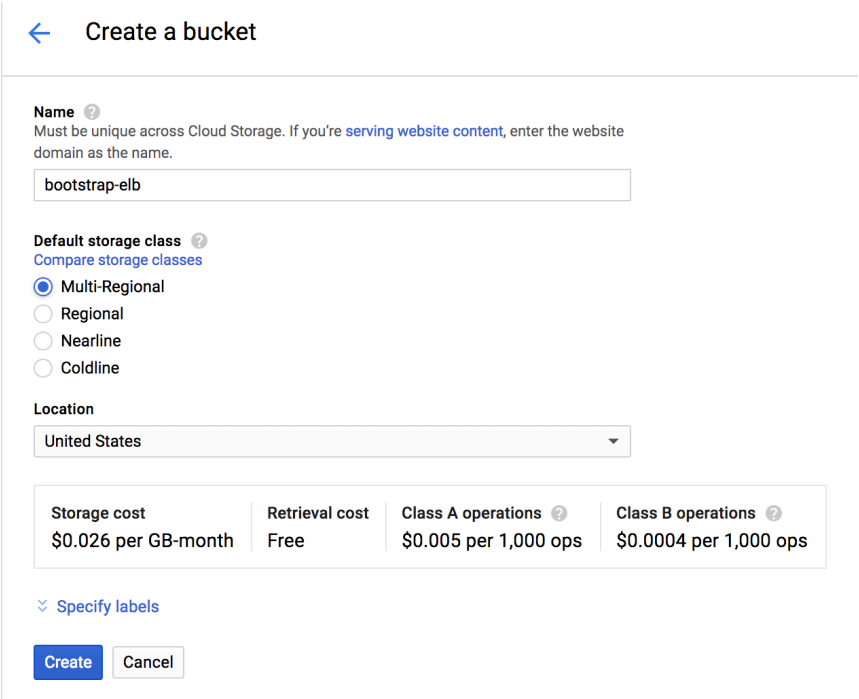
In order to create a Bootstrap bucket, navigate to **Storage > Browser**:



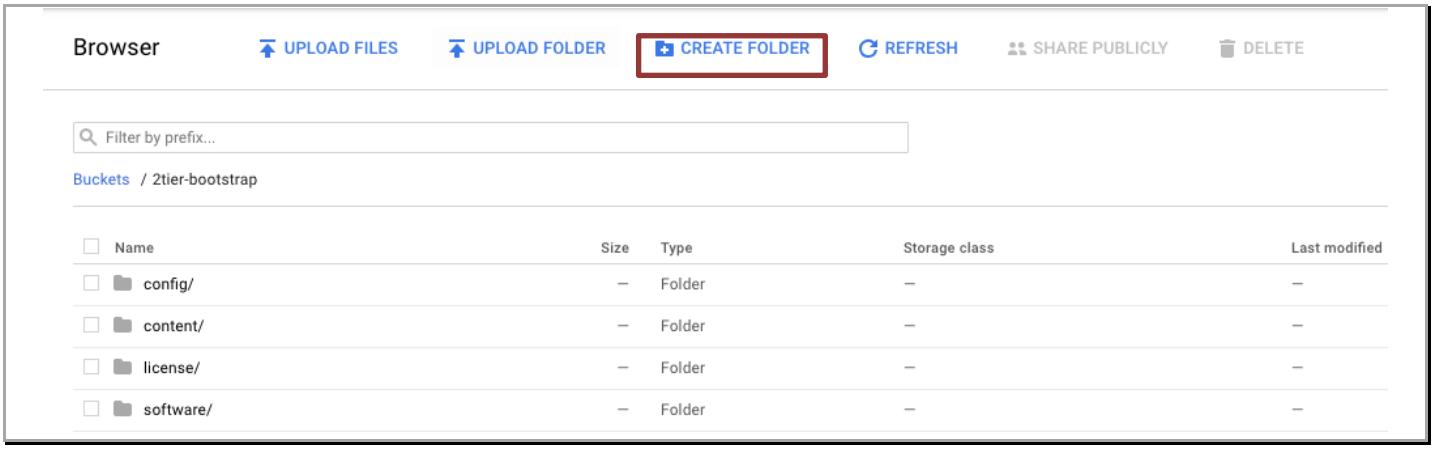
Click **Create Bucket**:



Specify a globally-unique bucket name and regional settings and click **Create**:



You will need to enter a globally unique bucket name. GCP will warn you if the name is not unique. Once the bucket is created, click on the newly created bucket and add four folders called **config, license, software** and **content** by clicking on **Create Folder**:

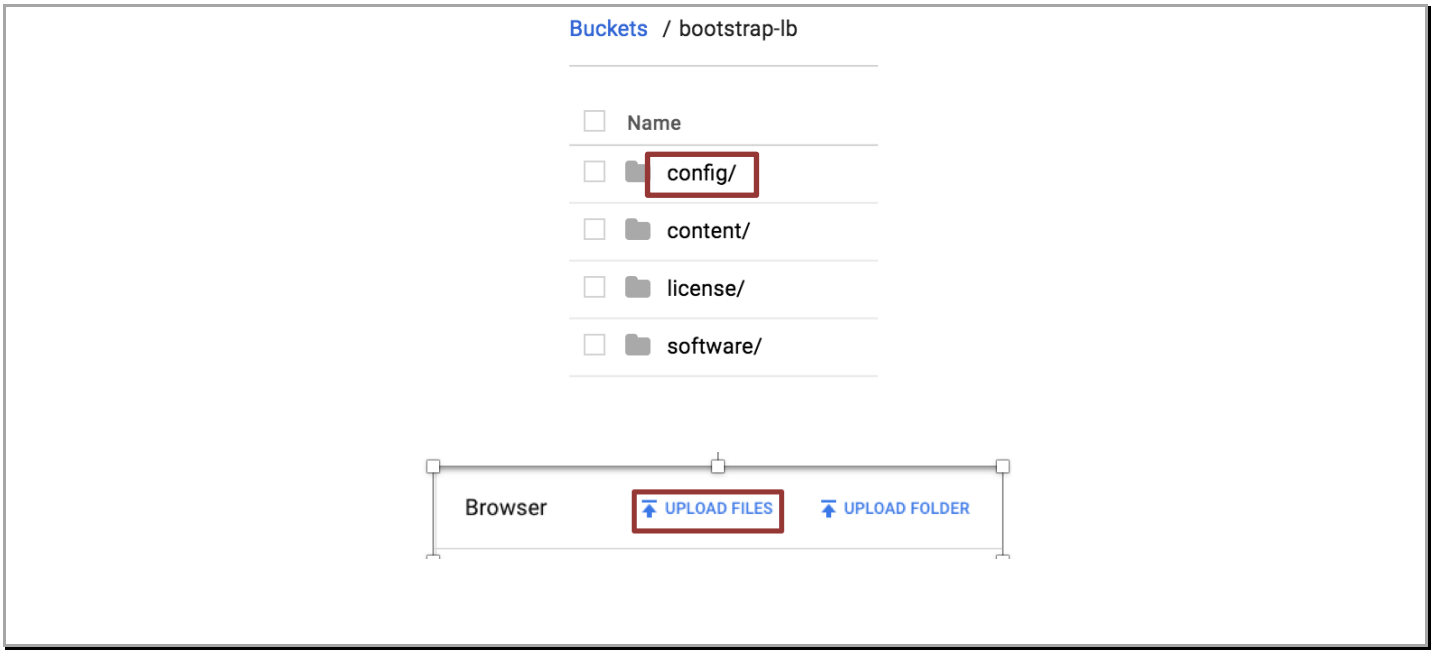


Download the following files using the links provided and save the files in a known location:

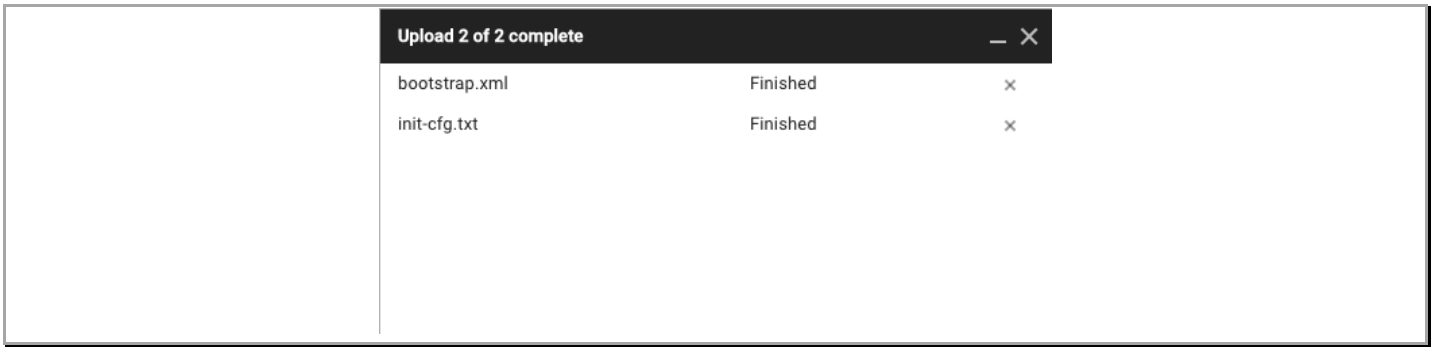
https://raw.githubusercontent.com/PaloAltoNetworks/wwce/master/googlecloud/pglynn/lb-sandwich/bootstrap.xml

https://raw.githubusercontent.com/PaloAltoNetworks/wwce/master/googlecloud/pglynn/lb-sandwich/init-cfg.txt

Now click on the **config** folder in the console and click **UPLOAD FILES:**



Select the two files (bootstrap.xml and init-cft.txt) downloaded previously and click **Open**:



NOTE: All four folders must be created for the bootstrapping process to occur. However, all folders DO NOT need to contain files.

NOTE: Please create the folders using the GUI or GCP CLI console. Creating folders locally on your machine and uploading them may not work as expected.

4.7 Download the Template Files

Download and save all of the template files to a known location by selecting **Clone or download**:

https://raw.githubusercontent.com/PaloAltoNetworks/wwce/master/googlecloud/pglynn/lb-sandwich/lb-sandwich.py

https://raw.githubusercontent.com/PaloAltoNetworks/wwce/master/googlecloud/pglynn/lb-sandwich/lb-sandwich.yaml

4.8 Gather Information and Update the Template File

Deploying the template in GCP requires modification of the .yaml file to include deployment-specific information. The minimum required information is:

```
project: <PROJECT NAME>

region: <REGION>

zone: <ZONE>

fwsourceimage: <URL TO FW SOURCE IMAGE>

bootstrapbucket: <BOOTSTRAP BUCKET NAME>

hostsourceimage: <URL TO WEBSERVER SOURCE IMAGE>

sshkey: <SSH KEY>
```

See the sample file

https://raw.githubusercontent.com/PaloAltoNetworks/wwce/master/googlecloud/pglynn/lb-sandwich/lb-sandwich.sample

for an example yaml configuration file.

5. Launch the Template

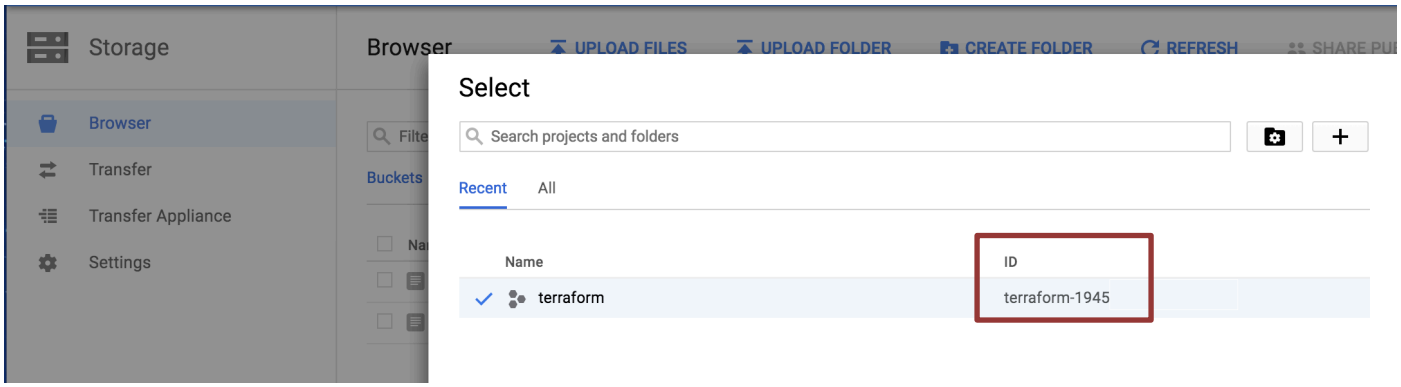
Navigate to a command shell navigate to the directory containing the downloaded template files:

Authenticate to the GCP environment from the command line with the command:

$ **gcloud auth login**

- Copy/paste the link into a browser and select the account to authenticate if a browser does not automatically launch:
- Review the requested permissions and click **Allow**:
- Copy the one-time verification code:
- Paste it into the window to complete the authentication request (ignore the warning):

Get the Project ID:



Set the target project for template deployment via command line:

$ gcloud config set project my_Project_id

Run Template Commands:

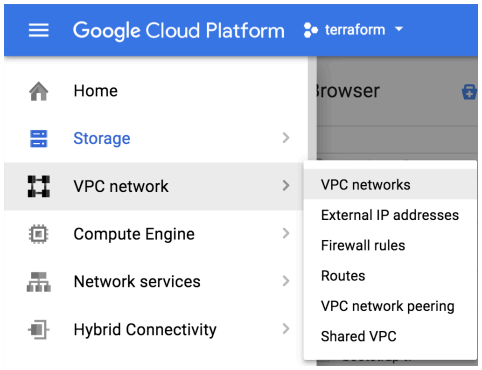
Initiate template deployment using command "gcloud deployment-manager deployments create <deployment name> --automatic-rollback-on-error --config lb-sandwich.yaml".

If all goes well, the deployment will report "COMPLETED" for all resources deployed. If not, additional information will be provided to assist the troubleshooting process.

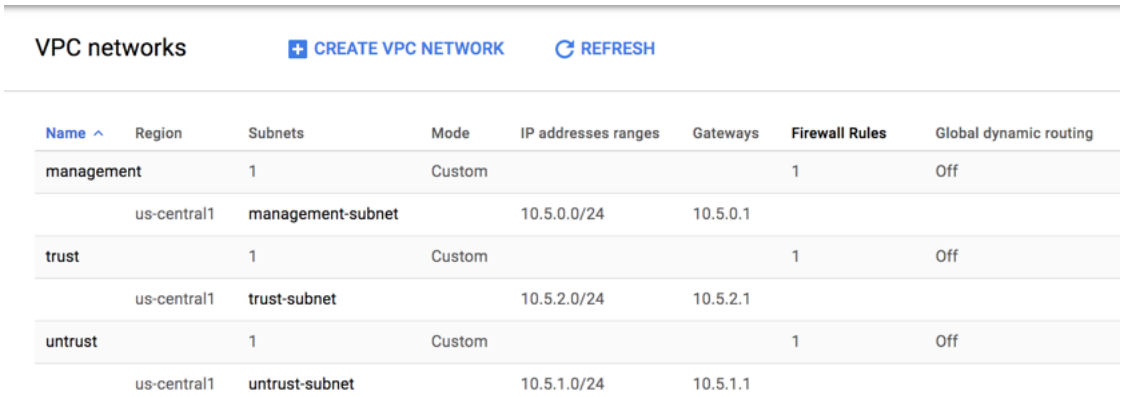
```
root@c22df743628d:~/Development/GCP/lbsandwich/python# clear; gcloud deployment-manager deployments cr
eate deployment-with-templates --automatic-rollback-on-error --config lb-sandwich.ptg
The fingerprint of the deployment is NrMad49-jp8VvRturv3iHA==
Waiting for create [operation-1524704222261-56ab5dd8e2f08-fcf14bd0-cba0e95a]...done.
Create operation operation-1524704222261-56ab5dd8e2f08-fcf14bd0-cba0e95a completed successfully.
NAME                                    TYPE                                    STATE      ERRORS  INTENT
firewall-backendservice                 compute.v1.backendService               COMPLETED  []
firewall-globalforwardingrule           compute.v1.globalForwardingRule         COMPLETED  []
firewall-healthcheck                    compute.v1.healthCheck                  COMPLETED  []
firewall-httpproxy                      compute.v1.targetHttpProxy              COMPLETED  []
firewall-urlmap                         compute.v1.urlMap                       COMPLETED  []
firewalla-instancegroup                 compute.v1.instanceGroupManager         COMPLETED  []
firewalla-instancetemplate              compute.v1.instanceTemplate             COMPLETED  []
firewallb-instancegroup                 compute.v1.instanceGroupManager         COMPLETED  []
firewallb-instancetemplate              compute.v1.instanceTemplate             COMPLETED  []
management                              compute.v1.network                      COMPLETED  []
management-firewall                     compute.v1.firewall                     COMPLETED  []
management-subnet                       compute.v1.subnetwork                   COMPLETED  []
trust                                   compute.v1.network                      COMPLETED  []
trust-firewall                          compute.v1.firewall                     COMPLETED  []
trust-subnet                            compute.v1.subnetwork                   COMPLETED  []
untrust                                 compute.v1.network                      COMPLETED  []
untrust-firewall                        compute.v1.firewall                     COMPLETED  []
untrust-subnet                          compute.v1.subnetwork                   COMPLETED  []
webserver-forwardingrule                compute.v1.forwardingRule               COMPLETED  []
webserver-healthcheck                   compute.v1.healthCheck                  COMPLETED  []
webserver-regionbackendservice          compute.v1.regionBackendService         COMPLETED  []
webservera-instancegroup                compute.v1.instanceGroupManager         COMPLETED  []
webservera-instancetemplate             compute.v1.instanceTemplate             COMPLETED  []
webserverb-instancegroup                compute.v1.instanceGroupManager         COMPLETED  []
webserverb-instancetemplate             compute.v1.instanceTemplate             COMPLETED  []
```

6. Review what was created

Let's review what the template has launched. The newly created networks can be viewed via **VPC Networks > VPC Network**:



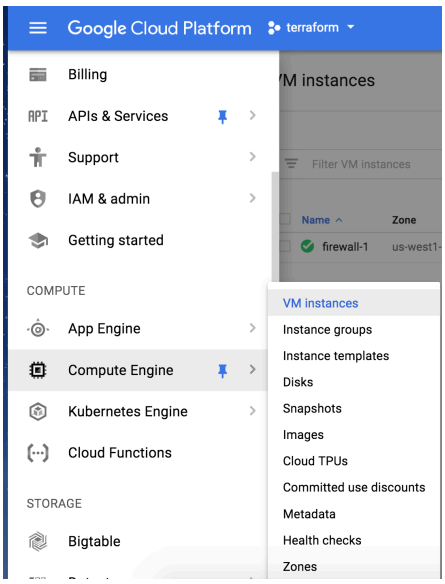
The template creates four networks: management-subnet, trust-subnet, and untrust-subnet.



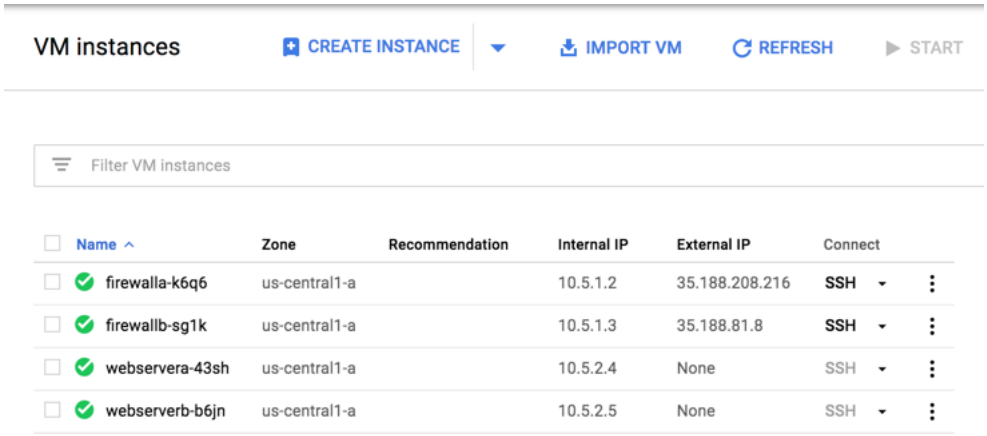
Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing
management		1	Custom			1	Off
	us-central1	management-subnet		10.5.0.0/24	10.5.0.1		
trust		1	Custom			1	Off
	us-central1	trust-subnet		10.5.2.0/24	10.5.2.1		
untrust		1	Custom			1	Off
	us-central1	untrust-subnet		10.5.1.0/24	10.5.1.1		

Note: A default network is automatically created when a GCP Project is instantiated. This default network can be ignored or deleted.

Deployed hosts can be viewed by navigating to **Compute Engine > VM Instances**:



High-level information regarding the deployed instances are available with the default view:



Also note the order in which the networks are attached to the firewalls. Click on firewalla and scroll down to see the network order.

VM instance details EDIT RESET CLONE STOP DELETE

firewalla-k6q6

Remote access

SSH | Connect to serial console

Enable connecting to serial ports

Logs
Stackdriver Logging
Serial port 1 (console)
More

Instance template
firewalla-instancetemplate

Machine type
n1-standard-4 (4 vCPUs, 15 GB memory)

In use by
firewalla-instancegroup

CPU platform
Intel Skylake

Zone
us-central1-a

Labels
None

Creation time
Apr 25, 2018, 7:58:06 PM

Network interfaces

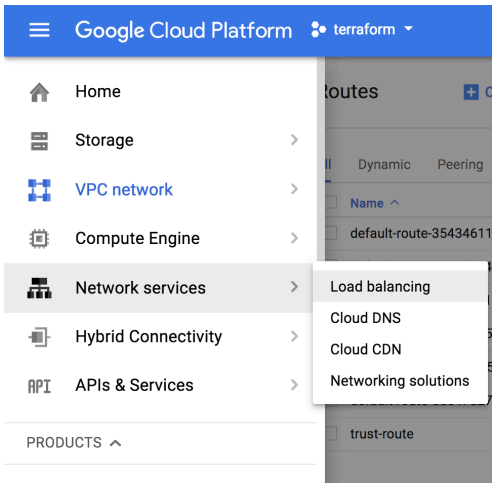
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
untrust	untrust-subnet	10.5.1.2	–	35.188.208.216 (ephemeral)	On
management	management-subnet	10.5.0.2	–	35.192.97.167 (ephemeral)	
trust	trust-subnet	10.5.2.2	–	None	

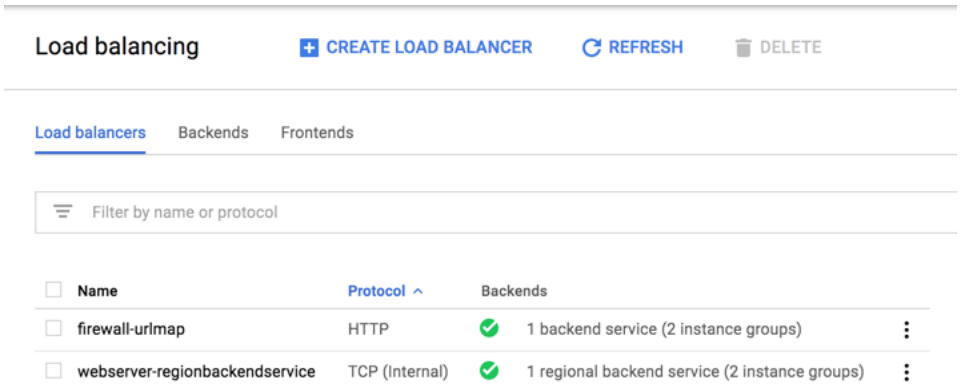
Public DNS PTR Record
None

Network tags
None

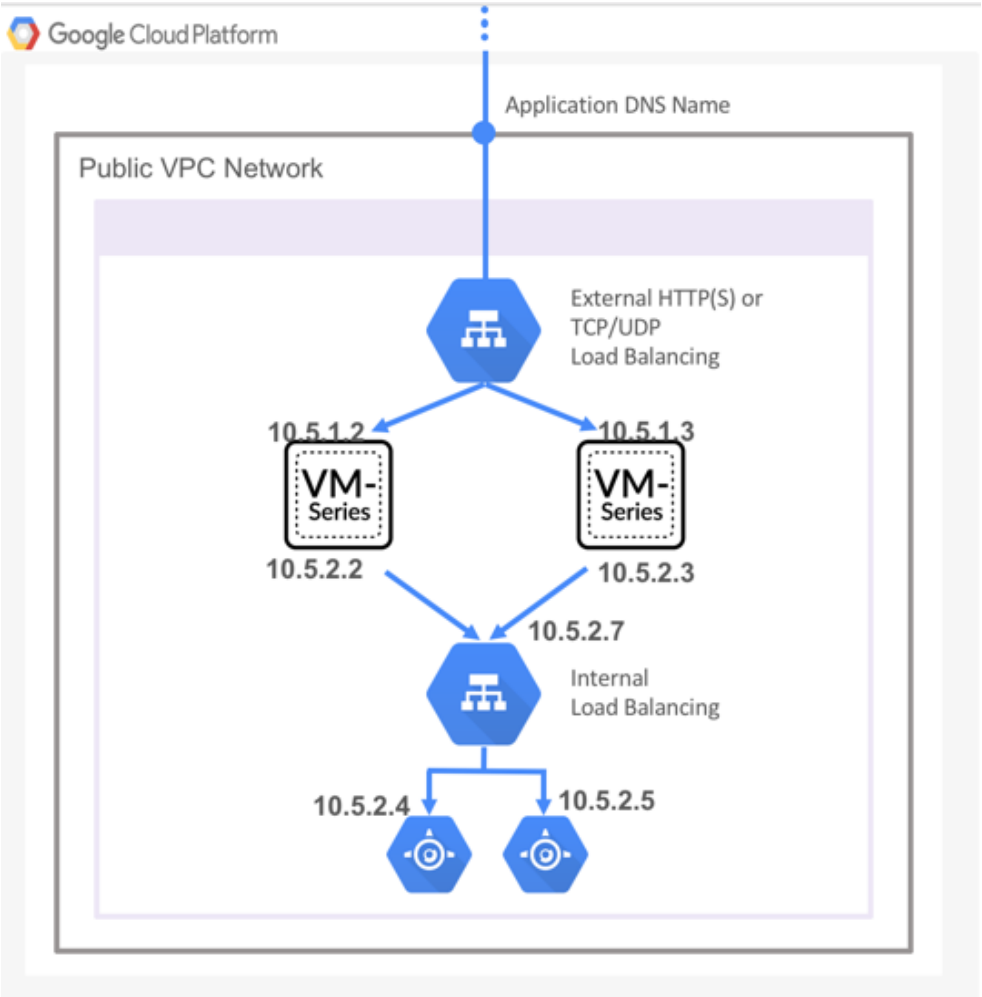
NOTE: The untrust subnet is first. The GCP Load Balancers only communicate with the lowest numbered interface on a VM. During the bootstrap phase of deployment, the init-cfg.txt told the VM-Series firewall to perform a management interface swap. Therefore, we must have the GCP networks in this order.

Lastly check your newly deployed Load Balancers by navigating to Network Services then select Load Balancing.



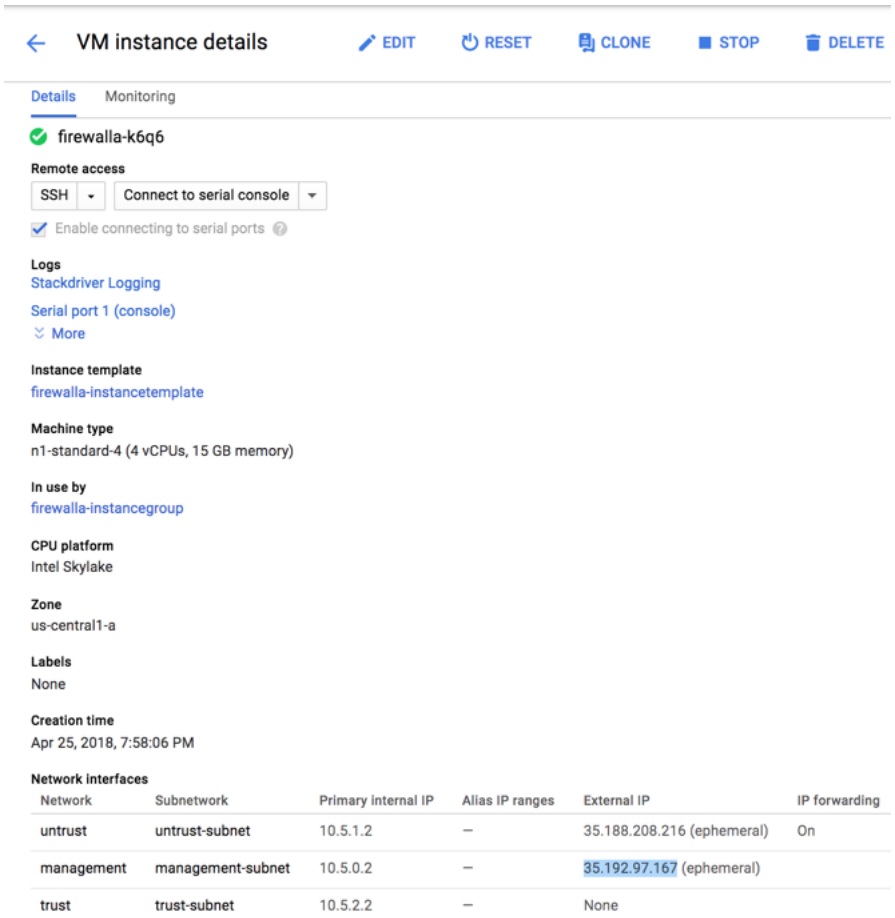


All of this matches the topology shown previously:

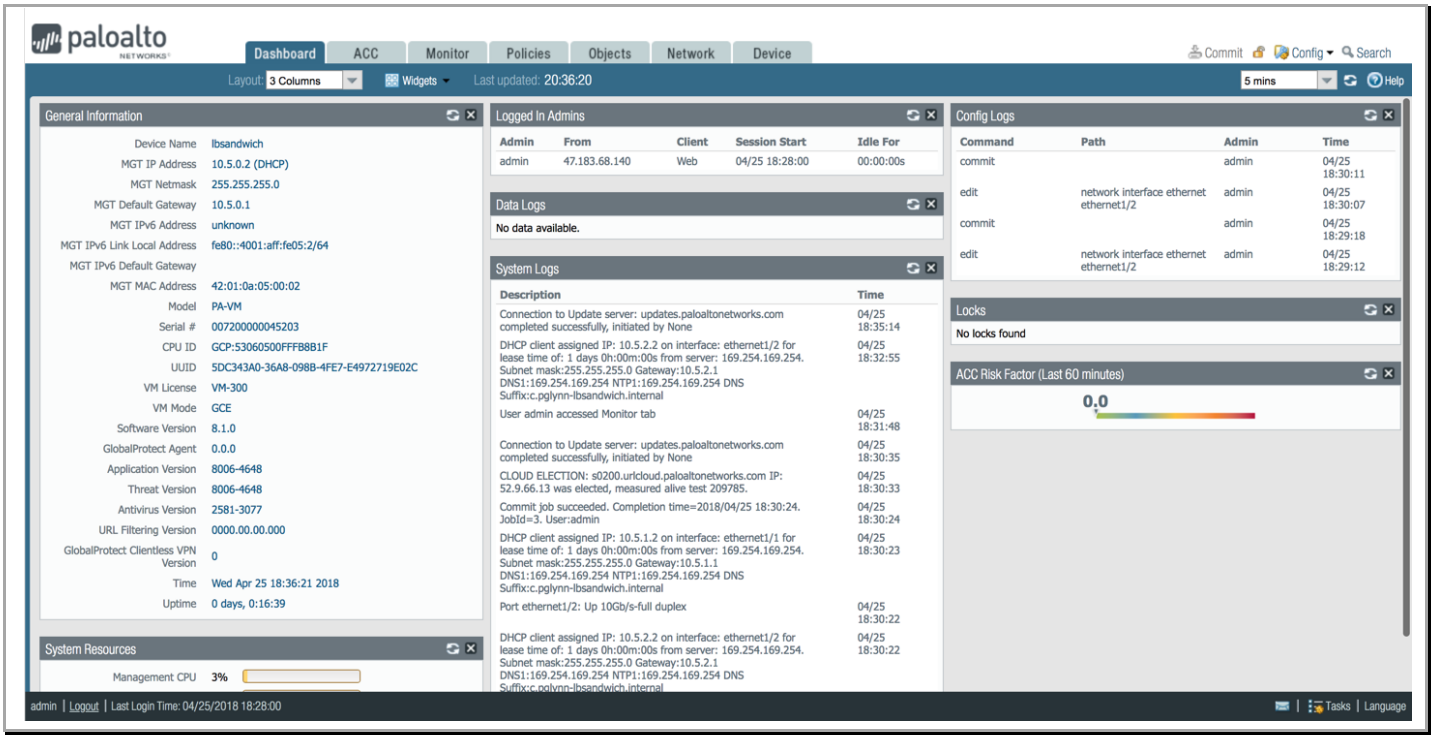


7. Access the firewall

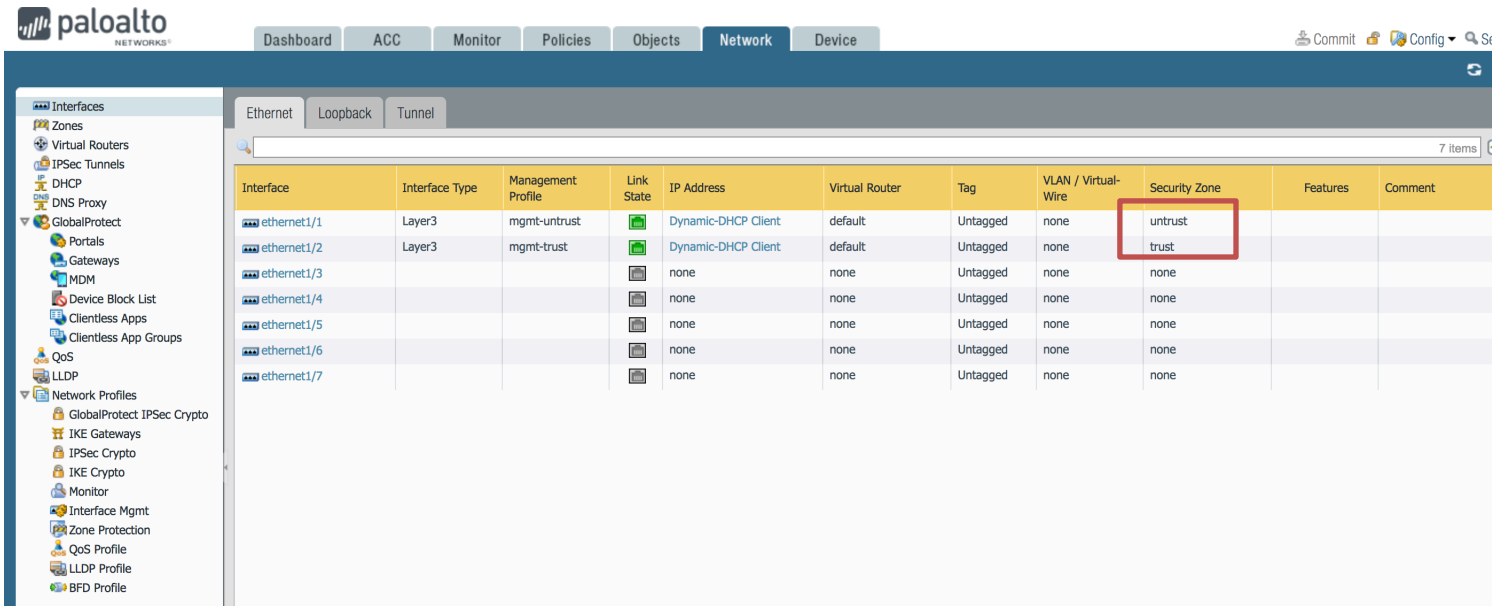
NOTE: Bootstrapping a VM-Series firewall takes approximately 9 minutes. Be patient☺ Once the template has been deployed successfully, it may be a while before the VM-Series firewall is up and you are able to log into the VM-Series firewall by browsing to the Management public IP Address. Recall we swapped the Management interface so you will need to click on the VM Series to get the Public IP address.



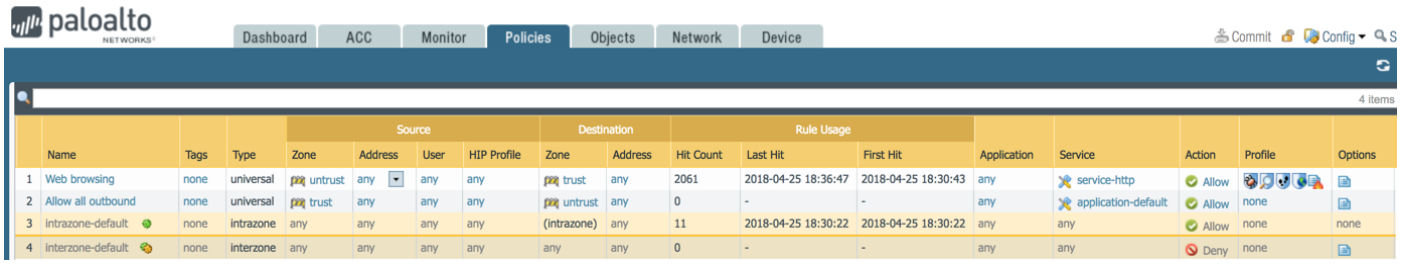
You should now be able to browse to the VM-Series firewall and login using the **username: admin** and password: **knav9Rav8eCk8Oj1coC3**



Here are the interfaces to zone mappings.

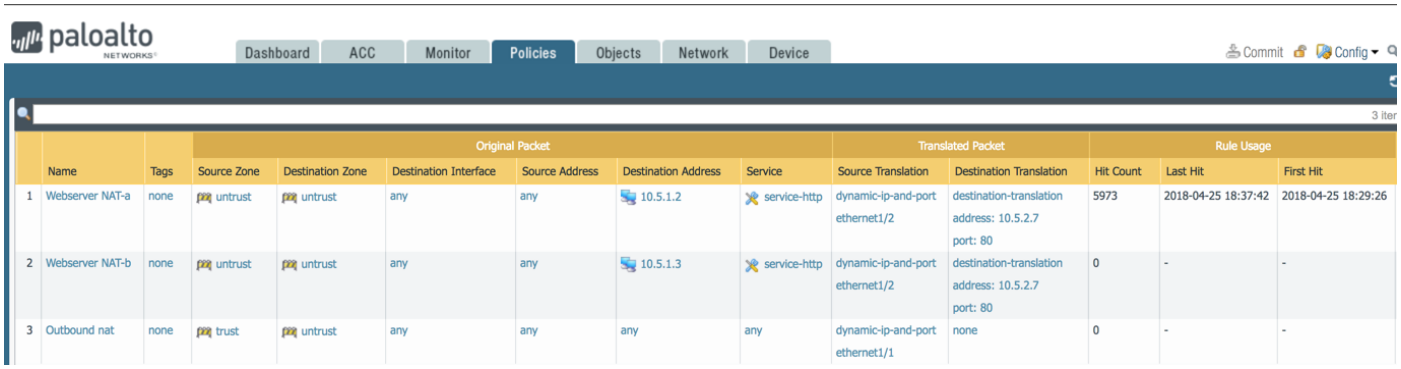


In the policies tab you can review the security policies:



	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage First Hit	Application	Service	Action	Profile	Options
1	Web browsing	none	universal	untrust	any	any	any	trust	any	2061	2018-04-25 18:36:47	2018-04-25 18:30:43	any	service-http	Allow		
2	Allow all outbound	none	universal	trust	any	any	any	untrust	any	0	-	-	any	application-default	Allow	none	
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	11	2018-04-25 18:30:22	2018-04-25 18:30:22	any	any	Allow	none	none
4	interzone-default	none	interzone	any	any	any	any	any	any	0	-	-	any	any	Deny	none	

And the NAT rules:



	Name	Tags	Original Packet Source Zone	Original Packet Destination Zone	Original Packet Destination Interface	Original Packet Source Address	Original Packet Destination Address	Original Packet Service	Translated Packet Source Translation	Translated Packet Destination Translation	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage First Hit
1	Webserver NAT-a	none	untrust	untrust	any	any	10.5.1.2	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.5.2.7 port: 80	5973	2018-04-25 18:37:42	2018-04-25 18:29:26
2	Webserver NAT-b	none	untrust	untrust	any	any	10.5.1.3	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.5.2.7 port: 80	0	-	-
3	Outbound nat	none	trust	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	0	-	-

8. Access the Webservers via ELB

Open a browser and browse to the IP address of the ELB. The IP of the ELB can be found under load balancers then expand the ELB(firewall-urlmap):

Load balancer details EDIT DELETE

firewall-urlmap

Details Monitoring Caching

Frontend

Protocol	IP:Port	Certificate
HTTP	35.186.218.130:80	–

Host and path rules

Hosts	Paths	Backend
All unmatched (default)	All unmatched (default)	firewall-backendservice

Backend

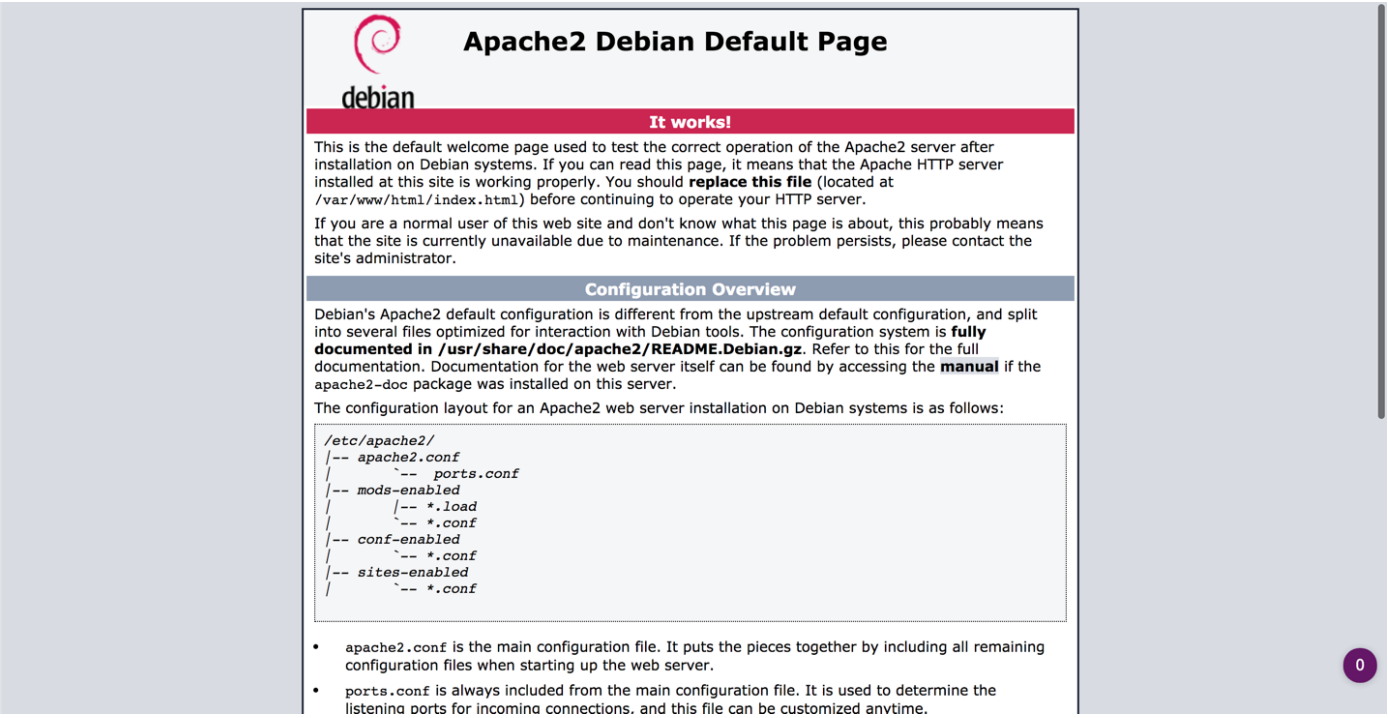
Backend services

1. firewall-backendservice

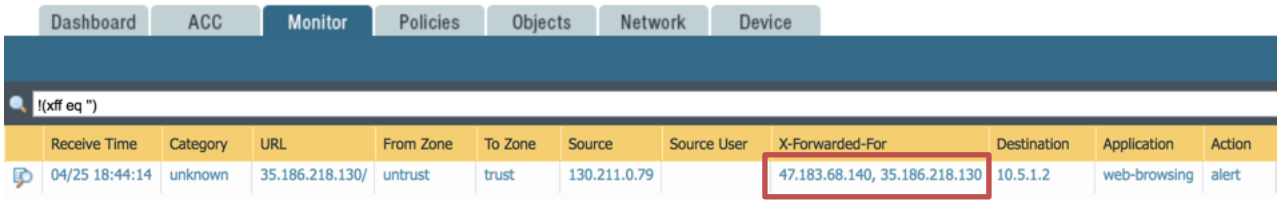
Endpoint protocol: **HTTP** Named port: **http** Timeout: **30 seconds** Health check: firewall-healthcheck Session affinity: **None** Cloud CDN: **disabled** Security policy: **None**

Advanced configurations

Instance group	Zone	Healthy	Autoscaling	Balancing mode	Capacity
firewalla-instancegroup	us-central1-a	1 / 1	Off	Max CPU: 80%	100%
firewallb-instancegroup	us-central1-a	1 / 1	Off	Max CPU: 80%	100%



The Firewall URL filtering logs will log the XFF in the URL filtering logs (you may need to check both firewalls):



You have now successfully deployed the template with a VM-Series firewall in GCP.

9. Cleanup

9.1 Delete the deployment

Once done, cleanup as follows:

- If you licensed the VM-Series firewall perform the De-License function.
  - https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/license-the-vm-series-firewall/deactivate-vm#_87329
- From the CLI, issue the command "gcloud deployment-manager deployments delete <deployment name>"
  - This will delete all the resources created via the template.

10. Conclusion

You have successfully deployed a template in GCP and demonstrated how the Palo Alto Next Generation VM-Series firewall can be deployed via automation to not only secure traffic throughout your GCP Project, but throughout your Enterprise Google Cloud Infrastructure.

Appendix A

Troubleshooting tips

1. Firewall not showing healthy

Occasionally, the firewall's trust interface will fail to acquire an IP address. In that case, the health check from the ELB will fail and the firewall will show as unhealthy. The fix is to manually set the interface to 'down' , commit, set the interface back to 'auto' and commit.

2. Bootstrapping not working

If the VM-Series firewall is up and you are able to access the login page, but unable to login using the username/password: admin/knav9Rav8eCk8Oj1coC3, then chances are bootstrapping has failed. There could be several reasons:

a. Corrupt configuration files

Please ensure that the bootstrap.xml and init-cft.txt files mentioned in Section 4.6 are not corrupted.

b. Incorrect bootstrap bucket-name

Another reason for bootstrapping to fail is that the bootstrap bucket name (Parameter: bootstrapbucket) was incorrectly entered in the template file. Please make sure the bucket name created in Section 4.6 is mentioned when launching the template.