

Ignite19-US-HOW-14-Protecting-Kubernetes

Hands-On-Workshop

Protecting your container workloads in Kubernetes

Terraform Version



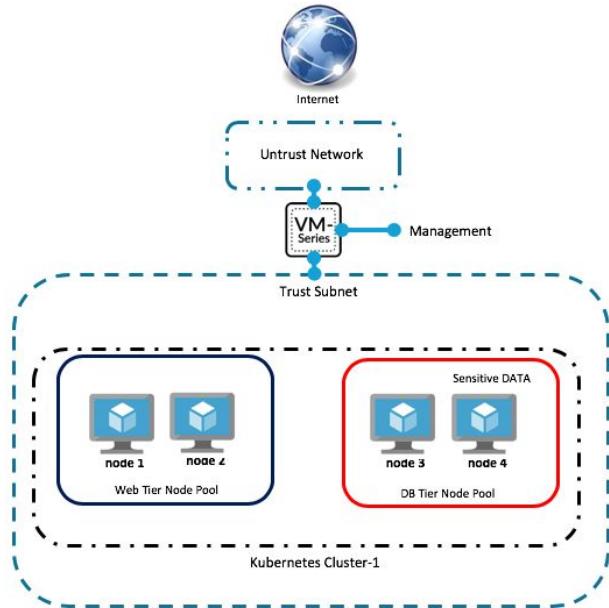
Table of Contents

Lab Overview	4
About GCP Terraform Templates	5
Support Policy	6
Activity 1 – GCP Setup	7
Task 1 – Create a Project	7
Task 2 – Enable the Needed APIs	9
Activity 2 – Terraform File Setup	11
Task 1 – Download Terraform files	11
Task 2 – Gather Information and Update the Variables.tf file	14
Activity 3 – Deploy the Terraform Template	22
Task 1 – Authenticate Google Cloud SDK	22
Task 2 – Deploy the Terraform Template	24
Activity 4 – Review what was deployed	27
Task 1 – Understand what has been initially deployed	27
Task 2 – Look around GCP console	28
Task 3 – Login into the firewall	32
Activity 5 – Container Image Scanning for Vulnerabilities	36
Task 1 – Connect to a Cloud Shell	37
Task 2 – Build and Scan the Application Container Image	40
Activity 6 – Kubernetes App Manifest Scanning for Security Misconfigurations	45
Task 1 – Scan the Application Manifest for Security Best Practices	46
Task 2 – Update the Manifest to Fix the Policy Violations	48
Activity 7 – Launch a two tiered application	50
Task 1 – Inspect the Guestbook Manifest file	50
Task 2 – Launch the Application	54
Task 3 – Explore what was just deployed	54
Activity 8 – Securing Inbound Traffic	59
Task 1 – Note the Internal Load Balancer’s IP Address	59
Task 2 – Update the Firewall’s NAT Policy	59
Task 3 – Connect to the Guestbook Frontend	61

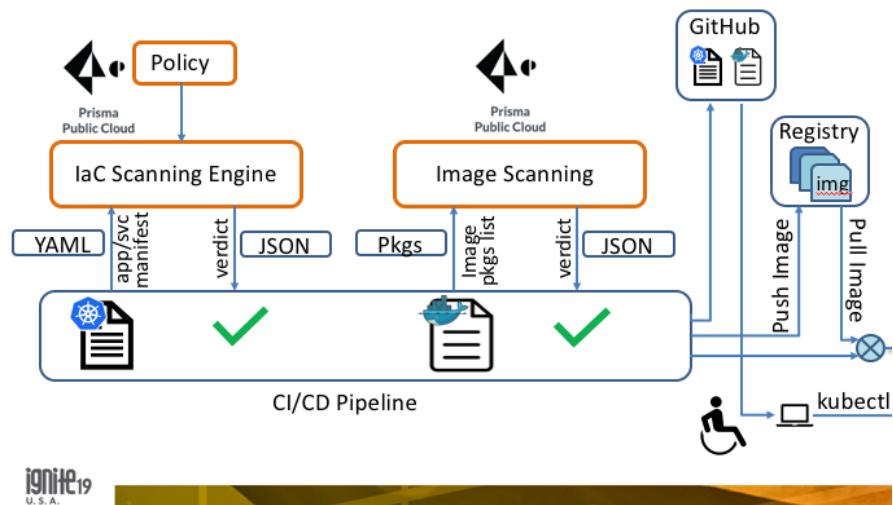
Activity 9 – Securing Outbound Traffic	64
Task 1 – Add Kube-API server route	64
Task 2 – Add Outbound Route	65
Task 3 – Test Outbound Pod Traffic	68
Activity 10 – Investigate Inter Node-Pool traffic	71
Task 1 – View Node Pool Setup	72
Task 2 – View GCP Routing Rules	75
Task 3 – View the VM-Series Firewall Routing	76
Task 4 – Validate North/South and East/West traffic in the firewall logs	77
Conclusion	79

Lab Overview

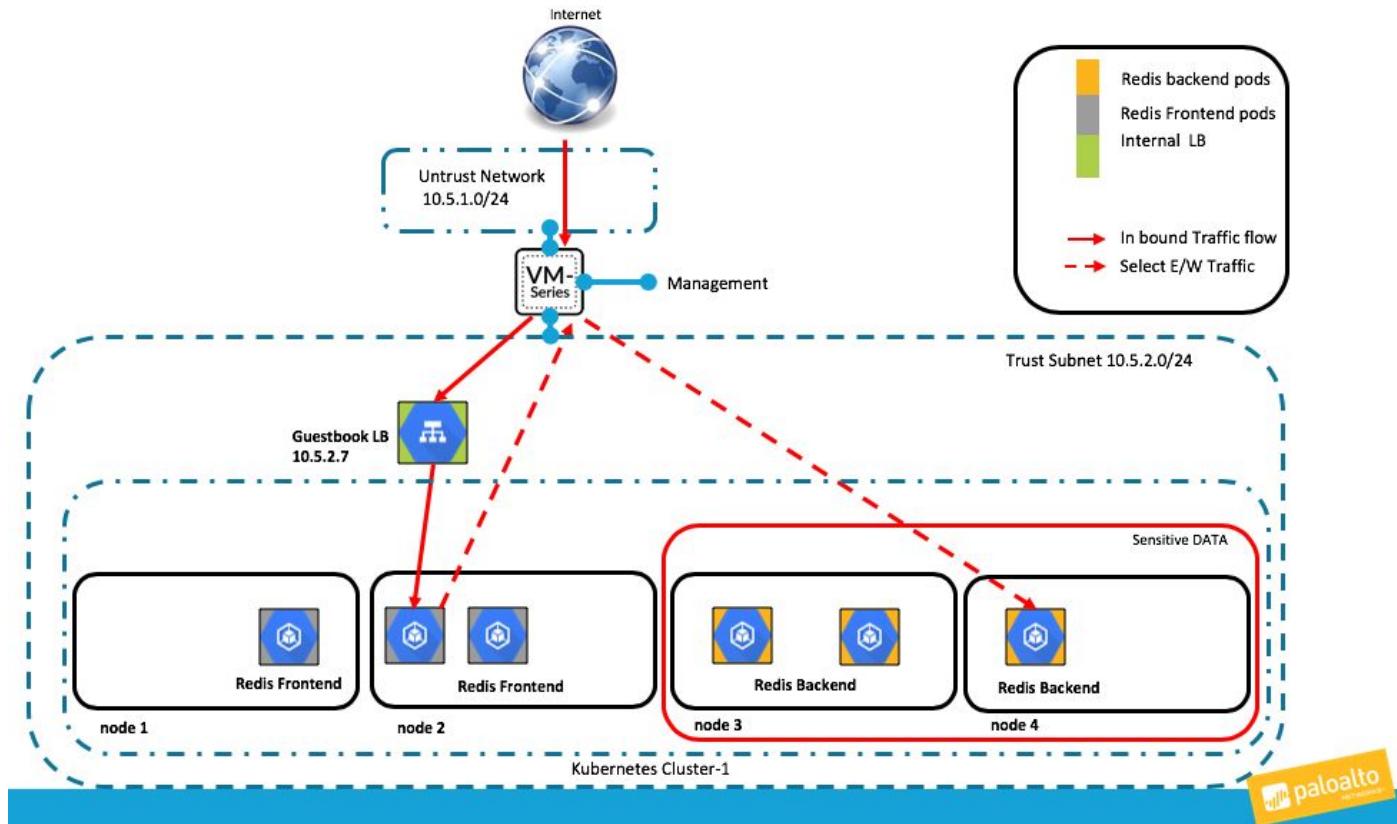
This lab will walk through deploying a Terraform template that deploys a Kubernetes(k8s) cluster, Palo Alto Networks VM-Series firewall into an existing GCP project. After successfully deploying the terraform template, the following infrastructure will be instantiated:



Then the lab will then guide through the use of the Prisma Public Cloud API Scanning of a container image and K8s Manifest file.



Finally the lab will deploy the manifest file to the k8s cluster and walk through visibility of both North/South and select East/West traffic flows. The following diagram shows the deployed pods with the traffic flows:



About GCP Terraform Templates

GCP Terraform Templates are files that can deploy, configure, and launch GCP resources such as VPC networks, subnets, security groups, firewall rules, route tables, Kubernetes clusters, 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/community/tutorials/managing-gcp-projects-with-terraform>

There are also many Terraform template s available here:

<https://github.com/GoogleCloudPlatform/terraform-google-examples>

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.

Instances Used

When deploying this Terraform template the following machine types are used:

Instance	Machine Type	QTY
PayGo Bundle 1 – VM-Series Firewall	n1-standard-4	1
Kubernetes Ubuntu Cluster Nodes	n1-standard-1	4
Internal Load Balancer		1

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

Prerequisites

Here are the prerequisites required to successfully launch this template:

- Terraform application - Instructions on the installation can be found here: <https://www.terraform.io/intro/getting-started/install.html>
- GCP account- Account creation can be done here: <https://cloud.google.com/free/>
- Google Cloud SDK- GCP template installations in this guide 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/>

Activity 1 – GCP Setup

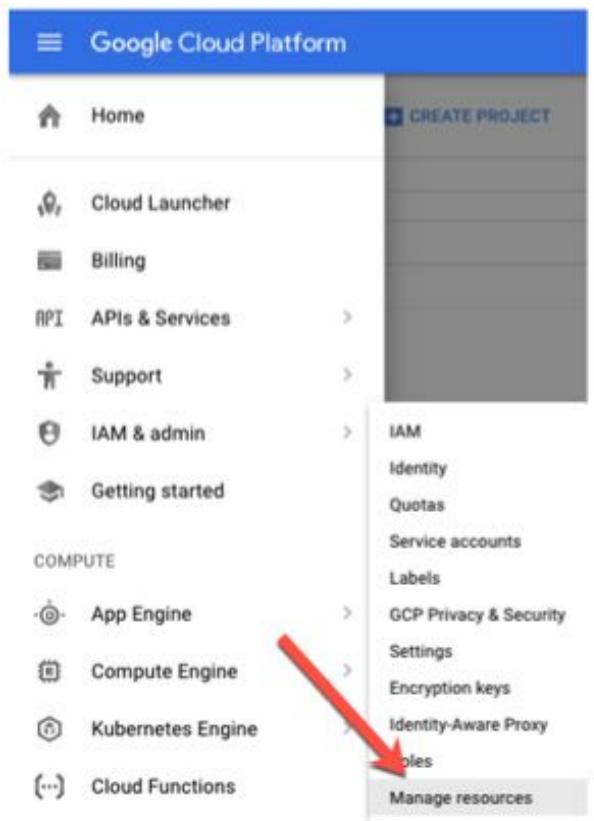
In this activity, you will:

- **Create a project**
- **Enable the APIs needed for this lab**

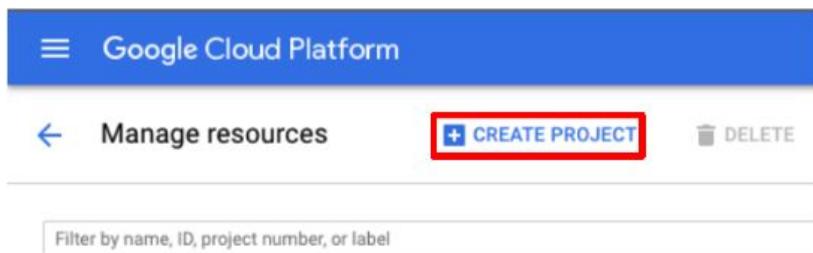
Task 1 – Create a Project

All GCP resources in this guide are deployed to a single project, which is an organizational boundary that separates users, resources, billing information, etc. It is similar to an AWS VPC or an Azure Resource Group. By default, GCP will create a project upon creation of an account.

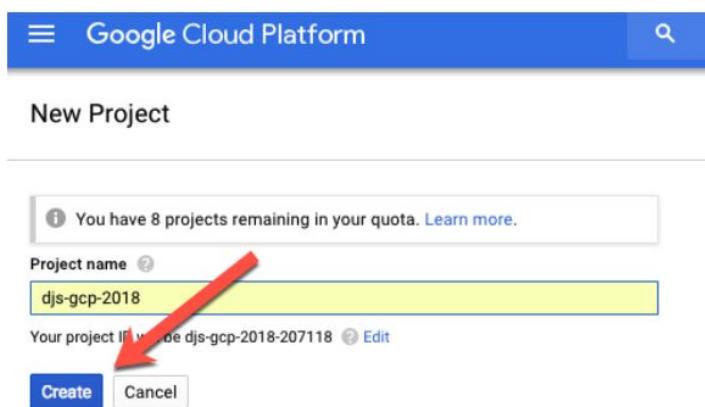
- To create an additional dedicated project, use the drop-down on the left and select **IAM & admin > Manage Resources**:



→ Click **Create Project**:



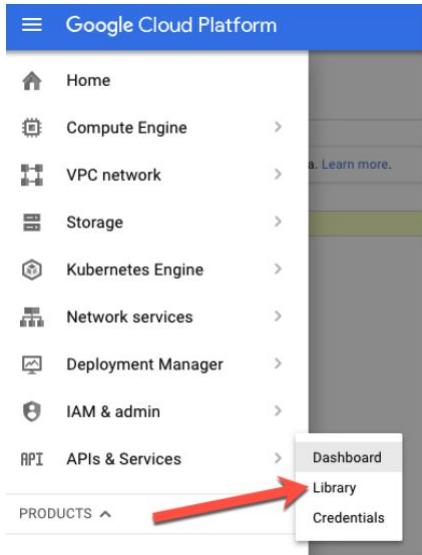
→ Specify a name for the project and click **Create**:



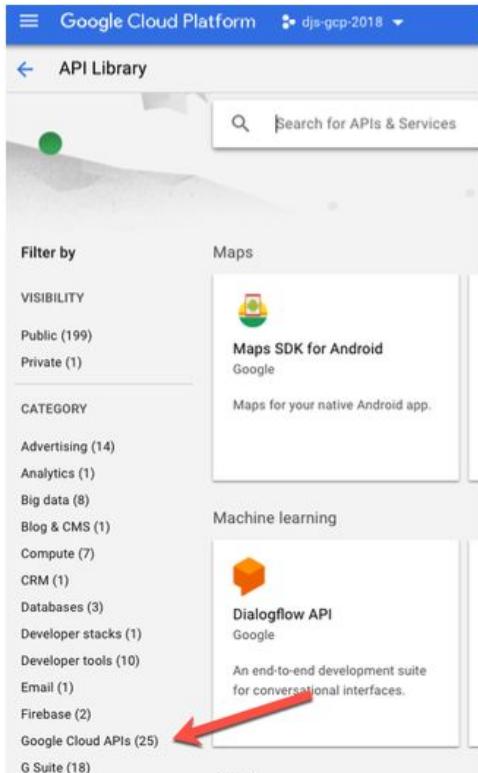
Note that project creation will take a few minutes.

Task 2 – Enable the Needed APIs

Deploying a template requires the Cloud Deployment Manager API be enabled on the project.
Navigate to **APIs & Services >Library**:



→ Select Google Cloud APIs on the Left-Hand-Side:



→ Select Google Cloud Deployment Manager V2 API:

The screenshot shows the Google Cloud Platform API Library interface. A red arrow points to the first item in the grid, which is the "Google Cloud Deployment Manager V2 API". This item has a blue icon of a monitor with a chart. The text below the icon reads: "The Google Cloud Deployment Manager V2 API provides services for configuring, deploying, and..."

you the benefits of App...	
Google Cloud Deployment Manager V2 API Google The Google Cloud Deployment Manager V2 API provides services for configuring, deploying, and...	Google Cloud SQL Google Google Cloud SQL is a hosted and fully managed relational database service on Google's...
Google Cloud Storage Google Google Cloud Storage is a RESTful service for storing and accessing your data on Google's ...	Google Container Registry API Google Google Container Registry provides secure, private Docker image storage on Google Cloud
Service Control API Google Google Service Control provides control plane functionality to managed services, such as...	Service Management API Google Google Service Management allows service producers to publish their services on Google

→ Select Enable:

The screenshot shows the "Google Cloud Deployment Manager V2 API" page. It features a large circular icon with a monitor and chart. Below the icon, the text reads: "The Google Cloud Deployment Manager V2 API provides services for configuring, deploying, and...". At the bottom, there are two buttons: a red "ENABLE" button and a grey "TRY THIS API" button.

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

End of Activity 1

Activity 2 – Terraform File Setup

In this activity, you will:

- **Download the Terraform Files needed to instantiate the environment**
- **Identify the variable parameters needed for Terraform and configure**

Task 1 – Download Terraform files

→ Navigate to the following GitHub repository to get the terraform files:

<https://github.com/PaloAltoNetworks/GCP-VM-Series-k8s-Prisma-Cloud-API>

For this lab, the Main.tf and Variables.tf files will need to be downloaded to your local machine.

→ Click on the Main.tf file:

PaloAltoNetworks / GCP-k8s-Prisma-Cloud-API Private

Watch 0 Star 0 Fork 0

Code Issues 1 Pull requests 0 Projects 0 Wiki Security Insights Settings

Deploys k8s cluster, VM-Series for N/S and E/W inspection and guides the use of the Prisma Cloud API scan of Manifest Edit

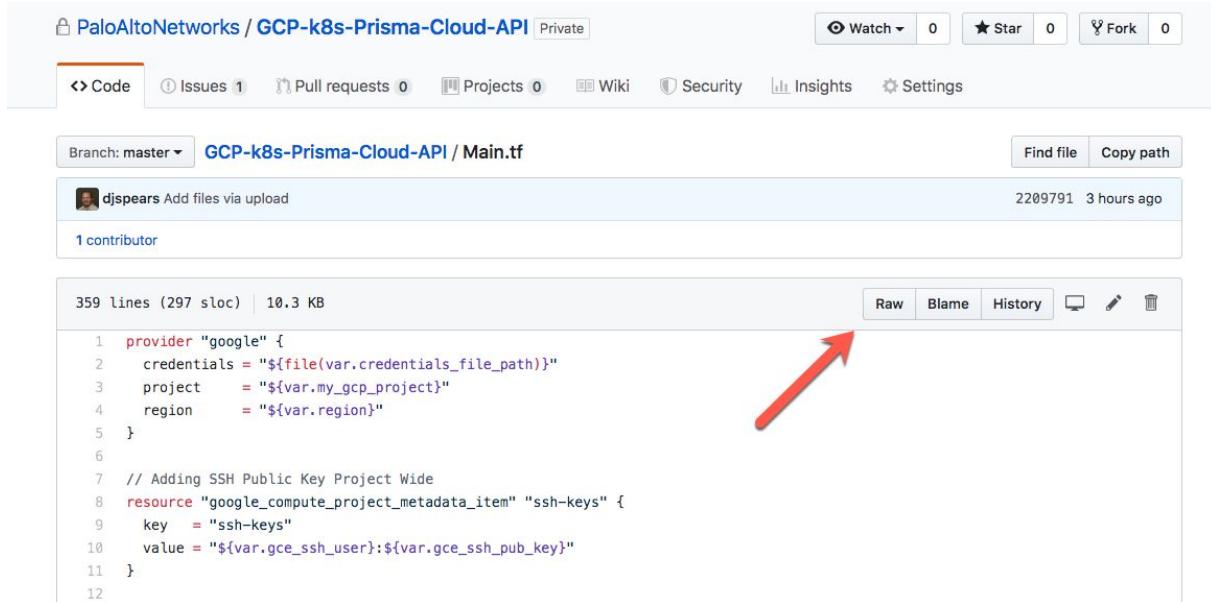
Manage topics

9 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find File Clone or download

File	Action	Time
README.md	Update README.md	Latest commit e6c6148 3 hours ago
Main.tf	Add files via upload	3 hours ago
Variables.tf	Add files via upload	3 hours ago
Terraform version Ignite19-US-HOW-14-Protecting-Kubernetes.pdf	Add files via upload	3 hours ago

→ Next Select Raw and save to a known local location:



PaloAltoNetworks / GCP-k8s-Prisma-Cloud-API · Private

Branch: master · GCP-k8s-Prisma-Cloud-API / Main.tf

djspears Add files via upload · 2209791 · 3 hours ago

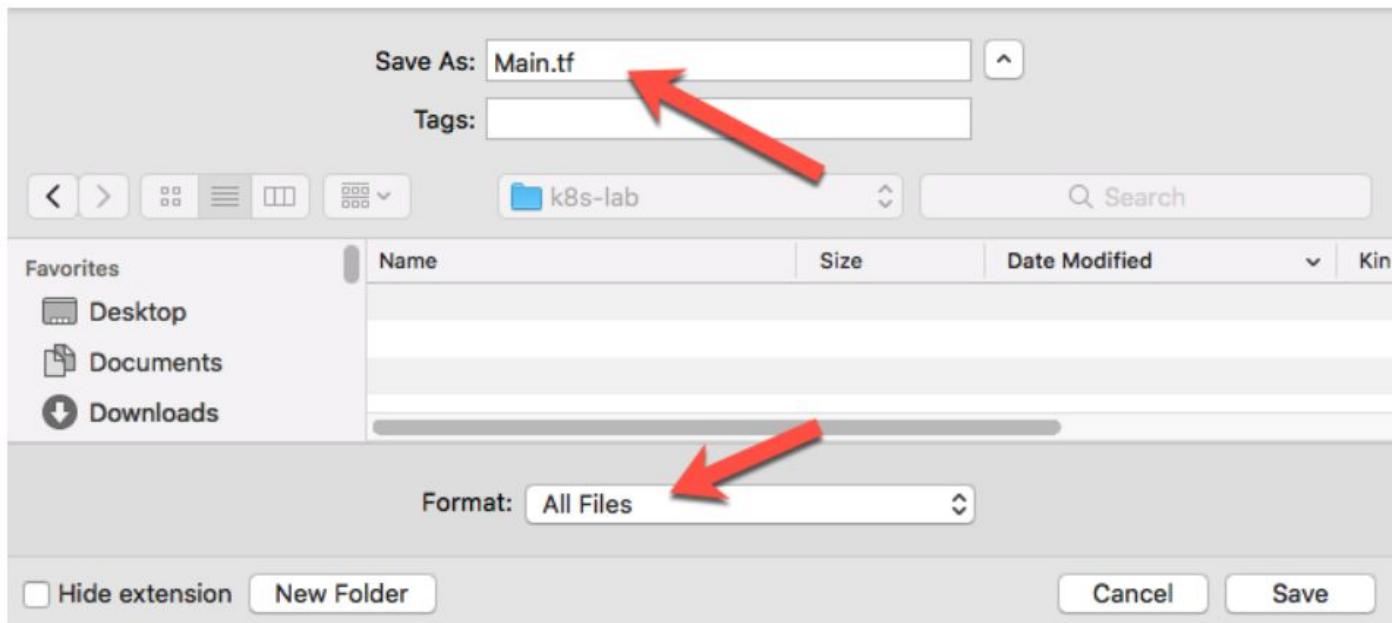
1 contributor

359 lines (297 sloc) | 10.3 KB

```
1 provider "google" {  
2   credentials = "${file(var.credentials_file_path)}"  
3   project     = "${var.my_gcp_project}"  
4   region      = "${var.region}"  
5 }  
6  
7 // Adding SSH Public Key Project Wide  
8 resource "google_compute_project_metadata_item" "ssh-keys" {  
9   key    = "ssh-keys"  
10  value  = "${var.gce_ssh_user}:${var.gce_ssh_pub_key}"  
11 }  
12
```

Raw Blame History

Make sure the .tf file extension is added to the file. The following screenshot shows the mac save as dialogue box where the extension needs to be added and the Format needs to be changed to All Files:



- Return to the repository and follow the previous steps to download the Variables.tf file to the same location as the Main.tf:

PaloAltoNetworks / GCP-k8s-Prisma-Cloud-API [Private] Watch 0 Star 0 Fork 0

Code Issues 1 Pull requests 0 Projects 0 Wiki Security Insights Settings

Branch: master GCP-k8s-Prisma-Cloud-API / Variables.tf Find file Copy path

djspears Add files via upload 2209791 3 hours ago

1 contributor

73 lines (56 sloc) | 2.01 KB

```
1 // PROJECT Variables
2 variable "container-ver" {
3     default = "1.11.10-gke.4"
4 }
5
6 variable "my_gcp_project" {
7     default = "datacenter-2018"
```

Task 2 – Gather Information and Update the Variables.tf file

The Terraform deployment files consist of a main file and a variables file. The Variables.tf file contains information that is easily modified and commonly changed for various situations. The variables in the Variables.tf file are used by the Main.tf file during deployment. Deploying this Terraform template in GCP does require modification of the template Variable.tf file to include deployment-specific information. The fields that must be updated are shown below:

```
// PROJECT Variables
variable "container_ver" {
  default = "1.11.10-gke.4"
}

variable "my_gcp_project" {
  default = "djs-gcp-2018"
}

variable "region" {
  default = "us-central1"
}

variable "zone" {
  default = "us-central1-a"
}

variable "credentials_file_path" {
  description = "Path to the JSON file used to describe your account credentials"
  default     = "/Users/dspears/GCP/k8-test/djs-gcp-2018-creds.json"
}

variable "gce_ssh_user" {
  description = "ssh user that is used in the public key"
  default     = "dspears@SJCMAIL"
}

variable "gce_ssh_pub_key" {
  description = "ssh key in the format: ssh-rsa <key> username"
  default     = "ssh-rsa AAAABen1XXUi0Zufpq4vPM00ajTggypJ7SRCg0YJxcdx4cr9ASNei5L0FqAixJD0+0izXfQEUm0/T dspears@SJCMAIL"

//The rest of the variables do not need to be modified for the K8s Lab
// VM-Series Firewall Variables

variable "firewall_name" {
  default = "firewall"
}

variable "image_fw" {
  default = "https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/global/images/vmseries-bundle1-810"
}

//default = "https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public/global/images/vmseries-byol-810"
}
```

A description of the fields that need to be updated are:

Container-ver This is the K8s Master version. Google updates versions often so it is likely that the version is no longer available.

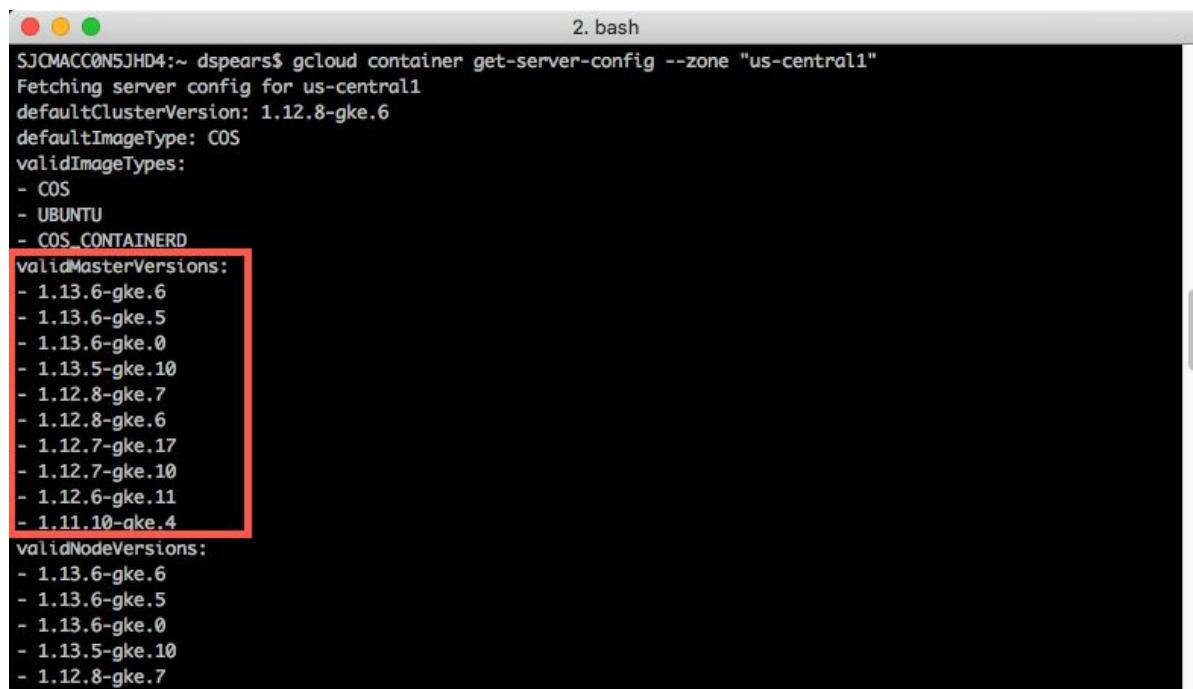
Project ID is the id that is associated with the GCP project that was created previously.

Credential file path is the path to the JSON file that has service credentials that will be used to deploy the template.

SSH User and SSH Pub Key are the SSH keys that can be used to access VM resources in the environment. In this lab the Firewall will be bootstrapped from an existing public GCP bucket. However, if that process fails, this SSH user can be used to access the firewall CLI.

- To validate the master k8s version run the following command:

```
gcloud container get-server-config --zone "us-central1"
```



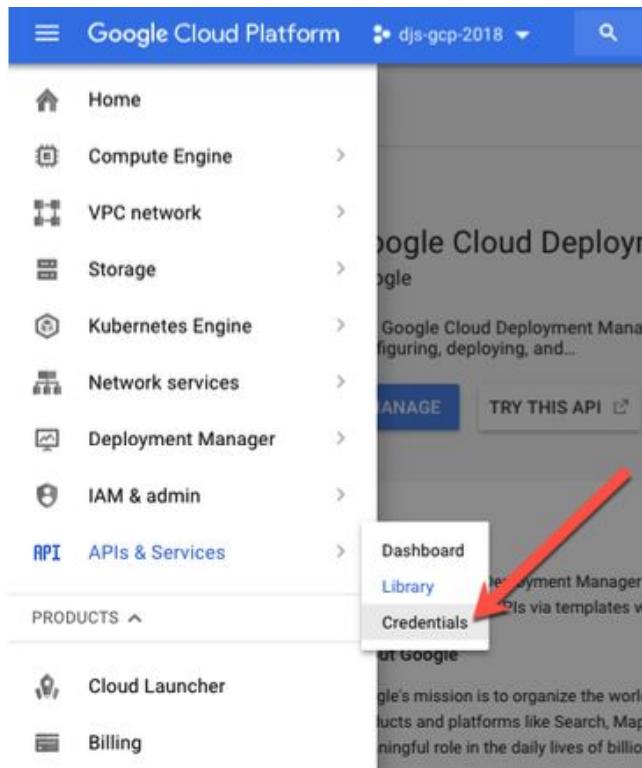
A terminal window titled '2. bash' showing the output of the command 'gcloud container get-server-config --zone "us-central1"'. The output includes server configuration details like defaultClusterVersion (1.12.8-gke.6) and defaultImageType (COS), followed by lists of validImageTypes (COS, UBUNTU, COS_CONTAINERD) and validMasterVersions (1.13.6-gke.6, 1.13.6-gke.5, 1.13.6-gke.0, 1.13.5-gke.10, 1.12.8-gke.7, 1.12.8-gke.6, 1.12.7-gke.17, 1.12.7-gke.10, 1.12.6-gke.11, 1.11.10-gke.4). A red box highlights the 'validMasterVersions' section.

```
SJOMACCON5JHD4:~ dspears$ gcloud container get-server-config --zone "us-central1"
Fetching server config for us-central1
defaultClusterVersion: 1.12.8-gke.6
defaultImageType: COS
validImageTypes:
- COS
- UBUNTU
- COS_CONTAINERD
validMasterVersions:
- 1.13.6-gke.6
- 1.13.6-gke.5
- 1.13.6-gke.0
- 1.13.5-gke.10
- 1.12.8-gke.7
- 1.12.8-gke.6
- 1.12.7-gke.17
- 1.12.7-gke.10
- 1.12.6-gke.11
- 1.11.10-gke.4
validNodeVersions:
- 1.13.6-gke.6
- 1.13.6-gke.5
- 1.13.6-gke.0
- 1.13.5-gke.10
- 1.12.8-gke.7
```

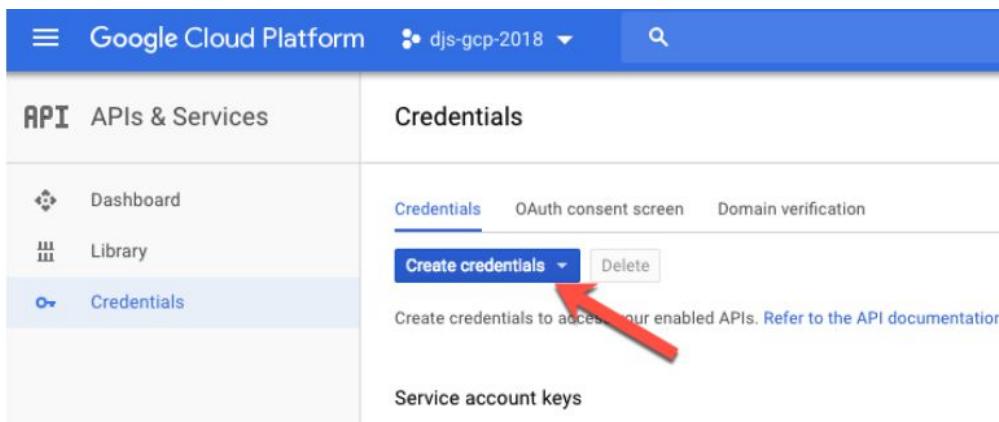
- Make sure a valid Master Version listed in the output is in the variables.tf file:

```
variable "container-ver" {
  default = "1.11.10-gke.4"
}
```

→ To create the credentials to access the APIs in JSON format. In GCP console go to (APIs & Services > Credentials:



→ Click Create Credentials:



→ Then select Service Account Key:

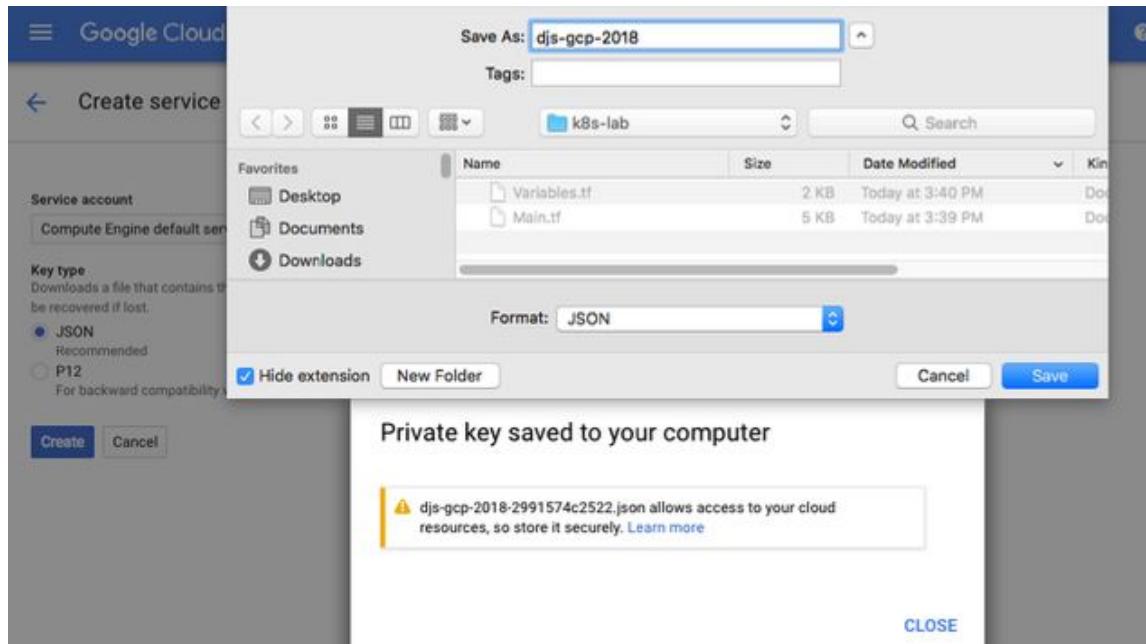
The screenshot shows the Google Cloud Platform interface. In the top navigation bar, it says "Google Cloud Platform" and "djs-gcp-2018". Below the navigation bar, there's a sidebar with "APIs & Services" and three options: "Dashboard", "Library", and "Credentials". The "Credentials" option is selected and highlighted in blue. The main content area is titled "Credentials" and has three tabs: "Credentials", "OAuth consent screen", and "Domain verification". A "Create credentials" button is visible. A dropdown menu is open over this button, containing four items: "API key", "OAuth client ID", "Service account key", and "Help me choose". A red arrow points from the text "Enables server-to-server, app-level authentication using robot accounts" towards the "Service account key" item.

→ Pick Compute Engine default service account and make sure the JSON format is ticked.
Click Create:

[←](#) Create service account key

The screenshot shows a dialog box titled "Create service account key". It has a "Service account" section with a dropdown menu showing "Compute Engine default service account" (which has a red arrow pointing to it) and "New service account". Below the dropdown is a note about recovering lost keys. There are two radio button options: "JSON" (selected) and "P12". The "JSON" option is described as "Recommended". The "P12" option is described as "For backward compatibility with code using the P12 format". At the bottom of the dialog are "Create" and "Cancel" buttons.

- Download the file to your computer. It is easy to put the credential file in the same folder as the terraform Main.tf and Variables.tf files:



- Use an editor of your choice to update the Variables.tf file with the appropriate path:

```
1 // PROJECT Variables
2 variable "my_gcp_project" {
3     default = "Your_Project_ID"
4 }
5
6 variable "region" {
7     default = "us-central1"
8 }
9
10 variable "zone" {
11     default = "us-central1-a"
12 }
13
14 variable "credentials_file_path" {
15     description = "Path to the JSON file used to describe your service account credentials"
16     default      = "/GCP/k8s-lab/djs-gcp-2018.json"
17 }
```

- If you do not already have an SSH key, the following example shows how to create a SSH key on a Mac using the ssh-keygen -t rsa command:

```

SJCMAC3024G8WL:k8s-lab dspears$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/dspears/.ssh/id_rsa): /GCP/k8s-lab/djs-gcp-key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /GCP/k8s-lab/djs-gcp-key.
Your public key has been saved in /GCP/k8s-lab/djs-gcp-key.pub.
The key fingerprint is:
SHA256:MbToaffF6JcWLsWt8+3QoUH6PomeK4ml0abailFOVDTA dspears@SJCMAC3024G8WL
The key's randomart image is:
+---[RSA 2048]---+
|   E.. .
|   . +o .
|   .o=.=
|   .B B o
|   .= B S
| .o* + = +
| .++ = = = o
|oooo+ oo* .
|=+=o o+...
+---[SHA256]---+
SJCMAC3024G8WL:k8s-lab dspears$ ls -la

```

In the previous example the keys were generated and stored in the same directory as the other lab files. The public and private keys can be seen using the ls -la command. I have also displayed the public key via the more command in the following screenshot:

```

SJCMAC3024G8WL:k8s-lab dspears$ ls -la
total 48
drwxr-xr-x@ 7 dspears  wheel          224 Jun 13 16:21 .
drwxr-xr-x  28 dspears  wheel          896 Jun 13 15:08 ..
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  5345 Jun 13 15:39 Main.tf
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  1560 Jun 13 16:11 Variables.tf
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  2328 Jun 13 16:08 djs-gcp-2018.json
-rw-----   1 dspears  wheel          1679 Jun 13 16:21 djs-gcp-key
-rw-r--r--   1 dspears  wheel          404 Jun 13 16:21 djs-gcp-key.pub
SJCMAC3024G8WL:k8s-lab dspears$ more djs-gcp-key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQJC9RA/kjVZ7pUrh4oMHLJP1jDeMc3pk0UCL3aQ9jthYJm/uWiVjLZ3NEjiHTfQQITt
kbWQkfCcWHhnQ9E9vtLkkiutpqT3wfm1nUeSA0rcTSFGMCB0tqVJds/u/KIAxYpS5I2Z/GYk1qcT9oXHSf/mrfq1w+9aIX9Hsaa3rY
NIEJA42T/00LnH1LzMa268L9aEMEIXoKrx9d9BMhv/RjhdIwuWqMiq0+x/KvPTrPNhK6sq/5UbWZbnvvccjyS1xAF2a0rW9rwQ3vh6m
sQZjwVU0m41vqHqRTNJQKmEUyv8P5oaeU57ed0AtuLMpCoNpb9015m912h7PAaCnugeJ/ dspears@SJCMAC3024G8WL
djs-gcp-key.pub (END)

```

→ Retrieve the username and key from the public key file. Then update the Variables.tf file:

```
// PROJECT Variables
variable "my_gcp_project" {
  default = "djs-gcp-2018"
}

variable "region" {
  default = "us-central1"
}

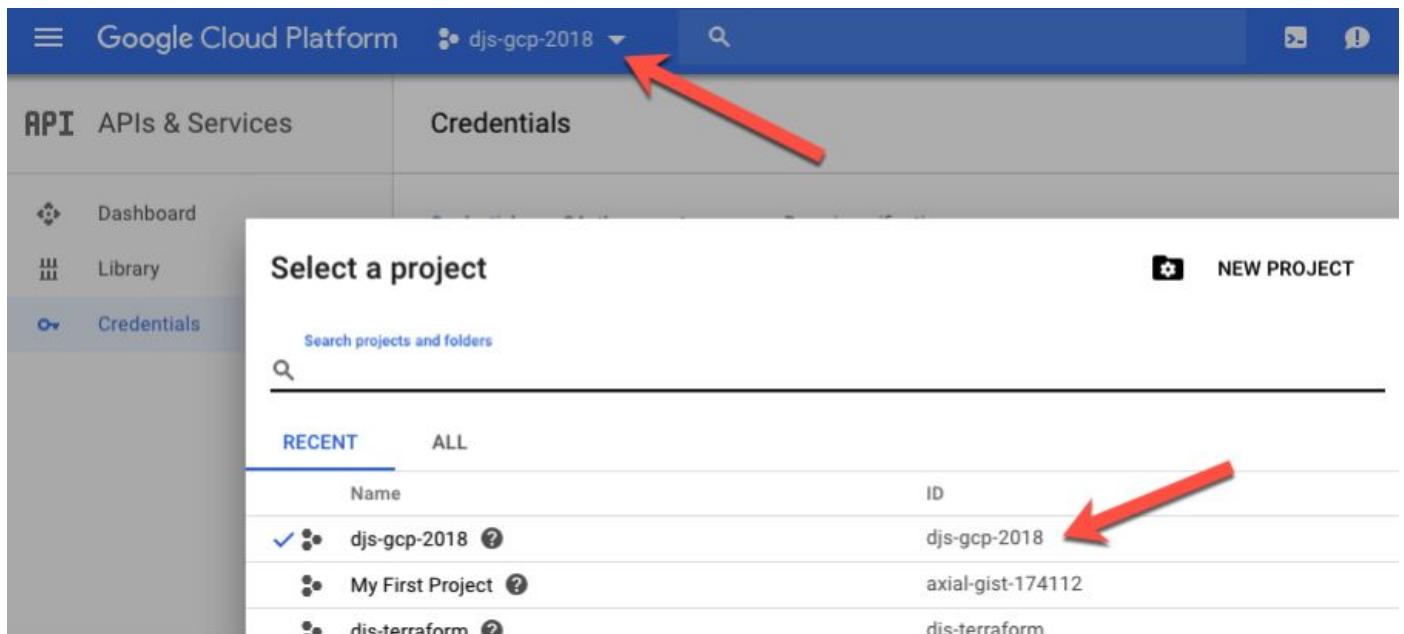
variable "zone" {
  default = "us-central1-a"
}

variable "credentials_file_path" {
  description = "Path to the JSON file used to describe your account credentials"
  default     = "/GCP/k8s-lab/djs-gcp-2018.json"
}

variable "gce_ssh_user" {
  description = "ssh user that is used in the public key"
  default     = "dspears$JOMAC3024G8WL"
}

variable "gce_ssh_pub_key" {
  description = "ssh key in the format: ssh-rsa <key> username"
  default     = "ssh-rsa AAAAB3NzaC1yc2EAAQABAAQc9RA/kjVZ7pUrh4oMHLJP1jDeMc3pk0UCL3aQ9jthYJm/uWlVjLZ3NEjiHTFQQITtkbWQkFcCWhhnQ9E9vtLkkiutpqT3wfm1nUe5A0rcTSFGMCB0taVJds/u/KIAxYpSSIZZ/GYk1qcT9oXHSf/mr
// The rest of the variables do not need to be modified for the K8s Lab
// VM-Series Firewall Variables
```

→ To get the GCP Project ID click the project selection drop down at the top of the GCP Console. The Project ID is displayed in the project selection window:



→ Update the Variables.tf file with the GCP ID:

```
// PROJECT Variables
variable "my_gcp_project" {
  default = "djs-gcp-2018"
}

variable "region" {
  default = "us-central1"
}

variable "zone" {
  default = "us-central1-a"
}

variable "credentials_file_path" {
  description = "Path to the JSON file used to describe your account credentials"
  default      = "/GCP/k8s-lab/djs-gcp-2018.json"
}

variable "gce_ssh_user" {
  description = " ssh user that is used in the public key"
  default     = "dspears@SJCMAC3024G8WL"
}

variable "gce_ssh_pub_key" {
  description = " ssh key in the format: ssh-rsa <key> username "
  default     = "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQC9RA/kjVZ7pUrh4oMHLJP1jDeMc3pk0UCL3aQ9jthYJm/uWiVjLZ3NEjiHTfQQITtkbWQkfCcWWhnQ9E9vtLkkiwutpqT3wf
// The rest of the variables do not need to be modified for the K8s Lab
// VM-Series Firewall Variables
```



End of Activity 2

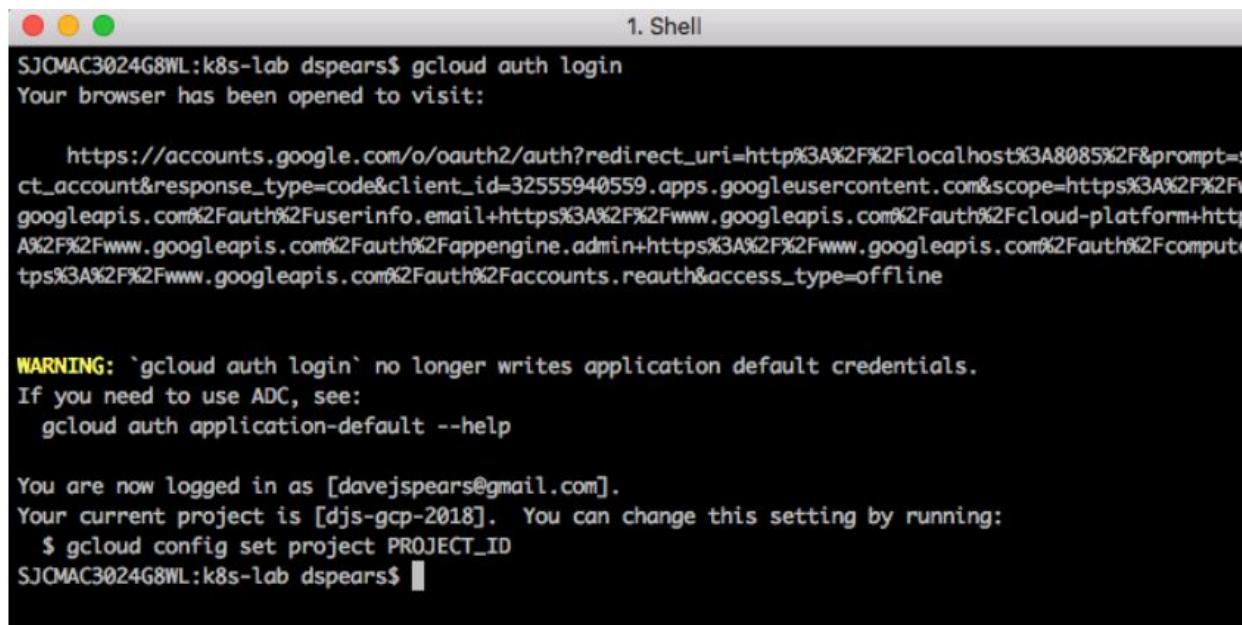
Activity 3 – Deploy the Terraform Template

In this activity, you will:

- **Authenticate Google Cloud SDK**
 - **Initialize and deploy the terraform template**
-

Task 1 – Authenticate Google Cloud SDK

- Open a terminal shell and navigate to the directory containing the Terraform template files. Authenticate to the GCP environment from the command line with the command: gcloud auth login
- Copy/paste the link into a browser(if needed) and select the account to authenticate if a browser does not automatically launch:



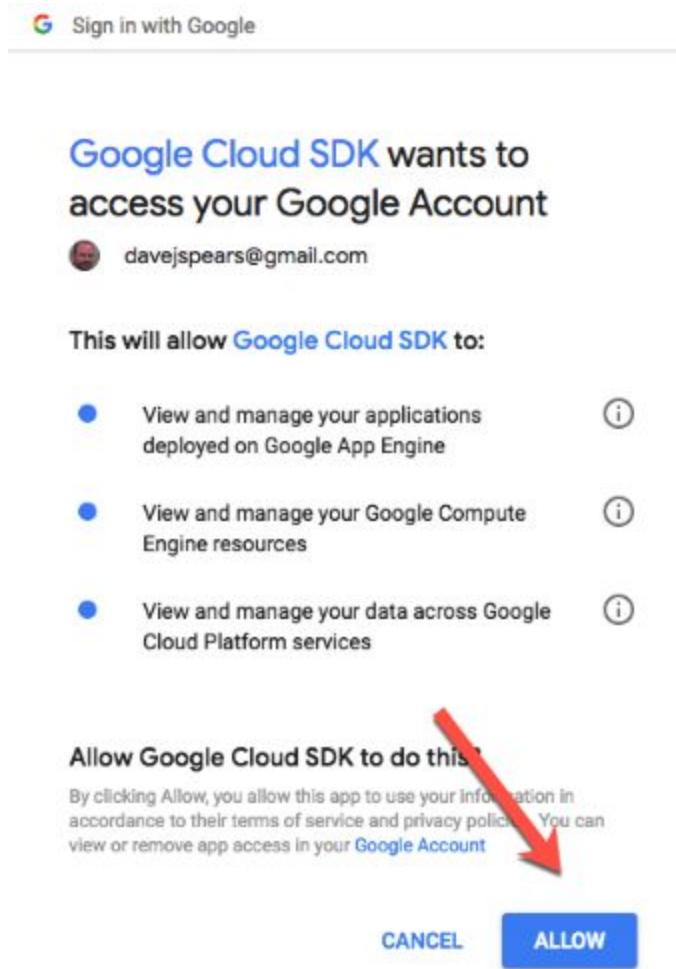
```
SJ0MAC3024G8WL:k8s-lab dspears$ gcloud auth login
Your browser has been opened to visit:

https://accounts.google.com/o/oauth2/auth?redirect_uri=http%3A%2F%2Flocalhost%3A8085%2F&prompt=s
ct_account&response_type=code&client_id=32555940559.apps.googleusercontent.com&scope=https%3A%2F%2Fw
googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+http
A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute
tps%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&access_type=offline

WARNING: `gcloud auth login` no longer writes application default credentials.
If you need to use ADC, see:
  gcloud auth application-default --help

You are now logged in as [davejspears@gmail.com].
Your current project is [djs-gcp-2018]. You can change this setting by running:
  $ gcloud config set project PROJECT_ID
SJ0MAC3024G8WL:k8s-lab dspears$
```

→ Review the requested permissions and click Allow:



→ Note the Project ID. If it is not the project that was created for the lab, use the **\$ gcloud config set project my_Project_id** command to change the project:

The screenshot shows a terminal window titled "1. Shell". It displays the command "gcloud config set project djs-gcp-2018" being run, followed by the message "Updated property [core/project].". The terminal prompt "SJC_MAC3024G8WL:k8s-lab dspears\$" is visible at the bottom.

```
SJC_MAC3024G8WL:k8s-lab dspears$ gcloud config set project djs-gcp-2018
Updated property [core/project].
SJC_MAC3024G8WL:k8s-lab dspears$
```

Task 2 – Deploy the Terraform Template

- Ensure you are in the directory with the Main.tf and Variables.tf files and execute the **terraform init** command which will initialize terraform:

```
1. Shell
SJ0MAC3024G8WL:k8s-lab dspears$ ls -la
total 136
drwxr-xr-x@ 10 dspears  wheel          320 Jun 13 18:40 .
drwxr-xr-x  28 dspears  wheel          896 Jun 13 15:08 ..
drwxr-xr-x   3 dspears  wheel          96 Jun 13 17:04 .terraform
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  5345 Jun 13 15:39 Main.tf
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  1857 Jun 13 17:54 Variables.tf
-rw-r--r--@  1 dspears  PALOALTONETWORK\Domain Users  2328 Jun 13 16:08 djs-gcp-2018.json
-rw-----   1 dspears  wheel          1679 Jun 13 16:21 djs-gcp-key
-rw-r--r--   1 dspears  wheel          404 Jun 13 16:21 djs-gcp-key.pub
-rw-r--r--   1 dspears  wheel          1793 Jun 13 18:40 terraform.tfstate
-rw-r--r--   1 dspears  wheel          38305 Jun 13 18:36 terraform.tfstate.backup
SJ0MAC3024G8WL:k8s-lab dspears$ terraform init

Initializing provider plugins...

The following providers do not have any version constraints in configuration,
so the latest version was installed.

To prevent automatic upgrades to new major versions that may contain breaking
changes, it is recommended to add version = "..." constraints to the
corresponding provider blocks in configuration, with the constraint strings
suggested below.

* provider.google: version = "~> 1.14"

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
SJ0MAC3024G8WL:k8s-lab dspears$ 
```

Once the terraform init has completed run the **terraform plan** command. This will show what changes will be implemented with the terraform script. This will also identify if there are any errors detected with the terraform files:

```
1. bash
id: <computed>
cluster: "cluster-1"
initial_node_count: <computed>
instance_group_urls.#: <computed>
management.#: <computed>
max_pods_per_node: <computed>
name: "1"
name_prefix: <computed>
node_config.#: <computed>
node_config.0.disk_size_gb: "32"
node_config.0.disk_type: <computed>
node_config.0.guest_accelerator.#: <computed>
node_config.0.image_type: "COS"
node_config.0.labels.%: "2"
node_config.0.labels.cluster: "the-cluster"
node_config.0.labels.pool: "db-pool"
node_config.0.local_ssd_count: <computed>
node_config.0.machine_type: "n1-standard-1"
node_config.0.oauth_scopes.#: "6"
node_config.0.oauth_scopes.1277378754: "https://www.googleapis.com/auth/monitoring"
node_config.0.oauth_scopes.1632638332: "https://www.googleapis.com/auth/devstorage.read_only"
node_config.0.oauth_scopes.172152165: "https://www.googleapis.com/auth/logging.write"
node_config.0.oauth_scopes.316356861: "https://www.googleapis.com/auth/service.management.readonly"
node_config.0.oauth_scopes.3663490875: "https://www.googleapis.com/auth/servicecontrol"
node_config.0.oauth_scopes.3859019814: "https://www.googleapis.com/auth/trace.append"
node_config.0.preemptible: "false"
node_config.0.service_account: <computed>
node_config.0.tags.#: "3"
node_config.0.tags.0: "the-cluster"
node_config.0.tags.1: "gke-node"
node_config.0.tags.2: "db-tier"
node_count: "2"
project: <computed>
region: "us-central1-a"
version: <computed>
zone: <computed>

Plan: 19 to add, 0 to change, 0 to destroy.

-----
Note: You didn't specify an "-out" parameter to save this plan, so Terraform
can't guarantee that exactly these actions will be performed if
"terraform apply" is subsequently run.

SJC0MACC0@NSJHD4:k8-EW-pods dspears$
```

→ Now run the **terraform apply** command to deploy the template. At the action prompt enter **yes**.

```
SJC0MACC0@NSJHD4:k8-EW-pods dspears$ terraform apply
google_compute_network.trust: Refreshing state... (ID: trust)

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

+ google_compute_firewall.allow-inbound
  + id: "1"
  + allow.#: "2"
  + allow.186047796.ports.#: "89"
  + allow.186047796.ports.0: "22"
  + allow.186047796.ports.1: "tcp"
  + allow.186047796.protocol: <computed>
  + destination_ranges.#: <computed>
  + direction: "allow-inbound"
  + name: "${google_compute_network.untrust.self_link}"
  + network: <computed>
  + priority: "1000"
  + project: <computed>
  + self_link: <computed>
  + source_ranges.#: "1"
  + source_ranges.1880289494: "0.0.0.0/0"

  node_config.0.image_type: "ubuntu"
  node_config.0.labels.%: "2"
  node_config.0.labels.cluster: "the-cluster"
  node_config.0.labels.pool: "default-pool"
  node_config.0.local_ssd_count: <computed>
  node_config.0.machine_type: "n1-standard-1"
  node_config.0.oauth_scopes.#: "1"
  node_config.0.oauth_scopes.1277378754: "https://www.googleapis.com/auth/moni

  node_config.0.preemptible: "false"
  node_config.0.service_account: <computed>
  node_pool.#: <computed>
  node_version: <computed>
  private_cluster: "false"
  project: <computed>
  region: "us-central1-a"
  subnetwork: "${google_compute_subnetwork.trust-self_link}"
  zone: <computed>

Plan: 12 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.

Enter a value: yes
```

It will take a few minutes to complete. If all goes well, Terraform will output; “Apply Complete!” and provide some additional output information about the resources deployed:

```
1. bash
google_container_node_pool.db_nodes: Still creating... (1m30s elapsed)
google_container_node_pool.db_nodes: Still creating... (1m40s elapsed)
google_container_node_pool.db_nodes: Still creating... (1m50s elapsed)
google_container_node_pool.db_nodes: Still creating... (2m0s elapsed)
google_container_node_pool.db_nodes: Still creating... (2m10s elapsed)
google_container_node_pool.db_nodes: Still creating... (2m20s elapsed)
google_container_node_pool.db_nodes: Creation complete after 2m27s (ID: us-central1-a/cluster-1/db-node-pool)
google_compute_route.k8mgmt: Creating...
dest_range:    "" => "35.188.144.123/32"
name:          "" => "cluster-endpoint-route"
network:       "" => "https://www.googleapis.com/compute/v1/projects/djs-gcp-2018/global/networks/trust"
next_hop_gateway: "" => "default-internet-gateway"
next_hop_network: "" => "<computed>"
priority:      "" => "100"
project:       "" => "<computed>"
self_link:     "" => "<computed>"
google_compute_route.trust: Creating...
dest_range:    "" => "0.0.0.0/0"
name:          "" => "trust-route"
network:       "" => "https://www.googleapis.com/compute/v1/projects/djs-gcp-2018/global/networks/trust"
next_hop_instance: "" => "firewall-1"
next_hop_instance_zone: "" => "us-central1-a"
next_hop_network: "" => "<computed>"
priority:      "" => "100"
project:       "" => "<computed>"
self_link:     "" => "<computed>"
google_compute_route.k8mgmt: Creation complete after 8s (ID: cluster-endpoint-route)
google_compute_route.trust: Still creating... (10s elapsed)
google_compute_route.trust: Still creating... (20s elapsed)
google_compute_route.trust: Creation complete after 26s (ID: trust-route)

Apply complete! Resources: 19 added, 0 changed, 0 destroyed.

Outputs:
k8s-cluster-endpoint = [
  35.188.144.123
]
k8s-cluster-name = [
  cluster-1
]
k8s-cluster_ipv4_cidr = [
  10.16.0.0/14
]
pan-tf-name = [
  firewall-1
]
```

End of Activity 3

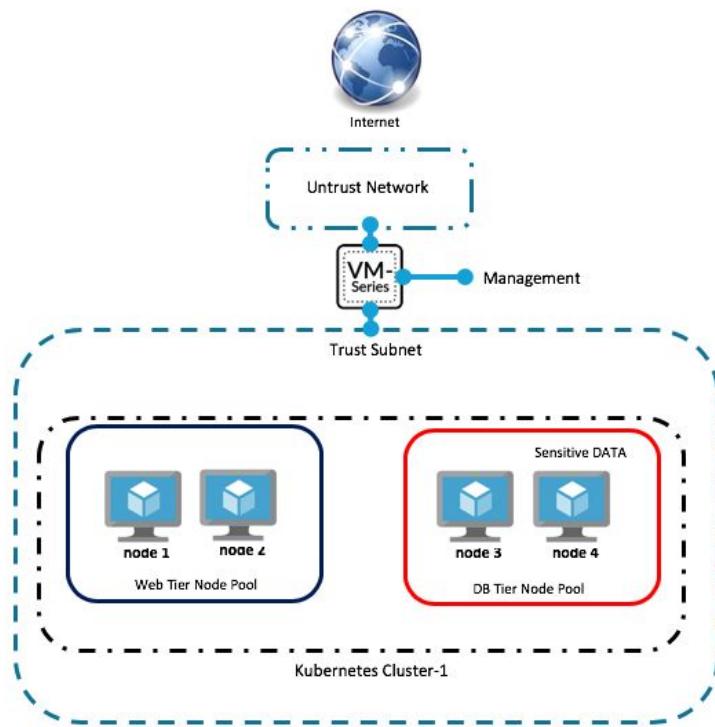
Activity 4 – Review what was deployed

In this activity, you will:

- **Review the resources that have been launched**
- **Log into the VM-Series firewall**
- **Confirm bootstrap success and firewall licensing**

Task 1 – Understand what has been initially deployed

During the lab environment creation a number of things have been deployed automatically. The following diagram shows the initial lab deployment:

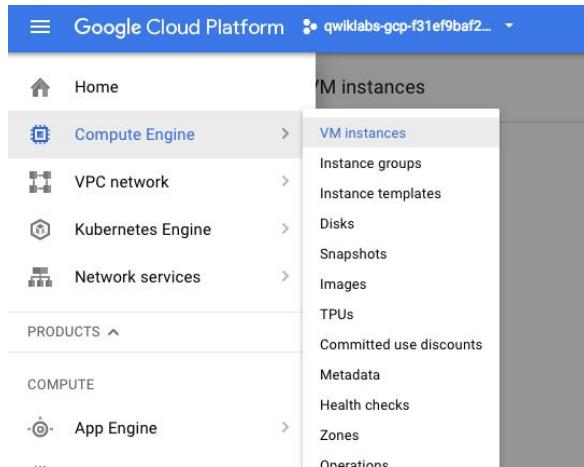


Some things to Note:

- A VM-Series Firewall has been bootstrapped with an initial configuration
- A K8s cluster has been created with 4 nodes in two separate node pools
- The VM-Series will be used for both North/South and East/West Inspection.

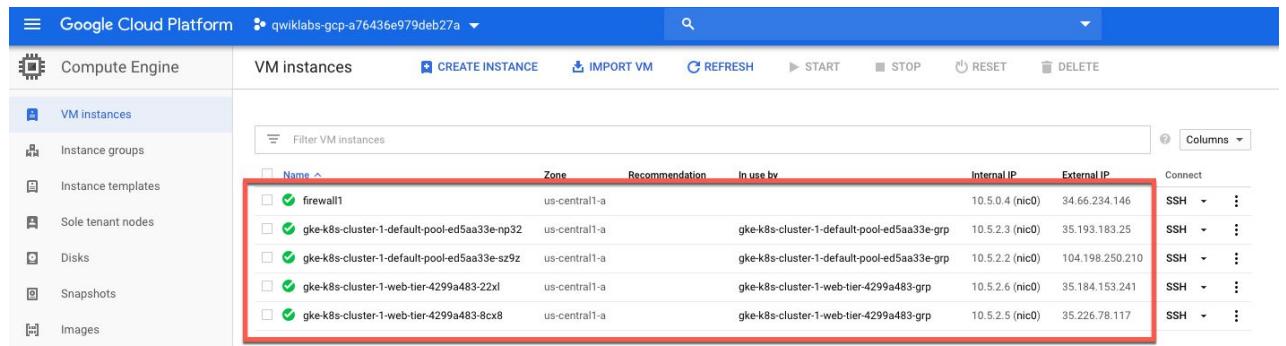
Task 2 – Look around GCP console

- Navigate to **Compute Engine > VM Instances** to see that VM-Series firewall has already been launched when the lab was started.



The screenshot shows the Google Cloud Platform navigation bar at the top with the project name "qwiklabs-gcp-f31ef9baf2...". Below it is a sidebar with sections like Home, Compute Engine, VPC network, Kubernetes Engine, Network services, PRODUCTS, COMPUTE, and App Engine. A dropdown menu under "Compute Engine" is open, showing options: VM instances, Instance groups, Instance templates, Disks, Snapshots, Images, TPUs, Committed use discounts, Metadata, Health checks, Zones, and Operations. The "VM instances" option is highlighted.

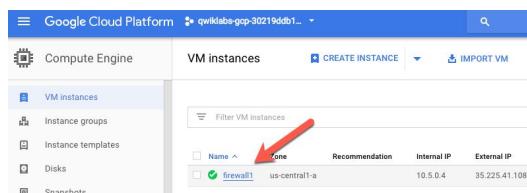
You should see a firewall and 4 nodes that were deployed as part of the k8's cluster:



The screenshot shows the "VM instances" page in the Google Cloud Platform. The left sidebar is identical to the previous one. The main area displays a table of VM instances. The first row, which is "firewall1", is highlighted with a red box. The columns in the table are Name, Zone, Recommendation, In use by, Internal IP, External IP, and Connect. The "firewall1" row has the following values: Name (firewall1), Zone (us-central1-a), Recommendation (None), In use by (None), Internal IP (10.5.0.4 (nic0)), External IP (35.225.41.108), and Connect (SSH). There are five other rows listed below it, each representing a node in the k8s cluster.

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
firewall1	us-central1-a			10.5.0.4 (nic0)	35.225.41.108	SSH
gke-k8s-cluster-1-default-pool-ed5aa33e-np32	us-central1-a		gke-k8s-cluster-1-default-pool-ed5aa33e-grp	10.5.2.3 (nic0)	35.193.183.25	SSH
gke-k8s-cluster-1-default-pool-ed5aa33e-sz92	us-central1-a		gke-k8s-cluster-1-default-pool-ed5aa33e-grp	10.5.2.2 (nic0)	104.198.250.210	SSH
gke-k8s-cluster-1-web-tier-4299a483-22xl	us-central1-a		gke-k8s-cluster-1-web-tier-4299a483-grp	10.5.2.6 (nic0)	35.184.153.241	SSH
gke-k8s-cluster-1-web-tier-4299a483-8cx8	us-central1-a		gke-k8s-cluster-1-web-tier-4299a483-grp	10.5.2.5 (nic0)	35.226.78.117	SSH

- Clicking on the **firewall1** opens a detailed view of the deployed firewall:



This screenshot is from the same "VM instances" page as the previous one. A red arrow points to the "Zone" column header, indicating it is being selected or sorted. The table shows the same data as before, with the first row "firewall1" still highlighted.

Note the **External IP Addresses** of the firewall on the firewall VM Instance details screen. These will be used later in the lab to connect the firewall and test application functionality:

The screenshot shows the 'VM instance details' page for a VM named 'firewall1'. The 'Network interfaces' table highlights the 'External IP' column, which contains three entries: '34.66.234.146 (ephemeral)', '35.225.61.208 (ephemeral)', and 'None'. A red box surrounds this column. The table also includes columns for Name, Network, Subnetwork, Primary internal IP, Alias IP ranges, Network Tier, IP forwarding, and Network details.

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	management	management-subnet	10.5.0.4	—	34.66.234.146 (ephemeral)	Premium	On	View details
nic1	untrust	untrust-subnet	10.5.1.4	—	35.225.61.208 (ephemeral)	Premium	On	View details
nic2	trust	trust-subnet	10.5.2.4	—	None	Premium	On	View details

→ Navigate to **VPC Network > VPC Networks** to see the different networks that have been created as part of the lab.

The screenshot shows the 'VPC networks' page. A dropdown menu is open over the 'VPC networks' section, listing options: 'External IP addresses', 'Firewall rules', 'Routes', 'VPC network peering', and 'Shared VPC'. The 'External IP addresses' option is highlighted.

You should see 3 non-default VPC networks: management, untrust and trust.

VPC network	VPC networks	CREATE VPC NETWORK	REFRESH
europe-west4	default	10.164.0.0/20	10.164.0.1
management	Custom		1
us-central1	management-subnet	10.5.0.0/24	10.5.0.1
trust	1	Custom	1
us-central1	trust-subnet	10.5.2.0/24	10.5.2.1
untrust	1	Custom	1
us-central1	untrust-subnet	10.5.1.0/24	10.5.1.1

- Navigate to **Kubernetes Engine > Clusters** and validate that the K8s cluster was successfully built and is running:

Kubernetes Engine	Kubernetes clusters	CREATE CLUSTER	DEPLOY	REFRESH	DELETE
A Kubernetes cluster is a managed group of VM instances for running containerized applications. Learn more					
Filter by label or name					
Kubernetes alpha clusters					
Name	Location	Cluster size	Total cores	Total memory	Master version
k8s-cluster-1	us-central1-a	4	4 vCPUs	15.00 GB	1.11.8-gke.6
Expiration time: May 25, 2019					

→ Clicking on the cluster will open a more detailed view of the k8s cluster that was deployed:

k8s-cluster-1

Cluster

- Master version: 1.11.8-gke.6
- Endpoint: 35.225.47.120
- Client certificate: Enabled
- Binary Authorization: Disabled
- Kubernetes alpha features: Enabled
- Expiration time: May 25, 2019, 9:35:03 AM
- Total size: 4
- Master zone: us-central1-a
- Node zones: us-central1-a
- Network: trust
- Subnet: trust-subnet
- VPC-native (alias IP): Disabled
- Pod address range: 10.16.0.0/14
- Intranode visibility: Disabled
- Stackdriver Logging: Enabled
- Stackdriver Monitoring: Enabled
- Private cluster: Disabled
- Master authorized networks: Disabled
- Network policy: Disabled
- Legacy authorization: Disabled
- Maintenance window: Any time
- Cloud TPU: Disabled
- Application-layer Secrets Encryption: Disabled
- Node auto-provisioning: Disabled
- Vertical Pod Autoscaling: Disabled

Labels: None

Add-ons

Permissions

Node Pools

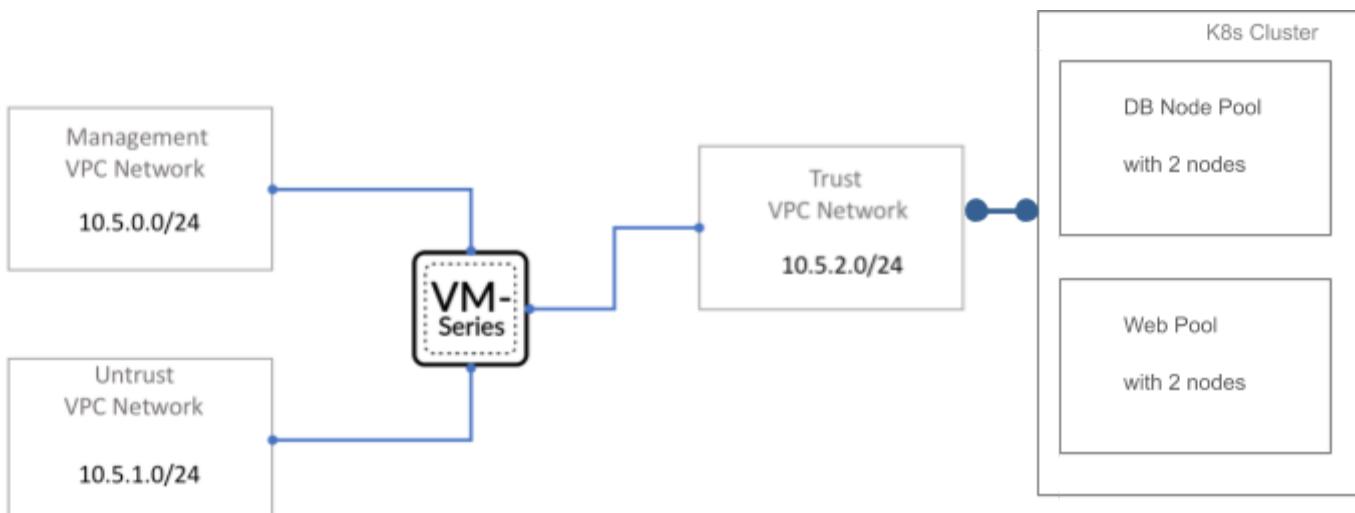
Node pools are separate instance groups running Kubernetes in a cluster. You may add node pools in different zones for higher availability, or add node pools of different type machines. To add a node pool, click Edit on the top bar. [Learn more](#)

default-pool (2 nodes, version 1.11.8-gke.6)
web-tier (2 nodes, version 1.11.8-gke.6)

Marketplace

Note: the **number of nodes (Total size)**, **node networks**, and **Pod IP address ranges** in the K8s Cluster details.

The following diagram describes the topology that has been deployed:

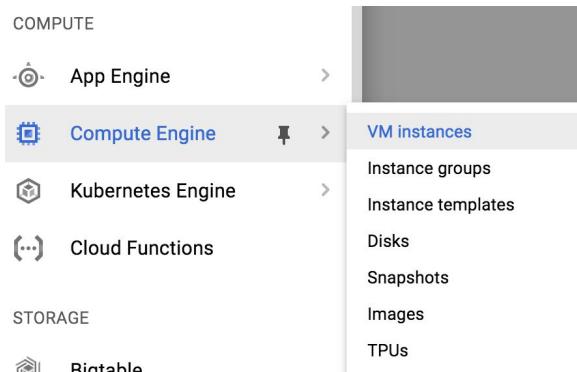


Feel free to navigate through other parts of the Google Cloud Console such as **VPC Networks > Routes, Firewall Rules**. This will come in handy in activities later on.

Task 3 – Login into the firewall

The VM-Series firewall deployed as part of the lab has been bootstrapped. Bootstrapping is a feature of the VM-Series firewall that allows you to load a predefined 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 automated deployment of the VM-Series.

- Navigate to **Compute Engine > VM Instances**



- Click on **firewall1** instance name to get more information and identify the management interface IP.

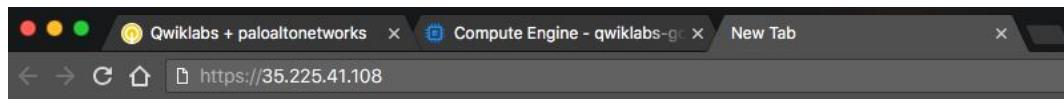
A screenshot of the Google Cloud Platform 'VM instances' page. The left sidebar shows 'Compute Engine' selected, with 'VM instances' also selected. The main area displays a table of VM instances. A red arrow points to the 'Zone' column for the 'firewall1' row, which shows 'us-central1-a'. The table includes columns for 'Name', 'Zone', 'Recommendation', 'Internal IP', and 'External IP'. The 'firewall1' row has a green checkmark next to its name.

Name	Zone	Recommendation	Internal IP	External IP
firewall1	us-central1-a		10.5.0.4	35.225.41.108

→ Copy the **External public IP** of the management interface

The screenshot shows the 'VM instance details' page for a VM named 'firewall1'. The left sidebar lists various Compute Engine options like VM instances, Instance groups, and Disks. The main pane displays the VM's configuration, including its machine type (n1-standard-4), CPU platform (Intel Sandy Bridge), zone (us-central1-a), and creation time (May 3, 2018, 9:49:47 AM). The 'Network interfaces' section shows three interfaces: 'management' (Subnet: management-subnet, IP: 10.5.0.4, External IP: 35.225.41.108), 'untrust' (Subnet: untrust-subnet, IP: 10.5.1.4, External IP: 35.226.118.220), and 'trust' (Subnet: trust-subnet, IP: 10.5.2.4, External IP: None). A red arrow points to the 'External IP' column.

→ Open another browser tab and navigate to the firewall management interface:



If you get a security exception, please ignore for this lab and proceed to the firewall login page. We are using a self-signed certificate which causes the exception. When presented with the login screen you should be able to login to the firewall using (Hint: It's a good idea to jot this password down or save it to a notepad as you will regularly need it):

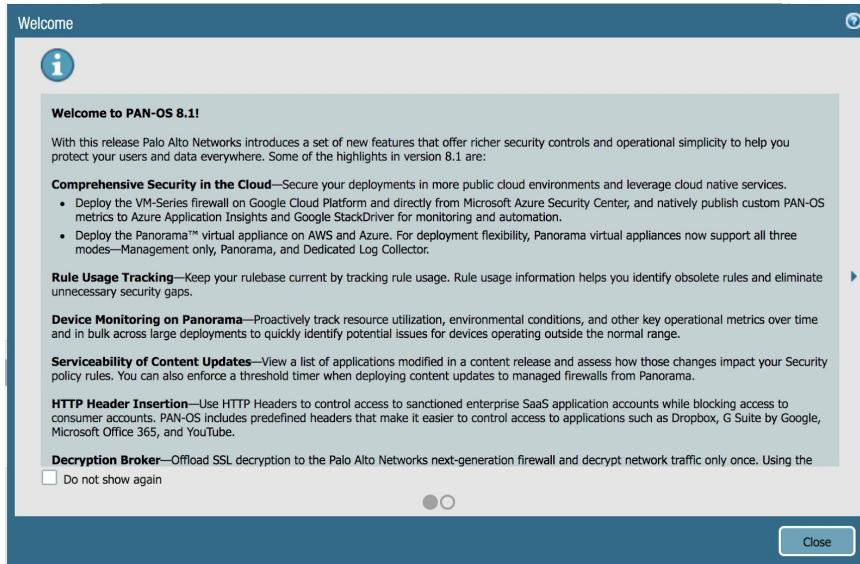
username: **admin**

password: **Pal0Alt0@123**

Note: Those are zeros not capital O's.



Once logged in you will see a **Welcome** screen, dismiss the welcome dialog box by clicking **Close**.



→ Click the **Policies** tab and you will notice a predefined security policy which was imported using the bootstrapping feature. There are also some predefined NAT policies:

The screenshot shows the Palo Alto Networks UI with the 'Policies' tab selected. On the left is a navigation sidebar with icons for Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main area displays two tables of policy rules.

Security Policies

Name	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action
1 to-guestbook-sec-pol...	universal	[p] untrust	any	any	[p] web	any	any	service-http	Allow	
2 to-wordpress-sec-pol...	universal	[p] untrust	any	any	[p] web	any	any	TCP8888	Allow	
3 EW	intrazone	[p] web	any	any	any	(intrazone)	any	dns mysql redis ssh web-browsing	any	Allow
4 Outbound-deny	universal	[p] web	any	any	[p] untrust	any	any			Deny
5 Outbound	universal	[p] web	any	any	[p] untrust	any	any			Allow
6 default-deny-all	universal	any	any	any	any	any	any			Deny
7 intrazone-default	intrazone	any	any	any	any	(intrazone)	any			Allow
8 interzone-default	intrazone	any	any	any	any	any	any			Allow

NAT Policies

Name	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action
1 to-guestbook-sec-pol...	universal	[p] untrust	any	any	[p] web	any	any	service-http	Allow	
2 to-wordpress-sec-pol...	universal	[p] untrust	any	any	[p] web	any	any	TCP8888	Allow	
3 EW	intrazone	[p] web	any	any	any	(intrazone)	any	dns mysql redis ssh web-browsing	any	Allow
4 Outbound-deny	universal	[p] web	any	any	[p] untrust	any	any			Deny
5 Outbound	universal	[p] web	any	any	[p] untrust	any	any			Allow
6 default-deny-all	universal	any	any	any	any	any	any			Deny
7 intrazone-default	intrazone	any	any	any	any	(intrazone)	any			Allow
8 interzone-default	intrazone	any	any	any	any	any	any			Allow

→ Click on the **Dashboard** tab, check to verify that the firewall has a serial number.

The screenshot shows the Palo Alto Networks Dashboard interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, and Policies, with 'Dashboard' selected. Below the navigation is a toolbar with Layout (3 Columns), Widgets, and a Last updated: 10:43 timestamp. The main area is divided into two windows: 'General Information' and 'System Resources'. The 'General Information' window displays various device details, including Device Name (k8sfwvmname), MGT IP Address (10.5.0.4 (DHCP)), MGT Netmask (255.255.255.0), MGT Default Gateway (10.5.0.1), MGT IPv6 Address (unknown), MGT IPv6 Link Local Address (fe80::4001:aff:fe05:4/64), MGT IPv6 Default Gateway (42:01:0a:05:00:04), Model (PA-VM), Serial # (unknown - highlighted with a red arrow), CPU ID (GCP-D7060200FFFFBBB1F), UUUID (E650FB87-E4A4-6529-E0A2-210F6BD425AB), VM License (none), VM Mode (GCE), Software Version (8.1.0), GlobalProtect Agent (0.0.0), Application Version (769-4439), URL Filtering Version (0000.00.00.000), GlobalProtect Clientless VPN Version (0), Time (Thu May 3 08:43:14 2018), and Uptime (0 days, 0:52:02). The 'System Resources' window shows Management CPU at 0% and Data Plane CPU at 0%, with a Session Count of 2 / 1248.

We are using the PayAsYouGo image from GCP Cloud Launcher. A license will be required to view the logs later in the lab.

End of Activity 4

Activity 5 – Container Image Scanning for Vulnerabilities

In this activity, you will:

- Scan your container images for security vulnerabilities using Prisma Public Cloud (formerly Redlock) free public APIs
 - Scan publicly available container images for security vulnerabilities
 - Patch the images
 - Push the patched image to your container registry
-

What are container images?

A container image is a lightweight, standalone, executable packaging of software which includes everything needed to run an application: code, runtime, libraries and local configuration.

Container images are made up of different layers. Every container image has a base layer (parent layer) which is usually an Operating System. The subsequent layers are built on top of it which might include language runtimes, libraries, and code (file, executables), etc.

Each of the layers are immutable and built on top of the previous layer. These layers are independent of each other. For example OpenSSL can be installed on many different base images (OS). Most of the layers are reusable such as base layer, libraries, language runtimes, which are pulled from internal or external shared repositories such as DockerHub, GitHub, npm, etc.

How are containers built?

Dockerfile:

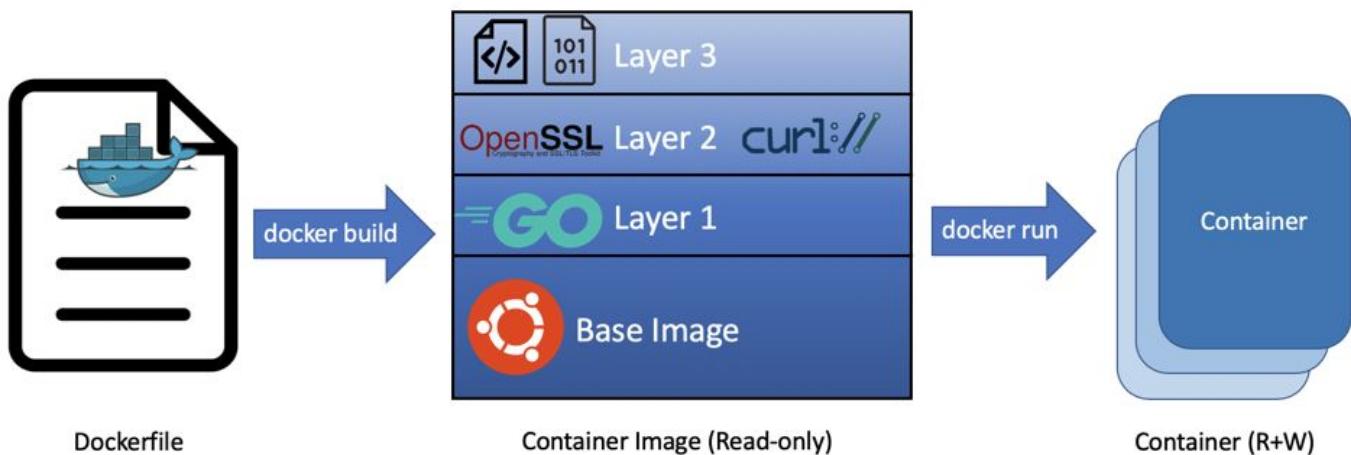
Dockerfile is the manifest with build instructions on how to build a specific container image.

Image:

Container images are read-only templates from which containers are launched. Each image contains a series of layers as explained above.

Container:

A container is a running and mutable (Read + Write) form of the image.



What does “scanning” my image mean?

Prisma Public Cloud (formerly Redlock) Image Scanning service provides free public API to scan your container images. When you “scan” an image, you are getting a list of all the vulnerabilities from all the packages and base OS installed in the image across all the layers. Each layer could contain multiple packages. The scan result will give you all the known vulnerabilities grouped by severity or package.

Task 1 – Connect to a Cloud Shell

NOTE: This is going to be done through the Kubernetes cluster so kubectl commands can be run later.

→ Click on **Kubernetes Engine > Clusters**

Setting	Value
Client certificate	Enabled
Binary Authorization	Disabled
Clusters	Enabled Jun 21, 2019, 2:20:20 PM
Workloads	4
Services	us-central1-a
Applications	us-central1-a trust
Configuration	trust-subnet
Storage	Disabled 10.16.0.0/14
Intranode visibility	Disabled
Stackdriver Logging	Enabled
Stackdriver Monitoring	Enabled
Private cluster	Disabled
Master authorized networks	Disabled

→ Click on the **Connect** button next to your cluster

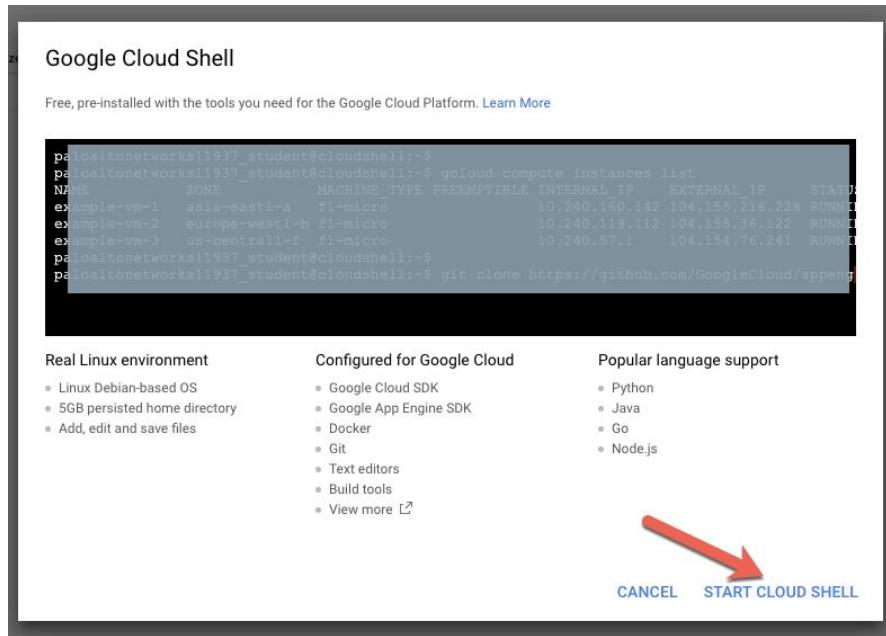
The screenshot shows the Google Cloud Platform interface for managing Kubernetes clusters. On the left, there's a sidebar with icons for Clusters, Workloads, Services, Applications, Configuration, and Storage. The main area is titled 'Kubernetes clusters' and contains a table with columns: Name, Location, Cluster size, Total cores, Total memory, Master version, Expiration time, Notifications, and Labels. One row is selected, labeled 'k8s-cluster-1'. At the bottom right of the table, there's a 'Connect' button with a red arrow pointing to it.

→ Hit **Run in Cloud Shell** in the popup window

This screenshot shows a modal dialog titled 'Connect to the cluster'. It provides two methods for connecting: 'Command-line access' and 'Cloud Console dashboard'. Under 'Command-line access', a terminal command is shown: `$ gcloud container clusters get-credentials k8s-cluster-1 --zone us-central1-a --project quickstart-gcp-c3704d48fc`. Below this is a blue 'Run in Cloud Shell' button, which has a red arrow pointing to it. The 'Cloud Console dashboard' section contains a 'Open Workloads dashboard' button. At the bottom right of the dialog is an 'OK' button.

Note: If you're doing this for the first time, you will also see the following popup window.

→ Hit **START CLOUD SHELL** in that window



→ Hit enter to execute the pre-populated command in the Cloud Shell to connect to the Kubernetes cluster

```
gcloud container clusters get-credentials k8s-cluster-1 --zone us-central1-a --project <project-id>
```



→ Open the Cloud Shell in a new tab for convenience (DO NOT CLOSE THE NEW TAB)



Task 2 – Build and Scan the Application Container Image

In this activity we will start by building our app container image, then we will scan it for security vulnerabilities.

We will build the frontend service for our Guestbook app. The Development team wrote the code, and now we are packaging the code in a container.

This is the Dockerfile, which describes what we are including in this image (base OS/image, code and code dependencies/libraries):

```
1 # Copyright 2016 The Kubernetes Authors.
2 #
3 # Licensed under the Apache License, Version 2.0 (the "License");
4 # you may not use this file except in compliance with the License.
5 # You may obtain a copy of the License at
6 #
7 #     http://www.apache.org/licenses/LICENSE-2.0
8 #
9 # Unless required by applicable law or agreed to in writing, software
10 # distributed under the License is distributed on an "AS IS" BASIS,
11 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
12 # See the License for the specific language governing permissions and
13 # limitations under the License.
14
15 FROM php:5-apache
16
17 RUN apt-get update
18 RUN pear channel-discover pear.nrk.io
19 RUN pear install nrk/Predis
20
21 # If the container's stdio is connected to systemd-journald,
22 # /proc/self/fd/{1,2} are Unix sockets and apache will not be able to open()
23 # them. Use "cat" to write directly to the already opened fds without opening
24 # them again.
25 RUN sed -i 's#ErrorLog /proc/self/fd/2#ErrorLog "|$/bin/cat 1>&2#" /etc/apache2/apache2.conf
26 RUN sed -i 's#CustomLog /proc/self/fd/1 combined#CustomLog "|/bin/cat" combined#' /etc/apache2/apache2.conf
27
28 # Add the application code to the image
29 ADD guestbook.php /var/www/html/guestbook.php
30 ADD controllers.js /var/www/html/controllers.js
31 ADD index.html /var/www/html/index.html
```

In this Dockerfile...

- We are using PHP:5-apache **base image** for our frontend app container (line 15)
https://hub.docker.com/_/php
- Installing and updating **dependencies** (line 17-19)
- Adding the frontend **app code**, PHP, JavaScript, and HTML to the image (line 29-31)

Now, let's build and scan this image.

- Download the lab repo in Cloud Shell by running below cmd:

```
git clone https://github.com/PaloAltoNetworks/ignite2019-how14.git
```

```
paloaltonetworks11946 student@cloudshell:~ (qwiklabs-gcp-161afff642864f2c)$ git clone https://github.com/PaloAltoNetworks/ignite2019-how14.git
Cloning into 'ignite2019-how14'...
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 23 (delta 5), reused 20 (delta 5), pack-reused 0
Unpacking objects: 100% (23/23), done.
paloaltonetworks11946 student@cloudshell:~ (qwiklabs-gcp-161afff642864f2c)$ ls
ignite2019-how14 README-cloudshell.txt
```

- Access the directory with the Dockerfile by running the following command:

```
cd ignite2019-how14/code
```

```
paloaltonetworks11946_student@cloudshell:~ (qwiklabs-gcp-161afff642864f2c)$ cd ignite2019-how14/code/
paloaltonetworks11946_student@cloudshell:~/ignite2019-how14/code (qwiklabs-gcp-161afff642864f2c)$ ls
controllers.js Dockerfile Dockerfile.withScanning guestbook.php index.html Makefile
```

- Edit the Dockerfile to add Prisma Public Cloud image scanning API call

- Open the Dockerfile in your favorite editor

nano Dockerfile

- Go to the end of the file and append the following two lines at the end

ARG rl_args

```
RUN SCAN_CMD=$(eval "curl https://vscanapidoc.redlock.io/scan.sh 2>/dev/null") && echo
"$SCAN_CMD" | sh
```

- Save and exit

Press **Ctrl + o** to save and then **Ctrl + x** to exit

After making the changes Dockerfile should look like this:

```
paloaltonetworks11946_student@cloudshell:~/ignite2019-how14/code (qwiklabs-gcp-161afff642864f2c)$ tail Dockerfile
# them. Use "cat" to write directly to the already opened fds without opening
# them again.
RUN sed -i 's#ErrorLog /proc/self/fd/2#ErrorLog "|$/bin/cat 1>\&2"#' /etc/apache2/apache2.conf
RUN sed -i 's#CustomLog /proc/self/fd/1 combined#CustomLog "|/bin/cat" combined#' /etc/apache2/apache2.conf

ADD guestbook.php /var/www/html/guestbook.php
ADD controllers.js /var/www/html/controllers.js
ADD index.html /var/www/html/index.html
ARG rl_args
RUN SCAN_CMD=$(eval "curl https://vscanapidoc.redlock.io/scan.sh 2>/dev/null") && echo "$SCAN_CMD" | sh
```

What we're doing here by adding the r1_args and SCAN_CMD is, we are listing all the packages installed in this image and getting the list of all the vulnerabilities associated with those packages from the **Prisma Public Cloud free public image scanning API**. The **Prisma Public Cloud** Infrastructure as Code Scanner will provide a pass/fail for the build based on the list of vulnerabilities we get back.

ARG r1_args is for passing the build arguments to configure when to pass/fail the build and how to group/see the scan result. See <https://vscanapidoc.redlock.io/> for more information.

Note: For your convenience, we have placed the final Dockerfile as `Dockerfile.withScanning` in the `ignite2019-how14/code` folder.

→ You can copy that one using the following command:

cp Dockerfile.withScanning Dockerfile

→ Build the Docker image using the following command. This will make the actual API call during the build and display the scan result.

docker build -t gb-frontend:v4 . -f ./Dockerfile

```
gpatel@cloudshell:~/examples/guestbook/php-redis (cps-containers-dev)$ docker build -t gb-frontend:v4 -f ./Dockerfile .
Sending build context to Docker daemon 11.26kB
Step 1/10 : FROM php:5-apache
--> 24c79195c1e
Step 2/10 : RUN apt-get update
--> Using cache
--> 786a33637fffc
Step 3/10 : RUN pear channel-discover pear.nrk.io
--> Using cache
--> f48f92067a15
Step 4/10 : RUN pear install nrk/Predis
--> Using cache
--> lc00a07d5aa
Step 5/10 : RUN sed -i 's#${ErrorLog} /proc/self/fd/2#${ErrorLog} "|$bin/cat 1>\&2"##' /etc/apache2/apache2.conf
--> Using cache
--> 1dbbebl114be
Step 6/10 : RUN sed -i 's#${CustomLog} /proc/self/fd/1 combined#${CustomLog} "|$bin/cat" combined##' /etc/apache2/apache2.conf
--> Using cache
--> 7d910a6b7a9c
Step 7/10 : ADD guestbook.php /var/www/html/guestbook.php
--> 4604211d0230
Step 8/10 : ADD controllers.js /var/www/html/controllers.js
--> cfe1bec97983
Step 9/10 : ADD index.html /var/www/html/index.html
--> 53be33fd4ee8
Step 10/10 : RUN SCAN_CMD=$(eval "curl https://vscanapidoc.redlock.io/scan.sh 2>/dev/null") && echo "$SCAN_CMD" | sh
--> Running in 9bdf91997513

{
  "Report": {
    "Summary": {
      "high_cve_count": 35, ←
      "medium_cve_count": 234, ←
      "low_cve_count": 97, ←
      "unknown_cve_count": 6, ←
      "total_cve_count": 372, ←
      "total_packages_count": 100, ←
      "failure_reason": "threshold_exceeded"
    }
  }
}
The command '/bin/sh -c SCAN_CMD=$(eval "curl https://vscanapidoc.redlock.io/scan.sh 2>/dev/null") && echo "$SCAN_CMD" | sh' returned a non-zero code: 1
gpatel@cloudshell:~/examples/guestbook/php-redis (cps-containers-dev)$
```

→ Next, analyze the completed results and take note of the following:

- Notice the docker build failing with a non-zero exit code
- It fails because the vulnerability scan result received from the Prisma Public Cloud image scan API endpoint indicate more than one packages have known vulnerabilities
- Notice that the final image would have had 38 high severity CVEs, 248 medium and 102 low severity CVEs, totaling 394 CVEs.

Note: Your results may be different as new CVEs are being identified.

- The number of packages analyzed are 100
- Failure reason is the number of CVEs exceeded the threshold (by default 1)

→ Next, get the list of CVEs grouped by the packages by passing the

--build-arg rl_args="report=detail;group_by=package"

argument to the docker build command

```
docker build -t gb-frontend:v4 . -f ./Dockerfile --build-arg  
rl_args="report=detail;group_by=package"
```

```
gpateel@cloudshell:~/examples/guestbook/php-redis (cps-containers-dev)$ docker build -t gb-frontend:v4 -f ./Dockerfile --build-arg rl_args="report=detail;group_by=package" .  
Sending build context to Docker daemon 11.26kB  
Step 1/11 : FROM php:5.6-apache  
--> 5c79195e0a46  
Step 2/11 : RUN apt-get update  
--> Using cache  
--> b515af831346  
Step 3/11 : RUN pear channel-discover pear.nrk.io  
--> Using cache  
--> 7b0b55fbcd  
Step 4/11 : RUN pear install nrk/Redis  
--> Using cache  
--> 7ac8167b4d6a  
Step 5/11 : RUN sed -i '$#ErrorLog /proc/self/fd/2#ErrorLog "|$bin/cat 1>\$2"' /etc/apache2/apache2.conf  
--> Using cache  
--> d95ea97c42f9  
Step 6/11 : RUN sed -i '$#CustomLog /proc/self/fd/1 combined#CustomLog "|$bin/cat" combined#' /etc/apache2/apache2.conf  
--> Using cache  
--> c256c2ff0e  
Step 7/11 : ADD guestbook.php /var/www/html/guestbook.php  
--> Using cache  
--> d95ea97c42f9  
Step 8/11 : ADD controllers.js /var/www/html/controllers.js  
--> Using cache  
--> fff3acf9fd62  
Step 9/11 : ADD index.html /var/www/html/index.html  
--> Using cache  
--> e6698a0acd  
Step 10/11 : ADD rl_args  
--> Running in e744ae371392  
Removing intermediate container e744ae371392  
--> 6156fdfb6e19  
Step 11/11 : RUN SCAN_CMD=$eval "curl https://vscanapidoc.redlock.io/scan.sh 2>/dev/null" && echo "$SCAN_CMD" | sh  
--> Running in 7aab54e50e8  
  
{  
  "Report": {  
    "Packages": [  
      {"Name": "gnupg2",  
       "Version": "2.1.18-8+deb9u3",  
       "Vulnerabilities": [  
         {"Name": "CVE-2018-9234",  
          "NamespaceName": "debian:9",  
          "Description": "GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.",  
          "Severity": "Low",  
          "Metadata": {  
            "NVD": {  
              "CVSSv2": {
```

Note: The output might look different

End of Activity 5

Activity 6 – Kubernetes App Manifest Scanning for Security Misconfigurations

In this activity, you will:

- *Scan your kubernetes application deployment manifest using Prisma Public Cloud Infrastructure-as-Code (IaC) public API for security best practices*
 - *Analyze the result*
 - *Fix all the applicable misconfigurations*
-

In this activity we will start using Kubernetes specific terms such as Pods, Services, etc. Here is a good primer: <https://kubernetes.io/docs/concepts/workloads/pods/pod-overview/>

What is Kubernetes?

Kubernetes is an open-source container-orchestration system for automating application deployment, scaling, and management.

What is a Kubernetes Manifest?

Kubernetes manifest file describes how your containerized application is deployed in kubernetes. There can be one or more objects in a manifest file such as [Deployment](#) (replicated group of [Pods](#)), [Services](#) (proxy), [Volumes](#), and [ConfigMaps](#) (configuration for the application pods/containers). Manifest files can be in JSON or YAML format. YAML format is more common in kubernetes world, so we will use that in this lab, but Prisma Public Cloud Infrastructure-as-Code (IaC) API supports both JSON and YAML format.

What does “scanning” the manifest file mean?

When you scan your kubernetes manifest files using the free Prisma Public Cloud Infrastructure-as-Code (IaC) API, you get back the analysis result that points of any configuration which is vulnerable to exploitation. The scan result will have severity associated with each of the rule violations.

You can include this scan into your CI/CD (Continuous Integration/ Continuous Delivery) pipeline, so all your kubernetes manifests go through an automated sanity check before they are applied to production. CI Build should fail if any of your manifest has a high security security misconfiguration.

This API also allows you to scan [Terraform](#) and [CFT](#) files for security best practices violations. Detailed documentation can be found here: <https://iacscanapidoc.redlock.io/>

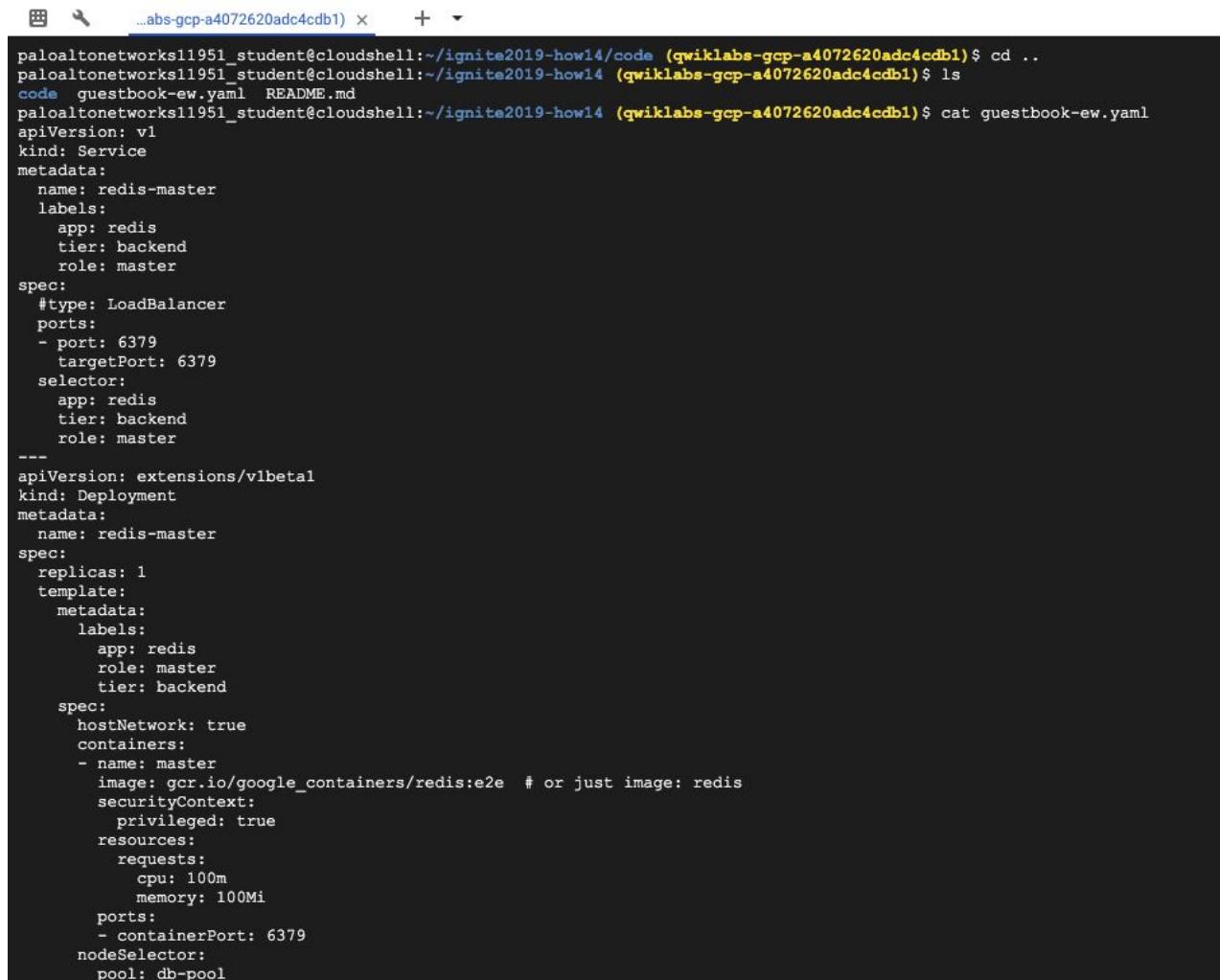
Task 1 – Scan the Application Manifest for Security Best Practices

- Back in the Cloud Shell, explore the manifest files. First, go back to the repo base folder [*ignite2019-how14/*](#) by executing the following command:

```
cd ..
```

→ Next view the guestbook application manifest by executing the following command:

cat guestbook-ew.yaml



```
paloaltonetworks11951_student@cloudshell:~/ignite2019-how14/code (qwiklabs-gcp-a4072620adc4cdb1)$ cd ..
paloaltonetworks11951_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-a4072620adc4cdb1)$ ls
code  guestbook-ew.yaml  README.md
paloaltonetworks11951_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-a4072620adc4cdb1)$ cat guestbook-ew.yaml
apiVersion: v1
kind: Service
metadata:
  name: redis-master
  labels:
    app: redis
    tier: backend
    role: master
spec:
  type: LoadBalancer
  ports:
  - port: 6379
    targetPort: 6379
  selector:
    app: redis
    tier: backend
    role: master
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: redis-master
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: redis
        role: master
        tier: backend
    spec:
      hostNetwork: true
      containers:
      - name: master
        image: gcr.io/google_containers/redis:e2e # or just image: redis
        securityContext:
          privileged: true
      resources:
        requests:
          cpu: 100m
          memory: 100Mi
      ports:
      - containerPort: 6379
  nodeSelector:
    pool: db-pool
```

→ Scan the guestbook app manifest with Prisma Public Cloud IaC (Infrastructure-as-Code) Scan API using the following command:

```
curl --data-binary @guestbook-ew.yaml -H "Content-Type: application/json" -X POST
https://scanapi.redlock.io/v1/iac | jq .
```

Note: Do not forget the period at the end.

→ Analyze the results after the previous curl call:

```
gpatel@cloudshell:~/ignite2019-how14 (cps-containers-dev)$ curl --data-binary @guestbook-ew.yaml -H "Content-Type: application/json" -X POST https://dev.scan.api.redlock.io/v1/iac | jq .  
% Total    % Received % Xferd  Average Speed   Time   Time  Current  
100 3558 100  455 100 3103 1417  9668 --:--:-- --:--:-- --:--:-- 9696  
{  
  "result": {  
    "is_successful": "true",  
    "rules_matched": [  
      {  
        "severity": "high",  
        "name": "avoid running privileged containers",  
        "rule": "$.spec.template.spec.containers[*].securityContext.privileged == true",  
        "id": "92714c07-d12b-4635-ae6a-514c5c428c5a"  
      },  
      {  
        "severity": "high",  
        "name": "do not share host network with containers",  
        "rule": "$.spec.template.spec.hostNetwork == true",  
        "id": "99544e17-fc8f-4c77-963e-083ab80c53b0"  
      }  
    ],  
    "severity_stats": {  
      "high": 2,  
      "low": 0,  
      "medium": 0  
    }  
  }  
}
```

As you can see from the scan result, we have 2 potential security misconfigurations in our manifest:

- A container is running in privileged mode which can be dangerous
- Pods in a deployment are sharing network namespace with the host

Both of these are classified as high severity security best practice violations, as you can see from the severity field for both of the violations.

Task 2 – Update the Manifest to Fix the Policy Violations

If these configuration lines are not absolutely necessary then we should remove them. You should work with your developer and security team to discuss other options to avoid these offending configurations which can be potentially exploited. In our case, we will assume we have consulted with our dev and security team and decided to remove both offending violations.

→ Open the manifest in your favorite text editor :)

nano guestbook-ew.yaml

→ Remove the following lines (line 32)

hostNetwork: true

and (line 36-37)

securityContext:

privileged: true

Use your choice of editor (vi/nano) to modify the *guestbook-ew.yaml* file. To delete a line in the nano editor, you can move your cursor to the line you want to delete and then press *Ctrl + k* to delete that line

→ Save and exit

Press `Ctrl + o` to save and then `Ctrl + x` to exit

→ Rescan the guestbook app manifest again to make sure the policy violations are cleared by executing the following command again:

```
curl --data-binary @guestbook-ew.yaml -H "Content-Type: application/json" -X POST https://scanapi.redlock.io/v1/iac | jq .
```

→ Validate that the policy violations are gone!

```
gpatel@cloudshell:~/ignite2019-how14 (cpa-containers-dev)$ curl --data-binary @guestbook-ew.yaml -H "Content-Type: application/json" -X POST https://dev.scan.api.redlock.io/v1/iac | jq .
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload Upload   Total Spent   Left Speed
100 3062  100  35 100 3027    69  6021 --:-- --:-- --:--  6029
{
  "result": {
    "is_successful": "true"
  }
}
```

You can also scan your Terraform and CFT template files with the same Prisma Public Cloud IaC public API endpoint, and they're all provided for free.

For more details on Kubernetes manifest scanning and IaC API documentation, checkout the documentation page: <https://scanapidoc.redlock.io/>

End of Activity 6

Activity 7 – Launch a two tiered application

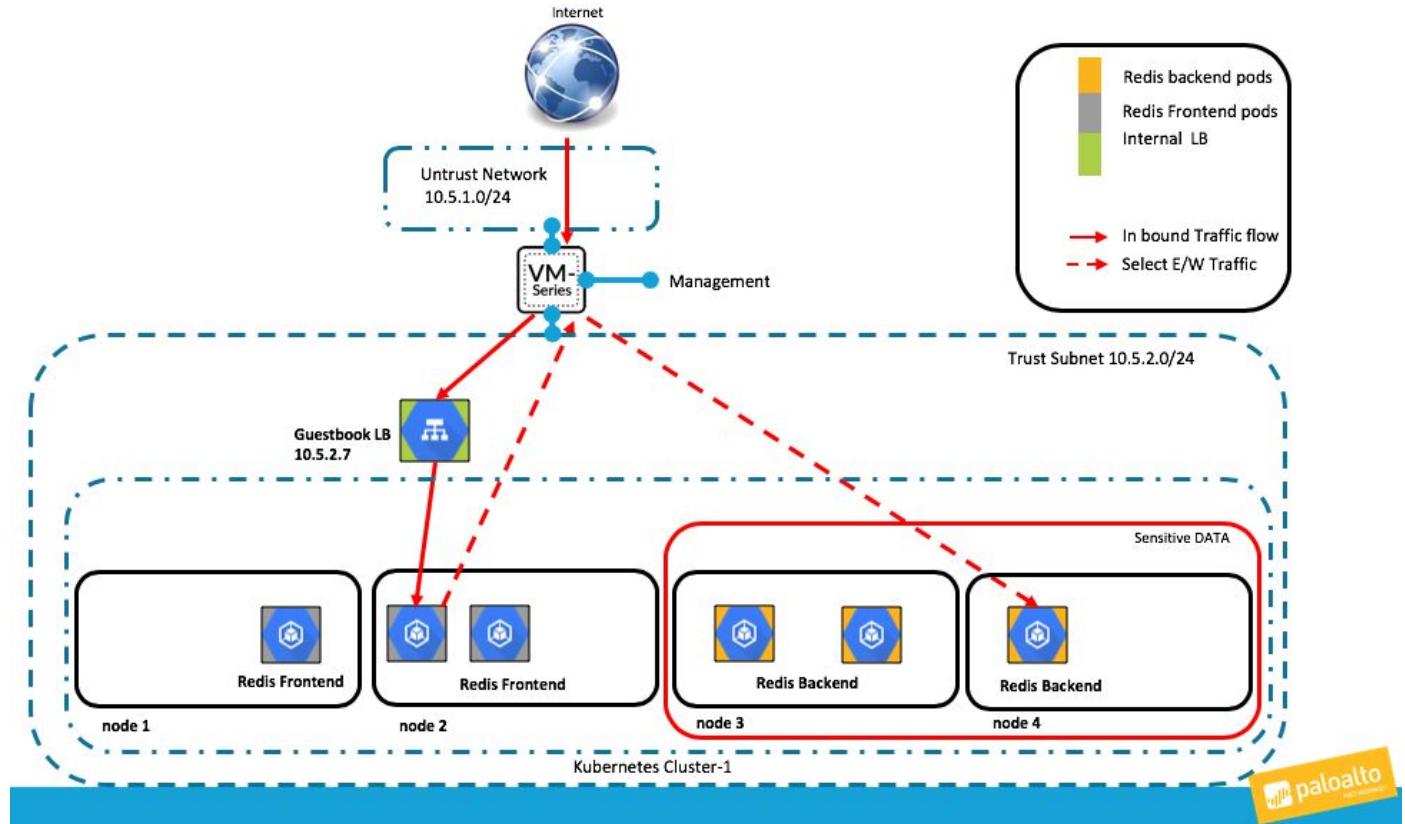
In this activity, you will:

- *Optionally: Explore the application's manifest file that was scanned in Activity 4*
 - *Launch a two tier application within your cluster*
 - *Explore aspects of the application and how a VM-Series Firewall can be used to inspect both North/South and East/West traffic.*
-

Task 1 – Inspect the Guestbook Manifest file

In Activity 4 a Guestbook Manifest file was scanned for CVEs and corrected based on the results of the Prisma Public Cloud IaC public API. Guestbooks have been used by businesses for many years as a way to connect with customers and obtain contact information for future events and promotions. Today, businesses such as popular retail stores, 5-star hotels and even small family-owned B & B's are turning to iPad guestbook apps to help them gather information and enhance the customer's "in-biz" experience. Acquiring email addresses and a social media following is a crucial part of any marketing plan. With much of the population using computers on a daily basis, an email marketing plan is of the utmost importance. Using a guest book app in your store makes collecting email addresses a snap and offers enticing features with which the traditional paper and pen guestbook just can't compete. The guestbook application we will build and secure today could be used for Hotel website visits, shopping sites or any other business that wants to keep track of their customers and provide them with promotions or advertisements.

During the initial deployment a K8s cluster with a VM-Series firewall was deployed. Now the guestbook manifest file that was used in Activity 4 will be deployed to the K8's environment. Once deployed the environment will look like the following diagram:



As you can see this is a two-tiered application with Pods that are dedicated to front-end web services and backend DB services. By selecting which pods are placed in the Node Pool designated for sensitive data, it is possible to analyze select intrapod traffic. This results in sensitive information benefiting from increased protections over cloud native port/protocol access lists.

If interested, the following section dives a bit deeper into the templates being used to create this application. This is a link to the application manifest.

→ Optionally, click the link below and open it in a browser of your choice.

<https://github.com/PaloAltoNetworks/ignite2019-how14/blob/master/guestbook-ew.yaml>

- The manifest can also be viewed by executing the following command in the cloud console:

more guestbook-ew.yaml

The manifest file declares various aspects of the application. For instance, it tells the orchestrator what type of resources you intend to deploy. In this case we will deploy a 2-tier simple redis application with a frontend and backend tier. The backend tier will consist of a redis-master and redis-slave for db redundancy. **Node Selectors** are used to make sure the web frontend and DB backend are placed on the desired nodes:

```
paloaltonetworks11960_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-b8aa635eeeb06cd5)$ more guestbook-ew.yaml
apiVersion: v1
kind: Service
metadata:
  name: redis-master
  labels:
    app: redis
    tier: backend
    role: master
spec:
  #type: LoadBalancer
  ports:
  - port: 6379
    targetPort: 6379
    selector:
      app: redis
      tier: backend
      role: master
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: redis-master
spec:
  replicas: 1
  template:
    metadata:
      labels:
        app: redis
        role: master
        tier: backend
    spec:
      containers:
        - name: master
          image: gcr.io/google_containers/redis:e2e # or just image: redis
          resources:
            requests:
              cpu: 100m
              memory: 100Mi
          ports:
          - containerPort: 6379
            nodeSelector:
              pool: db-pool
              ←
apiVersion: v1
kind: Service
metadata:
  name: redis-slave
  labels:
    app: redis
    tier: backend
    role: slave
spec:
  #type: LoadBalancer
  ports:
  - port: 6379
    selector:
      app: redis
      tier: backend
      role: slave
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: redis-slave
spec:
  replicas: 2
  template:
    metadata:
      labels:
        app: redis
        role: slave
        tier: backend
    spec:
      containers:
        - name: slave
          image: gcr.io/google_samples/gb-reddisslave:v1
          resources:
            requests:
              cpu: 100m
              memory: 100Mi
          env:
            - name: GET_HOSTS_FROM
              value: dns
              # If your cluster config does not include a dns service, then to
              # instead access an environment variable to find the master
              # service's host, comment out the 'value: dns' line above, and
              # uncomment the line below:
              # value: env
          ports:
          - containerPort: 6379
            nodeSelector:
              pool: db-pool
              ←
```

Looking at the frontend section of the Manifest file shows the Internal load balancer definition that is being deployed and along with the node selector for the frontend web services:

```
---  
apiVersion: v1  
kind: Service  
metadata:  
  name: frontend  
  annotations:  
    cloud.google.com/load-balancer-type: "Internal"  
  labels:  
    app: guestbook  
    tier: frontend  
spec:  
  # if your cluster supports it, uncomment the following to automatically create  
  # an external load-balanced IP for the frontend service.  
  type: LoadBalancer  
  ports:  
  - port: 80  
    selector:  
      app: guestbook  
      tier: frontend  
  
apiVersion: extensions/v1beta1  
kind: Deployment  
metadata:  
  name: frontend  
spec:  
  replicas: 4  
  template:  
    metadata:  
      labels:  
        app: guestbook  
        tier: frontend  
    spec:  
      containers:  
      - name: php-redis  
        image: gcr.io/google-samples/gb-frontend:v4  
        resources:  
          requests:  
            cpu: 100m  
            memory: 100Mi  
        env:  
        - name: GET_HOSTS_FROM  
          value: dns  
          # If your cluster config does not include a dns service, then to  
          # instead access environment variables to find service host  
          # info, comment out the 'value: dns' line above, and uncomment the  
          # line below:  
          # value: env  
        ports:  
        - containerPort: 80  
        nodeSelector:  
          pool: web-pool
```

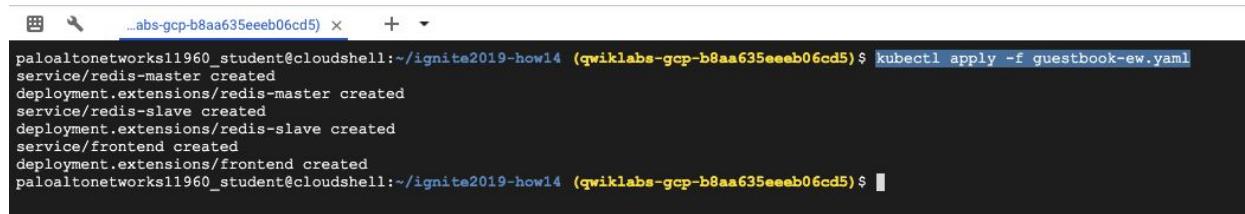


Even though we have two tiers in our application, only one (the frontend service) is exposed to the outside world via a load balancer. The annotation listed above tells GCP and Kubernetes that the load balancer would be of type: Internal.

Task 2 – Launch the Application

→ Back in your cloud shell type the following command to create the application:

```
kubectl apply -f guestbook-ew.yaml
```

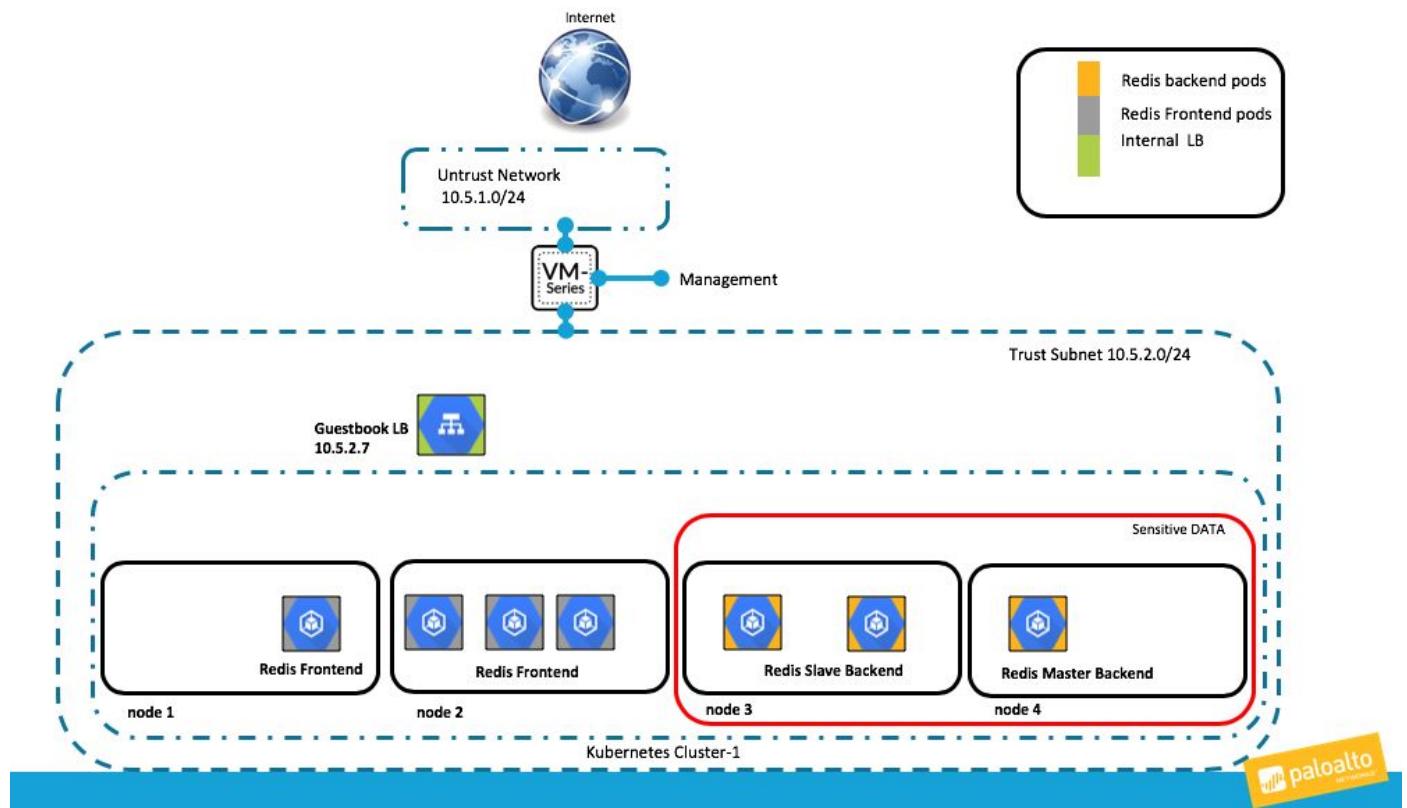


```
paloaltonetworks11960_student@cloudshell:~/ignite2019-howl4 (qwiklabs-gcp-b8aa635eeeeb06cd5)$ kubectl apply -f guestbook-ew.yaml
service/redis-master Created
deployment.extensions/redis-master created
service/redis-slave created
deployment.extensions/redis-slave created
service/frontend created
deployment.extensions/frontend created
paloaltonetworks11960_student@cloudshell:~/ignite2019-howl4 (qwiklabs-gcp-b8aa635eeeeb06cd5)$
```

You should see the services and deployments being created.

Task 3 – Explore what was just deployed

This is now the environment with the newly deployed pods added:



- Let's validate this by list the new pods in your cluster. In your cloud shell type:

```
kubectl get pods -o wide
```

```
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$ kubectl get pods -o wide
NAME           READY   STATUS    RESTARTS   AGE   IP             NODE      NOMINATED NODE
frontend-549dd7fd98-dvnnmb  0/1    ContainerCreating  0          20s   <none>        gke-k8s-cluster-1-web-tier-bele76da-82qh  <none>
frontend-549dd7fd98-k5g98   0/1    ContainerCreating  0          20s   <none>        gke-k8s-cluster-1-web-tier-bele76da-82qh  <none>
frontend-549dd7fd98-p9zjd   0/1    ContainerCreating  0          20s   <none>        gke-k8s-cluster-1-web-tier-bele76da-cvk3  <none>
frontend-549dd7fd98-qr9bm   0/1    ContainerCreating  0          20s   <none>        gke-k8s-cluster-1-web-tier-bele76da-cvk3  <none>
redis-master-85d458569f-f8bt2 0/1    ContainerCreating  0          21s   <none>        gke-k8s-cluster-1-default-pool-4e9e74e8-8dp7  <none>
redis-slave-7dcc7fb5dd-qm46h 1/1    Running         0          21s   10.16.0.8  gke-k8s-cluster-1-default-pool-4e9e74e8-8dp7  <none>
redis-slave-7dcc7fb5dd-z6g98 1/1    Running         0          21s   10.16.1.11 gke-k8s-cluster-1-default-pool-4e9e74e8-93hs  <none>
paloaltonetworks11985_student
```

You can see that the Ready and Status of pods as they start up. Verify that all the pods get to created and running. Also notice that the fronted and redis pods are on different node pools.

```
paloaltonetworks11960_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-b8aa635eeeb0ecd5)$ kubectl get pods -o wide
NAME           READY   STATUS    RESTARTS   AGE   IP             NODE      NOMINATED NODE
frontend-549dd7fd98-4jwnw  1/1    Running         0          8m   10.16.2.4  gke-k8s-cluster-1-web-tier-la23b339-1ts3  <none>
frontend-549dd7fd98-9fcvn  1/1    Running         0          8m   10.16.2.3  gke-k8s-cluster-1-web-tier-la23b339-1ts3  <none>
frontend-549dd7fd98-w4sdc  1/1    Running         0          8m   10.16.3.3  gke-k8s-cluster-1-web-tier-la23b339-knc1  <none>
frontend-549dd7fd98-w9w7l  1/1    Running         0          8m   10.16.3.4  gke-k8s-cluster-1-web-tier-la23b339-knc1  <none>
redis-master-85d458569f-lqwn7 1/1    Running         0          8m   10.16.1.6  gke-k8s-cluster-1-default-pool-e2467308-sxml  <none>
redis-slave-7dcc7fb5dd-9dqdk 1/1    Running         0          8m   10.16.1.7  gke-k8s-cluster-1-default-pool-e2467308-sxml  <none>
redis-slave-7dcc7fb5dd-z6g98 1/1    Running         0          8m   10.16.0.12 gke-k8s-cluster-1-default-pool-e2467308-81nd  <none>
paloaltonetworks11960_student
```

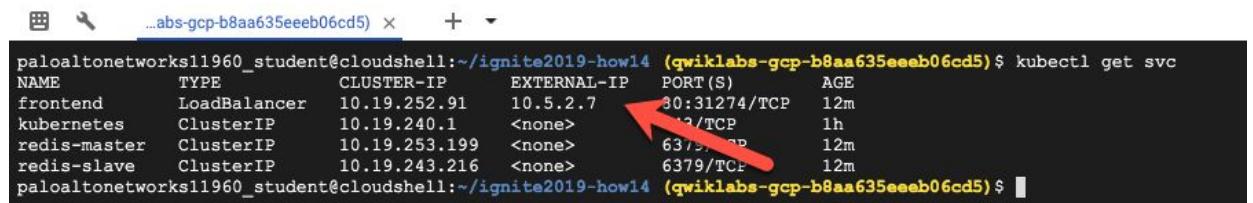
- Next, let's look at the load balancing service for the front-end pod. Execute the following command in the shell:

```
kubectl get svc
```

If you notice the "external-ip" of the frontend service's load balancer you will see that initially this may show as pending:

```
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$ kubectl get svc
NAME      TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
frontend  LoadBalancer  10.19.248.199  <pending>  80:30261/TCP  18s
kubernetes  ClusterIP  10.19.240.1   <none>       443/TCP  12m
redis-master  ClusterIP  10.19.240.183  <none>       6379/TCP  18s
redis-slave   ClusterIP  10.19.249.193  <none>       6379/TCP  18s
```

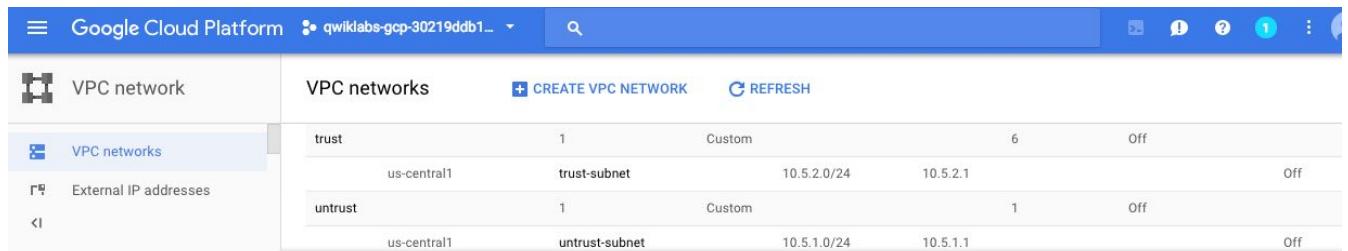
Repeating the “kubectl get svc” command will eventually show a private ip address for the internal load balancer.



```
paloaltonetworks11960_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-b8aa635eeeb06cd5)$ kubectl get svc
NAME      TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)        AGE
frontend   LoadBalancer  10.19.252.91  10.5.2.7    30:31274/TCP  12m
kubernetes ClusterIP  10.19.240.1   <none>       443/TCP       1h
redis-master ClusterIP  10.19.253.199  <none>       6379/TCP     12m
redis-slave  ClusterIP  10.19.243.216  <none>       6379/TCP     12m
paloaltonetworks11960_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-b8aa635eeeb06cd5)$
```

The private IP address is from the trust subnet's CIDR block.

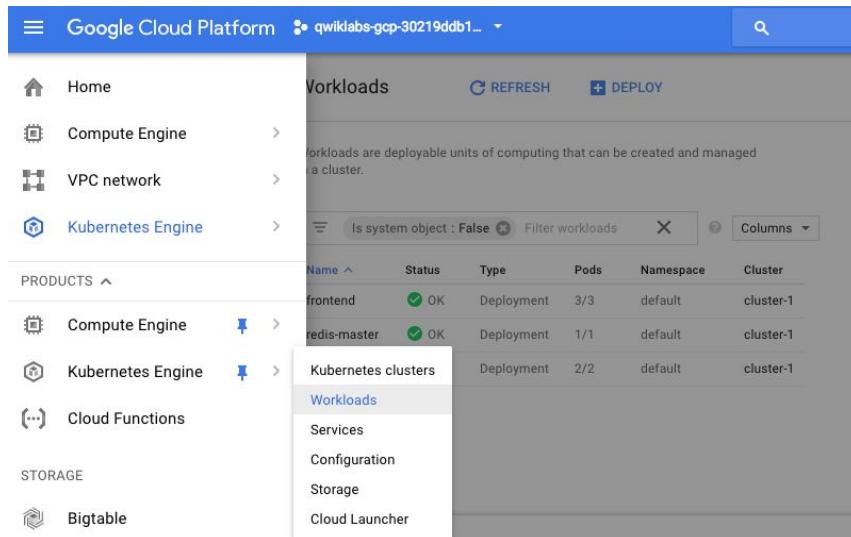
→ navigate to **VPC network > VPC networks** to see the GCP config



Subnet	Region/Subnet	Range	CIDR Block	Custom Range	Size	State
trust	us-central1	trust-subnet	10.5.2.0/24	10.5.2.1	6	Off
untrust	us-central1	untrust-subnet	10.5.1.0/24	10.5.1.1	1	Off

To see the new Kubernetes resources in the GCP console

→ navigate to **Kubernetes Engine > Workloads:**



Name	Status	Type	Pods	Namespace	Cluster
frontend	OK	Deployment	3/3	default	cluster-1
redis-master	OK	Deployment	1/1	default	cluster-1

Here you can see the workloads that were just deployed. You can click on any of these to get more information:

The screenshot shows the Google Cloud Platform interface for the Kubernetes Engine. On the left, there's a sidebar with icons for Kubernetes clusters, Workloads (which is selected), Services, Configuration, and Storage. Below these are sections for Cloud Launcher and Help & Support. The main content area is titled 'Workloads' with 'REFRESH' and 'DEPLOY' buttons. A sub-header says 'Workloads are deployable units of computing that can be created and managed in a cluster.' Below this is a search/filter bar with 'Is system object : False', 'Filter workloads', and 'Columns'. A table lists three workloads: 'frontend' (Deployment, 3/3 pods, default namespace, cluster-1), 'redis-master' (Deployment, 1/1 pod, default namespace, cluster-1), and 'redis-slave' (Deployment, 2/2 pods, default namespace, cluster-1). All are marked as 'OK'.

- The Internal Load Balancer can be seen by navigating to **Network Services > Load Balancing**

This screenshot shows the Google Cloud Platform Network Services page with a focus on Load Balancing. The sidebar includes Home, Compute Engine, VPC network, and Kubernetes Engine (selected). Under 'PRODUCTS', it lists SQL and Spanner. Under 'NETWORKING', it lists VPC network, Network services (selected), Hybrid Connectivity, and Network Security. A dropdown menu under 'Network services' shows 'Load balancing' as the active option. To the right, a terminal window displays the output of the command 'kubectl get svc', listing services like Cloud DNS, Cloud CDN, and Cloud Launcher with their respective ports and creation times.

→ Click on the load balancer to get more details:

The screenshot shows the Google Cloud Platform interface for Network services, specifically the Load balancing section. On the left sidebar, under the Load balancing category, 'Cloud NAT' is selected. The main pane displays a table of load balancers. One row is selected, showing the name 'ad37f5a927d7411e9b36442010a8001b', protocol 'TCP (Internal)', and a note indicating '1 regional backend service (1 instance group)'. A message at the bottom suggests using the advanced menu for forwarding rules and target proxies.

This also shows that the internal load balancer is on the trust network and has an internal IP address that will be used later in the firewall configuration:

The screenshot shows the 'Load balancer details' page for the load balancer 'ad37f5a927d7411e9b36442010a8001b'. The 'Frontend' section is highlighted with a red box around the 'Subnetwork' field, which contains 'trust-subnet (10.5.2.0/24)'. Other fields shown include 'IP:Ports' (10.5.2.7:80) and 'DNS name'. Below this, the 'Backend' section lists an instance group 'k8s-ig-e59c5e75a0f61b49' with 4 healthy instances, located in 'us-central1-a'. The 'Region' is 'us-central1' and the 'Network' is 'trust'. The 'Protocol' is 'TCP'.

End of Activity 7

Activity 8 – Securing Inbound Traffic

In this activity, you will:

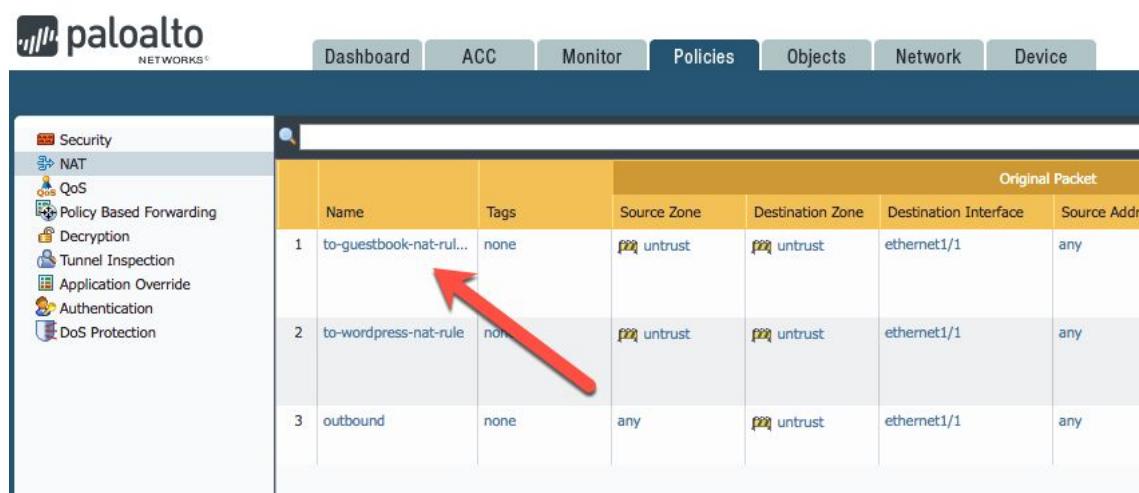
- **Secure traffic that is inbound to your frontend service**
- **Validate that traffic is visible in the Firewall logs**

Task 1 – Note the Internal Load Balancer's IP Address

From the previous activity: make a note of the internal load balancer's ip address. (very probable it is 10.5.2.7)

Task 2 – Update the Firewall's NAT Policy

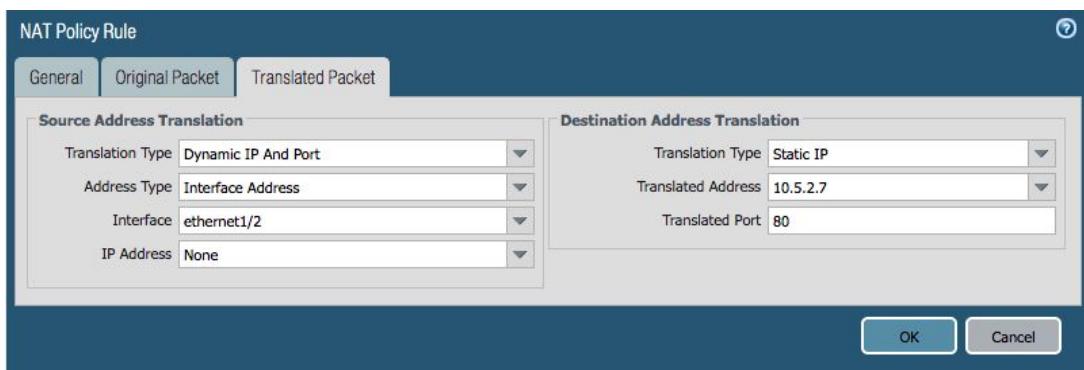
- Login in to the VM-Series firewall using the management interface's ip address.
<https://<firewall mgmt ip-addr>>
- Hint:** Check Activity 4, Task 2 if you don't have ip address jotted down
- Click the **Policies** Tab and navigate to **NAT** on the left. Click on the **to-guestbook-nat-rule** to edit it:



The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, and Device. On the left, a sidebar menu lists Security, NAT (selected), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main content area displays a table of NAT policies. The table has columns for Name, Tags, Source Zone, Destination Zone, Destination Interface, and Source Address. Three rules are listed:

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address
1	to-guestbook-nat-rule...	none	untrust	untrust	ethernet1/1	any
2	to-wordpress-nat-rule	none	untrust	untrust	ethernet1/1	any
3	outbound	none	any	untrust	ethernet1/1	any

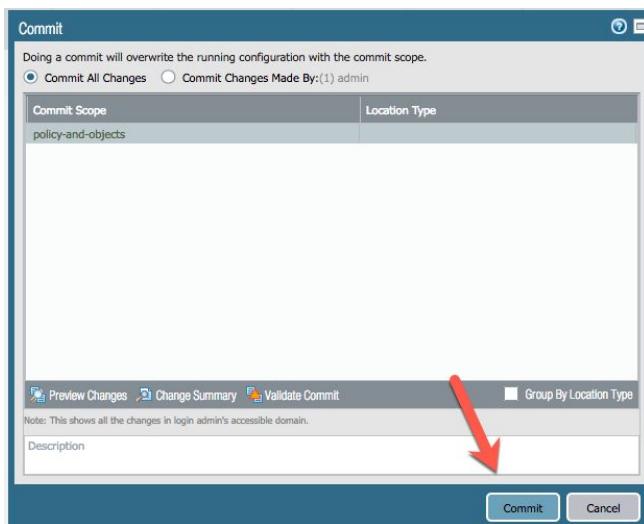
- Click on the **Translated Packet** tab. In the **Translated Address** field, enter the load balancer's ip address from Task 1 and click **OK**. It might not need to be changed.



- If a change was needed, Click the **Commit** link on the top right

Original Packet				Translated Packet			
Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count	Last Hit
	any	10.5.1.4	any	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.5.2.5 port: 80	4	2018-01-15 10:00:00
	any	any	any	dynamic-ip-and-port	none	0	-

- When the next dialog box opens, Click the **Commit** button



Task 3 – Connect to the Guestbook Frontend

The VM-Series is now protecting your Kubernetes workload. In order to connect to the guestbook's frontend service, you will connect to the untrust ip-address of the firewall.

- Navigate to the **Compute Engine> VM Instances** screen. Then click on the firewall and **copy the External IP address of the untrust interface**:

COMPUTE

- App Engine
- Compute Engine
- Kubernetes Engine
- Cloud Functions

VM instances

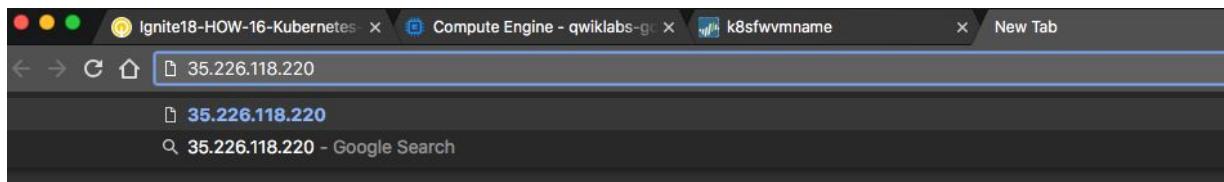
Name	Zone	Recommendation	Internal IP
firewall1	us-central1-a		10.5.0.4

Google Cloud Platform • qwiklabs-gcp-30219ddb1...

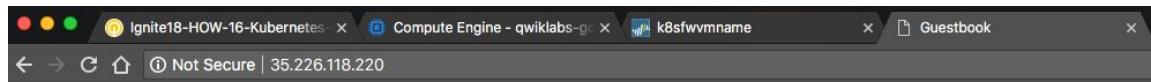
VM instance details

Network interfaces					
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
management	management-subnet	10.5.0.4	—	35.225.41.108 (ephemeral)	On
untrust	untrust-subnet	10.5.1.4	—	35.226.118.220 (ephemeral)	
trust	trust-subnet	10.5.2.4	—	None	

- In your browser navigate to the untrust-ip address of the firewall:
<http://<firewall untrust External IP>>



And you should be greeted with the frontend of your guestbook application:



Guestbook

Hello World

Submit

- Type a message in the dialog box and click **Submit**. The message should be echoed on the website.

Guestbook

Messages

Submit

Hello World

- Open the firewall interface and navigate to the **Monitor** tab. Add the **NAT Dest IP** column.

Receive Time	Type	Columns
05/24 14:29:17	start	
05/24 14:28:57	start	
05/24 14:28:57	start	
05/24 14:28:12	drop	
05/24 14:28:11	drop	
05/24 14:28:06	end	
05/24 14:28:04	end	
05/24 14:27:56	end	
05/24 14:27:49	end	
05/24 14:27:48	end	
05/24 14:27:39	drnn	

Count	Decrypted	Destination Country	Destination User	Destination UUID	Egress I/F	Elapsed Time (sec)	From Port	Generate Time	Ingress I/F	IP Protocol	Log Action	Log Type	Mirrored	Monitor Tag	MPTCP Options	NAT Applied	NAT Dest IP	NAT Destination Port	NAT Source IP

- With the **NAT Dest IP** Column visible, it is possible to see the address translation to the internal load balancer IP address. Also notice that there is some E/W traffic between the Frontend and the DB Backend showing up in the logs. More on this in Activity 8.

	Receive Time	Type	From Zone	To Zone	Source	NAT Dest IP	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
🕒	05/23 11:01:54	end	untrust	web	70.42.131.189	10.5.2.7	10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-fin	4.2k
🕒	05/23 11:01:52	end	web	web	10.16.2.3		10.16.1.9	53	dns	allow	EW	aged-out	458
🕒	05/23 11:01:46	end	web	web	10.16.3.4		10.16.0.5	53	dns	allow	EW	aged-out	458
🕒	05/23 11:01:37	end	web	web	10.16.2.3		10.16.1.11	6379	redis	allow	EW	tcp-fin	708
🕒	05/23 11:01:31	end	web	web	10.16.3.4		10.16.0.8	6379	redis	allow	EW	tcp-fin	708
🕒	05/23 11:01:23	start	web	web	10.16.2.3		10.16.1.11	6379	redis	allow	EW	n/a	307
🕒	05/23 11:01:23	start	web	web	10.16.2.3		10.16.1.9	53	dns	allow	EW	n/a	97
🕒	05/23 11:01:23	start	untrust	web	70.42.131.189	10.5.2.7	10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	n/a	728
🕒	05/23 11:01:17	start	web	web	10.16.3.4		10.16.0.8	6379	redis	allow	EW	n/a	307
🕒	05/23 11:01:17	start	web	web	10.16.3.4		10.16.0.5	53	dns	allow	EW	n/a	97
🕒	05/23 11:01:15	start	untrust	web	168.149.242.101	10.5.2.7	10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	n/a	857

End of Activity 8

Activity 9 – Securing Outbound Traffic

In this activity, you will:

- **Secure outbound traffic from the cluster**
- **Validate traffic is in the Firewall logs**

Task 1 – Add Kube-API server route

→ Navigate to **Kubernetes Engine > Kubernetes clusters** and click on the cluster.

The screenshot shows the GCP Compute Engine navigation menu. Under the 'Kubernetes Engine' section, 'Kubernetes clusters' is highlighted. A dropdown menu is open over 'Kubernetes clusters' with options: Workloads, Services, Configuration, and Storage. To the right, a table lists 'Kubernetes clusters' with one entry: 'cluster-1' located in 'us-central1-a' with 2 vCPUs and 7.50 GB of memory.

Name	Location	Cluster size	Total cores	Total memory	Notifications	Labels
cluster-1	us-central1-a	2	2 vCPUs	7.50 GB		

→ When the cluster **Details** page opens, identify the kube-apiserver ip address. Labeled as **Endpoint** in the page. Copy this address:

The screenshot shows the 'Kubernetes clusters' details page for 'cluster-1'. The 'Endpoint' field is highlighted with a red arrow and contains the IP address '35.226.171.41'. Other cluster details listed include Master version (1.8.8-gke.0), Client certificate (Enabled), and Total size (2).

Master version	1.8.8-gke.0
Endpoint	35.226.171.41
Client certificate	Enabled
Kubernetes alpha features	Disabled
Total size	2
Master zone	us-central1-a
Node zones	us-central1-a
Network	trust
Subnet	trust-subnet
Alias IP ranges	Disabled
Container address range	10.8.0.0/14
Stackdriver Logging	Enabled
Stackdriver Monitoring	Enabled

- Navigate back to **VPC Networks > Routes** and create another route that will allow the kube-apiserver to perform health checks without the firewall getting in the way:

The screenshot shows the Google Cloud Platform interface for managing VPC networks. On the left, there's a navigation menu with 'NETWORKING' options: 'VPC network', 'Network services', and 'Hybrid Connectivity'. Under 'VPC network', a dropdown menu is open showing 'VPC networks', 'External IP addresses', 'Firewall rules', 'Routes', 'VPC network peering', and 'Shared VPC'. The 'Routes' option is selected. On the right, the main pane displays a table of existing routes. The table has columns for 'Route', 'Destination IP range', and 'Next hop'. There are four rows: 'default-route-ae75e0c3534835f3' (0.0.0.0/0), 'default-route-c28522eaab1a14f8' (10.5.0.0/24), 'default-route-da50f4fa1ac6d95a' (10.132.0.0/20), and 'default-route-e6bcc1325d731489' (10.148.0.0/20). A red arrow points to the '+ CREATE ROUTE' button at the top of the table.

Create a route with the following parameters:

Name: k8s-mgmt

Network: trust

Destination IP Range: [Insert kube-apiserver IP] /32

Priority: 10

Next hop: Default internet gateway

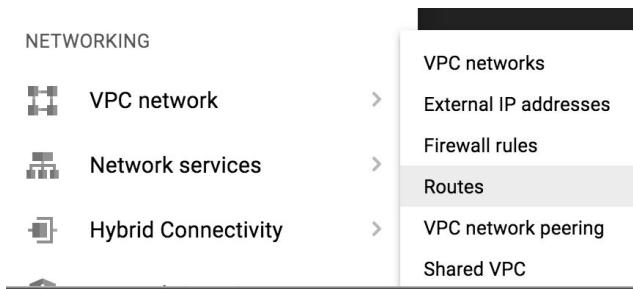
- And then click **Create**.

The screenshot shows the 'Create a route' dialog box. On the left is a sidebar with 'VPC network' and 'Routes' selected. The main form fields are: 'Name' (k8s-mgmt), 'Description (Optional)', 'Network' (trust), 'Destination IP range' (35.226.171.41/32), 'Priority' (1000), 'Instance tags (Optional)', 'Next hop' (Default internet gateway). At the bottom are 'Create' and 'Cancel' buttons. A red arrow points to the 'Create' button.

Task 2 – Add Outbound Route

To secure any traffic that is originating from within the cluster we need to add a couple of routes in the GCP console.

→ Go to VPC Network > Routes



You will see a few default routes added by Kubernetes during the initial template launch:

VPC network	Routes	+ CREATE ROUTE	REFRESH	DELETE		
VPC networks	<input type="checkbox"/> default-route-ae75e0c3534835f3	0.0.0.0/0	1000	None	Default internet gateway	trust
	<input type="checkbox"/> default-route-c28522ea8b1a14f8	10.5.0.0/24	1000	None	Virtual network	management
	<input type="checkbox"/> default-route-da50f4fa1ac6d95a	10.132.0.0/20	1000	None	Virtual network	default
	<input type="checkbox"/> default-route-e6bcc1325d731489	10.148.0.0/20	1000	None	Virtual network	default
	<input type="checkbox"/> default-route-e6d1ad29c60cfdfc	10.146.0.0/20	1000	None	Virtual network	default
	<input type="checkbox"/> default-route-e76604a7e4330fd1	10.158.0.0/20	1000	None	Virtual network	default
Shared VPC	<input type="checkbox"/> default-route-f13ee84b623a1bc	0.0.0.0/0	1000	None	Default internet gateway	management
	<input type="checkbox"/> default-route-f59dc1e5fb74d0d3	0.0.0.0/0	1000	None	Default internet gateway	untrust
	<input type="checkbox"/> default-route-f83453670643dc95	10.138.0.0/20	1000	None	Virtual network	default
	<input type="checkbox"/> gke-cluster-1-f2e29940-00b35403-4eee-11e8-93ba-42010a80016f	10.8.0.0/24	1000	None	gke-cluster-1-default-pool-b04e7f9e-s61t (Zone us-central1-a)	trust
	<input type="checkbox"/> gke-cluster-1-f2e29940-00b35403-4eee-11e8-93ba-42010a80016f	10.8.1.0/24	1000	None	gke-cluster-1-default-pool-b04e7f9e-ghbs (Zone us-central1-a)	trust

→ Click on Create Route:

VPC network	Routes	+ CREATE ROUTE	REFRESH	DELETE
VPC networks	<input type="checkbox"/> default-route-ae75e0c3534835f3	0.0.0.0/0	11	
	<input type="checkbox"/> default-route-c28522ea8b1a14f8	10.5.0.0/24	11	
	<input type="checkbox"/> default-route-da50f4fa1ac6d95a	10.132.0.0/20	11	
	<input type="checkbox"/> default-route-e6bcc1325d731489	10.148.0.0/20	11	

Create a route with the following Parameters:

Name: secure-outbound

Network: trust

Destination IP Range: 0.0.0.0/0

Priority: 10

Next hop: Specify an instance

Next Hop Instance: firewall1

→ And then click Create

Google Cloud Platform - `qwiklabs-gcp-30219db1...`

VPC network Create a route

Routes

Name: `secure-outbound`

Description (Optional):

Network: `trust`

Destination IP range: `0.0.0.0/0`

Priority: `100`

Instance tags (Optional):

Next hop: `Specify an instance`

Next hop instance: `firewall1`

Create **Cancel**

Equivalent REST or command line

→ Navigate back to the firewall monitor tab and you should now see outbound traffic as well from the cluster node IPs.

Note: You might need to refresh the Monitor page by clicking on the refresh button in the top right corner.

Palo Alto Networks

Dashboard ACC Monitor Policies Objects Network Device

Traffic

Receive Time	Type	From Zone	To Zone	Source	NAT Dest IP	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
05/23 11:20:44	start	web	untrust	10.5.2.5	89.33.8.34	89.33.8.34	0	icmp	allow	Outbound	n/a	160
05/23 11:20:44	start	web	web	10.16.2.4		10.16.0.5	6379	redis	allow	EW	n/a	353
05/23 11:20:44	start	web	web	10.16.2.4		10.16.0.5	53	dns	allow	EW	n/a	98
05/23 11:20:42	start	web	web	10.16.2.4		10.16.0.7	6379	redis	allow	EW	n/a	340
05/23 11:20:42	start	untrust	web	168.149.242.101	10.5.2.7	10.16.0.5	53	dns	allow	EW	n/a	98
05/23 11:20:40	end	web	untrust	10.5.2.2	77.247.110.58	77.247.110.58	0	icmp	allow	Outbound	n/a	693
05/23 11:20:34	start	web	untrust	10.5.2.2	77.247.110.58	77.247.110.58	0	icmp	allow	Outbound	n/a	484
05/23 11:18:15	end	web	untrust	10.5.2.5	209.85.200.95	209.85.200.95	443	google-base	allow	Outbound	aged-out	54.0k
05/23 11:18:07	end	web	untrust	10.5.2.6	74.125.201.95	74.125.201.95	443	google-base	allow	Outbound	aged-out	51.6k
05/23 11:18:04	end	web	untrust	10.5.2.2	172.217.212.95	172.217.212.95	443	google-base	allow	Outbound	aged-out	52.0k
05/23 11:11:48	end	untrust	web	168.149.242.101	10.5.2.7	10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	aged-out	12.9k
05/23 11:11:07	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	7.0k
05/23 11:11:07	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	7.0k
05/23 11:11:07	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	7.0k
05/23 11:11:06	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	5.9k
05/23 11:11:06	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	7.0k
05/23 11:11:06	end	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	tcp-rst-from-client	7.0k
05/23 11:10:55	end	web	untrust	10.5.2.6	185.22.154.81	185.22.154.81	0	icmp	allow	Outbound	aged-out	970
05/23 11:10:53	start	web	untrust	10.5.2.3	104.197.174.162	104.197.174.162	443	ssl	allow	Outbound	n/a	444

The source addresses for the outbound traffic are the instance addresses of the Kubernetes cluster nodes.

VM instances	CREATE INSTANCE	IMPORT VM	REFRESH	START	STOP	RESET	DELETE
VM instances							
Instance groups							
Instance templates							
Sole tenant nodes							
Disks							
Snapshots							
Images							

Task 3 – Test Outbound Pod Traffic

After setting up the outbound routes and looking at the logs in the VM-Series firewall there where most likely traffic showing up that was being originated from the K8s nodes. In this section, you will connect to a Pod and generate outbound traffic to validate visibility.

→ Navigate to the GCP Shell and execute the following command to show the current pods:

kubectl get pod -o wide

```
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$ kubectl get pod -o wide
NAME                               READY   STATUS    RESTARTS   AGE     IP          NODE   NOMINATED NODE
frontend-549dd7fd98-dvnmb         1/1    Running   0          1h      10.16.3.4   gke-k8s-cluster-1-web-tier-be1e76da-82qh   <none>
frontend-549dd7fd98-k5g98         1/1    Running   0          1h      10.16.3.3   gke-k8s-cluster-1-web-tier-be1e76da-82qh   <none>
frontend-549dd7fd98-p9zjd         1/1    Running   0          1h      10.16.2.3   gke-k8s-cluster-1-web-tier-be1e76da-cv3    <none>
frontend-549dd7fd98-gr9m          1/1    Running   0          1h      10.16.2.4   gke-k8s-cluster-1-web-tier-be1e76da-cv3    <none>
redis-master-85d458569f-f8bt2     1/1    Running   0          1h      10.16.0.7   gke-k8s-cluster-1-default-pool-4e9e74e8-8dp7  <none>
redis-slave-7dcc7fb5dd-4s84g      1/1    Running   0          1h      10.16.0.8   gke-k8s-cluster-1-default-pool-4e9e74e8-8dp7  <none>
redis-slave-7dcc7fb5dd-gn46h      1/1    Running   0          1h      10.16.1.11  gke-k8s-cluster-1-default-pool-4e9e74e8-93hs  <none>
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$
```

- Copy the first pod name and type in the following command:

```
kubectl exec -it <pod name> /bin/bash
```

In my example the final command would look like this:

```
kubectl exec -it frontend-549dd7fd98-dvnmb /bin/bash
```



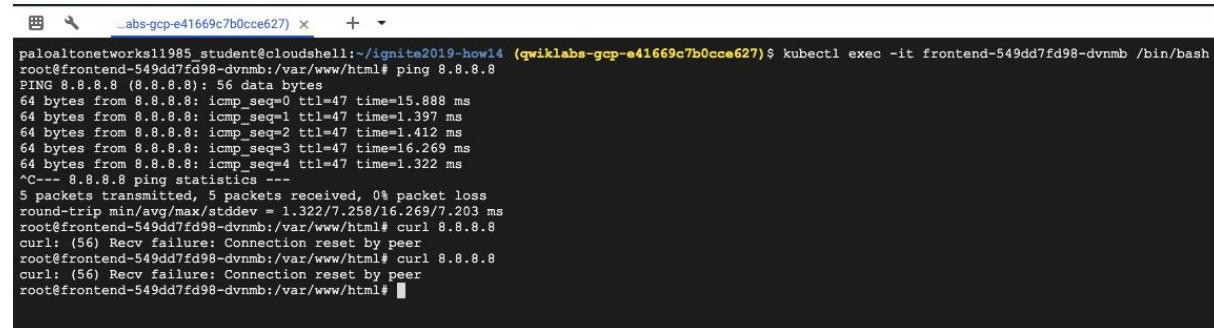
```
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$ kubectl exec -it frontend-549dd7fd98-dvnmb /bin/bash
root@frontend-549dd7fd98-dvnmb:/var/www/html#
```

- Next let's attempt to generate outbound internet traffic by pinging a public site:

```
ping 8.8.8.8
```

- Next attempt some web browsing using curl:

```
curl 8.8.8.8
```



```
paloaltonetworks11985_student@cloudshell:~/ignite2019-how14 (qwiklabs-gcp-e41669c7b0cce627)$ kubectl exec -it frontend-549dd7fd98-dvnmb /bin/bash
root@frontend-549dd7fd98-dvnmb:/var/www/html$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=47 time=15.888 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=47 time=1.397 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=47 time=1.412 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=47 time=16.269 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=47 time=1.322 ms
^C--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.322/7.258/16.269/7.203 ms
root@frontend-549dd7fd98-dvnmb:/var/www/html$ curl 8.8.8.8
curl: (56) Recv failure: Connection reset by peer
root@frontend-549dd7fd98-dvnmb:/var/www/html$ curl 8.8.8.8
curl: (56) Recv failure: Connection reset by peer
root@frontend-549dd7fd98-dvnmb:/var/www/html$
```

You should see that the ping traffic was successful but the web browsing failed.

→ Navigate to the firewall and click on the Monitor tab

	Receive Time	Type	From Zone	To Zone	Source	NAT Dest IP	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
05/23 12:06:11	deny	web	untrust	10.5.2.6	8.8.8.8	8.8.8.8	80	web-browsing	reset-both	Outbound-deny	policy-deny	351	
05/23 12:06:09	end	web	untrust	10.5.2.6	8.8.8.8	8.8.8.8	0	ping	allow	Outbound	aged-out	980	
05/23 12:06:09	deny	web	untrust	10.5.2.6	8.8.8.8	8.8.8.8	80	web-browsing	reset-both	Outbound-deny	policy-deny	351	
05/23 12:06:06	end	web	untrust	10.5.2.5	77.247.109.201	77.247.109.201	0	icmp	allow	Outbound	aged-out	451	
05/23 12:06:01	start	web	untrust	10.5.2.6	8.8.8.8	8.8.8.8	0	ping	allow	Outbound	n/a	490	
05/23 12:05:59	start	web	untrust	10.5.2.5	77.247.109.201	77.247.109.201	0	icmp	allow	Outbound	n/a	451	
05/23 12:05:36	end	web	untrust	10.5.2.2	92.118.160.37	92.118.160.37	0	icmp	allow	Outbound	aged-out	113	
05/23 12:05:31	start	web	untrust	10.5.2.2	92.118.160.37	92.118.160.37	0	icmp	allow	Outbound	n/a	113	
05/23 12:01:29	end	web	web	10.5.2.2		10.16.2.3	80	incomplete	allow	EW	aged-out	288	
05/23 12:00:14	end	web	untrust	10.5.2.5	206.189.86.188	206.189.86.188	0	icmp	allow	Outbound	aged-out	122	

Notice that the web-browsing traffic is being denied but the pings are allowed via a different rule.

→ Navigate to the Policies tab and look at the **Outbound-deny** rule Action column.

Name	Tags	Type	Source				Destination		Rule Usage			Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit			
1 to-guestbook-sec-pol...	none	universal	¶ untrust	any	any	any	¶ web	any	5	2019-05-23 11:27:54	2019-05-23 11:01:23	any	service-http	Allow
2 to-wordpress-sec-pol...	none	universal	¶ untrust	any	any	any	¶ web	any	2	2019-05-23 12:13:39	2019-05-23 11:48:47	any	TCP8888	Allow
3 EW	none	intrazone	¶ web	any	any	any	(intrazone)	any	57	2019-05-23 11:43:47	2019-05-23 11:01:23	dns	any	Allow
4 Outbound-deny	none	universal	¶ web	any	any	any	¶ untrust	any	52	2019-05-23 12:06:11	2019-05-23 11:43:49	ssh	any	Deny
5 Outbound	none	universal	¶ web	any	any	any	¶ untrust	any	311	2019-05-23 12:11:59	2019-05-23 11:10:53	any	any	Allow
6 default-deny-all	none	universal	any	any	any	any	any	any	1	2019-05-23 11:24:34	2019-05-23 11:24:34	any	any	Deny

The **Outbound-Deny** rule is blocking select traffic and providing an extra level of visibility. Now it is clear why the web traffic failed.

End of Activity 9

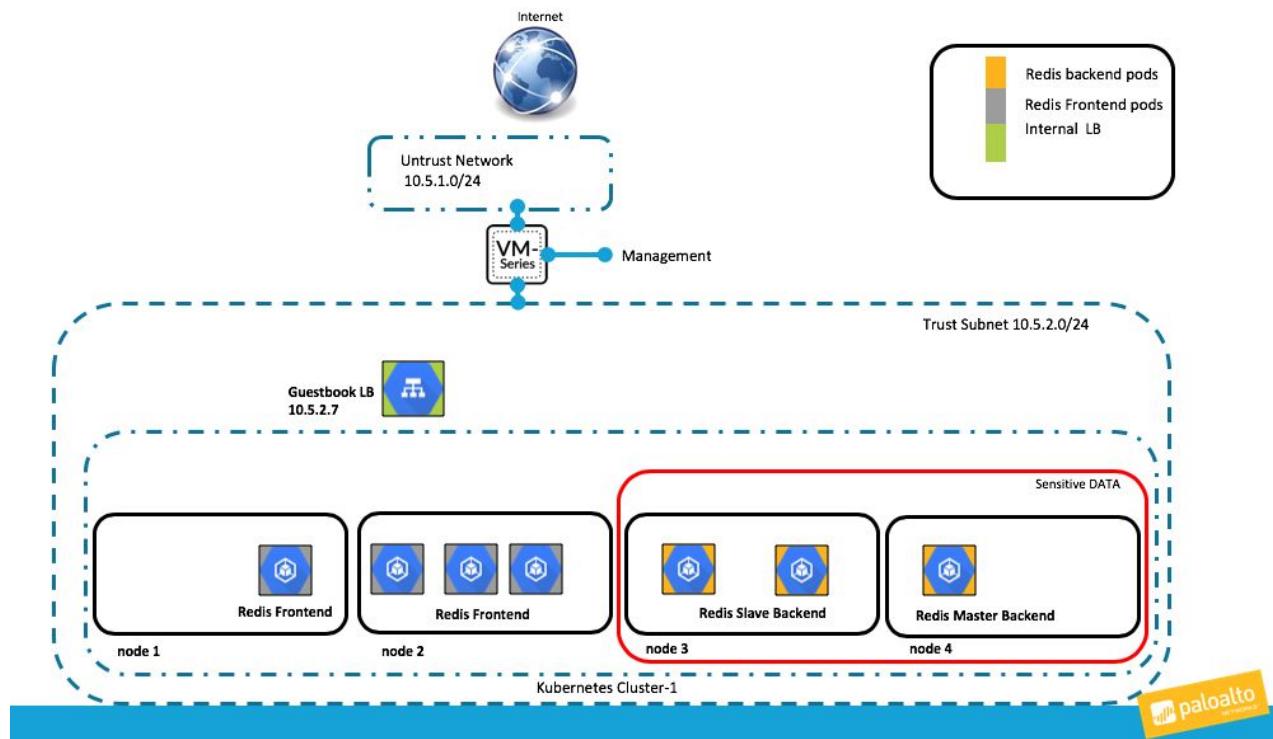
Activity 10 – Investigate Inter Node-Pool traffic

In this activity, you will:

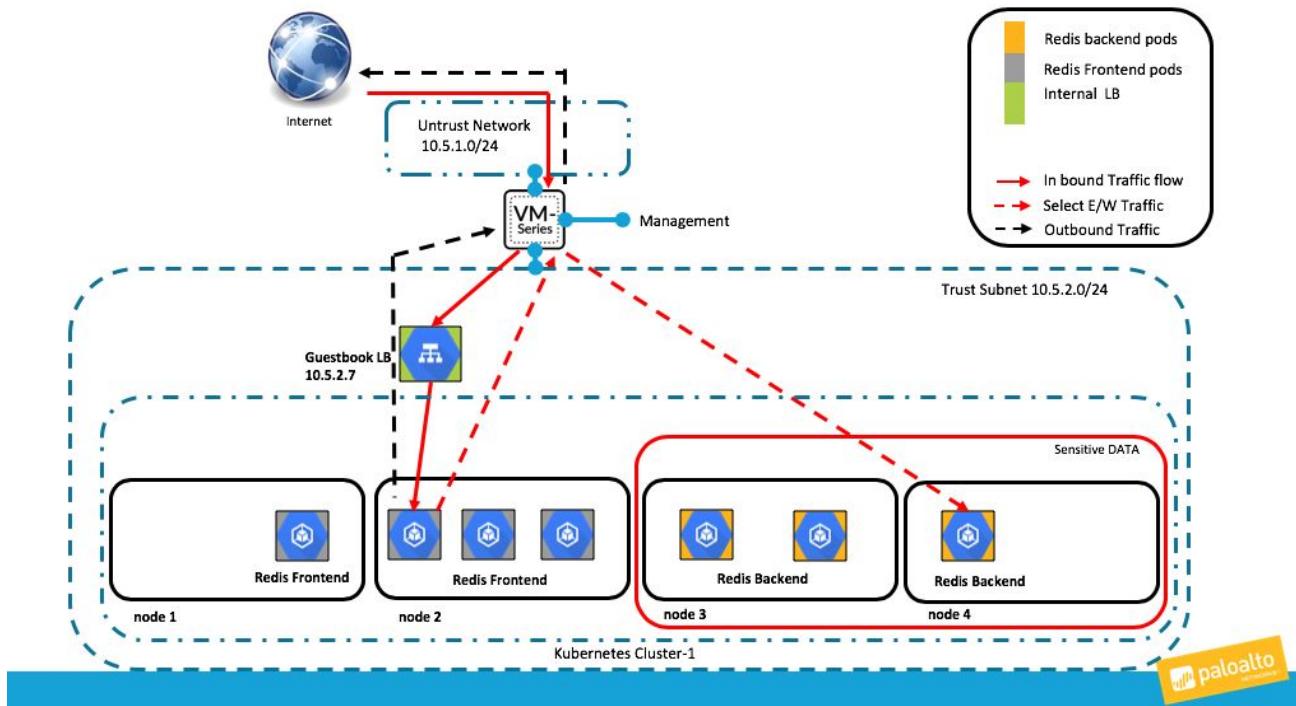
- **Investigate how Inter Node Traffic is being routed through the firewall**
- **Validate that traffic is visible in the Firewall logs**

One of the key challenges when deploying microservices is the lack of visibility of traffic that is flowing between services (or pods) within the cluster. When services are deployed that contain sensitive information it is important to increase the level of visibility. Being able to selectively gain a higher level of security over the cloud native port/protocol approaches increases the overall security posture of applications migrated to the cloud.

In this lab, Node Pools are being used to isolate pods that have sensitive information and traffic destined for these pods are being directed to the firewall for visibility. As shown previously the current environment is setup like this:



The following diagram shows how traffic is moving through the lab environment:



Task 1 – View Node Pool Setup

Each node has been associated with a Node-Pool during the initial setup. You can see the cluster nodes pools opening the GCP and Navigate to **Kubernetes Engine>Clusters**

→ Click k8s-cluster-1

Name	Location	Cluster size	Total cores	Total memory	Master version	Expiration time	Notifications	Labels
<input checked="" type="checkbox"/> k8s-cluster-1	us-central1-a	4	4 vCPUs	15.00 GB	1.11.8-gke.6	Jun 23, 2019		

→ Scroll down and click to expand each node pool

Legacy authorization: Disabled
 Maintenance window: Any time
 Cloud TPU: Disabled
 Application-layer Secrets Encryption: Disabled
 Node auto-provisioning: Disabled
 Vertical Pod Autoscaling: Disabled
 GKE usage metering: Disabled

Labels: None

Add-ons: None

Permissions: None

Node Pools

Node pools are separate instance groups running Kubernetes in a cluster. You may add node pools in different zones for higher availability, or add node pools of different type machines. To add a node pool, click Edit on the top bar. [Learn more](#)

default-pool (2 nodes, version 1.11.8-gke.6)	
web-tier (2 nodes, version 1.11.8-gke.6)	
+ Add node pool	

Look at the **Kubernetes Labels** section. Each node during deployment was given a label that automatically put it into the appropriate pool.

Name	Value
default-pool	cluster : the-cluster pool : db-pool
web-tier	cluster : the-cluster pool : web-pool

→ Next, click on the **Nodes** tab:

The screenshot shows the Google Cloud Platform interface for the Kubernetes Engine. On the left, there's a sidebar with icons for Clusters, Workloads, Services, Applications, Configuration, and Storage. The 'Clusters' icon is highlighted. In the main area, a cluster named 'k8s-cluster-1' is selected, indicated by a green checkmark. Below the cluster name, there are tabs for 'Details', 'Storage', and 'Nodes'. A red arrow points to the 'Nodes' tab, which is underlined in blue. The 'Details' section contains various configuration details like Master version (1.11.8-gke.6), Endpoint (35.238.209.14), and Node address range (10.16.0.0/14). The 'Storage' section is currently empty.

→ Click on one of the nodes:

This screenshot continues from the previous one, showing the 'Nodes' tab for 'k8s-cluster-1'. The 'Nodes' section is now visible, displaying a list of four nodes. A red arrow points to the first node in the list, 'gke-k8s-cluster-1-default-pool-9e39ce4a-4dsj'. The table has columns for Name, Status, CPU requested, and CPU alloc. All nodes are listed as 'Ready'. The 'Name' column is sorted by ascending name.

Name	Status	CPU requested	CPU alloc
gke-k8s-cluster-1-default-pool-9e39ce4a-4dsj	Ready	671 mCPU	940 mCP
gke-k8s-cluster-1-default-pool-9e39ce4a-qsvw	Ready	772 mCPU	940 mCP
gke-k8s-cluster-1-web-tier-729d6b34-0tgc	Ready	401 mCPU	940 mCP
gke-k8s-cluster-1-web-tier-729d6b34-mwgw	Ready	401 mCPU	940 mCP

→ Click on the **Details Tab** and view the **Pod CIDR** Range for this node.

Cluster	Node pool	Annotations	VM instance	Stackdriver logs
gke-k8s-cluster-1-default-pool-9e39ce4a-4dsj	default-pool	container.googleapis.com/instance_id: 2439816574803486813 node.alpha.kubernetes.io/ttl: 0 volumes.kubernetes.io/controller-managed-attach-detach: true	gke-k8s-cluster-1-default-pool-e39ce4a-4dsj	Kubelet logs, Docker logs, Other logs
Spec				
Pod CIDR 10.16.0.0/24				

You can repeat this for the other nodes and see that the nodes in each Node has a defined range for pod deployments.

Task 2 – View GCP Routing Rules

Now lets see how this is used within GCP to redirect traffic to the firewall.

→ Within GCP, Navigate to **VPC Network > Routes**

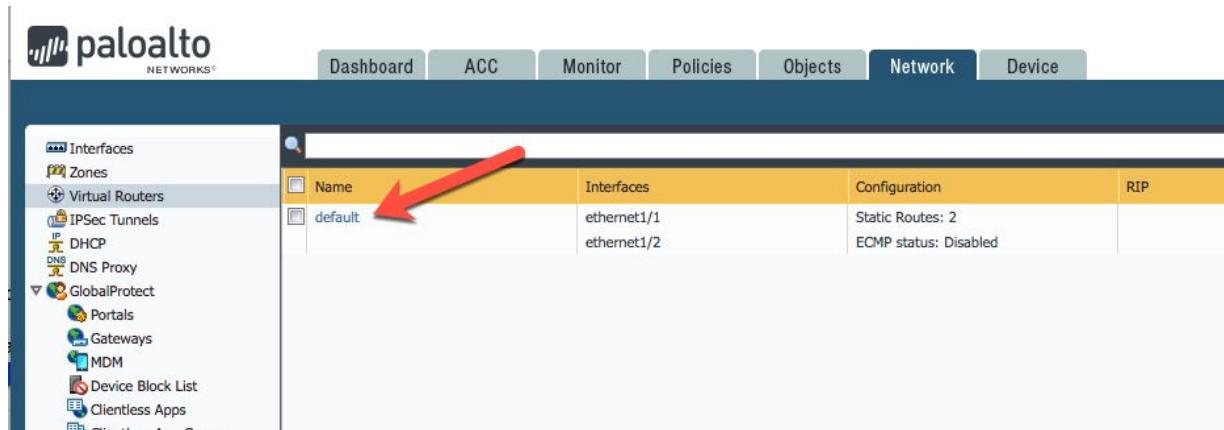
Route	Description	Network	Next Hop	Tier	Target	Trust
default-route-f3cc680ca53608d68	Default local route to the subnetwork 10.174.0.0/20.	10.174.0.0/20	1000	None	Virtual network default	default
default-route-f91937e174dcfbab8	Default local route to the subnetwork 10.170.0.0/20.	10.170.0.0/20	1000	None	Virtual network default	default
gke-k8s-cluster-1-5a0a1222-3c53150e-7e3e-11e9-9fd4-42010a8000a1	k8s-node-route	10.16.0.0/24	1000	None	Instance gke-k8s-cluster-1-default-pool-9e39ce4a-4dsj (zone us-central1-a)	trust
gke-k8s-cluster-1-5a0a1222-3c53150e-7e3e-11e9-9fd4-42010a8000a1	k8s-node-route	10.16.1.0/24	1000	None	Instance gke-k8s-cluster-1-default-pool-9e39ce4a-qsvw (zone us-central1-a)	trust
gke-k8s-cluster-1-5a0a1222-3c53150e-7e3e-11e9-9fd4-42010a8000a1	k8s-node-route	10.16.2.0/24	1000	None	Instance gke-k8s-cluster-1-web-tier-729db634-0tgc (zone us-central1-a)	trust
gke-k8s-cluster-1-5a0a1222-ca8077fb-7e3e-11e9-9fd4-42010a8000a1	k8s-node-route	10.16.3.0/24	1000	None	Instance gke-k8s-cluster-1-web-tier-729db634-mgqw (zone us-central1-a)	trust
route-dbpool-0	route to 16.0 for web-pool	10.16.0.0/24	10	web-tier	Instance firewall1 (zone us-central1-a)	trust
route-dbpool-1	route to 16.1 for web-pool	10.16.1.0/24	10	web-tier	Instance firewall1 (zone us-central1-a)	trust
route-webpool-2	route to 16.2 for db-pool	10.16.2.0/24	10	db-tier	Instance firewall1 (zone us-central1-a)	trust
route-webpool-3	route to 16.3 for db-pool	10.16.3.0/24	10	db-tier	Instance firewall1 (zone us-central1-a)	trust

Observe that we have used route tagging during the deployment to also get routes associated with Nodes so traffic that is being sent between the Node-Pools is getting redirected to the VM-Series Firewall.

Task 3 – View the VM-Series Firewall Routing

As a result of the GCP setup, the routing is setup on the VM-Series Firewall is very straight forward. Let's take a look.

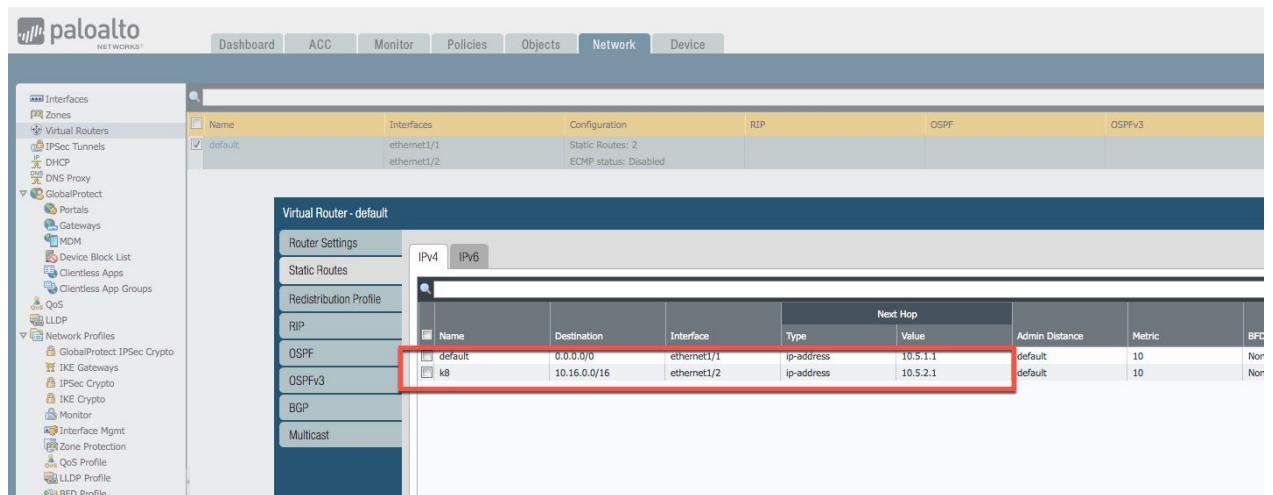
- On the VM-Series Firewall, Navigate to **Network > Virtual Routers** and click on **default**.



The screenshot shows the Network > Virtual Routers page. The left sidebar lists various network components like Interfaces, Zones, and GlobalProtect. The main table has columns for Name, Interfaces, Configuration, and RIP. The 'default' row is selected, highlighted with a red arrow. The 'Interfaces' column shows 'ethernet1/1' and 'ethernet1/2'. The 'Configuration' column shows 'Static Routes: 2' and 'ECMP status: Disabled'.

Name	Interfaces	Configuration	RIP
default	ethernet1/1 ethernet1/2	Static Routes: 2 ECMP status: Disabled	

- Click on **Static Routes**



The screenshot shows the Virtual Router - default configuration page. The left sidebar includes options like Router Settings, Static Routes, Redistribution Profile, RIP, OSPF, OSPFv3, BGP, and Multicast. The main area shows the 'Static Routes' tab selected. A red box highlights the 'Static Routes' table, which lists two routes: 'default' (Destination 0.0.0.0/0, Interface ethernet1/1, Next Hop 10.5.1.1) and 'k8' (Destination 10.16.0.0/16, Interface ethernet1/2, Next Hop 10.5.2.1). The table has columns for Name, Destination, Interface, Type, Value, Admin Distance, Metric, and BFD.

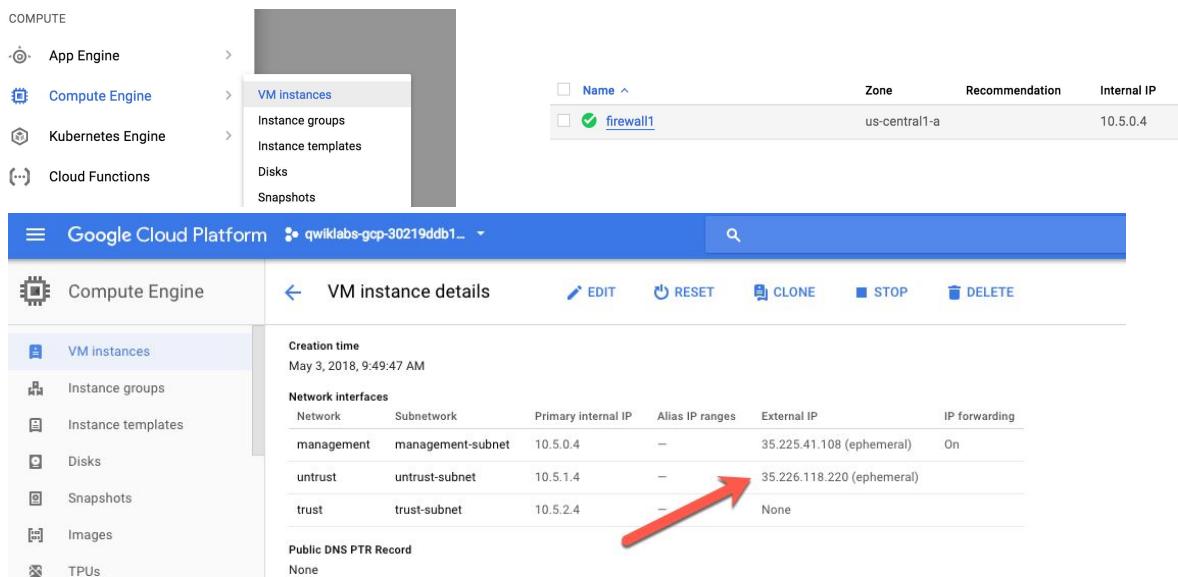
Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD
default	0.0.0.0/0	ethernet1/1	ip-address	10.5.1.1	default	10	Not Configured
k8	10.16.0.0/16	ethernet1/2	ip-address	10.5.2.1	default	10	Not Configured

Notice that there is a **10.16.0.0/16** route that will cover all the Pod CIDRs on the Nodes. This allows the firewall to send all inter pod traffic back to the GCP fabric without the need for SNAT.

Task 4 – Validate North/South and East/West traffic in the firewall logs

First, repeat the steps done in Activity 6, Task 3.

- Navigate to the **Compute Engine > VM Instances** screen. Then click on the firewall and copy the **External IP address** of the **untrust** interface:

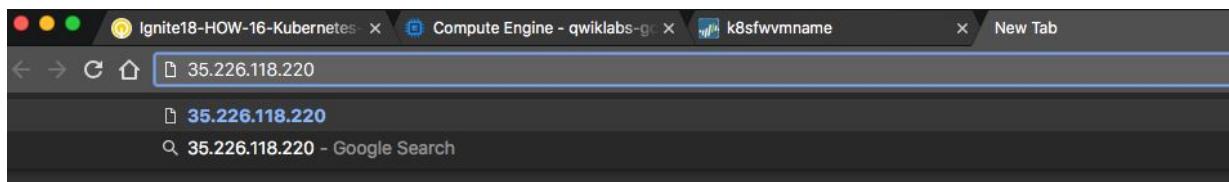


The screenshot shows the Google Cloud Platform Compute Engine interface. In the left sidebar, under the 'Compute' section, 'VM instances' is selected. On the main page, a VM instance named 'firewall1' is displayed. The 'Network interfaces' table shows three interfaces: 'management' (IP: 10.5.0.4), 'untrust' (IP: 10.5.1.4, highlighted with a red arrow), and 'trust' (IP: 10.5.2.4). The 'External IP' column for the 'untrust' interface shows '35.226.118.220 (ephemeral)'. The table also includes columns for 'Creation time' (May 3, 2018, 9:49:47 AM), 'Subnetwork', 'Primary internal IP', 'Alias IP ranges', and 'IP forwarding' (set to 'On').

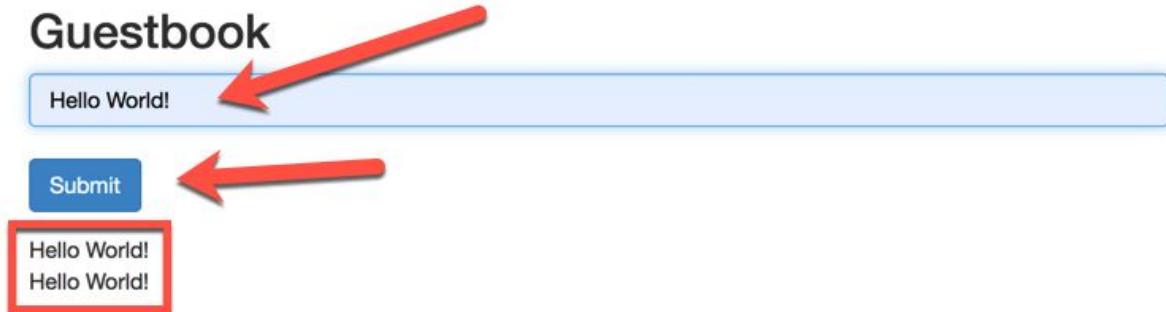
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
management	management-subnet	10.5.0.4	—	35.225.41.108 (ephemeral)	On
untrust	untrust-subnet	10.5.1.4	—	35.226.118.220 (ephemeral)	
trust	trust-subnet	10.5.2.4	—	None	

- In your browser navigate to the untrust-ip address of the firewall:

<http://<firewall untrust External IP>>



- This time when the Guestbook application comes up, enter something in the text field and click Submit.



If the text is echoed below the Submit button, that is showing that the application successfully wrote the entry to the redis backend.

- Navigate back to the Firewall and click on the Monitor Tab

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
06/02 19:07:31	end	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-rst-from-server	5.2k
06/02 19:07:28	end	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-rst-from-server	6.9k
06/02 19:05:59	start	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	n/a	693
06/02 19:05:56	start	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	n/a	678
06/02 19:00:18	drop	untrust	untrust	209.179.6.242		10.5.1.4	443	not-applicable	deny	default-deny-all	policy-deny	58
06/02 18:54:34	end	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-rst-from-server	6.1k
06/02 18:54:29	end	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-rst-from-server	1.8k
06/02 18:53:13	end	web	web	10.16.3.4		10.16.0.10	53	dns	allow	EW	aged-out	652
06/02 18:52:58	end	web	web	10.16.3.4		10.16.0.13	6379	redis	allow	EW	tcp-fin	708
06/02 18:52:44	start	web	web	10.16.3.4		10.16.0.13	6379	redis	allow	EW	n/a	307
06/02 18:52:39	start	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	tcp-rst-from-server	791
06/02 18:52:39	start	web	web	10.16.3.4		10.16.0.10	53	dns	allow	EW	n/a	97
06/02 18:52:38	start	untrust	web	168.149.242.101		10.5.1.4	80	web-browsing	allow	to-guestbook-sec-policy-1	n/a	783

Looking at the logs, it is evident that the firewall is seeing the inbound web traffic and the Redis traffic between the Frontend Pods and the Backend Redis pods. Also notice that the East/West traffic is hitting a specific rule that will give the ability to create an application based rule and also enable Threat analysis to protect the backend pods with more security capabilities than the native cloud ACL based constructs.

End of Activity 10

Conclusion

Congratulations! You have now successfully integrated the Palo Alto Networks VM-Series firewall to gain visibility into North/South traffic entering and leaving the Kubernetes cluster and E/W traffic between a Guestbook Application Frontend and Backend pods. You have also leveraged the Prisma Public Cloud free public APIs to ensure that the deployment is not introducing known CVEs from the repository via the manifest file.