

Hands-On Workshop

Cloud Security for Google Cloud Platform



<http://www.paloaltonetworks.com>

Table of Contents

Activity 0 –Login	3
Task 1 – Log into GCP Console	3
Activity 1 – Launch Deployment Manager Template.....	4
Task 1- Launch Template with Google Cloud Shell	5
Activity 2 – Review VPC and Resource Configurations	10
Task 1 - Review VPC Networks	10
Task 2 - Review Compute Engine	11
Activity 3 - Review PAN-OS WebUI	13
Task 1 - Access the firewall.....	14
Task 2 – Review the Networks and Polices tab.....	15
Task 3 – (Optional Not Needed for Qwiklab UTD) License the firewall [BYOL].....	18
Activity 4 – Safely Enable Applications.....	20
Task 1 - Verify Static Content on Web Server	20
Task 2 - Verify Dynamic Content on Web Server	21
Activity 5 - Safe Application Enablement.....	22
Task 1 - Attempt to SSH from the web server to the DB server.....	22
Task 2 - Trigger the SQL brute force attack and review logs	22
Task 3 - Lab Cleanup.....	24
Activity 6 – LAB 2-- Deploy Firewalls with Load Balancer	25
Task 1 –Launch Template with Google Cloud Shell	27
Activity 7 – Review the Deployment	31
Task 1 - Review VPC Networks	31
Task 2 - Review Compute Engine	32
Activity 8 - Review Firewall Configuration	35
Task 1 - Access the firewall.....	35
Task 2 – Review Monitor Tab.....	38
Activity 9 – Complete and Verify Firewall with Load Balancer Configuration .	40
Task 1 – Complete the firewall configuration	40
Task 2 – Verify the Configuration	44
Task 3 - Log X-Forwarded-For (Bonus).....	46

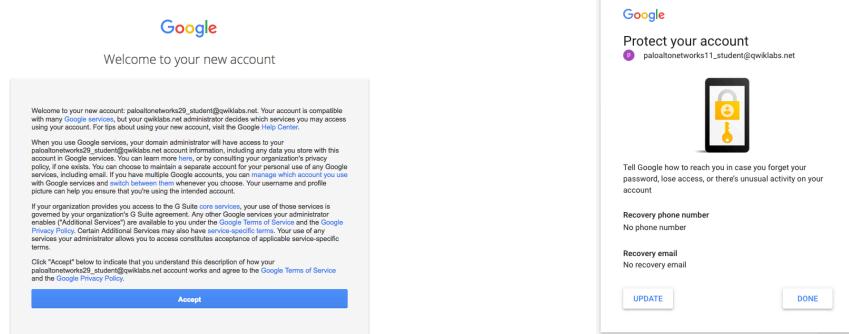
Activity 0 –Login

In this activity, you will:

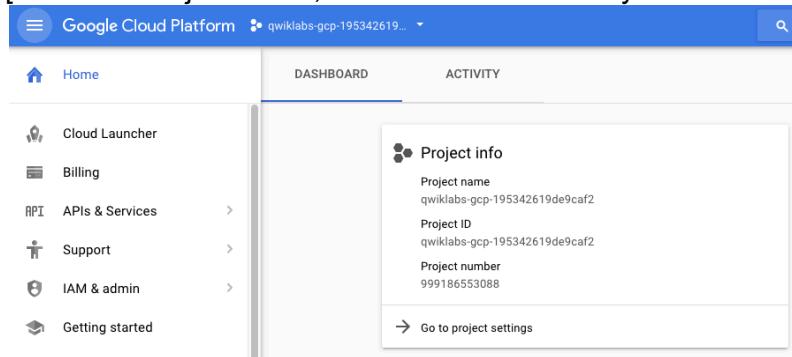
Log in to the GCP Console using the account provided.

Task 1 – Log into GCP Console

- Step 1:** Browse to <http://console.cloud.google.com> and login. If you do not have an account for GCP browse here <https://console.cloud.google.com/freetrial>
- Step 2:** Accept the Service agreement and click **Done** to login to the account. You can agree to the updated Term and Services as well.



- Step 3:** Once you have successfully logged in, you should have full access to the Google Cloud Platform console. [Note that Project name, ID and number will vary from the screenshots.]



End of Activity 0

Activity 1 – Launch Deployment Manager Template

GCP Deployment Manager Templates, are Python (or Jinja) files that can launch nearly all GCP resources including VPCs, subnets, security groups, route tables, plus many more. Templates are used for ease of deployment.

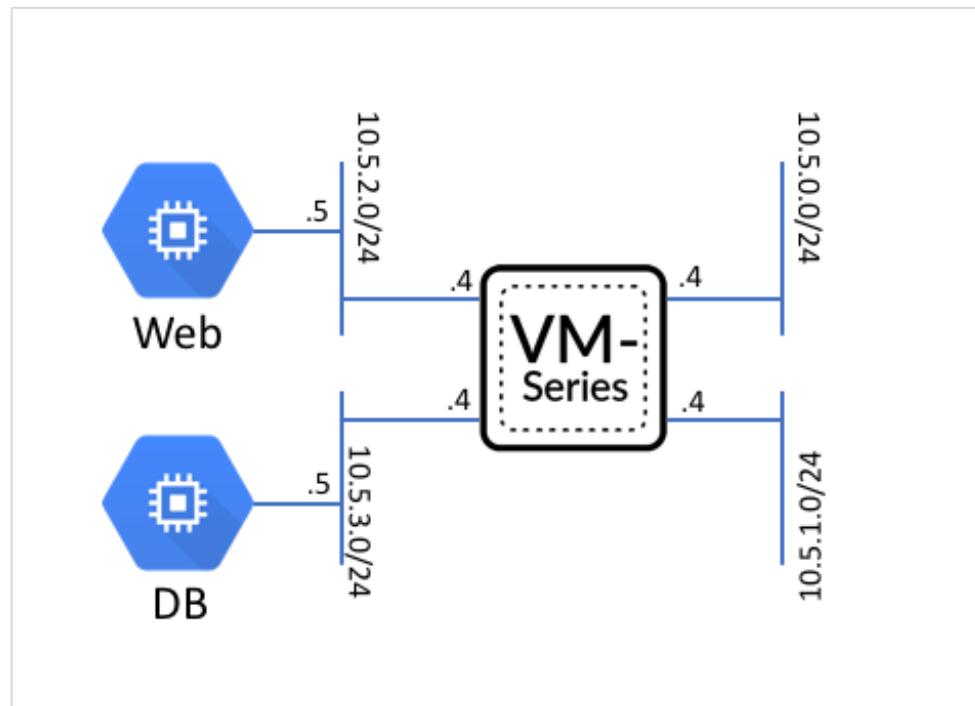
This lab will demonstrate how to deploy a sample template that launches everything that is shown below. This includes, a WordPress server, a MySQL server, a VM-Series firewall and the subnets. In addition, the firewall uses a native bootstrapping feature that allows for additional configuration of the firewall (such as routes, security policies, etc.) Once the sample template has been deployed, the network topology should align with the following:

For more information on Templates refer to Google's documentation

<https://cloud.google.com/deployment-manager/docs/how-to#adding-templates>

There are also many sample templates available here

<https://github.com/GoogleCloudPlatform/deploymentmanager-samples/tree/master/templates>



Template Instances used

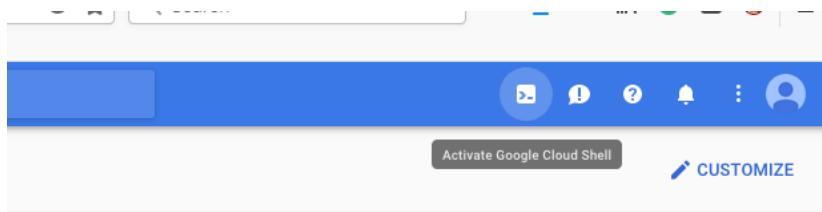
When using the sample template in this lab, the following machine types are used:

Instance name	Machine Type
WordPress Web Server	f1-micro
WordPress DB Server	f1-micro
VM Series Firewall	n1-standard-4

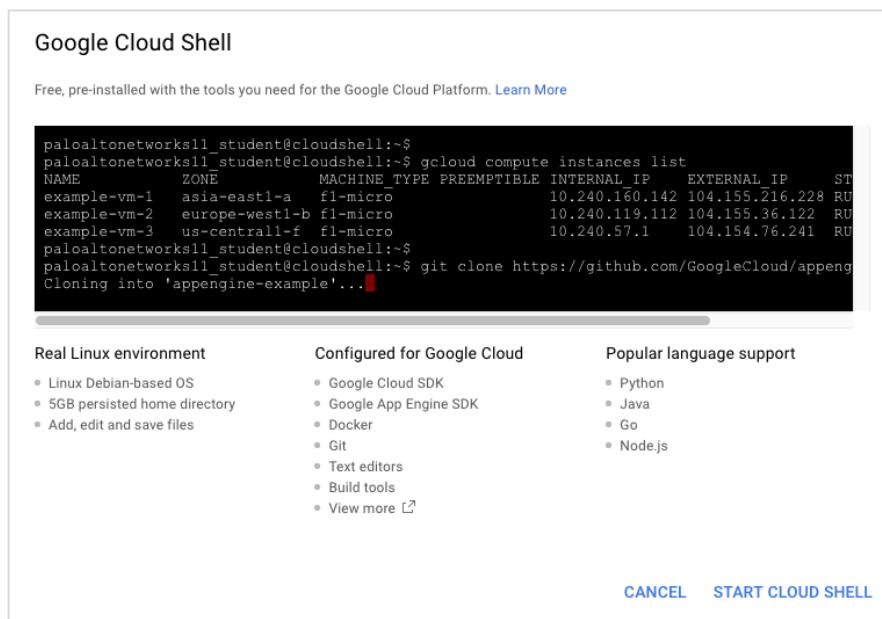
Task 1- Launch Template with Google Cloud Shell

Google Cloud Shell is a shell environment for managing resources hosted on Google Cloud Platform. You can perform some basic operations in Google Cloud Shell. You can learn more about it [here](#).

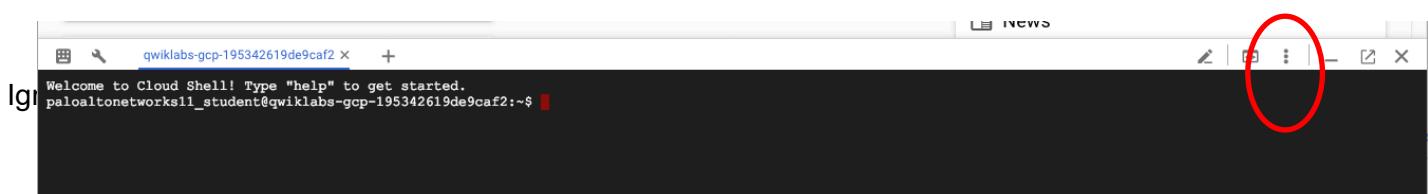
Step 1: Open Google Cloud Shell using the button on the upper right-hand corner.



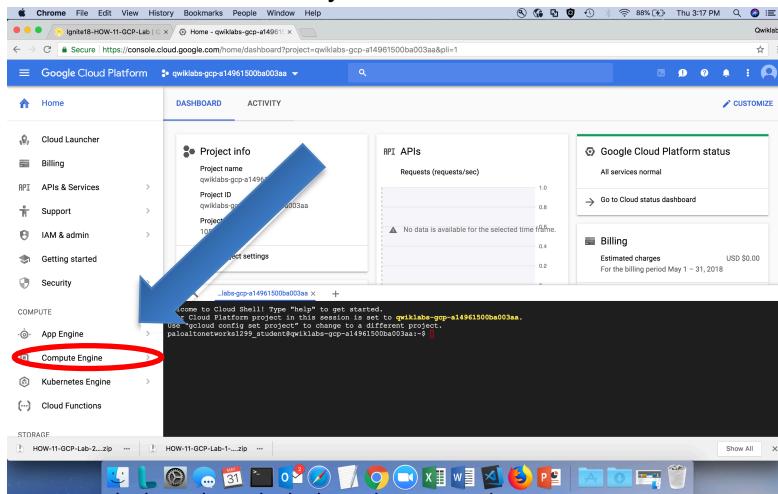
Step 2: Click **Start Cloud Shell** to open the Cloud Shell window below. Note, this could take a few minutes for Google Cloud Shell to be ready.



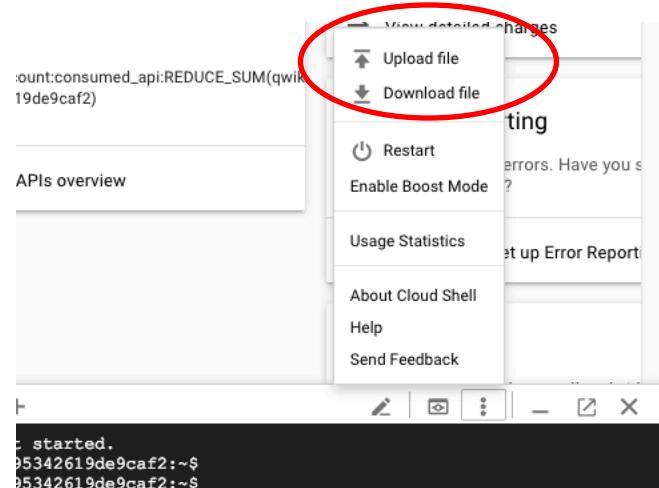
Once cloud shell is started and open click on the 3-dot ellipse to upload the deployment files



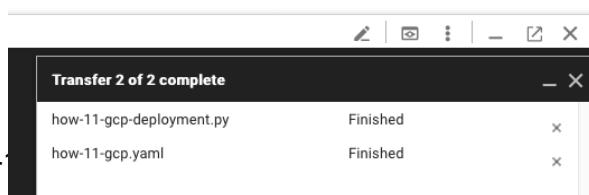
If you **DO NOT SEE** the 3-dot ellipse and your screen looks like this. Click on Compute Engine and the screen will reformat and you will see the 3-dots.



Step 3: Click the **Upload File** in upper right-hand corner of the Google Cloud Shell console.



Step 4: Upload the **how-11-gcp-lab1.yaml** and **how-11-gcp-lab1.py** file. Then close the Transfer window.



Step 5: In Cloud Shell prompt, you can use the **ls** command to confirm files have been uploaded.

```
paloaltonetworks29_student@qwiklabs-gcp-10607a6a0e3e9206:~$ ls  
how-11-gcp-deployment.py  how-11-gcp.yaml  README-cloudshell.txt
```

Step 6: Create a deployment using the following gcloud command:

```
gcloud deployment-manager deployments create <your-last-name> --config how-11-gcp-lab1.yaml
```

We recommend using your last name as the deployment name just for easy identification. You can use any name. This will run the deployment for about 3minutes. However, the firewall is still building the overall process take about 10-13 minutes.

```
paloaltonetworks30_student@qwiklabs-gcp-da84b98801115f1:~$ gcloud deployment-manager deployments create your-last-name --config how-11-gcp.yaml  
The fingerprint of the deployment is _v-6oMTxFQlbaeRD9B9Gsg==  
Waiting for create [operation-1524181038286-56a3c0d5c44b2-92b286a5-73bf7f29]...\\
```

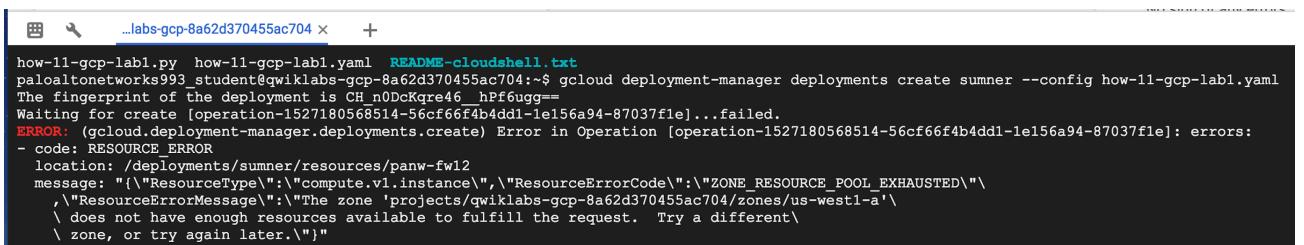
Step 7: When the deployment is completed, you will see the creation completed message for each operation.

```
paloaltonetworks31_student@qwiklabs-gcp-a04fd96beb99bb7:~$ gcloud deployment-manager deployments  
The fingerprint of the deployment is ShaykNSEu0viVd34sAXgA==  
Waiting for create [operation-1524186866688-56a3d68c2a002-54964a6b-a0f86b63]...done.  
Create operation operation-1524186866688-56a3d68c2a002-54964a6b-a0f86b63 completed successfully.  
NAME          TYPE      STATE    ERRORS  INTENT  
db-firewall90  compute.v1.firewall  COMPLETED  []  
db-network90   compute.v1.network  COMPLETED  []  
db-route90     compute.v1.route   COMPLETED  []  
db-subnet90    compute.v1.subnetwork  COMPLETED  []  
dbserver90     compute.v1.instance  COMPLETED  []  
mgmt-firewall90  compute.v1.firewall  COMPLETED  []  
mgmt-network90  compute.v1.network  COMPLETED  []  
mgmt-subnet90   compute.v1.subnetwork  COMPLETED  []  
panw-fw90       compute.v1.instance  COMPLETED  []  
public-firewall90  compute.v1.firewall  COMPLETED  []  
public-network90  compute.v1.network  COMPLETED  []  
public-subnet90   compute.v1.subnetwork  COMPLETED  []  
web-firewall90   compute.v1.firewall  COMPLETED  []  
web-network90    compute.v1.network  COMPLETED  []  
web-route90      compute.v1.route   COMPLETED  []  
web-subnet90     compute.v1.subnetwork  COMPLETED  []  
webservice90     compute.v1.instance  COMPLETED  []  
paloaltonetworks31_student@qwiklabs-gcp-a04fd96beb99bb7:~$
```

NOTE: If you receive a resource failure stating “ZONE_RESOURCE_POOL_EXHAUSTED”. You must delete your Deployment Manager Installation before trying again. To delete the deployment, use the command below in the cloud shell.

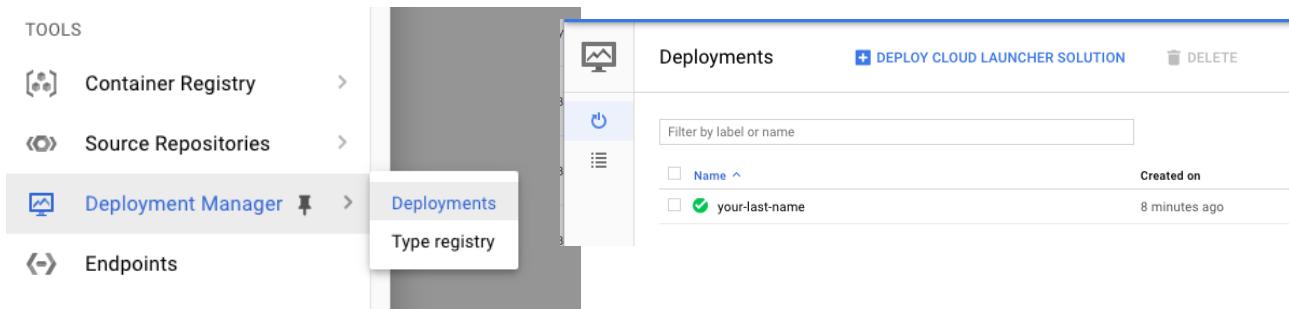
```
gcloud deployment-manager deployments delete <your-last-name>
```

Screen Shot of Resource Error Below

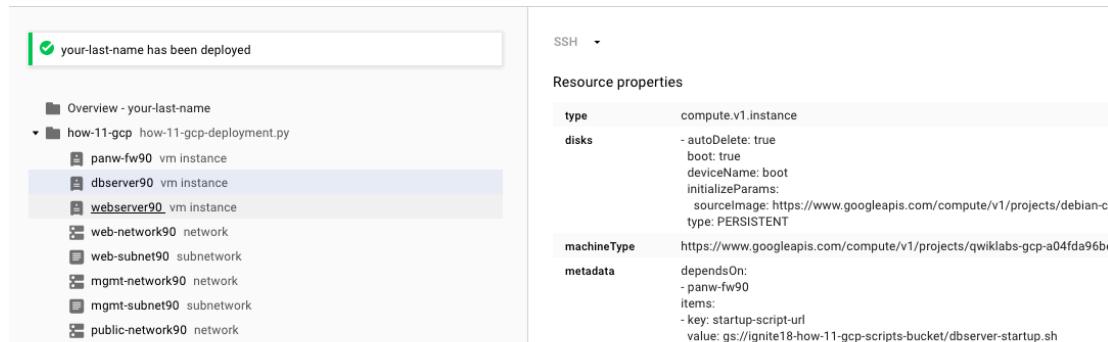


```
...labs-gcp-8a62d370455ac704 x +  
how-11-gcp-lab1.py how-11-gcp-lab1.yaml README-cloudshell.txt  
palcalonetworks993_student@gwklabs-gcp-8a62d370455ac704:~$ gcloud deployment-manager deployments create summer --config how-11-gcp-lab1.yaml  
The fingerprint of the deployment is CH_n0DcKqre46_hPf6ugg=  
Waiting for create [operation-1527180568514-56cf66f4b4dd1-1e156a94-87037f1e]...failed.  
ERROR: (gcloud.deployment-manager.deployments.create) Error in Operation [operation-1527180568514-56cf66f4b4dd1-1e156a94-87037f1e]: errors:  
- code: RESOURCE_EXHAUSTED  
  location: /deployments/summer/resources/panw-fw12  
  message: "{\"ResourceType\":\"compute.v1.instance\",\"ResourceErrorCode\":\"ZONE_RESOURCE_POOL_EXHAUSTED\"}  
  \"ResourceErrorMessage\":\"The zone 'projects/gwklabs-gcp-8a62d370455ac704/zones/us-west1-a'\\  
  \\ does not have enough resources available to fulfill the request. Try a different\\  
  \\ zone, or try again later.\"}"
```

Step 8: You can also go to the Deployment Manager > Manager service to view the deployment.



Step 9: Click the deployment that you have created and review the items that are created by the deployment manager.



This screenshot shows the 'your-last-name' deployment details. At the top, a success message says 'your-last-name has been deployed'. The left pane is a tree view of resources: Overview - your-last-name, how-11-gcp how-11-gcp-deployment.py, panw-fw90 vm instance, dbserver90 vm instance, webserver90 vm instance, web-network90 network, web-subnet90 subnetnetwork, mgmt-network90 network, mgmt-subnet90 subnetnetwork, public-network90 network. The 'webserver90' node is currently selected. The right pane shows 'Resource properties' for the selected resource. The properties listed are:

type	compute.v1.instance
disks	- autoDelete: true boot: true deviceName: boot initializeParams: sourceImage: https://www.googleapis.com/compute/v1/projects/debian-c type: PERSISTENT
machineType	https://www.googleapis.com/compute/v1/projects/qwklabs-gcp-a04fda96b
metadata	dependsOn: - panw-fw90 items: - key: startup-script-url value: gs://ignite18-how-11-gcp-scripts-bucket/dbserver-startup.sh

Custom Scripts/Linux Extensions

The template deploys Linux extensions to configure the firewall, web server (with Apache and WordPress) and database server (MySQL). Linux extensions are resources that can be used to configure Linux VMs. Each custom script downloads and runs a specific script (found in the Github repo) that configures a specific VM. The web-vm-custom script configures the firewall and the web server. The db-vm-custom script configures the database server

End of Activity 1

Activity 2 – Review VPC and Resource Configurations

In this activity, you will:

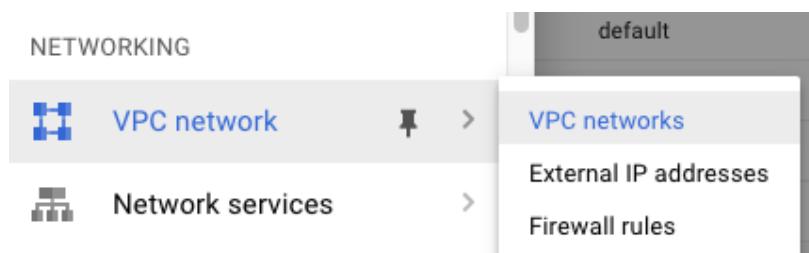
Review the VPC created with Deployment Manager Template

Review the GCE instances and the configuration created

Task 1 - Review VPC Networks

Let's review all the components we have launched in the VPC based on the deployment manager file.

Step 1: The VPC networks can be accessed via **VPC Networks > VPC Networks**. There you should see all networks created in your project:



Step 2: The VPC networks created by the deployment will have a random two-digit number to it. The **default** network is created by default.

Name	Region	Subnets	Mode	IP addresses ra
db-network90	1	Custom		
us-west1	db-subnet90		10.5.3.0/24	
default	15	Auto		
us-central1	default		10.128.0.0/20	
europe-west1	default		10.132.0.0/20	
us-west1	default		10.138.0.0/20	

Step 3: Three networks are created by the deployment. They are **db-network##**, **mgmt.-network##**, **public-network##** and **web-network##**.

mgmt-network90
us-west1
public-network90
us-west1
web-network90
us-west1

Note: Each network corresponds to an interface on the firewall. Although, you can create multiple subnets in a single network, a VM instance cannot have more than one interface on the same network.

Step 4: Click on the **Firewall rules** to review the rules that are created by the deployment.

The screenshot shows the GCP Firewall rules page. On the left, there is a sidebar with the following options: VPC network, VPC networks, External IP addresses, Firewall rules (which is selected and highlighted in blue), and Routes. On the right, there is a table listing three firewall rules:

	Rule Name	Action	IP Ranges	Protocols
<input type="checkbox"/>	mgmt-firewall90	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,443
<input type="checkbox"/>	public-firewall90	Apply to all	IP ranges: 0.0.0.0/0	tcp:80,221,222
<input type="checkbox"/>	web-firewall90	Apply to all	IP ranges: 0.0.0.0/0	tcp, udp, 1 more

Task 2 - Review Compute Engine

We will review the VM instances created by the deployment in this task.

Step 1: Go to the **Compute Engine > VM instances**. There are at least 3 instances created by in this deployment, Web server, a DB server and a VM-series firewall.

Name	Zone	Recommendation	Internal IP	External IP	Connect
<input checked="" type="checkbox"/> dbserver90	us-west1-a		10.5.3.5	None	SSH <input style="width: 20px; height: 20px;" type="button" value="..."/>
<input checked="" type="checkbox"/> panw-fw90	us-west1-a		10.5.0.4	35.203.136.122	SSH <input style="width: 20px; height: 20px;" type="button" value="..."/>
<input checked="" type="checkbox"/> webserver90	us-west1-a		10.5.2.5	None	SSH <input style="width: 20px; height: 20px;" type="button" value="..."/>

Step 2: Click the **panw-fw##** instance to view the details.

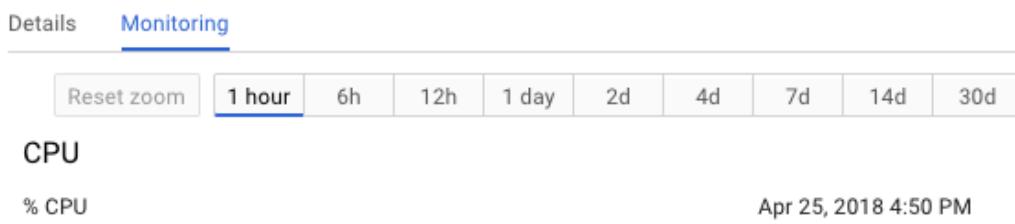
The screenshot shows the 'VM instance details' page for a VM named 'panw-fw90'. At the top, there are buttons for EDIT, RESET, CLONE, STOP, and DELETE. Below the title, there are two tabs: 'Details' (which is selected) and 'Monitoring'. Under the 'Details' tab, it shows the VM name 'panw-fw90'. It has sections for 'Remote access' (SSH, Connect to serial console, Enable connecting to serial ports checked), 'Logs' (Stackdriver Logging, Serial port 1 (console), More), and a summary table of network interfaces.

Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
mgmt-network82	mgmt-subnet82	10.5.0.4	—	35.203.170.133 (ephemeral)	On
public-network82	public-subnet82	10.5.1.4	—	35.185.255.13 (ephemeral)	
web-network82	web-subnet82	10.5.2.4	—	None	
db-network82	db-subnet82	10.5.3.4	—	None	

Step 3: Note that there are four network interfaces created for the firewall. The two external IP addresses will be used in the next task and we will come back here to get these two IPs.

Network interfaces					
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
mgmt-network82	mgmt-subnet82	10.5.0.4	—	35.203.170.133 (ephemeral)	On
public-network82	public-subnet82	10.5.1.4	—	35.185.255.13 (ephemeral)	
web-network82	web-subnet82	10.5.2.4	—	None	
db-network82	db-subnet82	10.5.3.4	—	None	

Step 4: Click the **Monitoring** tab to review some of the basic metrics monitored by GCP. Note that this VM is quite new, so you may not see a lot of data at this point.



Note: The VM-Series firewall on GCP can publish native PAN-OS metrics to Stackdriver, which you can use to monitor the firewalls. These metrics allow you to assess performance and usage patterns that you can use to take action for launching or terminating instances of the VM-Series firewalls. We will not go into the details at this point but you can discuss with instructor if you want to know more about how to enable Stackdriver monitoring on the VM-Series firewall.

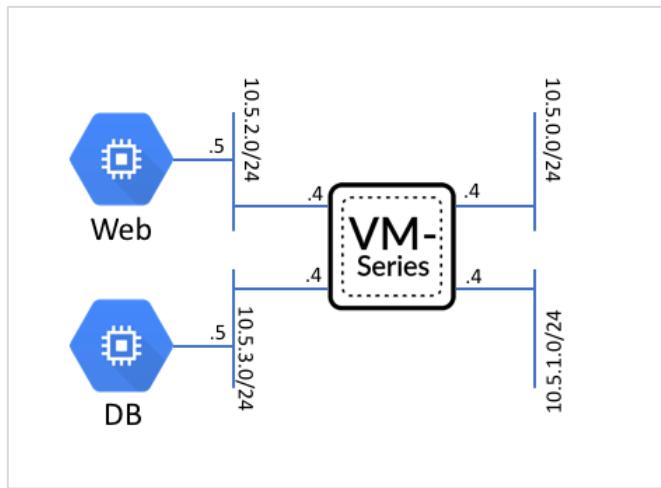
- Step 5:** Go to **VM Instances** and select the **dbserver##** instance to review the details for that instance. Under the network interfaces, note that there is no public IP for the dbserver.

Network interfaces					
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
db-network82	db-subnet82	10.5.3.5	—	None	Off

- Step 6:** Go to **VM Instances** and select the **webserver##** instance to review the details for that instance. Under the network interfaces, note that there is no public IP for the webserver as well.

Network interfaces					
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
web-network82	web-subnet82	10.5.2.5	—	None	Off

All of the VPC configuration should match the topology shown previously:



End of Activity 2

Activity 3 - Review PAN-OS WebUI

In this activity, you will:

- Login to the VM-Series firewall
- Review key portions of the firewall configurations

Task 1 - Access the firewall

Step 1: Once the template deployment is complete, the firewall will show a green checkmark indicating it is running. The firewall may be still executing the bootstrap function.

NOTE: Bootstrapping a VM-Series firewall takes approximately 15 minutes. So once the template has been deployed successfully, it may be a while before the firewall is up and you are able to log into the firewall.

Step 2: Identify the External IP address in the mgmt-network##, that will be the public IP where you can access the firewall on.

Network interfaces

Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
mgmt-network82	mgmt-subnet82	10.5.0.4	—	35.203.170.133 (ephemeral)	On
public-network82	public-subnet82	10.5.1.4	—	35.185.255.13 (ephemeral)	

In a new browser tab, open a <https://> using the mgmt external IP address.

Step 3: You should now be able to login to the firewall using:

username: **paloalto**

password: **Pal0Alt0@123**

Welcome

Welcome to PAN-OS 8.1!

With this release Palo Alto Networks introduces a set of new features that offer richer security controls and operational simplicity to help you protect your users and data everywhere. Some of the highlights in version 8.1 are:

- Comprehensive Security in the Cloud**—Secure your deployments in more public cloud environments and leverage cloud native services.
- Deploy the VM-Series firewall on Google Cloud Platform and directly from Microsoft Azure Security Center, and natively publish custom PAN-OS metrics to Azure Application Insights and Google StackDriver for monitoring and automation.
- Deploy the Panorama™ virtual appliance on AWS and Azure. For deployment flexibility, Panorama virtual appliances now support all three modes—Management only, Panorama, and Dedicated Log Collector.

Rule Usage Tracking—Keep your rulebase current by tracking rule usage. Rule usage information helps you identify obsolete rules and eliminate unnecessary security gaps.

Device Monitoring on Panorama—Proactively track resource utilization, environmental conditions, and other key operational metrics over time and in bulk across large deployments to quickly identify potential issues for devices operating outside the normal range.

Serviceability of Content Updates—View a list of applications modified in a content release and assess how those changes impact your security policy rules. You can also enforce a threshold timer when deploying content updates to managed firewalls from Panorama.

HTTP Header Insertion—Use HTTP Headers to control access to sanctioned enterprise SaaS application accounts while blocking access to unauthorized domains. PAN-OS includes predefined headers that make it easier to control access to applications such as Facebook, G Suite, and LinkedIn.

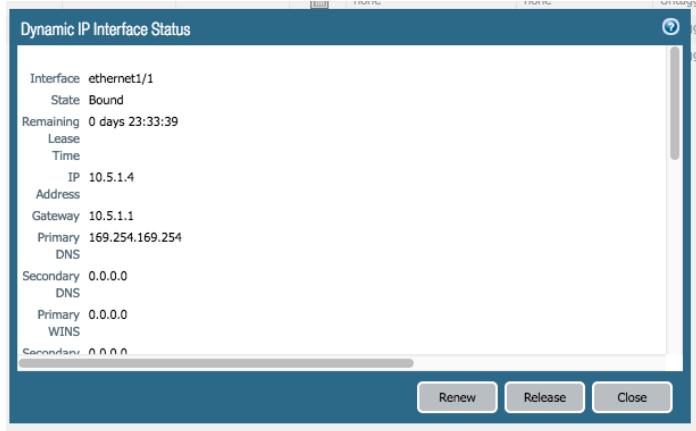
Do not show again Close

Task 2 – Review the Networks and Policies tab

Step 1: Click the **Networks** tab to see the interfaces to zone mappings:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3	Allow-HTTPS	Up	Dynamic-DHCP Client	default	Untagged	none	Untrust		
ethernet1/2	Layer3	Allow-HTTPS	Up	Dynamic-DHCP Client	default	Untagged	none	Web		
ethernet1/3	Layer3	Allow-HTTPS	Up	Dynamic-DHCP Client	default	Untagged	none	Db		
ethernet1/4			Up	none	none	Untagged	none	none		
ethernet1/5			Up	none	none	Untagged	none	none		
ethernet1/6			Up	none	none	Untagged	none	none		
ethernet1/7			Up	none	none	Untagged	none	none		

Step 2: Click the **Dynamic-DHCP-Client** under the IP Address to see the status of each interface.



Step 3: In the **Policies** tab you can review the security policies:

The screenshot shows the "Palo Alto Networks" web interface with the "Policies" tab selected. On the left, there is a navigation tree with categories like Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. Below the tree is a "Tag Browser" panel showing a single item: "Tag(#)" Rule none (6) 1-6. The main area displays a table of security rules:

Name	Tags	Type	Zone	Source			Destination			Rule Usage		
				Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	
SSH Inbound	none	universal	Untrust	any	any	any	Web	any	-	-	-	
SSH 221-222 Inbound	none	universal	Untrust	any	any	any	Db	any	0	-	-	
Allow all ping	none	universal	any	any	any	any	Web	any	0	-	-	
Web browsing	none	universal	Untrust	any	any	any	Web	any	60	2018-02-28 13:03:26	2018-02-28 13:03:26	
Allow all outbound	none	universal	Db	any	any	any	Untrust	any	35239	2018-02-28 13:12:35	2018-02-28 13:12:35	
Web to DB	none	universal	any	web-object	any	any	any	db-object	0	-	-	
Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	4	2018-02-27 12:31:51	2018-02-27 12:31:51	
Interzone-default	none	interzone	any	any	any	any	any	any	0	-	-	

At the bottom of the page, there is a footer bar with links for Object: Addresses, Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter, and a language selection dropdown. The URL https://35.224.8.98/# is also visible.

These policies are defined to allow ssh access on ports 221 and 222 to the web and db server respectively (for troubleshooting purposes), secures N/S traffic and E/W traffic between zones.

Step 4: Select NAT on the left menu, review the NAT policies allow for ssh access to the web and db servers as well as directing web traffic to the web server only. There is also a rule for source NAT from web and db servers to the outside world.

Name	Tags	Original Packet					Translated Packet		
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1 Web SSH	none	Untrust	Untrust	any	any	10.5.1.4	service-tcp-2...	dynamic-ip-and-port ethernet1/2	destination-translation address: web-object port: 22
2 DB SSH	none	Untrust	Untrust	any	any	10.5.1.4	service-tcp-2...	dynamic-ip-and-port ethernet1/3	destination-translation address: db-object port: 22
3 WordPress NAT	none	Untrust	Untrust	any	any	10.5.1.4	service-http	dynamic-ip-and-port ethernet1/2	destination-translation address: web-object port: 80
4 Outbound nat	none	any	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

Step 5: Check to make sure that the Dynamic Updates installed during the bootstrap process. You should see similar content in your Dynamic Updates area.

Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation
8024-4749	panupv2-all-contents-8024-4749.dms	Contents	Full		2018/05/24 10:50:02 PDT		✓		
▼ Applications and Threats Last checked: never Schedule: Every Wednesday at 01:02 (Download only)									
▼ GlobalProtect Clientless VPN Last checked: never Schedule: None									
▼ GlobalProtect Data File Schedule: None									

Step 6: If you do not have any dynamic updates or would like to make sure you have the latest Dynamic Updates complete the following. Select the 1.Device Tab in the Firewall. On the left menu screen select 2.Dynamic Updates. Note there are no threat updates. Select 3."Check Now" in the lower left corner of the Primary Screen. 4.Download the latest threat content update. Once downloaded you must select 5.install for the content to be active on your VM-Series FW.

1

2

3

4

5

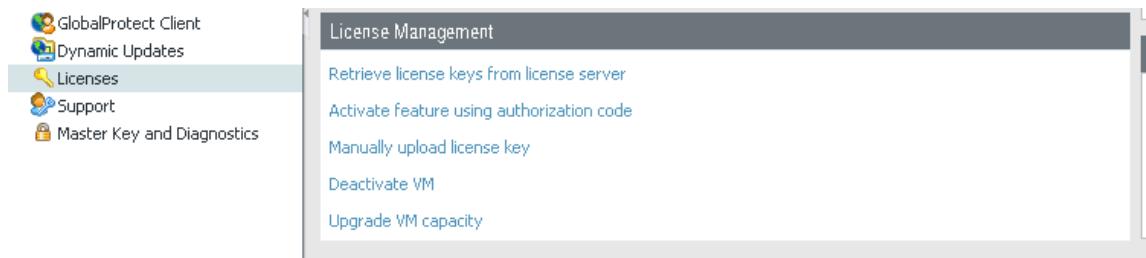
Task 3 – (Optional Not Needed for Qwiklab UTD) License the firewall [BYOL]

Skip to Activity 4 unless otherwise instructed.

If BYOL – Bring Your Own License instance is used, you will need to activate the firewall to fully utilize the all the features. The steps below demonstrate how to license a BYOL firewall instance through a registered Authorization code (provided by the instructor).

Note: PAYG – Pay As You Go licensing model is also available in Google Cloud Platform, where license and subscription fees can be included as part of the charges.

Step 1: Go to the **Device** tab and the **License** node, under the **License Management** widget.



Step 2: Click Activate feature using authorization code.

Step 3: Enter the authorization code if applicable. The firewall will reboot to install the new license. [The authorization code used in the lab will be disabled shortly after this lab.]

End of Activity 3

Activity 4 – Safely Enable Applications

In this activity, you will:

- Generate traffic on the firewall and review the traffic log
- Edit the security policy to allow inter-tier application traffic

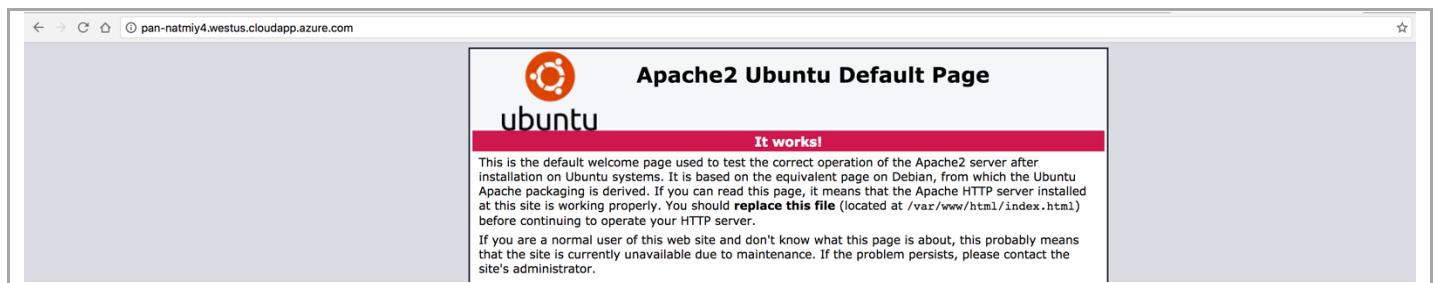
Task 1 - Verify Static Content on Web Server

Step 1: Identify the External IP address of the public-network## for Firewall, that will be the public IP of the web server.

Network interfaces

Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
mgmt-network82	mgmt-subnet82	10.5.0.4	—	35.203.170.133 (ephemeral)	On
public-network82	public-subnet82	10.5.1.4	—	35.185.255.13 (ephemeral)	

Step 2: Using the public-network## external IP on the firewall to access the static content of the webserver and you should see the screenshot below:



Step 3: Check firewall logs under the Monitor tab to verify that the traffic is passing through the firewall:

A screenshot of the Palo Alto Networks Firewall interface. The top navigation bar includes "Dashboard", "ACC", "Monitor" (which is selected), "Policies", "Objects", "Network", and "Device". The left sidebar has sections for "Logs" (selected), "Traffic", "Threat", "URL Filtering", "Wildfire Submissions", "Data Filtering", "HP Match", and "Configuration". The main content area shows a table of traffic logs with columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. Three entries are listed, all related to "app eq web-browsing" and "10.5.1.4" as the destination.

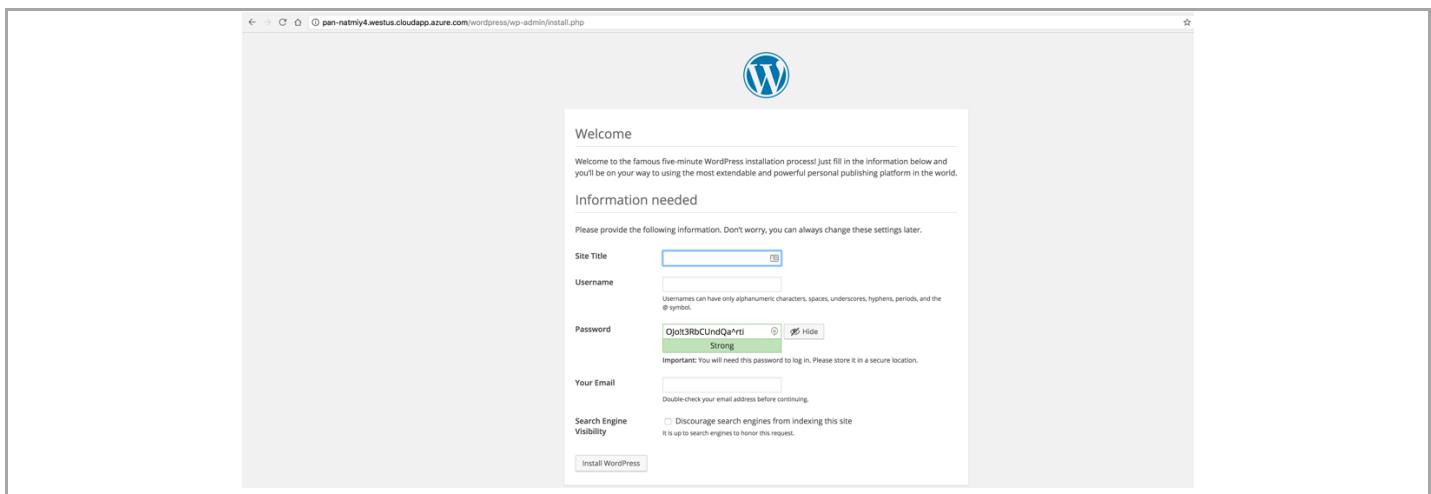
Task 2 - Verify Dynamic Content on Web Server

In this task, you will generate a WordPress content request from your web browser that will trigger a database query to the MySQL server. Like many web-based applications, WordPress uses a backend database to create, store, and retrieve dynamic content. You will use the WordPress application to show exactly this type of behavior and demonstrate how the VM-Series firewall will secure this traffic.

In the browser, go to the WordPress server (<http://public-network-external-IP/wordpress>)

And you should see the WordPress welcome page.

Note: You don't need to actually configure the new WordPress server. In its initial, un-configured state, it will generate the traffic we need to test the VM-Series firewall.



Now, head back to the firewall and verify that the traffic did indeed go through the firewall from web to db:

A screenshot of the Palo Alto Networks Firewall logs interface. The left sidebar shows navigation options like Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The main area is titled "(app eq mysql)". It displays a table of log entries with columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. The table shows four entries corresponding to the MySQL connection activity observed in the previous screenshot.

End of Activity 4

Activity 5 - Safe Application Enablement

In this activity, you will:

- Generate two simulated east/west (web tier to database tier) attacks
- Monitor the firewall logs to see the results of the attacks

Task 1 - Attempt to SSH from the web server to the DB server

This task will simulate a compromised web server that is being used to attack the database. This is a common attack strategy of getting a foothold on the web front-end server and then expanding to the other application tiers with the ultimate goal of accessing all data in the database.

Go to (<http://public-network-external-IP /sql-attack.html>) and simulate a web to db ssh attempt by clicking on the **LAUNCH WEB TO DB SSH ATTEMPT**.

LAUNCH WEB TO DB SSH ATTEMPT

This launches a CGI script that attempts to ssh as root to the db server from the web server. Now return to the firewall's monitor tab to note the failed traffic:

The screenshot shows the Palo Alto Networks Firewall interface. The 'Monitor' tab is selected. In the left sidebar, 'Logs' is expanded, showing 'Traffic' and 'SSH'. A search bar at the top right contains the query 'port dst eq 22'. The main table lists five failed SSH connection attempts. The columns include: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. All entries show a 'drop' type, 'not-applicable' application, and 'policy-deny' as the rule.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
01/30 23:36:23	drop	Trust	Trust	10.5.3.5		10.5.4.5	22	not-applicable	deny	Log default deny	policy-deny	74
01/30 23:36:22	drop	Trust	Trust	10.5.3.5		10.5.4.5	22	not-applicable	deny	Log default deny	policy-deny	74
01/30 23:34:07	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54
01/30 23:20:13	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54
01/30 22:58:14	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54

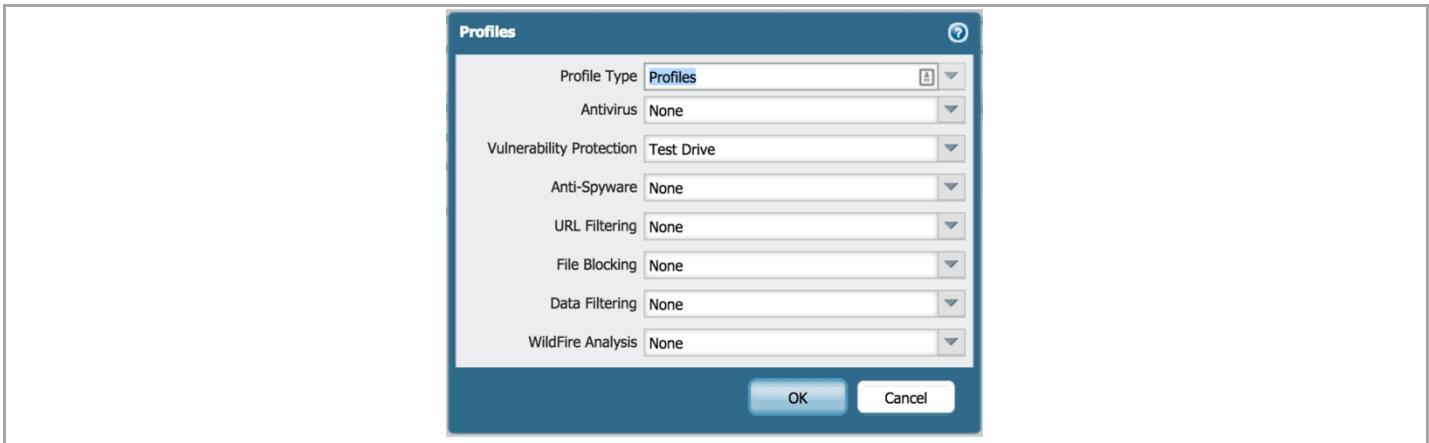
Task 2 - Trigger the SQL brute force attack and review logs

On the firewall's security policies tab, under Security, Rule 6, you will notice that the web to db traffic is protected further by a vulnerability profile:

The screenshot shows the Palo Alto Networks Firewall interface. The 'Policies' tab is selected. In the left sidebar, 'Security' is expanded, showing 'NAT', 'QoS', 'Policy Based Forwarding', 'Decryption', 'Application Override', 'Captive Portal', and 'DoS Protection'. The main table lists nine security rules. Rule 6, titled 'Web to DB', is highlighted. It has a 'universal' source zone, 'any' address, and 'any' user. The destination is 'any' with 'any' address. The application is 'db-object' and the service is 'mysql'. The action is 'Allow' and the profile is 'none'. The 'Options' column shows a lock icon for this specific row.

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1 SSH inbound	none	universal	Untrust	any	any	any	Trust	any	ping	application-d...	Allow	none	
2 SSH 221-222 inbound	none	universal	Untrust	any	any	any	Trust	any	ssh	service-tcp-2...	Allow	none	
3 Allow all ping	none	universal	any	any	any	any	any	any	ping	application-d...	Allow	none	
4 Web browsing	none	universal	Untrust	any	any	any	Trust	any	http	service-tcp-...	Allow	none	
5 Allow all outbound	none	universal	Trust	any	any	any	Untrust	any	any	application-d...	Allow	none	
6 Web to DB	none	universal	any	any	any	any	any	any	mysql	application-d...	Allow	lock	
7 Log default deny	none	universal	any	any	any	any	any	any	any	Deny	Deny	none	
8 intrazone-default	none	intrazone	any	any	any	any	(Intrazone)	any	any	Allow	Allow	none	
9 interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	Deny	none	

Now click on the icon in the Profile column and you will see all the threat protection profiles



Note the Vulnerability Protection profile. This is a custom profile created just for this lab. It is part of the default vulnerability protection profile but is called out separately for the purpose of this demo environment.

Let's finally trigger the attack. Head back to the sql-attack.html page at (<http://WebserverURL/sql-attack.html>)

Click on Launch Brute Force Attack to start a script that will generate multiple failed MySQL authentication attempts.



This will launch some scripted attacks on the SQL server and use the pre-configured threat protection to show and block those attacks on the VM-Series firewall. Now return to the firewall and click the Monitor tab and then click on Threats in the left-hand pane under Logs and notice the new vulnerability log message regarding the failed MySQL events:

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	URL
01/30 23:40:42	vulnerability	MySQL Login Authentication Failed	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	reset-client	Informational	

The CGI script you launched above attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity.

Task 3 - Lab Cleanup

If you have completed the above lab activities, we recommend deleting the deployment before moving on to the next activity.

Step 1: (optional) If you elected to work through Lab1, delete it prior to proceeding with Lab 2 by issuing the following command:

```
gcloud deployment-manager deployments delete <your-last-name>
```

End of Activity 5

Activity 6 – LAB 2-- Deploy Firewalls with Load Balancer

GCP Deployment Manager Templates, are Python (or Jinja) files that can launch nearly all GCP resources including VPC networks, subnets, security groups, route tables, etc. Templates are used for ease of deployment and are key to any auto-scaling environment.

This lab will demonstrate how to deploy a sample template that launches everything that is shown below. This includes:

1 – External Load Balancer (HTTP)

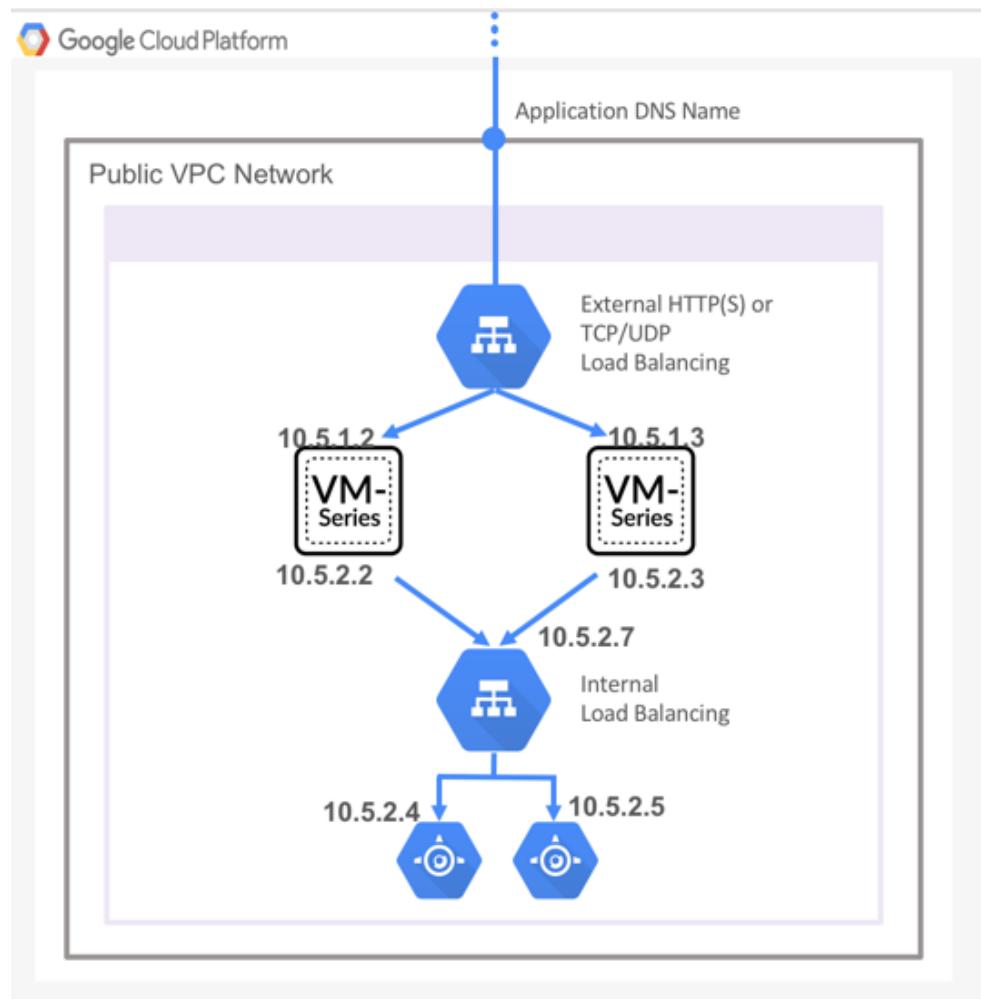
2 - VM-Series firewalls

1 – Internal Load Balancer (TCP/80)

2 – Webservers

Supporting infrastructure (VPC Network, Subnets, GCP Firewall Rules, etc.)

The firewall uses bootstrapping for a basic configuration (interface settings, administrative account, etc.) Once the sample template has been deployed, the network topology should align with the following:



For more information on Templates refer to Google's documentation

<https://cloud.google.com/deployment-manager/docs/how-to#adding-templates>

There are also many sample templates available here

<https://github.com/GoogleCloudPlatform/deploymentmanager-samples/tree/master/templates>

Template Instances used

When using the sample template in this lab, the following machine types are used:

Instance name	Machine Type
Web Servers	n1-standard-1
VM Series Firewalls	n1-standard-4

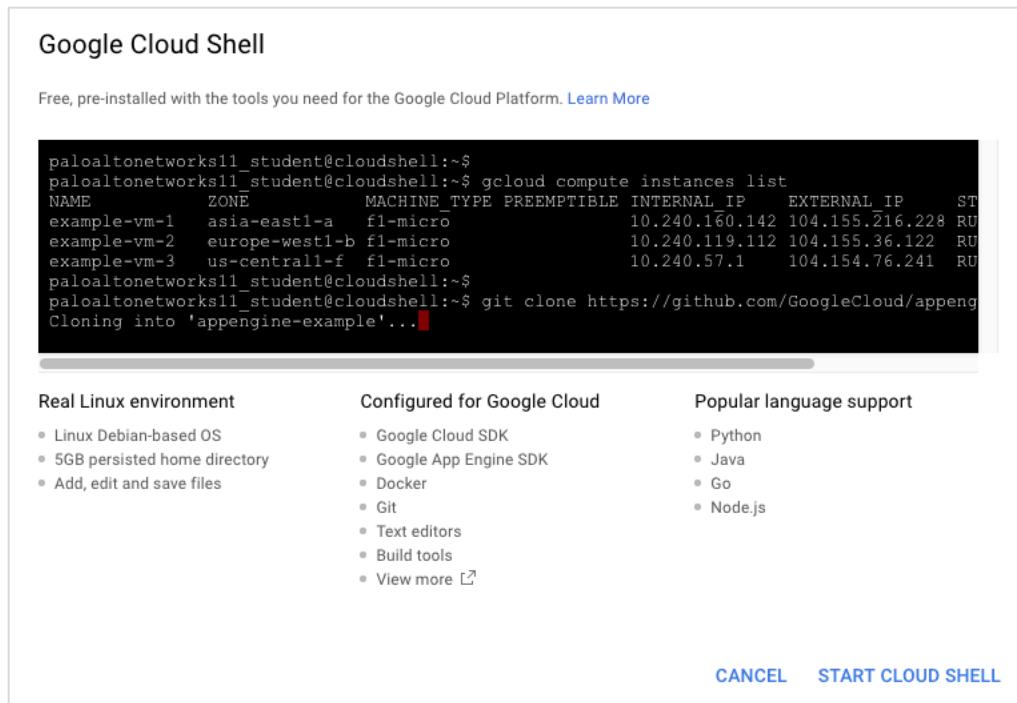
Task 1 –Launch Template with Google Cloud Shell

Google Cloud Shell is a shell environment for managing resources hosted on Google Cloud Platform. You can perform some basic operations in Google Cloud Shell. You can learn more about it [here](#).

Step 2: (optional) If you elected to work through Lab1, delete it prior to proceeding with Lab2 by issuing the following command:

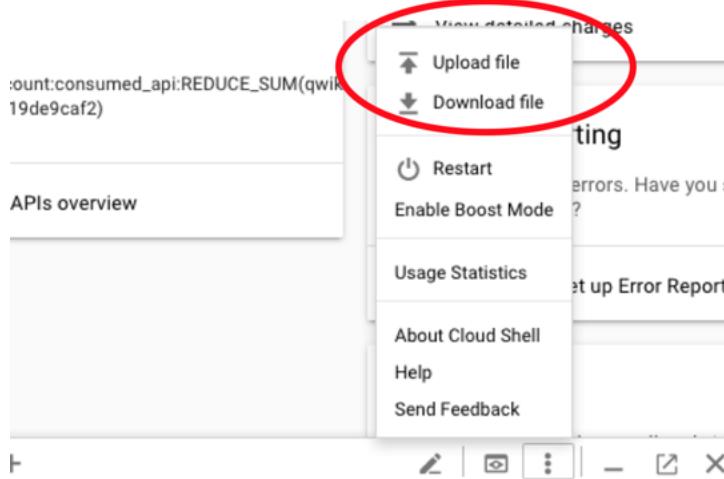
```
gcloud deployment-manager deployments delete <your-last-name>
```

Step 3: Click the start cloud shell icon in the upper right corner of the browser window () to open the Cloud Shell window below. Note that it may take a few minutes for Google Cloud Shell to be ready.



Step 4: Click the ellipses in upper right-hand corner of the Google Cloud Shell console and select **Upload File**. If you **Do Not See** the 3-dot ellipse please review Lab 1 >> Activity 1 >> Task 1 >> Step 2





Step 5: Upload the **how-11-gcp-lab2.yaml** and **how-11-gcp-lab2.py** file. Then close the Transfer window.



Step 6: In Cloud Shell prompt, you can use the **ls** command to confirm files have been uploaded.

```
my-project-vm-184222 ~
ssummer@my-project-vm-184222:~$ ls
how-11-gcp-lab2.py  how-11-gcp-lab2.yaml  README-cloudshell.txt
ssummer@my-project-vm-184222:~$
```

Step 7: Create a deployment using the command:

gcloud deployment-manager deployments create <your-last-name> --config how-11-gcp-lab2.yaml

Although you can use any text to for the deployment name, using your last name provides for easy identification.

```
tf-admin@tf-admin-1987:~$ ls
how-11-gcp-lab2.py  how-11-gcp-lab2.yaml  README-cloudshell.txt
tf_admin@tf-admin-1987:~$ gcloud deployment-manager deployments list
Listed 0 items.
tf_admin@tf-admin-1987:~$
tf_admin@tf-admin-1987:~$ gcloud deployment-manager deployments create sumner --config how-11-gcp-lab2.yaml
The fingerprint of the deployment is 2X1vBabE5EPwqntW6tfig==
Waiting for create [operation-1526964108647-56cc40947da59-7bcc3c4d-f376170d].../
```

Step 8: When the deployment is completed, you will see the creation completed message for each operation.

```

pglynnadmin@pglynn-lbsandwich:~$ gcloud deployment-manager deployments create spamboys --config lb-sandwich.yaml
The fingerprint of the deployment is AgYLiJL51J7V3rDM79FBWw==
Waiting for create [operation-1524880735187-56adef68bb038-598aa786-325f1bca]...done.
Create operation operation-1524880735187-56adef68bb038-598aa786-325f1bca completed successfully.
NAME          TYPE           STATE    ERRORS   INTENT
firewall-backendservice compute.v1.backendservice COMPLETED []
firewall-globalforwardingrule compute.v1.globalForwardingRule COMPLETED []
firewall-healthcheck        compute.v1.healthCheck  COMPLETED []
firewall-httpproxy          compute.v1.targetHttpProxy COMPLETED []
firewall-urlmap             compute.v1.urlMap      COMPLETED []
firewalla-instancegroup     compute.v1.instanceGroupManager COMPLETED []
firewalla-instancetemplate  compute.v1.instanceTemplate COMPLETED []
firewallb-instancegroup     compute.v1.instanceGroupManager COMPLETED []
firewallb-instancetemplate  compute.v1.instanceTemplate COMPLETED []
management            compute.v1.network      COMPLETED []
management-firewall       compute.v1.firewall     COMPLETED []
management-subnet          compute.v1.subnetwork  COMPLETED []
trust                  compute.v1.network      COMPLETED []
trust-firewall          compute.v1.firewall     COMPLETED []
trust-subnet             compute.v1.subnetwork  COMPLETED []
untrust                compute.v1.network      COMPLETED []
untrust-firewall         compute.v1.firewall     COMPLETED []
untrust-subnet            compute.v1.subnetwork  COMPLETED []
webserver-forwardingrule  compute.v1.forwardingRule COMPLETED []
webserver-healthcheck     compute.v1.healthCheck  COMPLETED []
webserver-regionbackendservice compute.v1.regionBackendService COMPLETED []
webservera-instancegroup   compute.v1.instanceGroupManager COMPLETED []
webservera-instancetemplate  compute.v1.instanceTemplate COMPLETED []
webserverb-instancegroup   compute.v1.instanceGroupManager COMPLETED []
webserverb-instancetemplate  compute.v1.instanceTemplate COMPLETED []
pqlynnadmin@pglynn-lbsandwich:~$ 

```

You can also go to the **Deployment Manager > Deployments** service to view the deployment:

The screenshot shows the Google Cloud Platform interface with the 'Deployment Manager' service selected. On the left, there's a navigation bar with 'Container Registry', 'Source Repositories', 'Deployment Manager', and 'Endpoints'. A tooltip 'Type registry' is displayed over the 'Deployment Manager' menu item. On the right, the 'Deployments' page is shown with a single entry named 'spamboys'.

Deployments	
<input type="button" value="DEPLOY CLOUD LAUNCHER SOLUTION"/>	<input type="button" value="DELETE"/>
Filter by label or name	
<input type="checkbox"/> Name ^	Created on
<input checked="" type="checkbox"/> spamboys	3 minutes ago

Step 9: Click the deployment that you have created and review the items that are created by the deployment manager.

The screenshot shows the 'Overview - spamboys' page for the deployment. It displays deployment properties and a list of created resources.

Deployment properties	
ID	7678909823740848
Created On	2018-04-27 (20:58:55)
Manifest Name	manifest-1524880735281
Config	View
Imports	lb-sandwich.py
Layout	View
Expanded Config	View

Resources Overview:

- spamboys has been deployed
- Overview - spamboys
 - lb-sandwich lb-sandwich.py
 - management network
 - untrust network
 - trust network
 - management-subnet subnetwork
 - untrust-subnet subnetwork
 - trust-subnet subnetwork
 - management-firewall firewall
 - untrust-firewall firewall
 - trust-firewall firewall
 - firewalla-instancetemplate vm instance template
 - firewallb-instancetemplate vm instance template
 - webservera-instancetemplate vm instance template

Although the template will run to completion in a few minutes, it may take up to 10 minutes for the firewalls to complete the bootstrap process and respond to login requests.

The next sections will guide you through the completion of the configuration of the firewalls to support the load balancers.

End of Activity 6

Activity 7 – Review the Deployment

In this activity, you will:

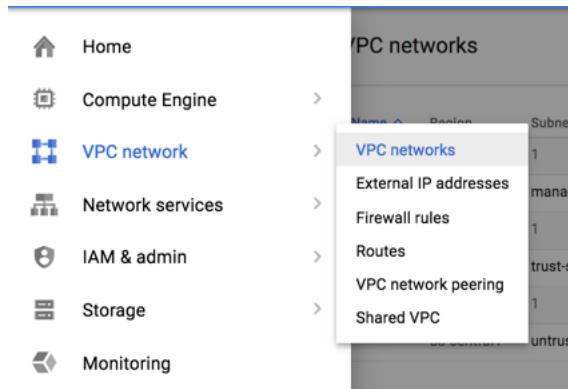
Review the GCP VPC Networks created via Deployment Manager Template

Review the GCE instances and the configuration created

Task 1 - Review VPC Networks

Let's review all the components we have launched in the VPC based on the deployment manager file.

Step 1: The VPC networks can be accessed via **VPC Networks > VPC Networks**. There you should see all networks created in your project:



Step 1: A **default** network is created when the project is instantiated and can safely be ignored. The three networks created by the deployment are **management, untrust, trust**:

VPC networks						CREATE VPC NETWORK	REFRESH
Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	
management	us-central1	management-subnet	Custom	10.5.0.0/24	10.5.0.1	1	
trust	us-central1	trust-subnet	Custom	10.5.2.0/24	10.5.2.1	1	
untrust	us-central1	untrust-subnet	Custom	10.5.1.0/24	10.5.1.1	1	

Note: Each network corresponds to an interface on the firewall. Although, you can create multiple subnets in a single network, a VM instance cannot have more than one interface attached to the same VPC network.

Step 2: Click on the **Firewall rules** to review the rules that are created by the deployment:

Step 2: Click one of the firewall instances to view the details:

The screenshot shows the 'VM instance details' page for a VM named 'firewalla-5h91'. The 'Details' tab is selected. Key information displayed includes:

- Remote access:** SSH, Connect to serial console, Enable connecting to serial ports (checked).
- Logs:** Stackdriver Logging, Serial port 1 (console), More.
- Instance template:** firewalla-instancetypetemplate.
- Machine type:** n1-standard-4 (4 vCPUs, 15 GB memory).
- In use by:** firewalla-instancegroup.

From here, it is possible to connect to the virtualized serial console of the instance as well as see the mappings between public IP addresses and the firewall interfaces.

Step 3: Click the on **Monitoring** to review some of the basic metrics monitored by GCP:



Note: In addition to the standard metrics you see here, the VM-Series firewall can publish native PAN-OS metrics to GCP Stackdriver. The additional metrics allow you to assess performance and usage patterns that you can use to make the decision to launch additional VM-Series firewalls or terminate unneeded instances. We will not go into the details here but you can get more information from your instructor or your SE.

Step 4: Return to the instance details page and scroll down to **Network Interfaces**. Notice that there are three network interfaces created for the VM-series firewall, management, eth1/1 for the public (untrust) network, and eth1/2 for the trust network.

VM instance details

EDIT RESET CLONE STOP DELETE

Network interfaces					
Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	IP forwarding
untrust	untrust-subnet	10.5.1.2	—	35.202.144.178 (ephemeral)	On
management	management-subnet	10.5.0.2	—	35.188.198.144 (ephemeral)	
trust	trust-subnet	10.5.2.2	—	None	

End of Activity 7

Activity 8 - Review Firewall Configuration

In this activity, you will:

- Login to the VM-Series firewall
- Review key portions of the firewall configurations

Task 1 - Access the firewall

NOTE: Bootstrapping a VM-Series firewall takes approximately 10 minutes. So once the template has been deployed successfully, it may be a while before the firewall is up and you are able to log into the firewall.

Step 1: Once the template deployment is complete, the firewall will show a green checkmark indicating it is running. Although you may see the checkmark, you may not be able to login immediately as the firewall may still be completing the bootstrap process:

VM instances					
CREATE INSTANCE IMPORT VM REFRESH START					
<input type="text"/> Filter VM instances					
Name	Zone	Recommendation	Internal IP	External IP	Connect
<input type="checkbox"/> ✓ firewalla-5h91	us-central1-a		10.5.1.2	35.202.144.178	SSH ✓ ⋮
<input type="checkbox"/> ✓ firewallb-wqqf	us-central1-a		10.5.1.3	23.236.57.44	SSH ✓ ⋮
<input type="checkbox"/> ✓ webservera-nsqj	us-central1-a		10.5.2.4	None	SSH ✓ ⋮
<input type="checkbox"/> ✓ webserverb-l32n	us-central1-a		10.5.2.5	None	SSH ✓ ⋮

Step 2: The GCP load balancer will only send traffic to the primary ethernet interface of an instance. Consequently, we need to swap the management and ethernet interfaces (eth0 is management by default). Retrieve the management interface public IP address by clicking on the firewall name and scrolling down to **Network Interfaces**:

VM instance details					
EDIT RESET CLONE STOP DELETE					
Network interfaces					
Network	Subnetwork	Primary Internal IP	Alias IP ranges	External IP	IP forwarding
untrust	untrust-subnet	10.5.1.2	—	35.202.144.178 (ephemeral)	On
management	management-subnet	10.5.0.2	—	35.188.198.144 (ephemeral)	
trust	trust-subnet	10.5.2.2	—	None	
Public DNS PTR Record					
None					

Step 3: Note the IP address and repeat the steps for the second firewall. You should be able to login to the firewall using the **username: paloalto** and password: **Pal0Alt0@123**

The screenshot shows the Palo Alto Networks Management interface. The top navigation bar includes Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The main content area has several tabs open:

- General Information:** Displays device details like Device Name (ibswich), MGT IP Address (10.5.0.2 (DHCP)), and various MAC and software versions.
- Logged In Admins:** Shows a single entry for 'paloalto' from IP 47.183.68.140 at 04/28 14:52:53.
- Data Logs:** No data available.
- System Logs:** A log of system events, including updates to the update server and connections to updates.paloaltonetworks.com.
- System Resources:** Shows Management CPU usage at 0%.

At the bottom, there are links for paloalto | Logout | Last Login Time: 04/28/2018 05:32:01 and standard navigation icons.

Step 4: The interface should be set up by the template deployment but you should review them and note the IP addresses on the interfaces:

The screenshot shows the Palo Alto Networks Management interface with the Network tab selected. The left sidebar contains a tree view of network components, with 'Interfaces' expanded. The main pane displays a table of interfaces:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		Up	Dynamic-DHCP Client	default	Untagged	none	untrust		
ethernet1/2	Layer3		Up	Dynamic-DHCP Client	default	Untagged	none	trust		
ethernet1/3			Up	none	none	Untagged	none	none		
ethernet1/4			Up	none	none	Untagged	none	none		
ethernet1/5			Up	none	none	Untagged	none	none		
ethernet1/6			Up	none	none	Untagged	none	none		
ethernet1/7			Up	none	none	Untagged	none	none		

At the bottom, there are links for paloalto | Logout | Last Login Time: 04/28/2018 05:32:01 and standard navigation icons.

Step 5: The default security policy has been modified to enable additional logging but is otherwise unaltered:

Name	Tags	Type	Zone	Address	User	HIP Profile	Source		Destination		Rule Usage		
							Zone	Address	Zone	Address	Hit Count	Last Hit	First Hit
1 intrazone-default	none	intrazone	any	any		any	(intrazone)	any	365706	2018-04-28 14:56:52	2018-04-28 14:56:52		
2 interzone-default	none	interzone	any	any		any	any	any	0	-	-		

Step 6: No NAT policy has been defined:

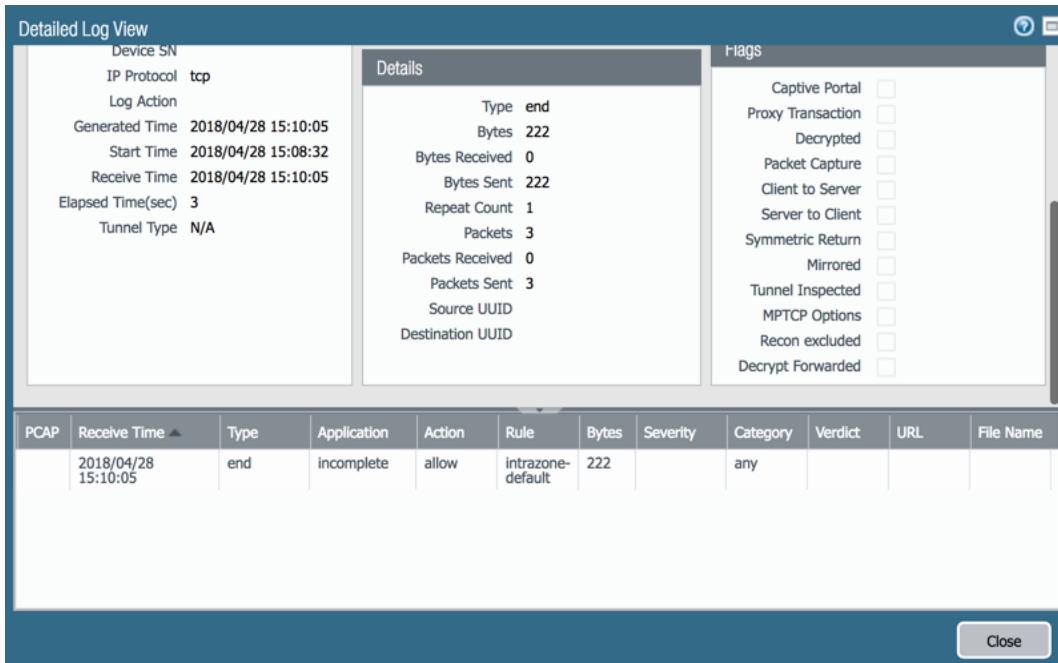
Name	Tags	Original Packet					Translated Packet		
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation

Task 2 – Review Monitor Tab

Step 1: Navigate to the **Monitor** tab. You should see traffic in the logs on port 80. This is the health check traffic that is coming from the external load balancer. If you look at the application column, you should see “incomplete”. This indicates that the firewall is unable to identify the application.

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor (which is selected), Policies, Objects, Network, and Device. On the right side of the header are buttons for Commit, Config, Search, Manual, Help, and other system controls. The left sidebar contains a tree view of monitoring categories: Logs (Traffic, Threat, URL Filtering, Wildfire Submissions, Data Filtering, HIP Match, User-ID, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet), PDF Reports (Manage PDF Summary, User Activity Report, SaaS Application Usage, Report Groups, Email Scheduler, Manage Custom Reports, Reports), and a general Reports section. The main content area displays a table of logs. The columns are: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. The table shows multiple entries for 04/28 15:10:05, all categorized as 'end' type traffic from 'untrust' to 'untrust' (Source: 35.191.255.0, Destination: 10.5.1.2, Port: 80) with 'incomplete' application and 'allow' action. The 'Rule' column consistently shows 'intrazone-default'. The 'Session End Reason' column shows 'aged-out' for most entries, except one which is '148'. The 'Bytes' column shows values ranging from 222 to 148. At the bottom of the log table, there are pagination controls (1 2 3 4 5 6 7 8 9 10), checkboxes for 'Resolve hostname' and 'Highlight Policy Actions', and a message 'Displaying logs 1 - 20 | 20 per page | DESC'. The footer of the interface includes links for paloalto | Logout | Last Login Time: 04/28/2018 05:32:01, and icons for Tasks and Language.

Step 2: Click on the icon () to show more detail about one of the traffic log entries. A new window will pop up:



The screenshot shows a 'Detailed Log View' window. At the top left, there's a summary table with fields like Device SN, IP Protocol (tcp), Log Action, Generated Time (2018/04/28 15:10:05), Start Time (2018/04/28 15:08:32), Receive Time (2018/04/28 15:10:05), Elapsed Time(sec) (3), and Tunnel Type (N/A). To the right of this is a 'Details' panel containing specific log details: Type (end), Bytes Received (0), Bytes Sent (222), Repeat Count (1), Packets (3), Packets Received (0), Packets Sent (3), Source UUID, and Destination UUID. Further right is a 'Flags' panel listing various flags with checkboxes, none of which are checked. Below these panels is a table with columns: PCAP, Receive Time, Type, Application, Action, Rule, Bytes, Severity, Category, Verdict, URL, and File Name. One row is visible, corresponding to the log entry above. At the bottom right of the window is a 'Close' button.

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
	2018/04/28 15:10:05	end	incomplete	allow	intrazone-default	222		any			

Note that **Bytes Received** is zero. This indicates that the firewall is only seeing one side of the session (the request from the load balancer). Because the intrazone policy is set to permit by default, the firewall is accepting the health checks from the load balancer but because there is no NAT rule in place to translate the traffic, the firewall does not know what to do and it gets dropped. We will fix that in a subsequent step.

End of Activity 8

Activity 9 – Complete and Verify Firewall with Load Balancer Configuration

Task 1 – Complete the firewall configuration

In this task, you will complete the firewall configuration and then verify that you can reach the web server through the firewall.

Step 1: Navigate to **Network Services > Load Balancing**:

The screenshot shows the 'Load balancing' interface. At the top, there are buttons for 'CREATE LOAD BALANCER', 'REFRESH', and 'DELETE'. Below this, a navigation bar has 'Load balancers' selected. A search bar is followed by a table with columns 'Name', 'Protocol', and 'Backends'. The table contains two rows:

Name	Protocol	Backends
firewall-urlmap	HTTP	1 backend service (2 instance groups)
webserver-regionbackendservice	TCP (Internal)	1 regional backend service (2 instance groups)

A note at the bottom says: 'To edit load balancing resources like forwarding rules and target proxies, go to the [advanced menu](#)'.

The **firewall-urlmap** load balancer is the internet-facing load balancer that is in front of the firewalls. It is showing unhealthy due to the lack of policies to process the traffic. The **webserver-regionbackendservice** is the internal load balancer that distributes traffic to the web servers on the backend.

Step 2: Click on **webserver-regionbackendservice**:

The screenshot shows the 'Load balancer details' page for 'webserver-regionbackendservice'. At the top, there are back, edit, and delete buttons. The main section displays the frontend configuration:

Protocol	Subnetwork	IP:Ports
TCP	trust-subnet (10.5.2.0/24)	10.5.2.7:80

Below this is the backend configuration:

Region: us-central1 Network: trust Endpoint protocol: TCP Session affinity: None Health check: webserver-healthcheck

Advanced configurations

Instance group	Zone	Healthy	Autoscaling
webservera-instancegroup	us-central1-a	1 / 1	Off
webserverb-instancegroup	us-central1-a	1 / 1	Off

Note the IP address associated with the frontend (10.5.2.7). This is the IP address that the firewall will need to send traffic to. Make a note of this address.

Step 3: Go back to the firewall and navigate to the **Network** tab:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		Up	Dynamic-DHCP Client	default	Untagged	none	untrust		
ethernet1/2	Layer3		Up	Dynamic-DHCP Client	default	Untagged	none	trust		
ethernet1/3			Up	none	none	Untagged	none	none		
ethernet1/4			Up	none	none	Untagged	none	none		
ethernet1/5			Up	none	none	Untagged	none	none		
ethernet1/6			Up	none	none	Untagged	none	none		
ethernet1/7			Up	none	none	Untagged	none	none		

Step 4: Click on ethernet1/1 (the external interface) and make a note of the IP address:

Dynamic IP Interface Status

Interface: ethernet1/1
State: Bound
Remaining Lease Time: 0 days 13:00:27
IP Address: 10.5.1.2
Address: 10.5.1.1
Gateway: 169.254.169.254
Primary DNS: 169.254.169.254
Secondary DNS: 0.0.0.0
Primary WINS: 0.0.0.0
Secondary WINS: 0.0.0.0
Primary NIS: 0.0.0.0
Secondary NIS: 0.0.0.0

Renew Release Close

Step 5: Navigate to the **Policies** tab and add a rule translating inbound connections on port 80 arriving at the external IP of the firewall to the frontend IP address of the internal load balancer:

The screenshot shows the Palo Alto Networks Firewall interface. On the left, there's a sidebar with icons for Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main area has tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, and Device. At the top right are buttons for Commit, Config, Search, and Help.

In the center, there's a table titled "Original Packet" with columns: Name, Tags, Source Zone, Destination Zone, Destination Interface, Source Address, Destination Address, Service, Source Translation, and Destination Translation. One row is shown for "Inbound-80" with values: Name (Inbound-80), Tags (none), Source Zone (untrust), Destination Zone (untrust), Destination Interface (any), Source Address (any), Destination Address (10.5.1.2), Service (service-http), Source Translation (dynamic-ip-and-port ethernet1/2), and Destination Translation (destination-translation address: 10.5.2.7).

On the left side, there's a "Tag Browser" window showing one item: "none (1)". It includes checkboxes for "Filter by first tag in rule" and "Rule Order" (which is selected). Below the browser is a toolbar with buttons for Add, Delete, Clone, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, and Reset Rule Hit Counter.

At the bottom, there's a footer bar with links for Object : Addresses, a login status (paloalto | Logout | Last Login Time: 04/28/2018 05:32:01), and links for Tasks and Language.

In addition to the destination translation, we also add a source NAT that hides the traffic behind the IP address of the internal interface of the firewall. What purpose does it serve?

- Step 6:** Replicate the changes to the second firewall (beware the IP address on the external interface) and commit the changes on both.
- Step 7:** Navigate to the **Monitor** tab and note the change in the logs. Instead of source and destination zone of **untrust** and application of **incomplete**, we now see that the source zone is **untrust** and the destination zone is **trust** and the application is **not-applicable**.

The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar has a tree view under 'Logs' with categories like Threat, URL Filtering, WildFire Submissions, Data Filtering, and more. The main area displays a table of logs. The columns include: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. The logs show numerous entries for 'drop' actions from 'untrust' to 'trust' zones, mostly for port 80 (HTTP) and application 'not-applicable'. The table has 20 pages, and the current page is 1. The bottom status bar shows 'Displaying logs 1 - 20'.

Progress but we are not there yet. What's up with that? Hint: the firewall policy permits **intrazone** traffic but denies **interzone** traffic.

Step 8: Jump back to the policy tab and add a **Security** rule that permits traffic from the **untrust** zone to the **trust** zone with a destination of the firewall external IP address, an application of **web-browsing** and a service of **application-default**:

The screenshot shows the 'Policies' tab in the Palo Alto Networks Firewall interface. The left sidebar lists policy categories: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. A 'Tag Browser' window is open at the bottom-left, showing a single tag named '1'. The main area displays a table of security rules. The columns include: Name, Tags, Type, Source (Zone, Address, User, HIP Profile), Destination (Zone, Address), Hit Count, Last Hit, and First Hit. The table shows three rules: 'Inbound-80' (universal type, source 'any', destination 'trust', port 80, application 'not-applicable'), 'intrazone-default' (intrazone type, source 'any', destination '(intrazone)', port 80, application 'not-applicable'), and 'interzone-default' (interzone type, source 'any', destination 'any', port 80, application 'not-applicable'). The bottom status bar shows 'Displaying 3 items'.

Step 9: Navigate back to the **Monitor** tab et voilà:

You can add the **NAT Source IP** and **NAT Dest IP** columns to see how the firewall is translating the addresses.

Step 10: Go back to the GCP console, **Network services > Load balancing** (Click **REFRESH** at the top if you are already there):

Name	Protocol	Backends
firewall-urlmap	HTTP	1 backend service (2 instance groups)
webserver-regionbackendservice	TCP (Internal)	1 regional backend service (2 instance groups)

Now we can see that the backend service associated with the internet-facing load balancer is reported as healthy.

Task 2 – Verify the Configuration

In this task, you will verify that you can reach the web server through the firewall.

Step 1: From the **Network services > Load balancing** section of the GCP console, click on the internet load balancer (**firewall-urlmap**) and note the public IP address associated with the load balancer:

Protocol	IP:Port	Certificate
HTTP	35.190.92.76:80	-

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

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

Step 2: Open a web browser, paste the address in and press enter:

The screenshot shows a web browser displaying the Apache2 Debian Default Page. The page header reads "Apache2 Debian Default Page" and features the "debian" logo. A red banner at the top says "It works!". Below it, there is a paragraph of text explaining the purpose of the page and how to replace the default index.html file. A "Configuration Overview" section provides details about the configuration layout, mentioning files like apache2.conf, ports.conf, and sites-enabled. A file tree diagram shows the directory structure under /etc/apache2/. At the bottom, there are two bullet points explaining the main configuration file and ports.conf.

```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|   |-- mods-enabled
|       |-- *.load
|       |-- *.conf
|   |-- conf-enabled
|       |-- *.conf
|   |-- sites-enabled
|       |-- *.conf

```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Success! You have validated that the traffic is passing through the firewall and reaching the webservers on the backend.

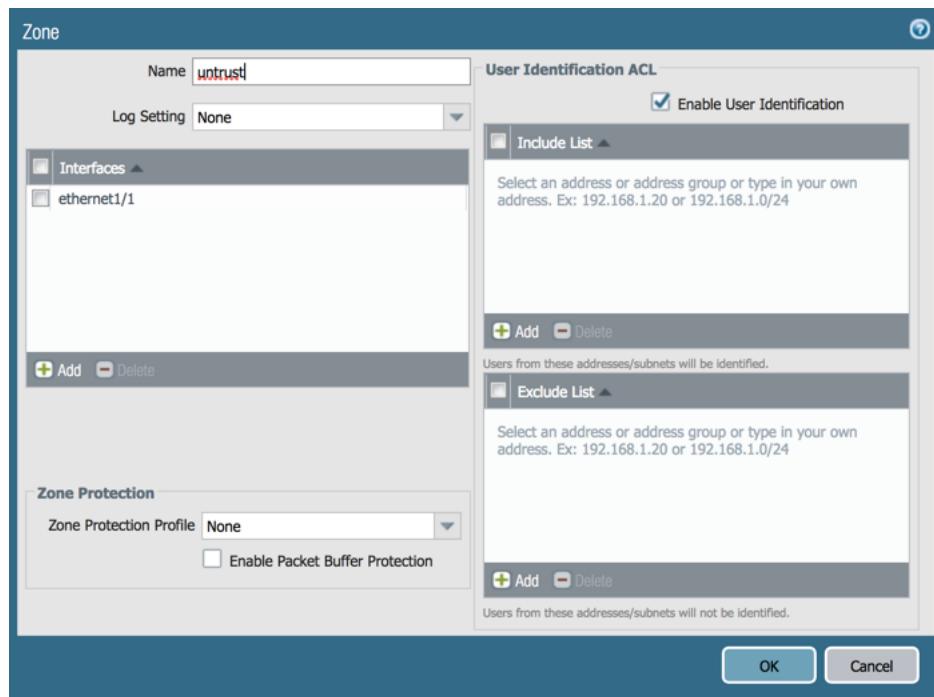
Task 3 - Log X-Forwarded-For (Bonus)

One side effect of using an application load balancer (ALB) is that the original source address is hidden from the firewall. Fortunately, most ALBs insert the original source address as an X-Forwarded-For (XFF) header that the VM-Series firewall can log. In this exercise, you will enable user-ID on the relevant interface, create a URL filtering profile to log XFF, and apply it to the firewall rule.

Step 1: On the firewall, navigate to the **Network** tab and then **Zones**:

The screenshot shows the Palo Alto Networks Firewall UI. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network (which is selected), and Device. On the right, there are buttons for Commit, Config, Search, and Help. The left sidebar contains a tree view of network objects: Interfaces, Zones (selected), Virtual Routers, IPSec Tunnels, DHCP, DNS Proxy, GlobalProtect (expanded to show Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups, QoS, LLDP), and Network Profiles (expanded to show GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, and BFD Profile). The main content area displays a table titled "User-ID" for zones. The table has columns: Name, Type, Interfaces / Virtual Systems, Zone Protection Profile, Packet Buffer Protection, Log Setting, Enabled, Included Networks, and Excluded Networks. Two rows are present: "trust" (layer3, ethernet1/2) and "untrust" (layer3, ethernet1/1). The "Enabled" column for the "untrust" row has a checked checkbox. The bottom of the screen shows standard UI elements like Add, Delete, PDF/CSV, and a footer with the Palo Alto Networks logo, Logout, Last Login Time (04/28/2018 05:32:01), and links for Tasks and Language.

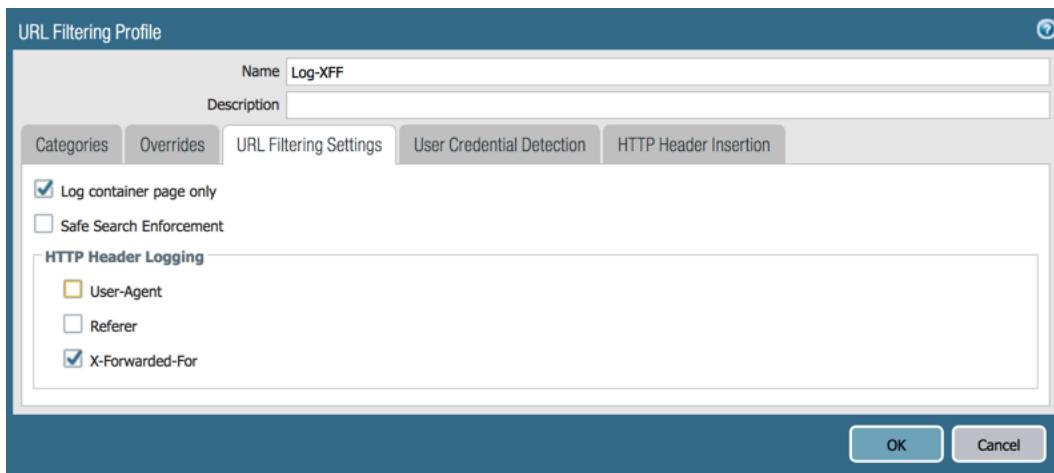
Step 2: Click on the **untrust** zone and tick the box **Enable User Identification**:



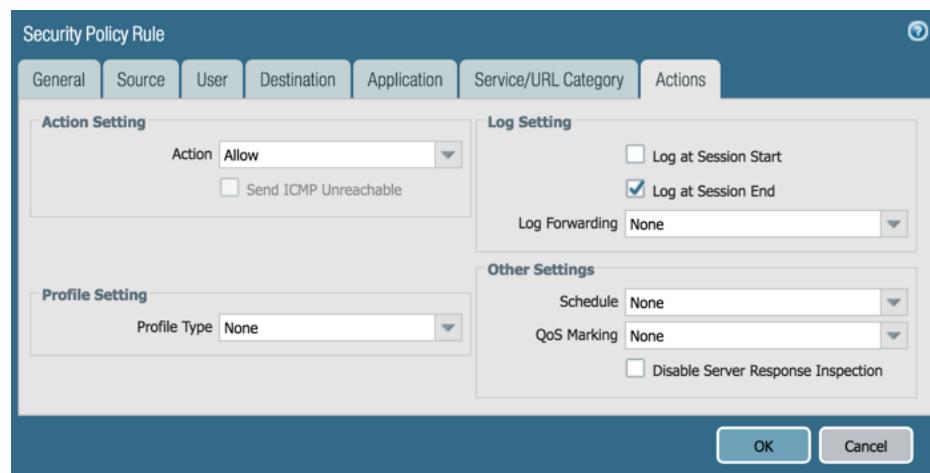
Step 3: Navigate to the **Objects tab > Security Profiles > URL Filtering** and create a new URL filtering profile setting **private-ip-addresses** to alert:

Category	Site Access	User Credential Submission
personal-sites-and-blogs	alert	allow
philosophy-and-political-advocacy	alert	allow
phishing	alert	block
<input checked="" type="checkbox"/> private-ip-addresses	alert	allow
proxy-avoidance-and-anonymizers	alert	allow
questionable	alert	block
real-estate	alert	allow
recreation-and-hobbies	alert	allow
reference-and-research	alert	allow
religion	alert	allow

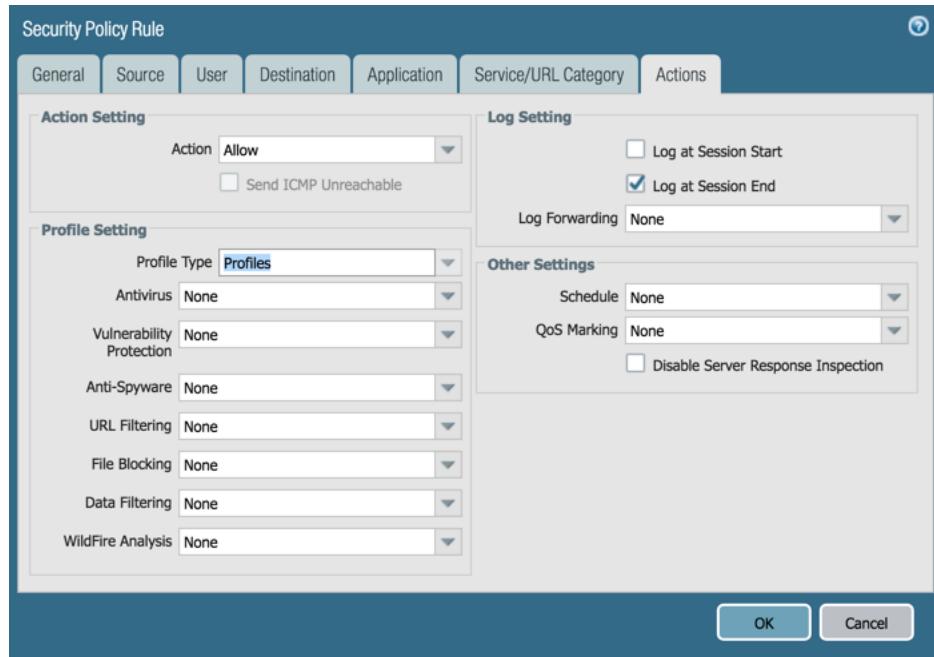
Step 4: Click on URL Filtering Settings and tick the **X-Forwarded-For** box under **HTTP Header Logging**:



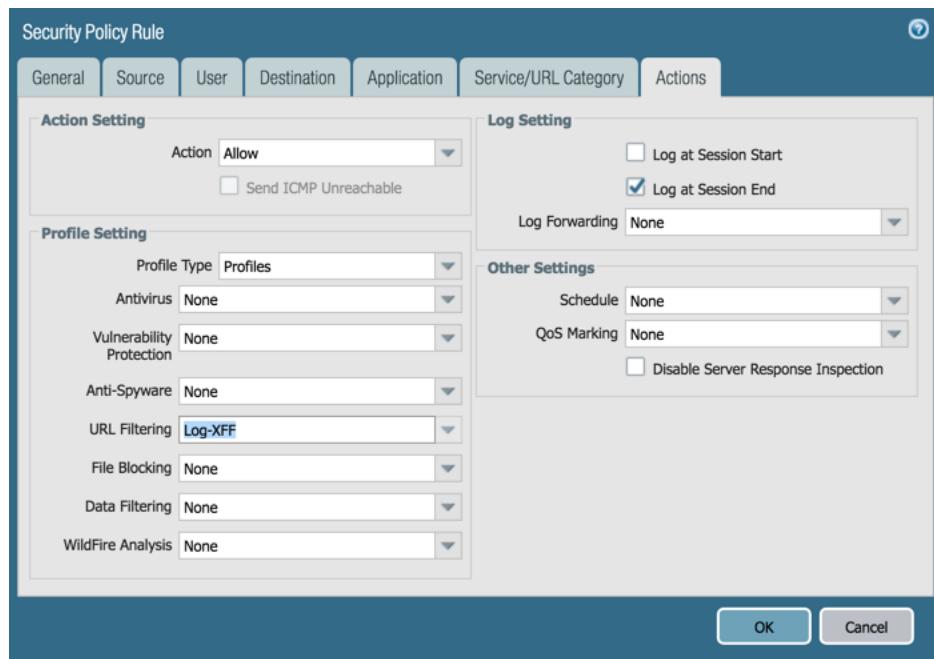
Step 5: Navigate to the **Policies** tab and edit the policy permitting the load balancer traffic. Click on the **Actions** tab:



Step 6: Click on the **Profile Type** dropdown and set it to **Profiles**:



Step 7: Set the **URL Filtering** profile to the one created earlier:



Step 8: Commit the changes and replicate to the other firewall.

Step 9: Refresh the connection to the public load balancer a few times and then navigate to the **Monitor** tab **URL Filtering**. Add the **X-Forwarded-For** column to the firewall log and apply the filter `(xff neq "")` to the logs to filter out the load balancer health checks (it may take a few moments for the logs to show up). Note: in the filter the " are apostrophe's not quotes.

The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar contains a tree view of logs, traffic, threat, URL filtering, WildFire submissions, data filtering, HIP match, user-ID, tunnel inspection, configuration, system, alarms, authentication, unified, packet capture, app scope, PDF reports, and reports. The main pane displays a log entry titled '(xff neq *)'. The log table has columns: Receive Time, Category, URL, From Zone, To Zone, Source, Source User, X-Forwarded-For, Destination, Application, Action, and Headers Inserted. The entry details are:

Receive Time	Category	URL	From Zone	To Zone	Source	Source User	X-Forwarded-For	Destination	Application	Action	Headers Inserted
04/28 18:32:47	unknown	35.190.92.76/	untrust	trust	130.211.1.15		47.183.68.140, 35.190.92.76	10.5.1.3	web-browsing	alert	

At the bottom, there are buttons for 'Resolve hostname' and 'Highlight Policy Actions', and a footer with 'Displaying logs 1 - 1 | 20 per page DESC'.

If all goes well, you should see the request traffic logged with the original source IP and the IP address of the external load balancer.

End of Activity 9

Conclusion

Congratulations!! You have now successfully integrated the PANW VM series firewall into GCP to gain visibility into East/West and North/South traffic entering and leaving your Google Cloud.

You have also configured and leveraged the VM Series to log X Forward-For information.

No Cleanup required the lab will self-destruct when the Lab timer reaches 00:00.

Thank you for taking the Ignite18-HOW-11-GCP-Lab.