Hands-on Workshop Guide

AWS + Palo Alto Networks Security Dev Day

VM-Series

Securing Applications on Amazon Web Services (AWS)

www.paloaltonetworks.com

Table of Contents

How to Use This Guide

The activities outlined in this workshop guide are meant to contain all the information necessary to navigate the workshop interface, complete the workshop activities, and troubleshoot any potential issues with the lab environment. This guide is meant to be used in conjunction with the information and guidance provided by your facilitator.

Notes

This workshop covers only basic topics and is not a substitute for training classes conducted by Palo Alto Networks Authorized Training Partners. Please contact your partner or regional sales manager for more information on available training sessions and how to register for one near you.

Unless specified, the Google Chrome® browser should be used to perform any tasks outlined in the following activities.

Terminology

Tab refers to the seven tabs along the top of each screen in the GUI.

Node refers to the options associated with each tab, found in the left-hand column of each screen.

Activity 0 - Workshop Login

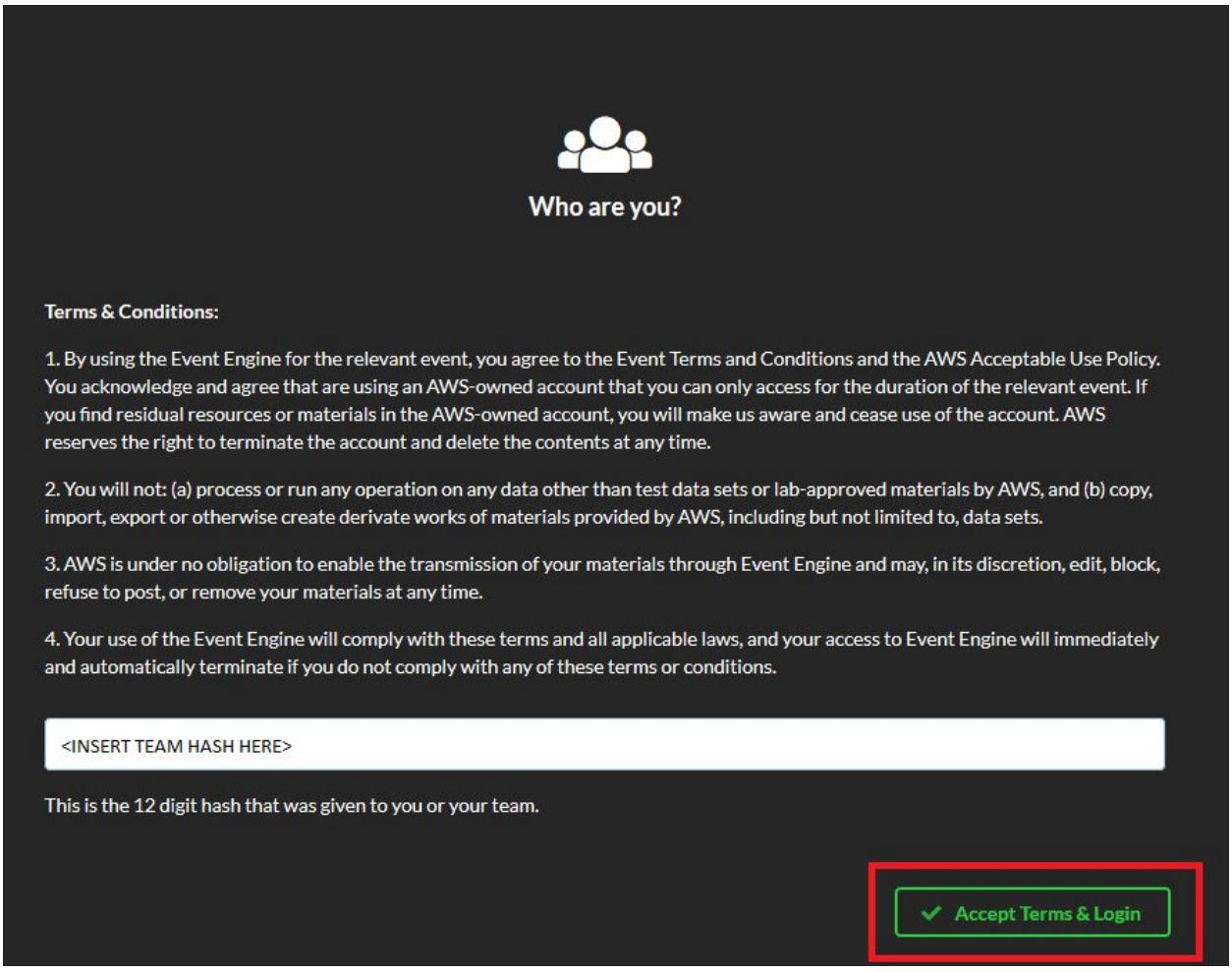
In this activity, you will:

- Log in to the Team Dashboard.
- Log in to the AWS Console using the account provided.

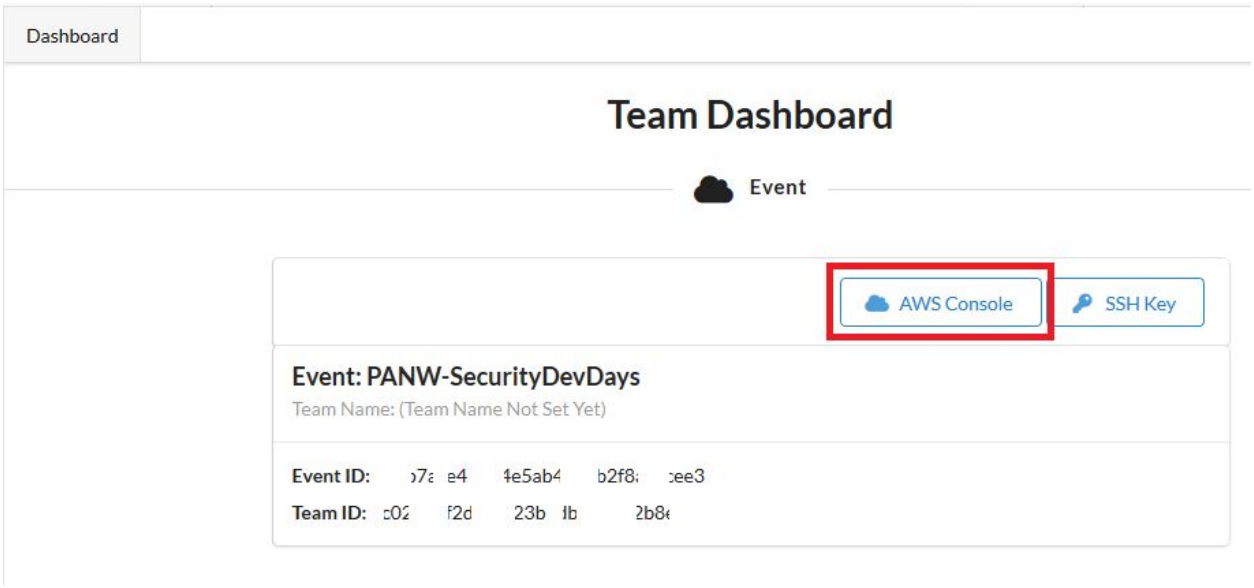
Task 1 - Log in to AWS Event Engine Team Dashboard

Step 1. Each team browse to the following URL: https://dashboard.eventengine.run/login

Step 2. You will be prompted to enter your Team Hash and click on "Accept Terms & Login".

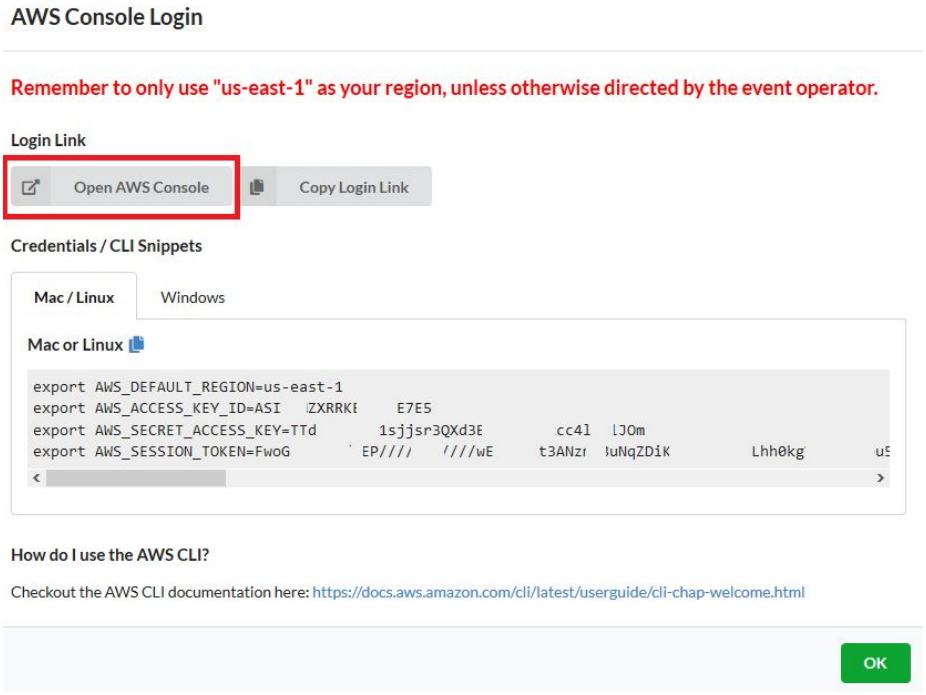


Step 3. Next, you will see your Team Dashboard, where you can click on "AWS Console".



Task 2 - Log in to AWS Console

Step 1. Click on the "Open AWS Console" tab.



Activity 1 - Review VPC and Resource Configurations

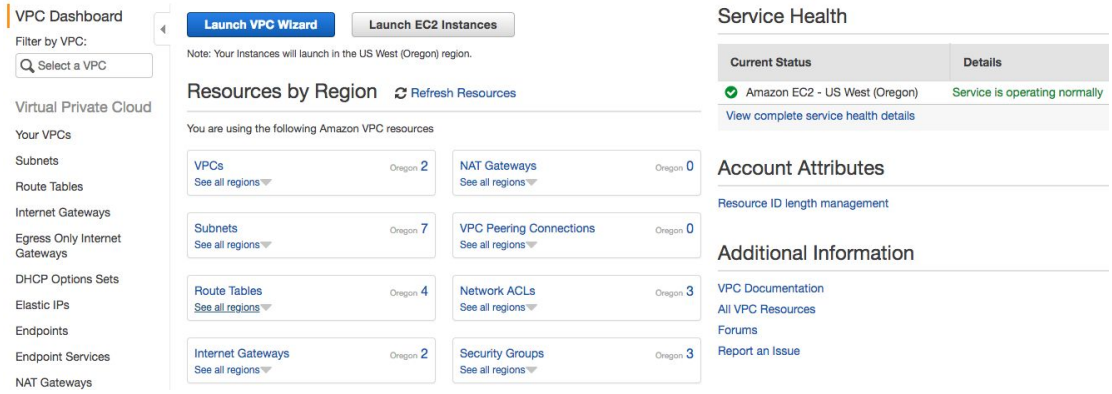
In this activity, you will:

- Review the VPC.
- Review the EC2 instances and the configuration

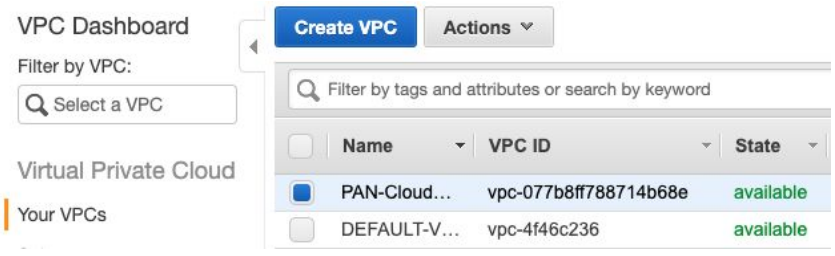
Task 1 - Review VPC

Let's review all of the components we have launched in the VPC.

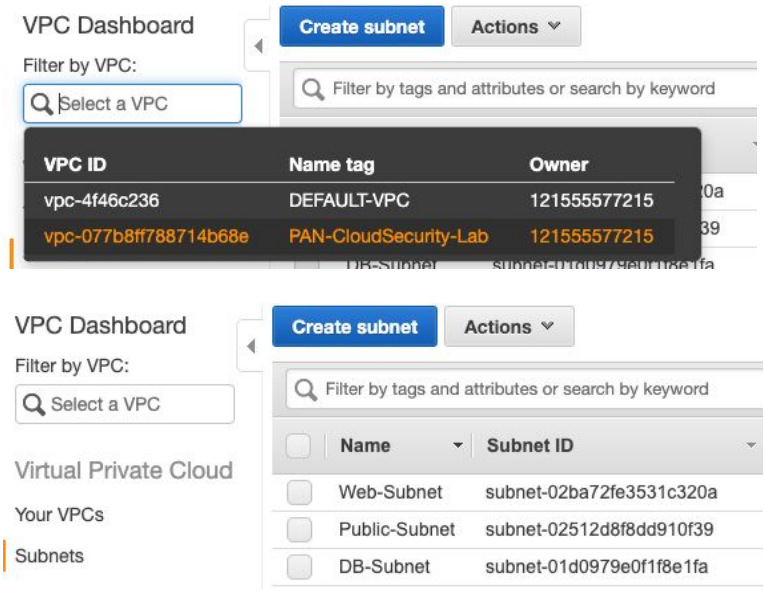
Step 1. The newly created VPC can be accessed via Services > VPC. There, you should see all VPCs created in your account:



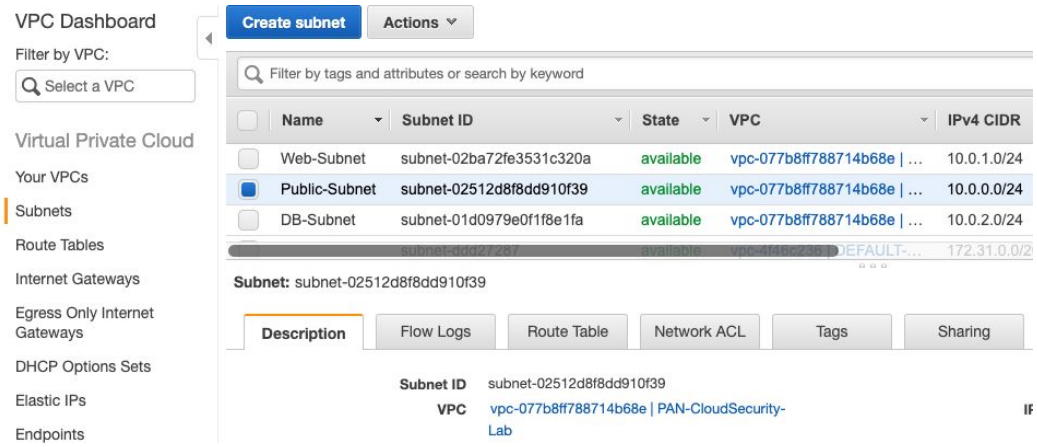
Step 2. The VPC created by the template is ***PAN-CloudSecurity-Lab***, you may also see the ***DEFAULT-VPC*** that is created by AWS®. All the AWS resources are created in the ***PAN-CloudSecurity-Lab***.



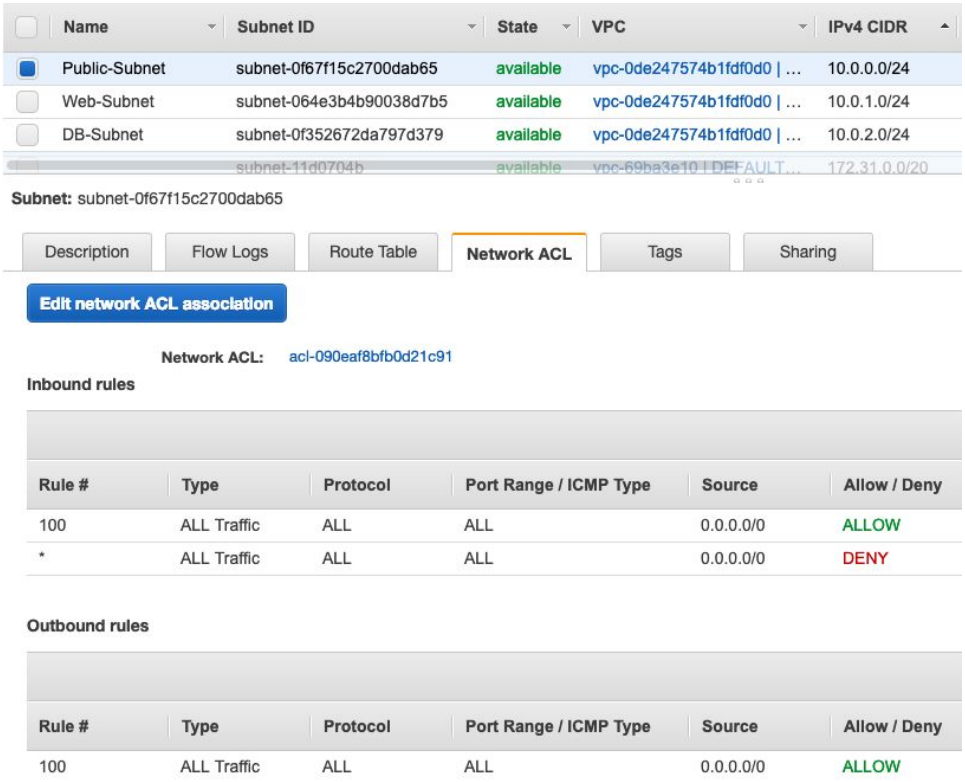
Step 3. On the left, you can review the major components created for this VPC, such as the subnets. Choose the ***PAN-CloudSecurity-Lab*** by using the ***Filter by VPC*** to look at all the subnets in this particular VPC. Note that all the subnets must be part of the CIDR block allocated for this VPC.



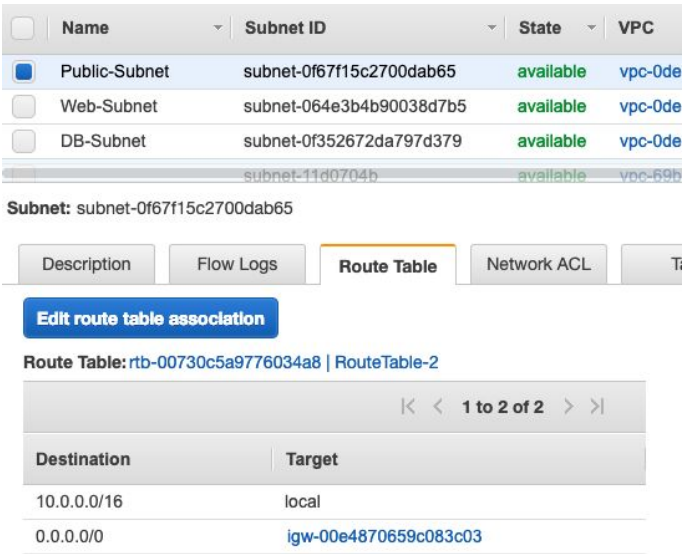
Step 4. Each subnet has a set of configurations. Select the ***Public-Subnet*** to review these configurations.



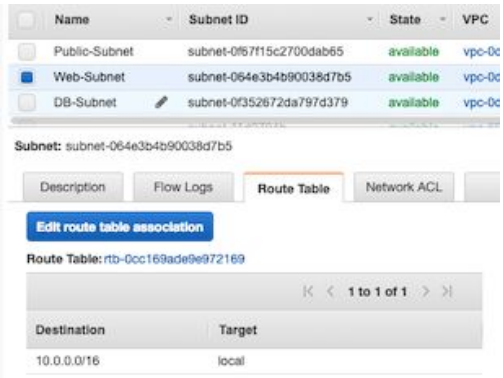
Step 5. Click on the ***Network ACL*** for this network. Note that all inbound and outbound traffic is allowed in this network.

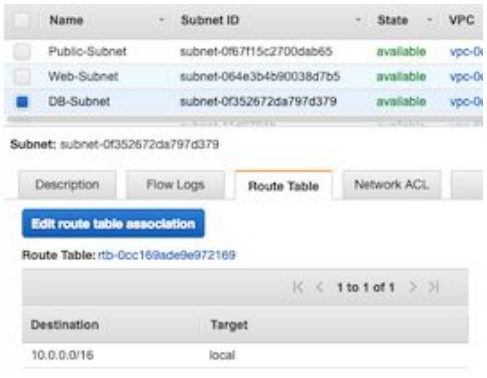


Step 6. Click on **Route Table** for the ***Public-Subnet***. Note that all traffic outside the local network is routed to the igw-xxxx, the AWS Internet-Gateway for this VPC. Note that the VM-Series firewall does NOT replace the AWS Internet-Gateway.

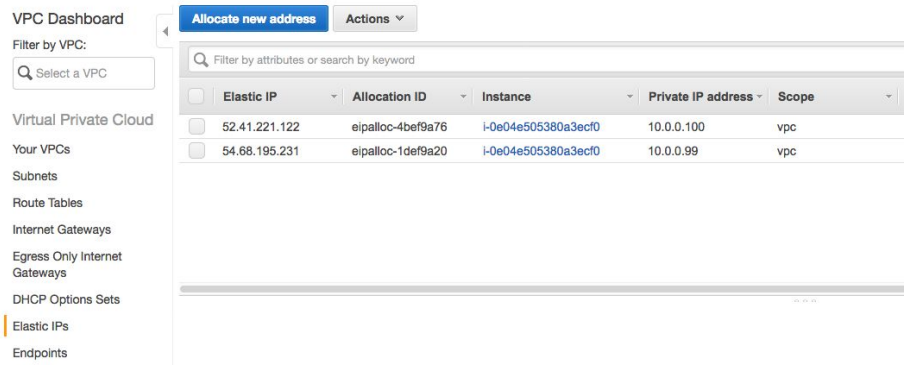


Step 7. Click on the ***Web-Subnet*** or the ***DB-Subnet*** and review the Route Table for that subnet. Note that there is no route to the Internet-Gateway. Routing for these two networks is handled by the VM-Series firewall.





Step 8. Review the Elastic IPs created. There are two Elastic IPs created in this VPC. Note that both are assigned to the same instance. Click on the instance ID to find out what that instance is. (The instance ID should lead you to either the firewall or the web server instance.)

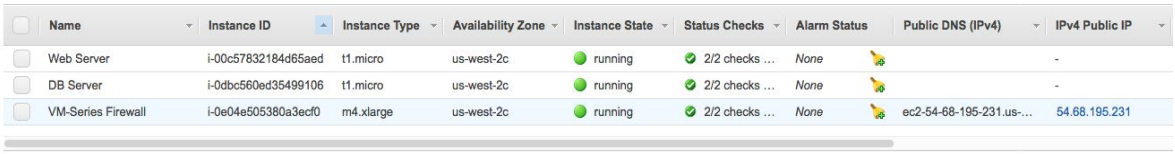


Task 2 - Review EC2 Instances

We will review the EC2 instances created by the CFT in this task.

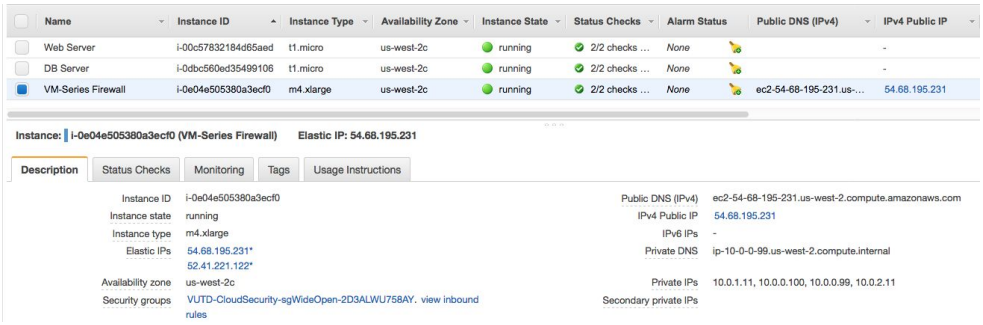
Step 1. Go to the EC2 Dashboard by clicking on ***Service > EC2***. There are at least three instances created by the CFT: web server, a DB server, and a VM-Series firewall.

Step 2. Click ***Running Instances*** to view these EC2 instances. The Instance State indicates if the instances are launched and running successfully. Note that there is no public IP address assigned to the web server. Remove any filter from the search bar if applicable.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Web Server	i-00c57832184d65aed	t1.micro	us-west-2c	running	2/2 checks ...	None		-
DB Server	i-0dbc560ed35499106	t1.micro	us-west-2c	running	2/2 checks ...	None		-
VM-Series Firewall	i-0e04e505380a3ecf0	m4.xlarge	us-west-2c	running	2/2 checks ...	None	ec2-54-68-195-231.us-...	54.68.195.231

Step 3. Select the ***VM-Series Firewall*** instance to review the details for that instance. Note the Elastic IP applied to this instance.



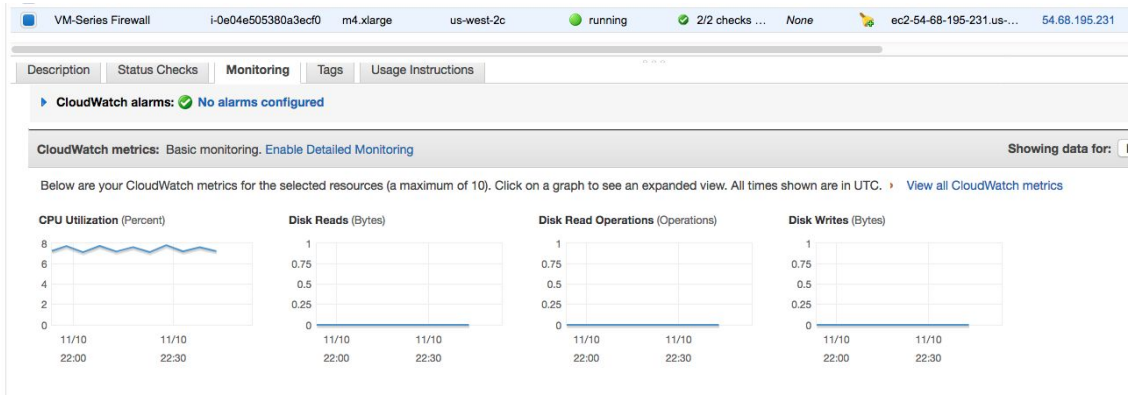
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Web Server	i-00c57832184d65aed	t1.micro	us-west-2c	running	2/2 checks ...	None		-
DB Server	i-0dbc560ed35499106	t1.micro	us-west-2c	running	2/2 checks ...	None		-
VM-Series Firewall	i-0e04e505380a3ecf0	m4.xlarge	us-west-2c	running	2/2 checks ...	None	ec2-54-68-195-231.us-...	54.68.195.231

Instance: i-0e04e505380a3ecf0 (VM-Series Firewall) Elastic IP: 54.68.195.231

Description | Status Checks | Monitoring | Tags | Usage Instructions

Instance ID	i-0e04e505380a3ecf0	Public DNS (IPv4)	ec2-54-68-195-231.us-west-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	54.68.195.231
Instance type	m4.xlarge	IPv6 IPs	-
Elastic IPs	54.68.195.231* 52.41.221.122*	Private DNS	ip-10-0-0-99.us-west-2.compute.internal
Availability zone	us-west-2c	Private IPs	10.0.1.11, 10.0.0.100, 10.0.0.99, 10.0.2.11
Security groups	VUTD-CloudSecurity-sgWideOpen-2D3ALWU758AY. view inbound rules	Secondary private IPs	

Step 4. Click the **Monitoring tab** to review some of the basic metrics monitored by AWS.



VM-Series Firewall | i-0e04e505380a3ecf0 | m4.xlarge | us-west-2c | running | 2/2 checks ... | None | ec2-54-68-195-231.us-... | 54.68.195.231

Description | Status Checks | **Monitoring** | Tags | Usage Instructions

CloudWatch alarms: No alarms configured

CloudWatch metrics: Basic monitoring. Enable Detailed Monitoring Showing data for:

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. View all CloudWatch metrics

CPU Utilization (Percent) 8 6 4 2 0 11/10 22:00 11/10 22:30

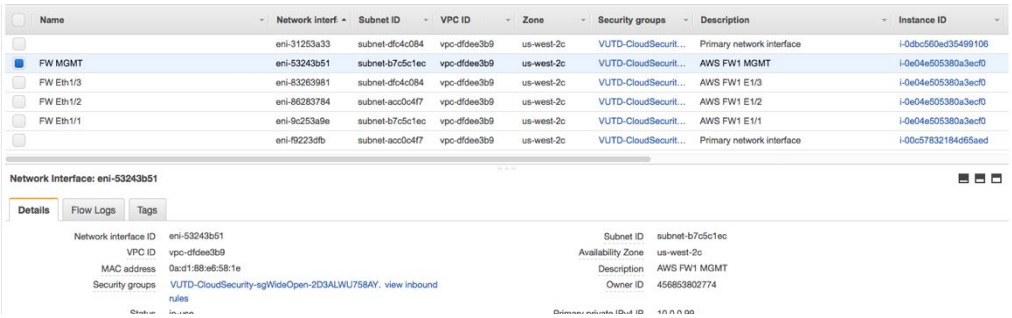
Disk Reads (Bytes) 1 0.75 0.5 0.25 0 11/10 22:00 11/10 22:30

Disk Read Operations (Operations) 1 0.75 0.5 0.25 0 11/10 22:00 11/10 22:30

Disk Writes (Bytes) 1 0.75 0.5 0.25 0 11/10 22:00 11/10 22:30

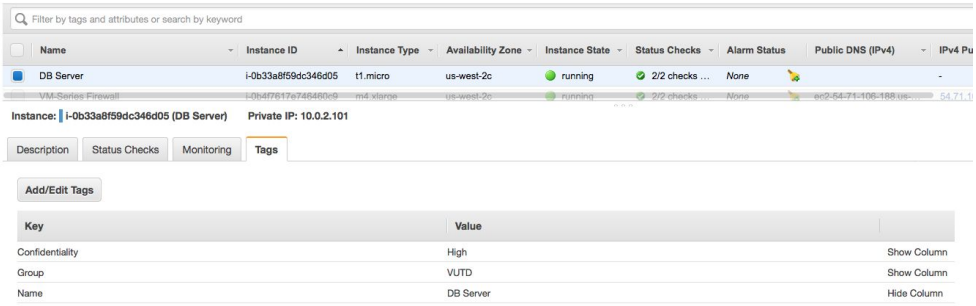
Note: The VM-Series firewall on AWS can publish native PAN-OS® metrics to AWS CloudWatch, which you can use to monitor the firewalls. These metrics allow you to assess performance and usage patterns that you can use to take action for launching or terminating instances of the VM-Series firewalls. You will learn more about how to enable CloudWatch monitoring on the VM-Series firewall in lab activity 8.

Step 5. Click on ***Network Interfaces*** on the left panel to review the network interfaces. Note that there are four network interfaces created for the VM-Series firewall: management, eth1/1 for the public network, eth1/2, and eth1/3 for the Web and DB network. Can you find which network interface has the second public IP address?

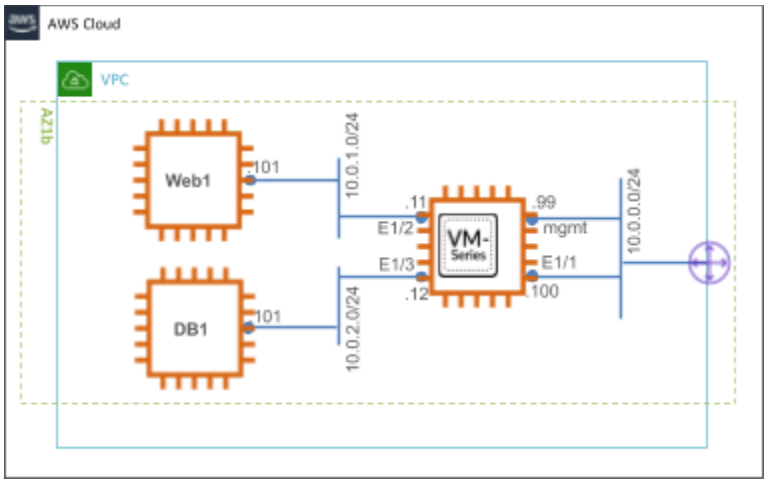


Scroll to the right as needed and look at the IPv4 Public IP column

Step 6. Go back to ***Instances*** and select the ***DB Server*** instance to review the details for that instance. Click on the Tags to see the tags configured for this VM. (AWS allows customers to assign metadata to their AWS resources in the form of *tags*. We will see how tags can be used with the VM-Series firewall in one of the later lab activities.)



All VPC configurations should match the following topology:



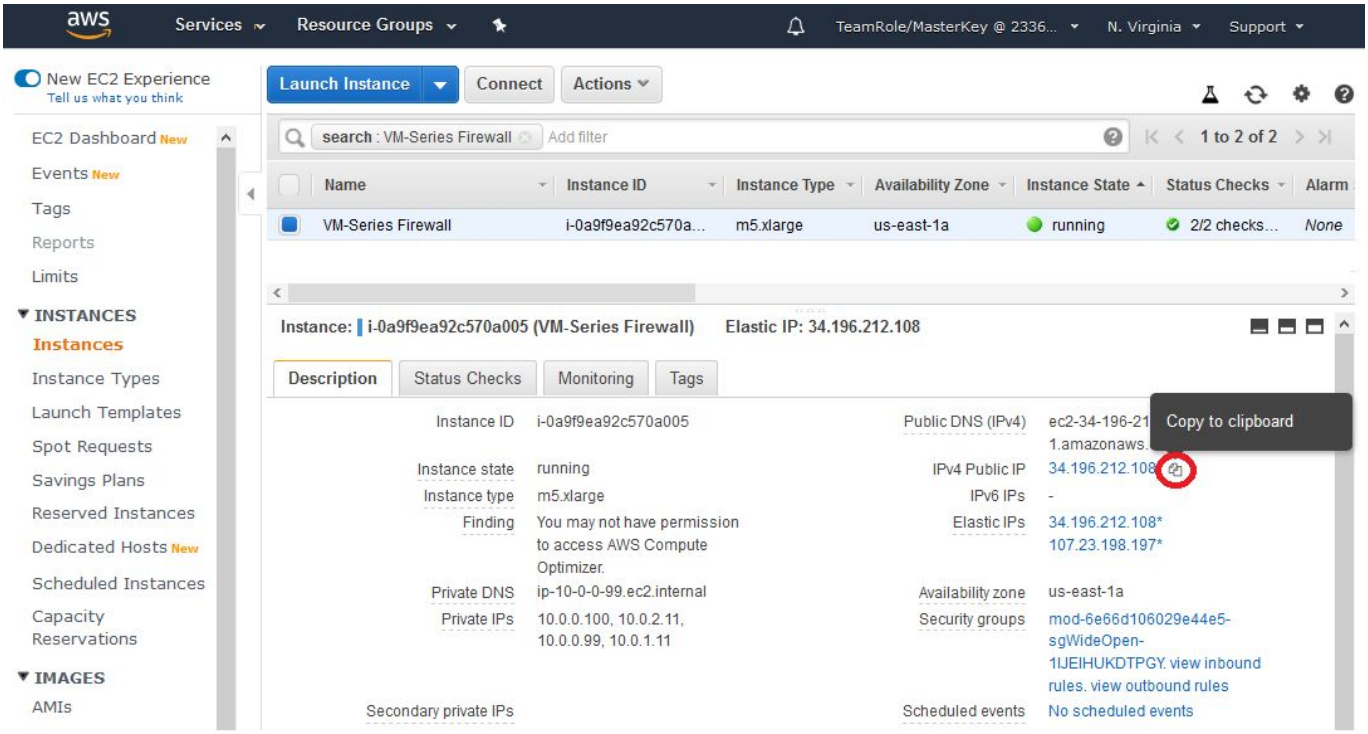
Activity 2 - Access and Review VM-Series Firewall and Servers

In this activity, you will:

- Access the VM-Series firewall and review it's configuration.
- Access the web and DB server to ensure the lab environment is set up correctly.

Task 1 - Access the VM-Series Firewall

Step 1. Go to the ***EC2*** console and search for VM-Series Firewall. Under the description, there will be an entry for IPv4 Public IP. "Click on Copy to clipboard".

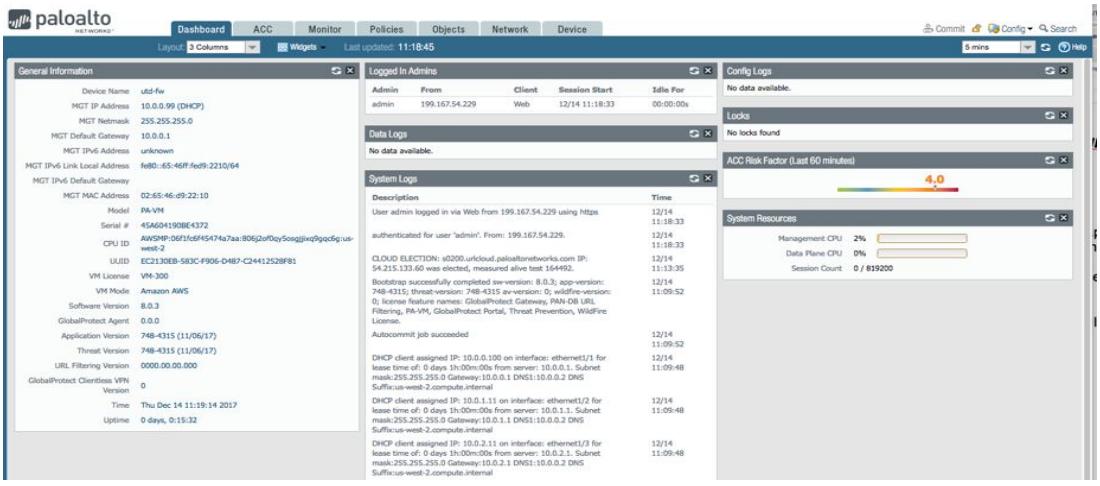


Log in to the firewall using the IP address. Open a browser, type “https://<IP-ADDRESS>” and then the following credentials (Note: you will get a browser certificate error due to self-signed certificates being used in the workshop):

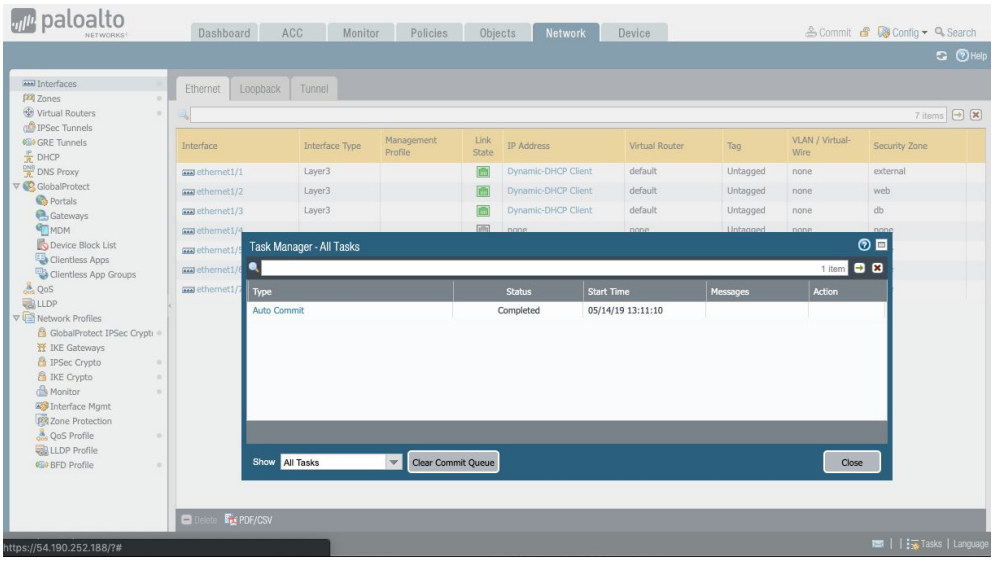
Username: **admin**

Password: **AWS@dmin123**

Step 2. After successfully logging in, you will see the default Dashboard view:



Step 3. Click on the **Network** tab to see the interfaces with zone settings. You should have three interfaces. If Link State is not green for all three interfaces, check the Auto Commit status. The Auto Commit status should be Complete.



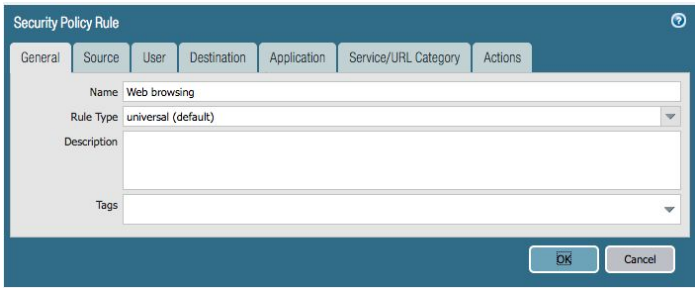
Step 4. Click on the **Policies** tab at the top of the page, and then **Security** in the left pane, to review the initial security policy:

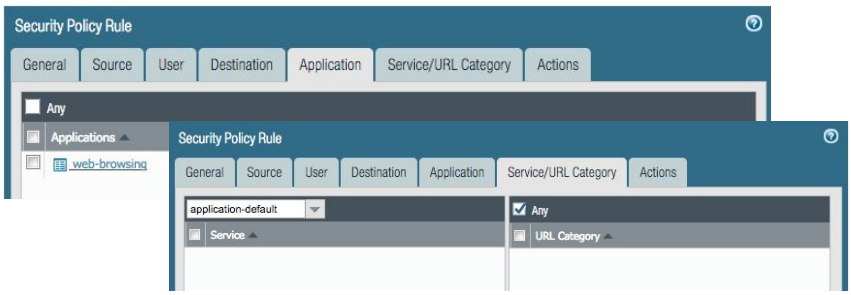
	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
1	SSH inbound	none	universal	external	any	any	any	db web	any	ssh ping	application-d...	Allow	none	
2	SSH 221-222 inbound	none	universal	external	any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

This is the initial policy that was in the bootstrap file used to configure the firewall. It has some basic policies to enable some protection that you will improve throughout the lab.

Step 5. Click on the ***Web browsing*** policy to review this policy that allows web requests from external (public) zones to the web server zone.

	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address					
4	Web browsing	none	universal	external	any	any	any	web	any	web-browsing	application-default	Allow	none	
8	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
9	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none

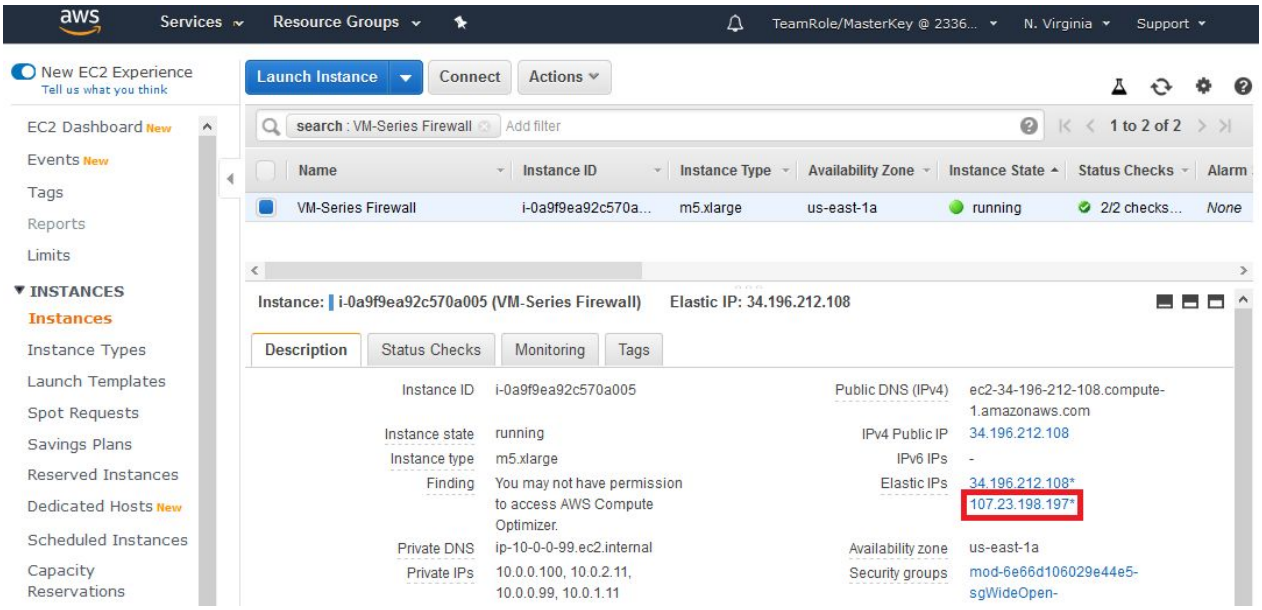


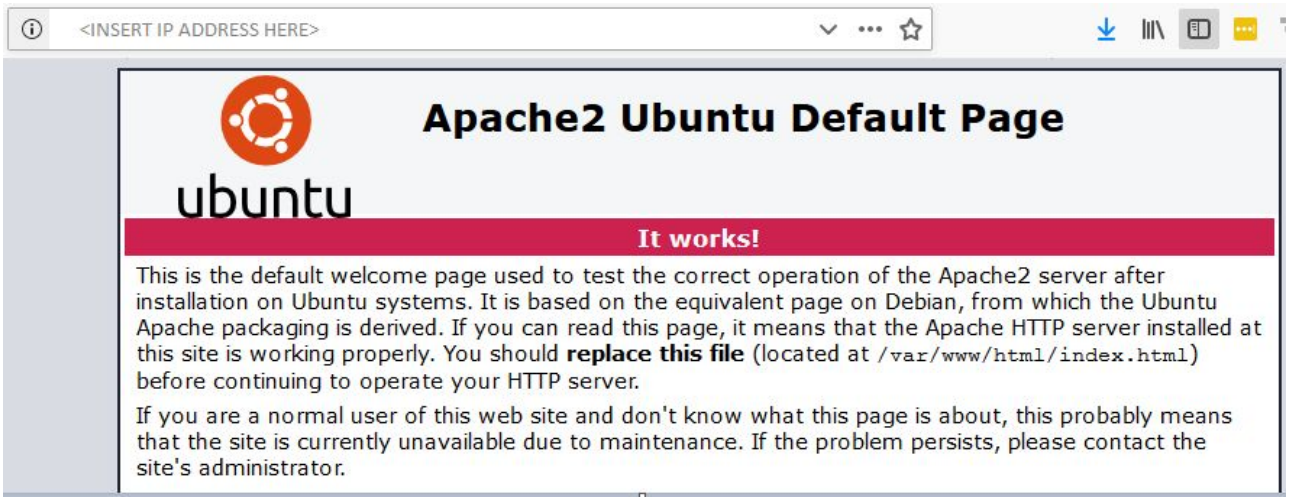


Task 2 - Access the Web Server

In this task, we will access the web server created by the CFT.

Step 1. Go back to ***EC2 Console*** and search for ***VM-Series Firewall*** again. Now, copy the second IP address from ***Elastic IPs*** and paste it into a web browser of your choice. You should see the Apache2 default page.



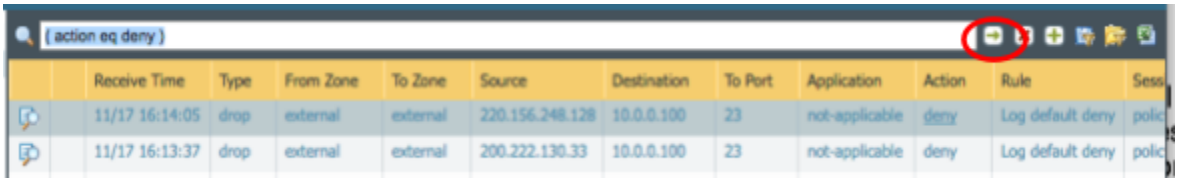


This indicates the web server is up and accessible from the internet.

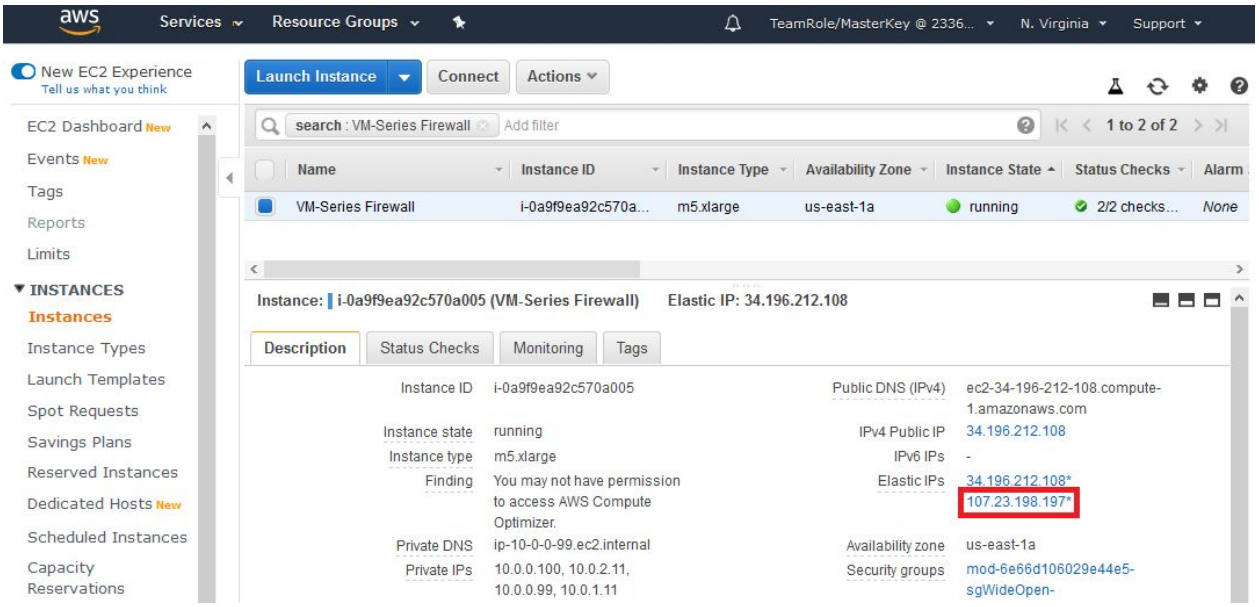
Step 2. Return to your firewall UI and click on the ***Monitor*** tab on the top of the page and ***Traffic*** under ***Logs*** in the left pane. You should see ***web-browsing*** logs such as:

Step 3. You may see other traffic from malicious scripts that are constantly scanning internet addresses for vulnerable services. If there is so much traffic that you cannot see your web-browsing logs, type an application filter above the logs with the text ***app eq web-browsing***, such as:

Step 4. Clear the filter, then enter ***action eq deny*** in the filter (or click on ***deny*** under ***Action***) and then click on ***Apply Filter*** arrow. Note that lots of traffic is being dropped from an ***external*** zone to an ***external*** zone. Those indicate traffic scanning the internet address for vulnerable services.



Step 5. Now, let us verify we can pass east-west (web to DB) traffic through the firewall. In this lab, the WordPress front application is also running on the web server. The database used by WordPress is configured on a database server instance in a different network. In the browser, head to the EC2 console and copy the second IP address, same as with the web server. Paste it into your browser and add "/wordpress" at the end (e.g., http://169.256.169.256/wordpress). You should then see the WordPress welcome screen:



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

Step 6. Head back to the firewall and verify that the traffic did indeed go through the firewall from **Web to DB** (Remove the last filter by clicking on the red x if needed):

	02/24 14:51:49	start	web	db	10.0.1.101		10.0.2.101	3306	mysql	allow	Web to DB	n/a	375
	02/24 14:51:48	start	web	db	10.0.1.101		10.0.2.101	3306	mysql	allow	Web to DB	n/a	375
	02/24 14:51:48	start	external	web	199.167.55.50		10.0.0.100	80	web-browsing	allow	Web browsing	n/a	705

Step 7. If you have trouble seeing the log entries for traffic you generated, you can create a traffic log filter as above with the entry **(app eq mysql) or (app eq web-browsing)** such as:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
02/12 05:18:39	end	external	web	52.52.133.159		10.0.0.100	80	web-browsing
02/12 05:18:33	end	web	db	10.0.1.101		10.0.2.101	3306	mysql
02/12 05:18:17	start	web	db	10.0.1.101		10.0.2.101	3306	mysql
02/12 05:18:17	start	external	web	52.52.133.159		10.0.0.100	80	web-browsing

Step 8. You have now successfully confirmed the deployment of the VM-Series firewall in AWS. Next, you will review a series of attack demo videos and configure your firewall to block each of these attacks plus many other threats.

Activity 3 - Protect Web Server from Brute Force Attacks

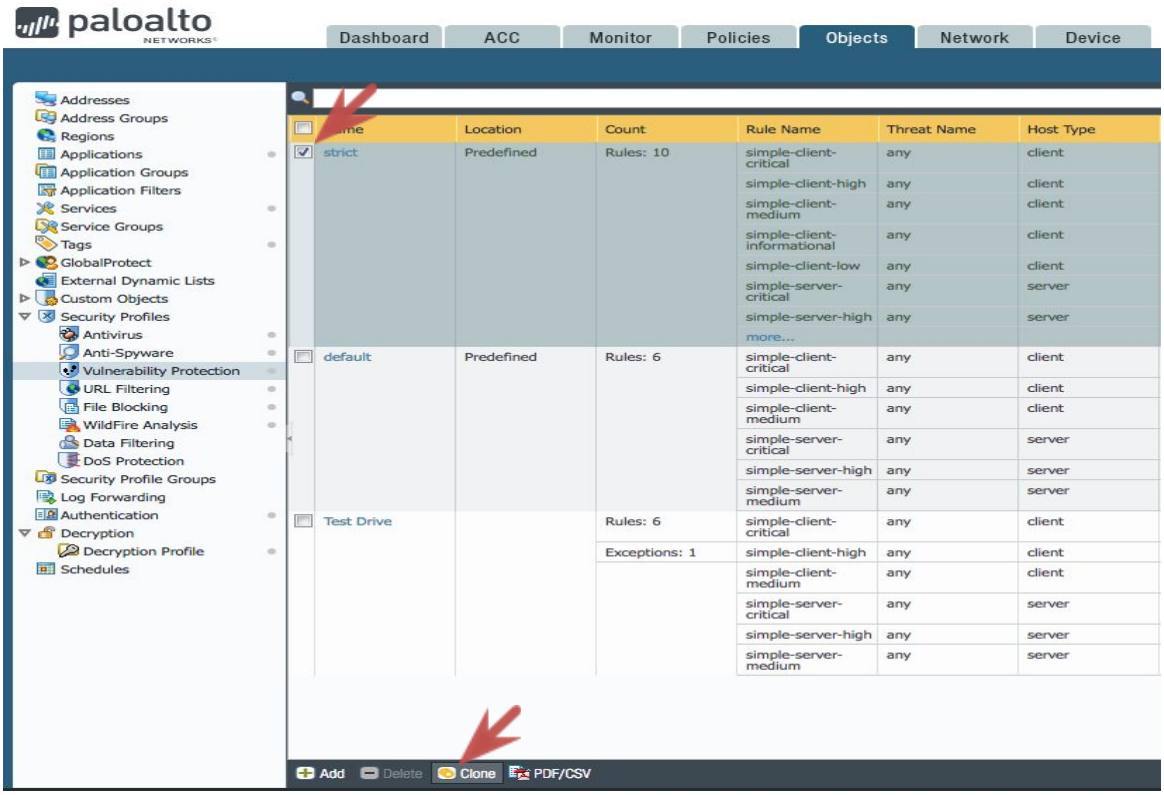
In this activity, you will:

- Configure the firewall to block many inbound attacks for web servers, including brute force login attacks for WordPress.

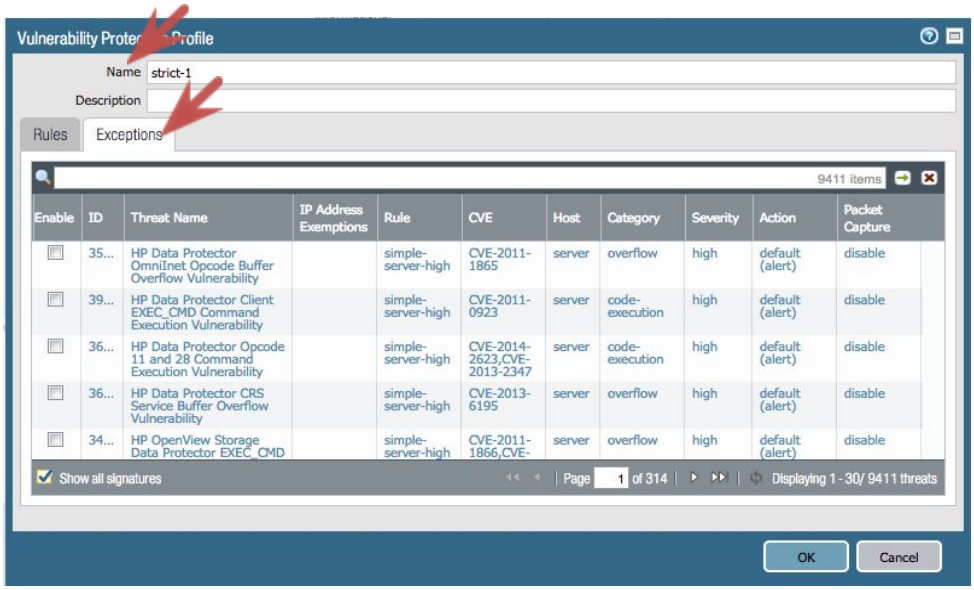
Task 1 - Create a New Vulnerability Protection Profile for WordPress

Step 1. In the VM-Series UI, click the ***Objects*** tab. On the left panel under ***Security Profiles***, click on ***Vulnerability Protection***.

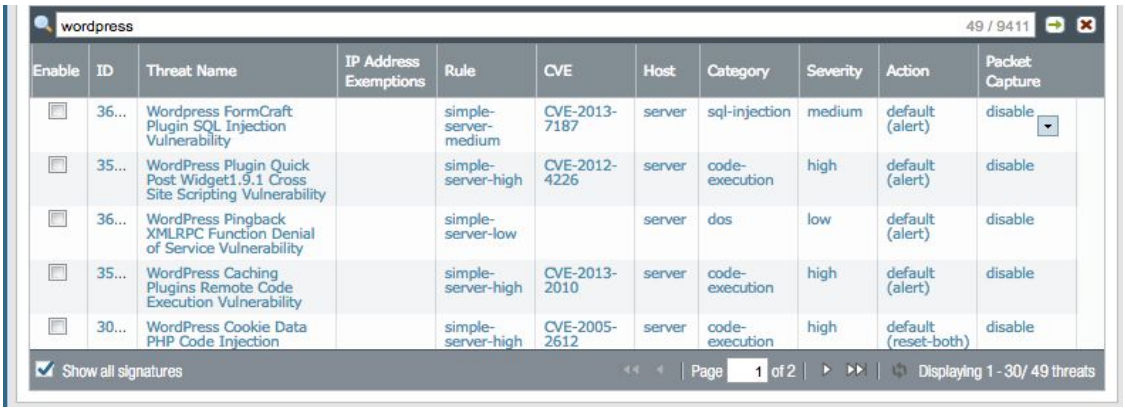
Step 2. Click the checkbox next to the built-in ***strict*** profile, and click on ***Clone*** at the bottom of the page. Then, click ***OK*** in the pop-up dialog. You should get a new ***strict-1*** profile at the bottom of the list.



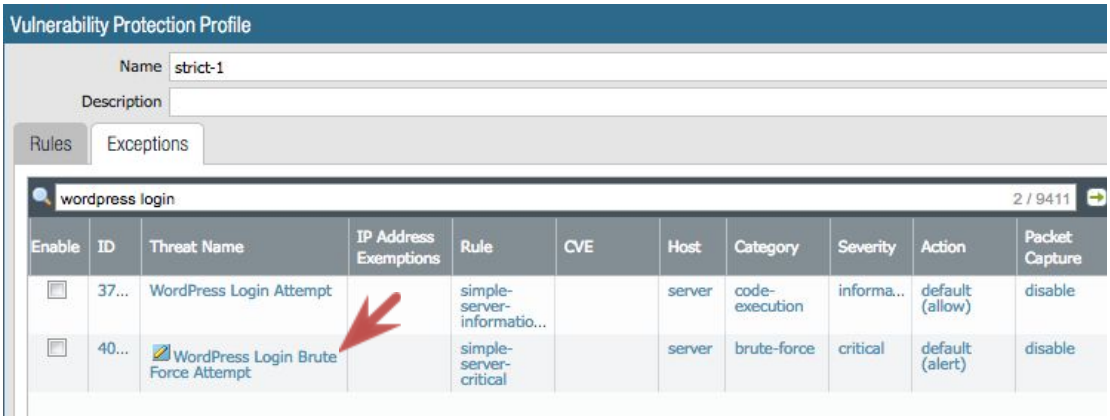
Step 3. Click on the name ***strict-1*** to bring up the profile configuration screen. Then, click on the ***Exceptions*** tab and check the ***Show all signatures*** option at the bottom of the page.



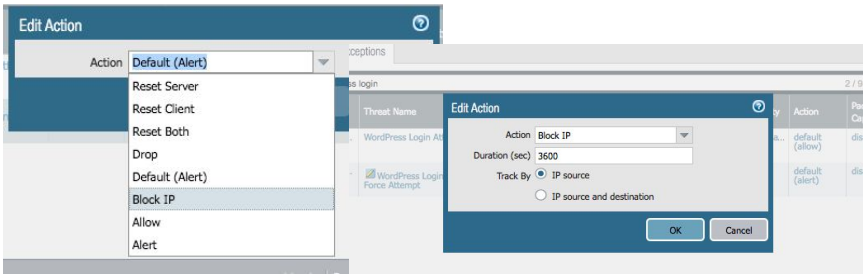
Step 4. Next, type ***wordpress*** in the search dialog and click the apply arrow. You should end up with about 50 matches.



Step 5. Notice the many WordPress vulnerabilities automatically prevented by the VM-Series firewall. Scroll down the list and find the ***WordPress Login Brute Force Attempt*** entry. It may be on Page 2, near the bottom of the list. You can change the filter to ***wordpress login*** to make it easier to find.

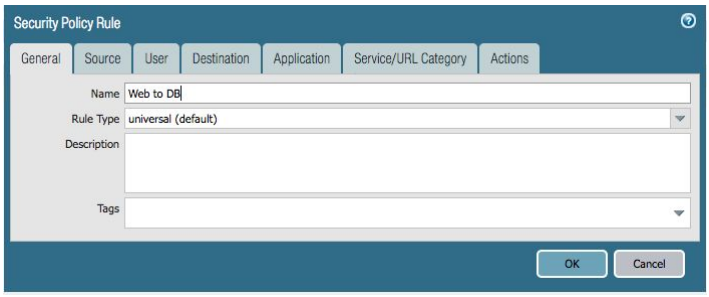


Step 6. This object has configuration options. Click on the ***default (alert)*** option in the ***Action*** column and change the default behavior from ***Alert*** to ***Block IP***. Set the duration to ***3600*** seconds (one hour), click ***OK*** on the ***Edit Action*** window, and click ***OK*** on the ***Vulnerability Protection Profile*** window.

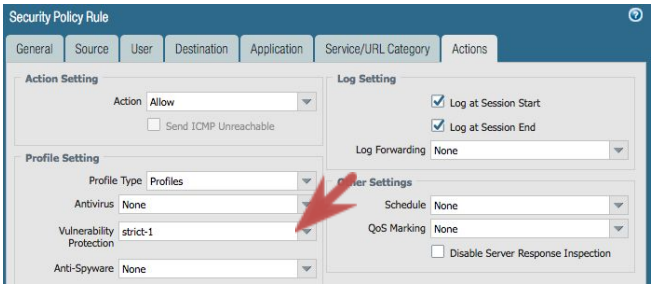


Task 2 - Apply the WordPress Protection in Policy

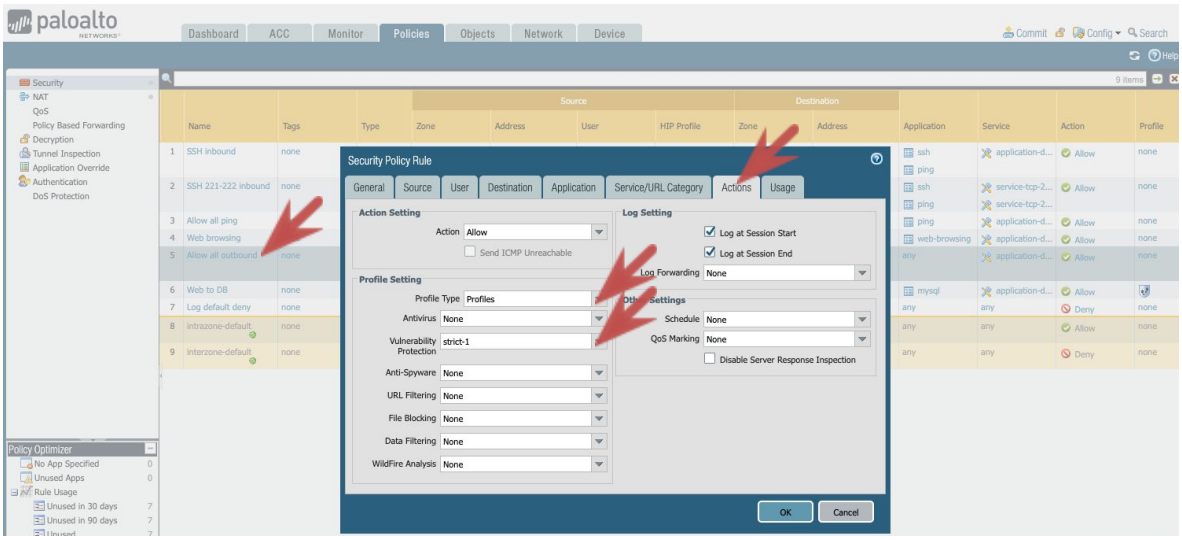
Step 1. Next, you need to edit your security profile to use this new vulnerability protection. Click on the ***Policies*** tab, and click on the ***Web to Db*** rule:



Step 2. Next, click on the ***Actions*** tab and change the ***Profile Setting*** for ***Vulnerability Protection*** option to ***strict-1***.

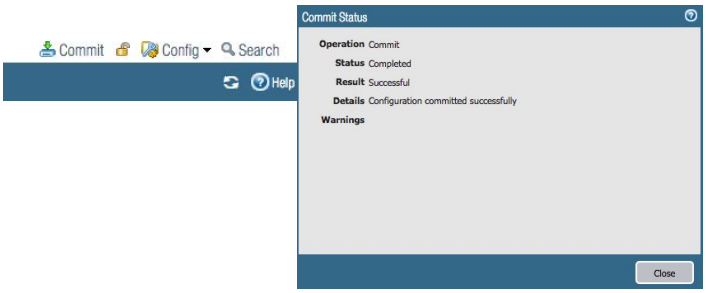


Step 3. Repeat the same steps above to add the ***strict-1*** vulnerability profile to the ***Allow all outbound*** rule. Click on the rule name, click on the ***Actions*** tab, change the ***Profile Type*** to ***Profiles***, and change the ***Vulnerability Protection*** setting to ***strict-1***.



At this point, you can commit your changes on the firewall.

Step 4. Click ***Commit*** on the top right of the screen to monitor the progress.



Note: If you have any commit errors, use the error description to resolve the conflict and recommit. Ask for assistance from your instructor if needed.

Activity 4 - Enable Outbound Security

In this activity, you will:

- Create an Application Group to simplify policy configuration
- Configure security policy to control outbound traffic. This will secure traffic generated by the web or DB server to prevent data exfiltration.

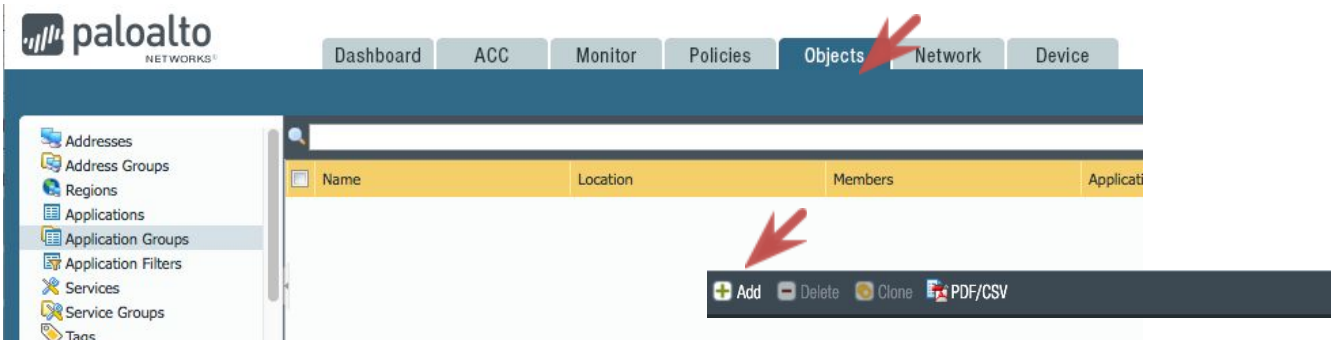
We will create a group of allowed outbound applications for the web server, named Allow-Outbound-Apps, and then apply it to the policy that will only allow these applications to go out on the default ports.

Allowed applications: SSL, NTP, DNS, web-browsing

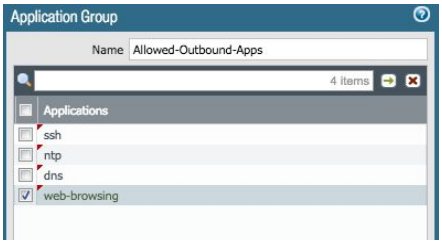
Since the web server is running as a WordPress server, you may want to allow your web browsing application to access any external links if needed. This will close all unnecessary services, such as FTP, telnet, SMTP, or POP, on your web server.

Task 1 - Create Application Group

Step 1. Return to the firewall UI, click the ***Objects*** tab and click ***Application Groups***. Click ***Add*** to create a new application group.

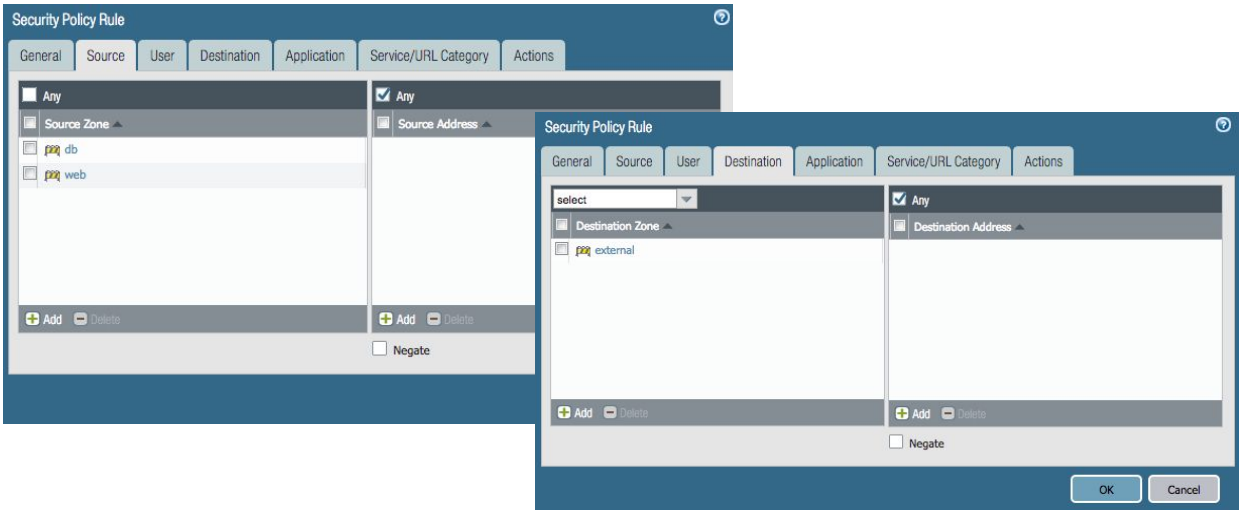


Step 2. Name the application group: ***Allowed-Outbound-Apps***. Add ***ssh, ntp, dns*** and ***web-browsing*** to this application group. Click ***OK*** to save the application group.



Task 2 - Limiting Outbound Traffic and Blocking File Exfiltration

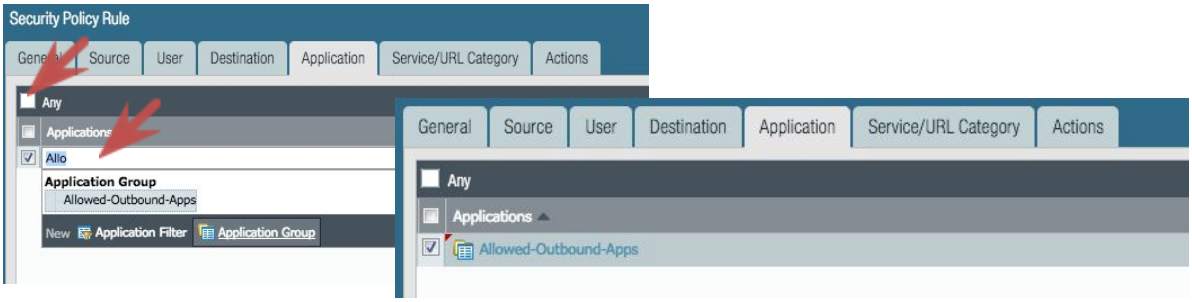
Step 1. Click on the ***Policies*** tab. Click on the ***Security*** option on the left panel if not already highlighted. Click on the ***Allow all outbound*** rule and review the ***Source*** and ***Destination*** tabs.



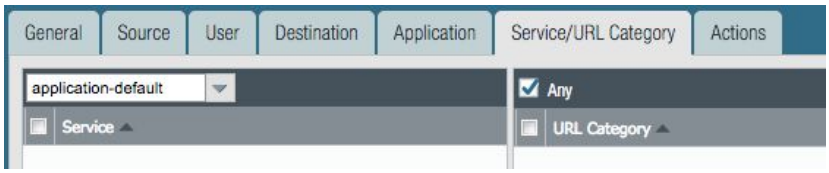
Step 2. We will limit outbound traffic only to the applications in the ***Allowed-Outbound-Apps*** applications group. This will greatly reduce any "call home" or "command and control" connections from the networks and thus further reduce risks in your network.

Note: The firewall does not just open up TCP port 80 or 443 and assume the traffic is web-browsing or SSL. The firewall verifies the application protocol is in use and used properly. This prevents, for example, an application like FTP from using 80 or 443 as a nonstandard port to exfiltrate data.

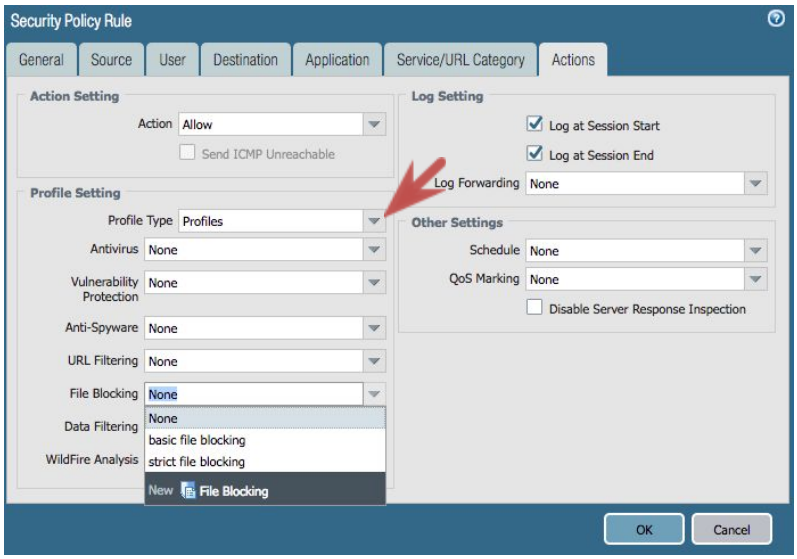
Step 3. Click on the ***Application*** tab and uncheck the ***Any*** checkbox. Type ***Allowed*** and select ***Allowed-Outbound-Apps*** in the search results list. Verify your rule looks like this before proceeding:



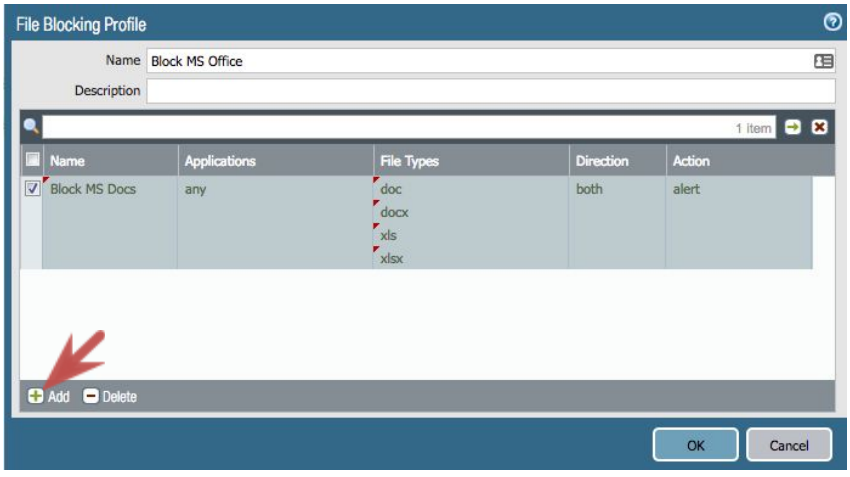
Step 4. Click on ***Service/URL Category*** tab. Note that ***application-default*** is selected and that will only allow applications to run on its default, but not others. Note also that you don't need to remember what the port numbers those applications use—the firewall will choose the default port number based on its App-ID™ database.



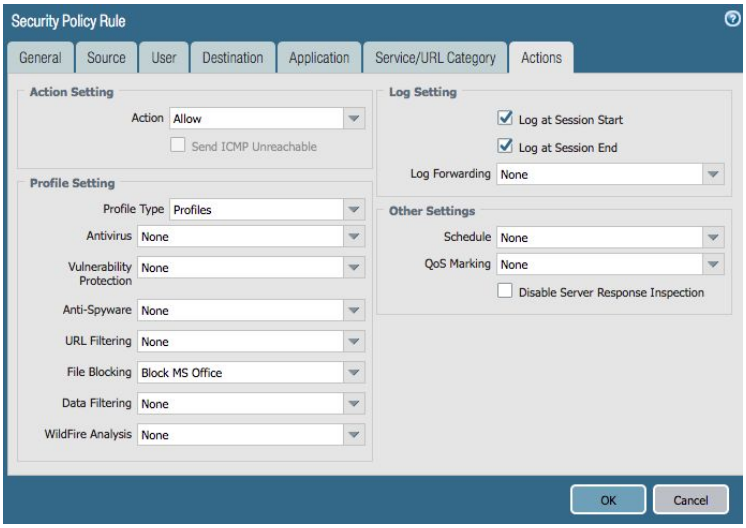
Step 5. Click on the ***Actions*** tab and change the ***Profile Type*** to ***Profiles***. Click on the ***File Block*** drop-down menu and select ***New File Blocking***.



Step 6. In the ***File Blocking Profile*** window, click in the ***Name*** field and give the profile a name: ***Block MS Office***. Then click ***Add*** near the bottom of the window and give the rule a name, such as ***Block MS Docs***. Under the ***File Types*** column, add ***doc, docx, xls,*** *and* ***xlsx***.



Step 7. Verify your screen matches the above, and then click ***OK***. Your ***Security Policy Rule*** should look like this:



Step 8. Click **OK** to close the policy window, now that you have changed the ***Allow all Outbound*** policy to allow limited outbound applications. It is a good practice to rename this policy to ***Limited Outbound*** and **Commit** the changes. Now, you have successfully limited the outbound application traffic, providing an extra layer of protection.

Activity 5 - Leverage a Threat Intelligence Cloud with VM-Series

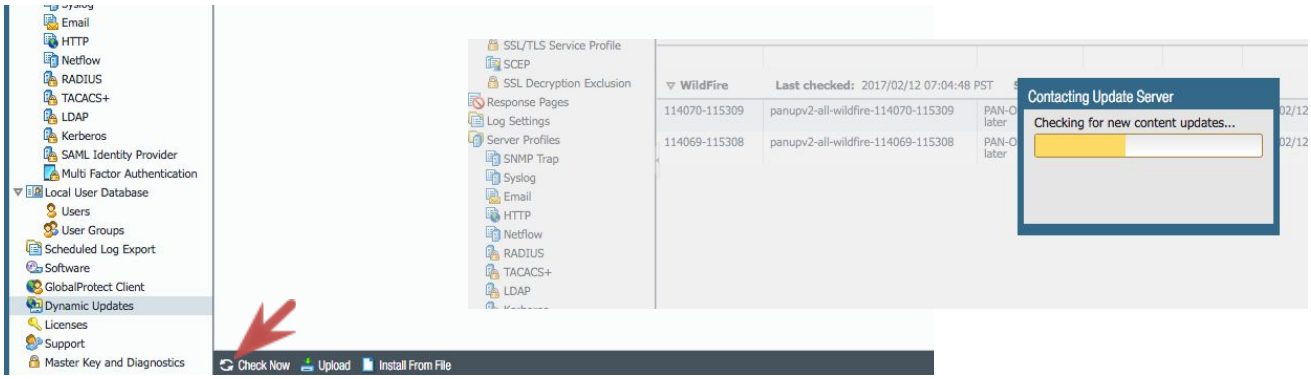
In this activity, you will:

- Configure an External Dynamic List that will be automatically updated based on an external source.
- Configure the firewall to block or allow traffic based on the external list contents.

Task 1 - External Dynamic List

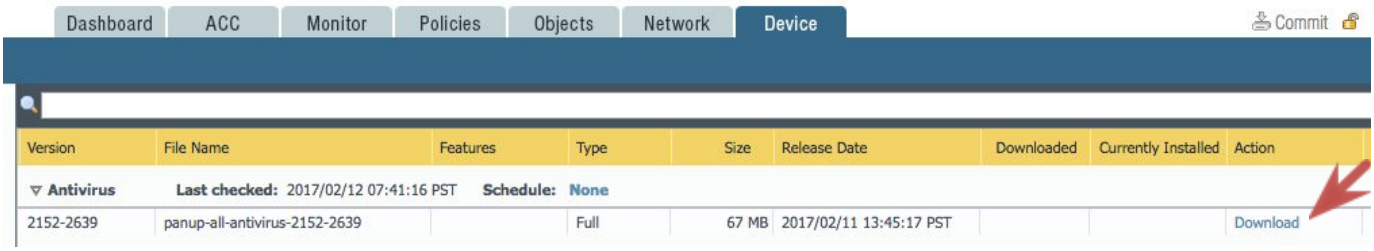
Step 1. In the firewall UI, click ***External Dynamic List*** in the ***Objects*** tab. You will not see any list in the External Dynamic List window.

Step 2. Update to the latest security content to ensure support for External Dynamic Lists. Click on the ***Device*** tab. Click on ***Dynamic Updates*** on the bottom left, and click on ***Check Now*** on the bottom.

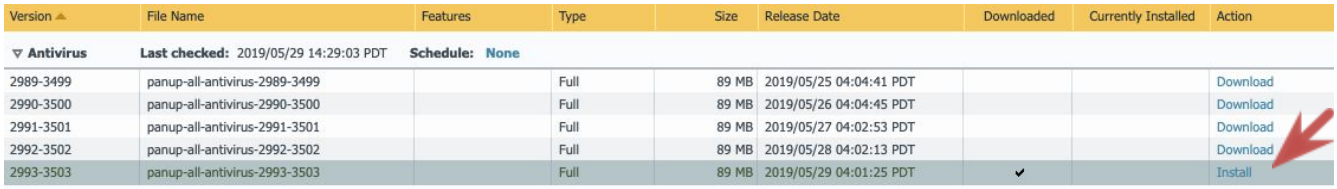


Step 3. Under ***Antivirus*** in the center pane, select the latest update and click ***Download*** in the ***Action*** column. The download will take a couple of minutes.

Note: You might have to install Application and Threat content before installing the Antivirus content, if it's not installed during the firewall bootstrap process.

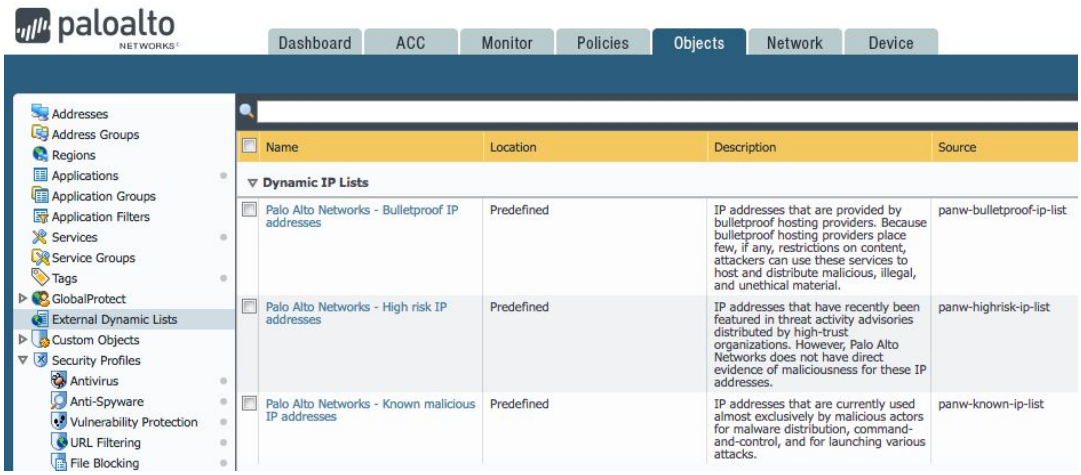


Step 4. Once the download is complete, click ***Install*** in the ***Action*** column. You should now have an installed Antivirus version at or above the following:



Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action
Antivirus	**Last checked:** 2019/05/29 14:29:03 PDT	**Schedule:** None						
2989-3499	panup-all-antivirus-2989-3499		Full	89 MB	2019/05/25 04:04:41 PDT			Download
2990-3500	panup-all-antivirus-2990-3500		Full	89 MB	2019/05/26 04:04:45 PDT			Download
2991-3501	panup-all-antivirus-2991-3501		Full	89 MB	2019/05/27 04:02:53 PDT			Download
2992-3502	panup-all-antivirus-2992-3502		Full	89 MB	2019/05/28 04:02:13 PDT			Download
2993-3503	panup-all-antivirus-2993-3503		Full	89 MB	2019/05/29 04:01:25 PDT	✔		Install

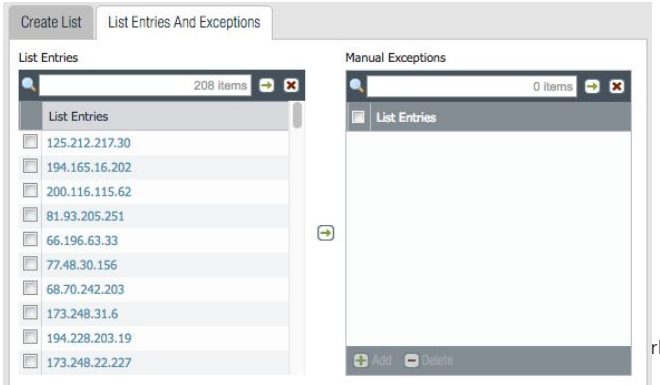
Step 5. This update will create three new Dynamic IP Lists. Click on the ***Objects*** tab, and click on ***External Dynamic Lists*** in the left pane. Review the three lists that are provided by Palo Alto Networks.



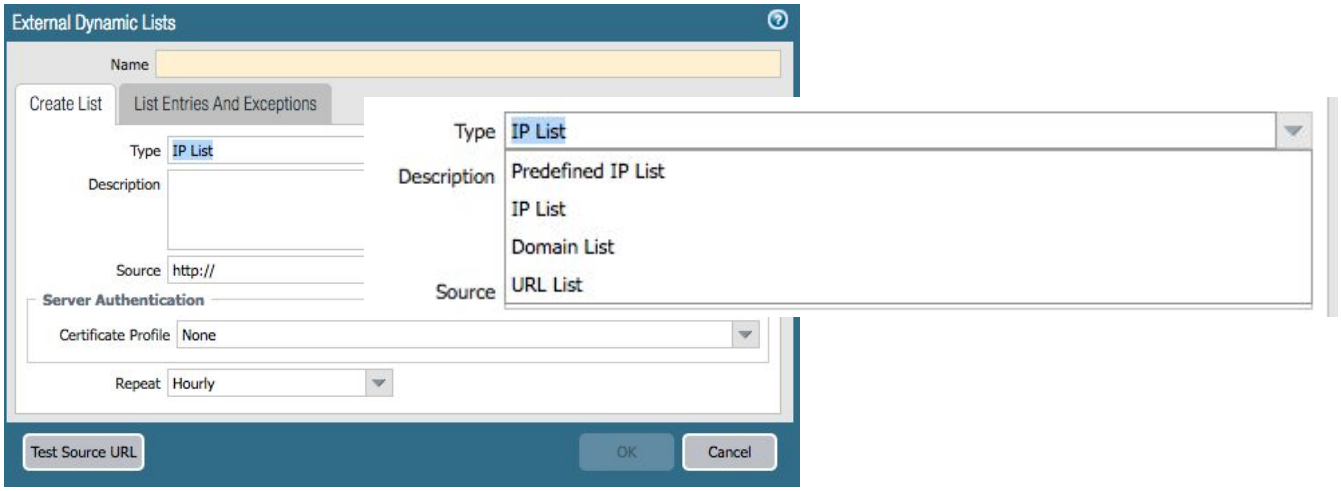
Step 6. Click on the name of the ***Palo Alto Networks – Known malicious IP addresses***. This will open up the External Dynamic List window. Note that it is Read-Only because it is a predefined list provided by Palo Alto Networks.

Step 7. Click on the ***List Entries and Exceptions***. This will show you the content of the list. Click ***Cancel*** to close the window.

Note: There is a possibility that List Entries will be empty because of polling time. To update the list immediately, make some changes in the firewall (e.g., change the firewall's hostname by navigating to **Device > Setup > General Settings** and clicking on the edit icon; configure, and commit). Repeat step 7 after commit.



Step 8. Click ***Add*** at the bottom to open up a new ***External Dynamic List*** window. You can create different types of dynamic list from different sources. Review the supported types in the ***Type*** drop-down list.

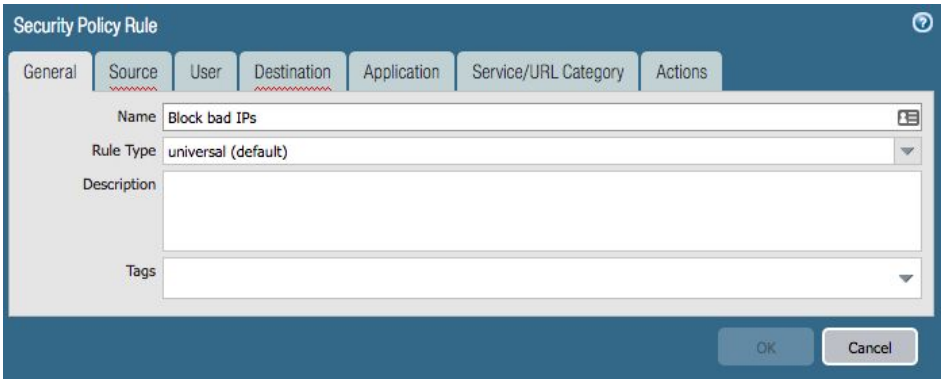


Step 9. We will not create an External Dynamic List here, but we will see how you can apply the predefined list to a policy in the next task. Click ***Cancel*** to close the window.

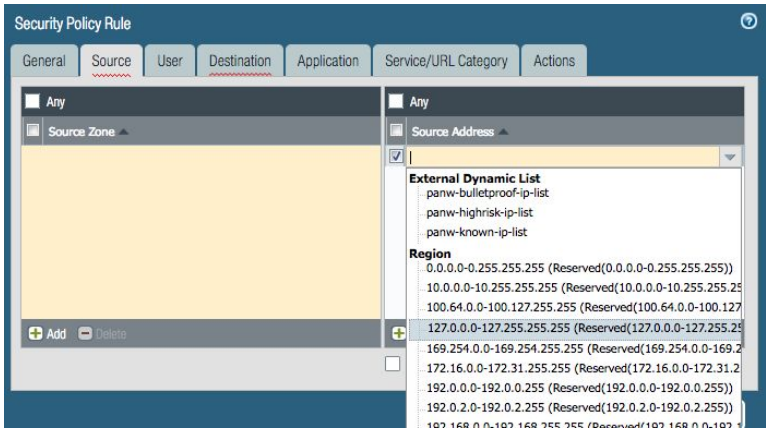
Task 2 - Create Policy Using the External Dynamic List

Step 1. Next, you will create a security policy to block any traffic to or from these known bad IPs. First, create a rule to block traffic from these IPs. Go to the ***Policies*** tab and select ***Security*** from the left pane if not already selected. Click ***Add*** at the bottom of the page.

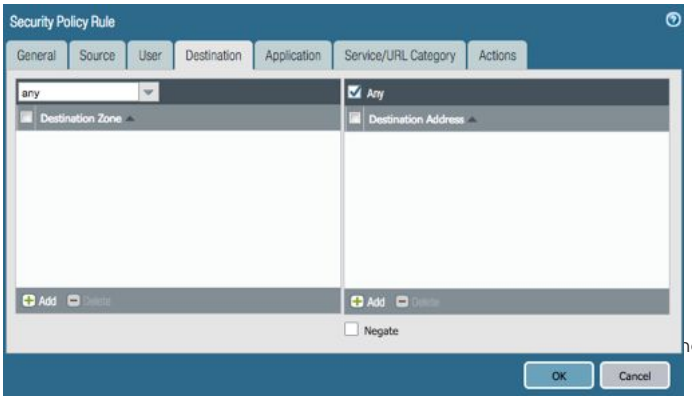
Step 2. Give the new rule a name, such as ***Block bad IPs***:



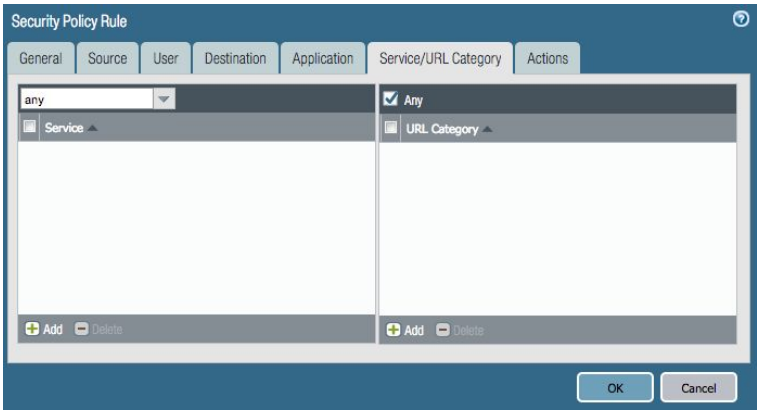
Step 3. Click on the ***Source*** tab and check ***Any*** for Source Zone. Then click ***Add*** in the ***Source Address*** window and add ***panw-highrisk-ip-list*** and ***panw-known-ip-list***.



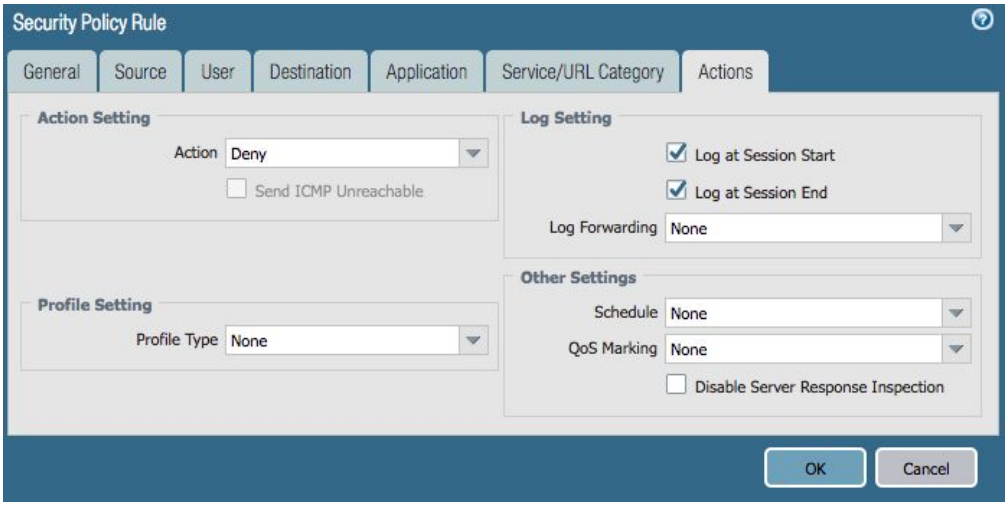
Step 4. Click on the ***Destination*** tab and set the zone to ***Any*** (keep the address at ***Any***).



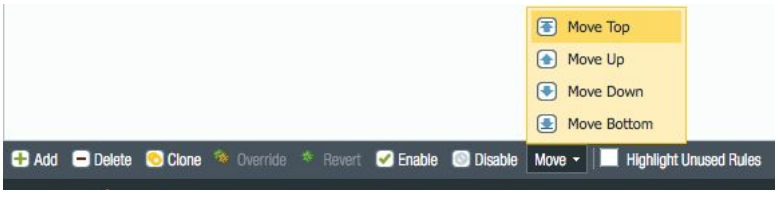
Step 5. Click on the ***Service/URL Category*** tab and change the service type to ***Any***.



Step 6. Click on the ***Actions*** tab and change the ***Action Setting*** to ***Deny***. Also select the ***Log Setting*** option ***Log at Session Start***.



Step 7. Highlight your new rule, click ***Move*** at the bottom of the page, and select ***Move Top***.



Step 8. Commit your changes.

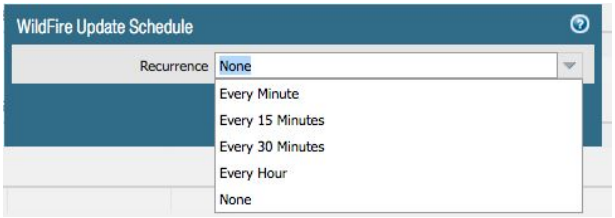
Extra: What if a server were compromised using some other technique (e.g., a user installed a pre-compromised AMI from an untrusted source)? How could the server be prevented from "phoning home" to receive command-and-control traffic? Configure your firewall to block outbound traffic to known bad destinations.

Task 3 - Configure Auto Dynamic Updates

The firewall can be configured to receive and install the latest dynamic updates based on the preferred interval. We will configure the WildFire® service to auto-update at specific intervals. WildFire deploys inline machine learning modules on the next-generation firewall (NGFW) to prevent new unknown file-based threats, protecting the first victim without any productivity delay.

Step 1. Click ***Dynamic Updates*** in the ***Device*** tab. In the ***WildFire*** section, click on ***None*** next to ***Schedule***.

Step 2. In the ***WildFire Update Schedule*** window, select ***Every 15 Minutes***. This will enable the firewall to download the latest WildFire updates at this interval.



Step 3. Select ***download-and-install*** in the ***Action*** field to ensure the updates are installed automatically.

Note: You can configure each dynamic update at a different internal, with different actions to cater to your needs.

Activity 6 - Use Dynamic Address Groups to Protect Dynamic EC2 Instances

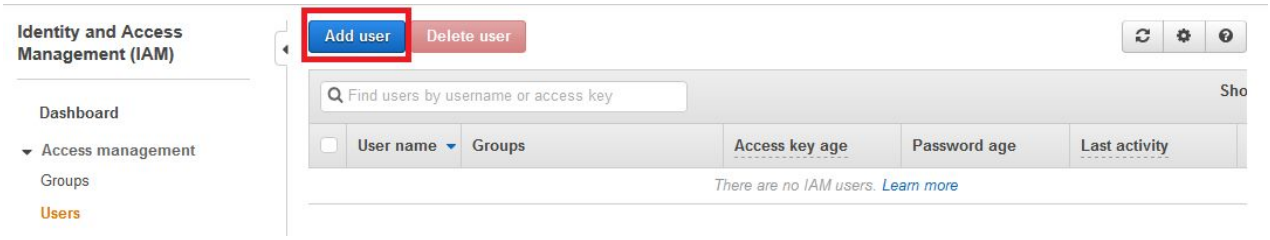
In this activity, you will:

- Enable the VM-Series firewall to integrate with the AWS VPC to retrieve VPC information.
- Configure the policy based on information retrieved.

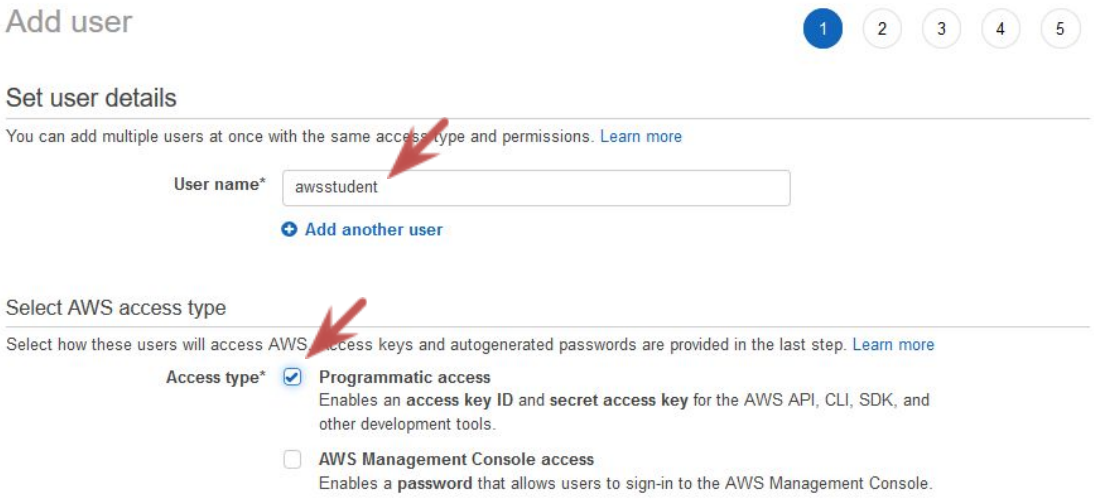
Task 1 - Create IAM Access Key for the Firewall Integration

An AWS access key is needed for the VM-Series to access the VM information in the VPC. We will create a new IAM user and access keys.

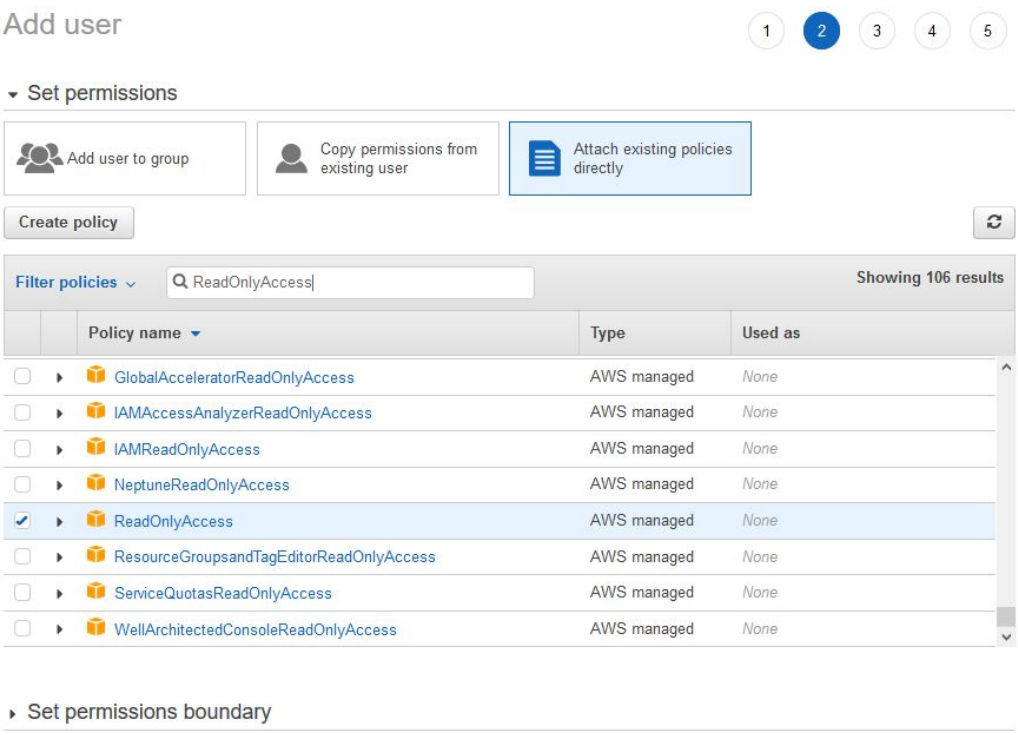
Step 1. In the AWS console, go to ***Services*** > ***IAM*** > ***Users***. Click on "Add user".



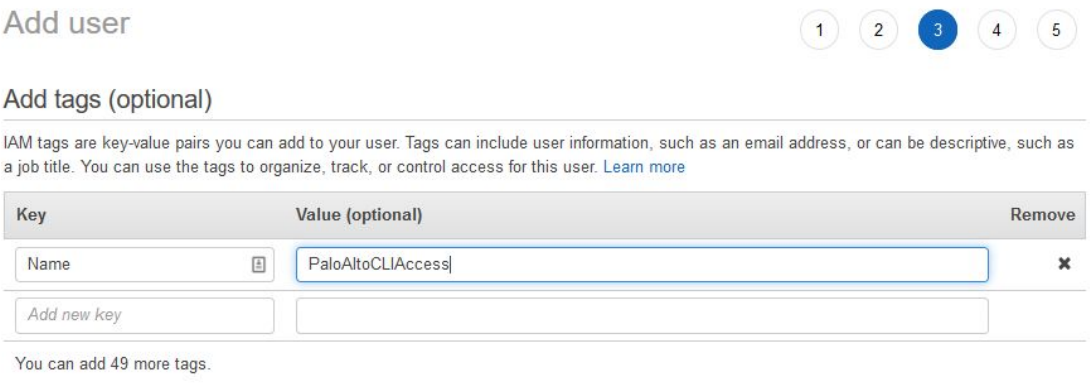
Step 2. Supply the username "awsstudent" and select "Programmatic access" as the access type. Then, click "Next:Permissions".



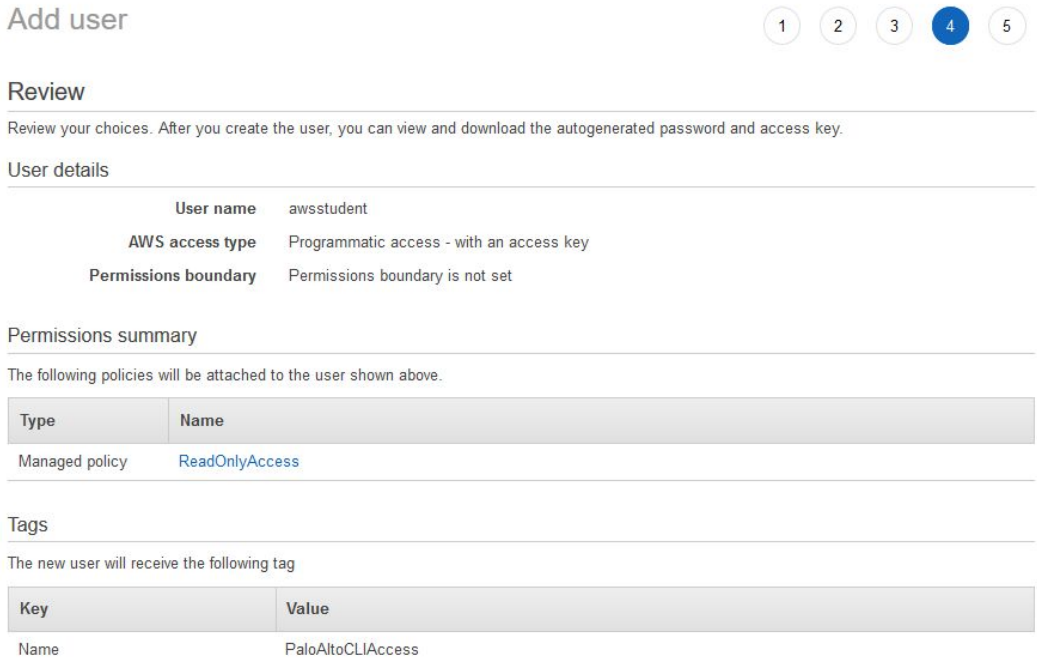
Step 3. Click on "Attach existing policies directly" and search for the "ReadOnlyAccess" policy (you need to scroll down to find it). Then, click "Next: Tags".



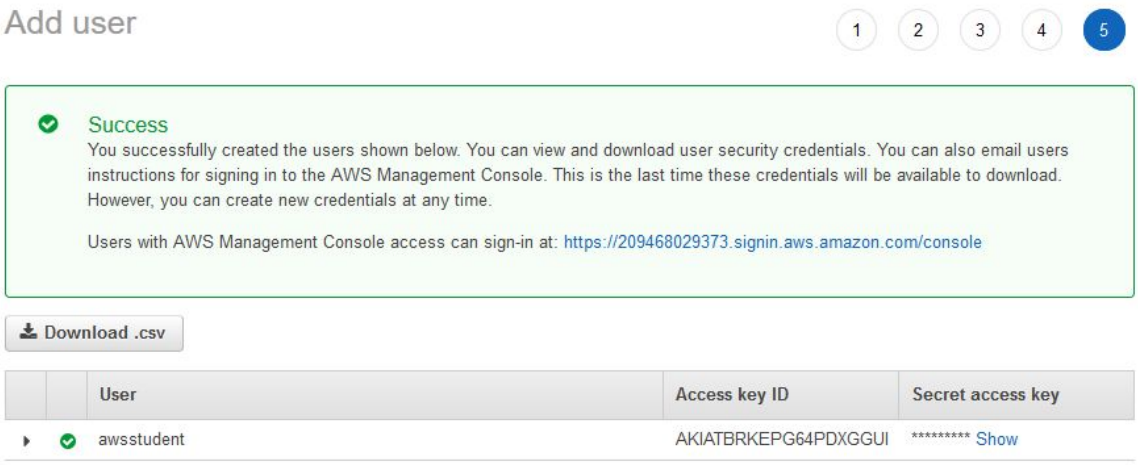
Step 4. Add "Name" for the first value, and then supply the value of the name (e.g., "PaloAltoCLIAccess"). Then, click "Next: Review".



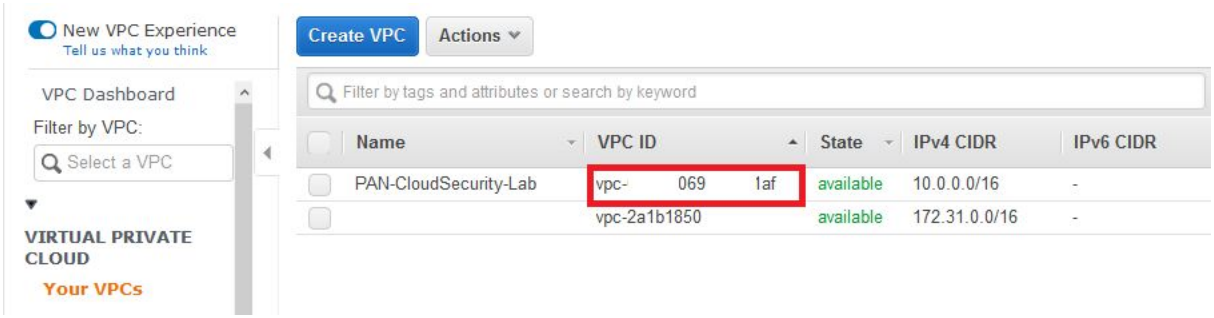
Step 5. Review new user details and click on "Create user".



Step 6. Download the .csv and save the Access Key and Secret Access Key, which you will need to use in the following tasks. Click on Close.

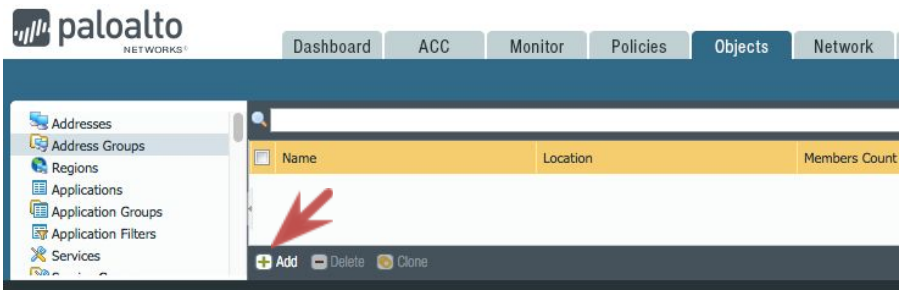


Step 7. Go to the **VPC Dashboard** and copy the **VPC-ID** for the lab VPC to a text file. You will need this for the configuration later.

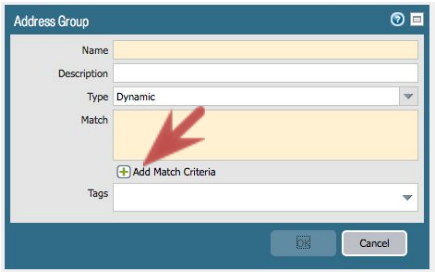


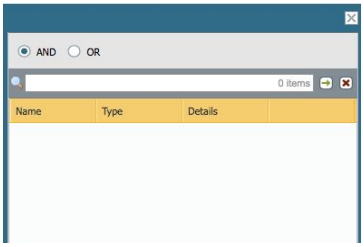
Task 2 - Review Dynamic Address Group in VM-Series

Step 1. In the VM-Series firewall, go to ***Address Groups*** in the ***Objects*** tab and click ***Add*** (at the bottom) to create a new address group.



Step 2. In the ***Address Group*** window, select ***Dynamic*** in ***Type***, then click ***Add Match Criteria***. You will see that the criteria window is empty.

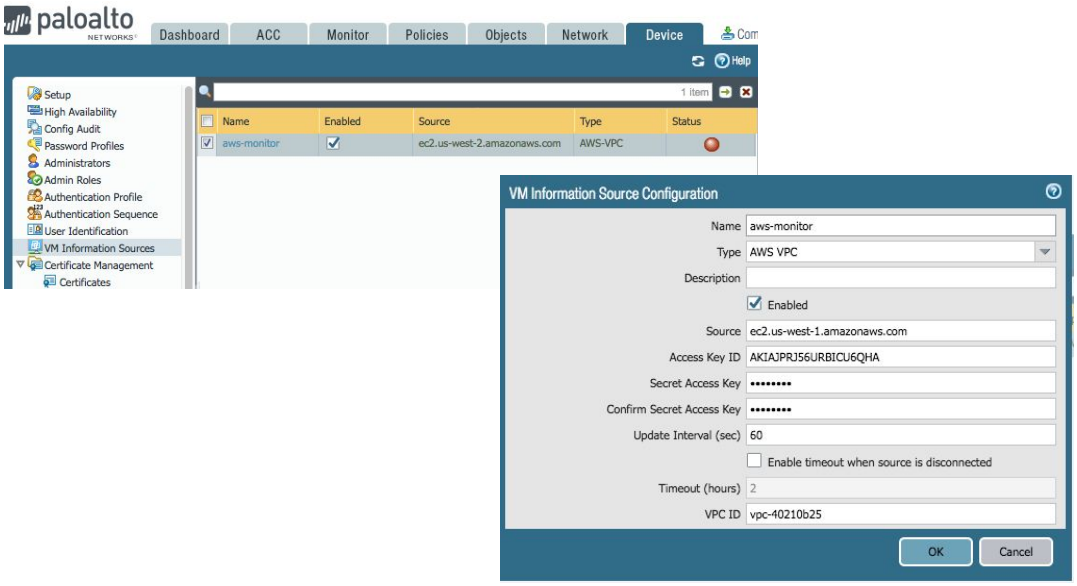




Step 3. Click ***Cancel*** to close the Address Group window. We will come back to create a Dynamic Address Group after we have configured the VM-Series to monitor your lab VPC.

Task 3 - Enable AWS Monitoring for Lab VPC

Step 1. In the VM-Series firewall, go to ***Device*** > ***VM Information Sources***. Note the red status indicator for the ***aws-monitor*** entry.



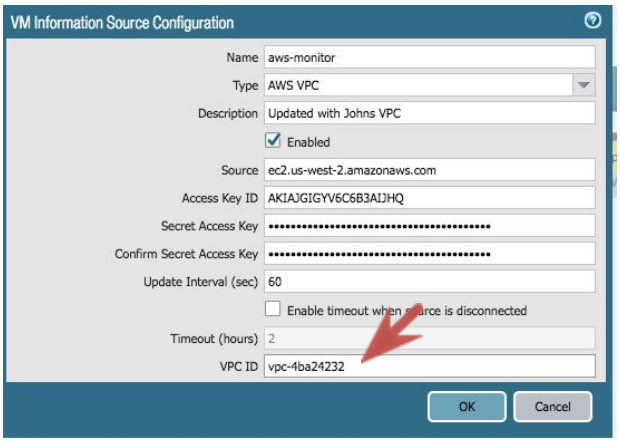
Step 2. The ***aws-monitor*** is created for you in the default lab configuration. Click the name to open the ***VM Information Source Configuration*** window.

Step 3. Add a short note to the Description field to indicate which VPC this configuration is for.

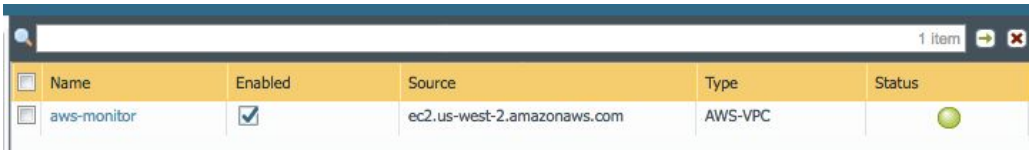
Step 4. Review the EC2 URL in the ***Source*** field to match the region you are using. If you are using ***us-west-2***, change the ***Source*** to ec2.us-west-2.amazonaws.com.

Step 5. Open the **accessKey.csv** file that you have downloaded in Task 1. Paste the **Access Key ID** and **Secret Access Key** to the configuration. Paste the Secret Access Key again into the confirmation field.

Step 6. Paste the VPC ID for the Lab VPC of your lab. Click ***OK*** to close the configuration window.



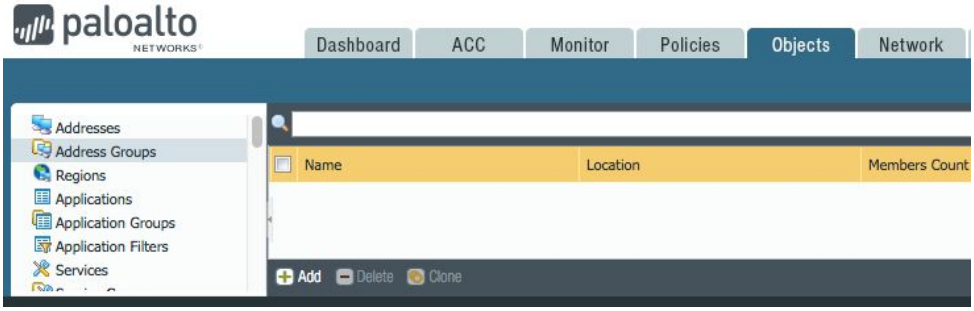
Step 7. Commit the changes. With the correct Source, Access Key, Secret Key, and VPC ID entered, you should see the status indicator update to green after committing the changes.



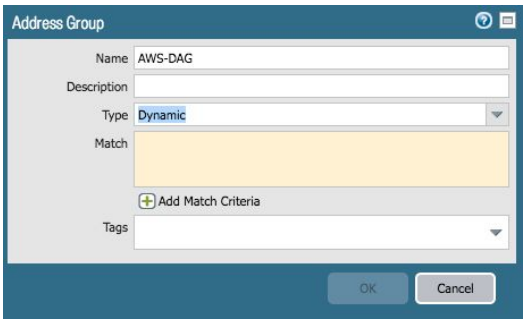
Note: If the ***aws-monitor*** status is still red, you will need to double-check the configuration and repeat Task 3 to ensure the status turns green before you can move on to Task 4.

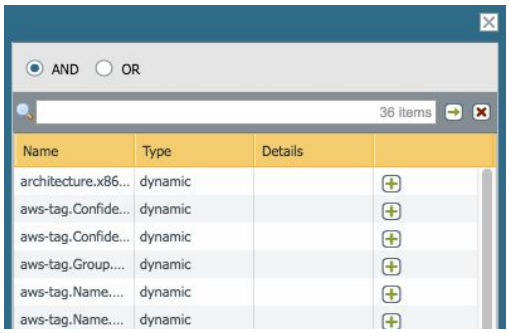
Task 4 - Create a Dynamic Address Group Using an AWS VPC Tag

Step 1. In the VM-Series firewall, go to ***Address Groups*** in the ***Objects*** tab. Click ***Add*** (at the bottom) to create a new address group.

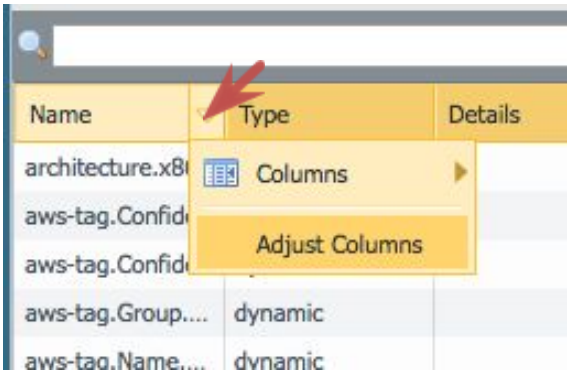


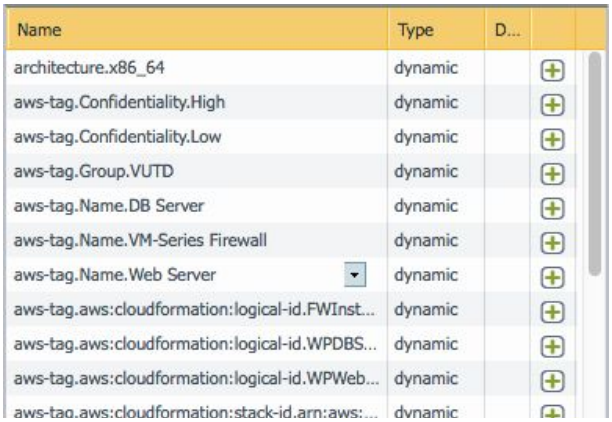
Step 2. Name it ***AWS-DAG*** or another name, select ***Dynamic*** in ***Type***, and then click ***Add Match Criteria***. You will see that the criteria window is now filled with dynamic info from the AWS VPC.





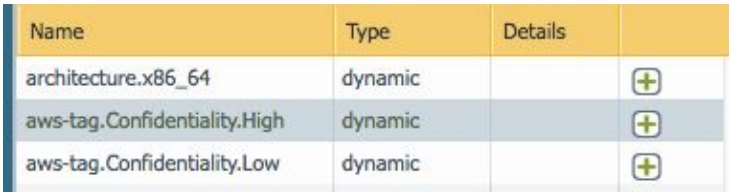
Step 3. In the criteria window, mouse over the column header ***Name***, click on the drop-down menu, and select ***Adjust Columns***. This will allow you to see the information much more easily. Take a look at the AWS attributes the VM-Series can monitor.

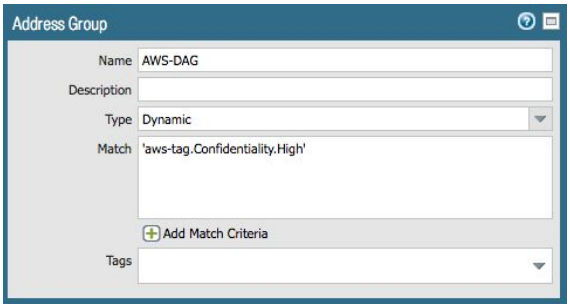




You can find the list of AWS VPC attributes the VM-Series can monitor here: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-aws/list-of-attributes-monitored-on-the-aws-vpc.

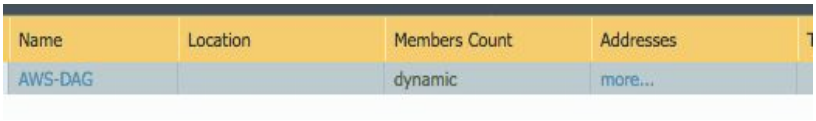
Step 4. Select the ***aws-tag.Confidentiality.High*** by clicking on the + below it. This will add this object to this Dynamic Address Group (DAG).





Step 5. Click ***OK*** to close the window, and click ***Commit*** to commit all changes.

Step 6. After clicking on Commit, click ***more...*** under the "Addresses" column for the address group you just created. You should be able to see the IP address of the VM that is tagged with "Confidentiality.High".

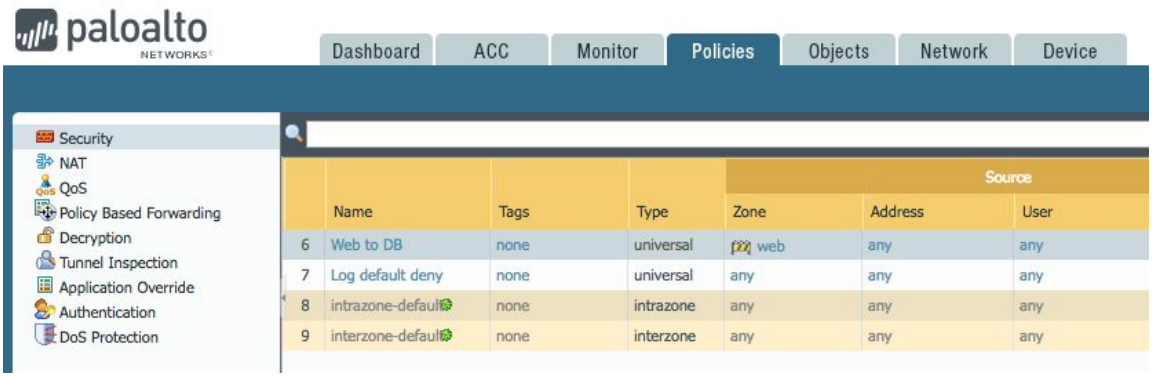


Step 7. Go to the EC2 dashboard in the AWS console. Determine if the database server tag and IP address match with what is in the VM-Series DAG.

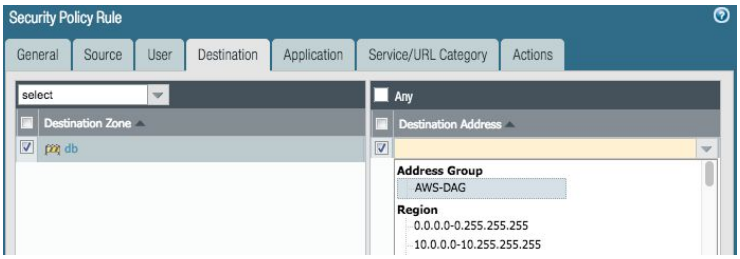
Task 5 - Create Policy with a Dynamic Address Group

Once a DAG is created successfully, you can apply specific policy with it. We will modify an existing policy using the DAG created in the previous task as an example.

Step 1. In the VM-Series, go to ***Policies*** > ***Security***, then click the ***Web to DB*** policy.

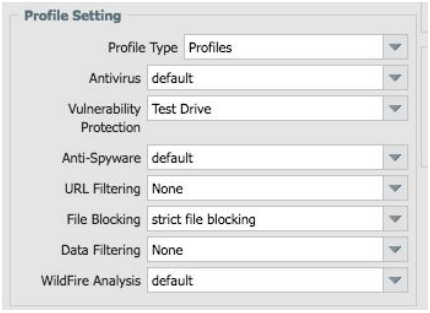


Step 2. Go to ***Destination***, click ***Add*** under the Destination Address, select the DAG you created in Task 4.



Step 3. Go to Actions, then select the following Profile to enhance the protection for this address group.

Antivirus: default
Vulnerability Protection: Test Drive
Anti-Spyware: default
File Blocking: strict file blocking
WildFire Analysis: default



Step 4. Click ***OK*** to close the window and commit the changes. You have created a more secure policy to protect specific addresses.

Activity 7 - Enable CloudWatch Integration to Publish PAN-OS Metrics

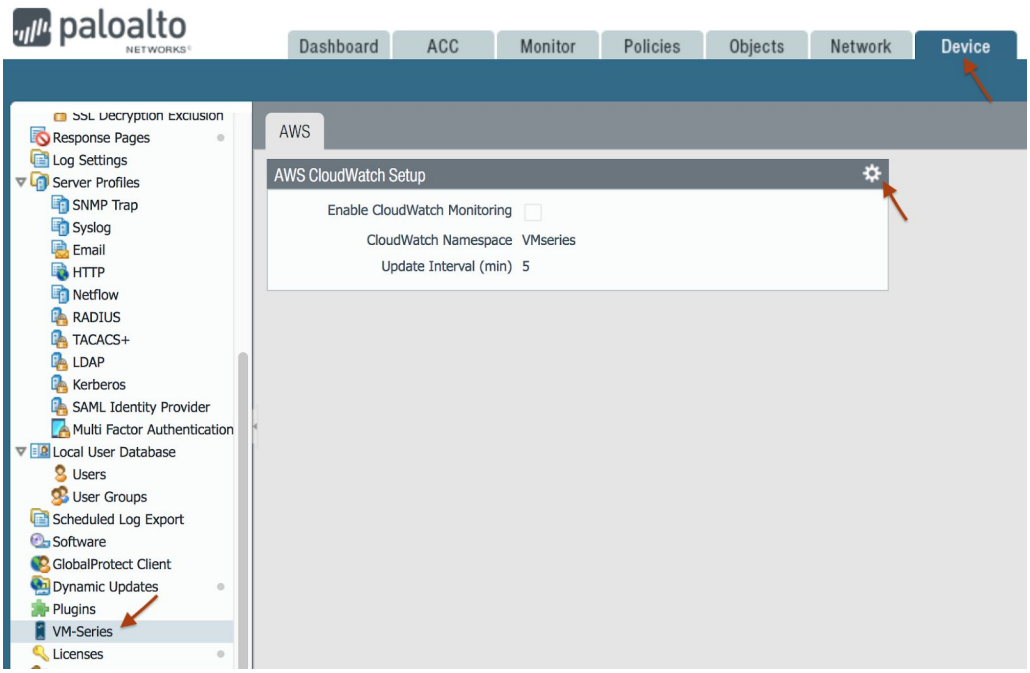
In this activity, you will:

- Enable the VM-Series firewall to integrate with AWS CloudWatch to publish native PAN-OS metrics to AWS namespace at a specified time interval.

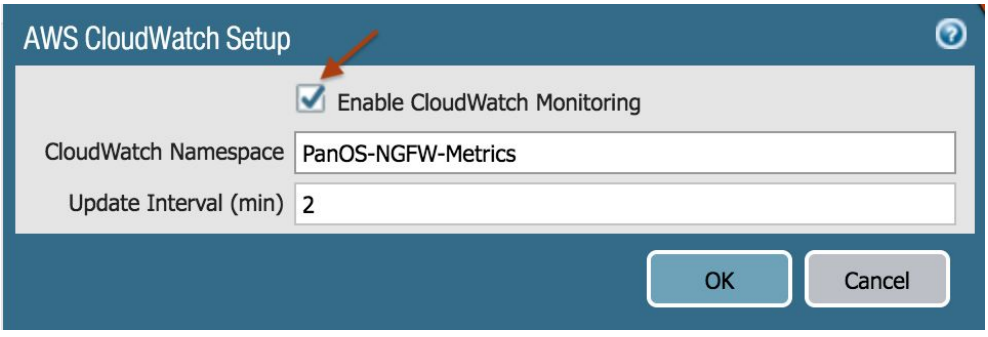
Task 1 - Enable CloudWatch on the VM-Series Firewall

In this task, you will configure the firewall VM-Series plugin to enable the integration with AWS CloudWatch.

Step 1. In the VM-Series firewall, go to ***Device***, scroll down in the left panel, select ***VM-Series***, and then click the edit icon .



Step 2. Select **Enable CloudWatch Monitoring** by clicking on the checkbox, then enter the **CloudWatch Namespace** PanOS-NGFW-Metrics or any other name. The namespace cannot begin with "AWS". You can also change **Update Interval** to 2 minutes. Update Interval is the frequency at which the firewall publishes metrics to CloudWatch. Click OK to close the window.

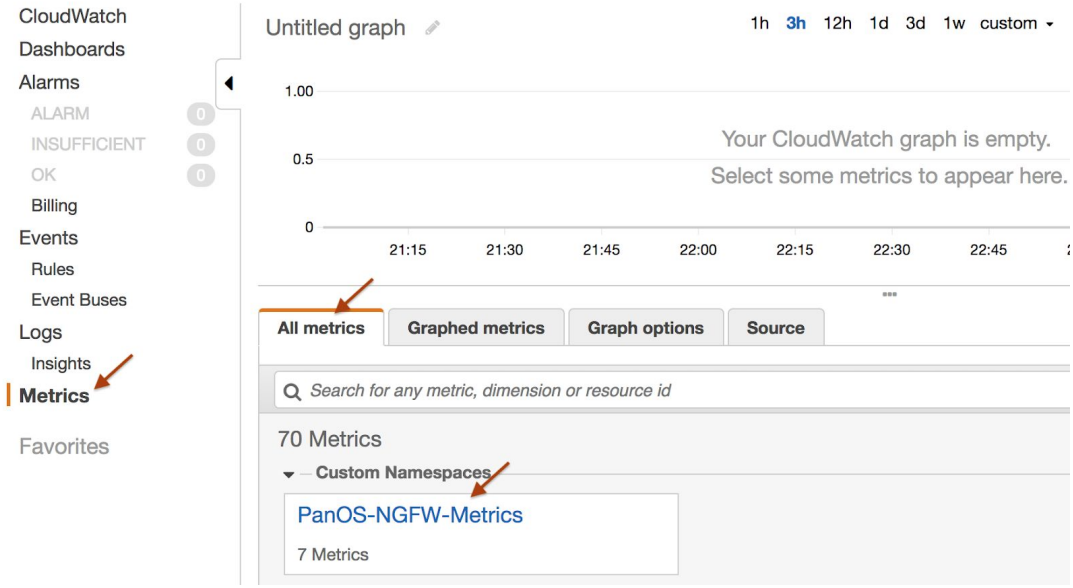


Step 3. From the top right, click Commit to save the changes. Disregard any commit warnings. When the commit is complete, click Close.

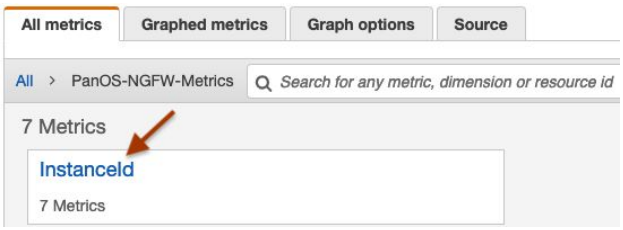
Task 2 - Verify That You Can See the Metrics on CloudWatch

In this task, you will select the specific metrics published by the firewall to AWS CloudWatch.

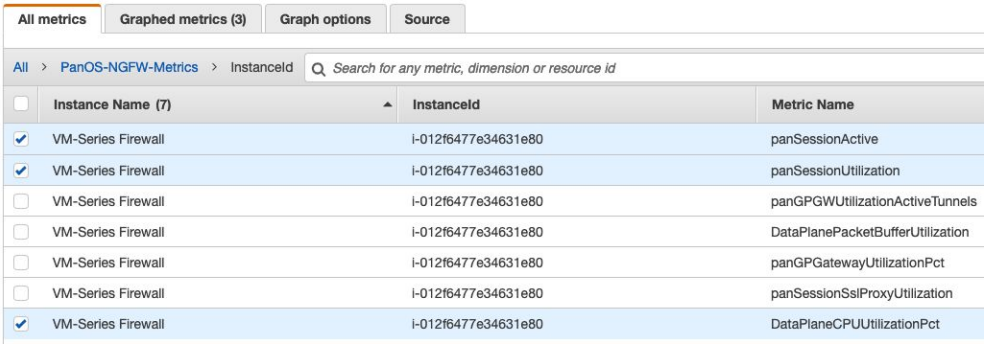
Step 1. On the AWS console, go to ***Services > CloudWatch > Metrics***, and then select the PanOS-NGFW-Metrics custom namespace or any other name entered in Step 2 of Task 1.



Step 2. Click on **InstanceId**.

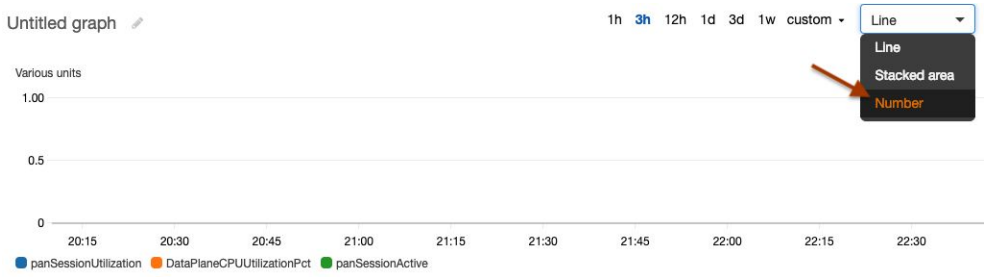


Step 3. You should see 7 metrics published by PAN-OS. These metrics allow you to access the firewall performance and usage patterns. Select the metrics highlighted in the screenshot below.



Instance Name (7)	InstanceId	Metric Name
VM-Series Firewall	i-012f6477e34631e80	panSessionActive
VM-Series Firewall	i-012f6477e34631e80	panSessionUtilization
VM-Series Firewall	i-012f6477e34631e80	panGPGWUtilizationActiveTunnels
VM-Series Firewall	i-012f6477e34631e80	DataPlanePacketBufferUtilization
VM-Series Firewall	i-012f6477e34631e80	panGPGatewayUtilizationPct
VM-Series Firewall	i-012f6477e34631e80	panSessionSslProxyUtilization
VM-Series Firewall	i-012f6477e34631e80	DataPlaneCPUUtilizationPct

Step 4. The metrics you selected in Step 3 will be displayed in the graph. Change the graph display to Number. You might see all zeros if the firewall doesn't have any active sessions and CPU utilization is very minimal.



Step 5. Open the AWS console in a new tab by right-clicking on ***Services***, and then go to ***CloudFormation > Output***. Click on the WebServerURL and WordpressURL to create some sessions on the firewall. Go back to the CloudWatch Metrics page and refresh the screen. You should see that the active session number has updated.

You can use these metrics to configure an AWS alarm. For example, when a firewall is securing a workload in AWS, you can configure an alarm that, when firewall session utilization is at a particular threshold, deploys or terminates an instance of the VM-Series firewall.

Congratulations! You have successfully completed this hands-on workshop.