



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

<u>How to Use This Guide</u>	4
<u>Activity 0 - Workshop Login</u>	5
<u>Activity 1 - Review VPC and Resource Configurations</u>	7
<u>Activity 2 - Access and Review VM-Series Firewall Servers</u>	13
<u>Activity 3 - Protect Web Server from Brute Force Attacks</u>	19
<u>Activity 4 - Enable Outbound Security</u>	23
<u>Activity 5 - Leverage a Threat Intelligence Cloud with the VM-Series</u>	27
<u>Activity 6 - Use Dynamic Address Groups to Protect Dynamic EC2 Instances</u>	33
<u>Activity 7 - Enable CloudWatch Integration to Publish PAN-OS Metrics</u>	42

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”.

Who are you?

Terms & Conditions:

1. By using the Event Engine for the relevant event, you agree to the Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivative works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of the Event Engine will comply with these terms and all applicable laws, and your access to Event Engine will immediately and automatically terminate if you do not comply with any of these terms or conditions.

<INSERT TEAM HASH HERE>

This is the 12 digit hash that was given to you or your team.

✓ Accept Terms & Login



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

The screenshot shows the "Team Dashboard" interface. At the top, there's a navigation bar with "Dashboard" selected. Below it is the main "Team Dashboard" section with a title "Event". In the "Event" section, there are two buttons: "AWS Console" (highlighted with a red box) and "SSH Key". Below these buttons, there's a box containing event details: "Event: PANW-SecurityDevDays" and "Team Name: (Team Name Not Set Yet)". Further down, it lists "Event ID" and "Team ID".

Task 2 - Log in to AWS Console

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

AWS Console Login

Remember to only use "us-east-1" as your region, unless otherwise directed by the event operator.

Login Link

Open AWS Console

Credentials / CLI Snippets

Mac / Linux Windows

Mac or Linux

```
export AWS_DEFAULT_REGION=us-east-1
export AWS_ACCESS_KEY_ID=AS1 1ZRRKf E7E5
export AWS_SECRET_ACCESS_KEY=TTd 1sjjsr3QXd3E cc41 lJOm
export AWS_SESSION_TOKEN=FwoG EP/// //wE t3ANzr !uNqZDik Lhh0kg ue
```

How do I use the AWS CLI?

Checkout the AWS CLI documentation here: <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html>

OK



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:

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, and NAT Gateways. The main area has tabs for 'Launch VPC Wizard' and 'Launch EC2 Instances'. A note says 'Your Instances will launch in the US West (Oregon) region.' Below this is a 'Resources by Region' section with tables for VPCs, Subnets, Route Tables, and Internet Gateways. To the right is a 'Service Health' section showing 'Amazon EC2 - US West (Oregon)' with a status of 'Service is operating normally'. There's also an 'Account Attributes' section and an 'Additional Information' section with links to documentation and forums.

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*.

The screenshot shows the AWS VPC Dashboard. It features a 'Create VPC' button and an 'Actions' dropdown. A search bar at the top allows filtering by tags and attributes or searching by keyword. Below is a table listing two VPCs: 'PAN-Cloud...' (VPC ID: `vpc-077b8ff788714b68e`, State: available) and 'DEFAULT-V...' (VPC ID: `vpc-4f46c236`, State: available).



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.

VPC Dashboard

Create subnet Actions ▾

Filter by VPC: Select a VPC

Filter by tags and attributes or search by keyword

VPC ID	Name tag	Owner
vpc-4f46c236	DEFAULT-VPC	121555577215
vpc-077b8ff788714b68e	PAN-CloudSecurity-Lab	121555577215

VPC Dashboard

Create subnet Actions ▾

Filter by VPC: Select a VPC

Filter by tags and attributes or search by keyword

Virtual Private Cloud

Your VPCs

Subnets

Name	Subnet ID
Web-Subnet	subnet-02ba72fe3531c320a
Public-Subnet	subnet-02512d8f8dd910f39
DB-Subnet	subnet-01d0979e0f1f8e1fa

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

VPC Dashboard

Create subnet Actions ▾

Filter by VPC: Select a VPC

Filter by tags and attributes or search by keyword

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Name	Subnet ID	State	VPC	IPv4 CIDR
Web-Subnet	subnet-02ba72fe3531c320a	available	vpc-077b8ff788714b68e ...	10.0.1.0/24
Public-Subnet	subnet-02512d8f8dd910f39	available	vpc-077b8ff788714b68e ...	10.0.0.0/24
DB-Subnet	subnet-01d0979e0f1f8e1fa	available	vpc-077b8ff788714b68e ...	10.0.2.0/24

Subnet: subnet-02512d8f8dd910f39

Description Flow Logs Route Table Network ACL Tags Sharing

Subnet ID: subnet-02512d8f8dd910f39
VPC: vpc-077b8ff788714b68e | PAN-CloudSecurity-Lab

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

Name	Subnet ID	State	VPC	IPv4 CIDR
Public-Subnet	subnet-0f67f15c2700dab65	available	vpc-0de247574b1fdf0d0 ...	10.0.0.0/24
Web-Subnet	subnet-064e3b4b90038d7b5	available	vpc-0de247574b1fdf0d0 ...	10.0.1.0/24
DB-Subnet	subnet-0f352672da797d379	available	vpc-0de247574b1fdf0d0 ...	10.0.2.0/24
	subnet-11d0704b	available	vpc-69ba3e10 DEFAULT...	172.31.0.0/20

Subnet: subnet-0f67f15c2700dab65

Description Flow Logs Route Table **Network ACL** Tags Sharing

Edit network ACL association

Network ACL: acl-090eaf8fb0d21c91

Inbound rules

Rule #	Type	Protocol	Port Range / ICMP Type	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound rules

Rule #	Type	Protocol	Port Range / ICMP Type	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW

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.

Name	Subnet ID	State	VPC
Public-Subnet	subnet-0f67f15c2700dab65	available	vpc-0de
Web-Subnet	subnet-064e3b4b90038d7b5	available	vpc-0de
DB-Subnet	subnet-0f352672da797d379	available	vpc-0de
	subnet-11d0704b	available	vpc-69b

Subnet: subnet-0f67f15c2700dab65

Description Flow Logs **Route Table** Network ACL Tags

Edit route table association

Route Table: rtb-00730c5a9776034a8 | RouteTable-2

Destination		Target
10.0.0.0/16		local
0.0.0.0/0		igw-00e4870659c083c03



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.

Name	Subnet ID	State	VPC
Public-Subnet	subnet-0f6715c2700dab65	available	vpc-0c
Web-Subnet	subnet-064e3b4b90038d7b5	available	vpc-0c
DB-Subnet	subnet-0f352672da797d379	available	vpc-0c

Name	Subnet ID	State	VPC
Public-Subnet	subnet-0f6715c2700dab65	available	vpc-0c
Web-Subnet	subnet-064e3b4b90038d7b5	available	vpc-0c
DB-Subnet	subnet-0f352672da797d379	available	vpc-0c

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.)

Elastic IP	Allocation ID	Instance	Private IP address	Scope
52.41.221.122	eipalloc-4bef9a76	i-0e04e505380a3ecf0	10.0.0.100	vpc
54.68.195.231	eipalloc-1def9a20	i-0e04e505380a3ecf0	10.0.0.99	vpc

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.

Running Instances	Elastic IPs
3	2

Dedicated Hosts	Snapshots
0	0

Volumes	Load Balancers
3	0

Key Pairs	Security Groups
1	3

Placement Groups
0



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.

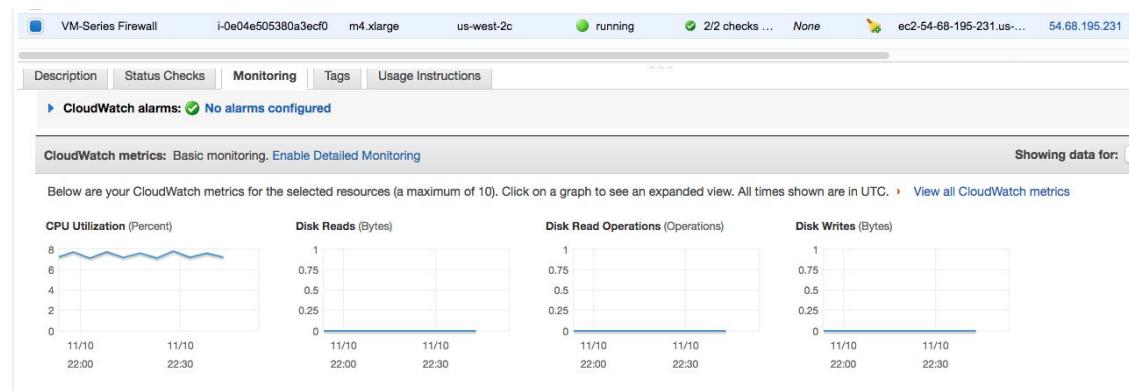
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Web Server	i-00c57832184d65aed	t1.micro	us-west-2c	running	2/2 checks ...	None		-
DB Server	i-0dbc560ed35499106	t1.micro	us-west-2c	running	2/2 checks ...	None		-
VM-Series Firewall	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*	Private DNS	ip-10-0-99.us-west-2.compute.internal
	52.41.221.122*		
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.



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?

Name	Network Interface	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID
FW MGMT	eni-51253a33	subnet-dfc4c084	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	Primary network interface	i-0dbc560ed35499106
FW Eth1/3	eni-53243b51	subnet-b7c5c1ec	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	AWS FW1 MGMT	i-0e04e505380a3ecf0
FW Eth1/2	eni-83263981	subnet-dfc4c084	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	AWS FW1 E1/3	i-0e04e505380a3ecf0
FW Eth1/1	eni-66283784	subnet-accc04f7	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	AWS FW1 E1/2	i-0e04e505380a3ecf0
	eni-9c253a9e	subnet-b7c5c1ec	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	AWS FW1 E1/1	i-0e04e505380a3ecf0
	eni-f9223dfb	subnet-accc04f7	vpc-dfdeeb9	us-west-2c	VUTD-CloudSecurit...	Primary network interface	i-0057832184d65a6d

Network Interface: eni-53243b51

Details Flow Logs Tags

Network interface ID: eni-53243b51
VPC ID: vpc-dfdeeb9
MAC address: 0ac1:88:e6:58:1e
Security groups: VUTD-CloudSecurity-sgWideOpen-2D3ALWJ758AY, view inbound rules

Subnet ID: subnet-b7c5c1ec
Availability Zone: us-west-2c
Description: AWS FW1 MGMT
Owner ID: 456863802774

Detailed interface ID: i-0e04e505380a3ecf0

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.)

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Pu
DB Server	i-0b33a8f59dc346d05	t1.micro	us-west-2c	running	2/2 checks ...	None	-	-
VM-Series Firewall	i-0b47617e74d4469	m4.xlarge	us-west-2c	running	2/2 checks ...	None	ec2-54-71-106-188.us...	54.71.1

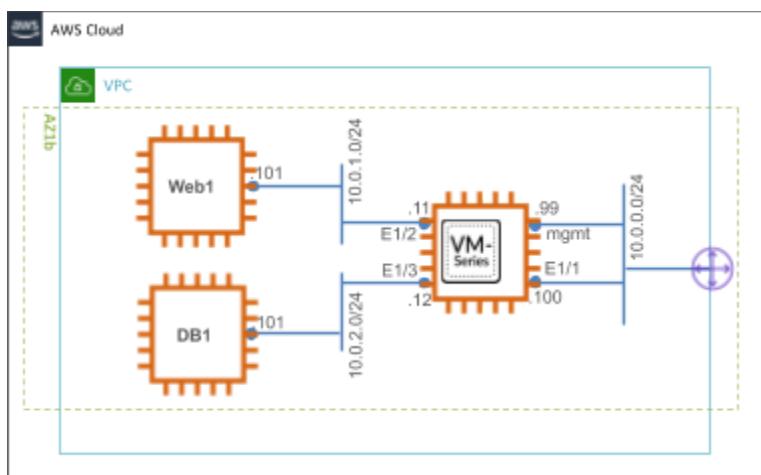
Instance: i-0b33a8f59dc346d05 (DB Server) Private IP: 10.0.2.101

Description Status Checks Monitoring Tags

Add/Edit Tags

Key	Value
Confidentiality	High
Group	VUTD
Name	DB Server

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 its 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”.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like Services, Resource Groups, and a New EC2 Experience toggle. The main area shows a table of instances. One row is selected for a VM-Series Firewall, with details like Instance ID (i-0a9f9ea92c570a005), Instance Type (m5.xlarge), and State (running). Below the table, a detailed view for the selected instance is shown. In the 'Description' tab, under the 'Public DNS (IPv4)' column, there's a tooltip with the value 'ec2-34-196-21-1.amazonaws.com' and a 'Copy to clipboard' button. This tooltip is circled in red. Other fields in the tooltip include 'IPv4 Public IP' (34.196.212.108) and 'Elastic IPs' (34.196.212.108*, 107.23.198.197*).



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:

General Information

Device Name	jd8-fw
MGT IP Address	10.0.0.99 (DHCP)
MGT Network	255.255.255.0
MGT Default Gateway	10.0.0.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::65:46ff:fed9:2210/64
MGT IPv6 Default Gateway	02:65:46:99:22:10
MGMT MAC Address	PA-VMM
Model	Serial # 45A604190BE4372
Serial #	45A604190BE4372
CPU ID	AVWMP-05f1cf645474a7aa:806j2ofDcy5osqjxq9pgodsg:us-west-2
UUID	E2C130EB-583C-F906-D4B7-C2412528F81
VM License	VM-300
VM Mode	Amazon AWS
Software Version	8.0.3
GlobalProtect Agent	0.0.0
Application Version	748-4315 (11/06/17)
Threat Version	748-4315 (11/06/17)
URL Filtering Version	0000.00.00.000
GlobalProtect Clients VPN Version	0
Time	Thu Dec 14 11:19:14 2017
Uptime	0 days, 0:15:32

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	199.167.54.229	Web	12/14 11:18:33	00:00:00s

Config Logs

No data available.

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 199.167.54.229 using https	12/14 11:18:33
authenticated for user 'admin'. From: 199.167.54.229.	12/14 11:18:33
CLoud ELECTION: v02000.unlocked.paloaltonetworks.com IP: 54.215.133.69 was elected, measured alive test 164992.	12/14 11:18:35
Bootsrap successfully completed. sw-version: 8.0.3; app-version: 748-4315; threat-version: 748-4315 av-version: 0; wildfire-version: 248-4315; license remote: GlobalProtect Gateway, PAN DB URL, Filtering, PA-VM, GlobalProtect, Portal, Threat Prevention, Wildfire License.	12/14 11:19:02
Autocommit job succeeded	12/14 11:09:52
DHCP client assigned IP 10.0.0.100 on interface ethernet1/1 for lease time of 0 days 15:00m:00s from server: 10.0.0.1. Subnet mask: 255.255.255.0 Gateway: 10.0.0.1 DNS1:10.0.0.2 DNS2:10.0.0.3 Cname: 10.0.0.1	12/14 11:09:48
DHCP client assigned IP 10.0.1.11 on interface ethernet1/2 for lease time of 0 days 15:00m:00s from server: 10.0.1.1. Subnet mask: 255.255.255.0 Gateway: 10.0.1.1 DNS1:10.0.0.2 DNS2:10.0.0.3 Cname: 10.0.0.1	12/14 11:09:48
DHCP client assigned IP 10.0.2.11 on interface ethernet1/3 for lease time of 0 days 15:00m:00s from server: 10.0.2.1. Subnet mask: 255.255.255.0 Gateway: 10.0.2.1 DNS1:10.0.0.2 DNS2:10.0.0.3 Cname: 10.0.0.1	12/14 11:09:48

ACC Risk Factor (Last 60 minutes)

4.0

System Resources

Management CPU	2%
Data Plane CPU	0%
Session Count	0 / 819200



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.

The screenshot shows the Palo Alto Networks Firewall interface. The left sidebar contains navigation links for various network components like Interfaces, Zones, Virtual Routers, and Policies. The main pane is titled 'Network' and displays a table of interfaces. The table columns include Interface, Interface Type, Management Profile, Link State, IP Address, Virtual Router, Tag, VLAN / Virtual-Wire, and Security Zone. The three interfaces listed are ethernet1/1, ethernet1/2, and ethernet1/3, all with 'Dynamic-DHCP Client' management profiles and 'external' security zones. Below the table, a 'Task Manager - All Tasks' dialog is open, showing one item: 'Auto Commit' with a status of 'Completed' and a start time of '05/14/19 13:11:10'. At the bottom of the screen, the URL 'https://54.190.252.188/#' is visible.

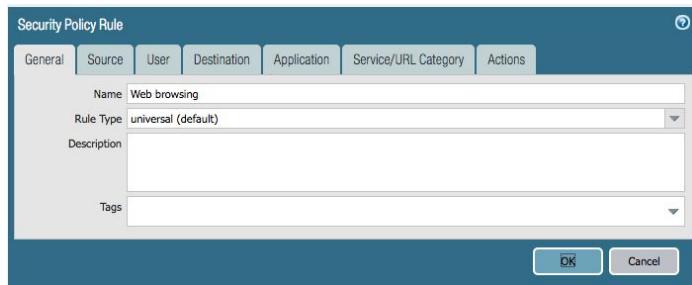
Step 4. Click on the **Policies** tab at the top of the page, and then **Security** in the left pane, to review the initial security policy:

ID	Name	Tags	Type	Source				Destination				Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address	Application	Service			
1	SSH inbound	none	universal	[!] external	any	any	any	[!] db	any	ssh	application-d...	Allow	none	[!]
2	SSH 221-222 inbound	none	universal	[!] external	any	any	any	[!] db	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	[!] external	any	any	any	[!] web	any	web-browsing	application-d...	Allow	none	[!]
5	Allow all outbound	none	universal	[!] db	any	any	any	[!] external	any	application-d...	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	(intrazone)	any	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
	Name	Tags	Type	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	green	intrazone	any	any	any	any	(intrazone)	any			Allow	none
9	interzone-default	green	interzone	any	any	any	any	any	any			Deny	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.

The screenshot shows the AWS EC2 Instances page. A search bar at the top contains 'search : VM-Series Firewall'. Below it, a table lists one instance named 'VM-Series Firewall' with the following details:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm
VM-Series Firewall	i-0a9f9ea92c570a005	m5.xlarge	us-east-1a	running	2/2 checks...	None

Below the table, a specific instance row is expanded:

Instance: i-0a9f9ea92c570a005 (VM-Series Firewall)		Elastic IP: 34.196.212.108
Description	Status Checks	Monitoring
Instance ID: i-0a9f9ea92c570a005	Public DNS (IPv4): ec2-34-196-212-108.compute-1.amazonaws.com	
Instance state: running	IPv4 Public IP: 34.196.212.108	
Instance type: m5.xlarge	IPv6 IPs: -	
Finding: You may not have permission to access AWS Compute Optimizer.	Elastic IPs: 34.196.212.108* 107.23.198.197*	
Private DNS: ip-10-0-99.ec2.internal	Availability zone: us-east-1a	
Private IPs: 10.0.0.100, 10.0.2.11, 10.0.0.99, 10.0.1.11	Security groups: mod-6e66d106029e44e5- sgWideOpen-	

The screenshot shows a web browser window with the URL bar containing '<INSERT IP ADDRESS HERE>'. The main content is the 'Apache2 Ubuntu Default Page' with the following text:

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

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:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
02/24 14:47:50	start	external	web	199.167.55.50		10.0.0.100	80	web-browsing	allow	Web browsing	n/a	814
02/24 14:47:49	end	external	web	199.167.55.50		10.0.0.100	80	web-browsing	allow	Web browsing	tcp-fin	5.1k

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:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
02/12 05:11:27	end	external	web	52.52.133.159		10.0.0.100	80	web-browsing

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.

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Action	Rule	Sess
11/17 16:14:05	drop	external	external	220.156.248.128	10.0.0.100	23	not-applicable	deny	Log default deny
11/17 16:13:37	drop	external	external	200.222.130.33	10.0.0.100	23	not-applicable	deny	Log default deny



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:

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under 'INSTANCES', 'Instances' is selected. The main pane displays a single instance named 'VM-Series Firewall' with the ID 'i-0a9f9fea92c570a005'. The instance is listed as 'running' in the 'Instance State' column. The 'Elastic IP' column shows '34.196.212.108' and '107.23.198.197*'. The '107.23.198.197*' address is highlighted with a red box. Other columns include 'Description', 'Status Checks', 'Monitoring', and 'Tags'.

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:

The screenshot shows a network monitoring interface with a search bar containing '(app eq mysql) or (app eq web-browsing)'. Below the search bar is a table with the following data:

	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.

The screenshot shows the Palo Alto Networks VM-Series UI interface. The top navigation bar includes Dashboard, ACC, Monitor, Policies, Objects (selected), Network, and Device. The left sidebar contains various object categories like Addresses, Applications, and Security Profiles. Under Security Profiles, the 'Vulnerability Protection' option is selected. The main pane displays a table of profiles. The 'strict' profile is highlighted with a yellow background and has a checked checkbox next to it. A red arrow points to this checkbox. At the bottom of the table, there is a row for 'Test Drive' with 'Rules: 6' and 'Exceptions: 1'. Below the table, there is a toolbar with buttons for Add, Delete, Clone (highlighted with a red arrow), and PDF/CSV.

Name	Location	Count	Rule Name	Threat Name	Host Type
strict	Predefined	Rules: 10	simple-client-critical simple-client-high simple-client-medium simple-client-informational simple-client-low simple-server-critical simple-server-high more...	any any any any any any any	client client client client client server server
default	Predefined	Rules: 6	simple-client-critical simple-client-high simple-client-medium simple-server-critical simple-server-high simple-server-medium	any any any any any any	client client client server server server
Test Drive		Rules: 6	simple-client-critical	any	client
		Exceptions: 1	simple-client-high simple-client-medium simple-server-critical simple-server-high simple-server-medium	any any any any any	client client server server server

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.

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	35...	HP Data Protector OmniNet Opcode Buffer Overflow Vulnerability		simple-server-high	CVE-2011-1865	server	overflow	high	default (alert)	disable
<input type="checkbox"/>	39...	HP Data Protector Client EXEC_CMD Command Execution Vulnerability		simple-server-high	CVE-2011-0923	server	code-execution	high	default (alert)	disable
<input type="checkbox"/>	36...	HP Data Protector Opcode 11 and 28 Command Execution Vulnerability		simple-server-high	CVE-2014-2623,CVE-2013-2347	server	code-execution	high	default (alert)	disable
<input type="checkbox"/>	36...	HP Data Protector CRS Service Buffer Overflow Vulnerability		simple-server-high	CVE-2013-6195	server	overflow	high	default (alert)	disable
<input type="checkbox"/>	34...	HP OpenView Storage Data Protector EXEC_CMD		simple-server-high	CVE-2011-1866,CVE-	server	overflow	high	default (alert)	disable

Show all signatures | Page 1 of 314 | ►► | Displaying 1 - 30 / 9411 threats

OK Cancel

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

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	36...	WordPress FormCraft Plugin SQL Injection Vulnerability		simple-server-medium	CVE-2013-7187	server	sql-injection	medium	default (alert)	disable
<input type="checkbox"/>	35...	WordPress Plugin Quick Post Widget1.9.1 Cross Site Scripting Vulnerability		simple-server-high	CVE-2012-4226	server	code-execution	high	default (alert)	disable
<input type="checkbox"/>	36...	WordPress Pingback XMLRPC Function Denial of Service Vulnerability		simple-server-low		server	dos	low	default (alert)	disable
<input type="checkbox"/>	35...	WordPress Caching Plugins Remote Code Execution Vulnerability		simple-server-high	CVE-2013-2010	server	code-execution	high	default (alert)	disable
<input type="checkbox"/>	30...	WordPress Cookie Data PHP Code Injection		simple-server-high	CVE-2005-2612	server	code-execution	high	default (reset-both)	disable

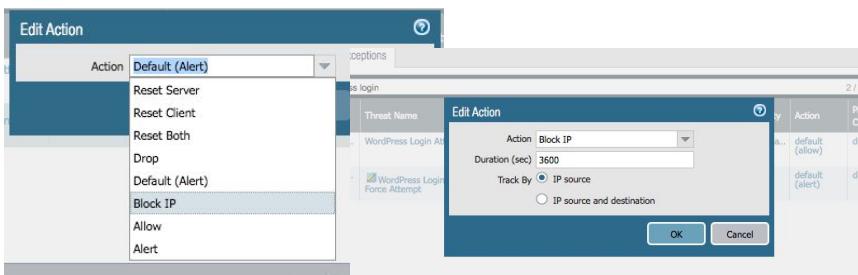
Show all signatures | Page 1 of 2 | ►► | Displaying 1 - 30 / 49 threats

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.

Enable	ID	Threat Name	IP Address Exemptions	Rule	CVE	Host	Category	Severity	Action	Packet Capture
<input type="checkbox"/>	37...	WordPress Login Attempt		simple-server-information...		server	code-execution	informational	default (allow)	disable
<input type="checkbox"/>	40...	WordPress Login Brute Force Attempt		simple-server-critical		server	brute-force	critical	default (alert)	disable

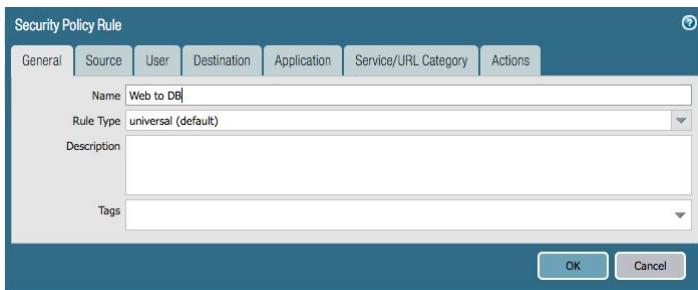


Step 6. This object has configuration options. Click on the *default (alert)* option in the *Action* column and change the default behavior from *Alert* to *Block IP*. Set the duration to 3600 seconds (one hour), click *OK* on the *Edit Action* window, and click *OK* on the *Vulnerability Protection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

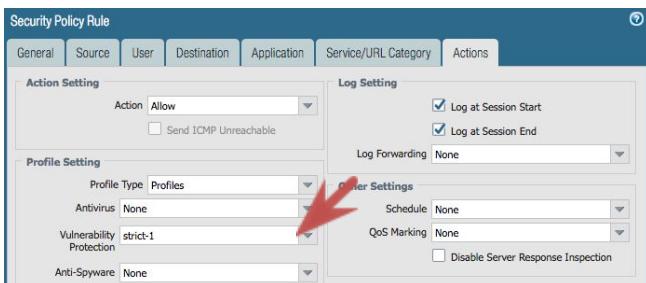


Task 2 - Apply the WordPress Protection in Policy

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*.

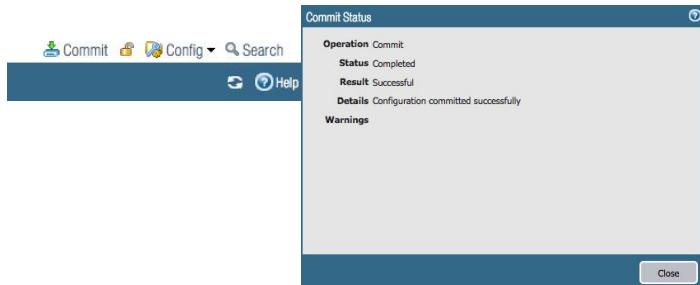


Step 3. Repeat the same steps above to add the **strict-1** vulnerability profile to the **Allow all outbound** rule. Click on the rule name, click on the **Actions** tab, change the **Profile Type** to **Profiles**, and change the **Vulnerability Protection** setting to **strict-1**.

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

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.

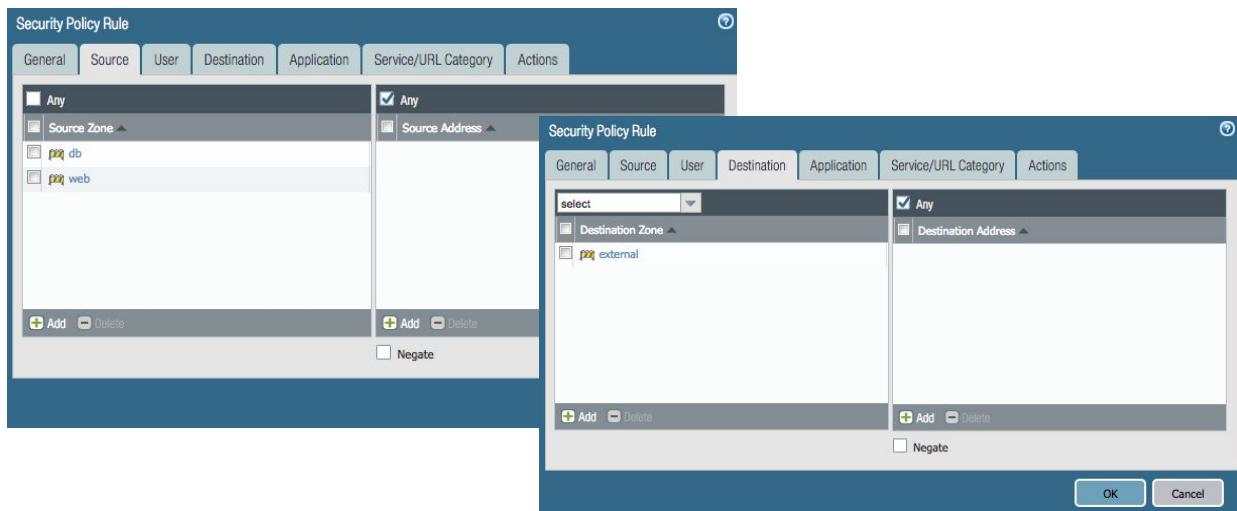


Step 2. Name the application group: **Allowed-Outbound-Apps**. Add **ssh**, **ntp**, **dns** and **web-browsing** to this application group. Click **OK** to save the application group.



Task 2 - Limiting Outbound Traffic and Blocking File Exfiltration

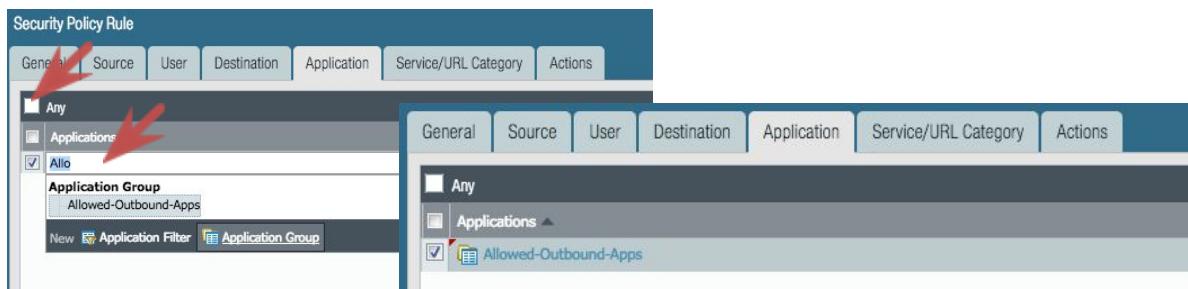
Step 1. Click on the **Policies** tab. Click on the **Security** option on the left panel if not already highlighted. Click on the **Allow all** rule and review the **Source** and **Destination** tabs.



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:

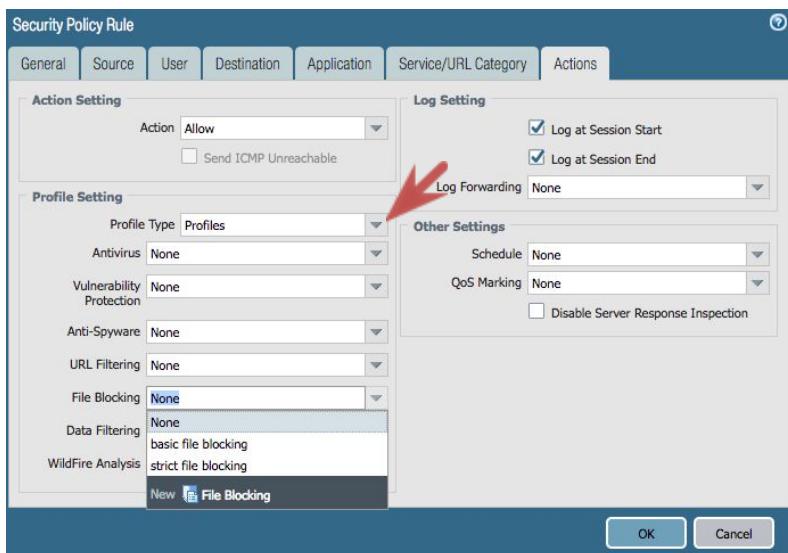




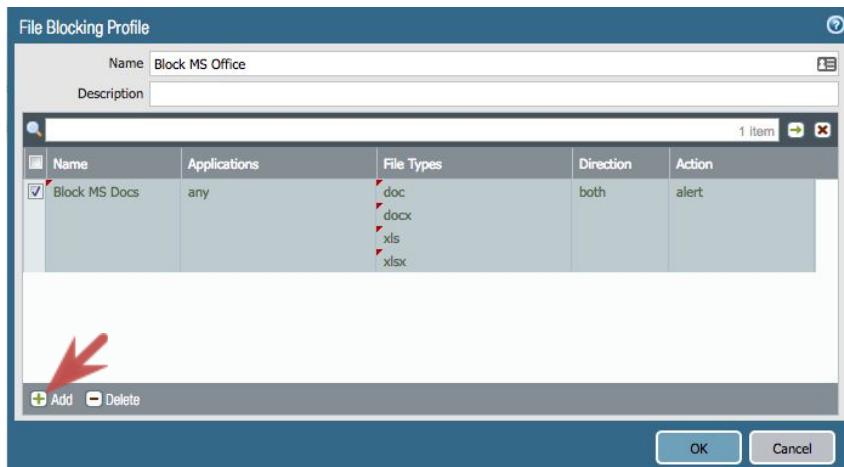
Step 4. Click on **Service/URL Category** tab. Note that **application-default** is selected and that will only allow applications to run on its default, but not others. Note also that you don't need to remember what the port numbers those applications use—the firewall will choose the default port number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

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Action Setting

Action: Allow Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: Block MS Office

Data Filtering: None

WildFire Analysis: None

Log Setting

Log at Session Start
 Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None Disable Server Response Inspection

OK Cancel

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.

5	Limited Outbound	none	universal	db web	any
---	------------------	------	-----------	-----------	-----

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

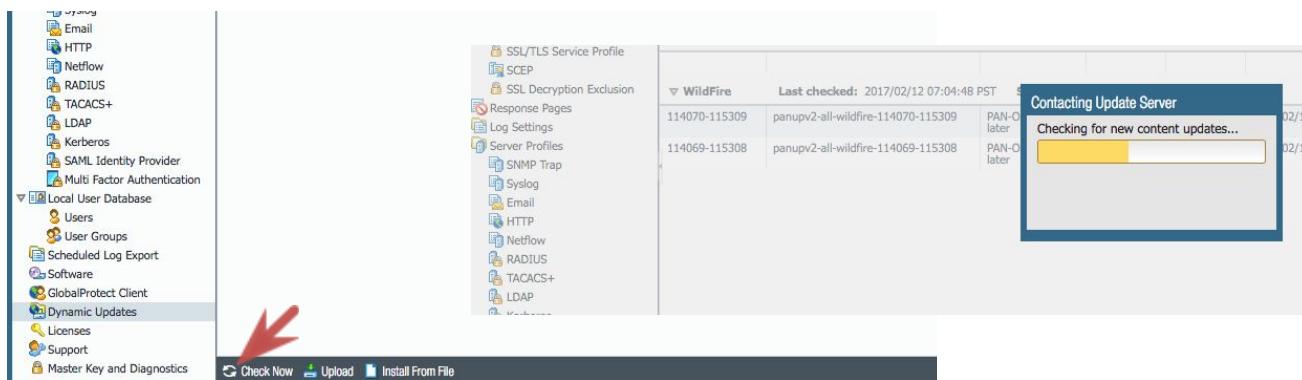
In this activity, you will:

- 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.

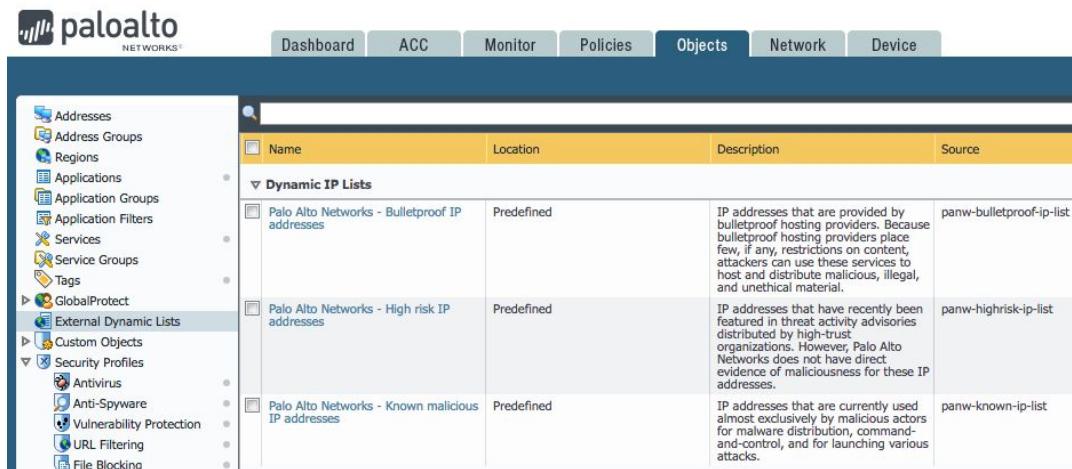
Note: You might have to install Application and Threat content before installing the Antivirus content, if it's not installed during the firewall bootstrap process.

The screenshot shows the Device tab with the Antivirus section selected. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device (which is active). There are also 'Commit' and 'Logout' buttons. Below the navigation is a search bar with a magnifying glass icon. The main area has a table with columns: Version, File Name, Features, Type, Size, Release Date, Downloaded, Currently Installed, and Action. A header row indicates the last check was on '2017/02/12 07:41:16 PST' and the schedule is 'None'. The table shows one entry: '2152-2639 panup-all-antivirus-2152-2639 Full 67 MB 2017/02/11 13:45:17 PST'. A red arrow points to the 'Download' button in the Action column for this entry.

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.

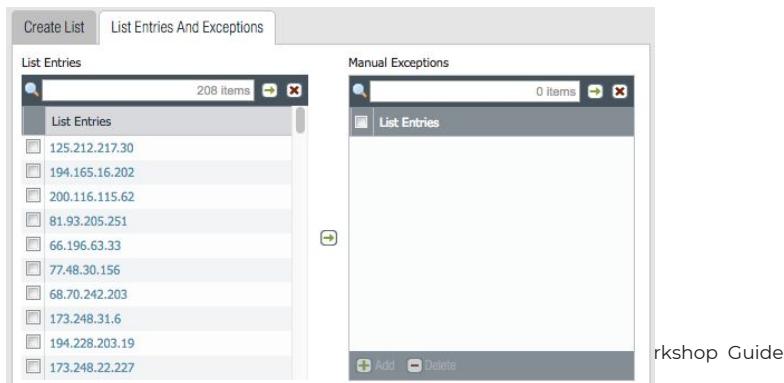


Name	Location	Description	Source
Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers often use these services to host and distribute malicious, illegal, and unethical material.	panw-bulletproof-ip-list
Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by third-party organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	panw-highrisk-ip-list
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used and exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	panw-known-ip-list

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.

The screenshot shows the 'External Dynamic Lists' configuration window. On the left, there's a form with fields for 'Name' (empty), 'Create List' tab selected, 'Type' set to 'IP List', 'Description' (empty), 'Source' set to 'http://', 'Server Authentication' section with 'Certificate Profile' set to 'None' and 'Repeat' set to 'Hourly', and a 'Test Source URL' button. On the right, a dropdown menu titled 'Type' is open, showing options: 'IP List' (selected), 'Predefined IP List', 'IP List', 'Domain List', and 'URL List'. At the bottom right are 'OK' and 'Cancel' buttons.

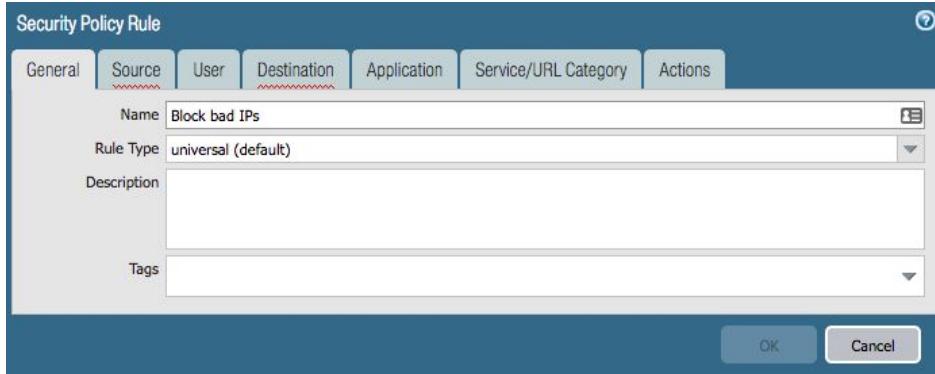
Step 9. We will not create an External Dynamic List here, but we will see how you can apply the predefined list to a policy in the next task. Click **Cancel** to close the window.

Task 2 - Create Policy Using the External Dynamic List

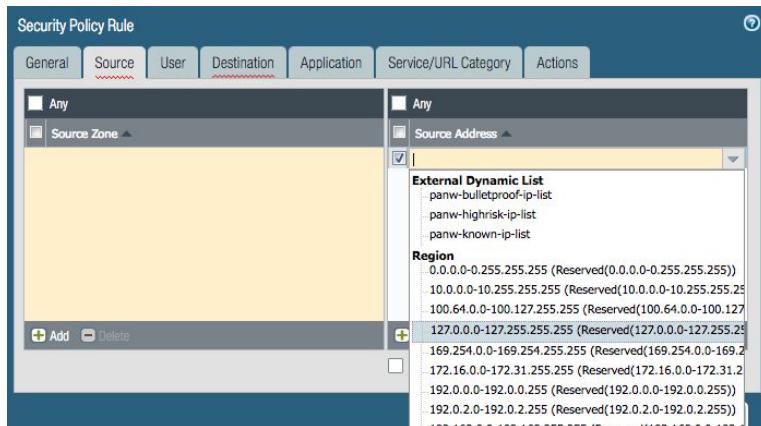
Step 1. Next, you will create a security policy to block any traffic to or from these known bad IPs. First, create a rule to block traffic from these IPs. Go to the **Policies** tab and select **Security** from the left pane if not already selected. Click **Add** at the bottom of the page.

The screenshot shows the 'Tag Browser' interface. It has a table with one item: 'none (5)' under 'Tag(#)' and '1-5' under 'Rule'. Below the table are filter options: 'Filter by first tag in rule' (checked), 'Rule Order' (radio button selected), and 'Alphabetical' (radio button). At the bottom are buttons for '+ Add', 'Delete', 'Clone', 'Override', 'Revert', 'Enable', 'Disable', 'Move', and 'Highlight Unused Rules'. A status bar at the bottom says 'Object : Addresses'.

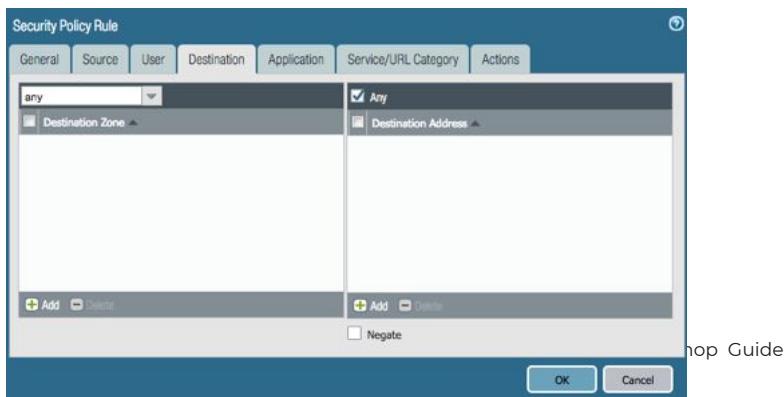
Step 2. Give the new rule a name, such as **Block bad IPs**:



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**.

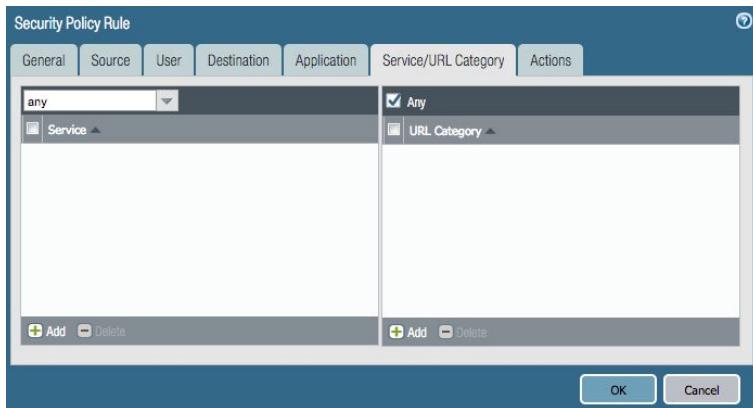


Step 4. Click on the **Destination** tab and set the zone to **Any** (keep the address at **Any**).

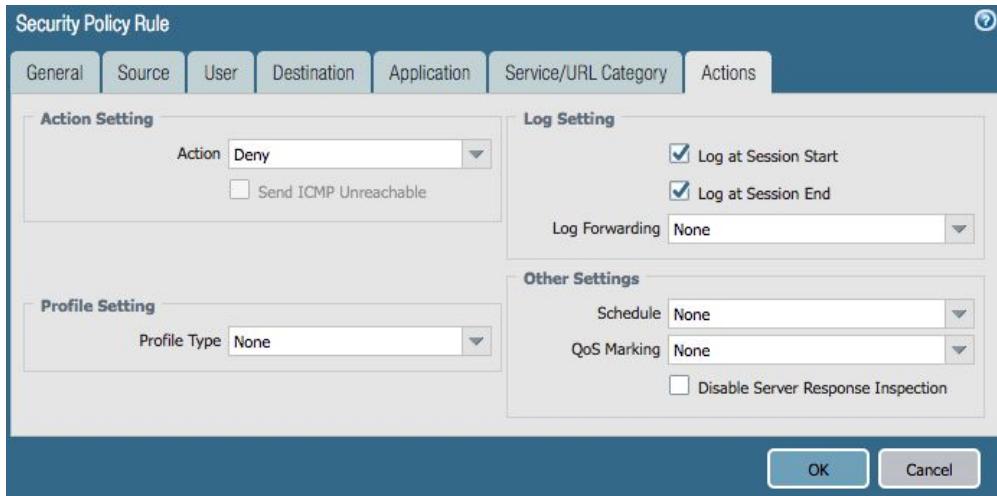




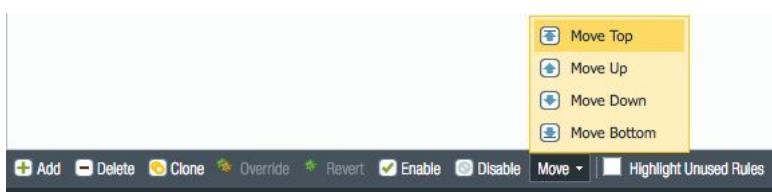
Step 5. Click on the *Service/URL Category* tab and change the service type to *Any*.



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*.



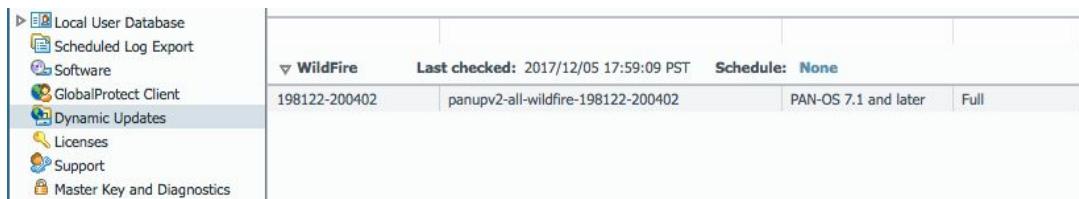
Step 8. Commit your changes.

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.

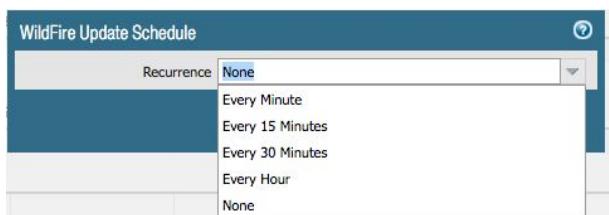
Task 3 - Configure Auto Dynamic Updates

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”.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a sidebar with options like 'Dashboard', 'Access management', 'Groups', and 'Users'. The 'Users' option is currently selected. At the top center, there are two buttons: 'Add user' (highlighted with a red box) and 'Delete user'. Below these buttons is a search bar labeled 'Find users by username or access key'. Underneath the search bar is a table header with columns: 'User name' (with a dropdown arrow), 'Groups', 'Access key age', 'Password age', and 'Last activity'. A message at the bottom of the table area says 'There are no IAM users. Learn more'.

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

The screenshot shows the 'Set user details' step of the 'Add user' wizard. At the top, it says 'Add user' and shows a progress bar with step 1 completed (blue circle) and steps 2 through 5 as empty circles. The main form has a section titled 'Set user details' with a note: 'You can add multiple users at once with the same access type and permissions. Learn more'. Below this is a 'User name*' input field containing 'awsstudent', with a red arrow pointing to it. There's also a link '+ Add another user'. The next section is 'Select AWS access type' with a note: 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more'. It contains two options: 'Access type*' with a checked checkbox for 'Programmatic access' (described as enabling access keys and secret access keys for the AWS API, CLI, SDK, and other tools) and an unchecked checkbox for 'AWS Management Console access' (described as enabling a password for the AWS Management Console). A red arrow points to the 'Programmatic access' checkbox.



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”.

Add user

1 2 3 4 5

Set permissions

Add user to group Copy permissions from existing user Attach existing policies directly

Create policy

Filter policies ▾ Showing 106 results

	Policy name	Type	Used as
<input type="checkbox"/>	GlobalAcceleratorReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	IAMAccessAnalyzerReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	NeptuneReadOnlyAccess	AWS managed	None
<input checked="" type="checkbox"/>	ReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	ResourceGroupsandTagEditorReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	ServiceQuotasReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	WellArchitectedConsoleReadOnlyAccess	AWS managed	None

Set permissions boundary

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

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
Name	PaloAltoCLIAccess	x
Add new key		

You can add 49 more tags.



Step 5. Review new user details and click on “Create user”.

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	awsstudent
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	ReadOnlyAccess

Tags

The new user will receive the following tag

Key	Value
Name	PaloAltoCLIAccess

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.

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://209468029373.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	awsstudent	AKIATBRKEPG64PDXGGUI	***** Show



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.

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
PAN-CloudSecurity-Lab	vpc-0691af	available	10.0.0.0/16	-
	vpc-2a1b1850	available	172.31.0.0/16	-

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.

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network

Addresses Address Groups Regions Applications Application Groups Application Filters Services

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.

Address Group

Name: [] Description: [] Type: Dynamic Match: [] Tags: []

+ Add Match Criteria

AND OR

0 items

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.

The screenshot shows the Palo Alto Networks VM Information Sources configuration interface. On the left, there is a sidebar with various navigation options like Setup, High Availability, and VM Information Sources. The main area has a table titled "VM Information Source Configuration" showing one item:

Name	Enabled	Source	Type	Status
aws-monitor	<input checked="" type="checkbox"/>	ec2.us-west-2.amazonaws.com	AWS-VPC	●

Below the table is a detailed configuration dialog box for the "aws-monitor" entry:

- Name:** aws-monitor
- Type:** AWS VPC
- Description:** (empty)
- Enabled:**
- Source:** ec2.us-west-1.amazonaws.com
- Access Key ID:** AKIAJPRJ56URBICU6QHA
- Secret Access Key:** *****
- Confirm Secret Access Key:** *****
- Update Interval (sec):** 60
- Timeout (hours):** 2
- VPC ID:** vpc-40210b25
- Enable timeout when source is disconnected:**

At the bottom right of the dialog are "OK" and "Cancel" buttons.

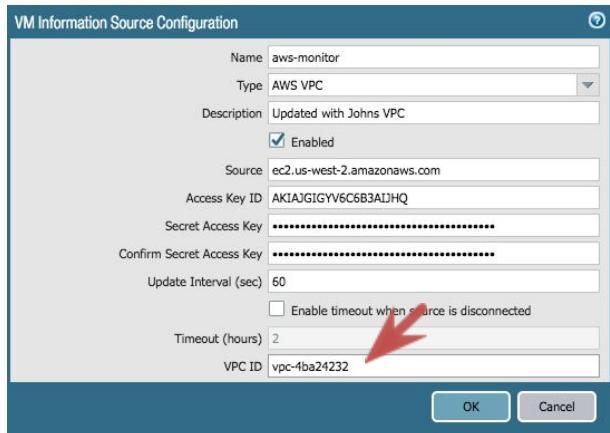
Step 2. The *aws-monitor* is created for you in the default lab configuration. Click the name to open the *VM Information Source Configuration* window.

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.

Name	Enabled	Source	Type	Status
aws-monitor	<input checked="" type="checkbox"/>	ec2.us-west-2.amazonaws.com	AWS-VPC	●

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.

Name	Type	Details
architecture.x86_64	dynamic	
aws-tag.Confidentiality.High	dynamic	
aws-tag.Confidentiality.Low	dynamic	
aws-tag.Group...	dynamic	
aws-tag.Name....	dynamic	
aws-tag.Name....	dynamic	

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.

Name	Type	D...
architecture.x86_64	dynamic	
aws-tag.Confidentiality.High	dynamic	
aws-tag.Confidentiality.Low	dynamic	
aws-tag.Group...	dynamic	
aws-tag.Name....	dynamic	

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).

Name	Type	Details
architecture.x86_64	dynamic	
aws-tag.Confidentiality.High	dynamic	
aws-tag.Confidentiality.Low	dynamic	

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”.

The screenshot shows two windows side-by-side. The left window is a table with columns: Name, Location, Members Count, and Addresses. It has one row for 'AWS-DAG' with 'dynamic' in Location and 'more...' in Addresses. The right window is titled 'Address Groups - AWS-DAG' and shows a table with columns: Address, Type, and Action. It contains one item: '10.0.2.101' (Type: registered-ip) with an 'Unregister Tags' action button.

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.

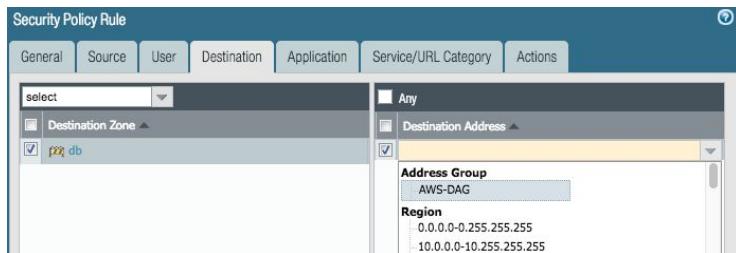
Task 5 - Create Policy with a Dynamic Address Group

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.

The screenshot shows the Palo Alto Networks VM-Series interface. The top navigation bar includes tabs: Dashboard, ACC, Monitor, Policies (selected), Objects, Network, and Device. On the left, a sidebar lists security features: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main content area displays the 'Web to DB' policy details. The table has columns: Name, Tags, Type, Zone, Address, and User. The policy details are: Name: Web to DB, Tags: none, Type: universal, Zone: web, Address: any, User: any. Below the table, there are four other policies listed: Log default deny, intrazone-default, interzone-default, and another unnamed 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

The screenshot shows the 'Profile Setting' dialog box. The 'Profile Type' is set to 'Profiles'. Under 'Protection', 'Antivirus' is 'default', 'Vulnerability Protection' is 'Test Drive', 'Anti-Spyware' is 'default', 'URL Filtering' is 'None', 'File Blocking' is 'strict file blocking', 'Data Filtering' is 'None', and 'WildFire Analysis' is '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

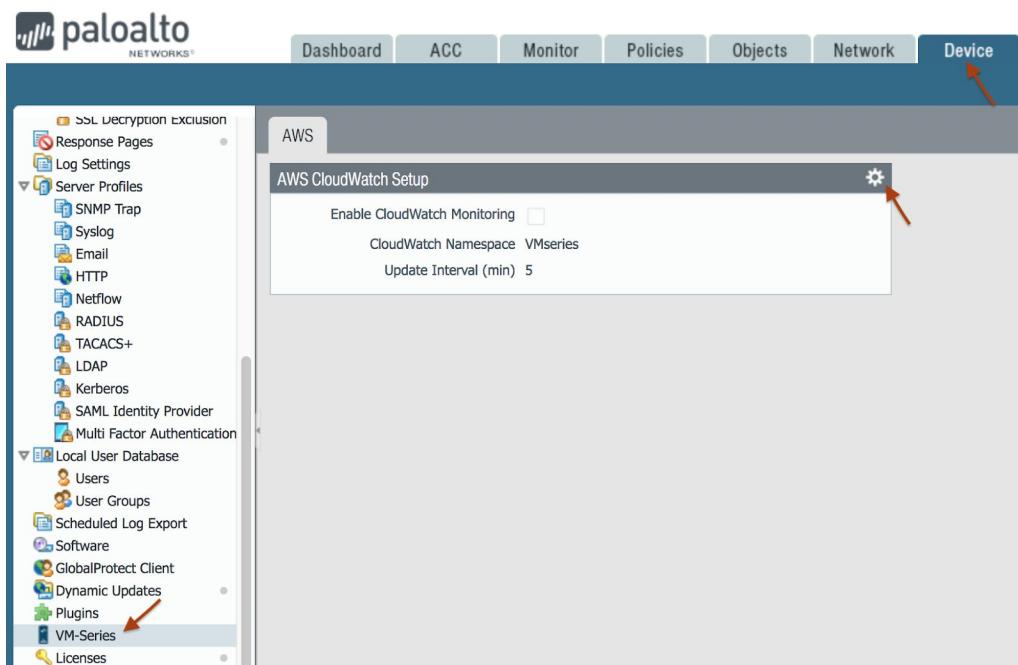
In this activity, you will:

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

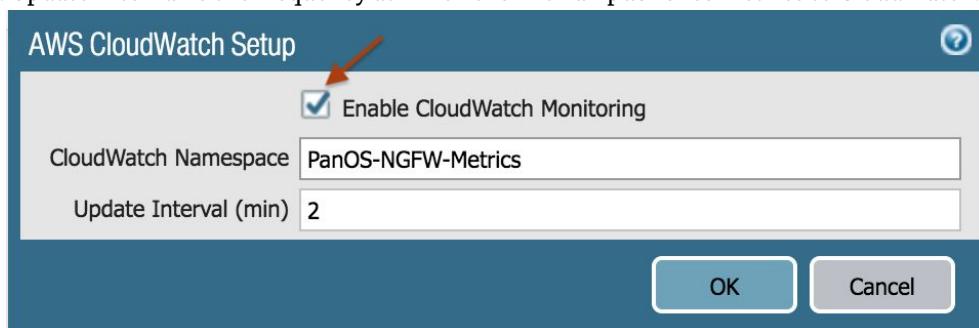
Task 1 - Enable CloudWatch on the VM-Series Firewall

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.

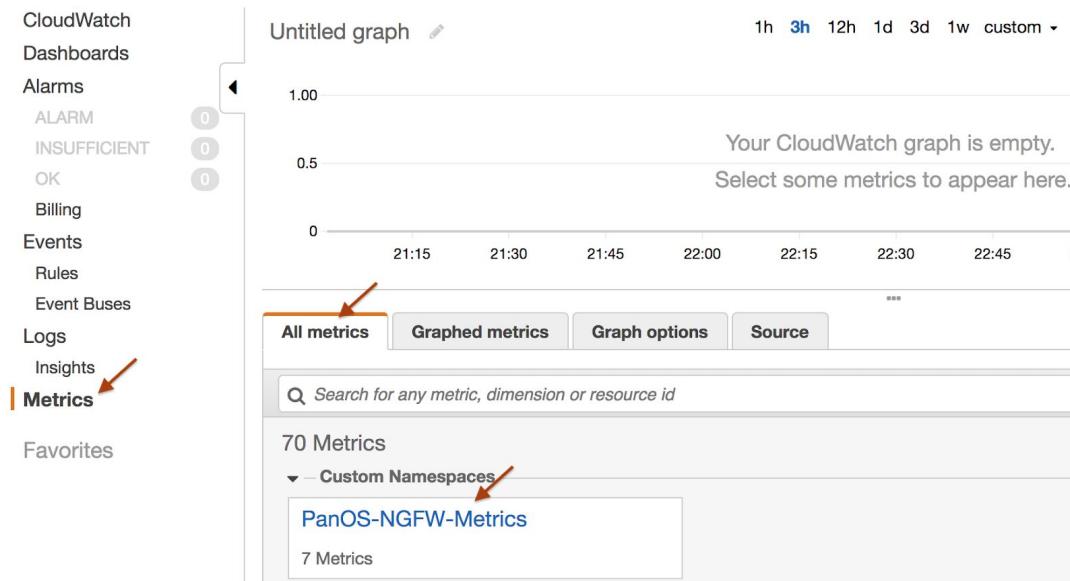


Step 3. From the top right, click Commit to save the changes. Disregard any commit warnings. When the commit is complete, click Close.

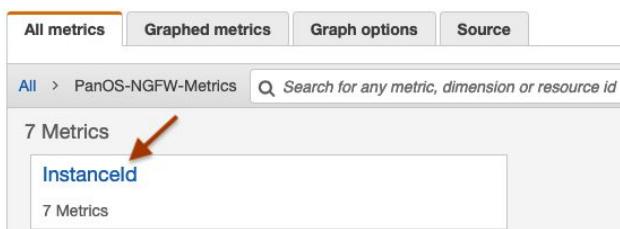
Task 2 - Verify That You Can See the Metrics on CloudWatch

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.



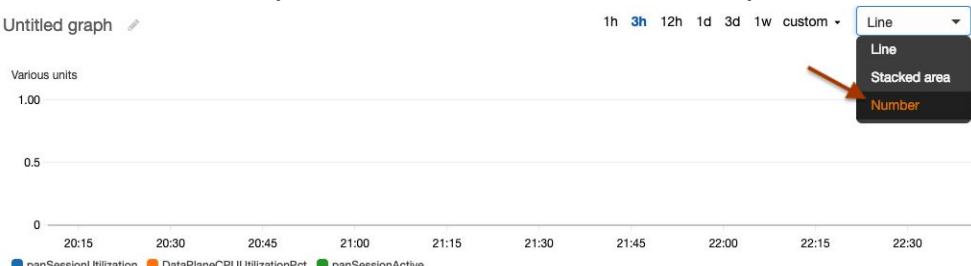
Step 2. Click on InstanceId.



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.

All metrics	Graphed metrics (3)	Graph options	Source
All > PanOS-NGFW-Metrics > InstanceId <input type="text" value="Search for any metric, dimension or resource id"/>			
Instance Name (7)	InstanceId	Metric Name	
<input checked="" type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	panSessionActive	
<input checked="" type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	panSessionUtilization	
<input type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	panGPGWUtilizationActiveTunnels	
<input type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	DataPlanePacketBufferUtilization	
<input type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	panGPGatewayUtilizationPct	
<input type="checkbox"/> VM-Series Firewall	i-012f6477e34631e80	panSessionSslProxyUtilization	
<input checked="" type="checkbox"/> 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.