



# **PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS**

## **Lab 11: Controlling Access to Network Resources with User-ID**

**Document Version: 2025-10-13**

## Contents

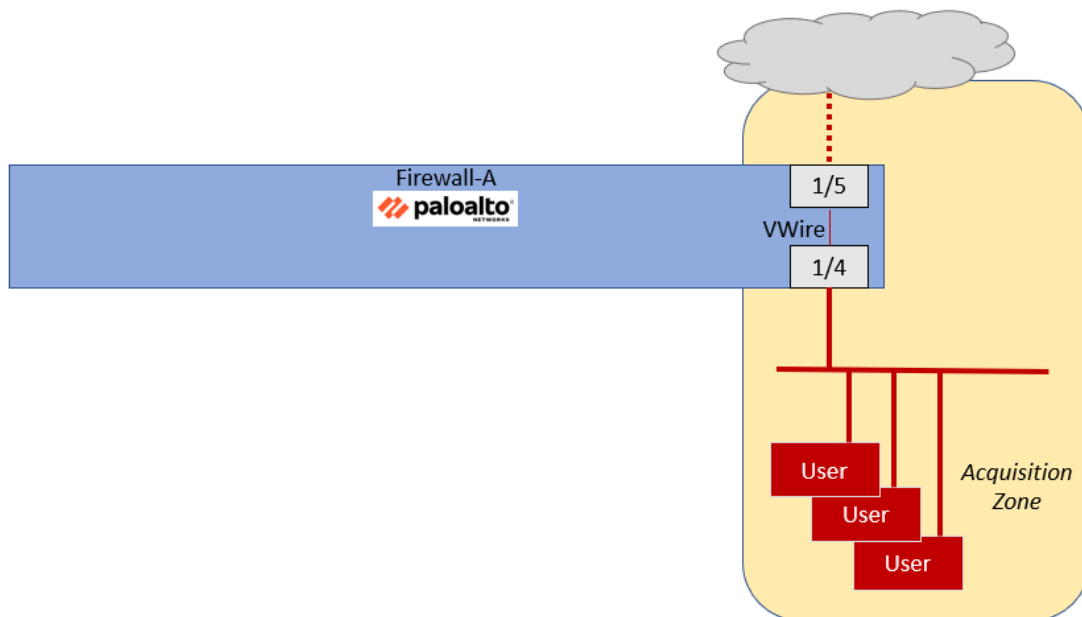
Introduction .....	3
Objective .....	4
Lab Topology .....	5
Theoretical Lab Topology.....	5
Lab Settings .....	6
Lab Guidance.....	6
1 Controlling Access to Network Resources with User-ID – High Level Lab Steps .....	7
1.1 Apply a Baseline Configuration to the Firewall .....	7
1.2 Examine Firewall Configuration.....	7
1.3 Generate Traffic from the Acquisition Zone .....	7
1.4 Modify the Acquisition-Allow-All Security Policy Rule .....	8
1.5 Create Marketing Apps Rule .....	8
1.6 Create Deny Rule .....	8
1.7 Commit the Configuration .....	9
1.8 Generate Traffic from the Acquisition Zone .....	9
1.9 Examine User-ID Logs .....	9
1.10 Examine Firewall Traffic Log .....	9
1.11 Clean Up the Desktop .....	9
2 Controlling Access to Network Resources with User-ID – Detailed Lab Steps .....	10
2.1 Apply a Baseline Configuration to the Firewall .....	10
2.2 Examine Firewall Configuration.....	14
2.3 Generate Traffic from the Acquisition Zone.....	16
2.4 Enable User-ID on the Acquisition Zone.....	20
2.5 Modify the Acquisition-Allow-All- Zone .....	21
2.6 Create Marketing Apps Rule.....	22
2.7 Create Deny Rule .....	25
2.8 Generate Traffic from the Acquisition Zone.....	29
2.9 Exam User-ID Logs .....	30
2.10 Examine Firewall Traffic Log.....	32

## Introduction

Your organization recently acquired another company, and you have been tasked to create appropriate security Policy rules for traffic generated by these new users.

Your firewall has been configured with a virtual wire that allows traffic to the Internet from the users in the newly acquired company. The firewall also has a new security zone in place called Acquisition that contains all new users.

The firewall has an existing Security Policy rule that allows all users in the Acquisition zone to access any application on the internet. Your task is to restrict users in this new organization to approved corporate applications only.

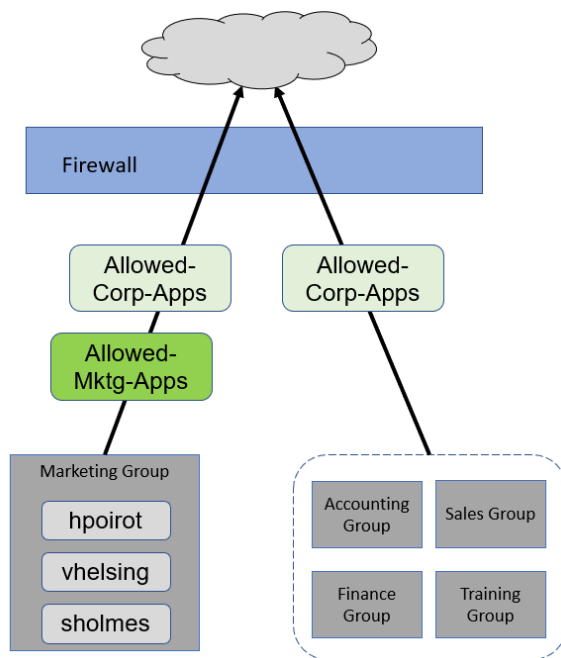


The approved corporate applications include DNS, web-browsing, and SSL.

You also need to ensure that only users in the marketing group are allowed to use social media applications such as Facebook, Instagram, and others.

Another firewall administrator has created the appropriate Application Groups for you.

The firewall receives User-ID and Group membership information about users in this new company from an XML upload sent by network authentication devices. (Note that this is simulated in this lab and outside the scope of this course).



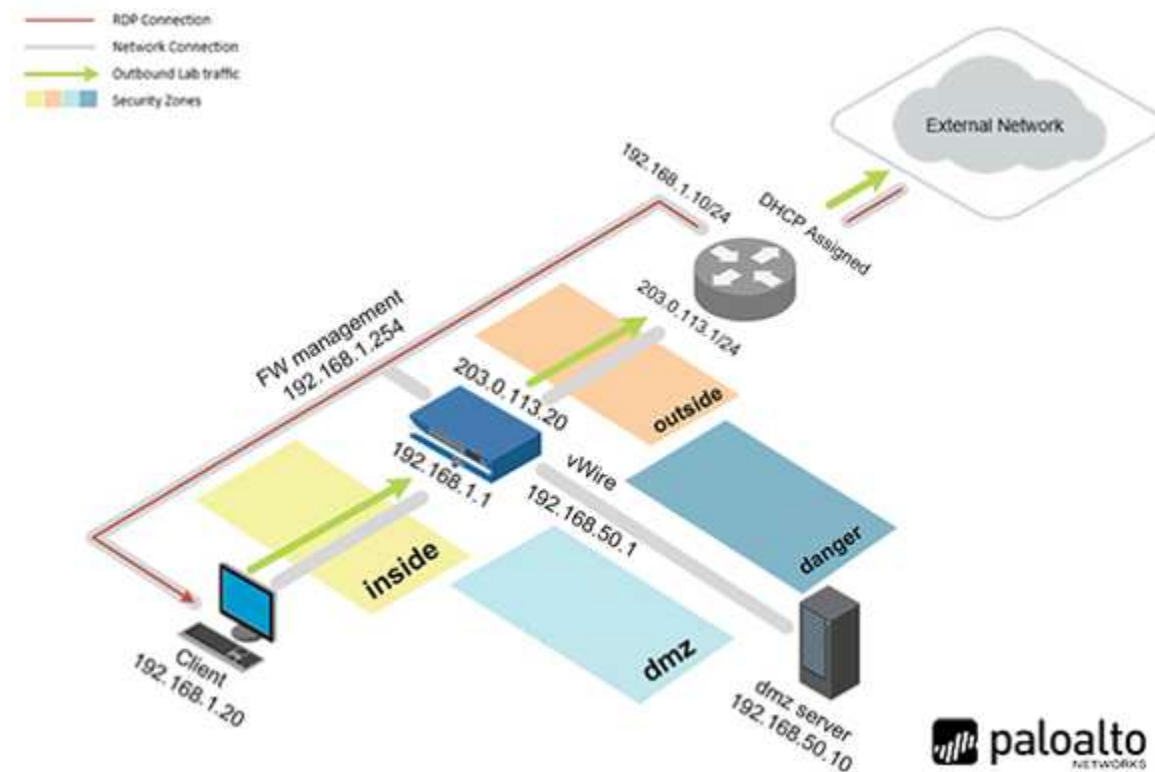
You also need to create a Security Policy rule that explicitly denies any other traffic generated by users in the Acquisition zone. Although the interzone-default rule will deny any traffic not expressly allowed, creating an explicit deny rule will allow you to examine the kinds of applications users in the Acquisition zone are attempting to access.

## Objective

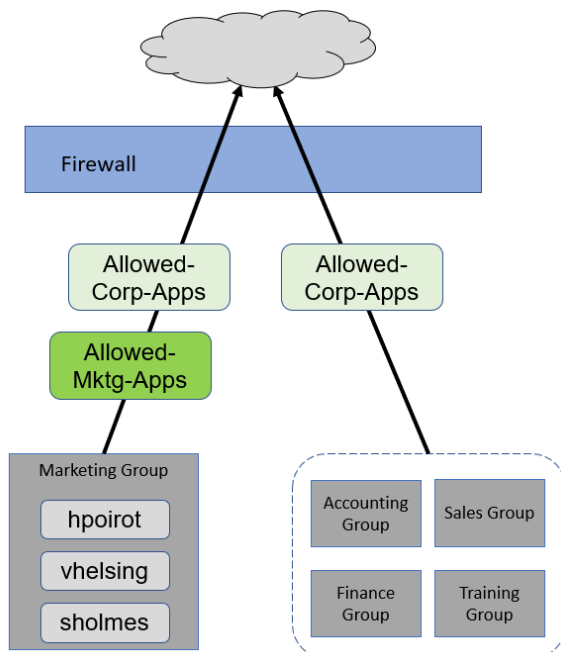
In this lab, you will perform the following tasks:

- Examine current configuration.
- Enable User-ID technology in the Acquisition zone.
- Generate traffic.
- Modify Security Policy to meet requirements.

## Lab Topology



## Theoretical Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!
vRouter	192.168.1.10	root	Pal0Alt0

## Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.



### Please Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

## 1 Controlling Access to Network Resources with User-ID – High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

### 1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-11.xml** to the Firewall.

### 1.2 Examine Firewall Configuration

- Review the settings that another administrator has configured for Application Groups and Security Policy rules, and verify the following settings on the **Acquisition-Allow-All** Security Policy rule.

Parameter	Value
Source Zone	Acquisition
Source Address	Any
Destination Zone	any
Destination IP	Any
Application	Any
Action	Allow

- Clear the counters for all Security Policy rules.
- Use the information below to verify that the configuration contains two new **Application Groups**.

Name	Applications
Allowed-Corp-Apps	dns web-browsing ssl
Allowed-Mktg-Apps	facebook-base instagram-base twitter-base myspace-base linkedin-base

### 1.3 Generate Traffic from the Acquisition Zone

- Use **Remmina** to connect to the **Server-Extranet** host.
- Change to the appropriate directory.  
**cd /home/paloalto42/pcaps92019/app.pcaps <Enter>**
- Run the following command to start generating traffic in the Acquisition Zone:

### ./Appgenerator-2.sh <Enter>

- While the script is running, examine the firewall Traffic log under **Monitor > Logs > Traffic**.
- Note that almost all traffic is hitting the **Acquisition-Allow-All Rule**.
- Add the **Source User** column to the Traffic Log.

## 1.4 Modify the Acquisition-Allow-All Security Policy Rule

- Change the name of the Security Policy rule **Acquisition-Allow-All** to **Allow-Corp-Apps**.
- Change the Description field to **Allows only approved apps for Acquisition users**.
- Set the Applications to use only the **Allowed-Corp-Apps** Application Group.

## 1.5 Create Marketing Apps Rule

- Use the information below to create a Security Policy rule to allow only Marketing users to access the Allowed-Mktg-Apps.

Parameter	Value
Name	Allow-Mktg-Apps
Description	Allows only users of marketing group to access Mktg apps
Source Zone	Acquisition
Source User	marketing
Destination Zone	any
Application	Allowed-Mktg-Apps
Dependent Applications	Add to Current Rule
Action	Allow

## 1.6 Create Deny Rule

- Use the information below to create a new Security Policy rule that will deny any other application traffic for users in the Acquisition zone.

Parameter	Value
Name	Deny-All-Others
Description	Denies non-approved applications for users in Acquisition zone
Source Zone	Acquisition
Source User	Any
Destination Zone	any
Application	Any
Action	Deny

- Place the **Deny-All-Others** rule at the bottom of the Security Policy.



## 1.7 Commit the Configuration

- Commit the changes before proceeding.

## 1.8 Generate Traffic from the Acquisition Zone

- Use the Extranet-Server connection in the Remmina application to run the **Appgenerator-2.sh** script again.
- While the script is running, move to the next section in which you will examine the firewall logs.

## 1.9 Examine User-ID Logs

- Use the firewall CLI and the web interface to examine information about User-ID.
- The firewall should have numerous entries with username-to-ip-address mappings in the User-ID log.
- Use the Remmina application to connect to the CLI of **Firewall-A**.
- Use the following command to display entries for User-ID:

**show user ip-user-mapping all <Enter>**

- Close the firewall SSH connection.

## 1.10 Examine Firewall Traffic Log

- Create and apply filters in the Traffic log to answer the questions in this section.
  - Which rule does the firewall use when it encounters youtube-base traffic?
  - Which rule does the firewall use when it encounters dns traffic?
  - Which rule does the firewall use when it encounters facebook-base?
  - Which users are allowed access to facebook-base?
  - Is the user sholmes allowed to access instagram-base?
  - Is the user bbart allowed to access instagram-base?

## 1.11 Clean Up the Desktop

- In the Traffic log window on the firewall, clear any filters you have in place.
- In the Remmina application window, close the SSH connections to the firewall and the Server-Extranet.
- Close the main Remmina application window.

## 2 Controlling Access to Network Resources with User-ID – Detailed Lab Steps

It is recommended to use this section if you prefer detailed guidance to complete the objectives for this lab. It is strongly recommended that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

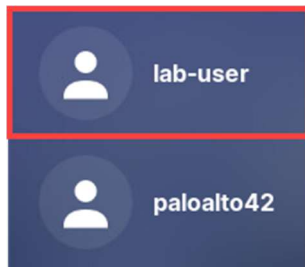
### 2.1 Apply a Baseline Configuration to the Firewall

In this section, you will connect to the Firewall and load the Firewall configuration file.

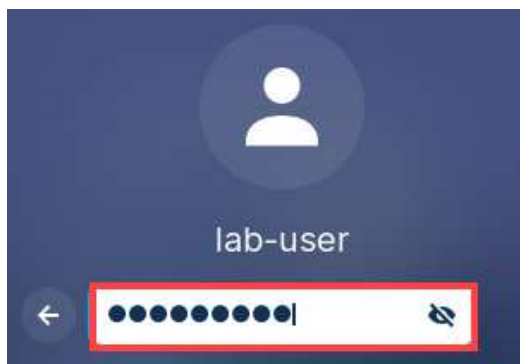
1. Click on the **Client** tab to access the Client PC.



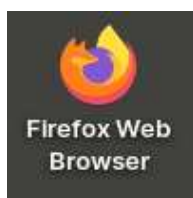
2. On the *Zorin* desktop, click **lab-user**.



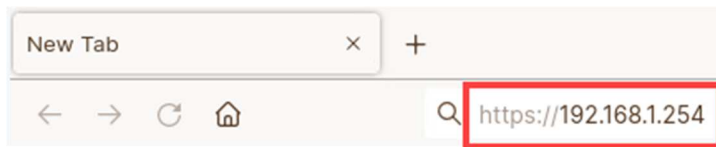
3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.



5. In the *Firefox* address field, type **https://192.168.1.254** and press **Enter**.

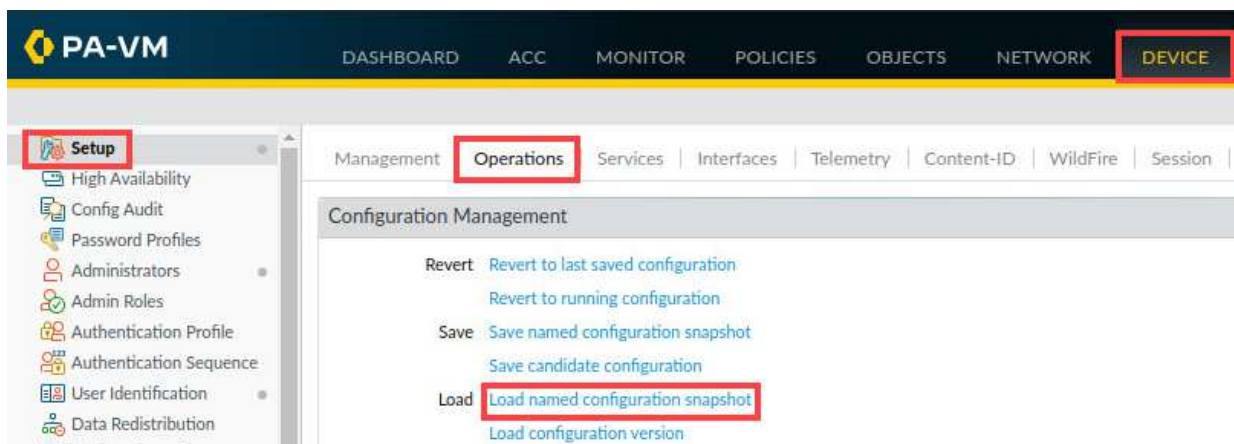


6. Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.

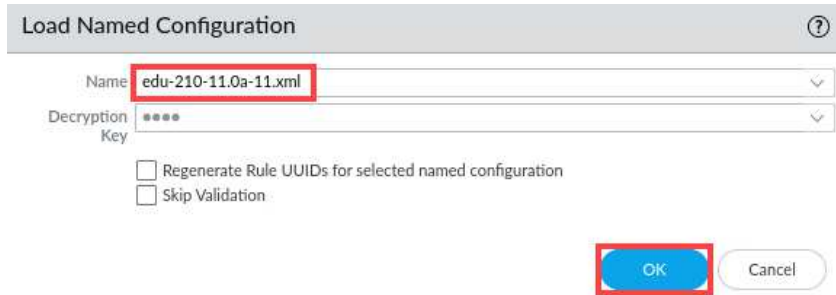


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

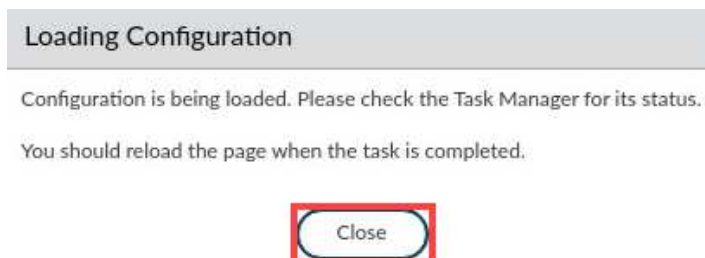


8. In the *Load Named Configuration* window, select **edu-210-11.0a-11.xml** from the *Name* drop-down box and click **OK**.



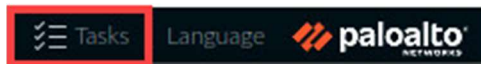
The dialog box titled "Load Named Configuration" has a "Name" dropdown menu with "edu-210-11.0a-11.xml" selected. Below it is a "Decryption Key" field with four asterisks. There are two checkboxes: "Regenerate Rule UUIDs for selected named configuration" and "Skip Validation". At the bottom are "OK" and "Cancel" buttons.

9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.

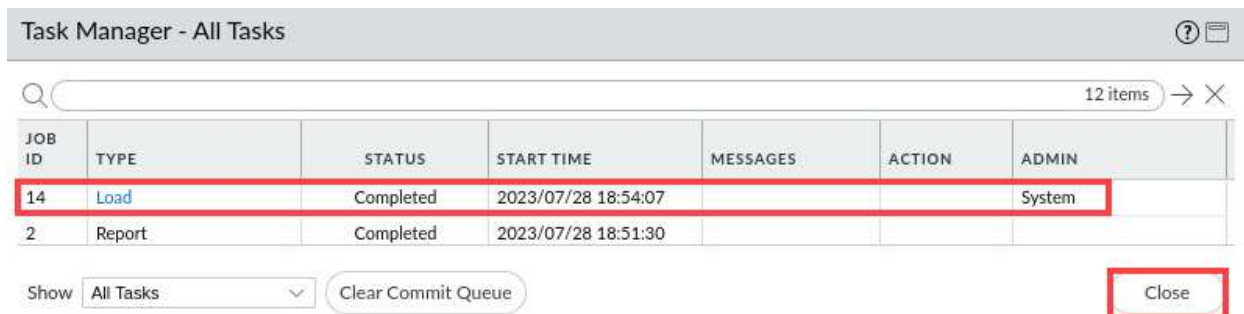


The "Loading Configuration" message box states: "Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed." There is a "Close" button at the bottom.

10. Click the **Tasks** icon located at the bottom-right of the web interface.



11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**



The "Task Manager - All Tasks" window shows a table of tasks. The first row is highlighted with a red box.

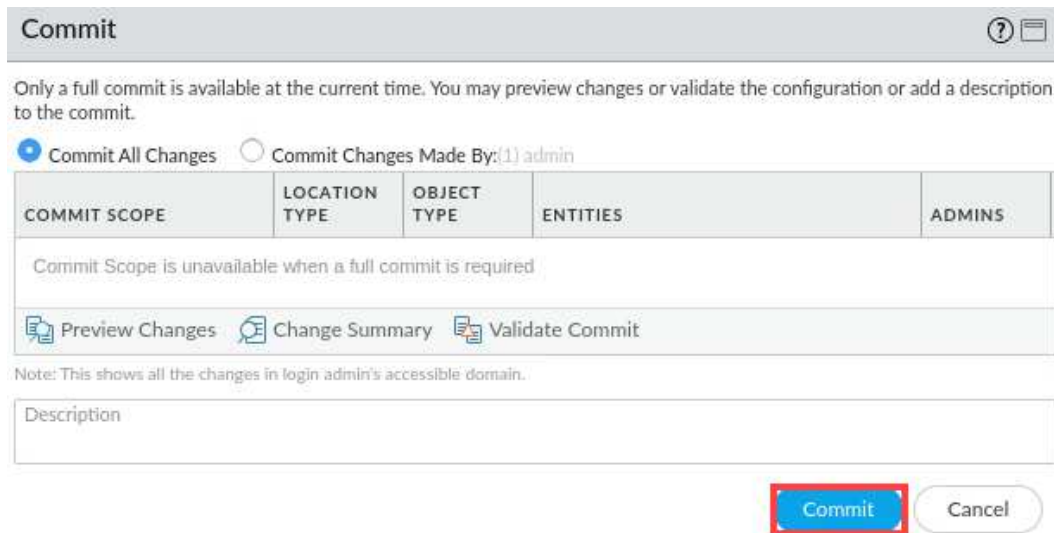
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

Below the table, there is a "Show" dropdown menu set to "All Tasks", a "Clear Commit Queue" button, and a "Close" button.

12. Click the **Commit** link located at the top-right of the web interface.



13. In the *Commit* window, click **Commit** to proceed with committing the changes.






**Commit** ⓘ

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

☒ Commit All Changes ☐ Commit Changes Made By: (1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
Commit Scope is unavailable when a full commit is required				

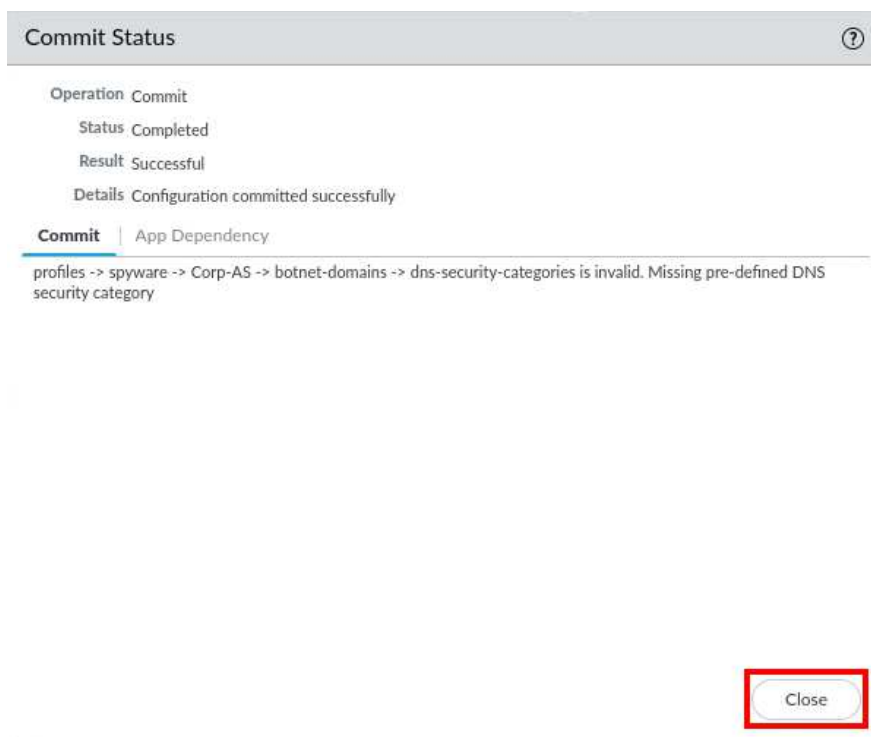
 Preview Changes
  Change Summary
  Validate Commit

Note: This shows all the changes in login admin's accessible domain.

Description

**Commit** Cancel

14. When the commit operation is complete, click **Close** to continue.



**Commit Status** ⓘ

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

**Commit** | App Dependency

profiles -> spyware -> Corp-AS -> botnet-domains -> dns-security-categories is invalid. Missing pre-defined DNS security category

**Close**



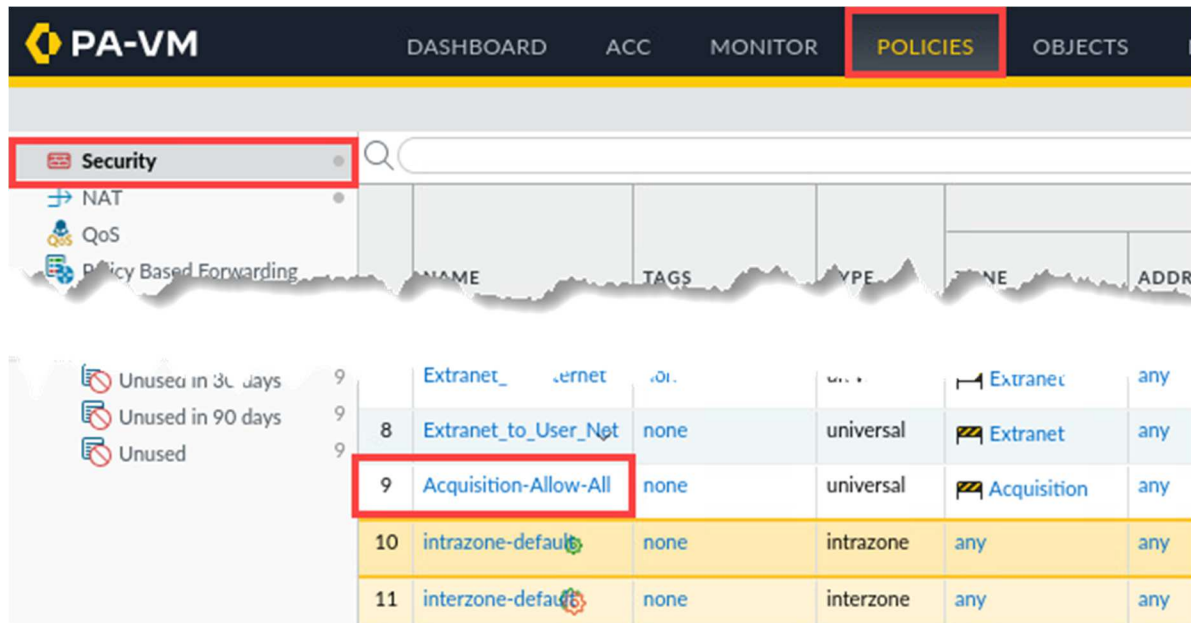
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 2.2 Examine Firewall Configuration

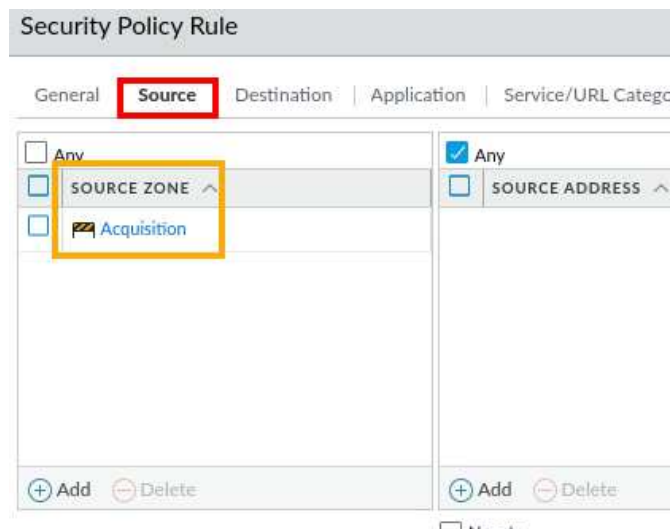
In this section, you will review the settings that another administrator has configured for Application Groups and Security policy rules.

1. Select **Policies > Security**. Scroll down and click the **Acquisition-Allow-All** policy.



	NAME	TAGS	TYPE	ZONE	ADDR
9	Extranet_to_User_Net	none	universal	Extranet	any
9	<b>Acquisition-Allow-All</b>	none	universal	Acquisition	any
10	intrazone-default	none	intrazone	any	any
11	interzone-default	none	interzone	any	any

2. In the *Security Policy Rule*, select the **Source** tab. Note that the *Source Zone* is set to **Acquisition**.



Security Policy Rule

General **Source** Destination Application Service/URL Category

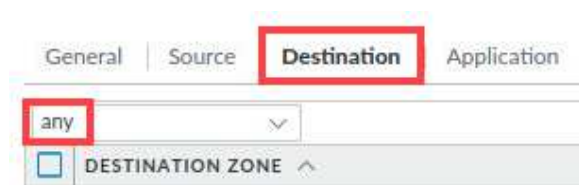
☐ Any ☒ Any

☐ SOURCE ZONE ☐ SOURCE ADDRESS

☐ Acquisition

+ Add - Delete + Add - Delete

3. Select the **Destination** tab. Note that the *Destination Zone* is set to **any**.

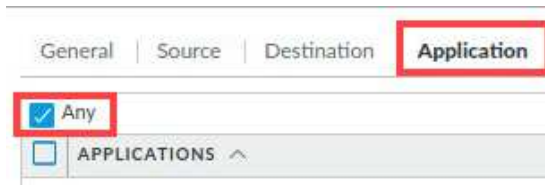


General Source **Destination** Application

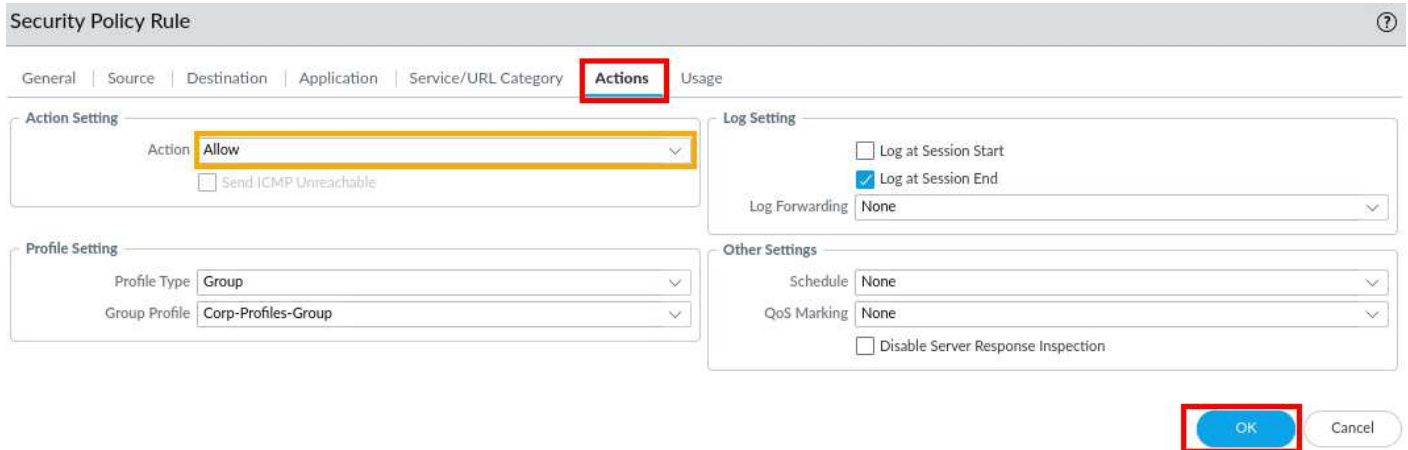
**any**

☐ DESTINATION ZONE

4. Select the **Application** tab. Note that the *Application* is set to **Any**.



5. Select the **Actions** tab. Note that the **Action** is set to **Allow**. Click **OK**.



**Please  
Note**

This Security policy rule allows any host in the Acquisition security zone to access any application anywhere.

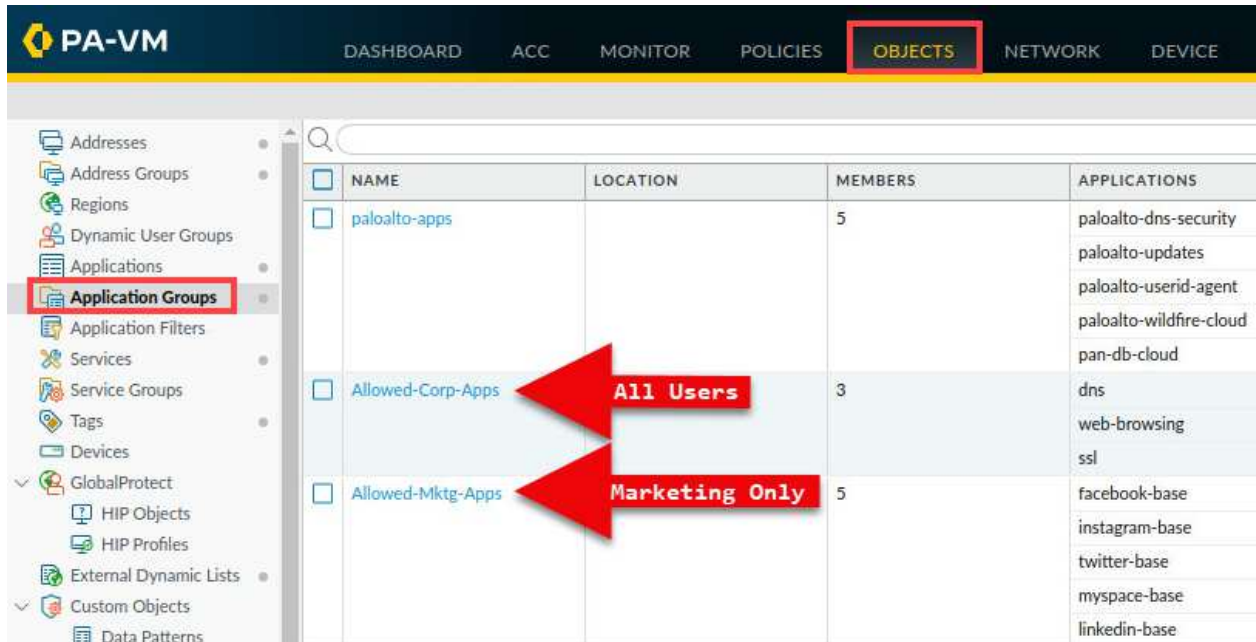
6. Clear the counters for all Security policy rules by clicking **Reset Rule Hit Counter > All rules** at the bottom of the window.



7. In the *Reset* window, click **Yes**.



8. Select **Objects > Application Groups** and note the two new **Application Groups**.



NAME	LOCATION	MEMBERS	APPLICATIONS
<input type="checkbox"/> paloalto-apps		5	paloalto-dns-security paloalto-updates paloalto-userid-agent paloalto-wildfire-cloud pan-db-cloud
<input type="checkbox"/> Allowed-Corp-Apps		3	dns web-browsing ssl
<input type="checkbox"/> Allowed-Mktg-Apps		5	facebook-base instagram-base twitter-base myspace-base linkedin-base

**Please Note**

You will configure the firewall to allow all users in the Acquisition zone to use the Allowed-Corp-Apps. However, only users in the Marketing group will be able to use applications in the Allowed-Mktg-Apps group.

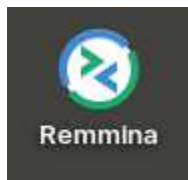
9. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



## 2.3 Generate Traffic from the Acquisition Zone

In this section, you will configure a packet capture on the firewall's data plane. The goal of the packet capture is to identify a unique bit pattern that can be used to create a custom application signature.

1. On the client desktop, open the **Remmina** application.



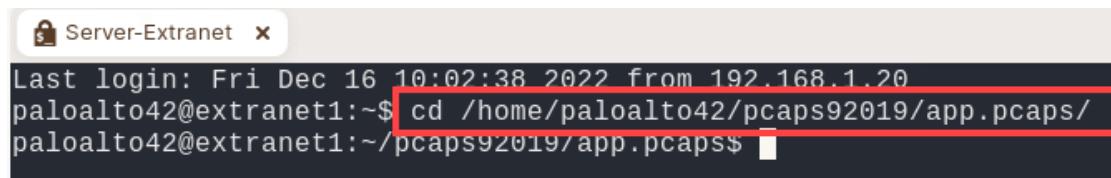


2. Double-click the entry for **Server-Extranet**.



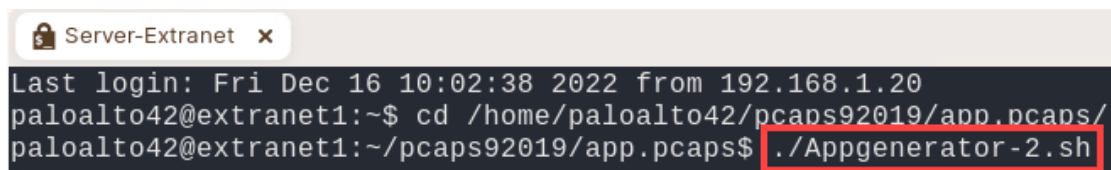
3. In the CLI connection enter the following command.

```
paloalto42@extranet1:~$ cd /home/paloalto42/pcaps92019/app.pcaps/ <Enter>
```



4. In the CLI connection enter the following command.

```
paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh <Enter>
```



5. Verify the **Appgenerator-2** script is running.

```

Server-Extranet x
This simulated traffic does not leave the lab environment since
it is generated only within a limited vWire deployment.

The simulated traffic should match a variety of AppIDs which you
can see in the Traffic Log and in Custom Reports.

The script will take about 10 minutes.

=====

Actual: 1913 packets (1505332 bytes) sent in 5.46 seconds
Rated: 275557.1 Bps, 2.20 Mbps, 350.18 pps
Flows: 111 flows, 20.31 fps, 1913 flow packets, 0 non-flow
Statistics for network device: ens224
    Successful packets:      1913
    Failed packets:         0
    Truncated packets:      0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
Actual: 2560 packets (2057325 bytes) sent in 7.31 seconds
Rated: 281384.6 Bps, 2.25 Mbps, 350.13 pps
Flows: 116 flows, 15.86 fps, 2560 flow packets, 0 non-flow
Statistics for network device: ens224
    Successful packets:      2560
    Failed packets:         0
    Truncated packets:      0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0

```



Allow the *Appgenerator-2* script to complete before continuing to the next step.

```

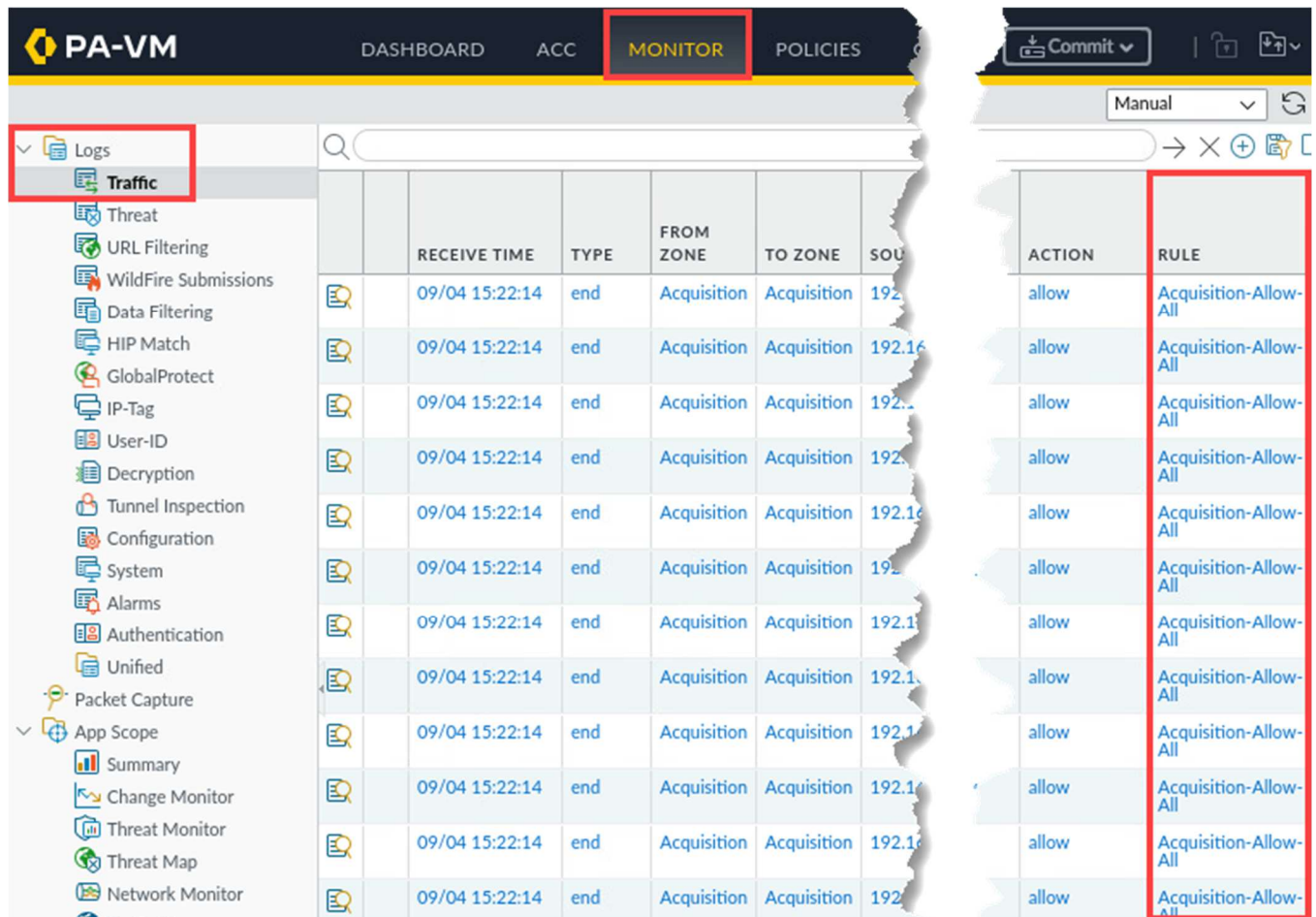
Server-Extranet x
Elapsed time for this script was 214 seconds.
#####
# Process Complete ! #
#####
paltoalto42@extranet1:~/pcaps92019/app.pcaps$

```

6. Re-open the *PA-VM firewall* web interface by clicking on the **Firefox** icon in the task bar.



7. Select **Monitor > Logs > Traffic**. Clear any filters in place. Note that almost all traffic is hitting the **Acquisition-Allow-All** rule. Please allow the Firewall 3 to 6 minutes for the traffic logs to update.

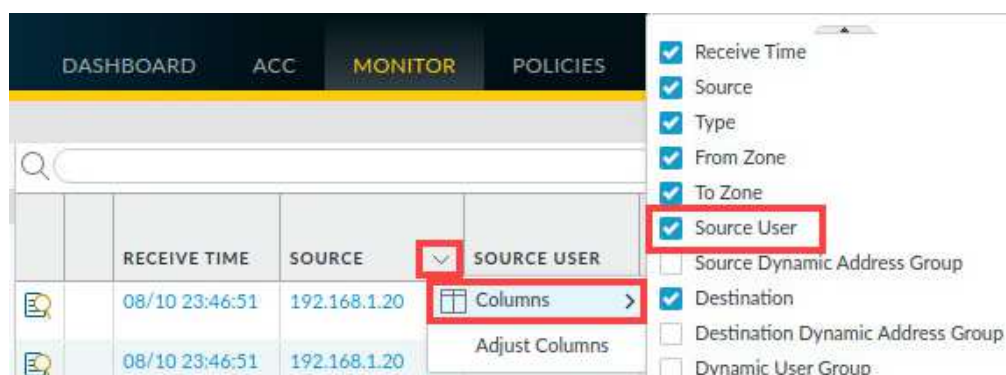


RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	ACTION	RULE
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All
09/04 15:22:14	end	Acquisition	Acquisition	192.168.1.10	allow	Acquisition-Allow-All

**Please Note**

Some columns have been hidden to show what is presented in the above screen shot. You may hide and show columns as needed for the duration of this lab.

8. Add the **Source User** column if necessary to the table by clicking the small triangle in any header and choosing **Columns > Source User**.



RECEIVE TIME	SOURCE	SOURCE USER
08/10 23:46:51	192.168.1.20	
08/10 23:46:51	192.168.1.20	

- Drag and drop the **Source User** column between the **Receive Time** and **Source** columns.



	RECEIVE TIME	SOURCE	SOURCE USER
	08/10 23:46:51	1	✓ SOURCE USER
	08/10 23:46:51	192.168.1.20	

RECEIVE TIME	SOURCE USER	SOURCE
08/10 23:46:51		192.168.1.20
08/10 23:46:51		192.168.1.20

**Please Note**

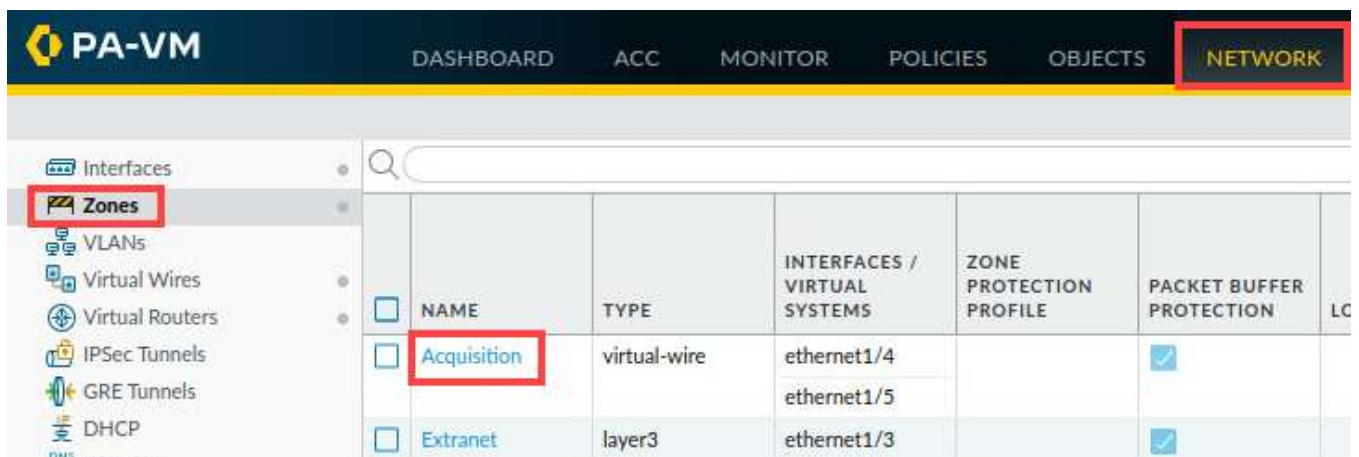
This action will make it easier for you to locate Source User information later in this lab.

- Leave the *Palo Alto Networks Firewall* window open and continue to the next task.

## 2.4 Enable User-ID on the Acquisition Zone

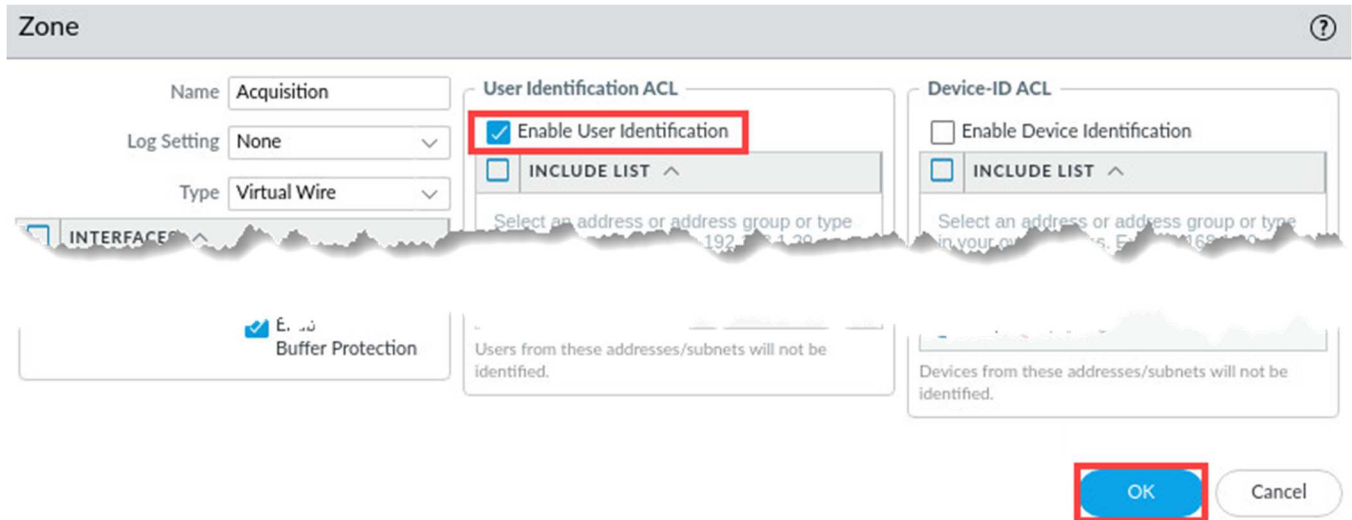
In this section you will enable User-ID on the Acquisition security zone as part of the process of enabling User-ID on a firewall.

- Select **Network > Zones**. Click **Acquisition** to open the zone.



PA-VM						
DASHBOARD ACC MONITOR POLICIES OBJECTS <b>NETWORK</b>						
Interfaces						
<b>Zones</b>						
VLANs						
Virtual Wires						
Virtual Routers						
IPSec Tunnels						
GRE Tunnels						
DHCP						
DNS						
	<input type="checkbox"/>	NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION
	<input type="checkbox"/>	Acquisition	virtual-wire	ethernet1/4 ethernet1/5		<input checked="" type="checkbox"/>
	<input type="checkbox"/>	Extranet	layer3	ethernet1/3		<input checked="" type="checkbox"/>

- In the Zone window, select the **Enable User Identification** check box. Click **OK**.

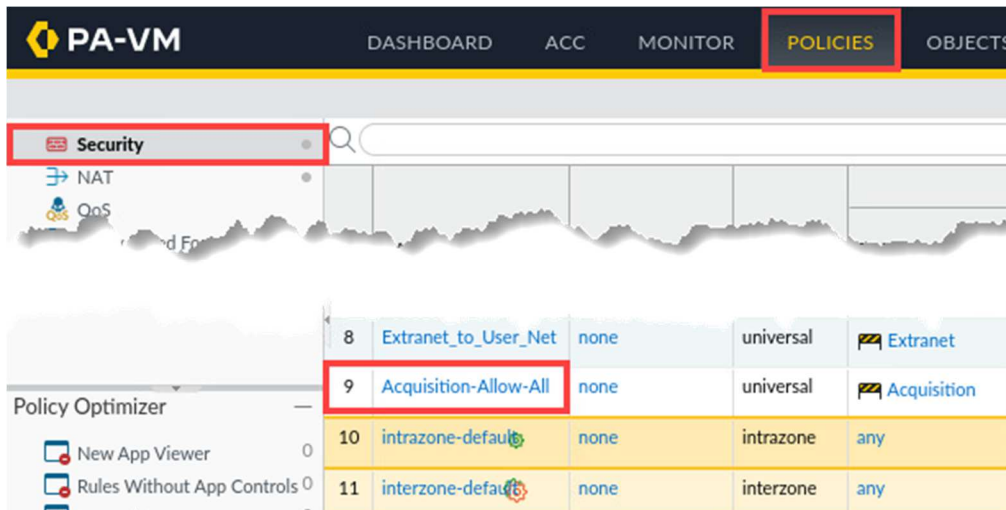


- Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 2.5 Modify the Acquisition-Allow-All- Zone

In this section, you will now change the set of applications that Acquisition users are allowed to access by modifying the existing *Acquisition-Allow-All* rule.

- Select **Policies > Security**. Scroll down and click **Acquisition-Allow-All**.



Policy ID	Policy Name	Action	Log	Category	Application
8	Extranet_to_User_Net	none	universal	Extranet	
9	Acquisition-Allow-All	none	universal	Acquisition	
10	intrazone-default	none	intrazone	any	
11	interzone-default	none	interzone	any	

- In the *Security Policy Rule* window, under the *General* tab, change the name of this rule to **Allow-Corp-Apps**. For *Description*, type **Allows only approved apps for Acquisition users**.



Security Policy Rule

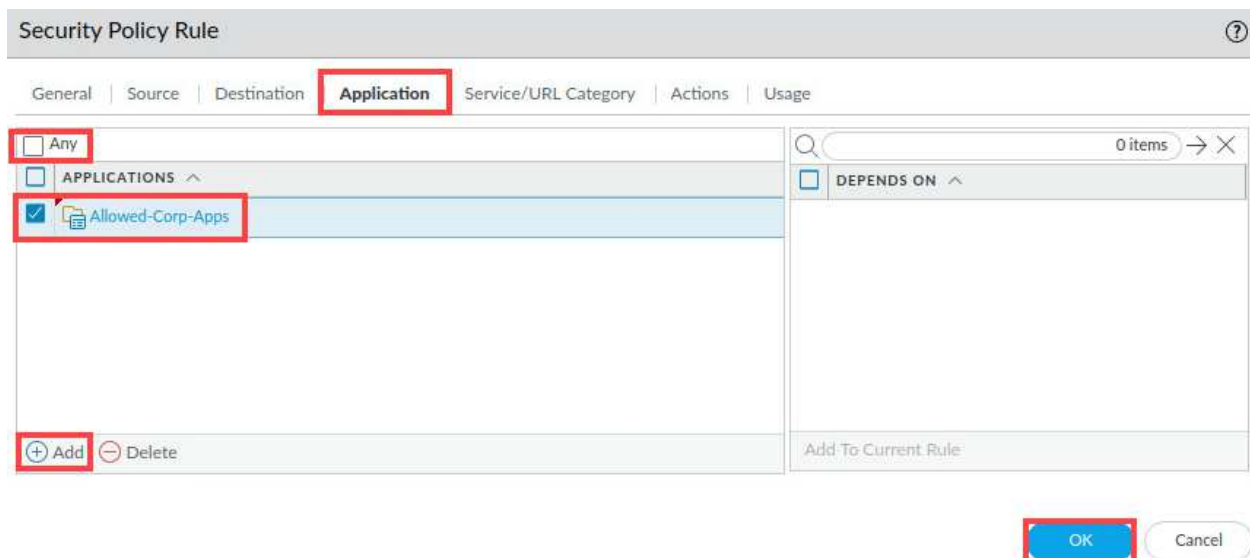
**General** | Source | Destination | Application | Service/URL Category

Name: **Allow-Corp-Apps**

Rule Type: universal (default)

Description: **Allows only approved apps for Acquisition users**

- Select the **Application** tab, uncheck the option for *Any*. Click **Add** and enter the first few letters of the **Allowed-Corp-Apps** to display the *Application Groups* available. Click **OK**.



Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions | Usage

☐ Any

☐ APPLICATIONS ^

☒ Allowed-Corp-Apps

☐ DEPENDS ON ^

☒ Add ☐ Delete

Add To Current Rule

**OK** Cancel

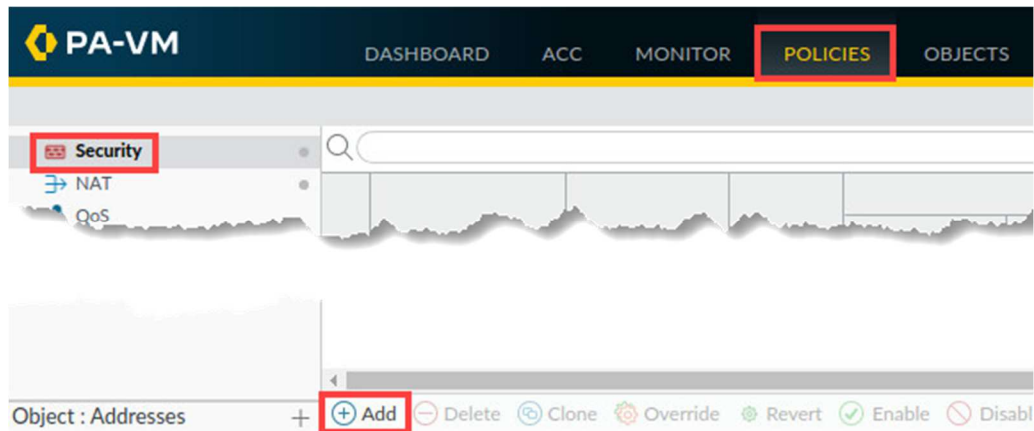
- Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 2.6 Create Marketing Apps Rule

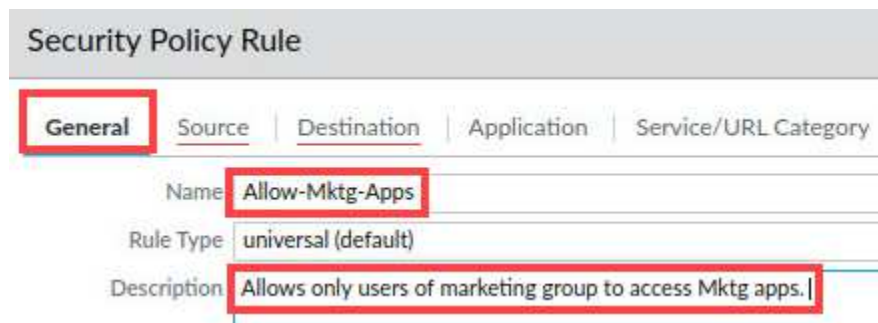
In this section, you will create a new Security policy rule to allow only Marketing users to access the Allowed-Mktg-Apps.



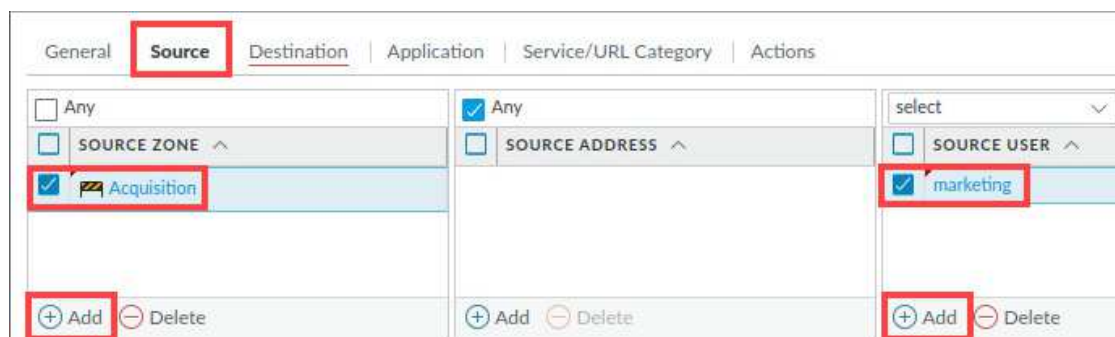
1. Select **Policies > Security**. Click **Add**.



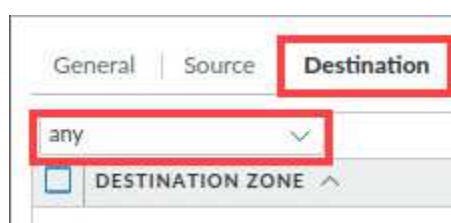
2. In the *Security Policy Rule* window, under the *General* tab, enter **Allow-Mktg-Apps** for the *Name*. For *Description*, enter Allows only users of marketing group to access Mktg apps.



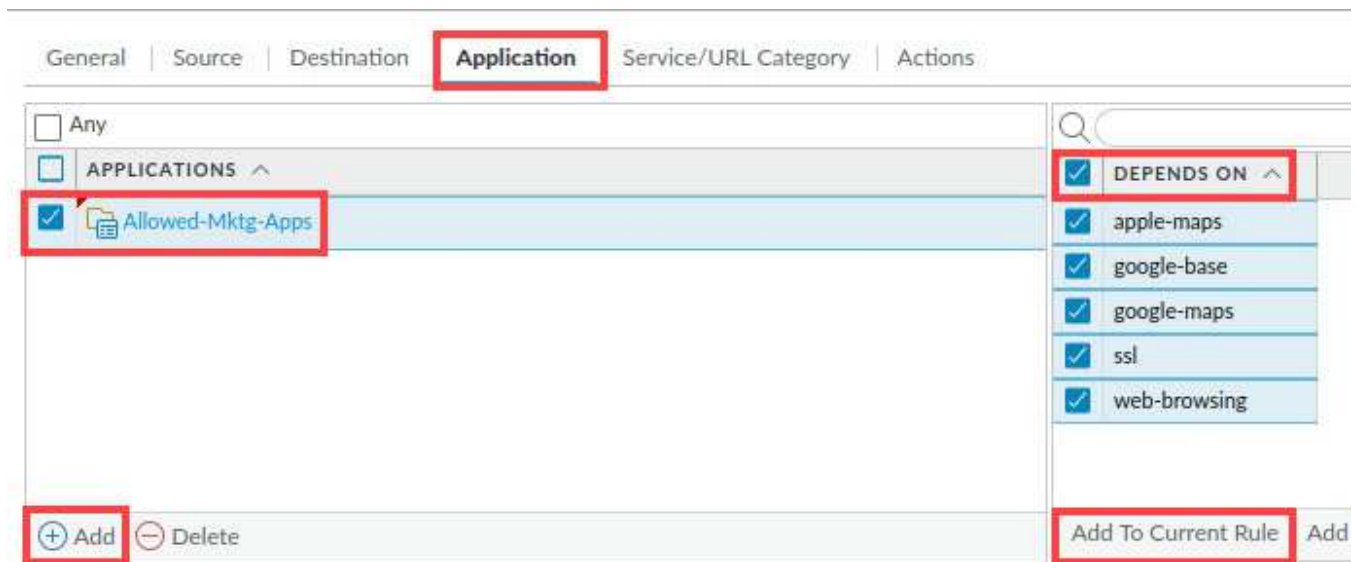
3. Select the **Source** tab, under *Source Zone*, click **Add**. Select **Acquisition**. Under the *Source User* column, click **Add** and enter **marketing**.



4. Select the **Destination** tab. Use the drop-down list at the top to select **any** in the *Destination Zone*.



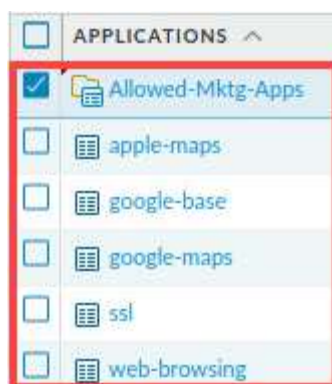
5. Select the **Application** tab and *uncheck* the option for **Any**. Click **Add** and enter the first few letters of the **Allowed-Mktg-Apps** to display the *Application Groups* available. Select **Allowed-Mktg-Apps**. In the right side of the *Application* window, place a **check** box beside **DEPENDS ON**. Click **Add to Current Rule**.



**Please Note**

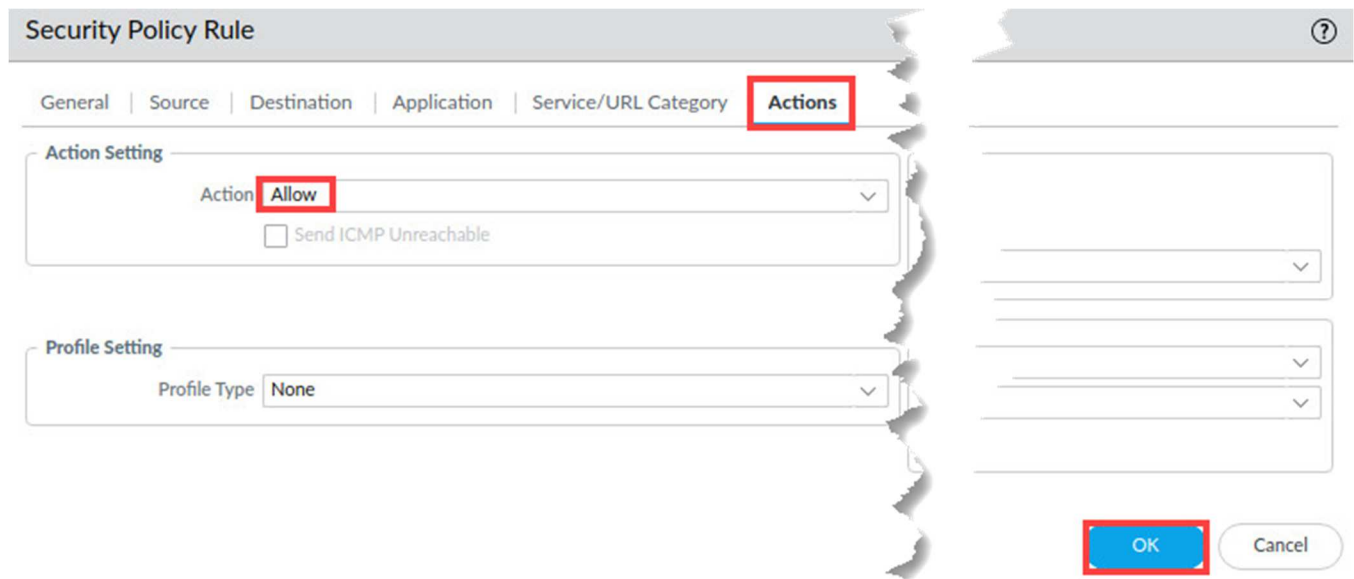
This action will select all the individual applications under the DEPENDS ON column. Note that the list of applications in the Depends On column may differ from the example here.

6. Notice the *applications* have now been added to the *Applications* window.





7. Select the **Actions** tab and verify the *Action* is set to **Allow**. Click **OK**.



**Please Note**

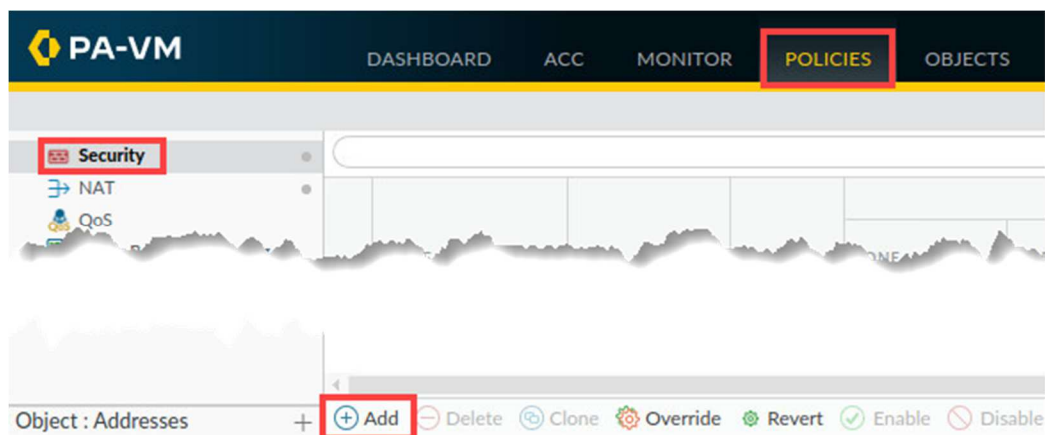
When you create a new Security policy rule, the default setting for Action is Allow. However, it is always a good practice to verify this setting before closing the window.

8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

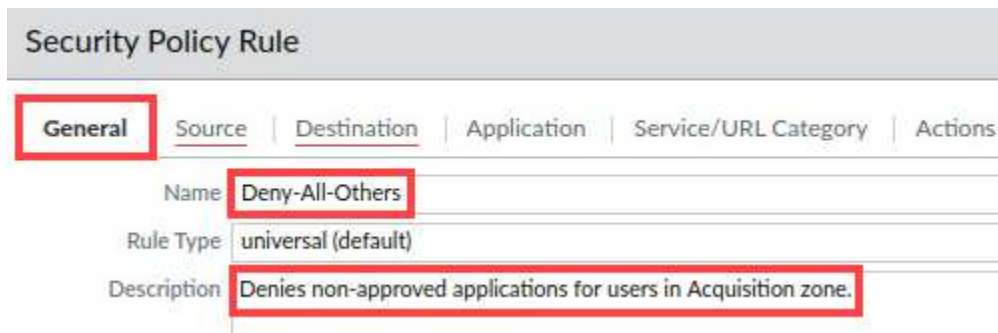
## 2.7 Create Deny Rule

In this section, you will create a new Security Policy rule that will deny any other application traffic for users in the Acquisition zone.

1. Select **Policies > Security**. Click **Add**.



- In the *Security Policy Rule* window, under the *General* tab, enter **Deny-All-Others** for the *Name*. For *Description*, enter **Denies non-approved applications for users in Acquisition zone.**



**Security Policy Rule**

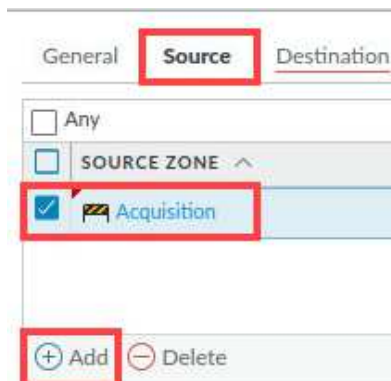
**General** | Source | Destination | Application | Service/URL Category | Actions

Name: **Deny-All-Others**

Rule Type: universal (default)

Description: **Denies non-approved applications for users in Acquisition zone.**

- Select the tab for **Source**, click **Add** and select **Acquisition**.



General | **Source** | Destination

☐ Any

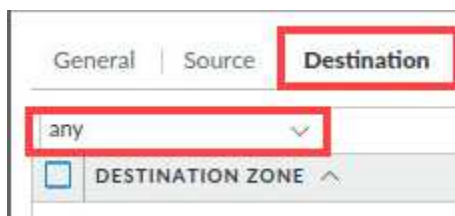
☐ SOURCE ZONE ^

☒ Acquisition

**Please Note**

Note that you do not need to specify any users or user groups under the Source User column. Because the drop-down list is set to any, this rule will deny traffic to any user, regardless of group membership.

- Select the tab for **Destination**, use the drop-down list at the top to select **any**.

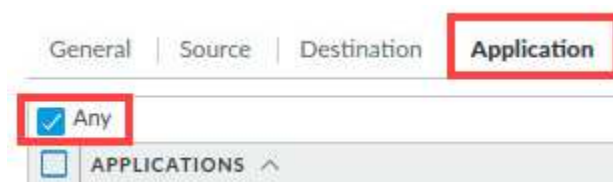


General | Source | **Destination**

any

☐ DESTINATION ZONE ^

- Select the tab for **Application** and verify that **Any** is checked.

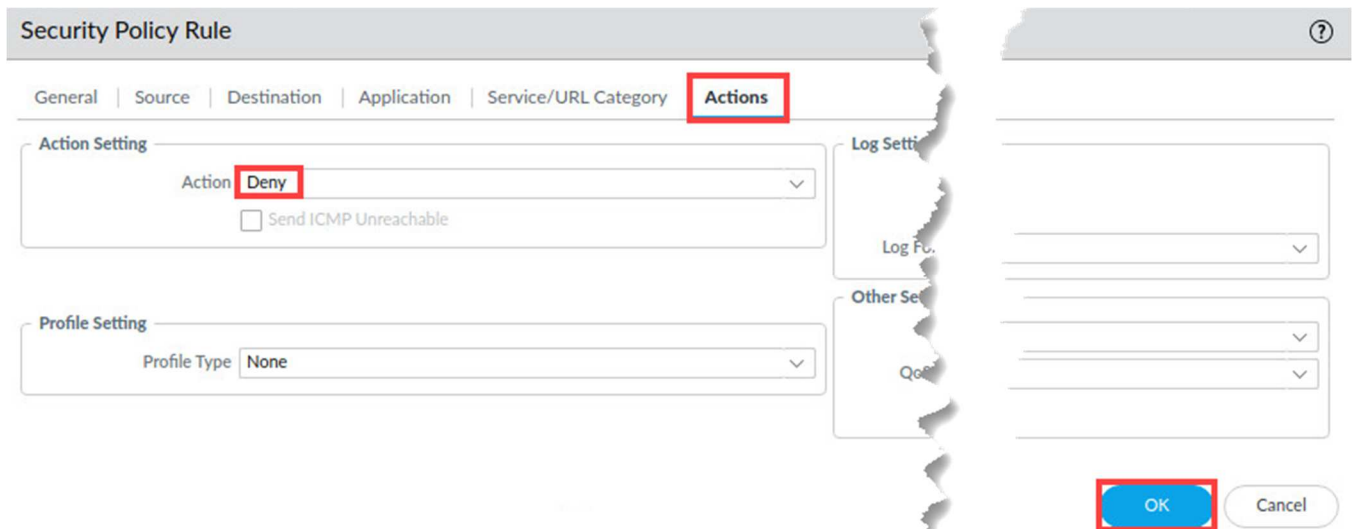


General | Source | Destination | **Application**

☒ Any

☐ APPLICATIONS ^

6. Select the **Actions** tab and change the **Action Setting** to **Deny**. Click **OK**.



**Security Policy Rule**

General | Source | Destination | Application | Service/URL Category | **Actions**

**Action Setting**

Action: **Deny**

☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: **None**

**Log Setting**

Log File: **Log File**

**Other Settings**

Queue: **Queue**

**OK** Cancel

7. Verify that the **Deny-All-Others** rule appears at the bottom of the Security policy.

8	Allow-Corps-Apps	none	universal	Acquisition	any	any
9	Allow-Mktg-Apps	none	universal	Acquisition	any	marketing
10	Deny-All-Others	none	universal	Acquisition	any	any
11	intrazone-default	none	intrazone	any	any	any

+ Add - Delete Clone Override Revert Enable Disable Move PDF/CSV High

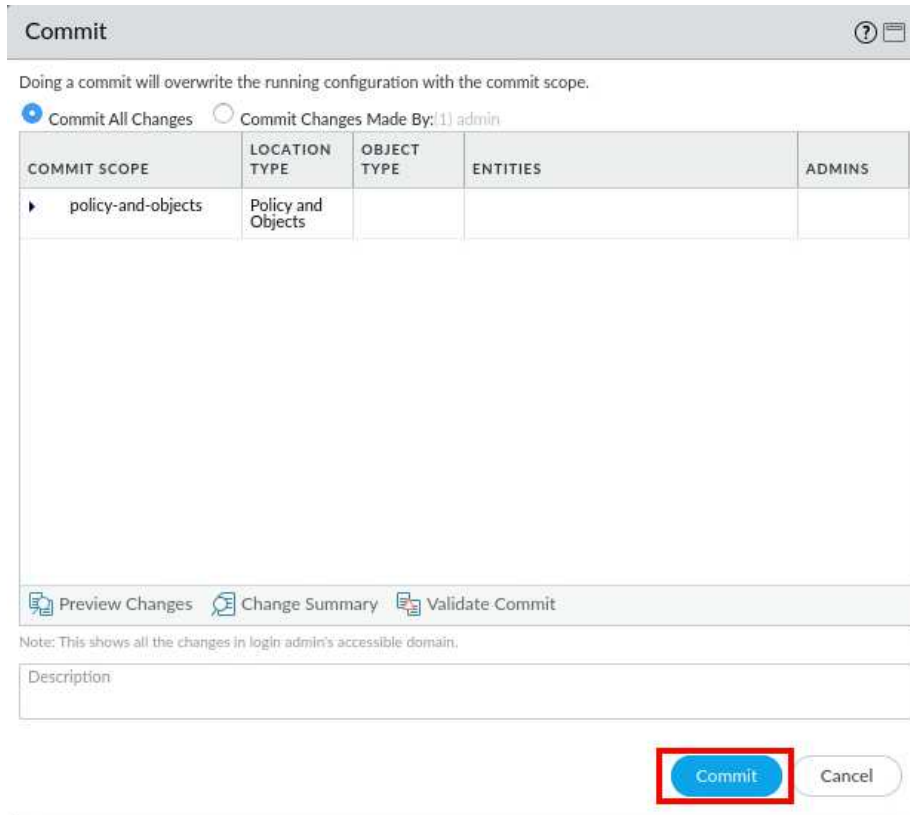


If the “Deny-All-Others” rule does not appear at the bottom of the ruleset, use the Move Down button to place the rule just above the “intrazone-default” rule.

8. Click the **Commit** link located at the top-right of the web interface.



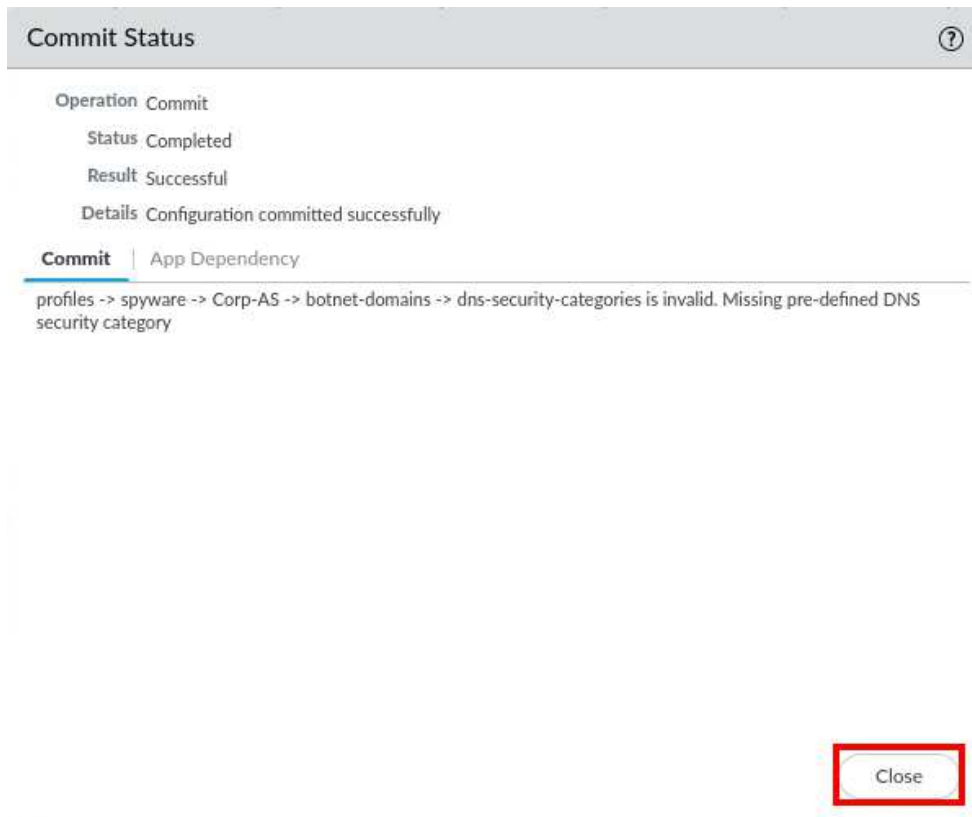
9. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the 'Commit' window. At the top, it says 'Doing a commit will overwrite the running configuration with the commit scope.' Below this are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: 1) admin'. A table follows with columns: COMMIT SCOPE, LOCATION TYPE, OBJECT TYPE, ENTITIES, and ADMINS. The first row shows 'policy-and-objects' under COMMIT SCOPE and 'Policy and Objects' under LOCATION TYPE. Below the table are three buttons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. A note states: 'Note: This shows all the changes in login admin's accessible domain.' Below the note is a 'Description' text area. At the bottom right, there are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
policy-and-objects	Policy and Objects			

10. When the commit operation successfully completes, click **Close** to continue.



The screenshot shows the 'Commit Status' window. It displays the following information: Operation: Commit, Status: Completed, Result: Successful, Details: Configuration committed successfully. Below this is a tabbed interface with 'Commit' selected and 'App Dependency' as an option. Under the 'Commit' tab, there is a message: 'profiles -> spyware -> Corp-AS -> botnet-domains -> dns-security-categories is invalid. Missing pre-defined DNS security category'. At the bottom right, there is a 'Close' button (highlighted with a red box).

11. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



## 2.8 Generate Traffic from the Acquisition Zone

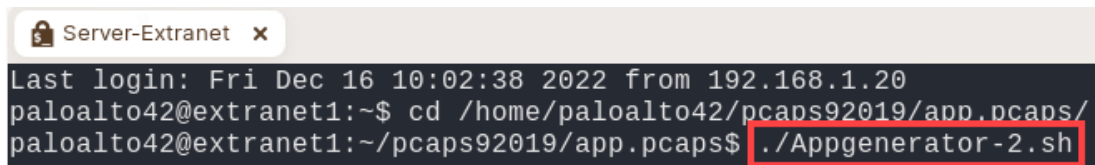
In this section, you will generate traffic from the Acquisition zone using the Extranet-Server.

1. Open the **Remmina** application by clicking on the **Server-Extranet** tab in the *task bar*.

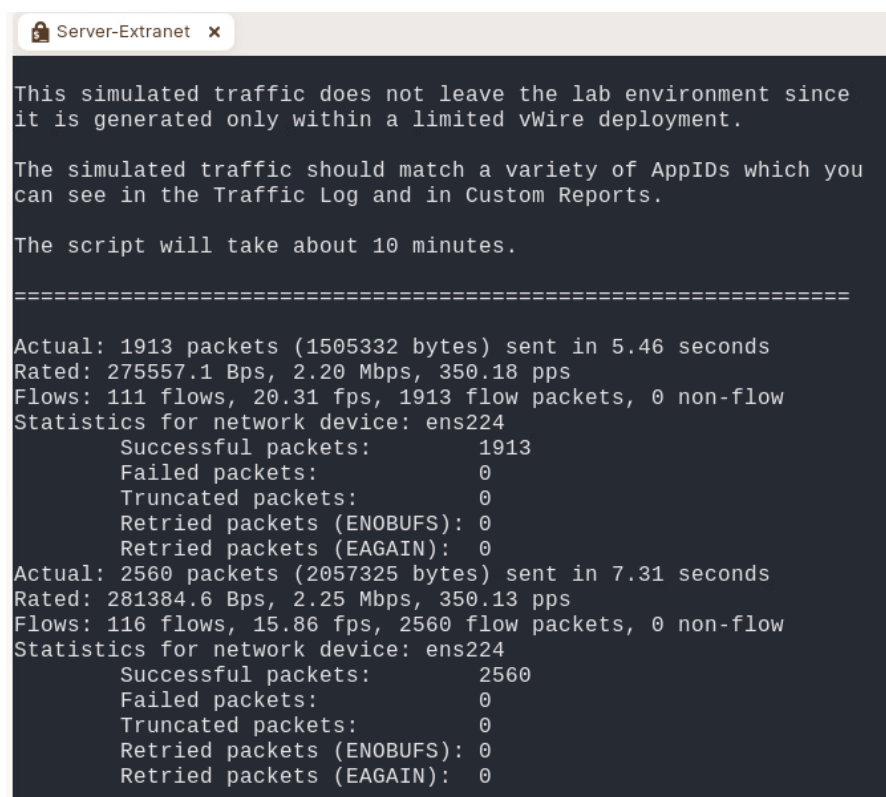


2. Ensure you are still in the **app.pcaps** directory. In the CLI connection enter the following command.

```
paloalto42@extranet1:~/pcaps92019/app.pcaps$ ./Appgenerator-2.sh
```

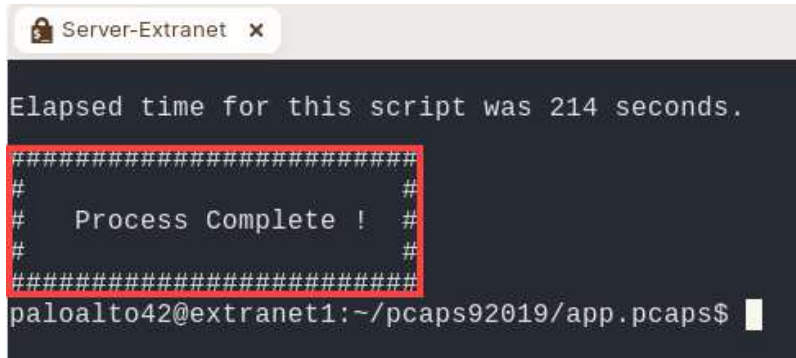


3. Verify the **Appgenerator-2** script is running.





Allow the *Appgenerator-2* script to complete before continuing to the next task.



```

Server-Extranet x
Elapsed time for this script was 214 seconds.
#####
# Process Complete ! #
#####
paloalto42@extranet1:~/pcaps92019/app.pcaps$

```

4. Close the **Server-Extranet** connection by clicking the **X** icon.



5. Re-open the *PA-VM firewall* web interface by clicking on the **Firefox** icon in the task bar.

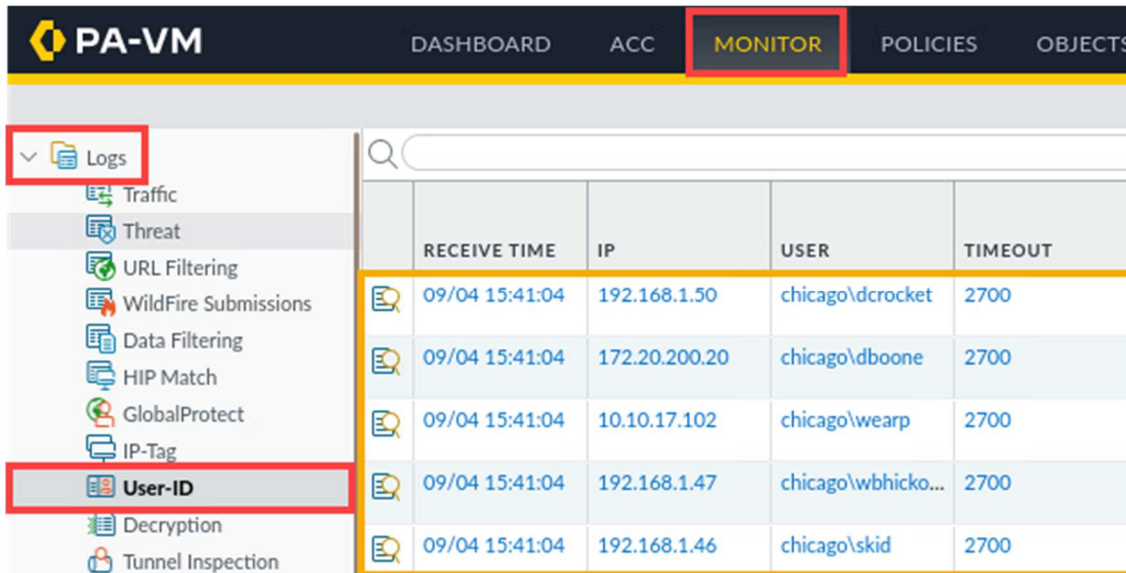


6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 2.9 Exam User-ID Logs

You can see information about User-ID through the firewall CLI or in the web interface. In this section, you will use both tools to examine User-ID entries.

1. Select **Monitor > Logs > User-ID**. The firewall should have numerous entries with *username-to-ip-address* mappings. If the *User* mappings are not showing, repeat **Task 2.8**.

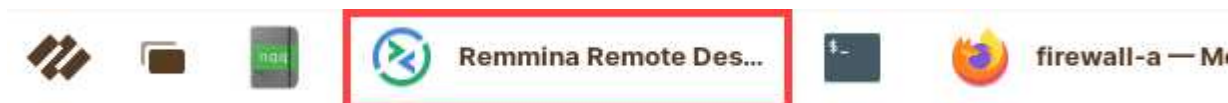


	RECEIVE TIME	IP	USER	TIMEOUT
	09/04 15:41:04	192.168.1.50	chicago\dcrocket	2700
	09/04 15:41:04	172.20.200.20	chicago\dboone	2700
	09/04 15:41:04	10.10.17.102	chicago\wearp	2700
	09/04 15:41:04	192.168.1.47	chicago\wbhicko...	2700
	09/04 15:41:04	192.168.1.46	chicago\skid	2700

2. Minimize the PA-VM firewall by clicking minimize in the upper right of the web interface and continue to the next task.



3. On the *client* desktop, in the *task bar*, re-open the **Remmina** application.



4. Double-click the entry for **Firewall-A**.



Name	Group	Server	Plugin	Last used
Berlin-Client		192.168.1.25	SSH	2022-11-21 - 09:01:12
Firewall-A		192.168.1.254	SSH	2022-12-16 - 07:51:14
Firewall-B		192.168.1.253	SSH	2022-11-21 - 08:51:34
Panorama		192.168.1.252	SSH	2022-12-14 - 10:34:19
Server-Extranet		192.168.50.10	SSH	2023-12-11 - 21:28:43

**Please Note**

The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.



- In the firewall CLI, enter the following command to display entries for *User-ID*. Examine the *User-ID* information.

```
admin@firewall-a> show user ip-user-mapping all <Enter>
```

```
admin@firewall-a> show user ip-user-mapping all
```

IP MaxTimeout(s)	Vsys	From	User	IdleTimeout(s)
10.10.24.102 2134	vsys1	XMLAPI	chicago\jcaesar	2134
192.168.1.9 2134	vsys1	XMLAPI	chicago\nnickleby	2134
10.4.5.101 2134	vsys1	XMLAPI	chicago\tsawyer	2134
192.168.1.104 2134	vsys1	XMLAPI	chicago\mrhyde	2134
192.168.1.22 2134	vsys1	XMLAPI	chicago\hpoirot	2134
192.168.1.43	vsys1	XMLAPI	chicago\jringo	2134

- Close the *Firewall-A* window by clicking the **close** icon.



- Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar and continue to the next task.

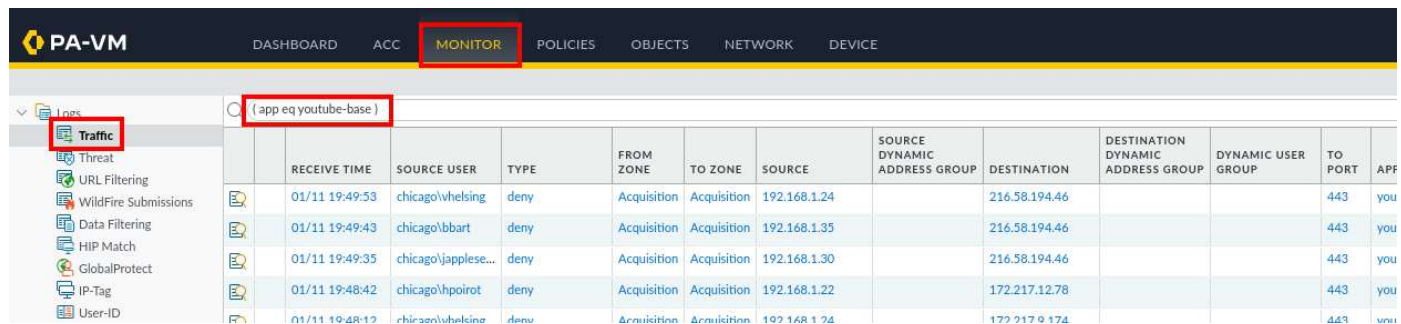


## 2.10 Examine Firewall Traffic Log

Create and apply filters to view rules and users.



1. Select **Monitor > Logs > Traffic**. In the filter builder, type ( **app eq youtube-base** ). Click **Apply Filter**.



	RECEIVE TIME	SOURCE USER	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPL
	01/11 19:49:53	chicago\vhelsing	deny	Acquisition	Acquisition	192.168.1.24		216.58.194.46			443	you
	01/11 19:49:43	chicago\bbart	deny	Acquisition	Acquisition	192.168.1.35		216.58.194.46			443	you
	01/11 19:49:35	chicago\japplese...	deny	Acquisition	Acquisition	192.168.1.30		216.58.194.46			443	you
	01/11 19:48:42	chicago\hpoirot	deny	Acquisition	Acquisition	192.168.1.22		172.217.12.78			443	you
	01/11 19:48:12	chicago\vhelsing	deny	Acquisition	Acquisition	192.168.1.24		172.217.12.78			443	you

- Q1. Which security policy does the firewall use when it encounters youtube-base traffic?
- a. Allow-Corp-Apps
  - b. Allow-PANW-Apps
  - c. Block-from-Known Sources
  - d. Deny-All-Others

2. Clear the filter and in the filter builder, type ( **app eq dns** ). Click **Apply Filter**.



	RECEIVE TIME	SOURCE USER	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPL
	01/11 20:03:32		end	Users_Net	Internet	192.168.1.254		8.8.8.8			53	dns-b
	01/11 20:03:32		end	Users_Net	Internet	192.168.1.254		8.8.8.8			53	dns-b
	01/11 20:03:32		end	Users_Net	Internet	192.168.1.254		8.8.8.8			53	dns-b
	01/11 20:03:27		end	Users_Net	Internet	192.168.1.254		8.8.8.8			53	dns-b

- Q2. Which security policy does the firewall use when it encounters dns traffic?
- a. Allow-Corp-Apps
  - b. Users\_to\_Internet
  - c. Block-from-Known Sources
  - d. Deny-All-Others

3. Clear the filter and in the filter builder, type ( **app eq facebook-base** ). Click **Apply Filter**.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE USER	SOURCE	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION
	09/04 15:41:08	deny	Acquisition	Acquisition	chicago\bbart	192.168.1.35		31.13.70.36			443	facebook-base	reset-both
	09/04 15:37:04	deny	Acquisition	Acquisition	chicago\bbart	192.168.1.35		31.13.70.36			443	facebook-base	reset-both
	09/04 15:37:04	deny	Acquisition	Acquisition	chicago\jappleseed	192.168.1.30		31.13.70.36			443	facebook-base	reset-both
	09/04 15:37:04	deny	Acquisition	Acquisition	chicago\jappleseed	192.168.1.30		31.13.70.36			443	facebook-base	reset-both

- Q3. Which security policy does the firewall use when it encounters facebook-base traffic? Choose all that apply.
- a. Allow-Corp-Apps
  - b. Allow-PANW-Apps

- c. Allow-Mktg-Apps
- d. Deny-All-Others

4. In the filter builder, type ( **app eq facebook-base** ) and ( **action eq allow** ). Click **Apply Filter**.

(( app eq facebook-base ) and ( action eq allow ))													→	×	+	📄	📄	?
								S...		DES		TO						
								D...		D...								
								A...		A...								
								GRG		GRG								

Q4. Which users are allowed access to facebook-base?

- a. No Users are allowed to access Facebook.
- b. chicago\hpoirot
- c. chicago\sholmes
- d. chicago\vhelsing

5. Clear the filter and in the filter builder, type ( **app eq instagram-base** ) and ( **user.src eq 'chicago\sholmes'** ). Click **Apply Filter**.

( app eq instagram-base ) and ( user.src eq 'chicago\sholmes' )						
	RECEIVE TIME	SOURCE USER	TYPE	FROM ZONE	TO ZONE	SO

Q5. Is the user sholmes allowed to access instagram-base?

- a. Yes
- b. No

6. Clear the filter and in the filter builder, type ( **app eq instagram-base** ) and ( **user.src eq 'chicago\bbart'** ). Click **Apply Filter**.

( app eq instagram-base ) and ( user.src eq 'chicago\bbart' )							
	RECEIVE TIME	SOURCE USER	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE DYNAMIC ADDRESS GR

Q6. Is the user bbart allowed to access instagram-base?

- a. Yes
- b. No

7. The lab is now complete; you may end your reservation.