PALO ALTO NETWORKS EDU 210

Lab 11: Blocking Threats with User-ID

Document Version: 2022-07-18

Contents

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 vWire 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.)

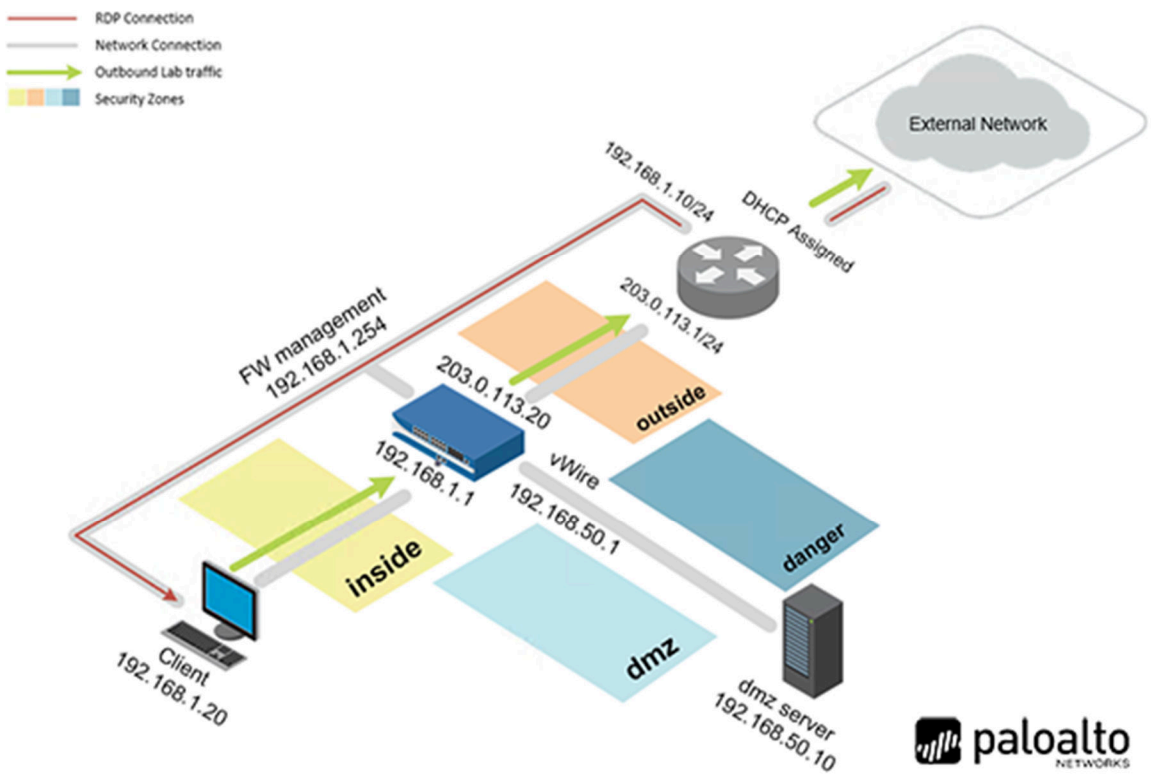
In this lab, you will create a security policy rule that explicitly denies any other traffic generated by users in the Acquisition zone. Although the interzone-default rule will deny any traffic not expressly allowed, the creation of an explicit deny rule will allow you to examine the kinds of applications users in the Acquisition zone are attempting to access.

Objective

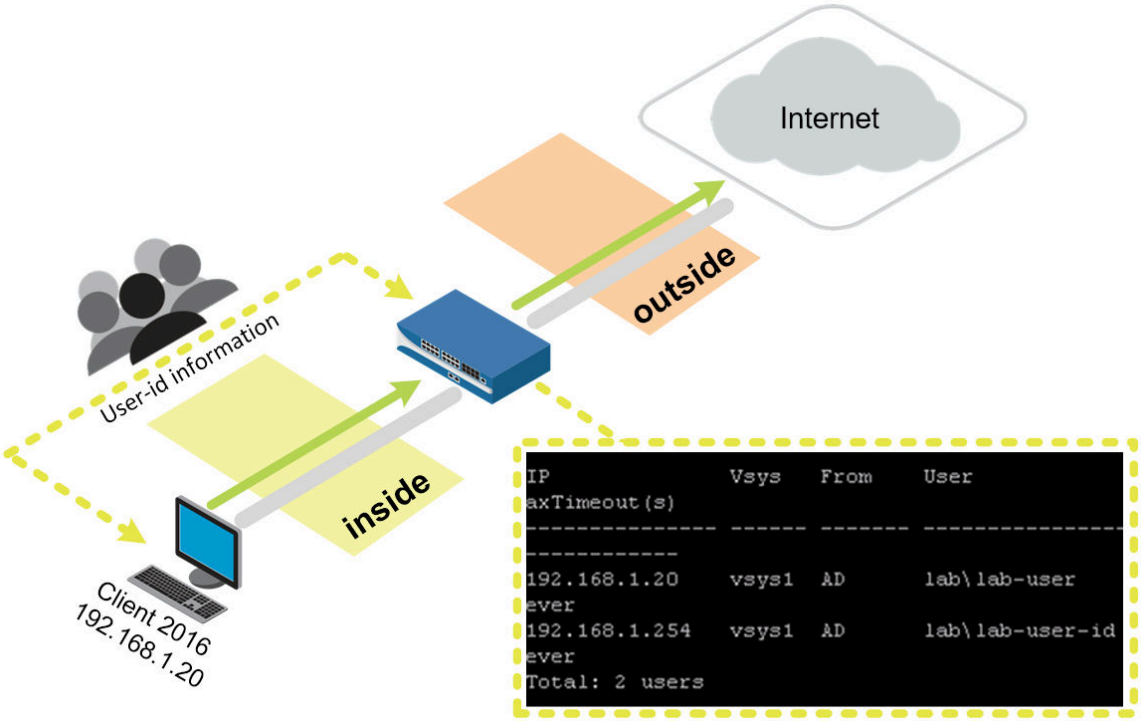
In this lab, you will perform the following tasks:

- Examine current configuration
- Enable User-ID technology on 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 to complete the lab. The task sections below provide details on the use of this information.

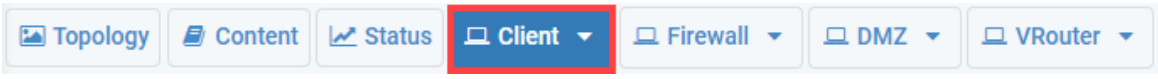
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Blocking Threats with User-ID

1.1 Apply a Baseline Configuration to the Firewall

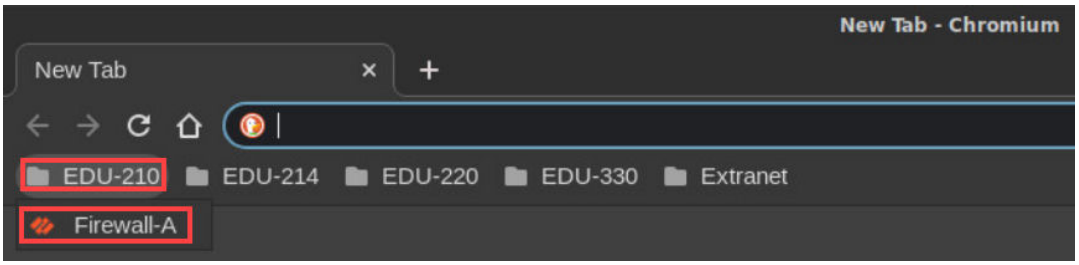
In this section, you will load the Firewall configuration file.

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

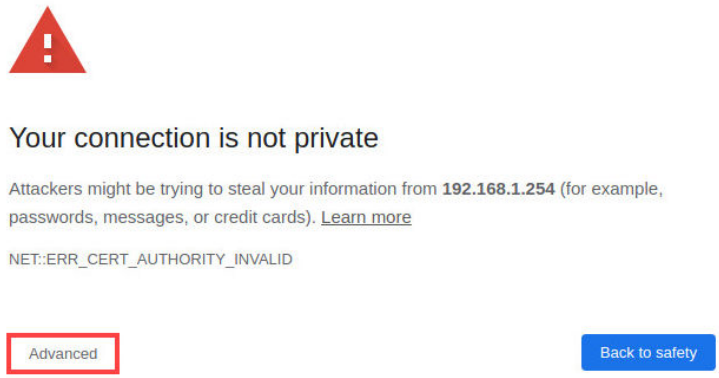


2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

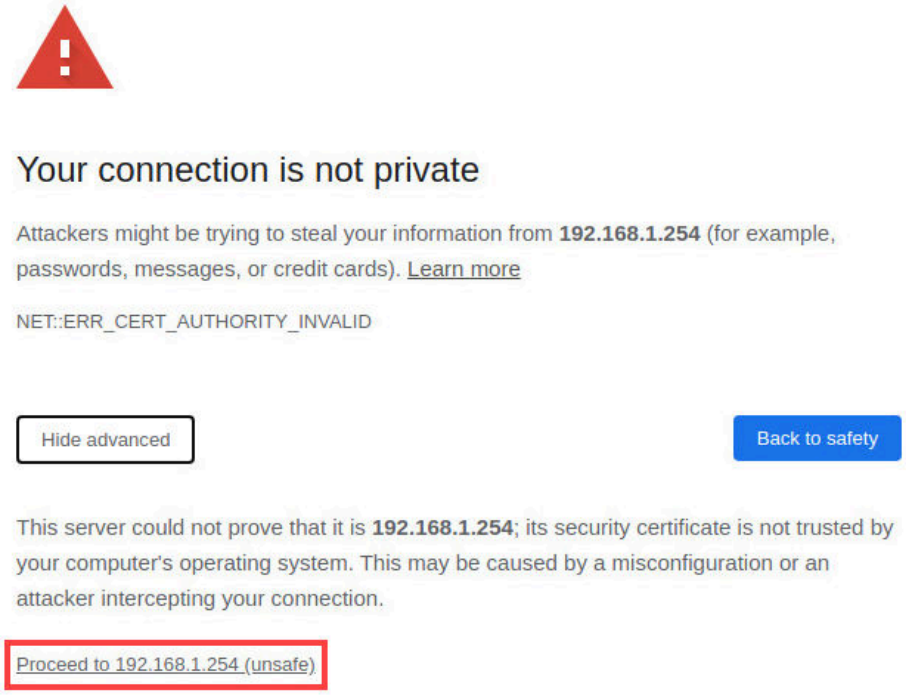


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



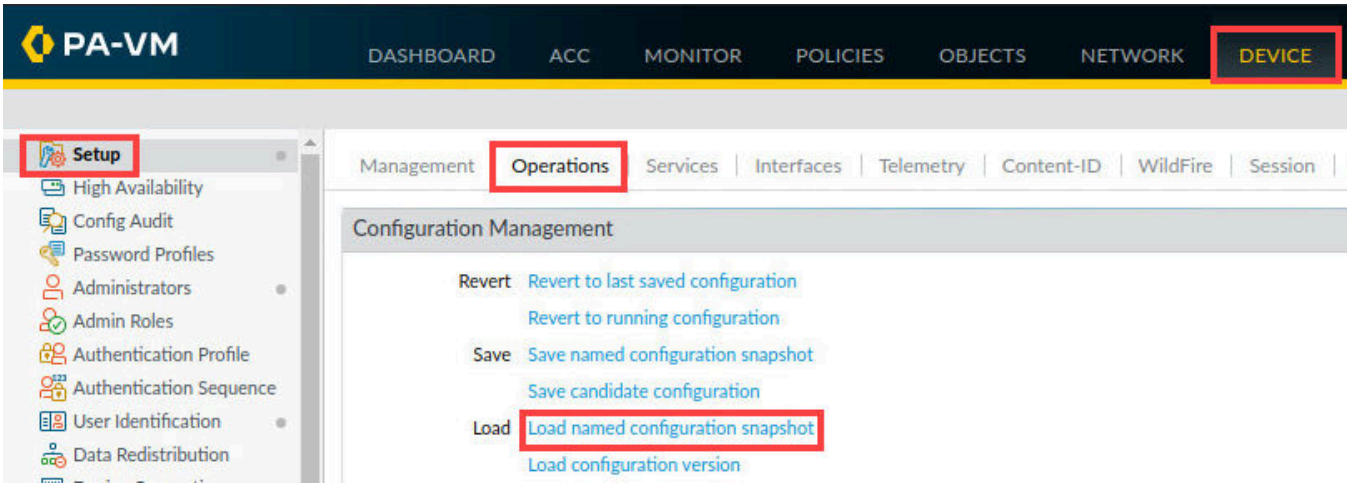
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

5. Click on **Proceed to 192.168.1.254 (unsafe)**.

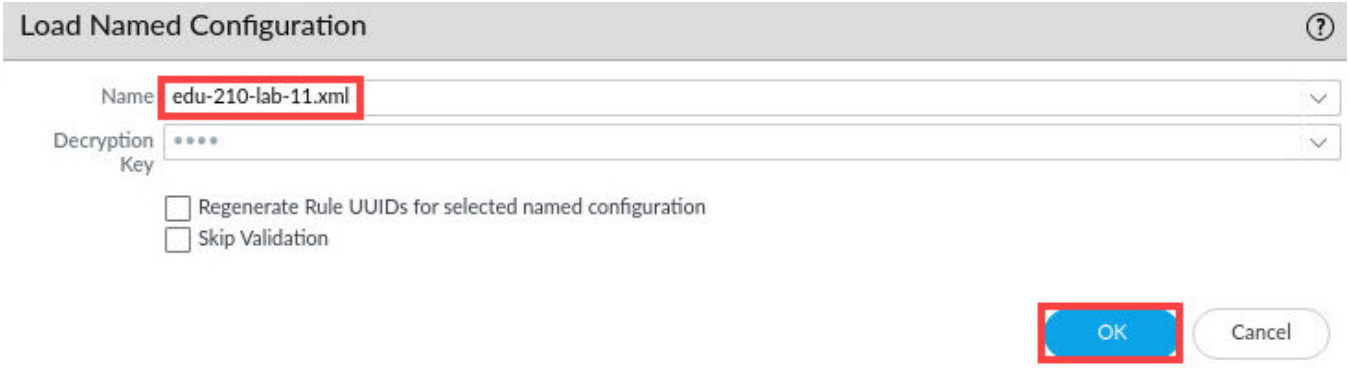


6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

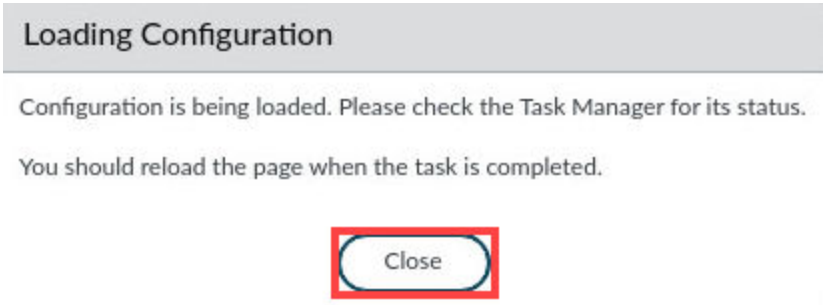
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



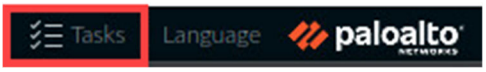
8. In the *Load Named Configuration* window, select **edu-210-lab-11.xml** from the *Name* dropdown box and click **OK**.



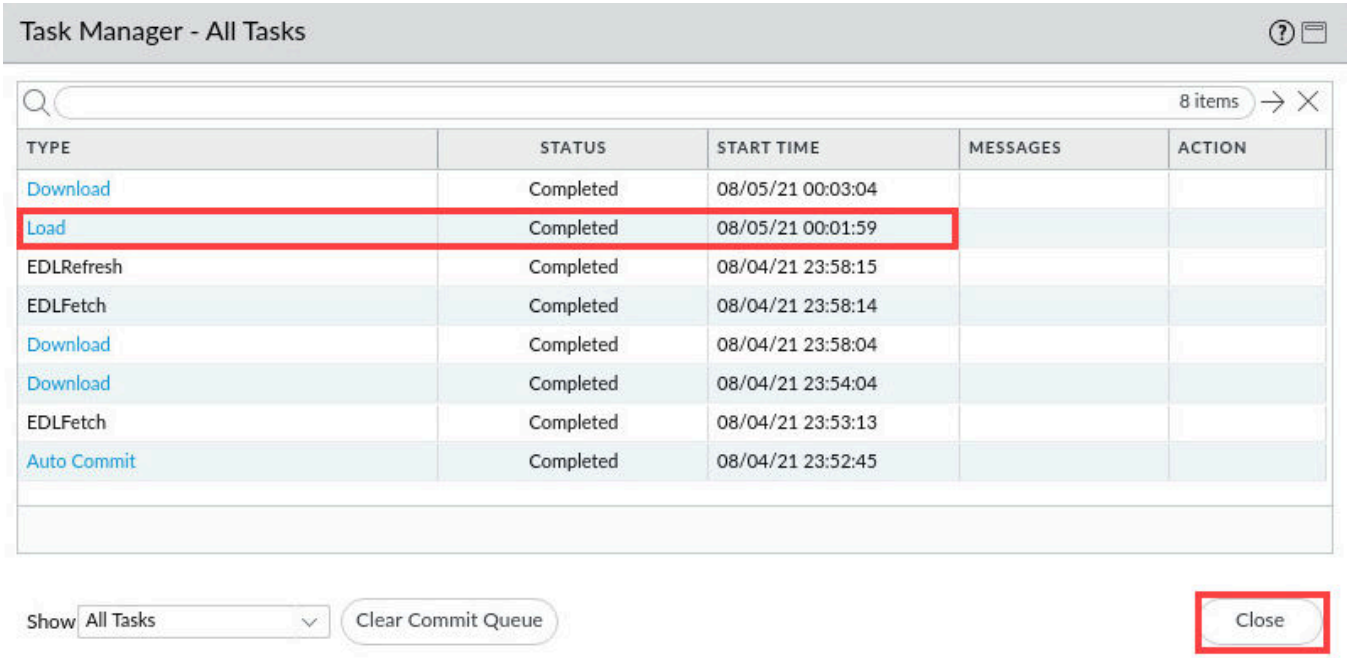
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



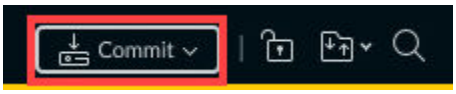
10. Click the **Tasks** icon located at the bottom-right of the web interface.



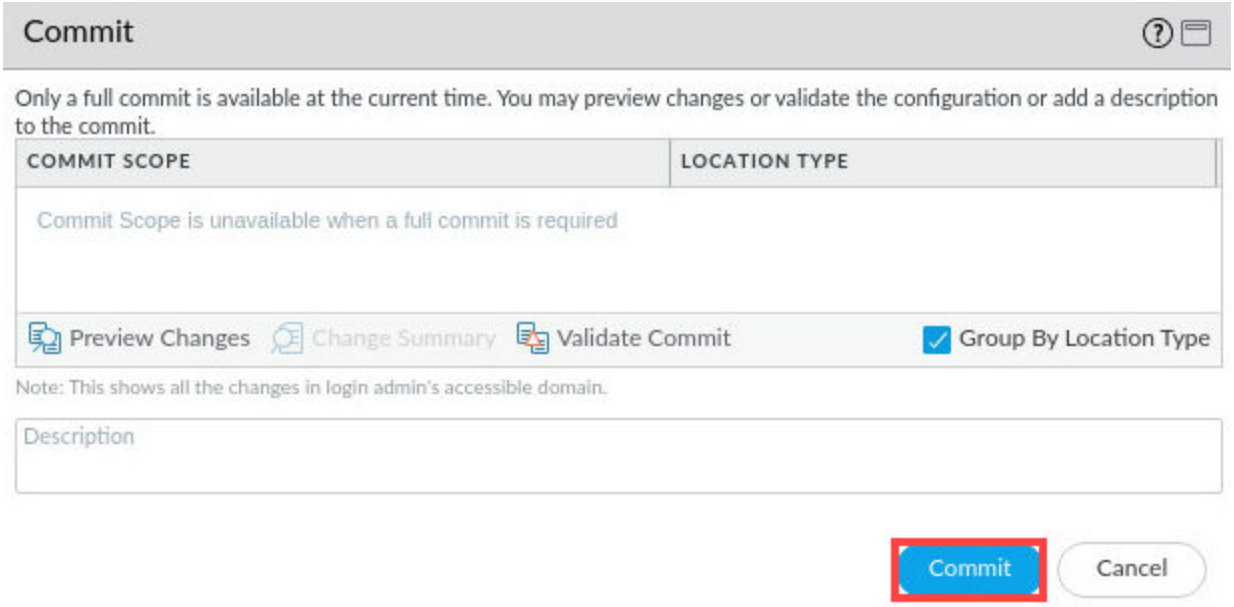
11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



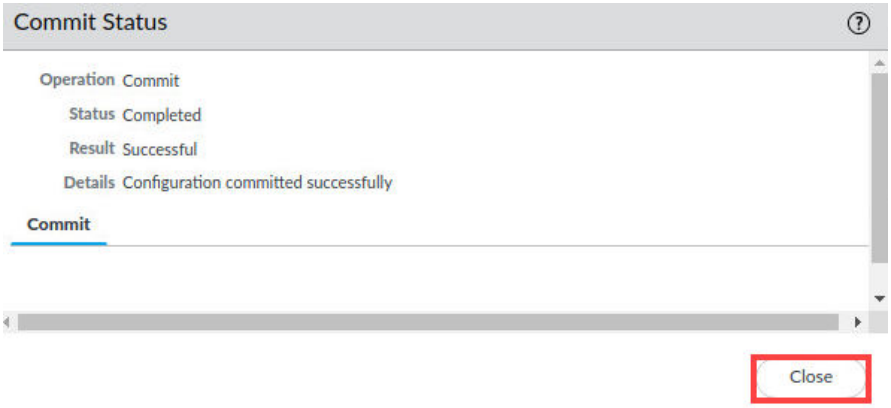
12. Click the **Commit** link located at the top-right of the web interface.



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



14. When the *Commit* operation successfully completes, click **Close** to continue.



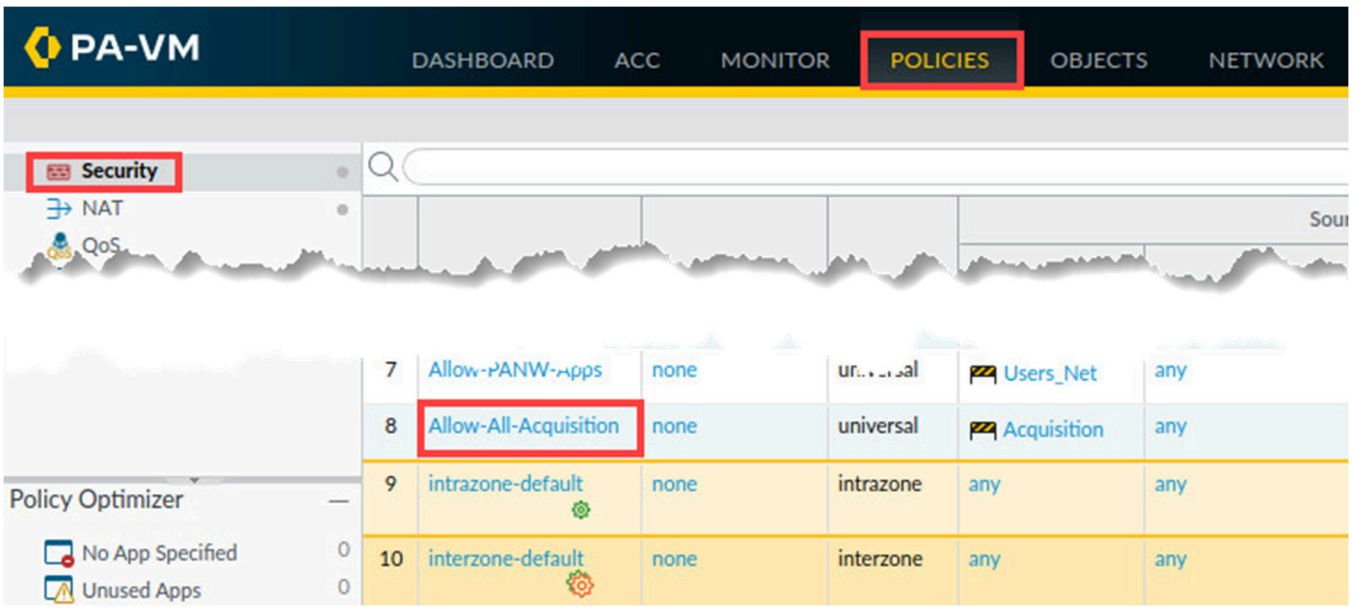
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

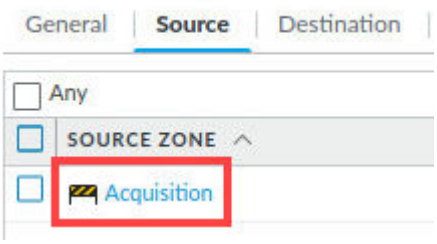
1.2 Examine Firewall Configuration

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

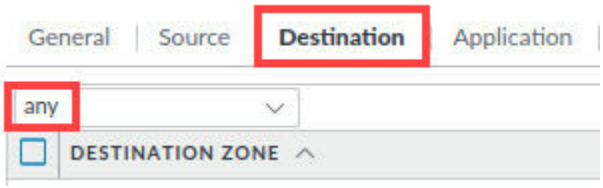
1. Select **Policies > Security**. Click the **Allow-All-Acquisition** policy.



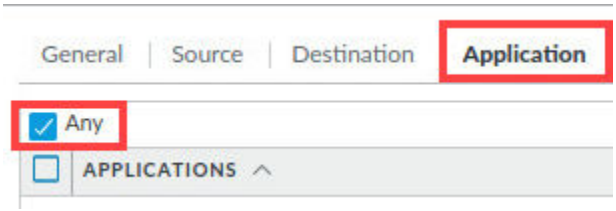
2. In the *Security Policy Rule*, select the **Source** tab. Note that the *Source Zone* is set to **Acquisition**.



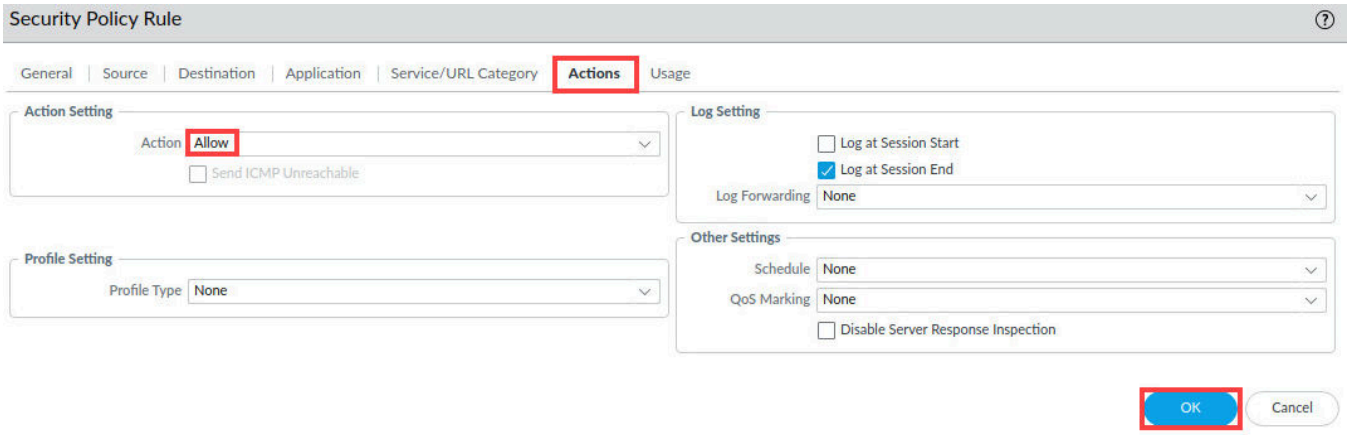
3. Select the **Destination** tab. Note that the *Destination Zone* is set to **any**.



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**.



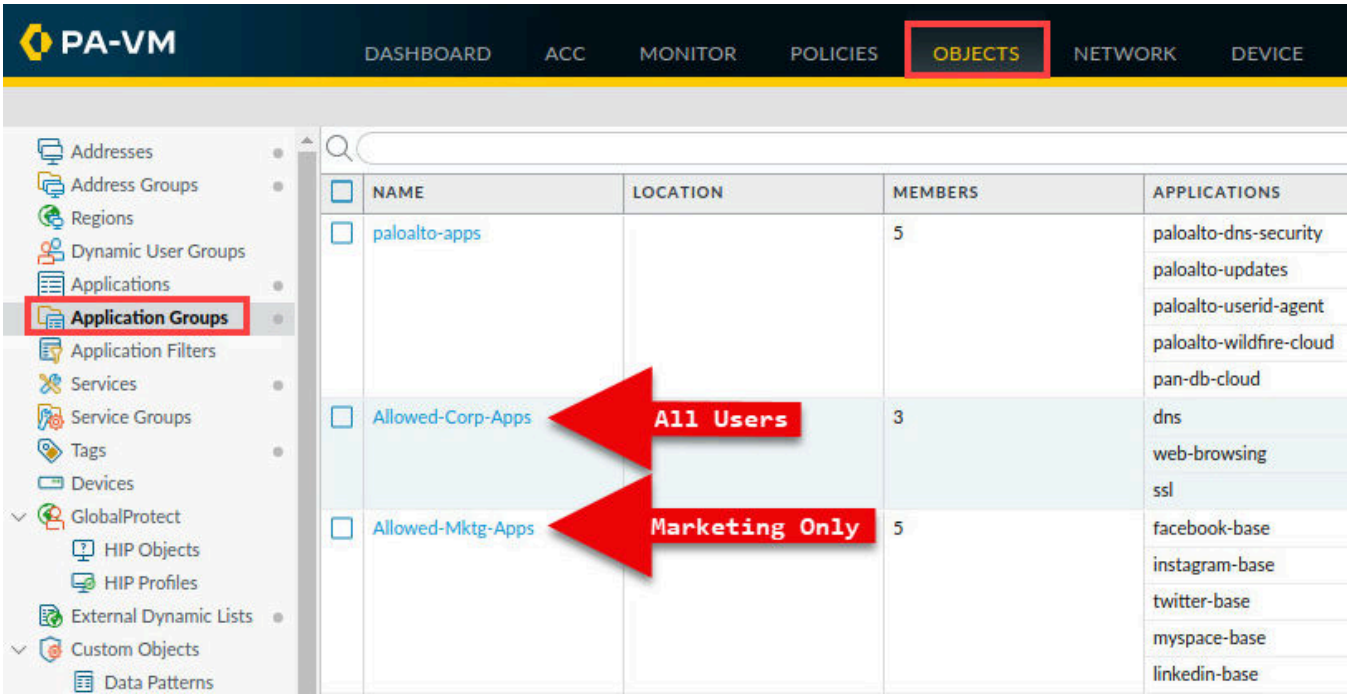
Please Note

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.**



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.

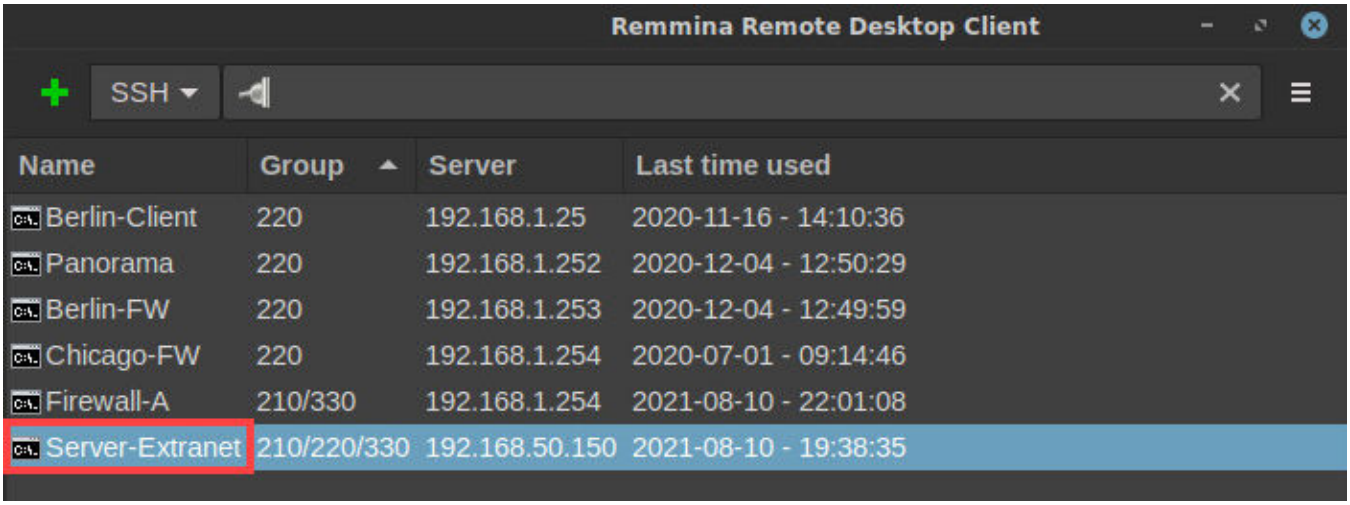
9. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 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.

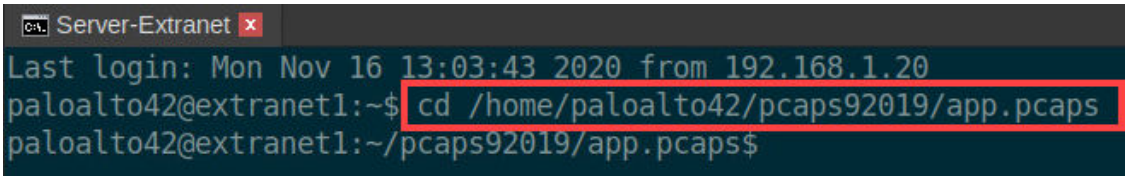
1. On the *client desktop*, open the **Remmina** application.

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



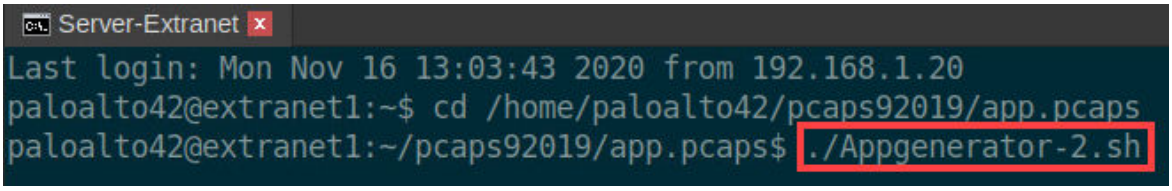
3. In the CLI connection, enter the following command.

```
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.

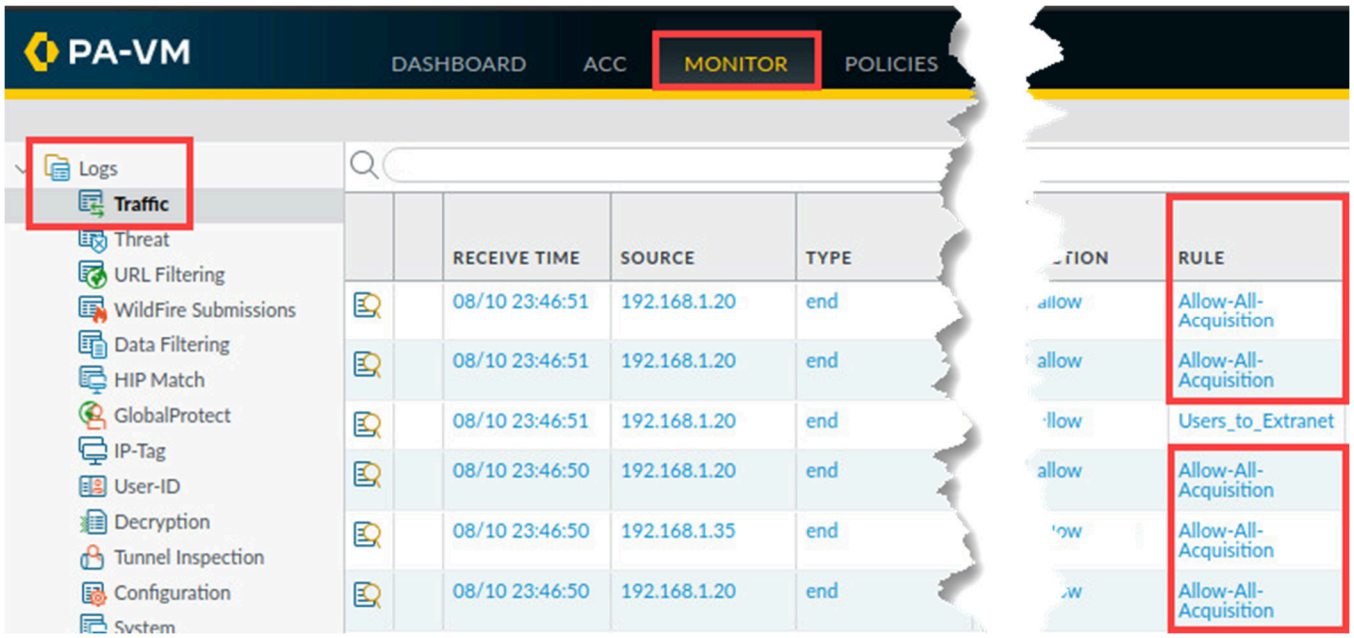
```
processing file: pcap9-5.g.pcapng
Actual: 3368 packets (3048202 bytes) sent in 10.36 seconds.          Rated: 294228.0 bps, 2.24 Mbps, 325.10 pps
Statistics for network device: ens224
        Attempted packets:         3368
        Successful packets:        3368
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
sending out ens224
processing file: pcap9-5.h.pcapng
Actual: 6131 packets (6552730 bytes) sent in 19.33 seconds.          Rated: 338992.8 bps, 2.59 Mbps, 317.18 pps
Statistics for network device: ens224
        Attempted packets:         6131
        Successful packets:        6131
        Failed packets:            0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
sending out ens224
```

STOP

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

6. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

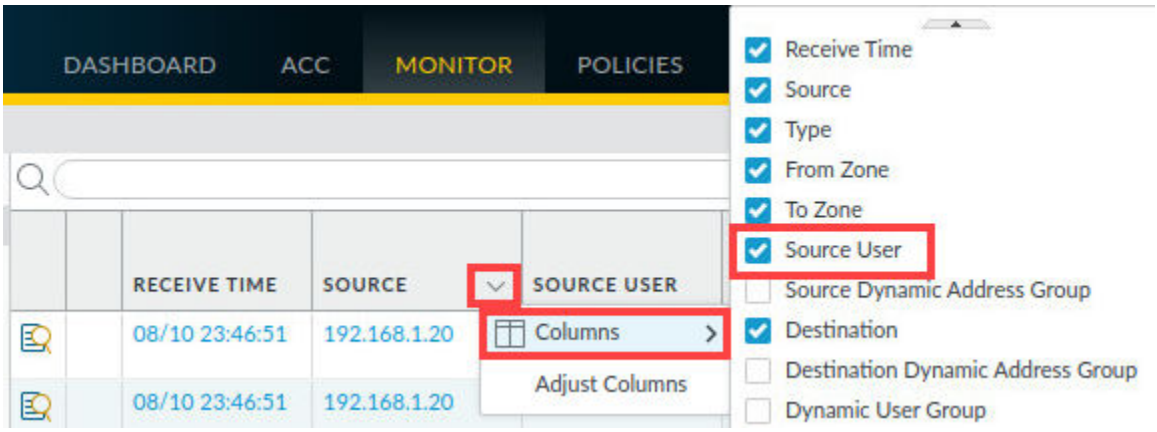
7. Select **Monitor > Logs > Traffic**. Clear any filters in place. Note that almost all traffic is hitting the **Allow-All-Acquisition Rule**. Please allow the firewall 3 to 6 minutes for the traffic logs to update.



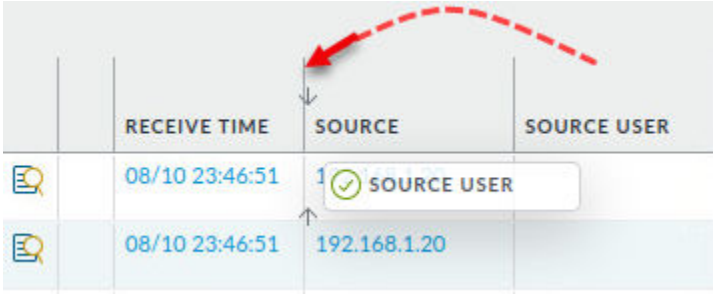
Please Note

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**.



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



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

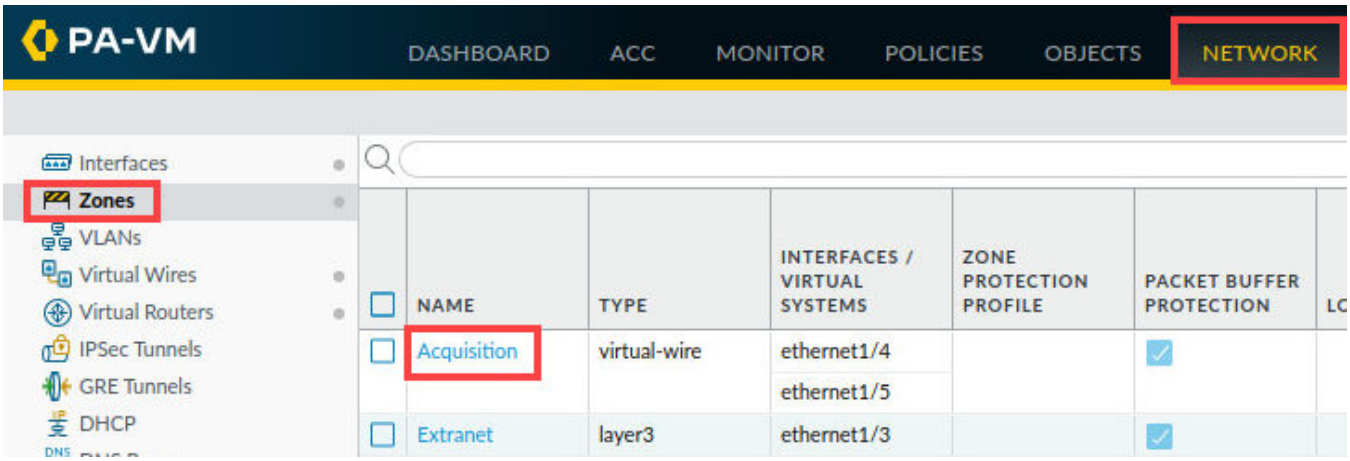
> **Please Note** This action will make it easier for you to locate Source User information later in this lab.

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

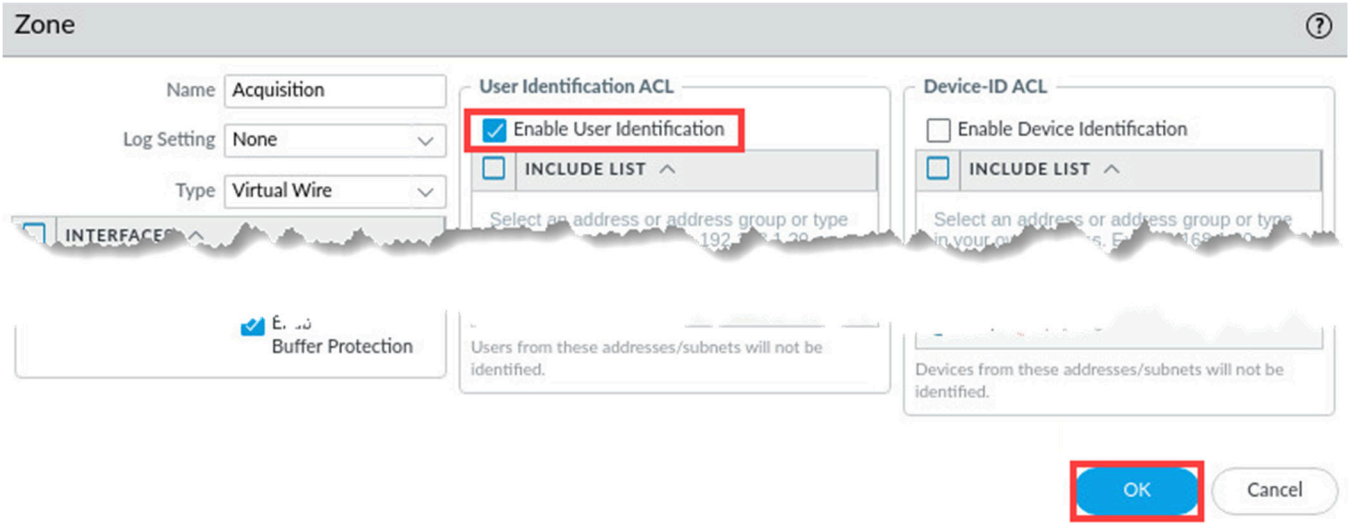
1.4 Enable User-ID on the Acquisition Zone

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.

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



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

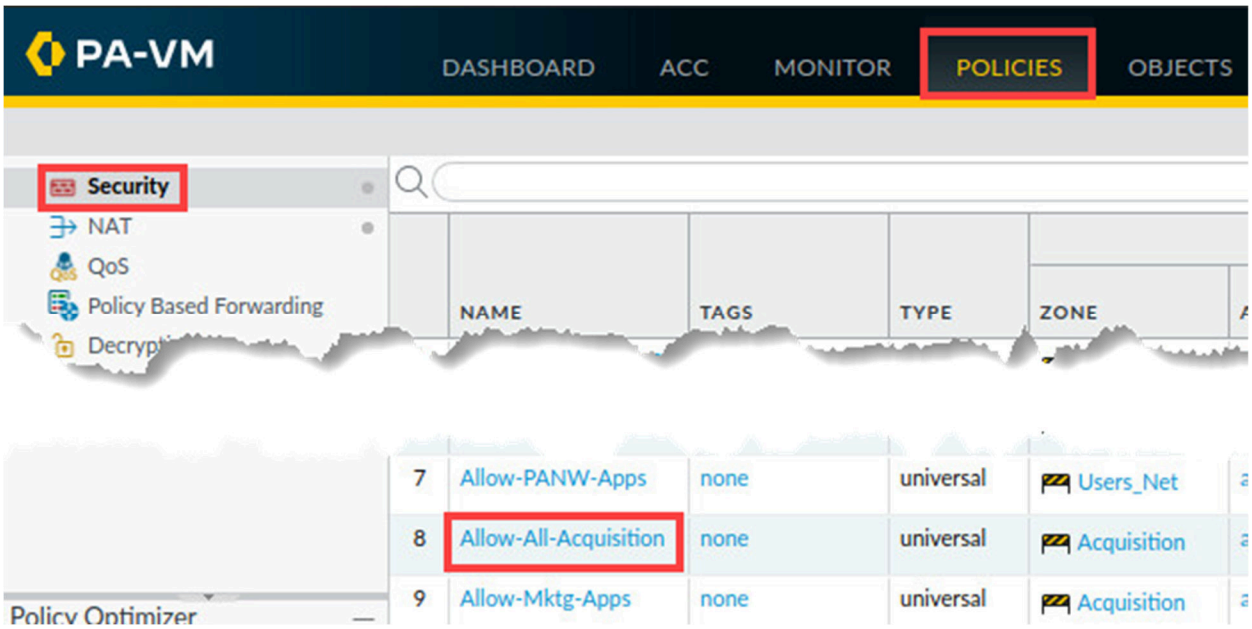


3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.5 Modify the Allow-All-Acquisition Zone

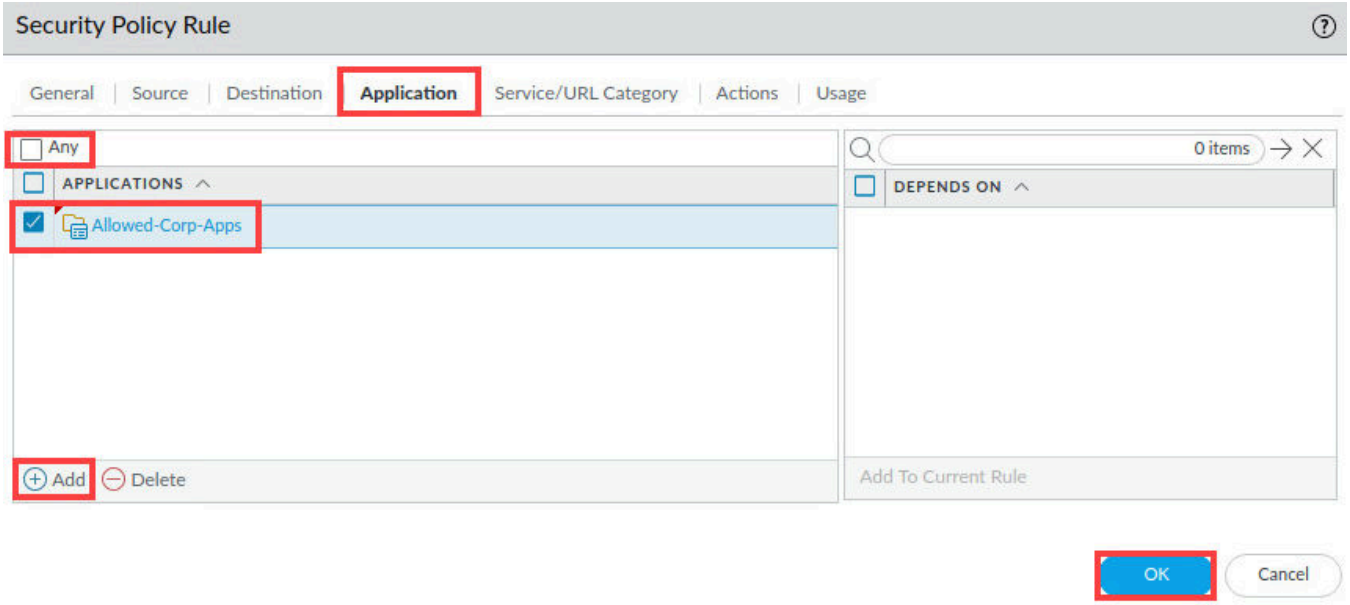
In this section, you will now change the set of applications that Acquisition users are allowed to access by modifying the existing **Allow-All-Acquisition** rule.

1. Select **Policies > Security**. Click **Allow-All-Acquisition**.



2. 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`**.

3. 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**.

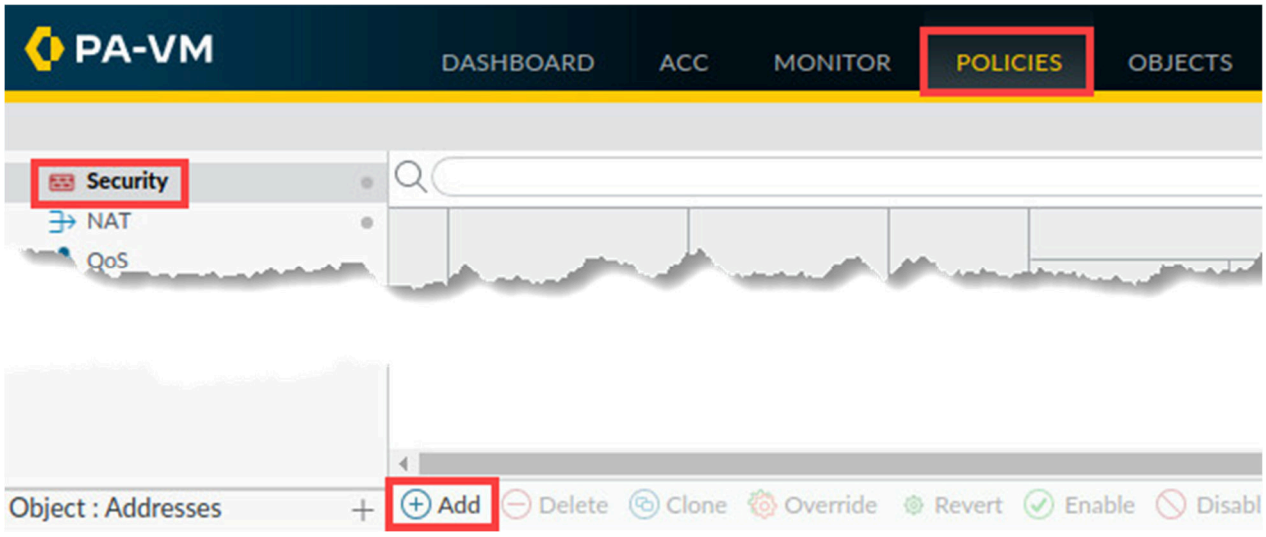


4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

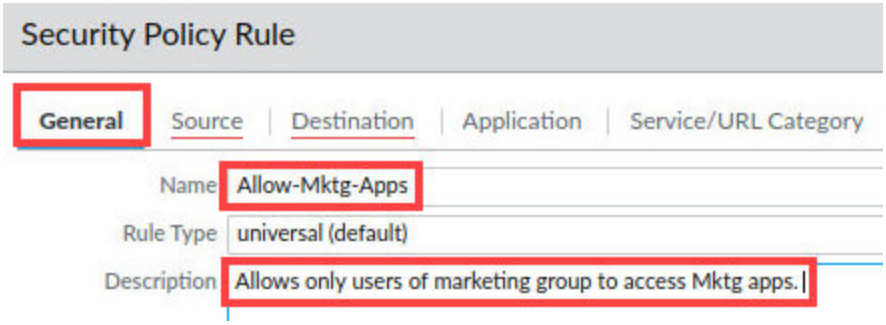
1.6 Create Marketing Apps Rule

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

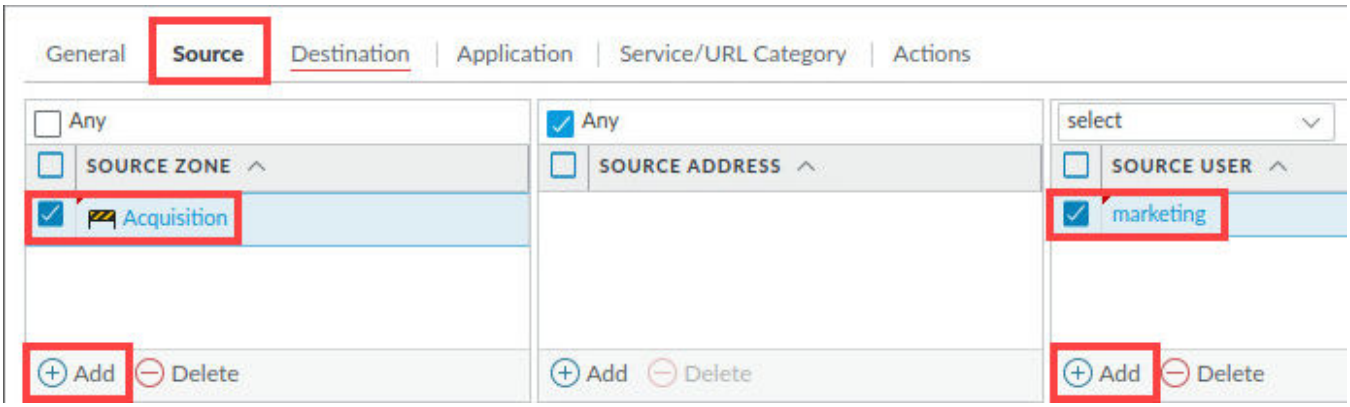
1. Select **Policies > Security**. Click **Add**.



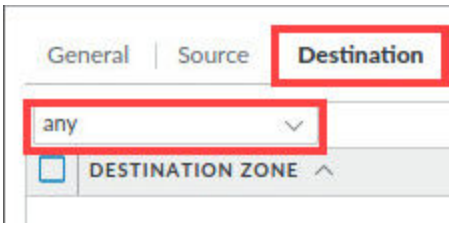
2. In the *Security Policy Rule* window, under the *General* tab, enter **`Allow-Mktg-Apps`** for the *Name*. For *Description*, enter **`Allows only users of marketing group to access Mktg apps`**.



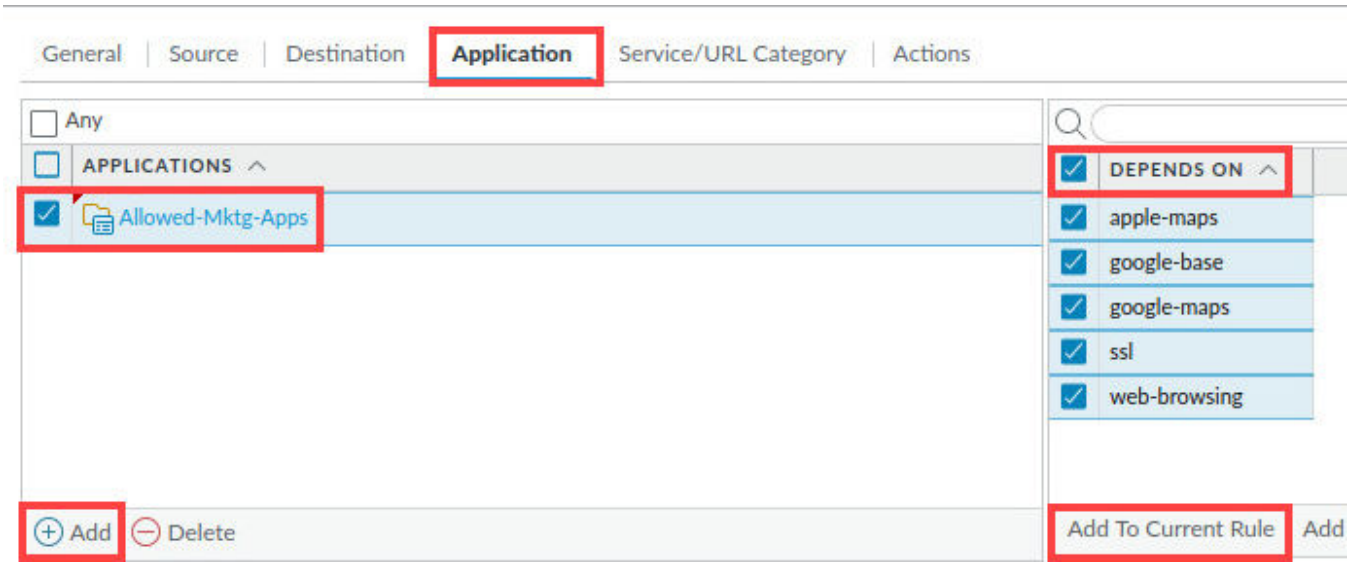
3. Select the **Source** tab, under *Source Zone*, click **Add.** Select **Acquisition**. Under the *Source User* column, click **Add** and enter **`marketing`**.



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

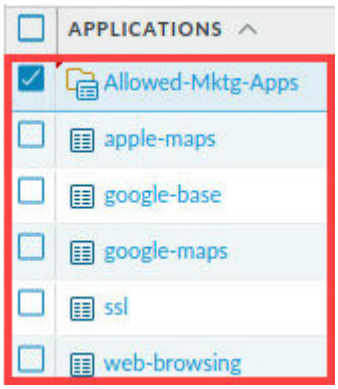


5. Select the **Application** tab and u*ncheck* the option for **Any**. Click **Add** and enter the first few letters of the **Allowed-Mktg-App**s to display the *Application Groups* available. Select **Allowed-Mktg-Apps**. On the right side of the *Application* window, place a **check** in the checkbox beside **DEPENDS ON.** Click **Add to Current Rule**.

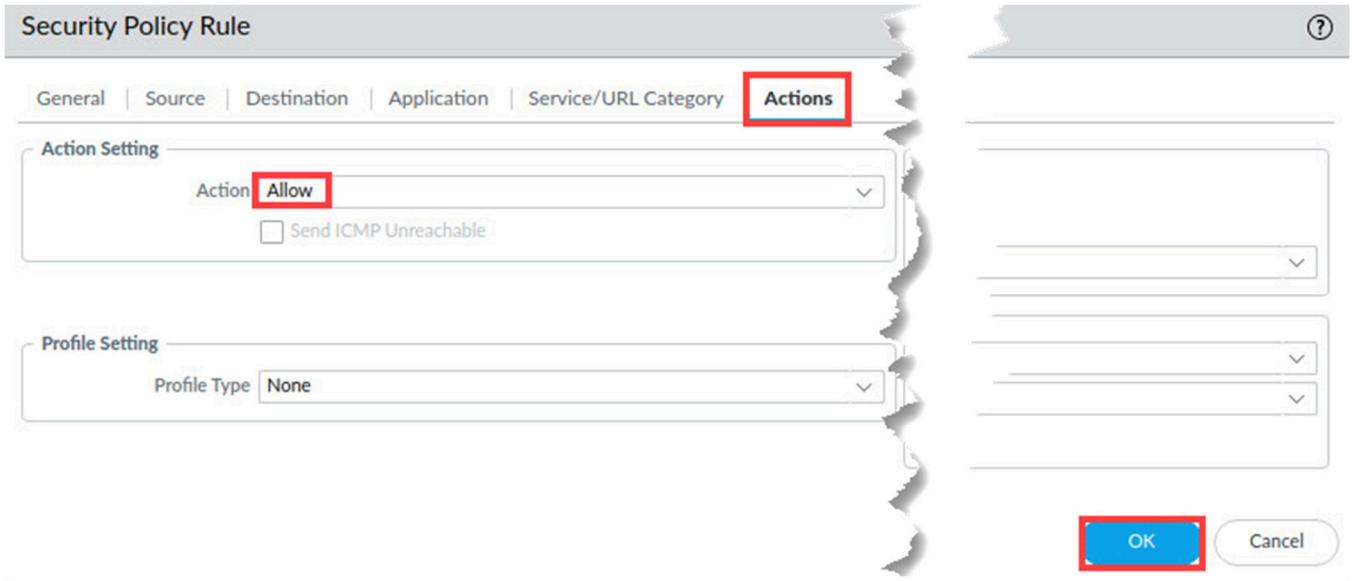


Please Note This action will select all the individual applications under the DEPENDS ON column.

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

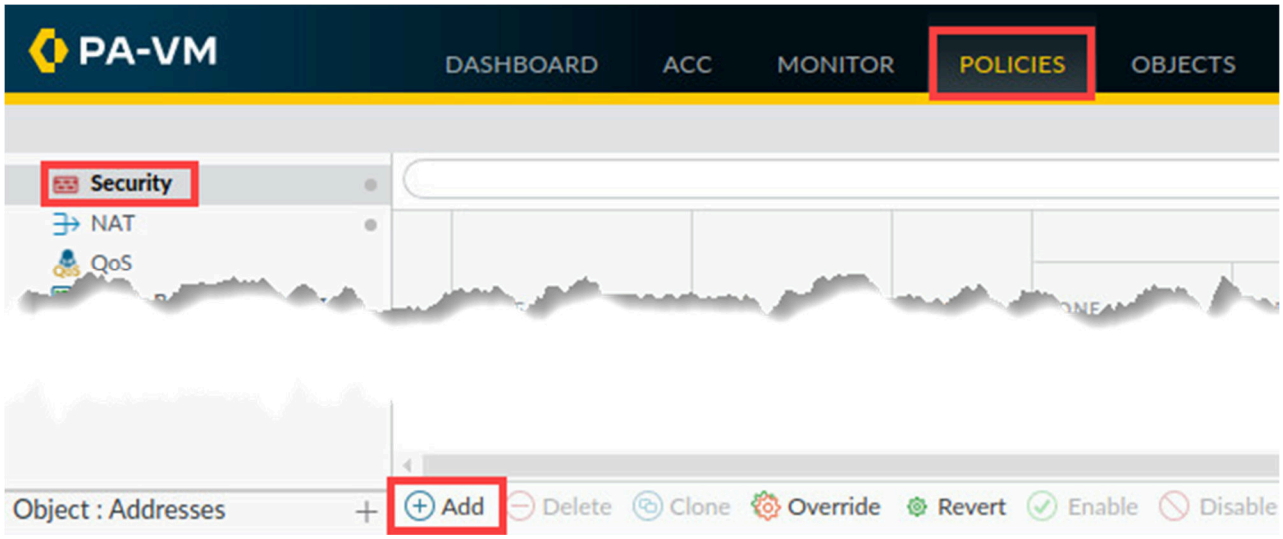
When you create a new Security policy rule, the default setting for Action is Allow. However, it is always a good practice to verify this setting before closing the window.

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

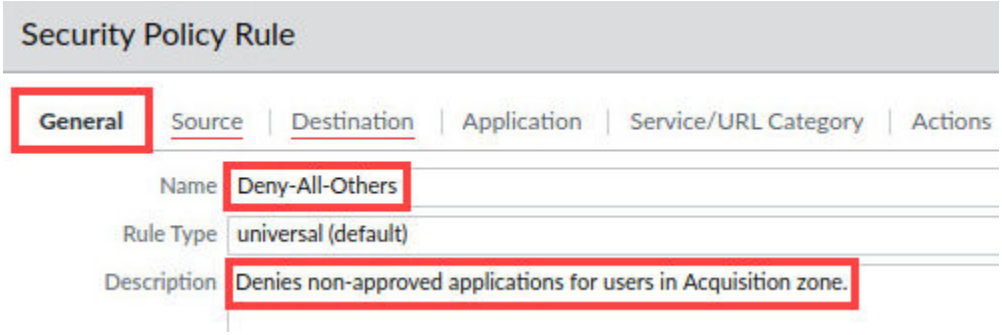
1.7 Create Deny Rule

In this section, you will create a security policy rule that allows hosts in the Users_Net to access the Custom Application in the Extranet zone.

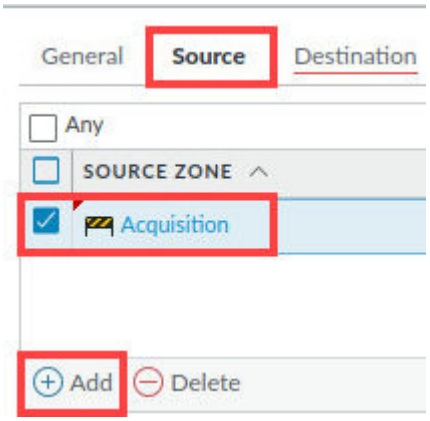
1. Select **Policies > Security**. Click **Add**.



2. 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`**.

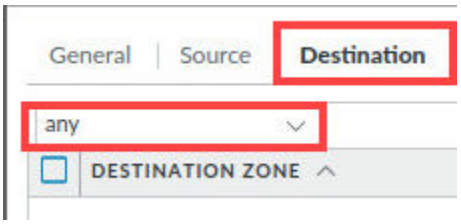


3. Select the tab for **Source,** click **Add,** and select **Acquisition**.

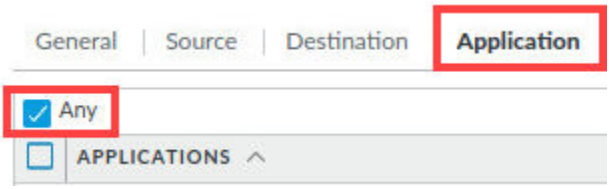


> **Please Note**
> Note that you do not need to specify any users or user groups under the Source User column. Because the dropdown list is set to any, this rule will deny traffic to any user, regardless of group membership.

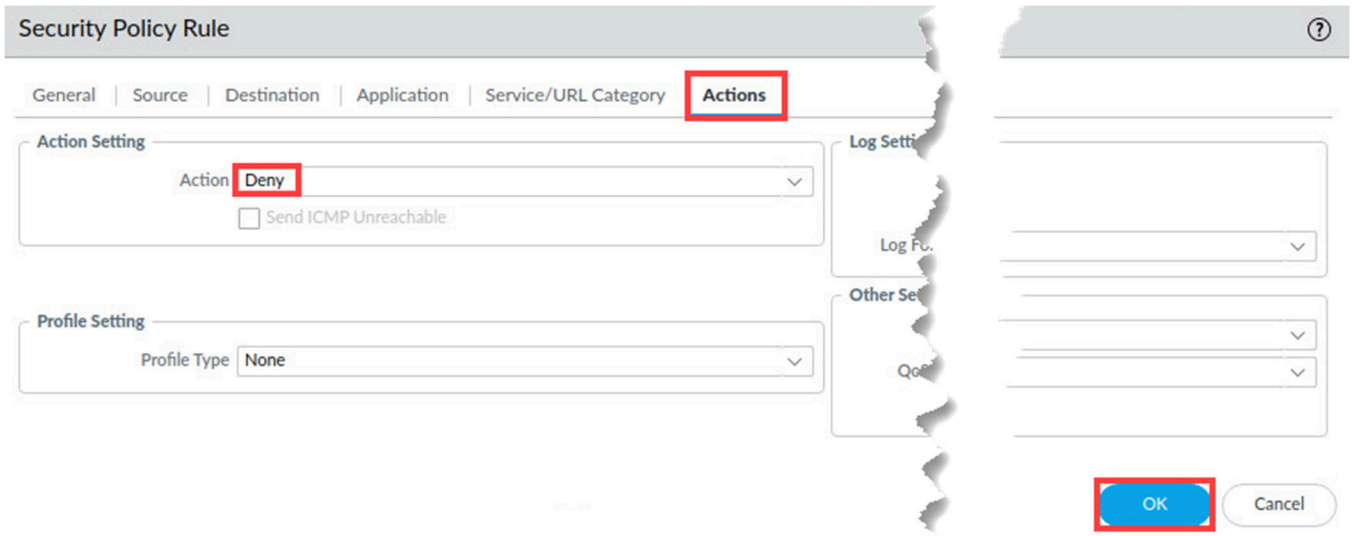
4. Select the tab for **Destination,** use the dropdown list at the top to select **any**.



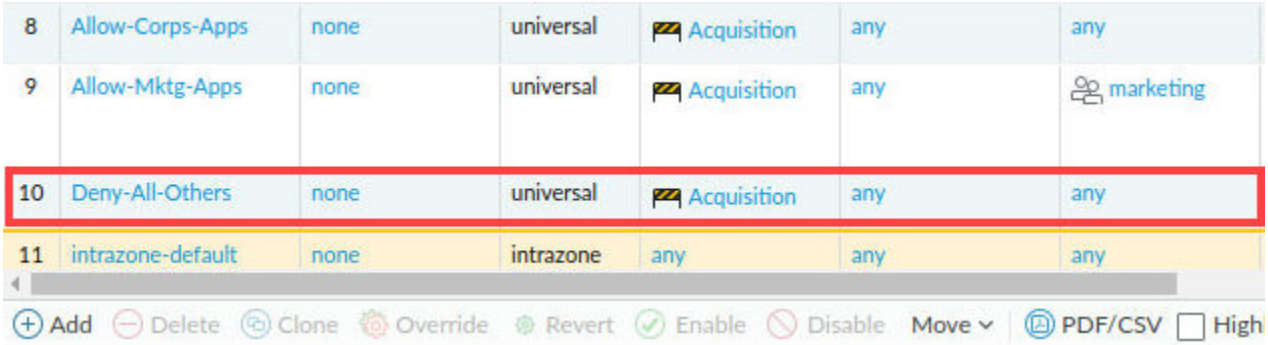
5. Select the tab for **Application** and verify that **Any** is checked.



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



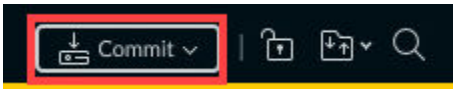
7. Verify that the **Deny-All-Others** rule appears at the bottom of the security policy.



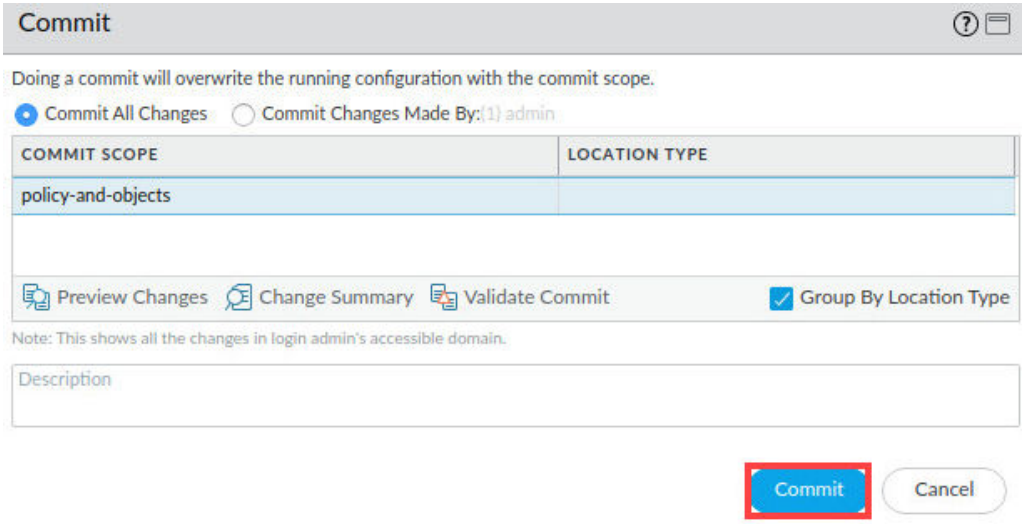
STOP

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.

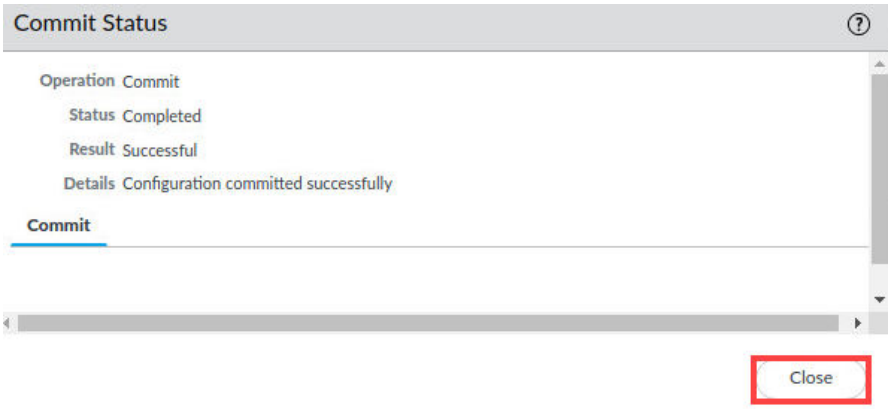
8. Click the **Commit** link located at the top-right of the web interface.



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



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



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

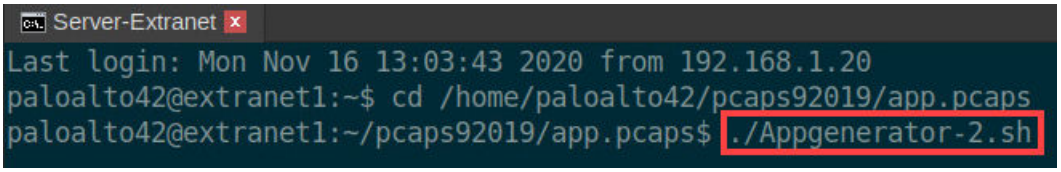
1.8 Generate Traffic from the Acquisition Zone

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

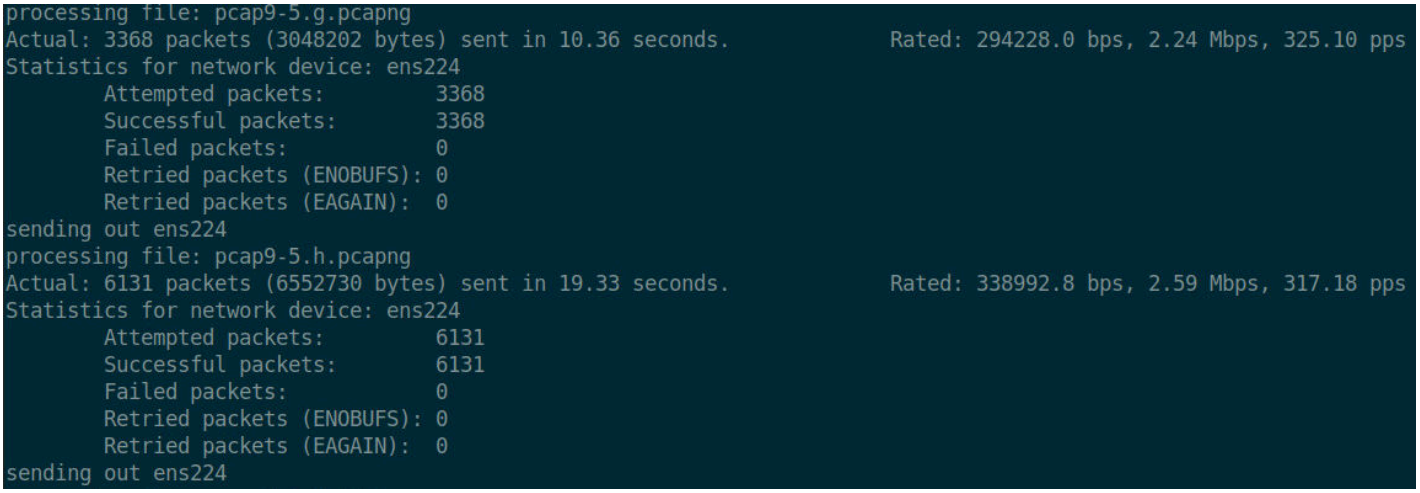
1. Open the **Remmina** application by clicking on the *Server-Extranet* tab in the taskbar if necessary.

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.



STOP

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

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

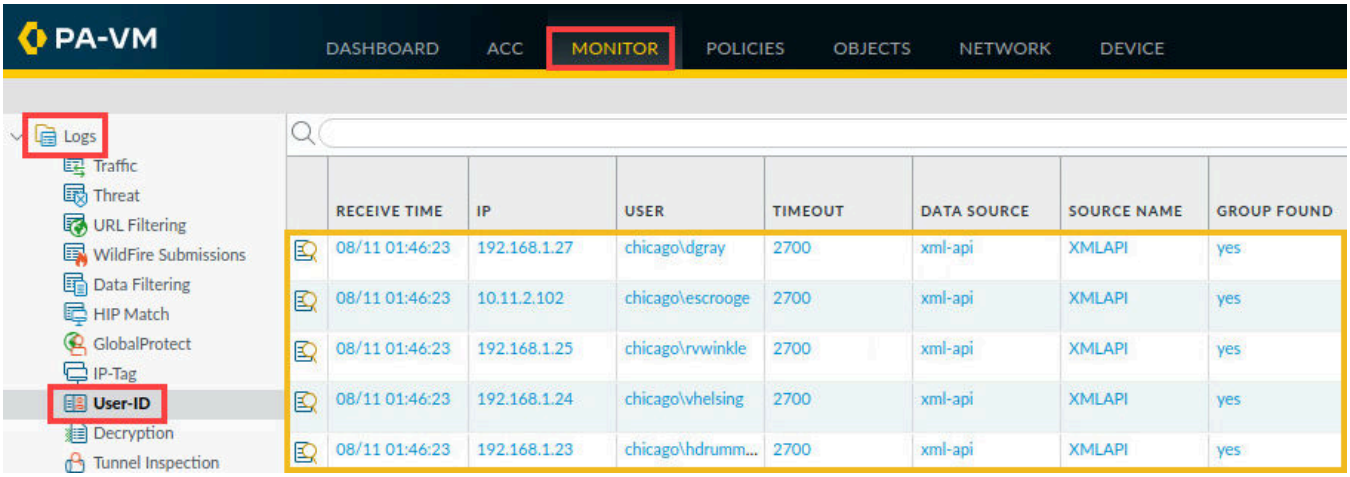
5. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

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

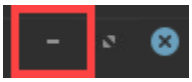
1.9 Exam User-ID Logs

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.

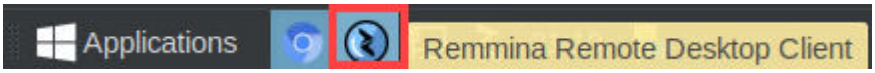
1. Select **Monitor > Logs > User-ID**. The firewall should have numerous entries with *username-to-ip-address* mappings. If the *User* mappings are not showing, repeat **Task 11.8**.



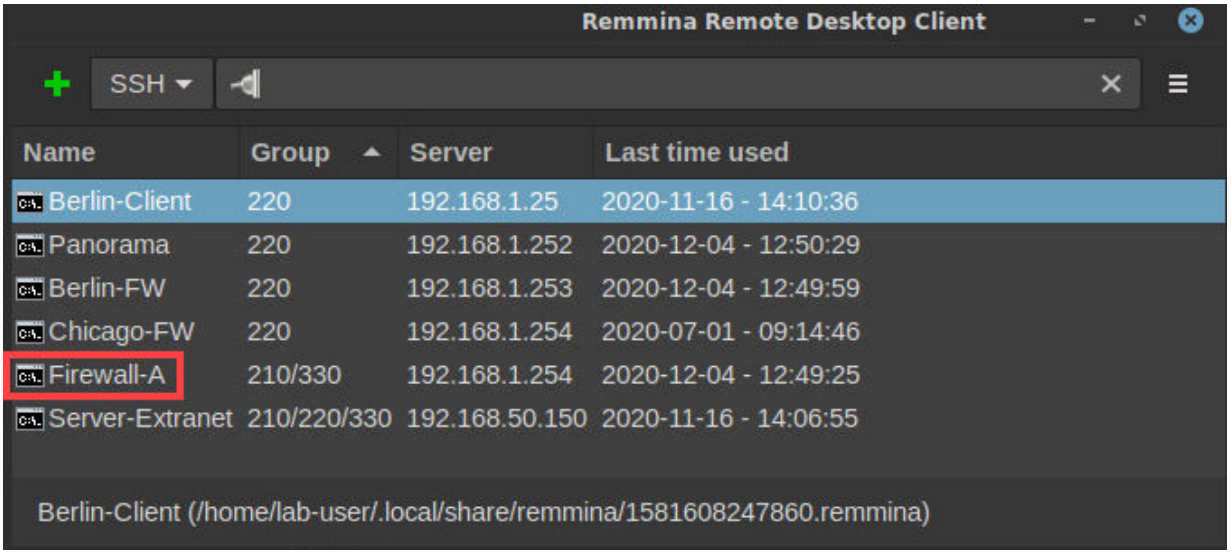
2. Minimize the PA-VM firewall by clicking minimize in the upper-right of the web interface and continue to the next task.



3. On the *client desktop*, in the taskbar, reopen the **Remmina** application.



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



5. If you get *Connecting to 'Firewall-A'…* window, click **OK**.

> **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.

6. 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                                      Vsys            From    User                            IdleTimeout(s) MaxTimeout(
s)
---------------------------------------- ---------------- ------- ------------------------------- -------------- -----------
10.10.24.102                            vsys1           XMLAPI  chicago\jcaesar                 2078           2078
192.168.1.9                             vsys1           XMLAPI  chicago\nnickleby               2078           2078
10.4.5.101                              vsys1           XMLAPI  chicago\tsawyer                 2078           2078
192.168.1.104                           vsys1           XMLAPI  chicago\mrhyde                  2078           2078
192.168.1.22                            vsys1           XMLAPI  chicago\hpoirot                 2078           2078
192.168.1.43                            vsys1           XMLAPI  chicago\jringo                  2078           2078
192.168.1.36                            vsys1           XMLAPI  chicago\bbill                   2078           2078
192.168.1.41                            vsys1           XMLAPI  chicago\gronimo                 2078           2078
lines 1-11...skipping...
```

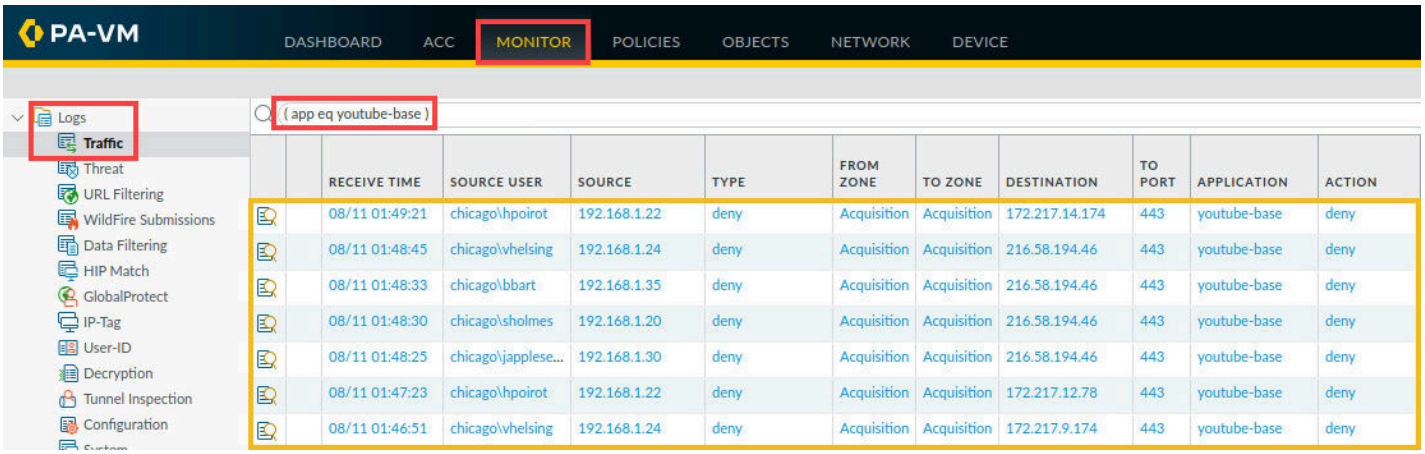
7. Close the *Firewall-A* window by clicking the **close** icon.

8. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar and continue to the next task.

1.10 Examine Firewall Traffic Log

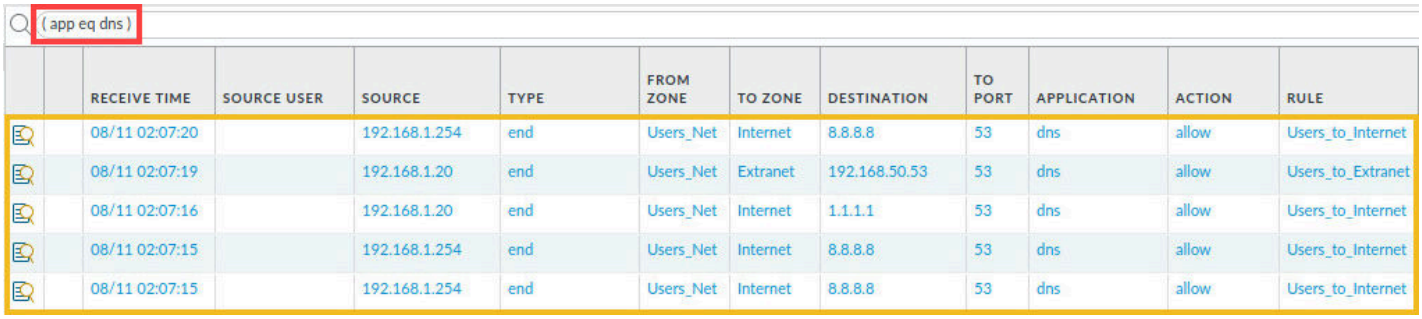
Create and apply filters to view rules and users.

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



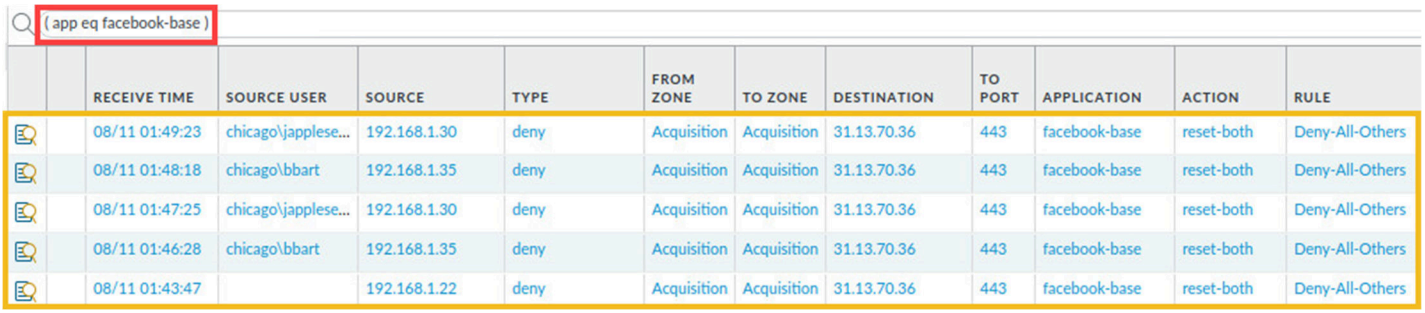
RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION
08/11 01:49:21	chicago\hpoirot	192.168.1.22	deny	Acquisition	Acquisition	172.217.14.174	443	youtube-base	deny
08/11 01:48:45	chicago\vhelsing	192.168.1.24	deny	Acquisition	Acquisition	216.58.194.46	443	youtube-base	deny
08/11 01:48:33	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	216.58.194.46	443	youtube-base	deny
08/11 01:48:30	chicago\sholmes	192.168.1.20	deny	Acquisition	Acquisition	216.58.194.46	443	youtube-base	deny
08/11 01:48:25	chicago\japplese...	192.168.1.30	deny	Acquisition	Acquisition	216.58.194.46	443	youtube-base	deny
08/11 01:47:23	chicago\hpoirot	192.168.1.22	deny	Acquisition	Acquisition	172.217.12.78	443	youtube-base	deny
08/11 01:46:51	chicago\vhelsing	192.168.1.24	deny	Acquisition	Acquisition	172.217.9.174	443	youtube-base	deny

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



RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
08/11 02:07:20		192.168.1.254	end	Users_Net	Internet	8.8.8.8	53	dns	allow	Users_to_Internet
08/11 02:07:19		192.168.1.20	end	Users_Net	Extranet	192.168.50.53	53	dns	allow	Users_to_Extranet
08/11 02:07:16		192.168.1.20	end	Users_Net	Internet	1.1.1.1	53	dns	allow	Users_to_Internet
08/11 02:07:15		192.168.1.254	end	Users_Net	Internet	8.8.8.8	53	dns	allow	Users_to_Internet
08/11 02:07:15		192.168.1.254	end	Users_Net	Internet	8.8.8.8	53	dns	allow	Users_to_Internet

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



RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
08/11 01:49:23	chicago\japplese...	192.168.1.30	deny	Acquisition	Acquisition	31.13.70.36	443	facebook-base	reset-both	Deny-All-Others
08/11 01:48:18	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.36	443	facebook-base	reset-both	Deny-All-Others
08/11 01:47:25	chicago\japplese...	192.168.1.30	deny	Acquisition	Acquisition	31.13.70.36	443	facebook-base	reset-both	Deny-All-Others
08/11 01:46:28	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.36	443	facebook-base	reset-both	Deny-All-Others
08/11 01:43:47		192.168.1.22	deny	Acquisition	Acquisition	31.13.70.36	443	facebook-base	reset-both	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)

	RECEIVE TIME	SOURCE USER	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
	08/10 23:46:43		192.168.1.35	end	Acquisition	Acquisition	31.13.70.36	443	facebook-base	allow	Allow-All-Acquisition
	12/02 04:35:18		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
	12/02 04:35:18		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
	12/02 04:32:04		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1
	12/02 04:06:33		192.168.1.20	end	inside	outside	31.13.69.228	443	facebook-base	allow	egress-outside-content-id-1

5. 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	SOURCE	TYPE	FROM ZONE	TO ZONE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
	08/11 01:49:10	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.174	443	instagram-base	reset-both	Deny-All-Others
	08/11 01:47:15	chicago\bbart	192.168.1.35	deny	Acquisition	Acquisition	31.13.70.174	443	instagram-base	reset-both	Deny-All-Others

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