



## **PALO ALTO NETWORKS EDU 210**

### **Lab 10: Blocking Threats Using Custom Applications**

**Document Version: 2022-07-18**

## Contents

Introduction .....	3
Objective .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Blocking Threats Using Custom Applications.....	6
1.1 Apply a Baseline Configuration to the Firewall .....	6
1.2 Gather Custom Application Information .....	10
1.3 Configure a Packet Capture .....	12
1.4 Packet Capture Application Traffic.....	15
1.5 Analyze the Packet Capture.....	18
1.6 Create a Custom Application with a Signature.....	20
1.7 Add the Custom Application to the Security Policy.....	25
1.8 Test the Custom Application .....	28

## Introduction

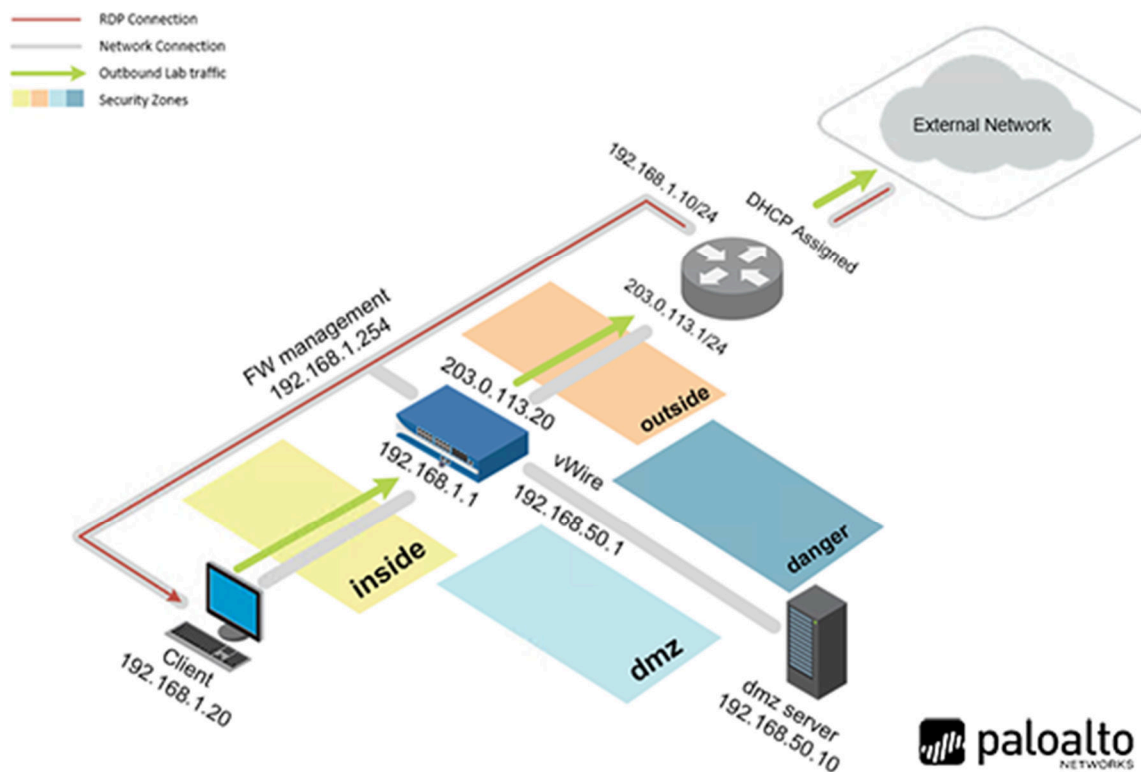
Your company uses a very old application written long ago that provides critical information to the accounting department. This application has not been upgraded yet. There are plans to have a new version developed, but no one seems to have the time to take on the task. You must isolate and secure this application so that the firewall can identify it. However, the application developer (who no longer works for the company) designed the application to run on TCP port 80 and use the HTTP protocol. Because the application is so like general web-browsing, you need to identify unique characteristics of this application traffic so that you can create a custom signature for it.

## Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Gather custom application information
- Configure a packet capture
- Capture application traffic
- Analyze the packet capture
- Create a custom application with a signature
- Add the custom application to the security policy
- Test the custom application signature

## 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	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

## 1 Blocking Threats Using Custom Applications

### 1.1 Apply a Baseline Configuration to the Firewall

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

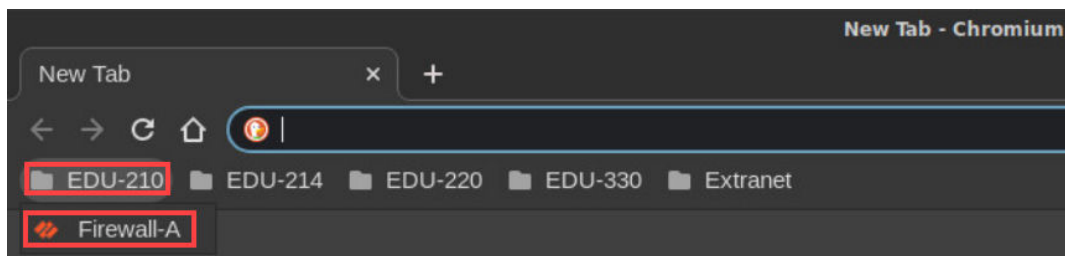
1. Click on the **Client** tab to access the Client PC.



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.



#### Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Advanced

Back to safety



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.

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



## Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

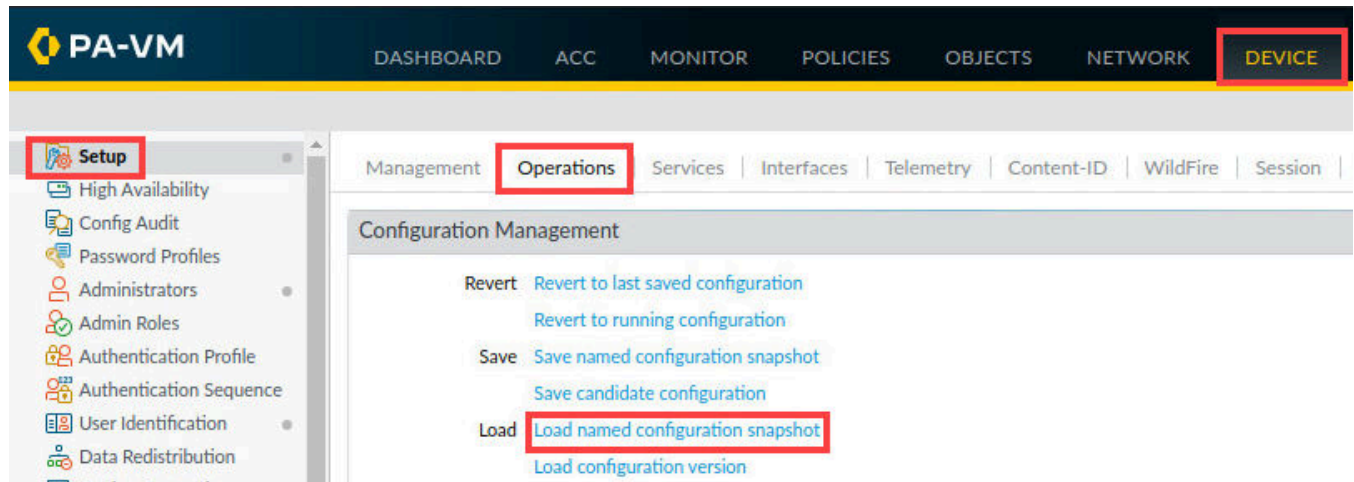
[Proceed to 192.168.1.254 \(unsafe\)](#)

- Log in to the firewall web interface as username **admin**, password **Pa10Alt0!**.

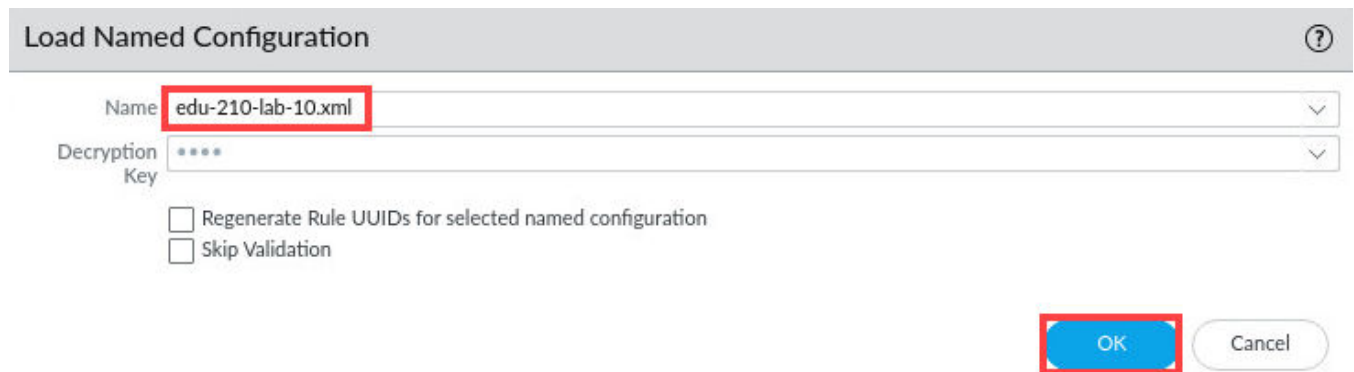


The image shows the Palo Alto Networks login page. It features the Palo Alto Networks logo at the top. Below the logo, there is a username field containing the text "admin" and a password field filled with dots. A blue "Log In" button is positioned below the password field. The entire login form is enclosed in a yellow rectangular border.

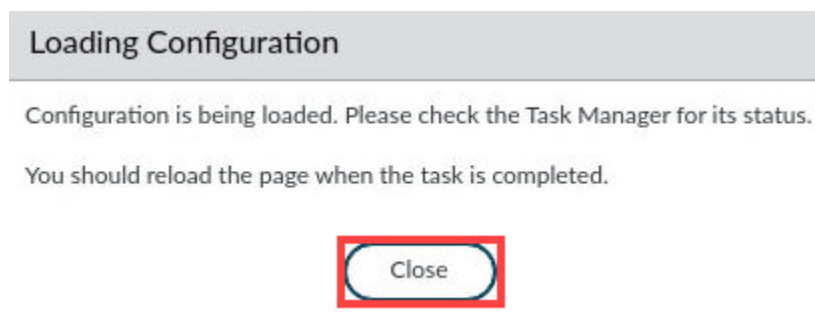
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named **configuration snapshot** underneath the *Configuration Management* section.



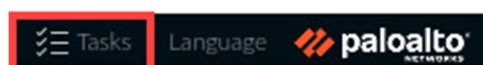
8. In the *Load Named Configuration* window, select **edu-210-lab-10.xml** from the *Name* dropdown box and click **OK**.



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**.

Task Manager - All Tasks

8 items

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show All Tasks Clear Commit Queue

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.

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 SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

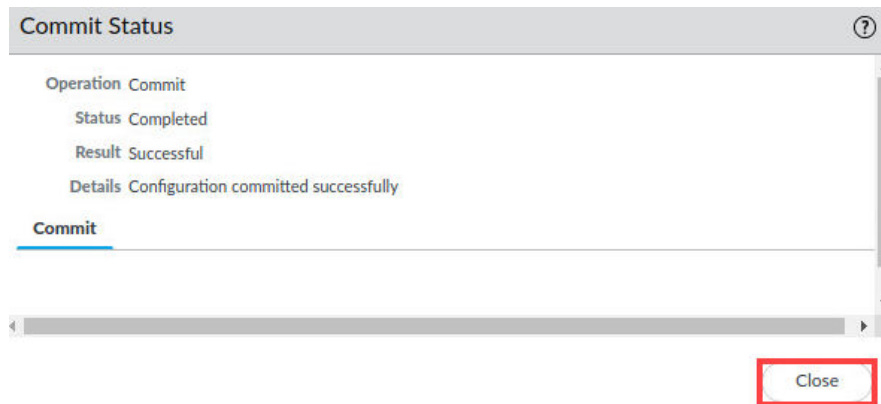
[Preview Changes](#)
[Change Summary](#)
[Validate Commit](#)
☒ Group By Location Type

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

Description

Commit Cancel

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.

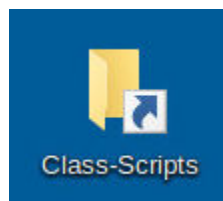
15. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



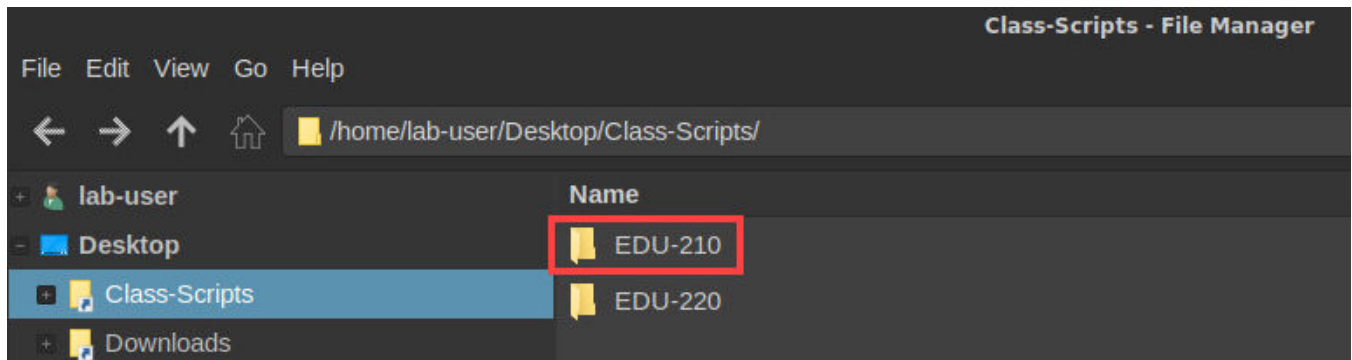
## 1.2 Gather Custom Application Information

You will gather information about the traffic that this application uses so that you can create a custom application signature.

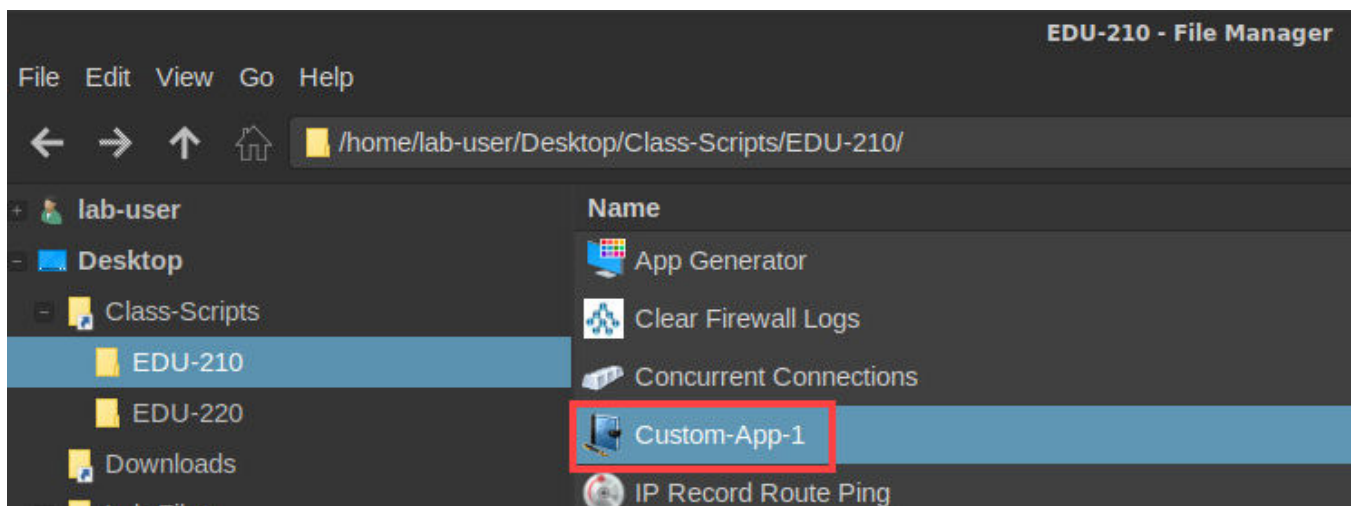
1. On the *client desktop*, double-click the folder for **Class-Scripts**.



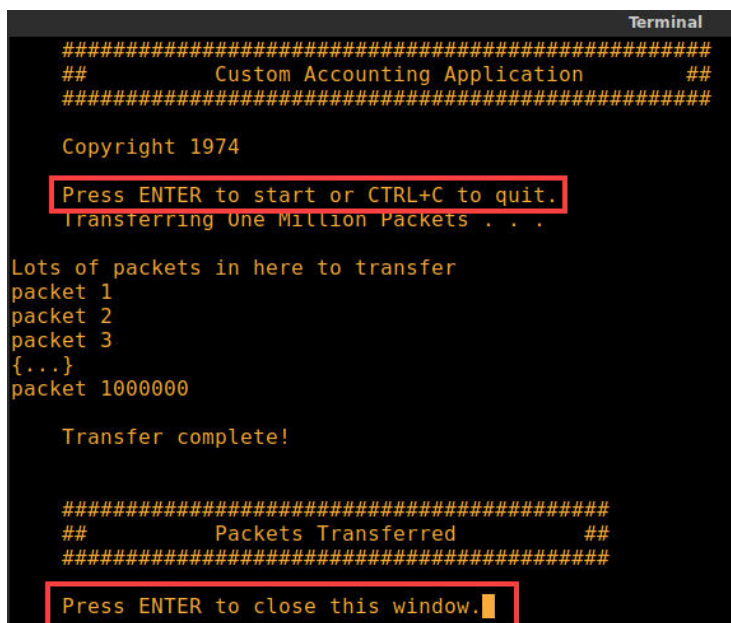
2. Open the **EDU-210** folder.



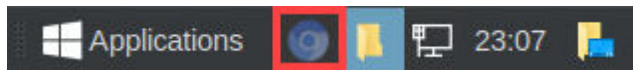
3. Double-click the icon for **Custom-App-1**.



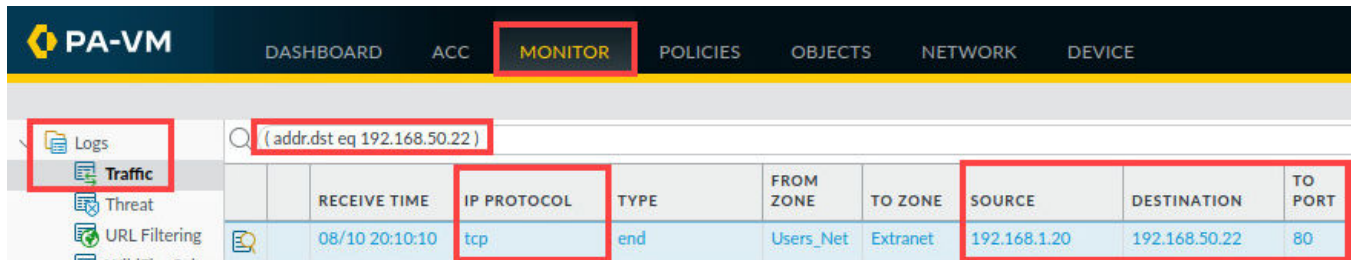
4. Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.



- If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



- In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter ( `addr.dst eq 192.168.50.22` ) in the filter builder. Write down the *Source IP address*, *Destination IP address*, *Port number*, and the *IP protocol*. If the *IP Protocol* column is not displayed, place your mouse pointer over any column header and select **Columns > IP Protocol**.



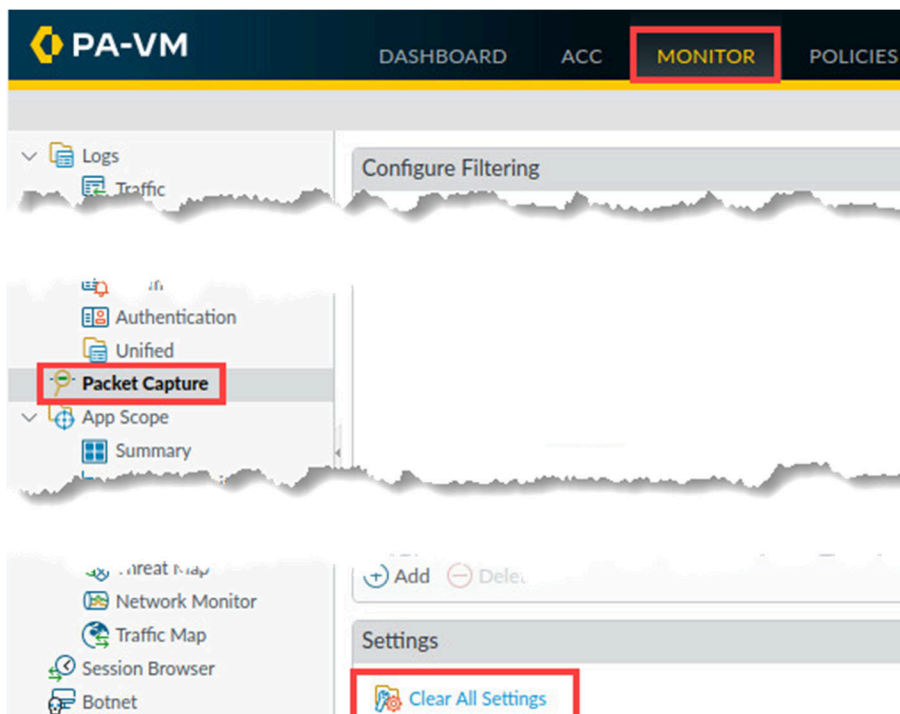
RECEIVE TIME	IP PROTOCOL	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT
08/10 20:10:10	tcp	end	Users_Net	Extranet	192.168.1.20	192.168.50.22	80

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

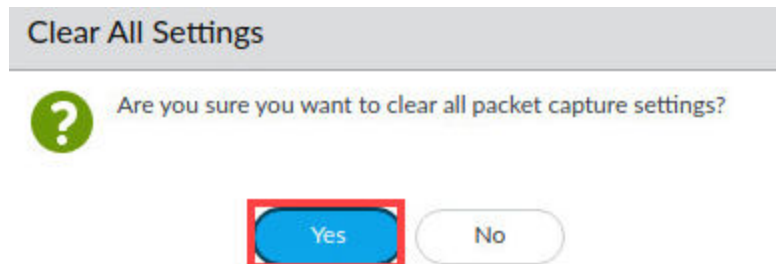
### 1.3 Configure a Packet Capture

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.

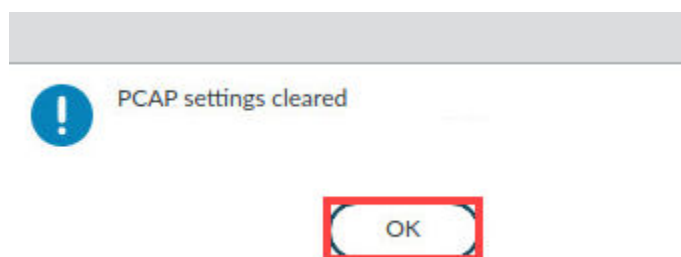
- In the web interface, select **Monitor > Packet Capture**. Click **Clear All Settings**.



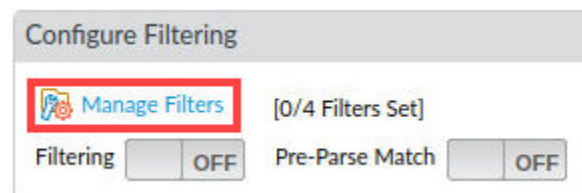
2. In the *Clear All Settings* window, click **Yes**.



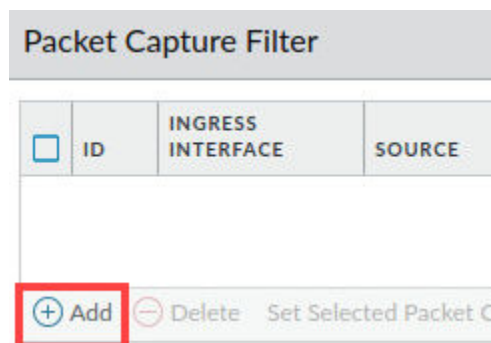
3. In the *PCAP settings cleared* window, click **OK**.



4. In the *Configure Filtering* window, click **Manage Filters**.



5. In the *Packet Capture Filter* window, click **Add**.



6. In the *Packet Capture Stage* window, configure the following. Click **OK**.

Parameter	Value
<b>Id</b>	<b>1</b>
<b>Ingress Interface</b>	<b>ethernet1/2</b>
<b>Source</b>	<b>192.168.1.20</b>
<b>Destination</b>	<b>192.168.50.22</b>
<b>Dest Port</b>	<b>80</b>
<b>Proto</b>	<b>6</b> (This number is assigned to TCP.)
<b>Non-IP</b>	<b>exclude</b>

Packet Capture Filter
?

<input type="checkbox"/>	ID	INGRESS INTERFACE	SOURCE	DESTINATION	SRC PORT	DEST PORT	PROTO	NON-IP	IPV6
<input checked="" type="checkbox"/>	1	ethernet1/2	192.168.1.20	192.168.50.22		80	6	exclude	<input type="checkbox"/>

+ Add
- Delete
Set Selected Packet Capture Filter

OK

Cancel



In Internet Protocol v4, there is a value called protocol to associate the next level protocol. 6 is the number assigned to TCP.

7. Toggle the *Filtering* button to **ON**.

Configure Filtering

Manage Filters
[1/4 Filters Set]

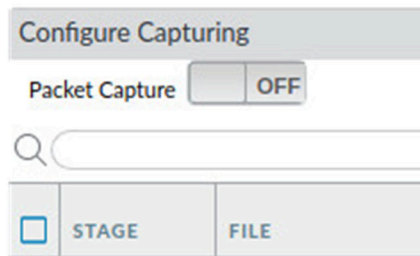
Filtering

ON

Pre-Parse Match

OFF

- Under the section for *Configure Capturing*, click **Add** to configure a file for the receive stage on the firewall.

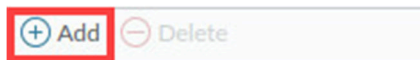


Configure Capturing

Packet Capture ☐ OFF

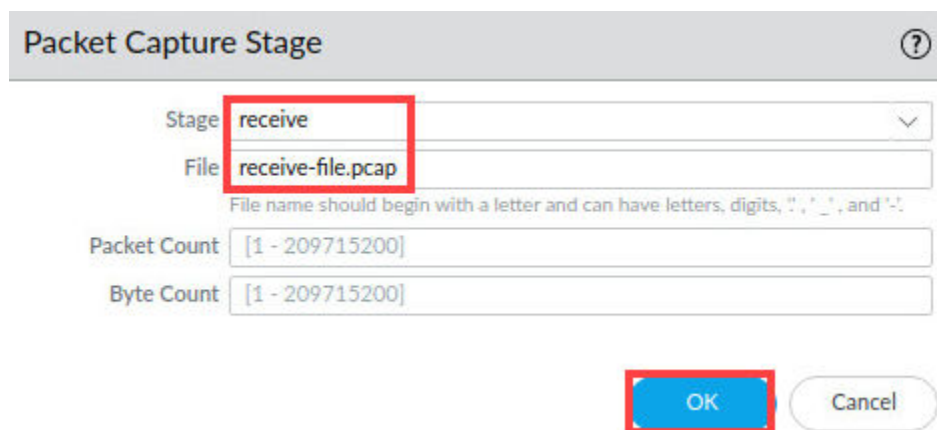
Search:

<input type="checkbox"/>	STAGE	FILE
--------------------------	-------	------



- In the *Packet Capture Stage* window, configure the following. Click **OK**.

Parameter	Value
Stage	receive
File	receive-file.pcap



Packet Capture Stage ?

Stage:

File:   
File name should begin with a letter and can have letters, digits, ".", "\_", and "-."

Packet Count:

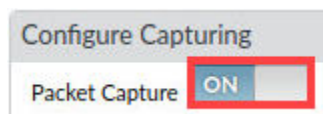
Byte Count:

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

#### 1.4 Packet Capture Application Traffic

In this section, you will take a packet capture on the firewall while using the Custom Application on the client host.

- Ensure you are still located at **Monitor > Packet Capture**. Toggle *Packet Capture* to **ON**.

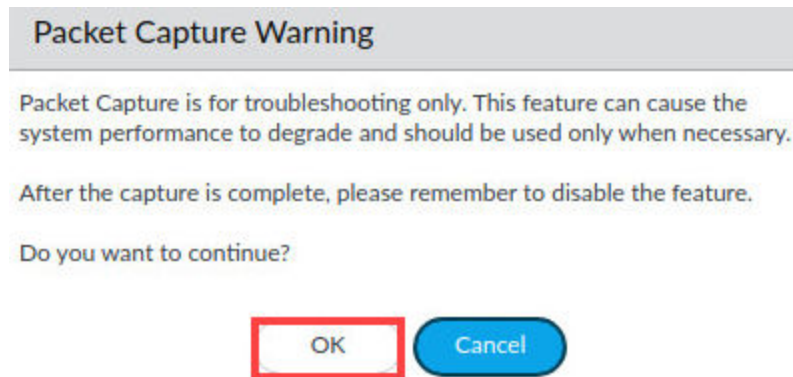


Configure Capturing

Packet Capture ☒ ON



2. In the *Packet Capture Warning* window, click **OK**.

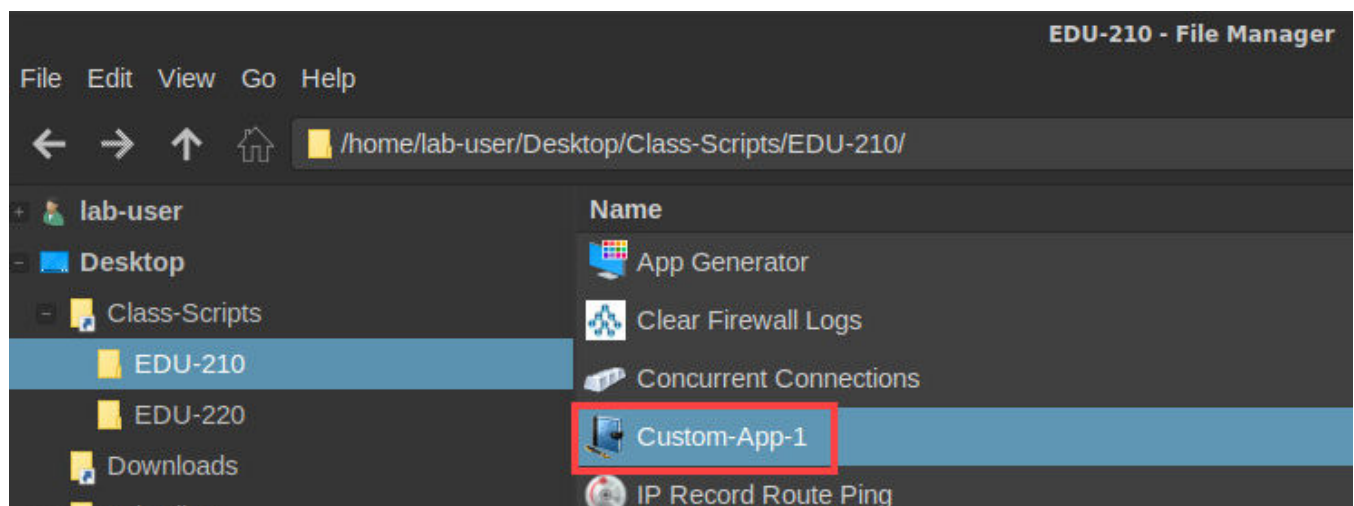


**Please Note** The firewall is now actively capturing packets that match the filter you created. The packets are being stored on the firewall in the receive-file.pcap you designated.

3. Minimize the *Palo Alto Networks Firewall*.

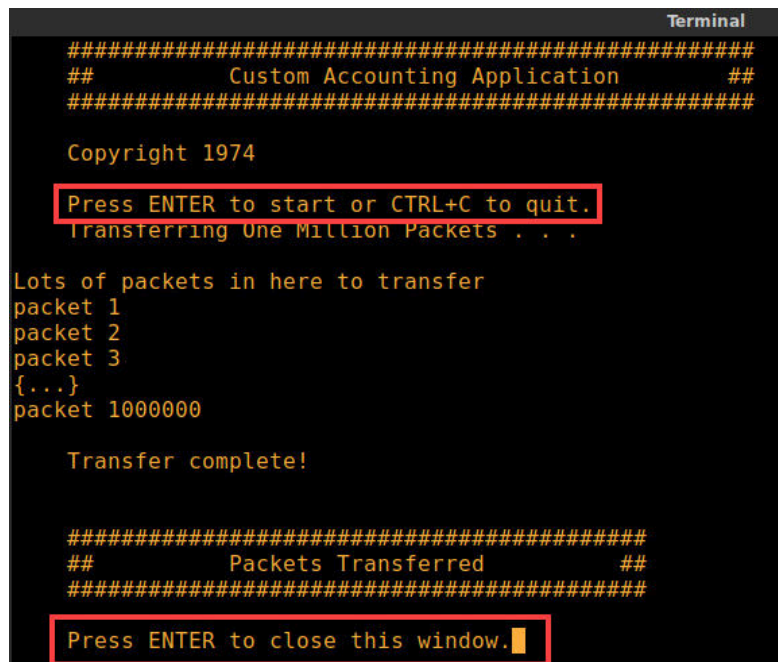


4. Open the **EDU-210** folder by clicking on the **File Manager** tab in the taskbar if necessary. Double-click the icon for **Custom-App-1**.





- Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.



```

Terminal
#####
##      Custom Accounting Application      ##
#####

Copyright 1974

Press ENTER to start or CTRL+C to quit.
Transferring One Million Packets . . .

Lots of packets in here to transfer
packet 1
packet 2
packet 3
{...}
packet 1000000

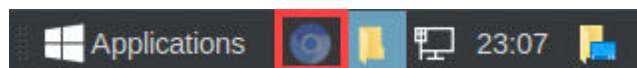
Transfer complete!

#####
##      Packets Transferred      ##
#####

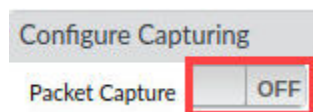
Press ENTER to close this window.

```

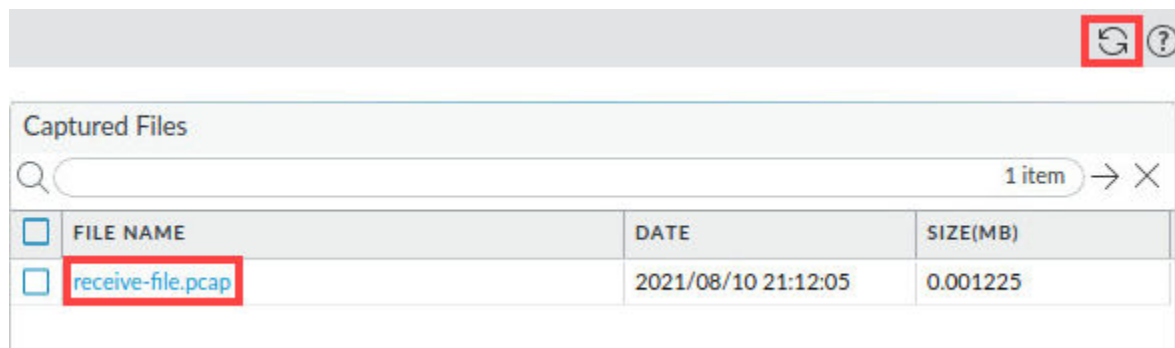
- If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



- Ensure you are still located at **Monitor > Packet Capture**. Toggle *Packet Capture* to **OFF**.



- Refresh the web interface display to view the **receive-file** listed in the *Captured Files* panel. Click **receive-file.pcap** to open it in Wireshark and continue to the next task.



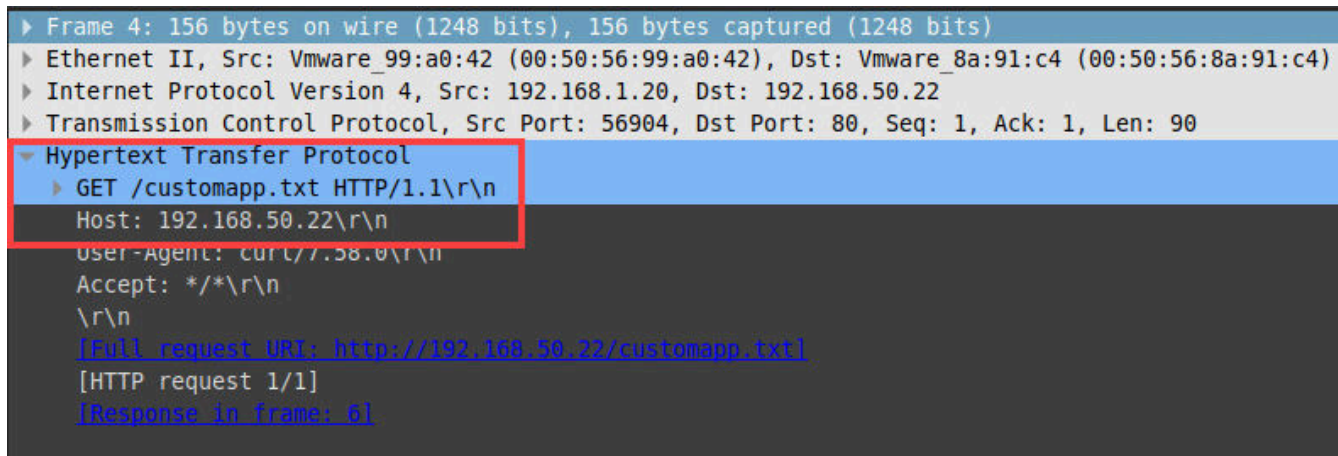
## 1.5 Analyze the Packet Capture

In this section, you will use Wireshark to analyze the packet capture to discover a unique bit pattern that identifies traffic to the Custom Application.

1. In the *Wireshark* window, find and highlight the first entry for **GET**.

1	0.000000	192.168.1.20	192.168.50.22	TCP	74	56904 → 80 [SYN] Seq=0 Win=2
2	0.000582	192.168.50.22	192.168.1.20	TCP	74	80 → 56904 [SYN, ACK] Seq=0
3	0.000642	192.168.1.20	192.168.50.22	TCP	66	56904 → 80 [ACK] Seq=1 Ack=1
4	0.000681	192.168.1.20	192.168.50.22	HTTP	156	GET /customapp.txt HTTP/1.1
5	0.000717	192.168.50.22	192.168.1.20	TCP	66	80 → 56904 [ACK] Seq=1 Ack=9

2. In the Wireshark window, click **Hypertext Transfer Protocol** to expand the display and notice that the HTTP request header included a **GET /custom-app.txt** entry and the Host **192.168.50.22**.



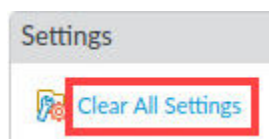
**Please  
Note**

You will use the HTTP GET method, and the URI path customapp.txt to build a custom application signature for the Custom Application

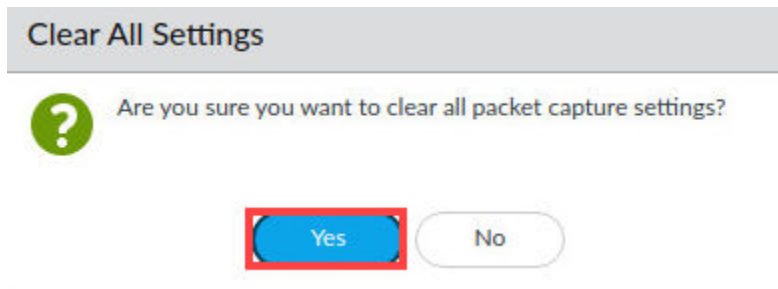
3. Close the **Wireshark** window.



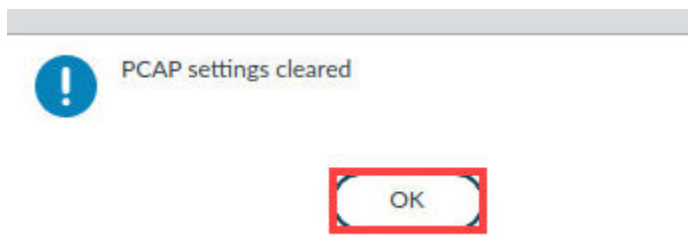
4. Ensure you are still located at **Monitor > Packet Capture**. Click **Clear All Settings**.



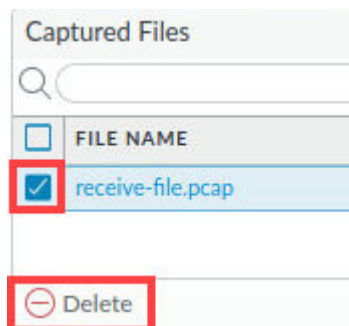
5. In the *Clear All Settings* window, click **Yes**.



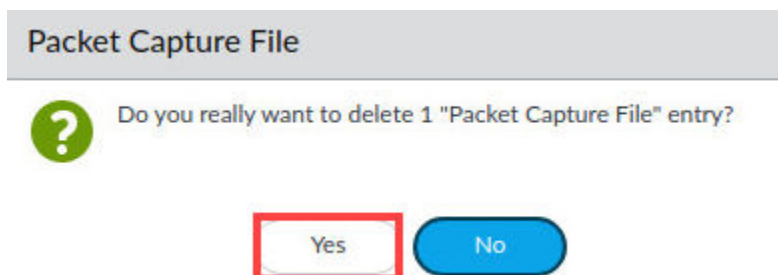
6. In the *PCAP settings clear* window, click **OK**.



7. In the *Captured Files* window, select the checkbox next to **receive-file-pcap**. Click **Delete**.



8. In the *Packet Capture File* window, click **Yes**.

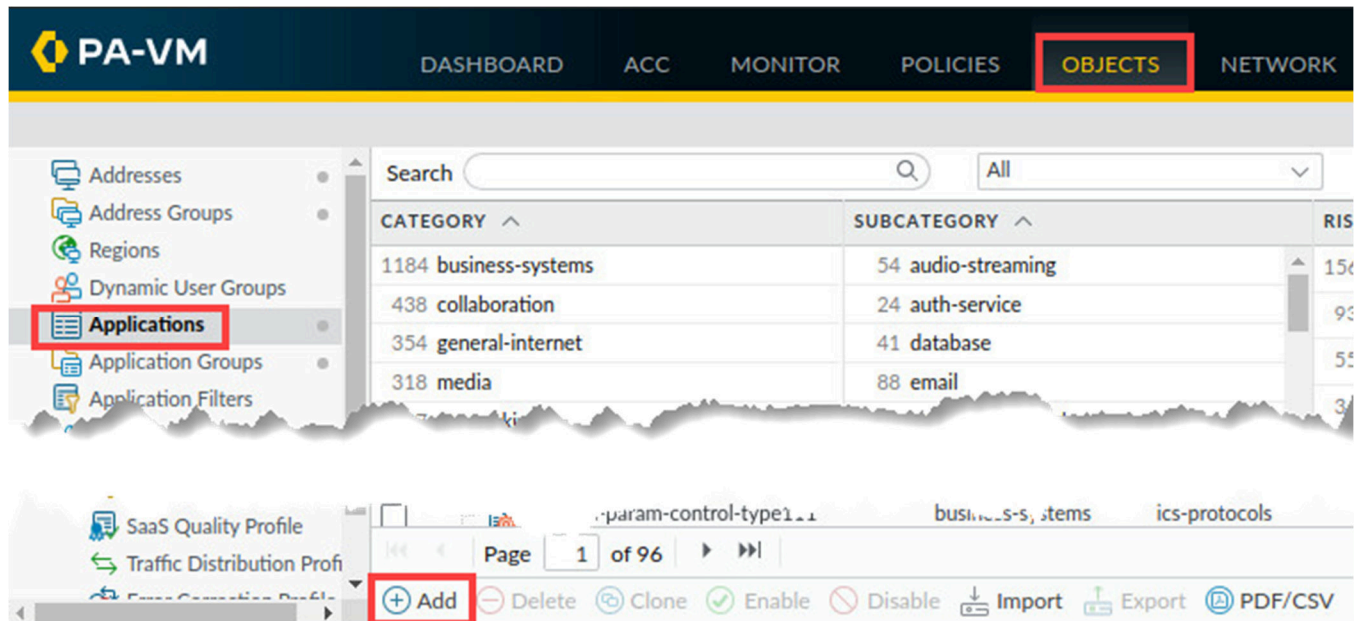


9. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 1.6 Create a Custom Application with a Signature

In this section, you will use the information discovered in the packet capture to create a unique signature that can identify HTTP traffic to the Internal Company Custom Application.

1. In the web interface, select **Objects > Applications**. Click **Add**.



2. In the *Application* window, on the **Configuration** tab. Configure the following.

Parameter	Value
Name	Custom-App-1
Category	business-systems
Subcategory	office-programs
Technology	client-server
Parent App	None
Risk	1

Application ?

**Configuration** | Advanced | Signatures

---

**General**

Name Custom-App-1

Description

---

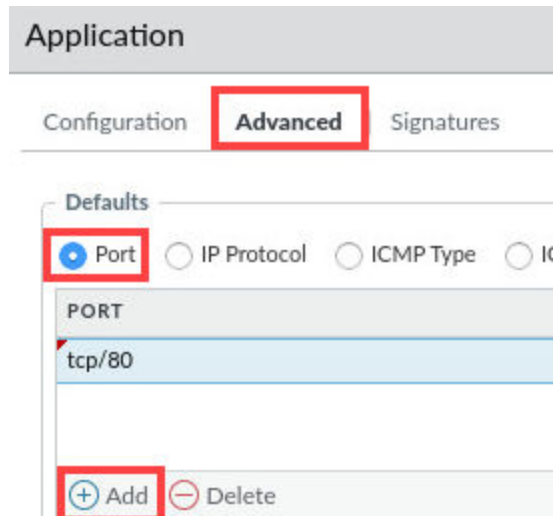
**Properties**

Category business-systems Subcategory office-programs Technology client-server

Parent App None Risk 1

3. Click the **Advanced** tab and configure the following.

Parameter	Value
Port	Select <b>radio button</b>
Port	Click <b>Add</b> and type <b>tcp/80</b>



Application

Configuration **Advanced** Signatures

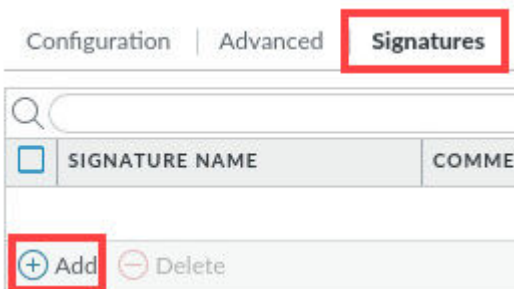
Defaults

☒ Port ☐ IP Protocol ☐ ICMP Type ☐ IK

PORT

tcp/80

4. Click the **Signatures** tab. Click **Add**.



Configuration | Advanced **Signatures**

SEARCH

<input type="checkbox"/>	SIGNATURE NAME	COMMENTS
--------------------------	----------------	----------

5. In the *Signature* window, configure the following. Click **Add or Condition**.

Parameter	Value
Signature Name	Signature-1
Scope	Transaction
Ordered Condition Match	Leave selected (Neither choice affects the signature.)

**Signature**

Signature Name **Signature-1**

Comment

Scope ☒ Transaction ☐ Session

☒ Ordered Condition Match

☐ AND CONDITION ☐ COND... ☐ OPERATOR

**+ Add Or Condition** **+ Add And Condition** **-**

6. In the *New and Condition – Or Condition* window, configure the following. Click **Add**.

Parameter	Value	custom
Operator	Pattern Match	
Context	http-req-uri-path	
Pattern	customapp.txt	

**New And Condition - Or Condition** ?

Operator **Pattern Match**

Context **http-req-uri-path**

Pattern **customapp.txt**

0 items → ×

QUALIFIER	VALUE
<b>+ Add</b>	<b>- Delete</b>

7. In the *Qualifier* window, configure the following and then click **OK**.

Parameter	Value
Qualifier	http-method
Value	GET

Qualifier ?

Qualifier

Value

**OK** Cancel

8. Click **OK** to close the *New And Condition – Or Condition* window.

**OK** Cancel

9. Click **OK** to close the *Signature* window.

Signature ?

Signature Name

Comment

Scope ☒ Transaction ☐ Session

☒ Ordered Condition Match

<input type="checkbox"/>	AND CONDITION	COND...	OPERATOR	CONTEXT	PATTERN	QUALIFIER
And Condition 1						
<input type="checkbox"/>	And Condition 1	Or Condi... 1	pattern-match	http-req-uri-path	customapp.txt	http-method: GET

**OK** Cancel



10. Click **OK** to close the *Application* window.

**Application** ?

Configuration | Advanced | **Signatures**

Search 1 item → ×

<input type="checkbox"/>	SIGNATURE NAME	COMMENT	ORDERED CONDITION MATCH	SCOPE
<input checked="" type="checkbox"/>	Signature-1		<input checked="" type="checkbox"/>	Transaction

+ Add − Delete

OK
Cancel

11. To display only custom applications, select **Custom applications** on the filter dropdown menu. A new entry for **Custom-App-1** appears at the top of the *Application* list.


Search Q

**CATEGORY** ^ **SUBCATEGORY**

1 business-systems 1 office-p

**Custom applications** ▼

- All
- Custom applications**
- Disabled applications
- Tagged applications

<input type="checkbox"/>	NAME	CATEGORY	SUBCATEGORY
<input type="checkbox"/>	 Custom-App-1	business-systems	office-programs

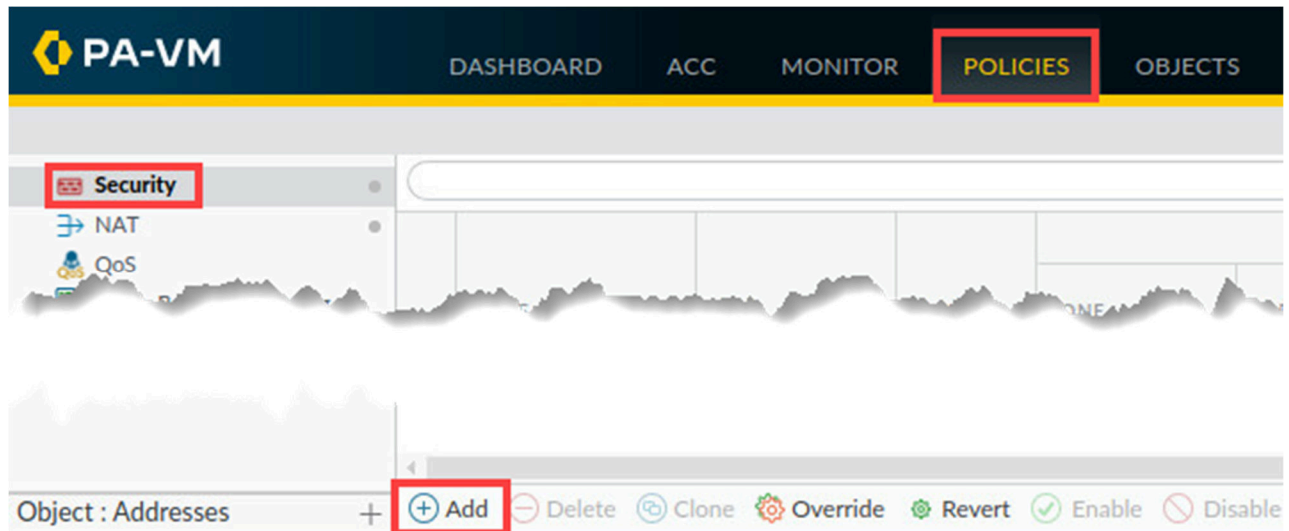
12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.



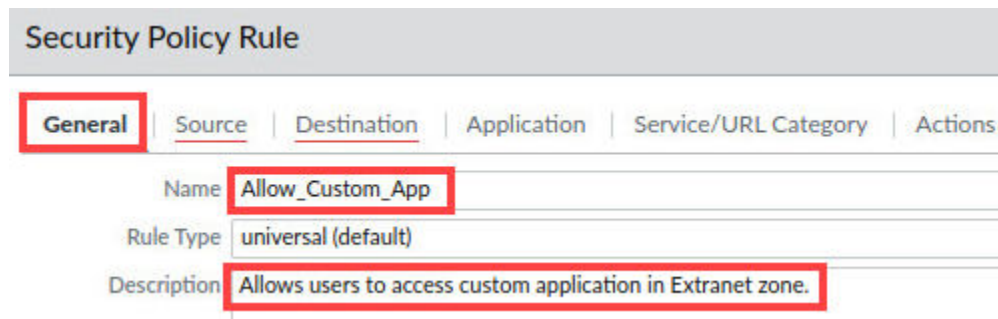
## 1.7 Add the Custom Application to the Security Policy

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.

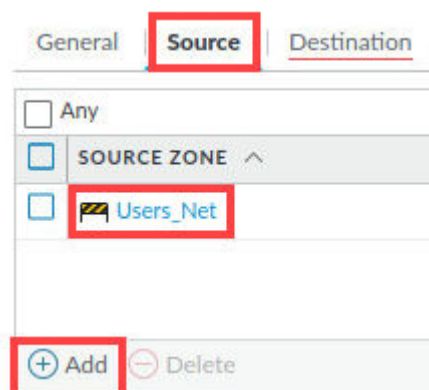
1. Select **Policies > Security**. Click **Add**.



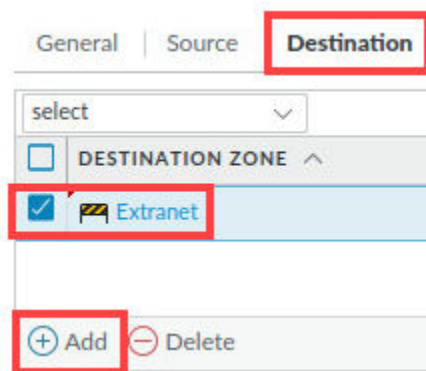
2. In the *Security Policy Rule* window, under the **General** tab, enter **Allow\_Custom\_App** for the *Name*. For *Description*, enter **Allows users to access custom application in Extranet zone.**



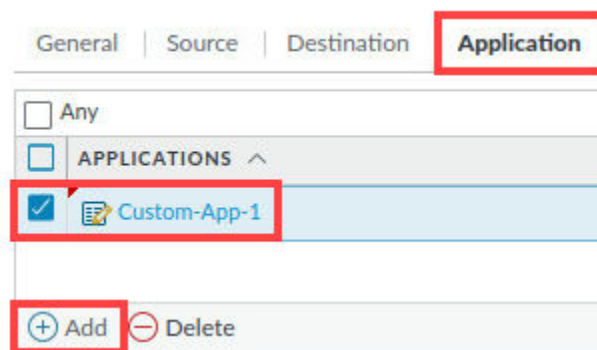
3. Select the tab for **Source**, under the *Source Zone* section, click **Add** and select **Users\_Net**.



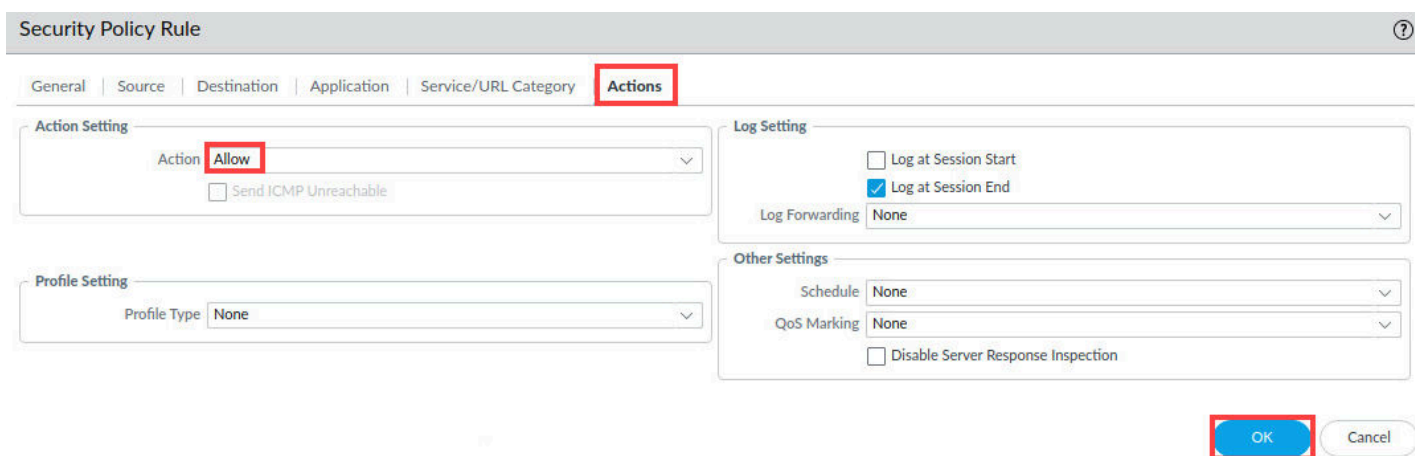
4. Select the tab for **Destination**, under the *Destination Zone* section, click **Add** and select **Extranet**.



5. Select the **Application** tab, click **Add** and enter the first few letters of the **Custom-App-1** name to locate the entry.



6. Select the **Actions** tab and verify that the *Action Setting* is set to **Allow**. Click **OK**.





7. Highlight the **Allow\_Custom\_App** entry without opening it.

5	Extranet_to_Internet	none	universal	Extranet	any	any	any	Internet
6	Allow-PANW-Apps	none	universal	Users_Net	any	any	any	Internet
7	Allow_Custom_App	none	universal	Users_Net	any	any	any	Extranet

8. Use the **Move > Move up** button at the bottom of the window to relocate this rule just above **Users\_to\_Extranet**.

2	migrated-ftp-port-ba...	none	universal	Users_Net	any	any
3	Allow_Custom_App	none	universal	Users_Net	any	any
4	Users_to_Extranet	none	universal	Users_Net	any	any
5	Users_to_Internet	none	universal	Users_Net	any	any
9	interzone-default	none	interzone	any	any	any





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



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

**Commit**

Doing a commit will overwrite the running configuration with the commit scope.

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

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes
 Change Summary
 Validate Commit
☒ Group By Location Type

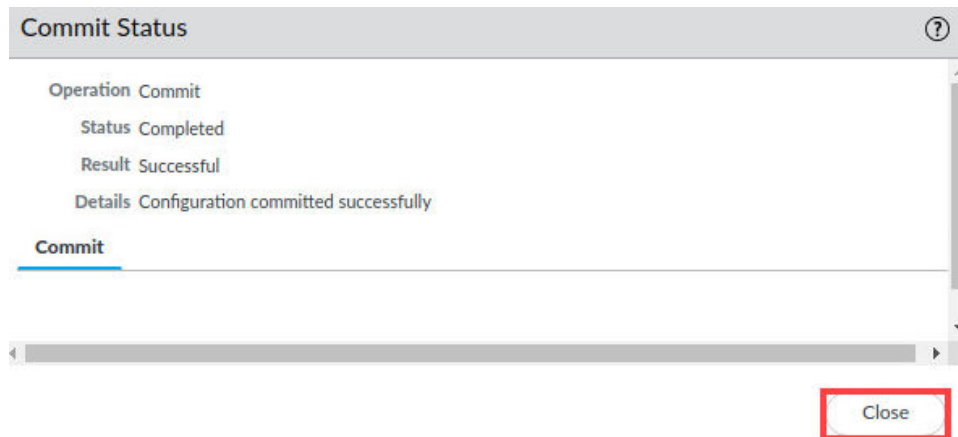
Note: This shows all the changes in login admin's accessible domain.

Description

Commit

Cancel

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



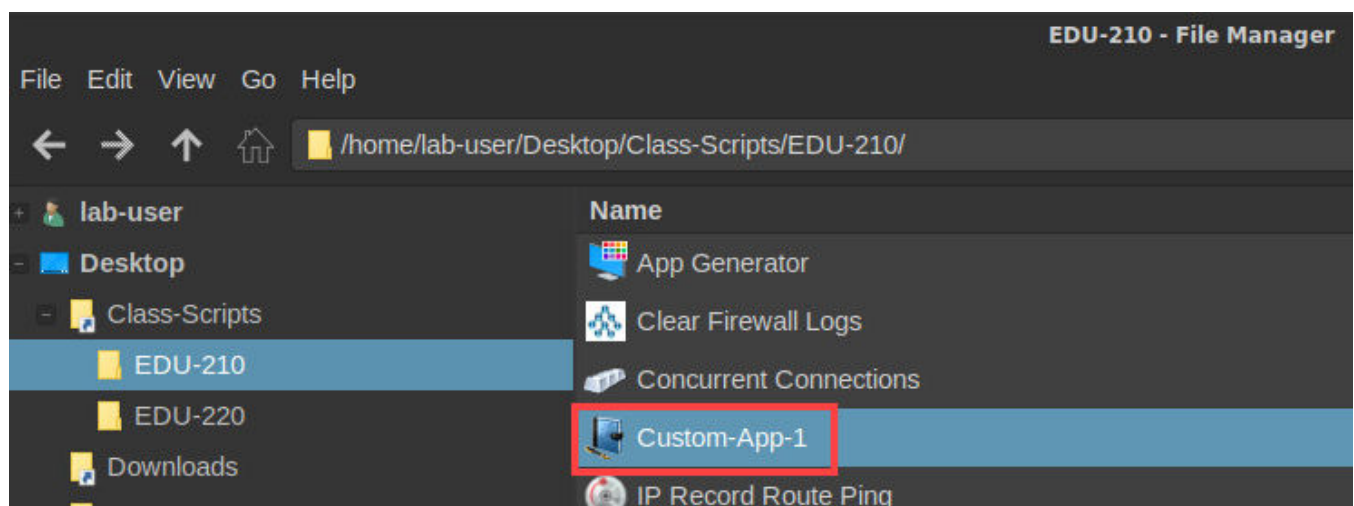
12. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



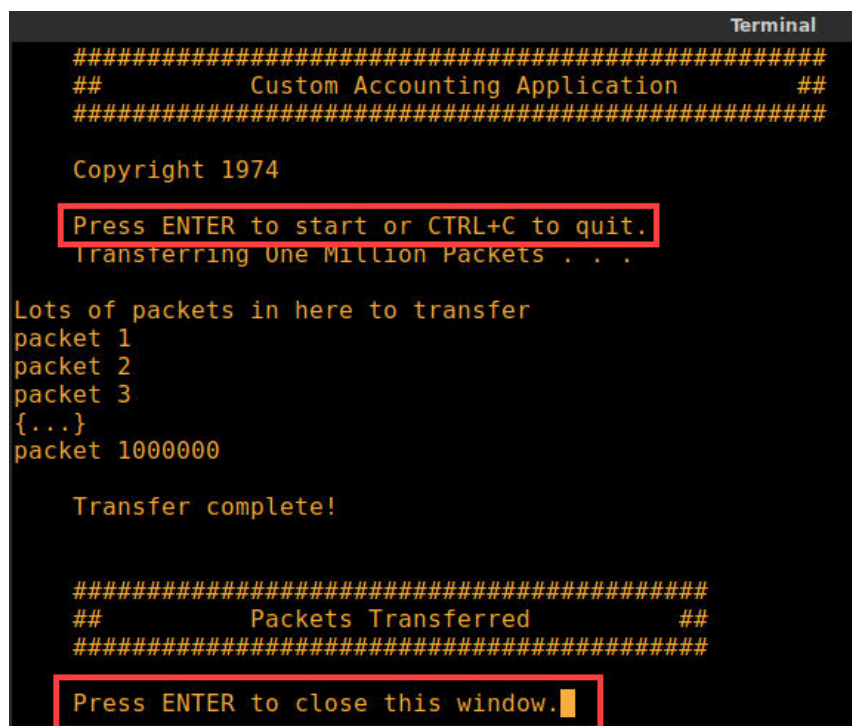
## 1.8 Test the Custom Application

In this section, you will run the Custom Application to determine whether the firewall correctly identifies the traffic.

1. Open the **EDU-210** folder by clicking on the **File Manager** tab in the taskbar if necessary. Double-click the icon for **Custom-App-1**.



- Press **Enter** to start the *Custom-App-1* script. Allow the script to complete. Once the *Custom-App-1* script completes, press **Enter**.



```

Terminal
#####
##      Custom Accounting Application      ##
#####

Copyright 1974

Press ENTER to start or CTRL+C to quit.
Transferring One Million Packets . . .

Lots of packets in here to transfer
packet 1
packet 2
packet 3
{...}
packet 1000000

Transfer complete!

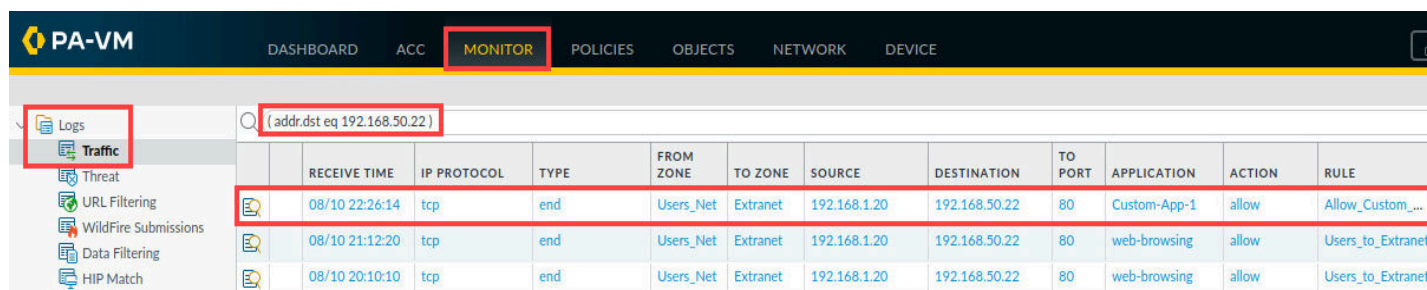
#####
##      Packets Transferred      ##
#####

Press ENTER to close this window.
  
```

- If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



- In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter ( `addr.dst eq 192.168.50.22` ) in the filter builder. Notice the *Application* label is **Custom-App-1** and how the custom application enables more granular logging of application traffic. The traffic no longer was generically identified as web-browsing



	RECEIVE TIME	IP PROTOCOL	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
	08/10 22:26:14	tcp	end	Users_Net	Extranet	192.168.1.20	192.168.50.22	80	Custom-App-1	allow	Allow_Custom...
	08/10 21:12:20	tcp	end	Users_Net	Extranet	192.168.1.20	192.168.50.22	80	web-browsing	allow	Users_to_Extranet
	08/10 20:10:10	tcp	end	Users_Net	Extranet	192.168.1.20	192.168.50.22	80	web-browsing	allow	Users_to_Extranet

**Please Note**

Note that you may need to use the refresh button several times to see the new entry in the Traffic Log. The sessions must end before the firewall writes an entry to the Traffic log

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