PALO ALTO NETWORKS EDU 210

Lab 9: Maintaining Application-Based Policies

Document Version: 2022-07-18

Contents

Introduction

Your organization runs several common application servers on non-standard ports. For example, there are several web servers in your network that use TCP port 8080 instead of the default TCP port 80. You need to make certain that you configure the firewall to allow web-browsing traffic even when that traffic is using TCP port 8080. To accomplish this task, you will configure a new service object and incorporate it into a security policy rule for web-browsing.

You will also use the Policy Optimizer utility on the firewall to migrate the port-based FTP rule to an application-based rule.

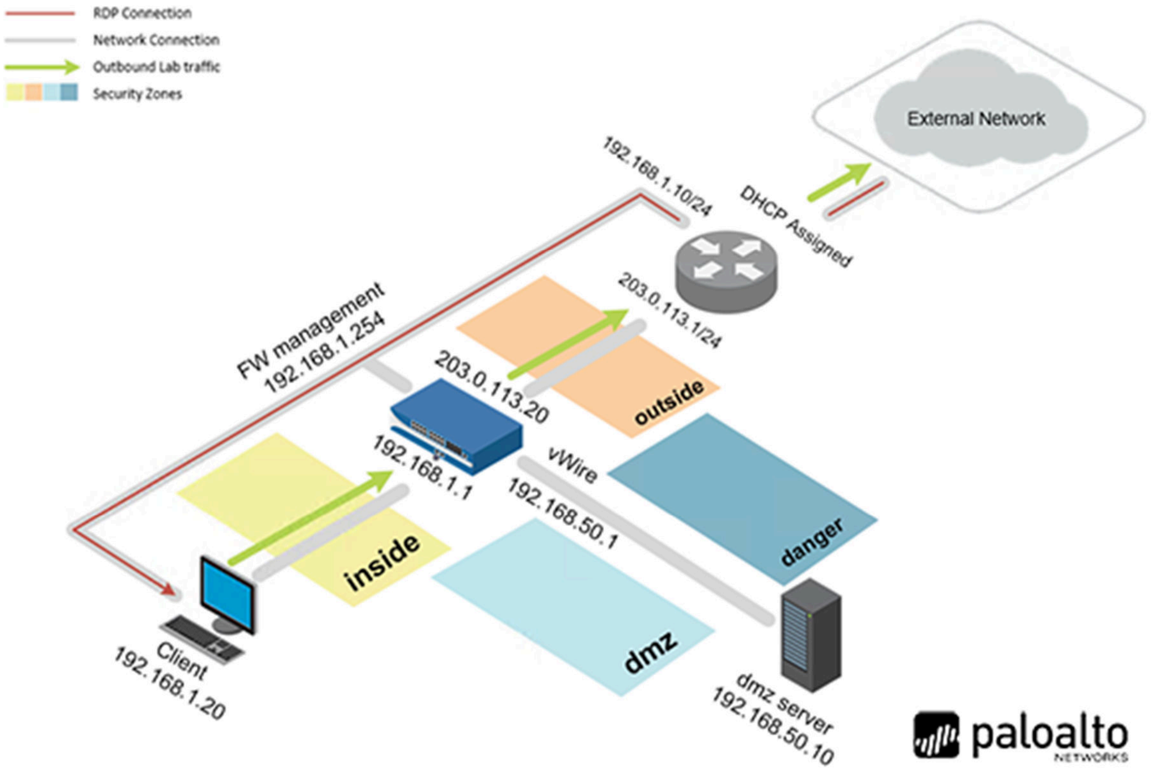
In the last section, you will make certain that your firewall is consistently up to date with the latest signatures and information from Palo Alto Networks. You need to make sure that the firewall downloads and incorporates these updates automatically, so you will schedule the process.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create a custom Service object for HTTP
- Add the new service to the security policy
- Test Access to the web server on port 8080
- Revert the web server to port 80
- Create an FTP application-based security policy rule
- Test the application-based security policy
- Remove the FTP rules
- Scheduling App-ID updates

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!`**

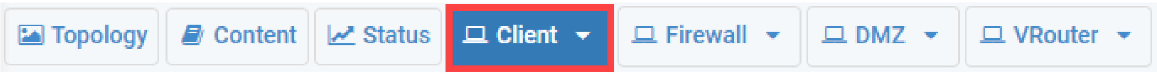
1 Maintaining Application-Based Policies

1.1 Apply a Baseline Configuration to the Firewall

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

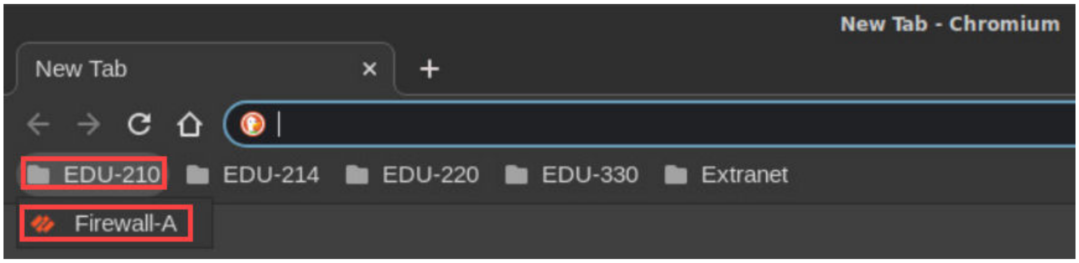
> ⚠ In this lab, *Task 1.6* is optional. This task includes a step that only updates the Policy Optimizer statistics on the firewall every hour, on the hour. To complete Task 9.6, you will want to be closer to the top of the hour. If you start at the bottom of the hour, please note that the lab will possibly take about two hours to complete due to waiting for the top of the hour.
>
> If you plan on completing *Task 1.6*, it is recommended that you start this lab 30 minutes before the top of the hour to minimize your wait time to complete this lab.
>
> If you choose to skip *Task 1.6*, without using the Policy Optimizer, and manually adding the FTP Application based policy, please continue to start this lab at *Task 1.1*, skip *Task 1.6* and continue on with *Task 1.7* and onwards.

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

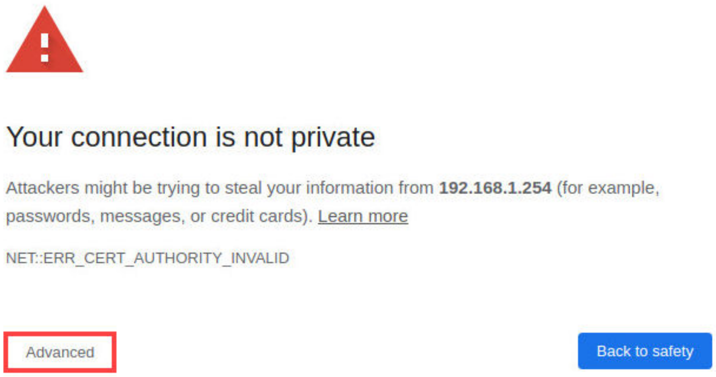


2. Double-click the **Chromium Web Browser** icon located on the desktop.

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.



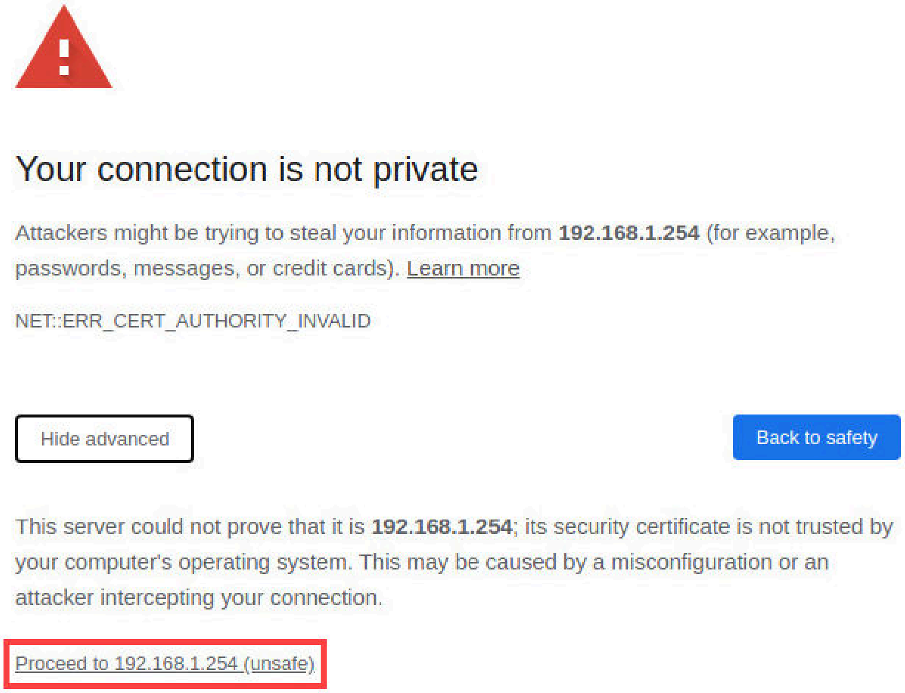
Your connection is not private

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

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)**.



Your connection is not private

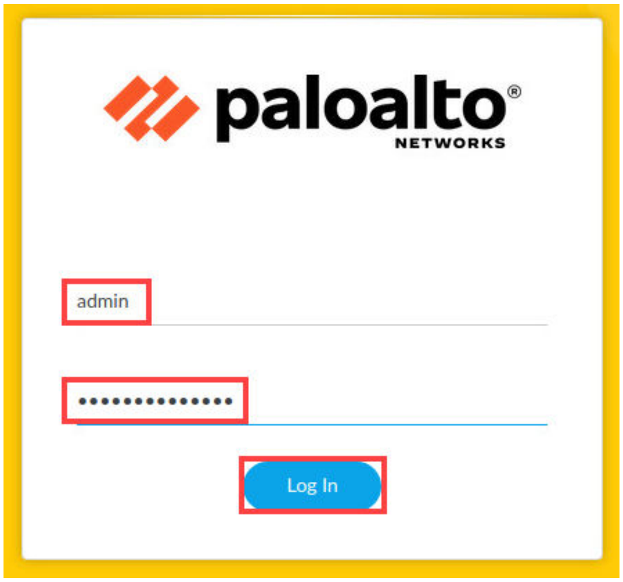
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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)

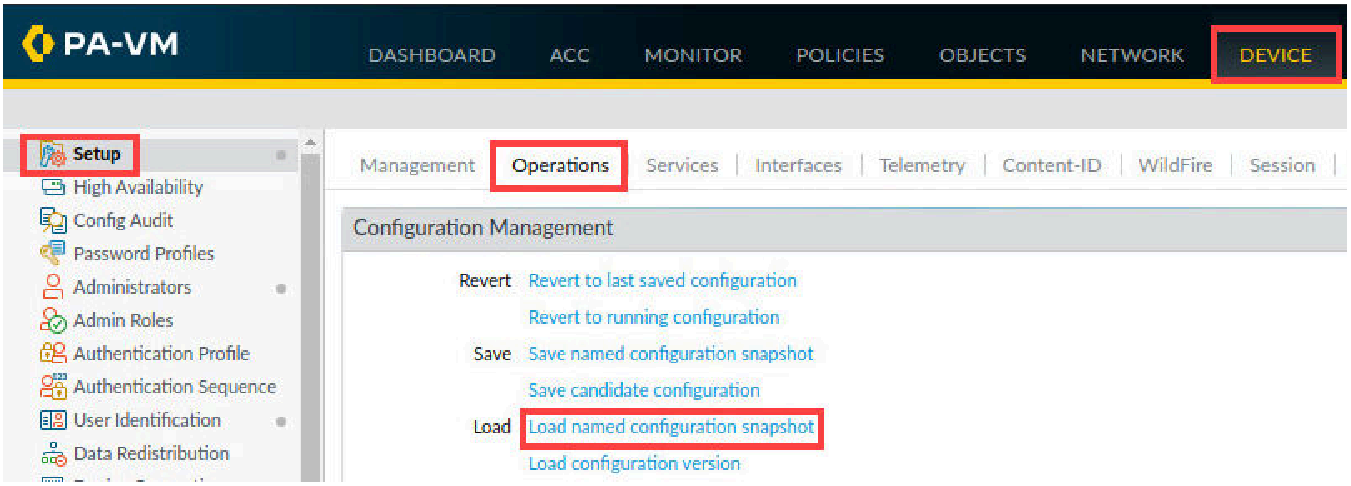
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!`**.



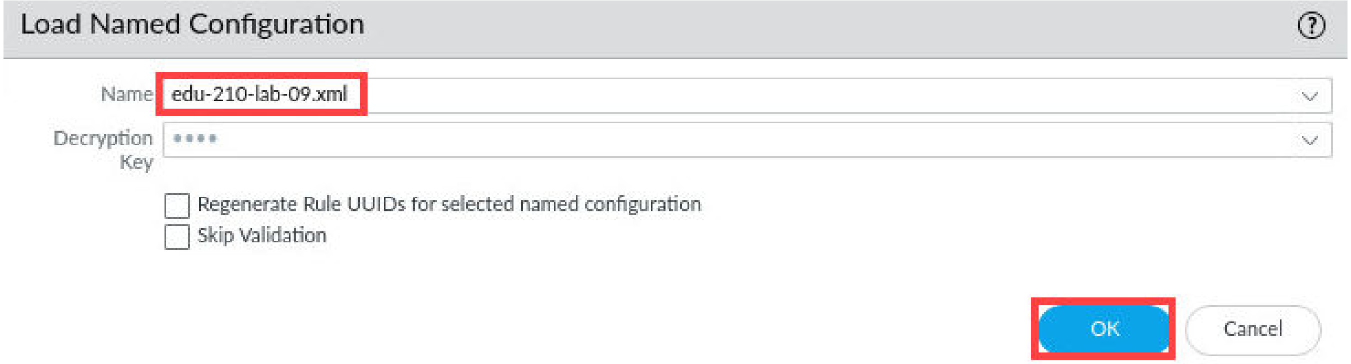
admin

••••••••••••••

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-09.xml** from the *Name* dropdown box and click **OK**.



Load Named Configuration

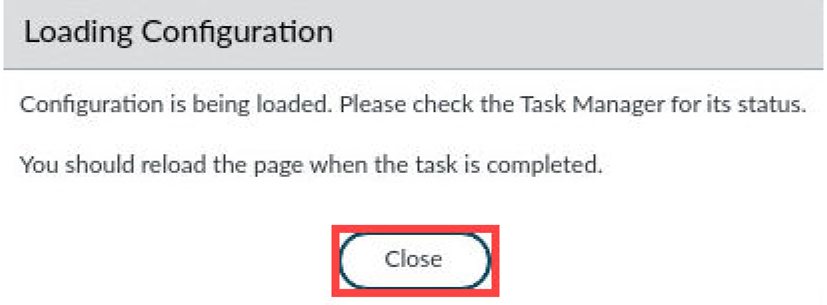
Name: edu-210-lab-09.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

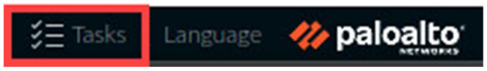
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



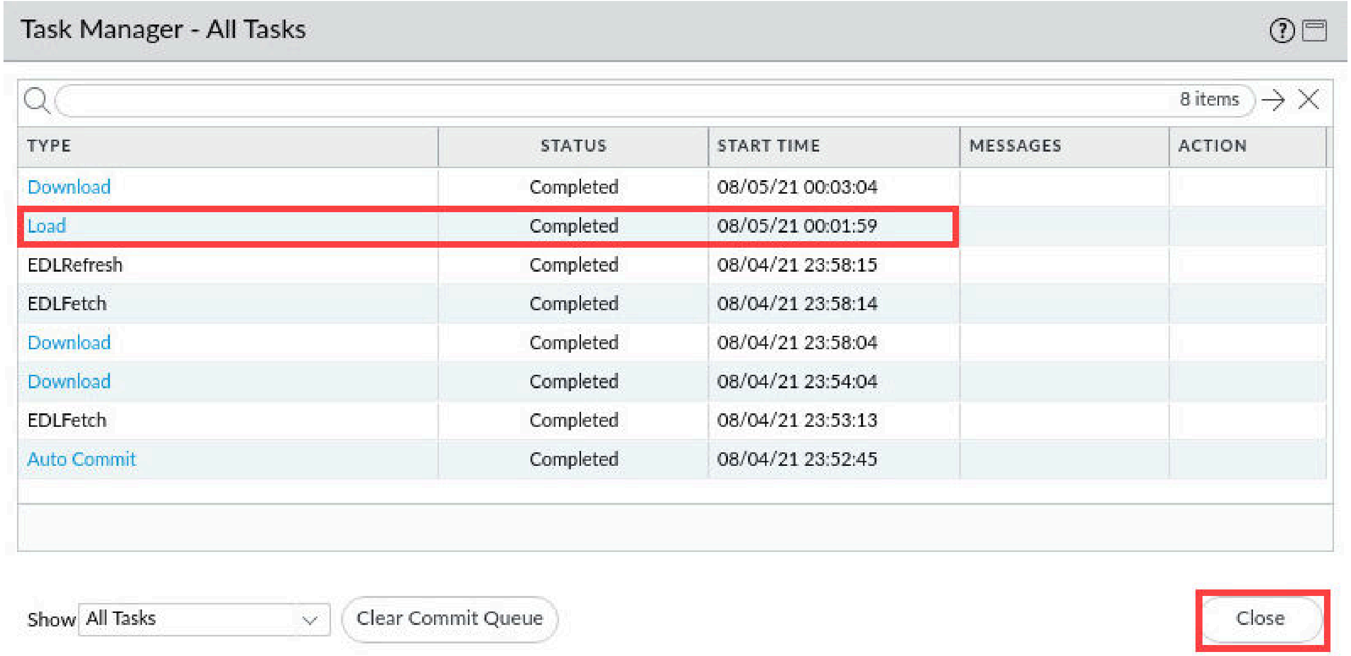
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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

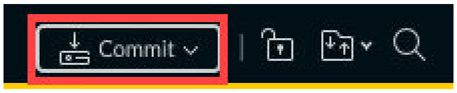


11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

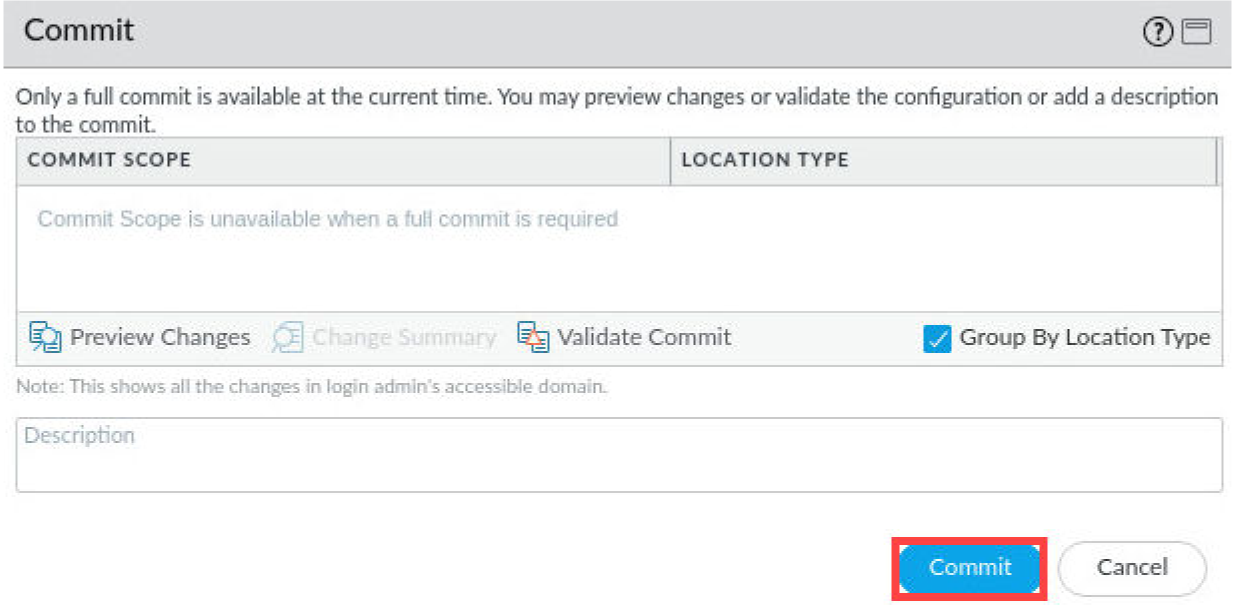


TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13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

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.

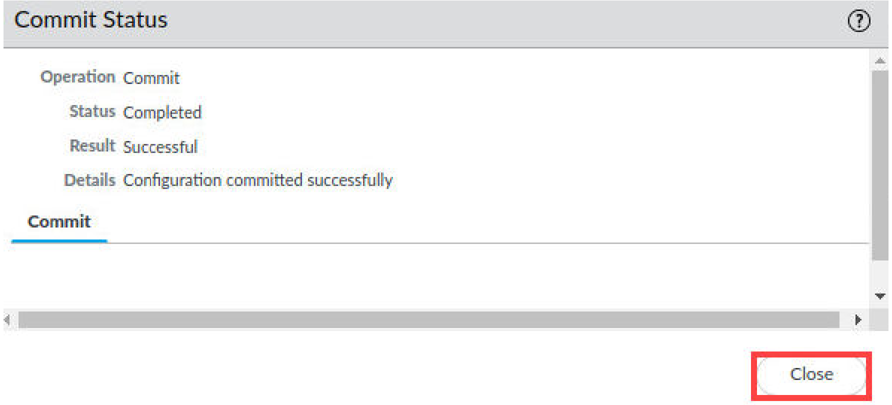


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope is unavailable when a full commit is required

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

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



Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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.

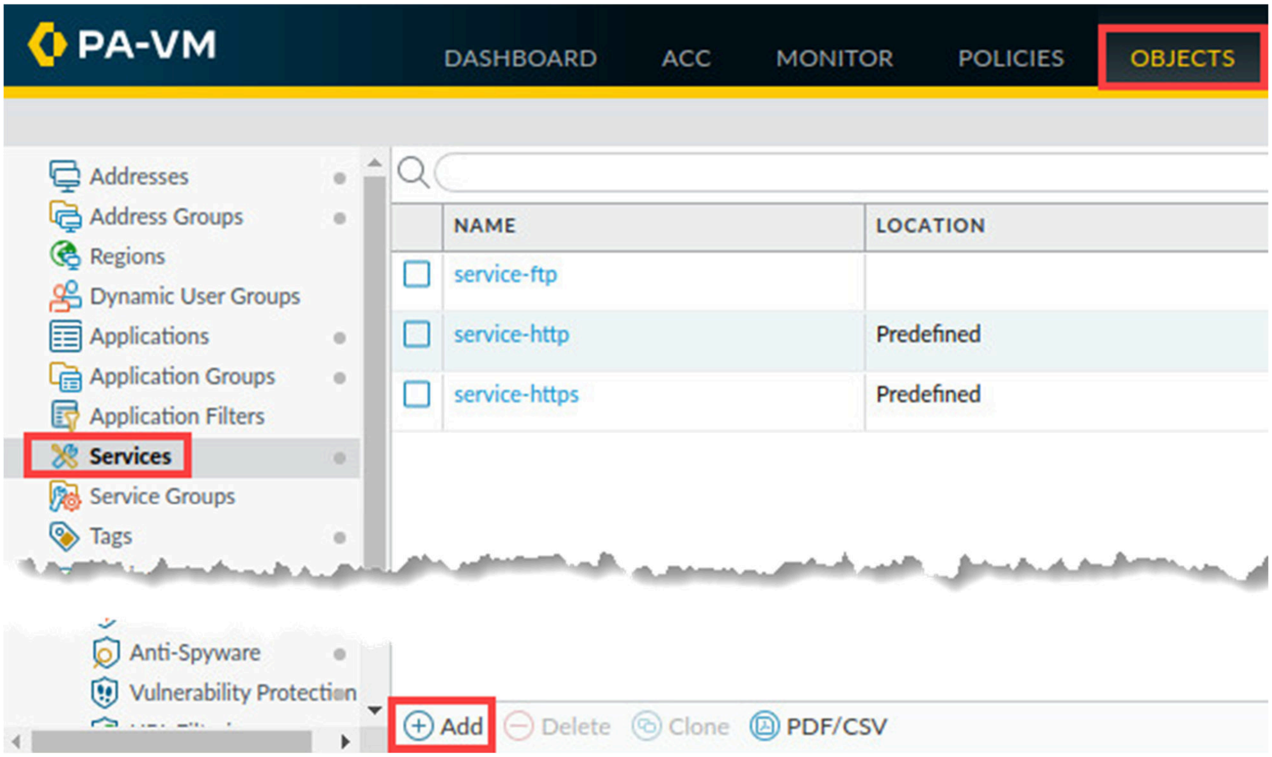
16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create a Custom Service Object for HTTP

In some networks, servers run common applications on non-standard ports: for example, running a web server on TCP port 8080 instead of TCP port 80. Palo Alto firewalls expect to see HTTP traffic running on the standard TCP port 80 and will block HTTP traffic that is not running on the application default port. To allow this type of non-standard port traffic, you can create a service object and use it as part of your Security policy rule definition.

In this section, you will create a custom service for TCP port 8080. You will add this custom service to the Security policy later in this lab exercise.

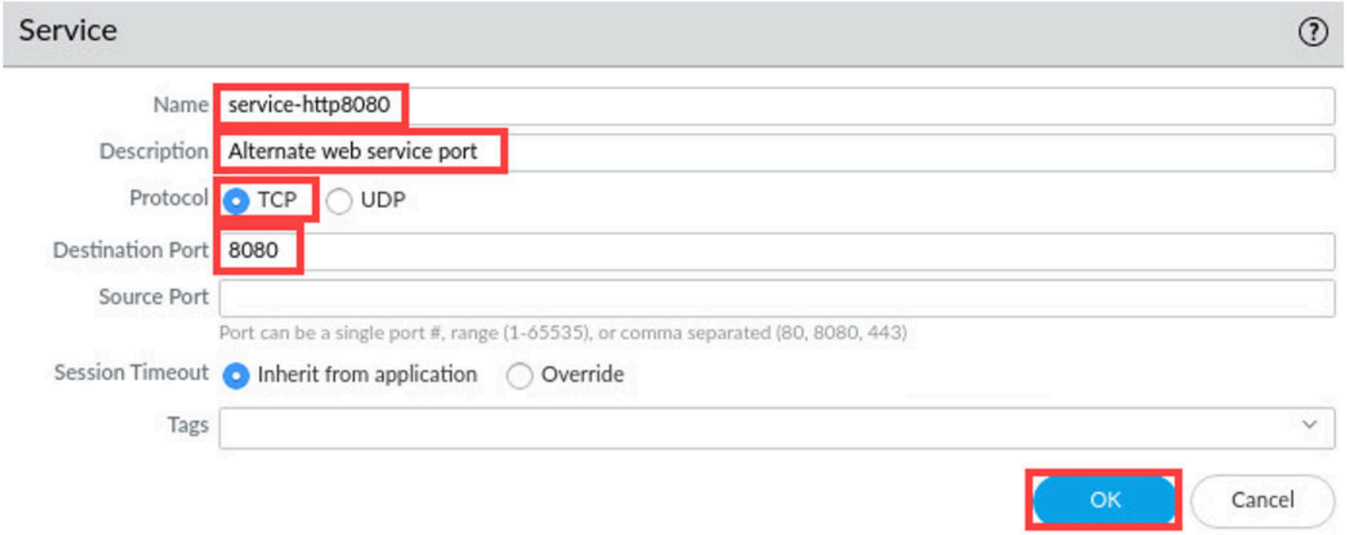
1. Navigate to **Objects > Services**. Click **Add** at the bottom of the *Services* window.



NAME	LOCATION
service-ftp	
service-http	Predefined
service-https	Predefined

2. In the *Service* window, configure the following. Click **OK**.

Parameter	Value
Name	`service-http8080`
Description	`Alternate web service port.`
Protocol	TCP
Destination Port	`8080`



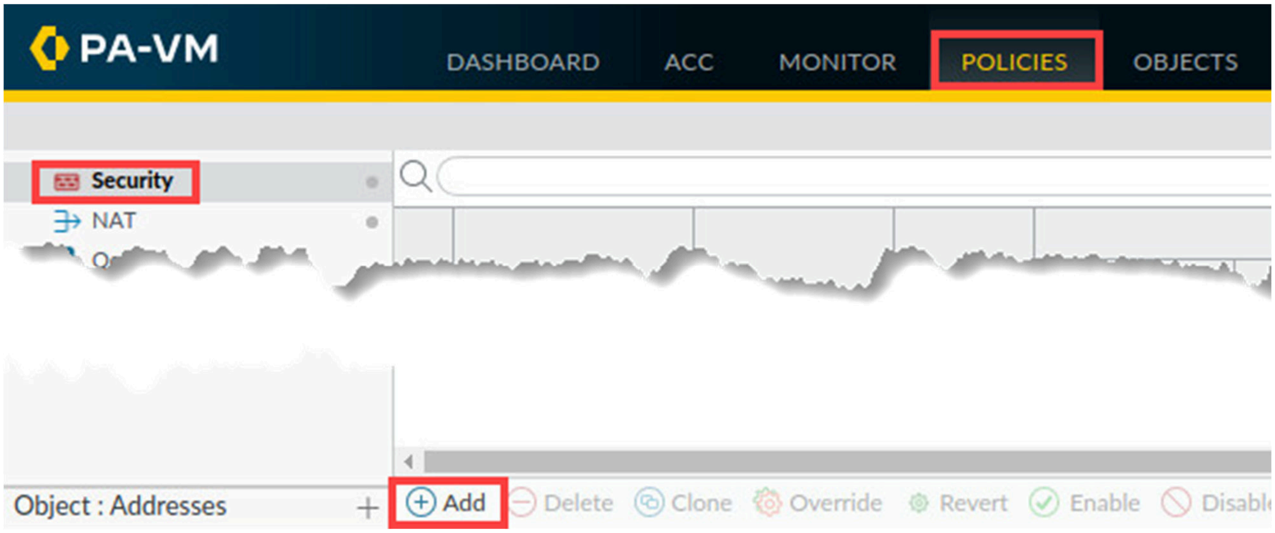
Name: service-http8080
Description: Alternate web service port
Protocol: ● TCP ○ UDP
Destination Port: 8080
Source Port:
Port can be a single port #, range (1-65535), or comma separated (80, 8080, 443)
Session Timeout: ● Inherit from application ○ Override

3. Leave the firewall open and continue to the next task.

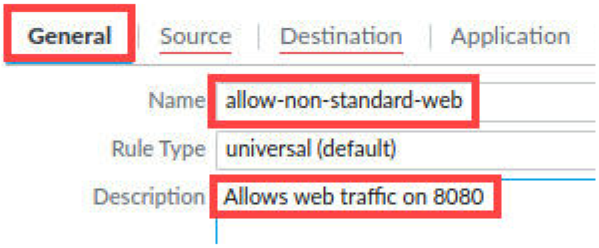
1.3 Add the New Service to the Security Policy

In this section, you will add a security policy rule to enable the firewall to match and pass web-browsing traffic using the non-standard TCP port 8080.

1. In the web interface, select **Policies > Security**. Click **Add** at the bottom of the security policy window.



2. On the *General* tab, type **`allow-non-standard-web`** as the *Name*. For *Description*, enter **`Allows web traffic on 8080.`**



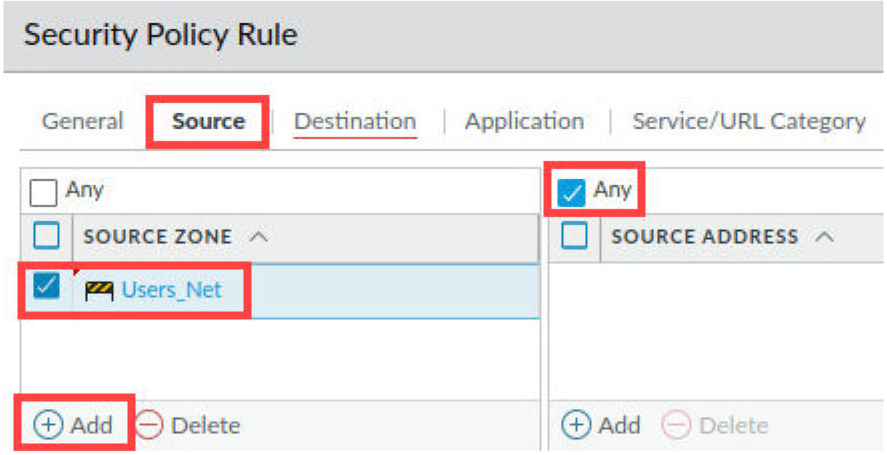
Name: allow-non-standard-web

Rule Type: universal (default)

Description: Allows web traffic on 8080

3. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	Users_Net
Source Address	Any


Security Policy Rule

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

□ Any

SOURCE ZONE

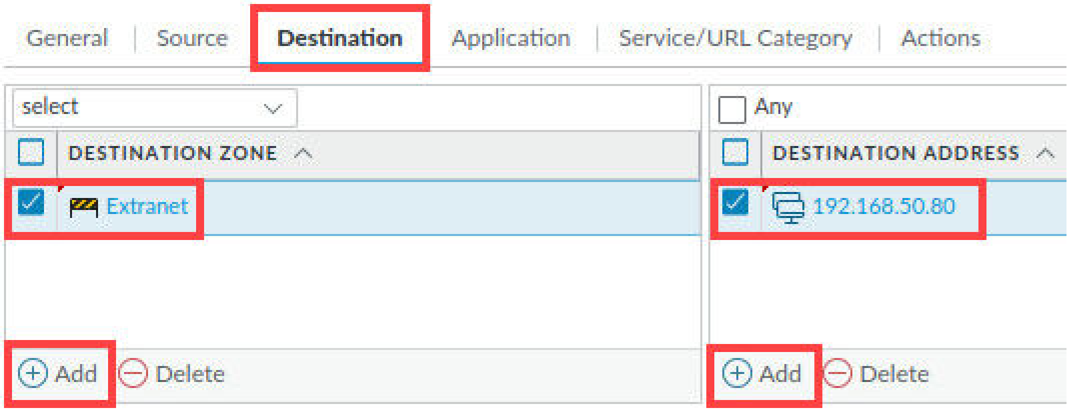
☑ Users_Net

☑ Any

SOURCE ADDRESS

4. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Extranet
Destination Address	`192.168.50.80`


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

select

DESTINATION ZONE

☑ Extranet

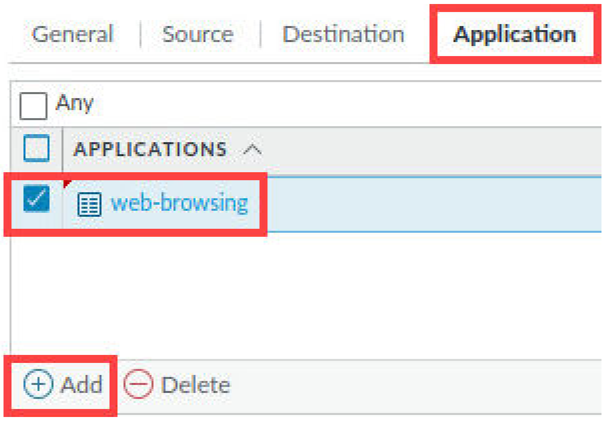
□ Any

DESTINATION ADDRESS

☑ 192.168.50.80

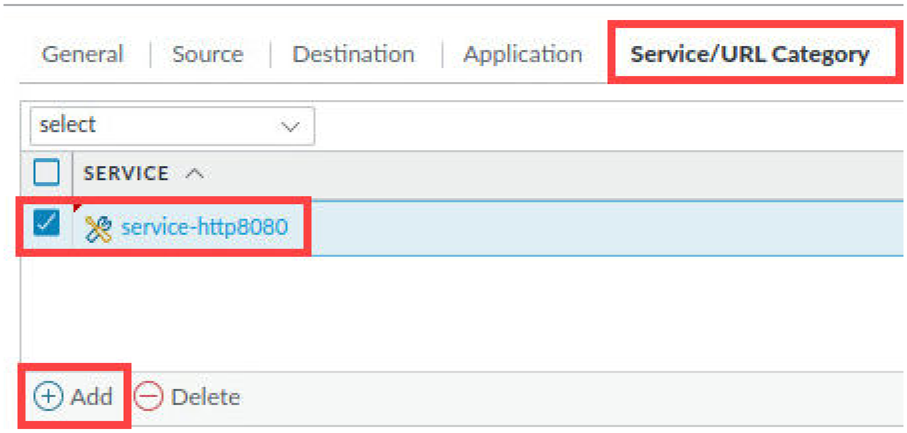
5. Click the **Application** tab and verify the following:

Parameter	Value
Applications	Web-Browsing



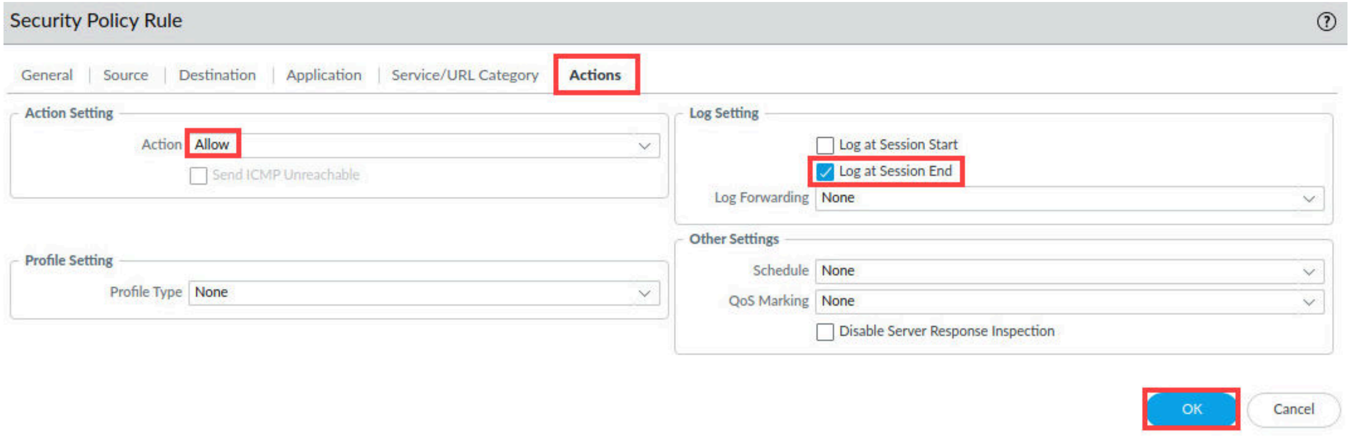
6. Click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	service-http8080



7. Click the **Actions** tab and verify the following. Click **OK**.

Parameter	**Value**
Action	**Allow**
Log Setting	**Log at Session End**



Security Policy Rule

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

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

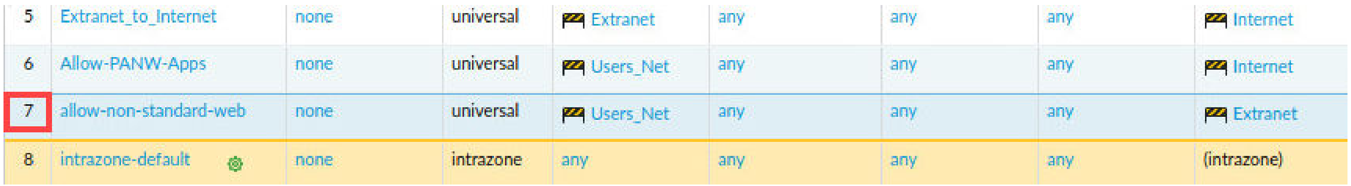
Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

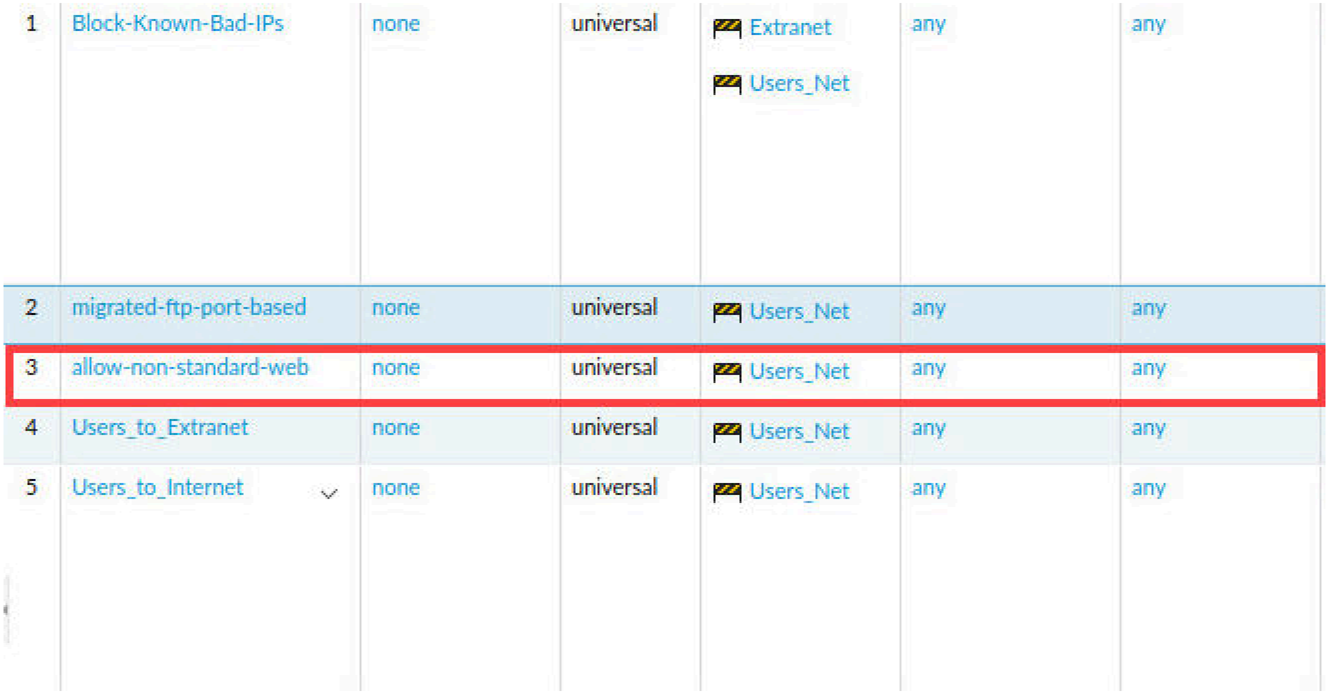
OK Cancel

8. Select, but do not open, the **allow-non-standard-web** rule in the security policy.



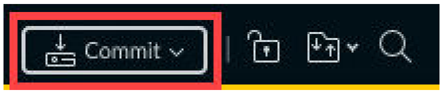
5	Extranet_to_Internet	none	universal	Extranet	any	any	any	Internet
6	Allow-PANW-Apps	none	universal	Users_Net	any	any	any	Internet
7	allow-non-standard-web	none	universal	Users_Net	any	any	any	Extranet
8	intrazone-default	none	intrazone	any	any	any	any	(intrazone)

9. Use your mouse pointer to drag-and-drop the **allow-non-standard-web** rule to just above the **Users_to_Extranet** rule.

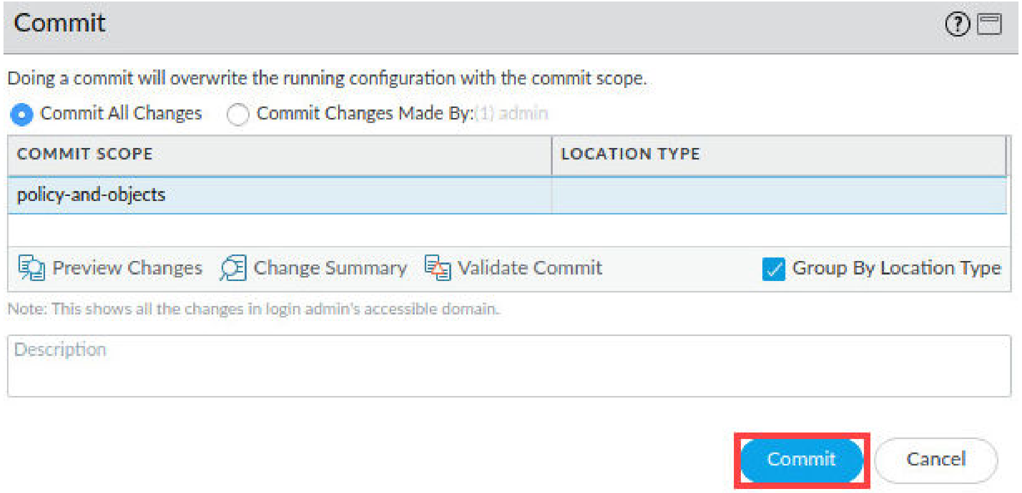


1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any	any
2	migrated-ftp-port-based	none	universal	Users_Net	any	any
3	allow-non-standard-web	none	universal	Users_Net	any	any
4	Users_to_Extranet	none	universal	Users_Net	any	any
5	Users_to_Internet	none	universal	Users_Net	any	any

10. Click the **Commit** button at the upper-right of the web interface.



11. In the *Commit* window, click **Commit**.


Commit

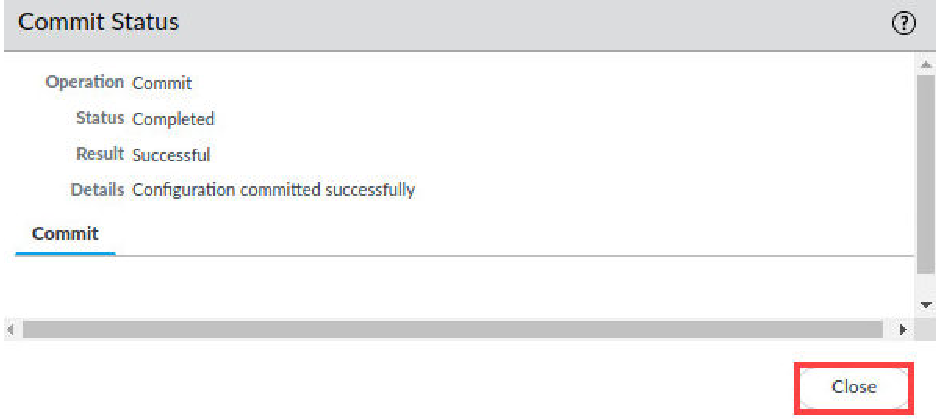
Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

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

12. Wait until the *Commit* process is complete. Click **Close**.


Commit Status

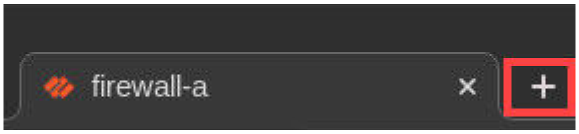
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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

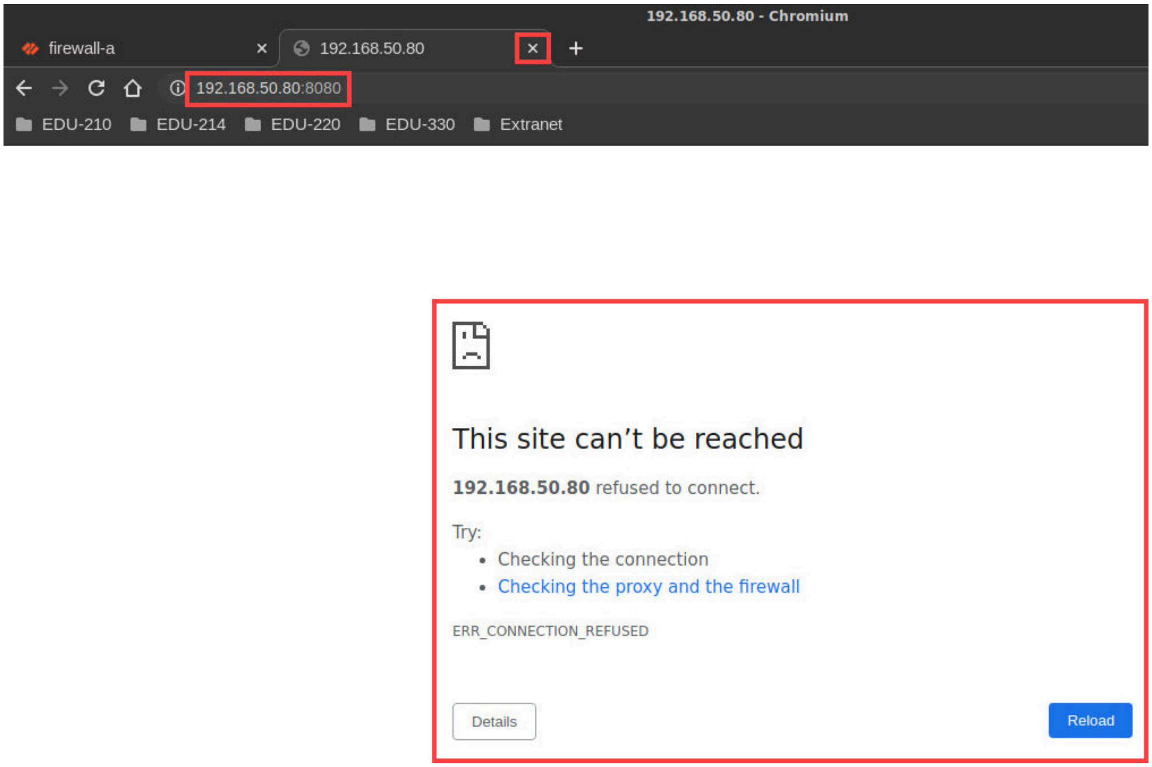
1.4 Test Access to the Web Server on Port 8080

In this section, you will test whether the security policy allows access to the web server running on the non-standard TCP port 8080.

1. Open a new tab in **Chromium**.



2. Type **`http://192.168.50.80:8080`** and press **Enter**. The connection will fail because the web server is not using port **8080**. Close the *Chromium* tab after the connection fails.



This site can't be reached

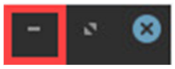
192.168.50.80 refused to connect.

Try:

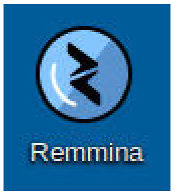
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

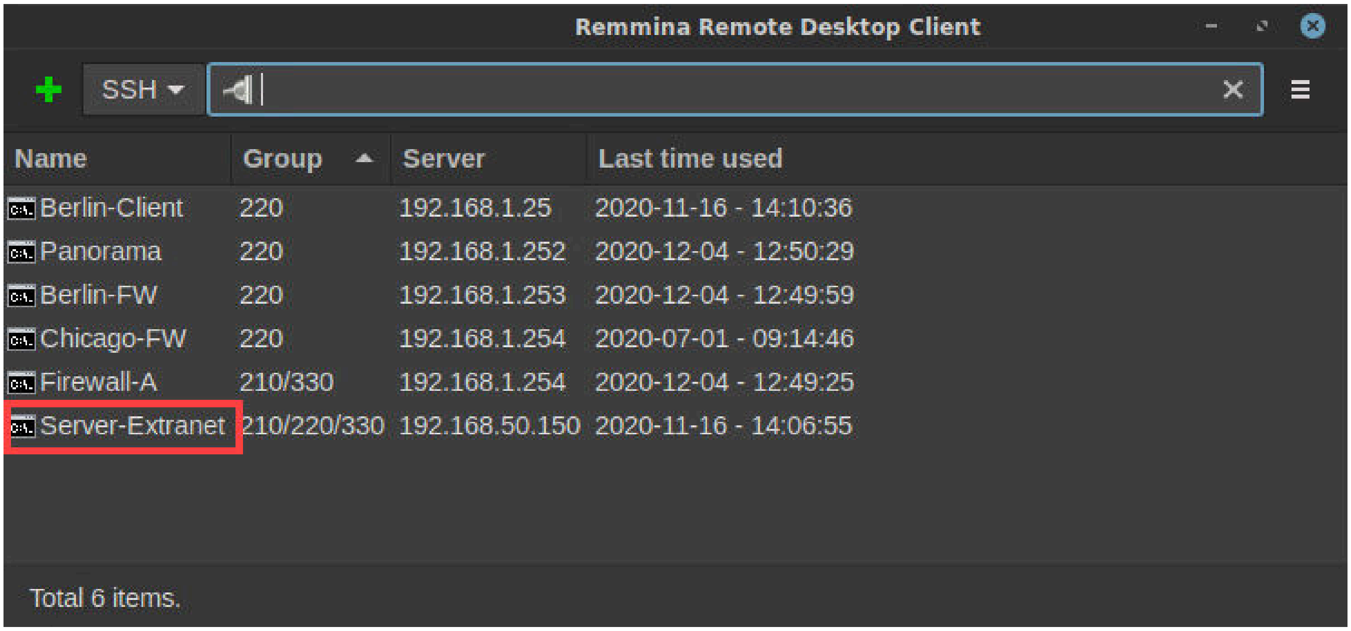
3. Minimize the *Palo Alto Networks Firewall*.



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



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



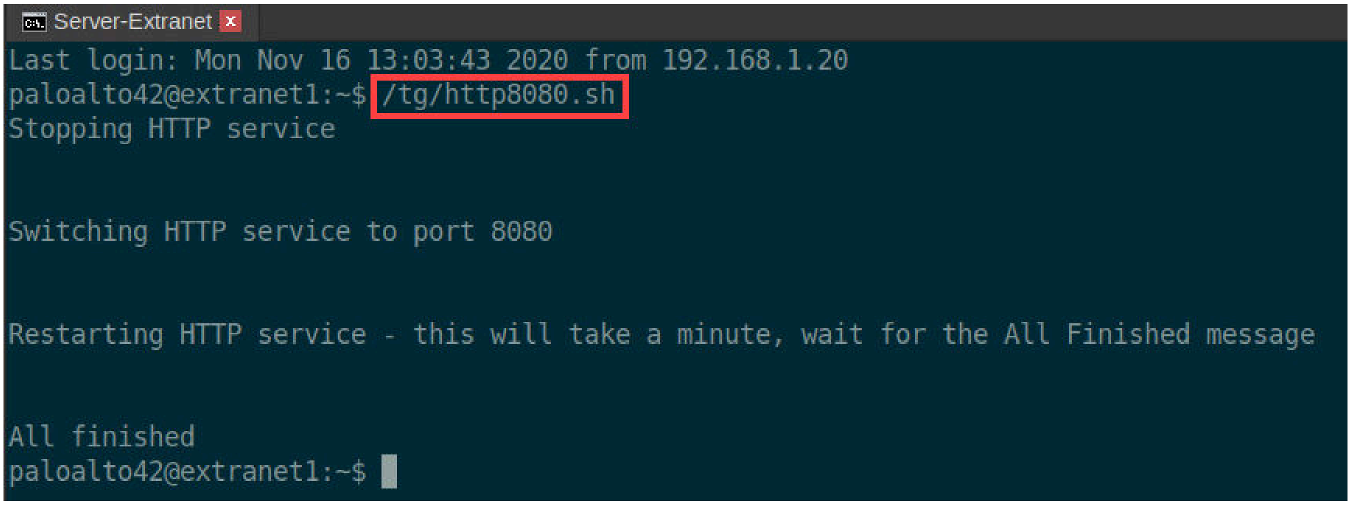
Name	Group	Server	Last time used
Berlin-Client	220	192.168.1.25	2020-11-16 - 14:10:36
Panorama	220	192.168.1.252	2020-12-04 - 12:50:29
Berlin-FW	220	192.168.1.253	2020-12-04 - 12:49:59
Chicago-FW	220	192.168.1.254	2020-07-01 - 09:14:46
Firewall-A	210/330	192.168.1.254	2020-12-04 - 12:49:25
Server-Extranet	210/220/330	192.168.50.150	2020-11-16 - 14:06:55

Please Note

This script will connect you to the Extranet lab server using SSH.

6. Run the following command to change the HTTP service port from 80 to 8080.

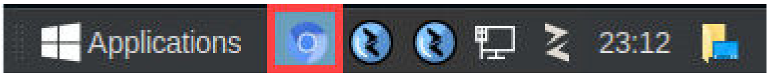
```
paloalto42@extranet1:~$ /tg/http8080.sh <Enter>
```



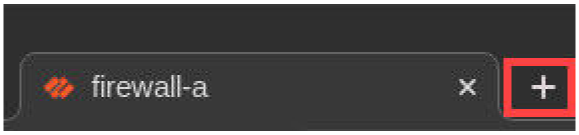
```
Last login: Mon Nov 16 13:03:43 2020 from 192.168.1.20
paloalto42@extranet1:~$ /tg/http8080.sh
Stopping HTTP service


Switching HTTP service to port 8080


Restarting HTTP service - this will take a minute, wait for the All Finished message


All finished
paloalto42@extranet1:~$
```

7. Leave the **Remmina** connection to the *Extranet* server open.

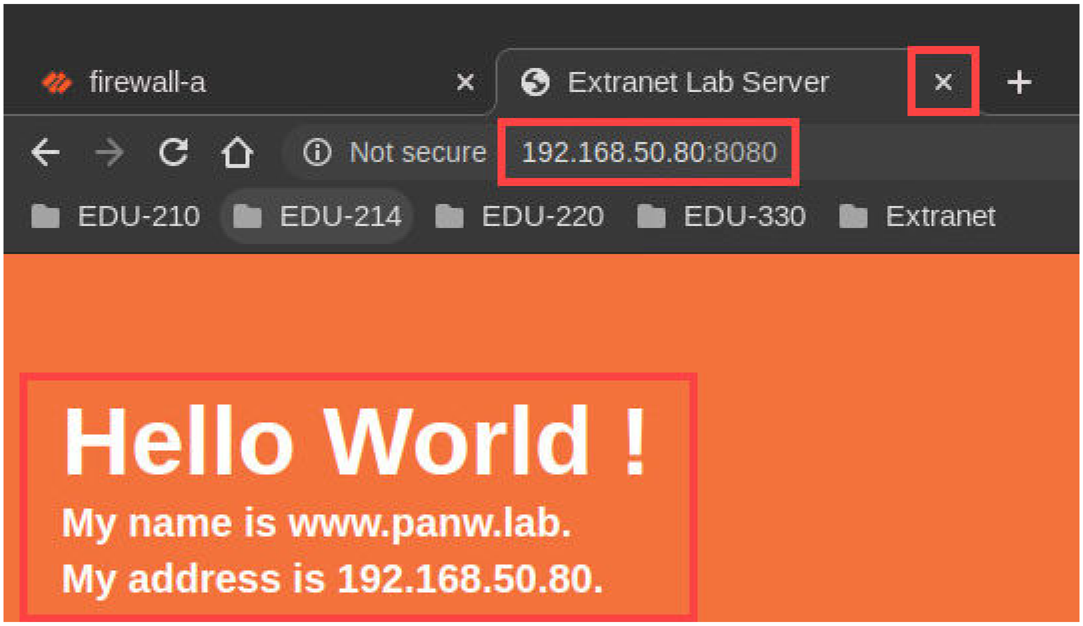
8. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.



9. Open a new tab in **Chromium**.



10. Type **`http://192.168.50.80:8080`** and press **Enter**. You should be connected to the server now that the service port has been changed to *8080*. Close the **Chromium** tab.

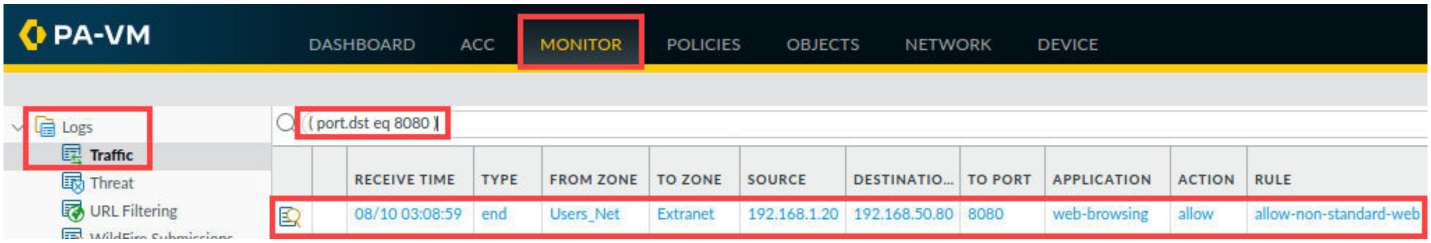


Hello World !

My name is www.panw.lab.

My address is 192.168.50.80.

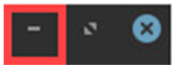
11. In the firewall web interface, select **Monitor > Logs > Traffic.** Clear any filters you have in place. Find the log entries for the web traffic to port *8080*. You can use the filter **`( port.dst eq 8080 )`** to find the log entry.



(port.dst eq 8080)

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
08/10 03:08:59	end	Users_Net	Extranet	192.168.1.20	192.168.50.80	8080	web-browsing	allow	allow-non-standard-web

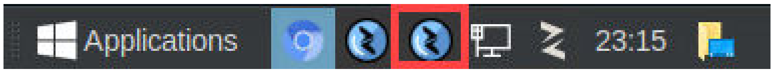
12. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



1.5 Revert the Web Server to Port 80

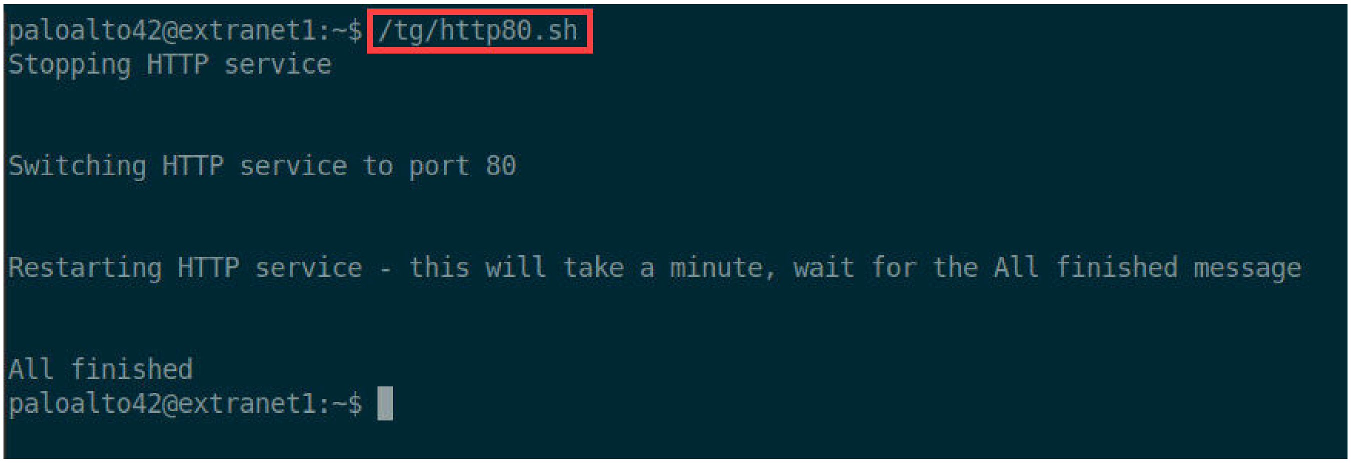
In this section, you will run a script on the Extranet host to configure the web server to listen on its standard TCP port 80. You also will remove the Security policy rule that enabled web server access on the non-standard port.

1. Reopen *Remmina* by clicking on the **Remmina** icon in the taskbar.



2. Run the following command to change the *HTTP service port* from **8080** to **80**.

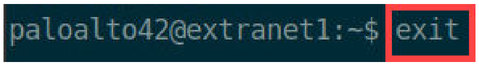
```
paloalto42@extranet1:~$ /tg/http80.sh <Enter>
```



```
paloalto42@extranet1:~$ /tg/http80.sh
Stopping HTTP service


Switching HTTP service to port 80


Restarting HTTP service - this will take a minute, wait for the All finished message


All finished
paloalto42@extranet1:~$ 
```

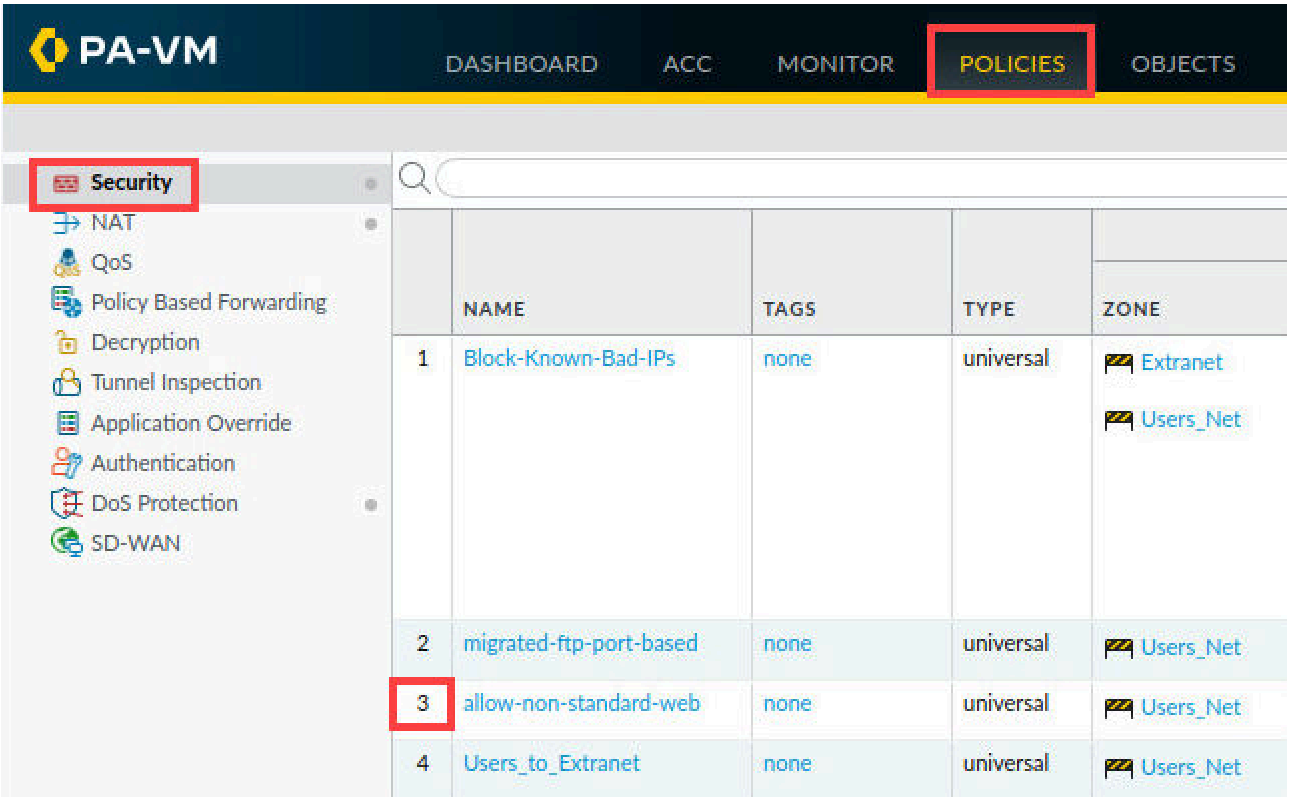
3. Close your *Remmina* connection to the **Extranet server** by entering the command below.

```
paloalto42@extranet1:~$ exit <Enter>
```



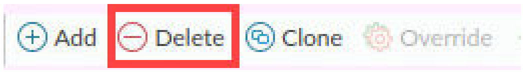
```
paloalto42@extranet1:~$ exit
```

4. In firewall web interface, select **Policies > Security**. Select, but do not open, the **allow-non-standard-web** rule in the security policy.

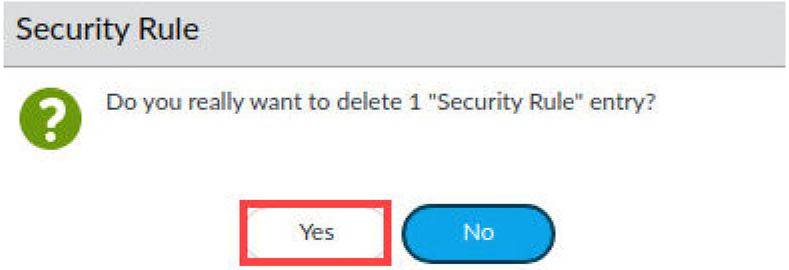


	NAME	TAGS	TYPE	ZONE
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net
2	migrated-ftp-port-based	none	universal	Users_Net
3	allow-non-standard-web	none	universal	Users_Net
4	Users_to_Extranet	none	universal	Users_Net

5. At the bottom of the window, click **Delete** to remove the rule.

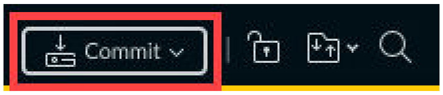


6. In the *Security Rule* window, click **Yes** to delete the allow-non-standard-web security policy.

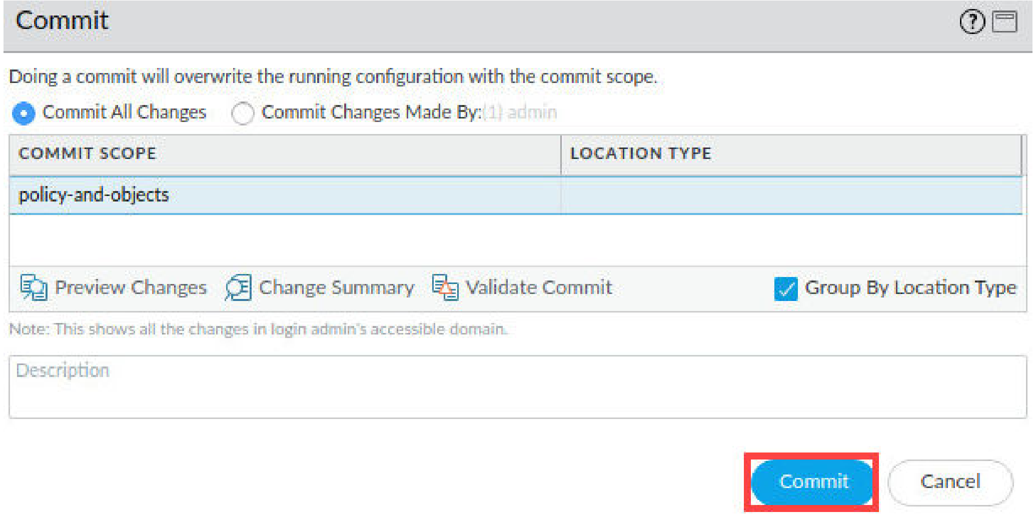

Security Rule

Do you really want to delete 1 "Security Rule" entry?

7. Click the **Commit** button at the upper-right of the web interface.



8. In the *Commit* window, click **Commit**.



Commit

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

● Commit All Changes ○ Commit Changes Made By: (1) admin

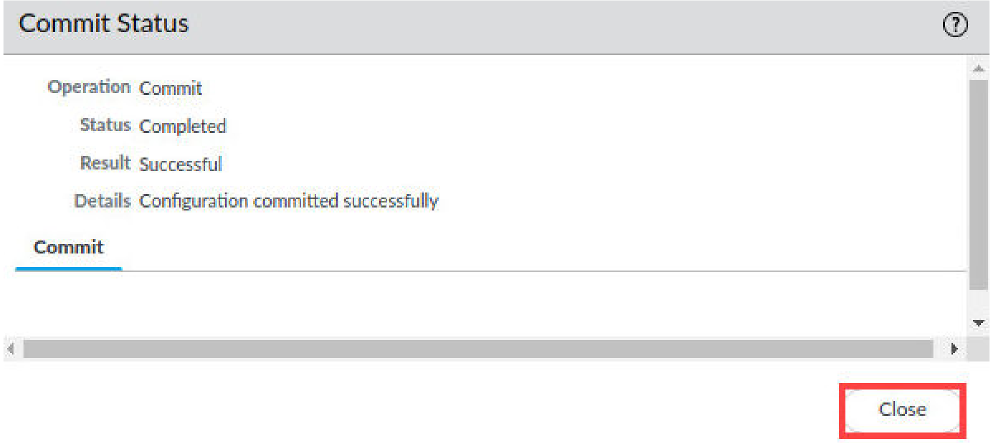
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes | Change Summary | Validate Commit | ☑ Group By Location Type

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

Description

9. Wait until the *Commit* process is complete, click **Close**.



Commit Status

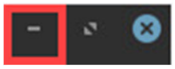
Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

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



1.6 Create an FTP Application-Based Security Policy Rule with Policy Optimizer

The goal of this exercise is to simulate the process of migrating from a port-based rule to an application-based rule. In the previous lab, you created a port-based rule that allowed FTP traffic from the Users_Net zone to the Extranet zone and then opened a session to the FTP server.

By now, the beginning of the hour should have passed, so the Policy Optimizer tool should have recorded the FTP traffic through the port-based FTP rule, which will enable you to use the Policy Optimizer tool to migrate from the port-based rule to an application-based rule.

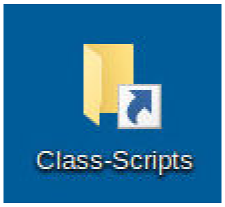
In this section, you will use the Policy Optimizer tool's cloning method to create an application-based rule to match and allow FTP traffic from the Users_Net zone to the Extranet zone.

⚠ To complete this task, you will want to be closer to the top of the hour. If you start at the bottom of the hour, please note that the lab will possibly take about two hours to complete due to waiting for the top of the hour.

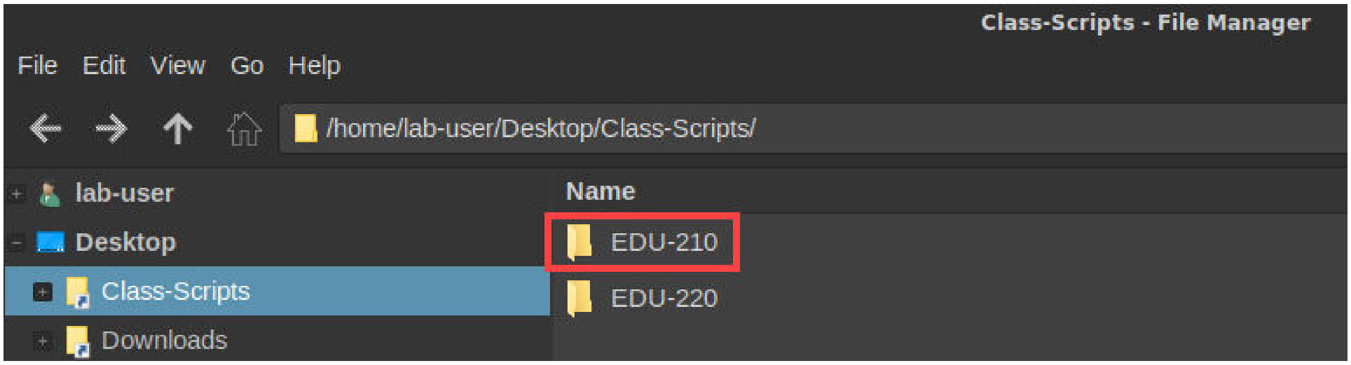
It is recommended that you start this lab 30 minutes before the top of the hour to minimize your wait time to complete this lab.

If you would like to skip this task without using the Policy Optimizer, and manually add the FTP Application based policy, please skip to task 9.7.

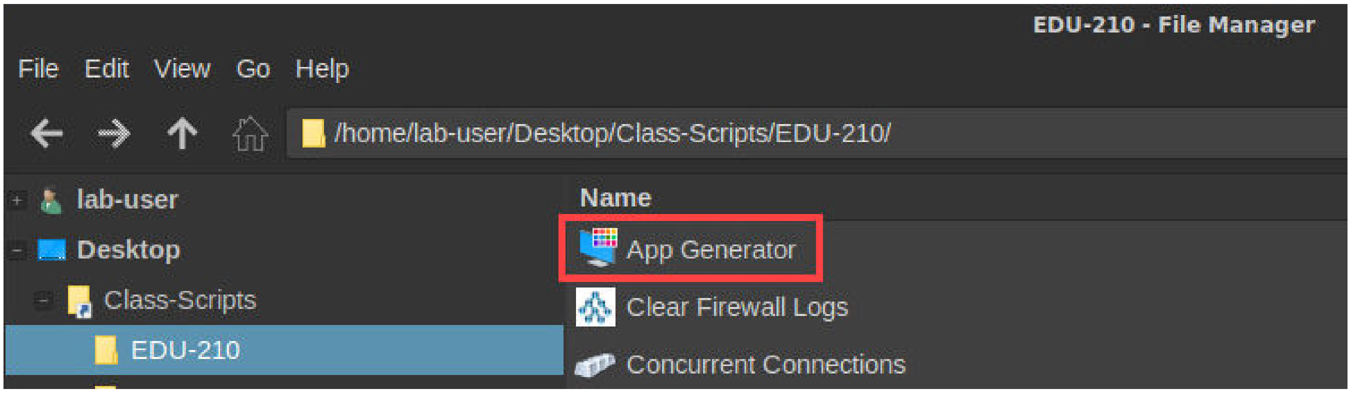
1. On the *client desktop*, double-click the folder for **Class-Scripts**.



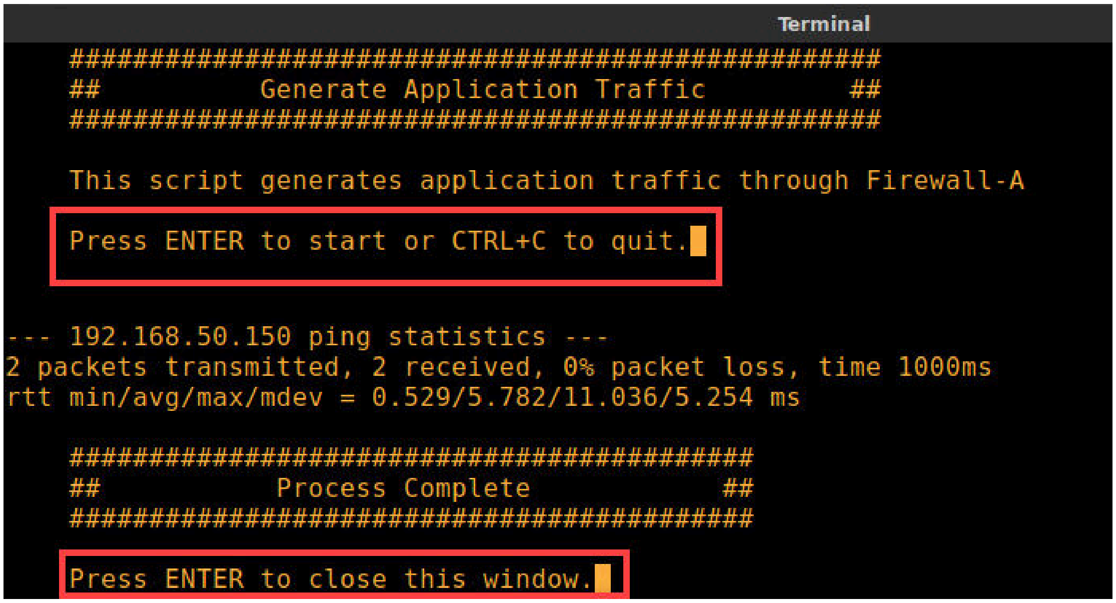
2. Open the **EDU-210** folder.



3. Double-click the icon for **App Generator**.

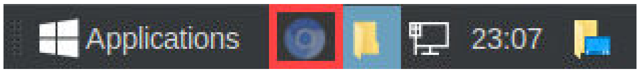


4. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes, press **Enter**.

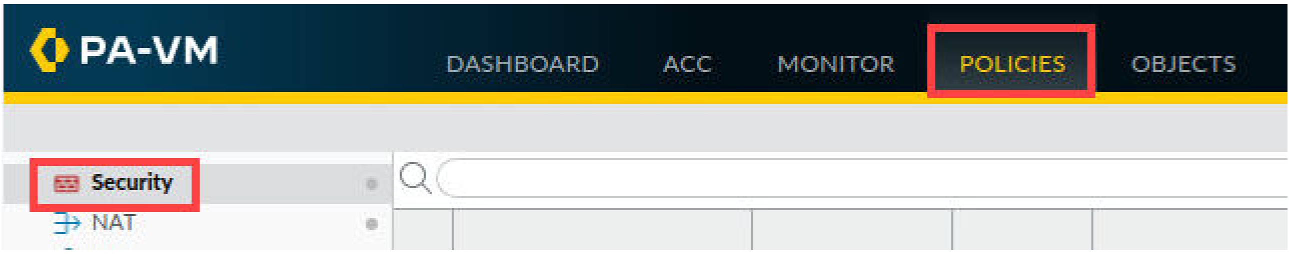


```
    ###################################################
    ##          Generate Application Traffic         ##
    ###################################################

    This script generates application traffic through Firewall-A

    Press ENTER to start or CTRL+C to quit.


--- 192.168.50.150 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.529/5.782/11.036/5.254 ms

    ###########################################
    ##            Process Complete           ##
    ###########################################

    Press ENTER to close this window.
```

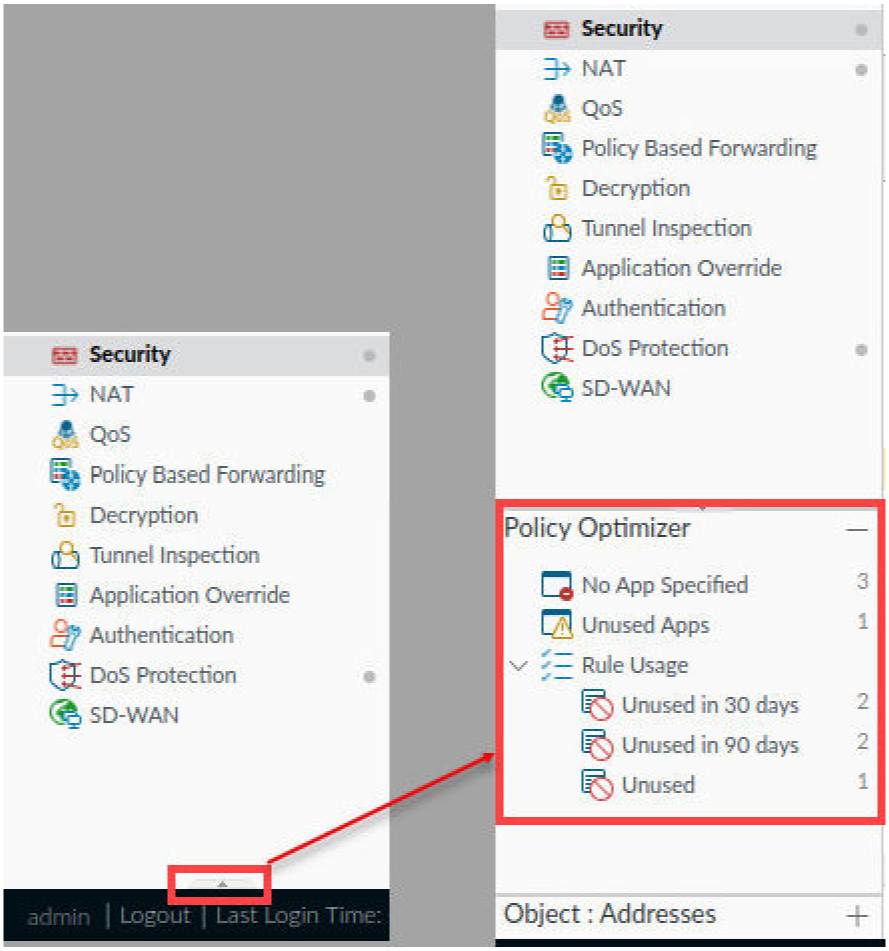
5. Reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.



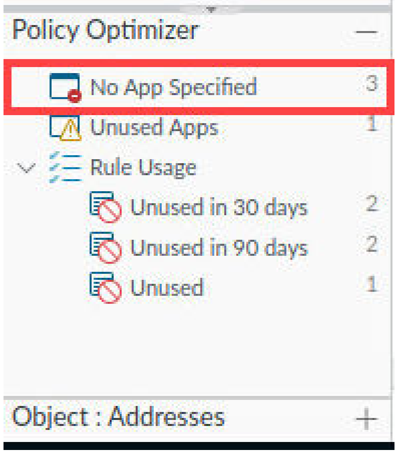
6. In the *firewall* interface, select **Policies > Security**.



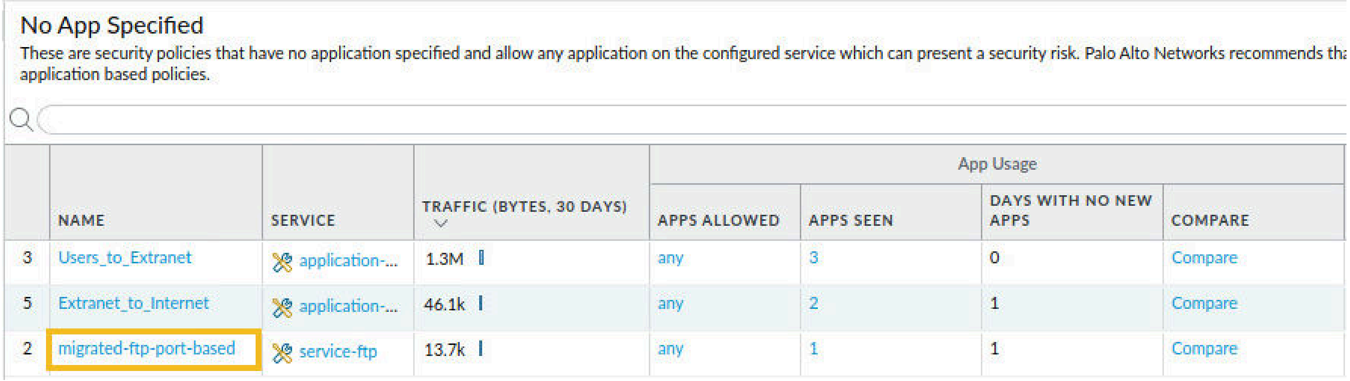
7. If necessary, open the **Policy Optimizer** panel by clicking the **Up arrow** beneath the list of policies on the left side of the web interface.



8. Select **Policy Optimizer > No App Specified**.



9. View the *No App Specified* window. If you do not see an entry for **migrated-ftp-port-based** in the list, wait until the top of the hour has passed. The firewall updates these statistics every hour, on the hour.

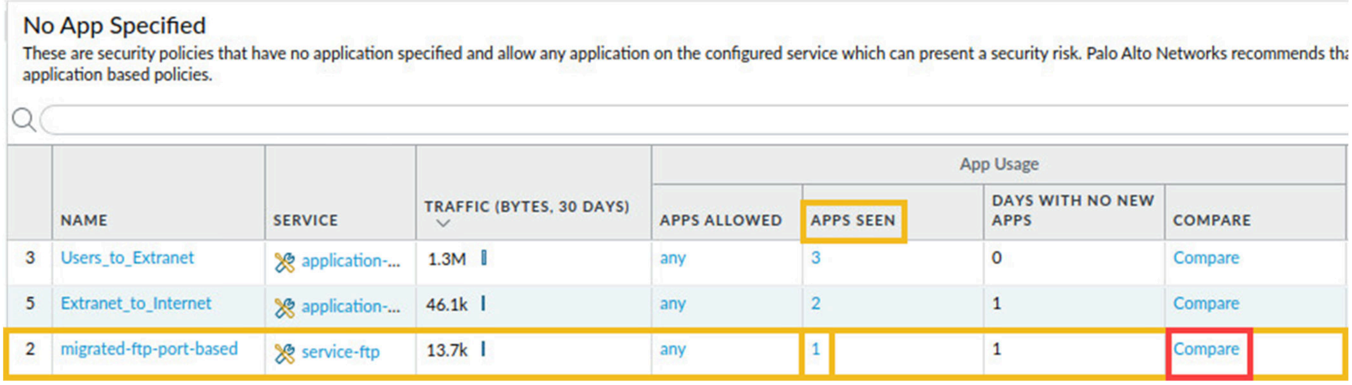


No App Specified

These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends tha application based policies.

				App Usage			
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
3	Users_to_Extranet	application-...	1.3M	any	3	0	Compare
5	Extranet_to_Internet	application-...	46.1k	any	2	1	Compare
2	migrated-ftp-port-based	service-ftp	13.7k	any	1	1	Compare

10. In the *migrated-ftp-port-based* rule, notice the number **1** in the Apps Seen column indicates that only a single application has been seen by this port-based rule. However, this window does not tell you which application. Click **Compare**.

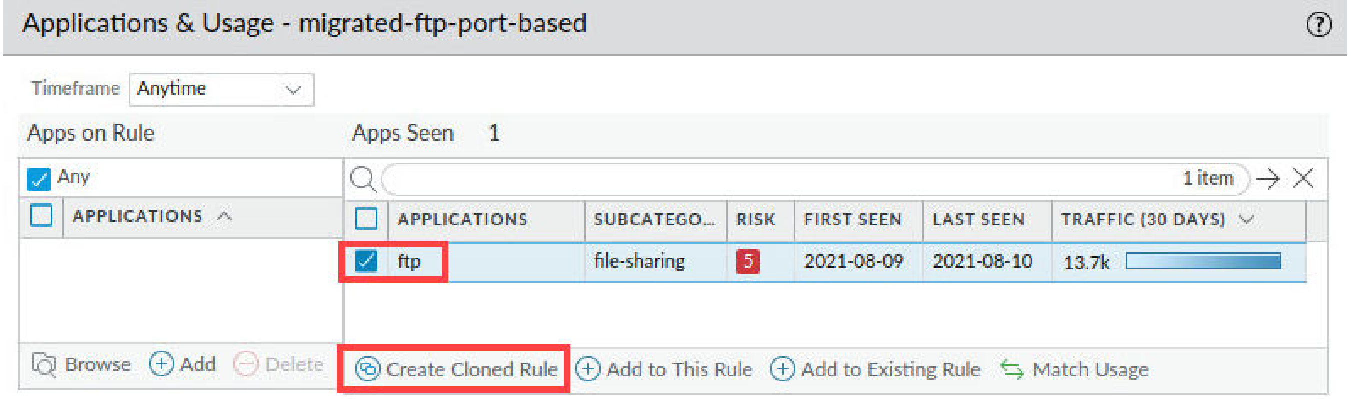


No App Specified

These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends tha application based policies.

				App Usage			
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
3	Users_to_Extranet	application-...	1.3M	any	3	0	Compare
5	Extranet_to_Internet	application-...	46.1k	any	2	1	Compare
2	migrated-ftp-port-based	service-ftp	13.7k	any	1	1	Compare

11. In the *Applications & Usage – migrated-ftp-port-based* window, notice the application **ftp** has been seen. Select the **ftp** checkbox to select the application and click **Create Cloned Rule** to create an application-based FTP rule.



Applications & Usage - migrated-ftp-port-based

Timeframe: Anytime

Apps on Rule

☑ Any

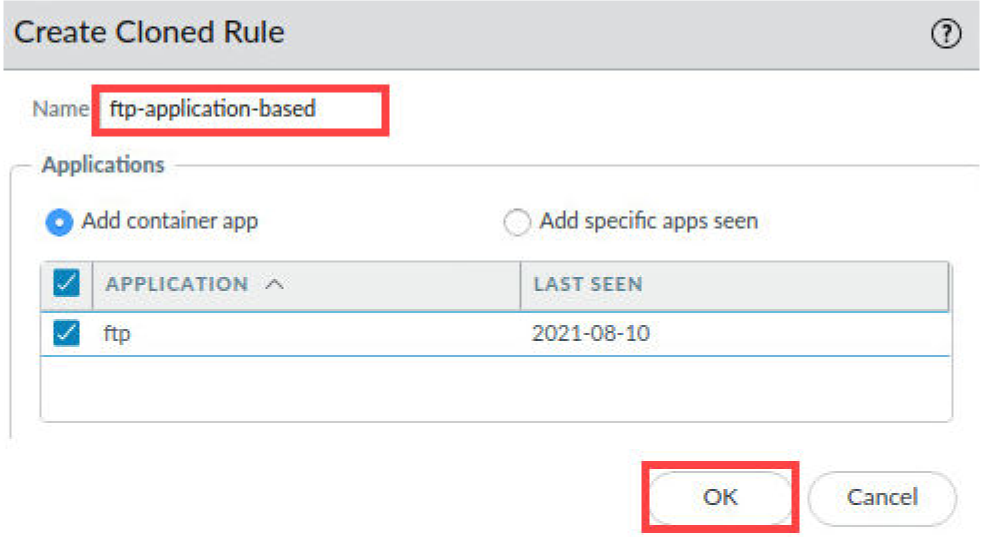
□ APPLICATIONS

Apps Seen 1

1 item

□	APPLICATIONS	SUBCATEGO...	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
☑	ftp	file-sharing	5	2021-08-09	2021-08-10	13.7k

12. In the *Clone* window, type **`ftp-application-based`** as the *Name* of the new rule. Click **OK**.



Create Cloned Rule

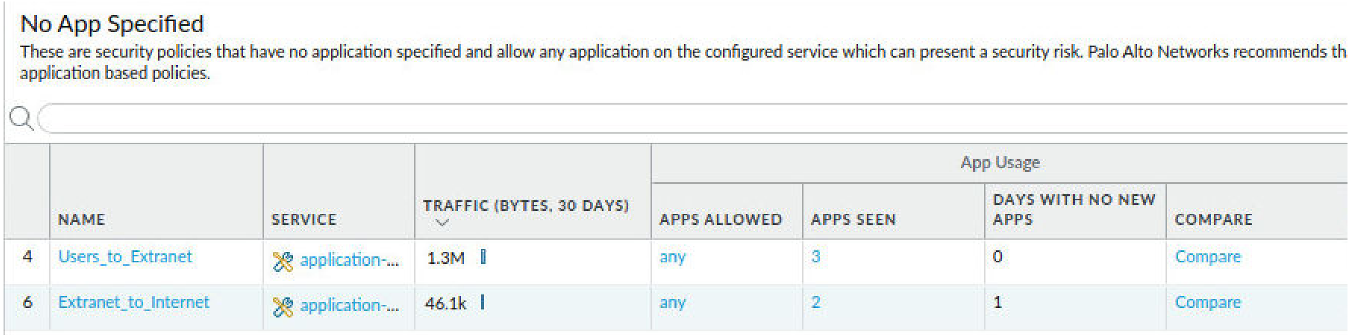
Name: ftp-application-based

Applications

● Add container app ○ Add specific apps seen

☑	APPLICATION	LAST SEEN
☑	ftp	2021-08-10

13. In the **No App Specified** window, the **`migrated-ftp-port-based`** rule is removed.



No App Specified

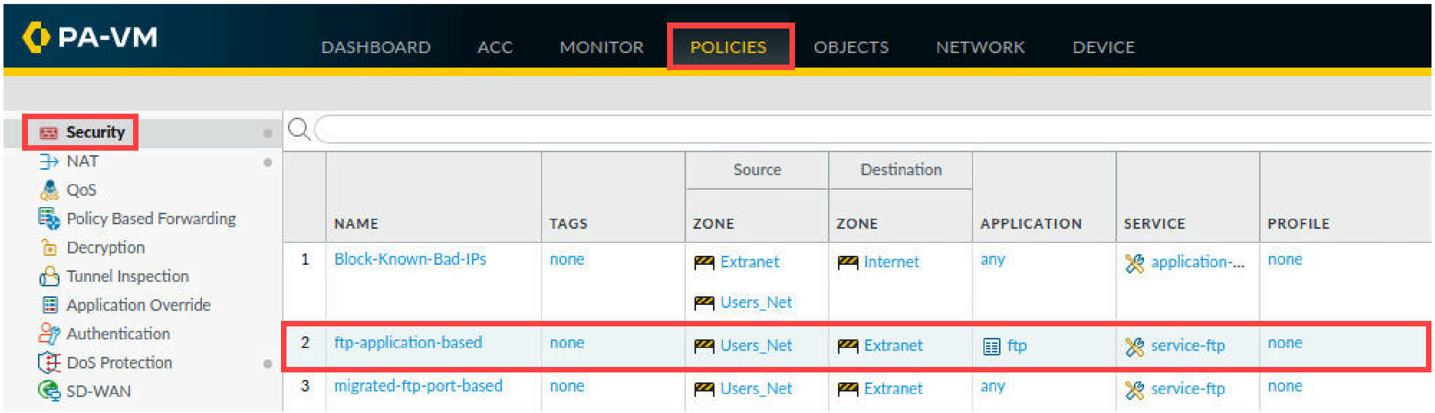
These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks recommends th application based policies.

				App Usage			
	NAME	SERVICE	TRAFFIC (BYTES, 30 DAYS)	APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
4	Users_to_Extranet	application-...	1.3M	any	3	0	Compare
6	Extranet_to_Internet	application-...	46.1k	any	2	1	Compare

Please Note

The firewall has moved the ftp application from the "migrated-ftp-port-based" rule to the new "ftp-application-based" rule.

14. Select **Policies > Security**. The new **ftp-application-based** rule has been added to your security policy.

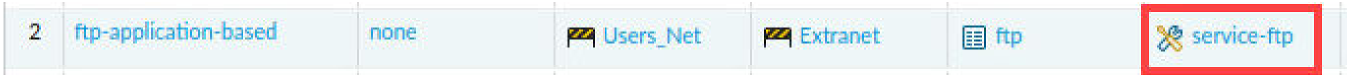


			Source	Destination			
	NAME	TAGS	ZONE	ZONE	APPLICATION	SERVICE	PROFILE
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet	any	application-...	none
2	ftp-application-based	none	Users_Net	Extranet	ftp	service-ftp	none
3	migrated-ftp-port-based	none	Users_Net	Extranet	any	service-ftp	none

Please Note

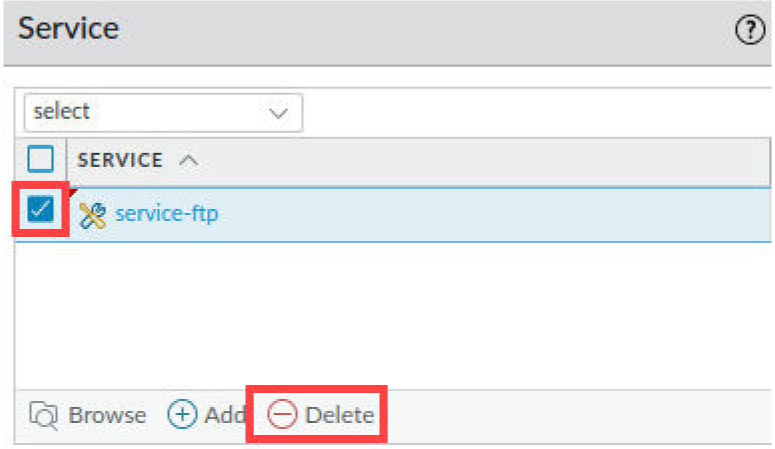
Notice the *Policy Optimizer* moved the new **ftp-application-based** rule to precede the **migrated-ftp-port-based** security rule and match *FTP traffic* before the **migrated-ftp-port-based** rule. Take note of the service listed in the service column. It is **service-ftp**.

15. On the *ftp-application-based* rule, click **service-ftp** in the *Service* column.



2	ftp-application-based	none	Users_Net	Extranet	ftp	service-ftp

16. In the *Service* window, select the **service-ftp** checkbox and then click **Delete** to delete the service.



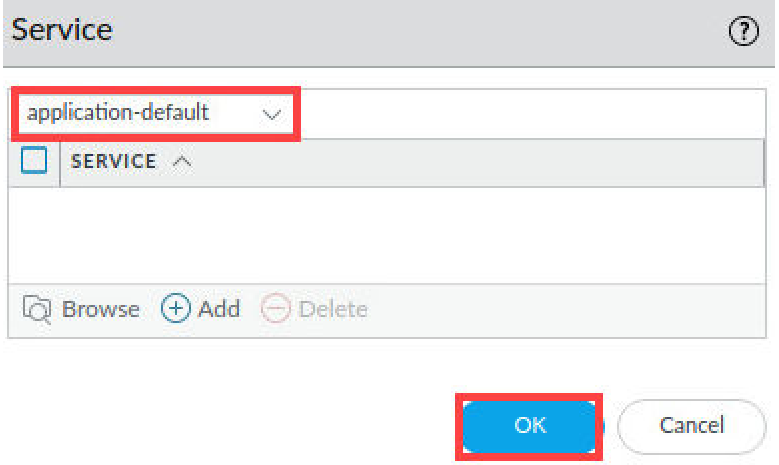
Service

select

□ SERVICE

☑ service-ftp

17. After deleting *service-ftp*, notice the service changed to **application-default**. Click **OK**.

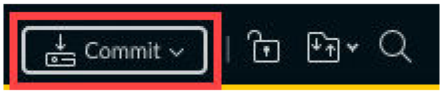


Service

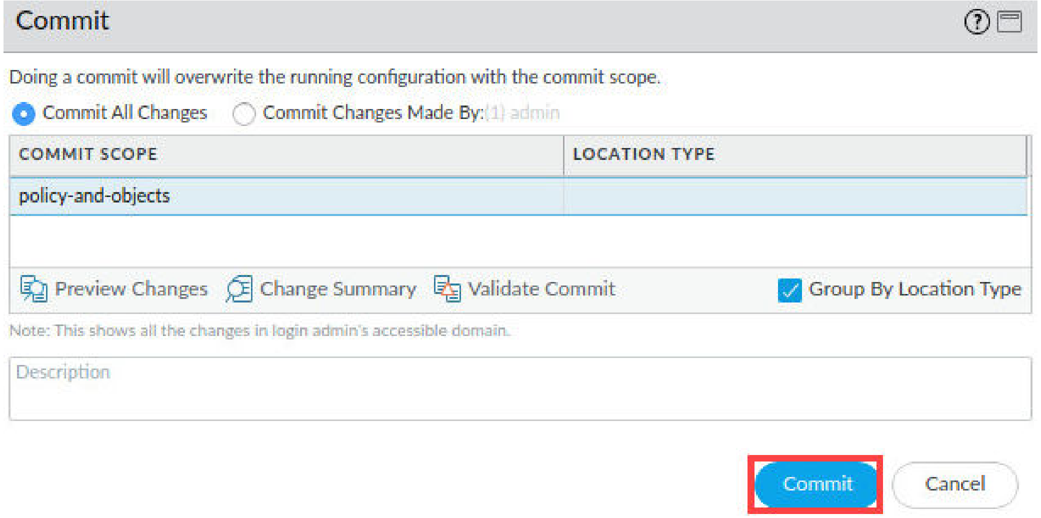
application-default

□ SERVICE

18. Click the **Commit** button at the upper-right of the web interface.



19. In the *Commit* window, click **Commit**.



Commit

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

● Commit All Changes ○ Commit Changes Made By:(1) admin

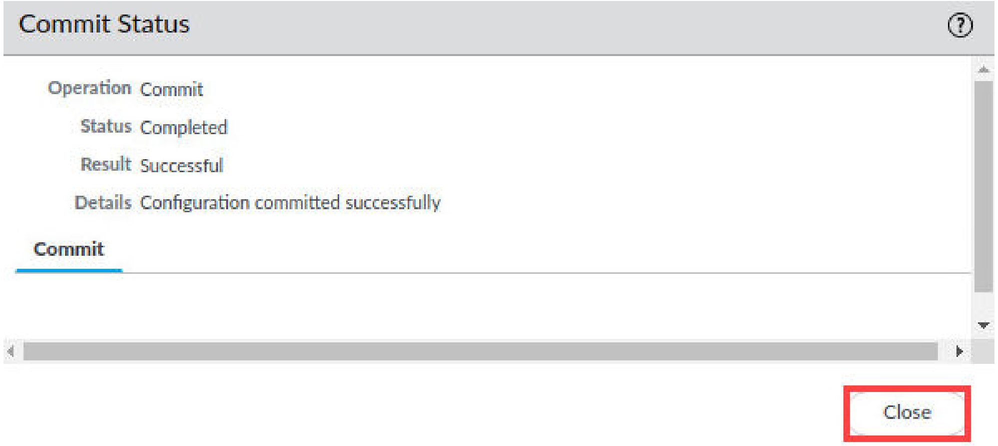
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

20. Wait until the *Commit* process is complete, click **Close**.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

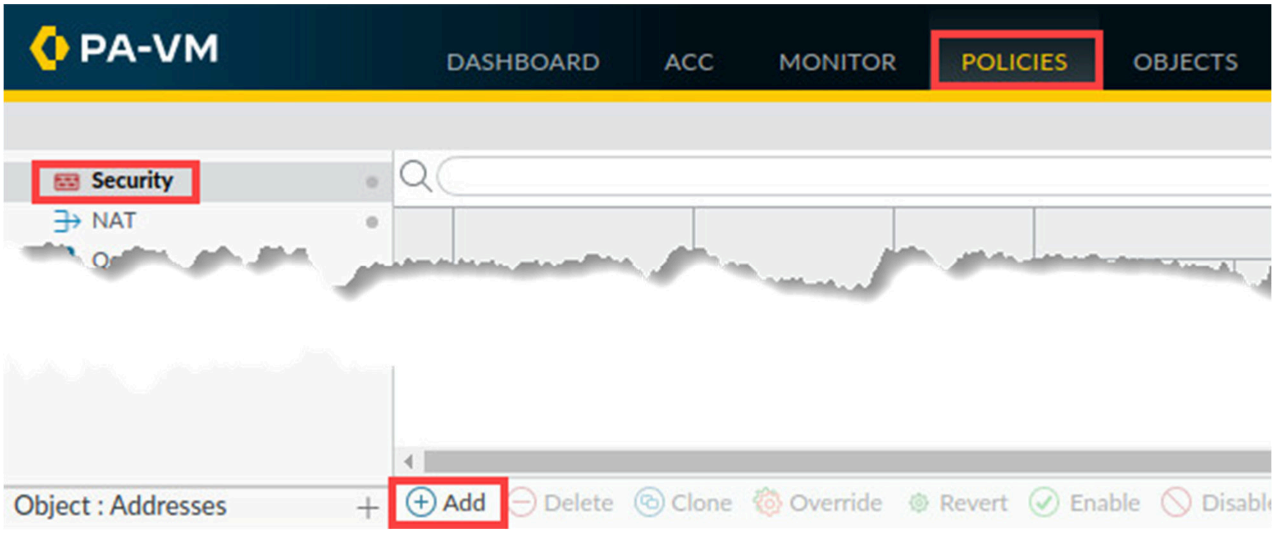
21. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Manually Create FTP Application-Based Security Policy

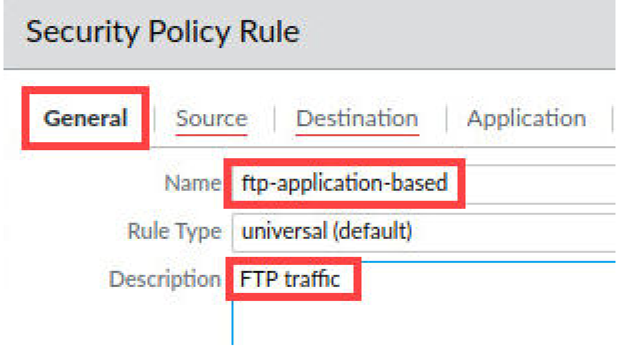
STOP If you completed task 9.6 using the Policy Optimizer, skip this task and continue to task 9.8.

In this section, you will manually create an FTP Application-Based Security Policy.

1. In the web interface, select **Policies > Security**. Click **Add** at the bottom of the security policy window.



2. On the *General* tab, type **`ftp-application-based`** as the *Name*. For *Description*, enter **`FTP traffic`**.



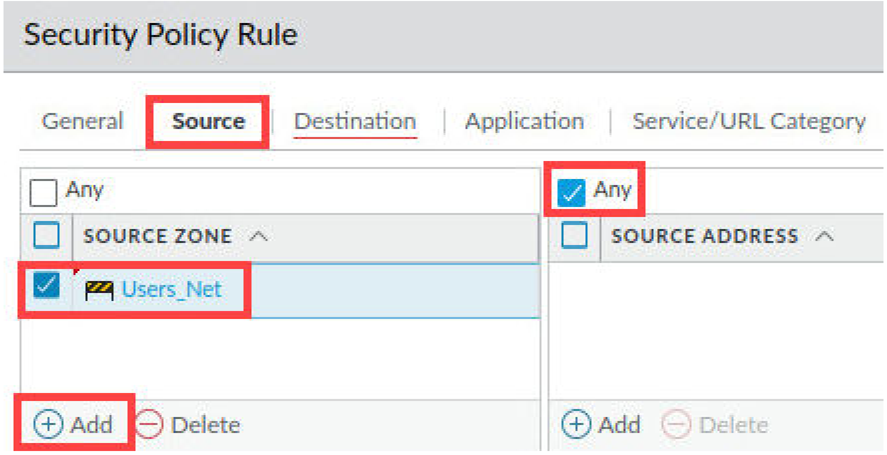
Name ftp-application-based

Rule Type universal (default)

Description FTP traffic

3. Click the **Source** tab and configure the following:

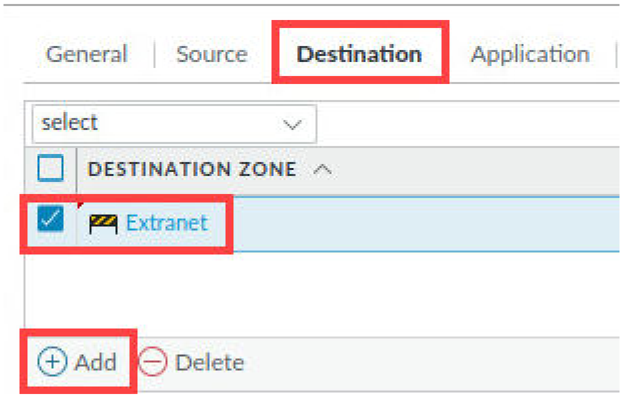
Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**



Security Policy Rule

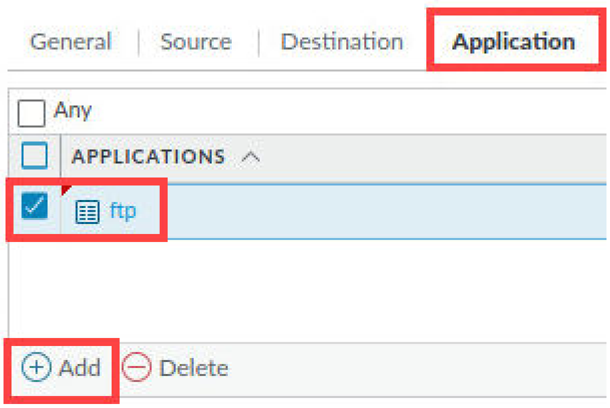
4. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	**Extranet**



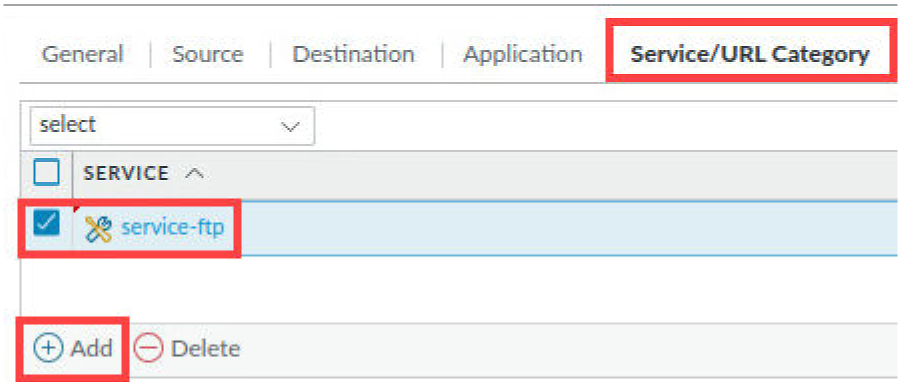
5. Click the **Application** tab and add the following:

Parameter	**Value**
Applications	**ftp**



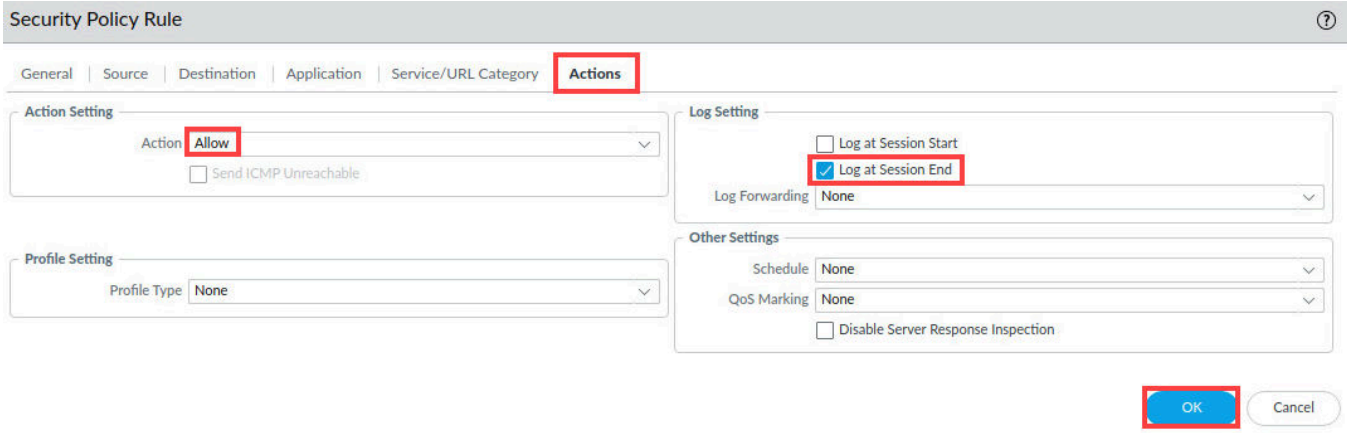
6. Click the **Service/URL Category** tab and configure the following:

Parameter	**Value**
Service	**service-ftp**



7. Click the **Actions** tab and verify the following. Click **OK**.

Parameter	Value
Action	Allow
Log Setting	Log at Session End



Security Policy Rule

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

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

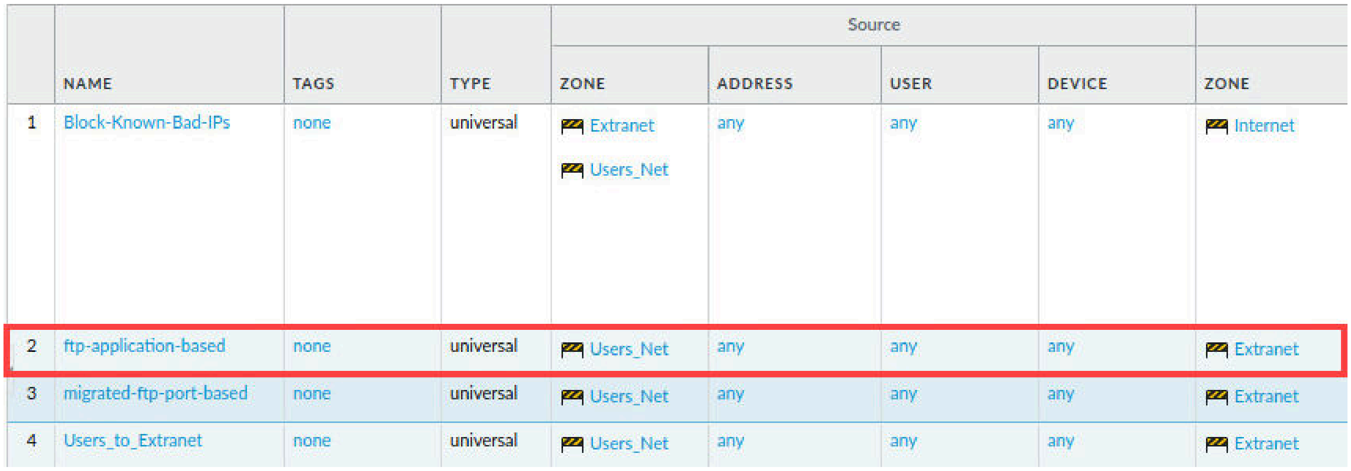
Other Settings

Schedule: None

QoS Marking: None

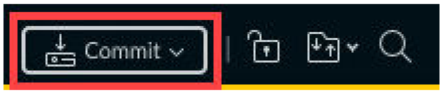
□ Disable Server Response Inspection

8. Use your mouse pointer to drag-and-drop the **ftp-application-based** security policy above the **migrated-ftp-port-based** rule.

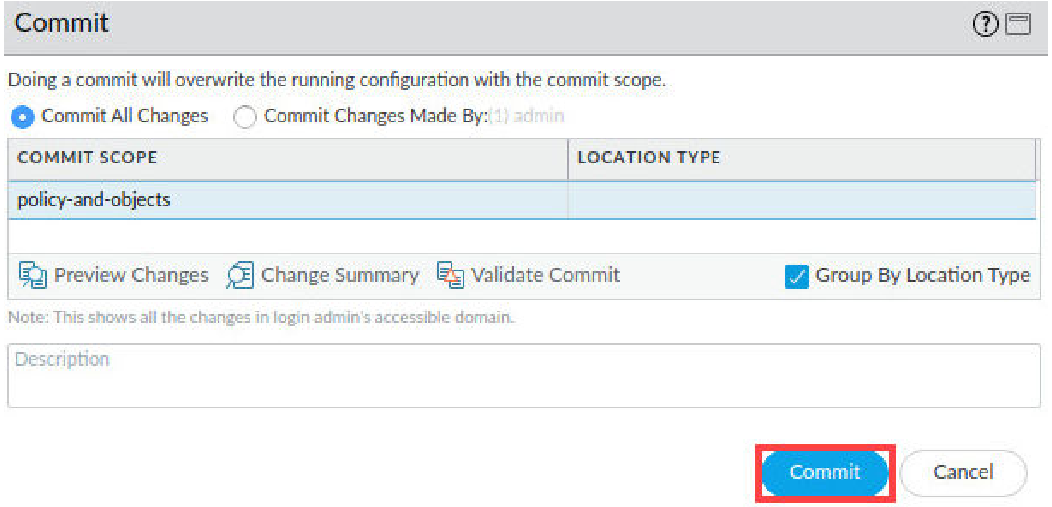


				Source				
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any	any	any	Internet
2	ftp-application-based	none	universal	Users_Net	any	any	any	Extranet
3	migrated-ftp-port-based	none	universal	Users_Net	any	any	any	Extranet
4	Users_to_Extranet	none	universal	Users_Net	any	any	any	Extranet

9. Click the **Commit** button at the upper-right of the web interface.



10. In the *Commit* window, click **Commit**.



Commit

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

● Commit All Changes ○ Commit Changes Made By: (1) admin

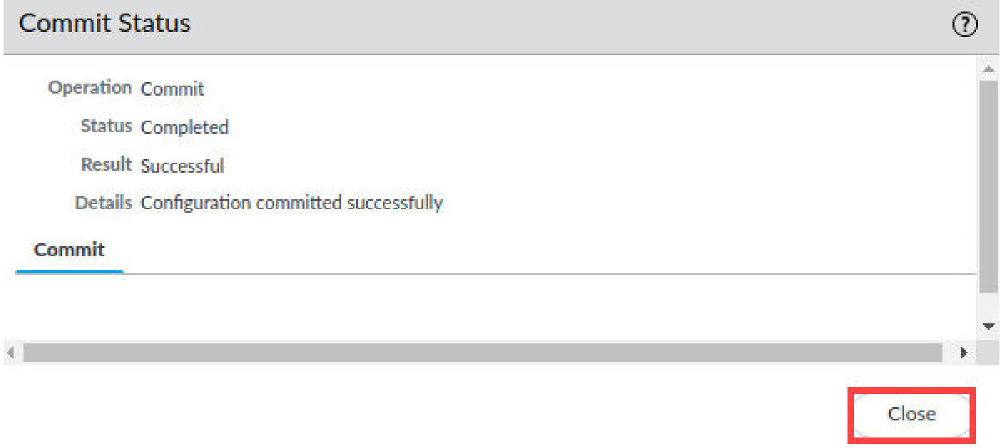
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

11. Wait until the *Commit* process is complete. Click **Close**.



Commit Status

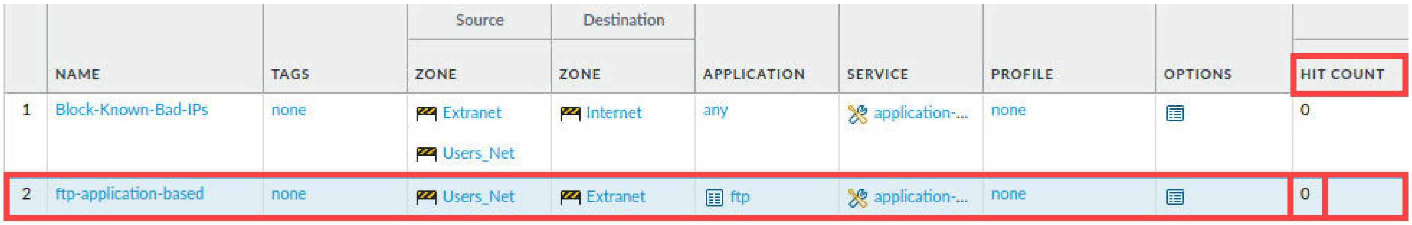
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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

1.8 Test the Application-Based Security Policy

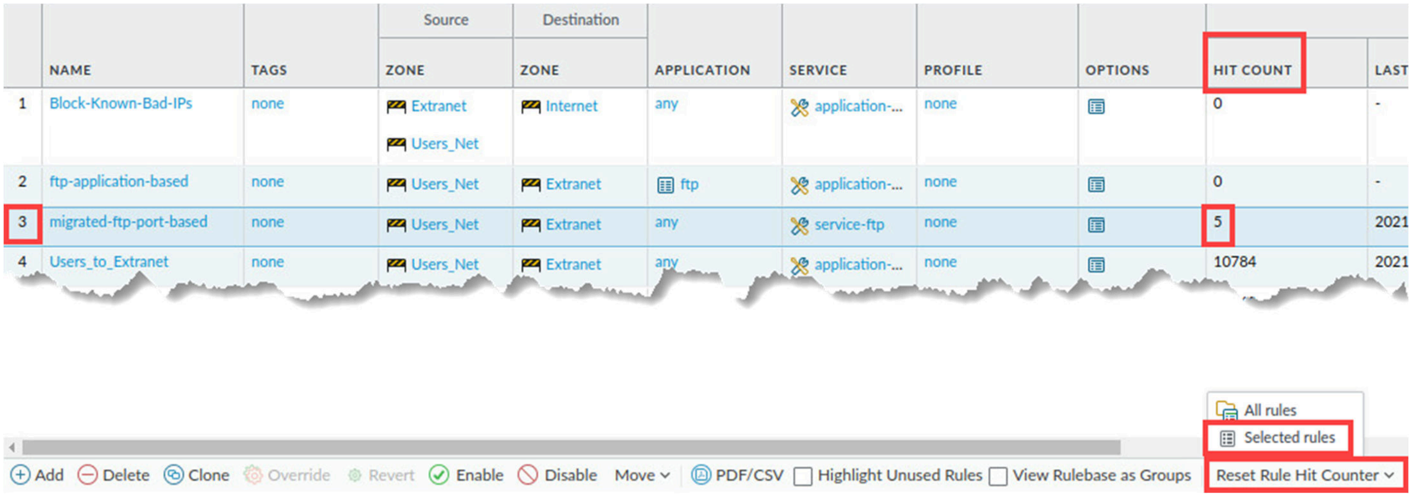
In this section, you will generate FTP traffic from your client host to the FTP server in the Extranet zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. The FTP traffic should match the application-based rule and not the port-based rule.

1. Ensure you are still viewing the *Security policies*. In the **ftp-application-based** rule, note that the *Hit Count* is **0**.



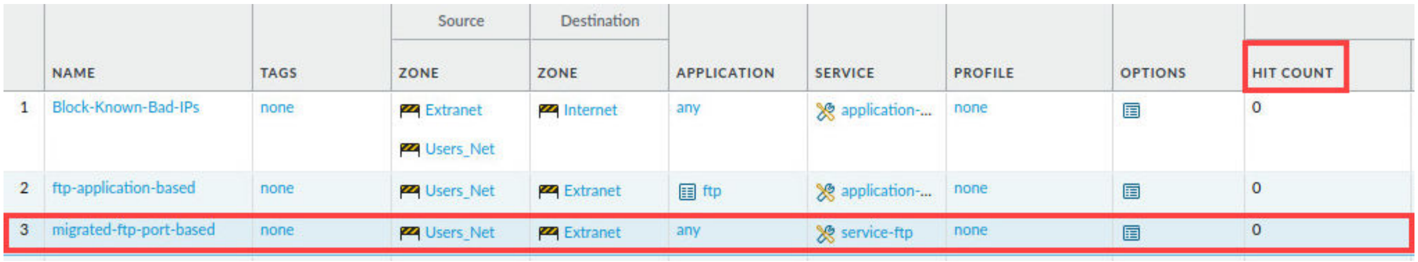
			Source	Destination					
	NAME	TAGS	ZONE	ZONE	APPLICATION	SERVICE	PROFILE	OPTIONS	HIT COUNT
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet	any	application-...	none	▤	0
2	ftp-application-based	none	Users_Net	Extranet	ftp	application-...	none	▤	0

2. Highlight the entry for the **migrated-ftp-port-based** rule. At the bottom of the window, click **Reset Rule Hit Counter > Selected rules** if it shows a hit count. This number may vary and will not hinder the completion of this task.



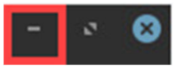
			Source	Destination						
	NAME	TAGS	ZONE	ZONE	APPLICATION	SERVICE	PROFILE	OPTIONS	HIT COUNT	LAST
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet	any	application-...	none	▤	0	-
2	ftp-application-based	none	Users_Net	Extranet	ftp	application-...	none	▤	0	-
3	migrated-ftp-port-based	none	Users_Net	Extranet	any	service-ftp	none	▤	5	2021
4	Users_to_Extranet	none	Users_Net	Extranet	any	application-...	none	▤	10784	2021

3. The *counter* has been reset to **zero** for the *migrated-ftp-port-based* rule. This will allow you to determine whether traffic is hitting the migrated-ftp-port-based rule during a test.

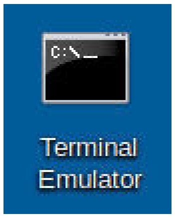


			Source	Destination					
	NAME	TAGS	ZONE	ZONE	APPLICATION	SERVICE	PROFILE	OPTIONS	HIT COUNT
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet	any	application-...	none	▤	0
2	ftp-application-based	none	Users_Net	Extranet	ftp	application-...	none	▤	0
3	migrated-ftp-port-based	none	Users_Net	Extranet	any	service-ftp	none	▤	0

4. Minimize the *Palo Alto Networks Firewall*.

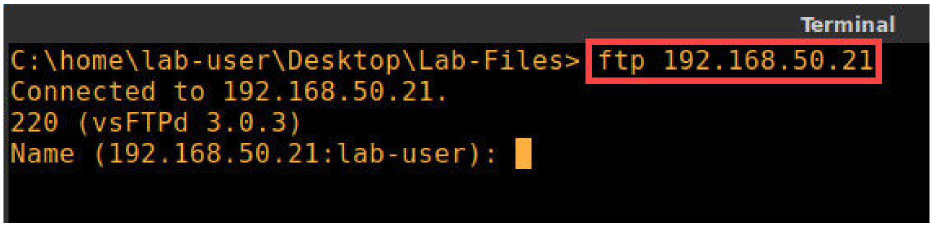


5. Open the **Terminal Emulator** on the *client desktop*.



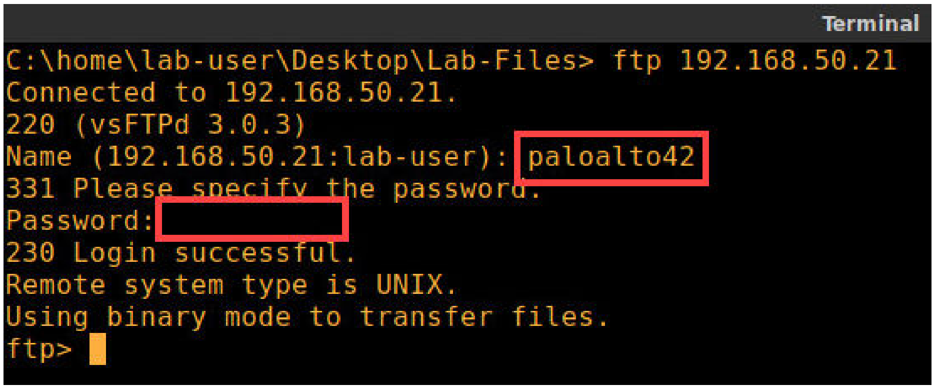
6. Issue the following command below.

```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21 <Enter>
```



```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21
Connected to 192.168.50.21.
220 (vsFTPd 3.0.3)
Name (192.168.50.21:lab-user):
```

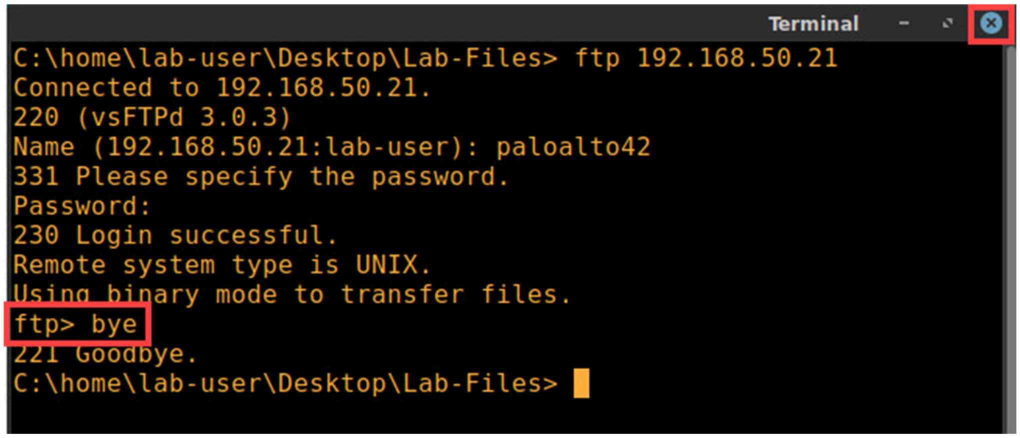
7. Log in with the username **`paloalto42`** and the password **`Pal0Alt0!`**.



```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21
Connected to 192.168.50.21.
220 (vsFTPd 3.0.3)
Name (192.168.50.21:lab-user): paloalto42
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

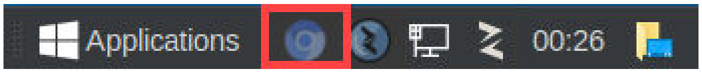
8. Type **bye** <Enter> at the FTP command prompt. Click the **X** to close the *terminal.*

```
C:\home\lab-user\Desktop\Lab-Files> bye <Enter>
```

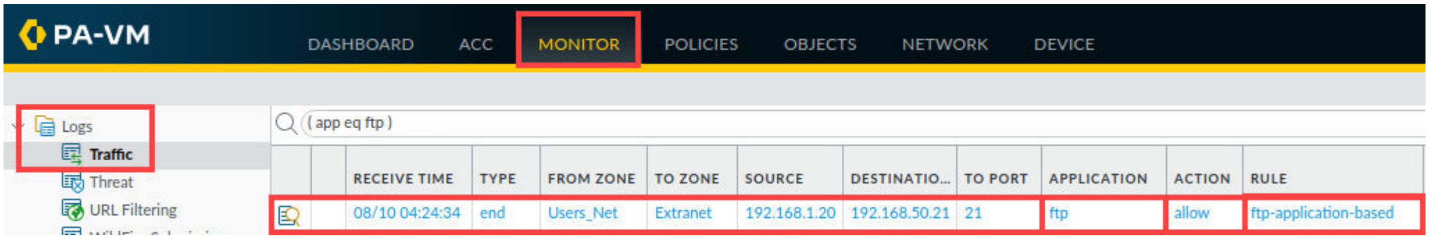


```
C:\home\lab-user\Desktop\Lab-Files> ftp 192.168.50.21
Connected to 192.168.50.21.
220 (vsFTPd 3.0.3)
Name (192.168.50.21:lab-user): paloalto42
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
C:\home\lab-user\Desktop\Lab-Files>
```

9. Reopen the *Pa-VM firewall* by clicking on the **Chromium** icon in the taskbar.



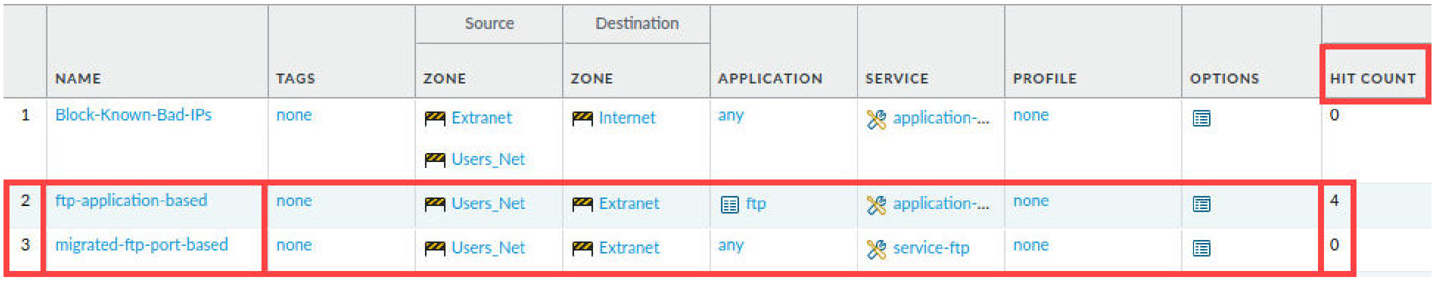
10. In the web interface, select **Monitor > Logs > Traffic.** Clear any filters you have in place. Apply the filter **`(app eq ftp)`** to help you locate the log entry for the FTP session.



(app eq ftp)

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
	08/10 04:24:34	end	Users_Net	Extranet	192.168.1.20	192.168.50.21	21	ftp	allow	ftp-application-based

11. Select **Policies > Security**. Examine the **Hit Count** values for the *ftp-application-based* rule and the *migrated-ftp-port-based* rule. The hit count is now reversed because the order of the security rule was to hit the *ftp-application-based* security rule first.



			Source	Destination					
	NAME	TAGS	ZONE	ZONE	APPLICATION	SERVICE	PROFILE	OPTIONS	HIT COUNT
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet	any	application-...	none	▤	0
2	ftp-application-based	none	Users_Net	Extranet	ftp	application-...	none	▤	4
3	migrated-ftp-port-based	none	Users_Net	Extranet	any	service-ftp	none	▤	0

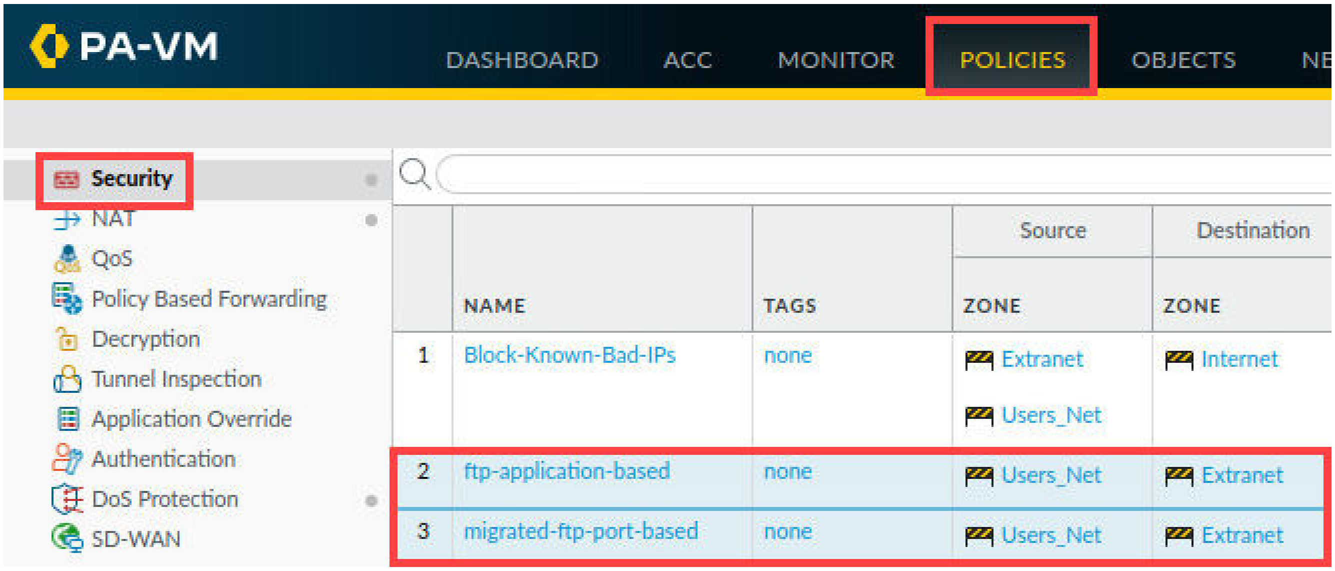
> **Please Note**
>
> In a real migration, you would disable the port-based rule for a while and wait to see if any FTP sessions are affected. After you are confident that the new application-based rule is matching all required FTP traffic, you would delete the port-based rule.

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

1.9 Remove the FTP Rules

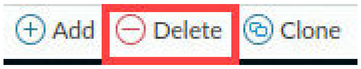
In this section, you will remove the application-based and port-based FTP rules from the Security policy.

1. Ensure you are at **Policies > Security**. Use your **Shift-key** and mouse pointer to select both the **ftp-application-based** and **migrated-ftp-port-based** rules.

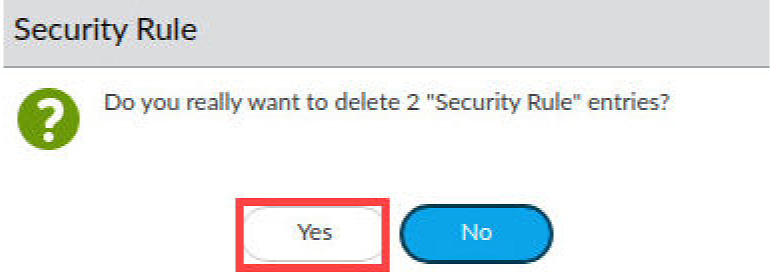


			Source	Destination
	NAME	TAGS	ZONE	ZONE
1	Block-Known-Bad-IPs	none	Extranet Users_Net	Internet
2	ftp-application-based	none	Users_Net	Extranet
3	migrated-ftp-port-based	none	Users_Net	Extranet

2. Click **Delete** to remove the rules.

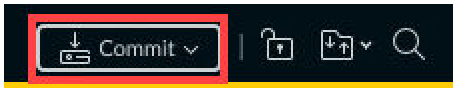


3. In the *Security Rule* window, click **Yes** to confirm the removal.

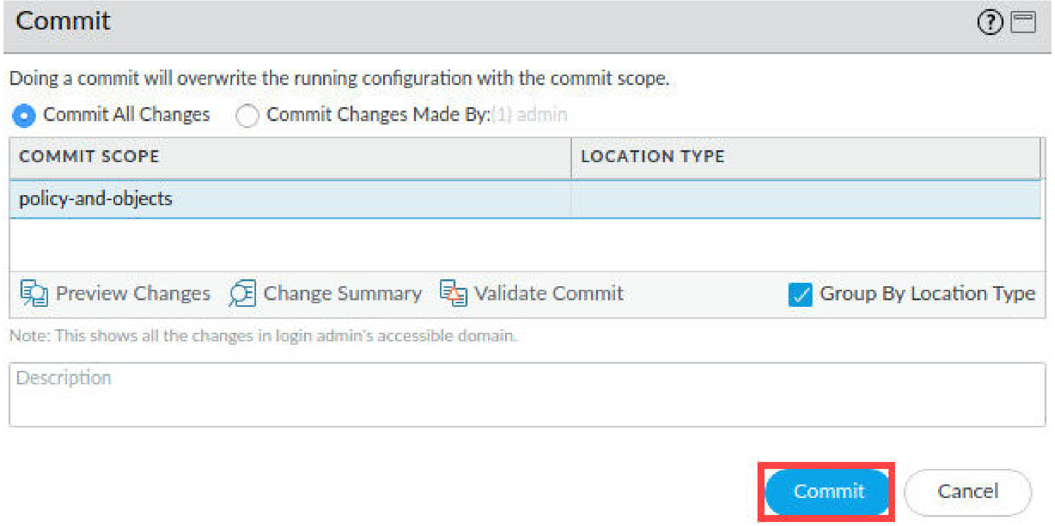

Security Rule

Do you really want to delete 2 "Security Rule" entries?

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



5. In the *Commit* window, click **Commit**.



Commit

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

● Commit All Changes ○ Commit Changes Made By:(1) admin

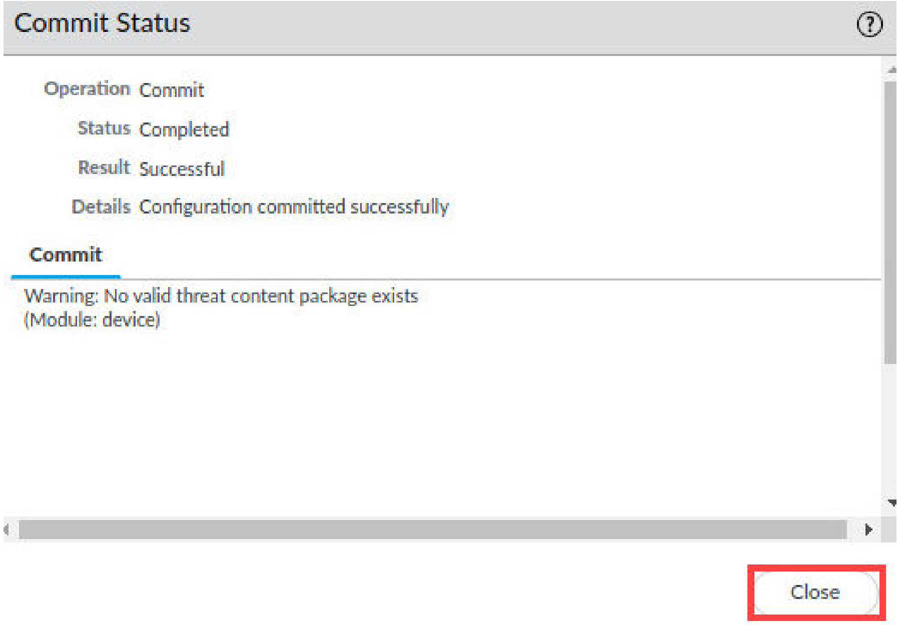
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

6. Wait until the *Commit* process is complete**.** Click **Close**.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Warning: No valid threat content package exists
(Module: device)

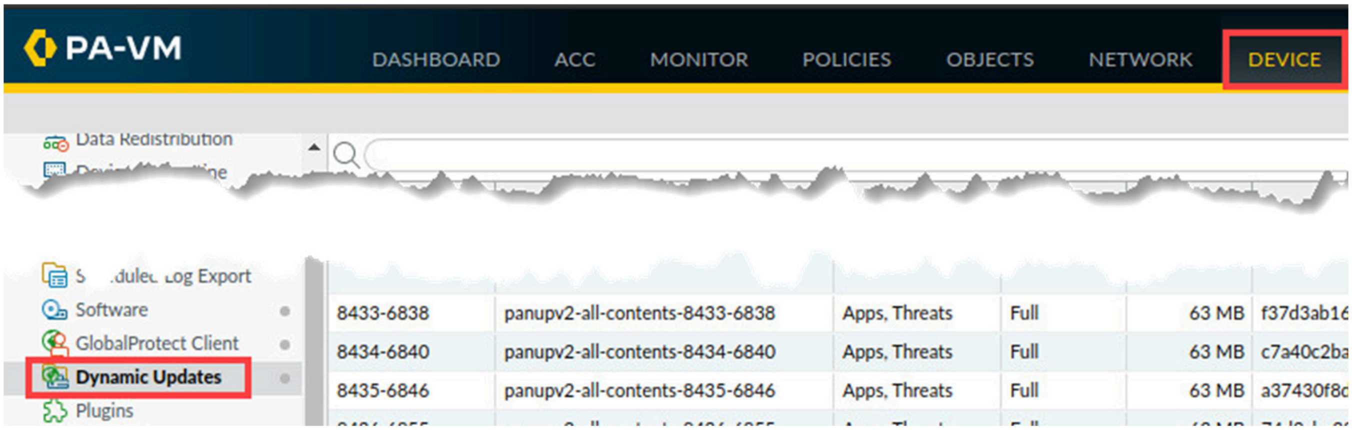
7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.10 Scheduling App-ID Updates

Keeping the firewall updated with new signatures for threats, viruses, and applications is critical. You can perform the update tasks manually, but a far more efficient method is to schedule the process.

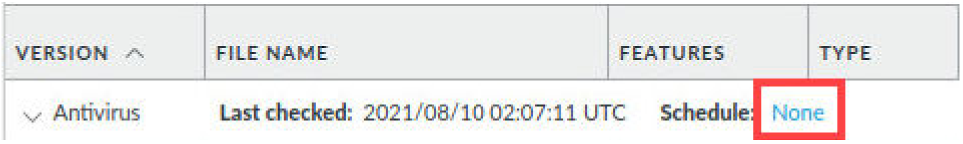
In this section, you will configure the firewall to check for and retrieve any new content updates for Anti-Virus, Vulnerabilities, Threats, and Applications.

1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.



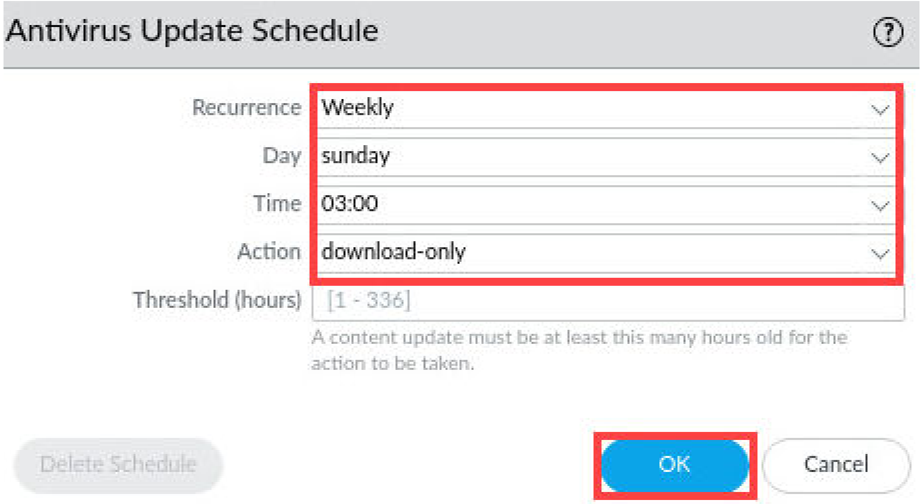
8433-6838	panupv2-all-contents-8433-6838	Apps, Threats	Full	63 MB	f37d3ab16
8434-6840	panupv2-all-contents-8434-6840	Apps, Threats	Full	63 MB	c7a40c2ba
8435-6846	panupv2-all-contents-8435-6846	Apps, Threats	Full	63 MB	a37430f8c

2. In the row for **Antivirus**, click the link for **None** beside **Schedule**.



VERSION	FILE NAME	FEATURES	TYPE
Antivirus	Last checked: 2021/08/10 02:07:11 UTC	Schedule: None	

3. In the *Antivirus Update Schedule* window, set the *Recurrence* to **Weekly**, select **Sunday** for the *Day*, set the *time* to **03:00,** and set the *Action* to **download-only**. Click **OK**.



Antivirus Update Schedule

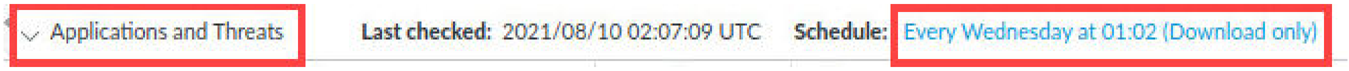
Recurrence	Weekly
Day	sunday
Time	03:00
Action	download-only
Threshold (hours)	[1 - 336]

A content update must be at least this many hours old for the action to be taken.

Please Note

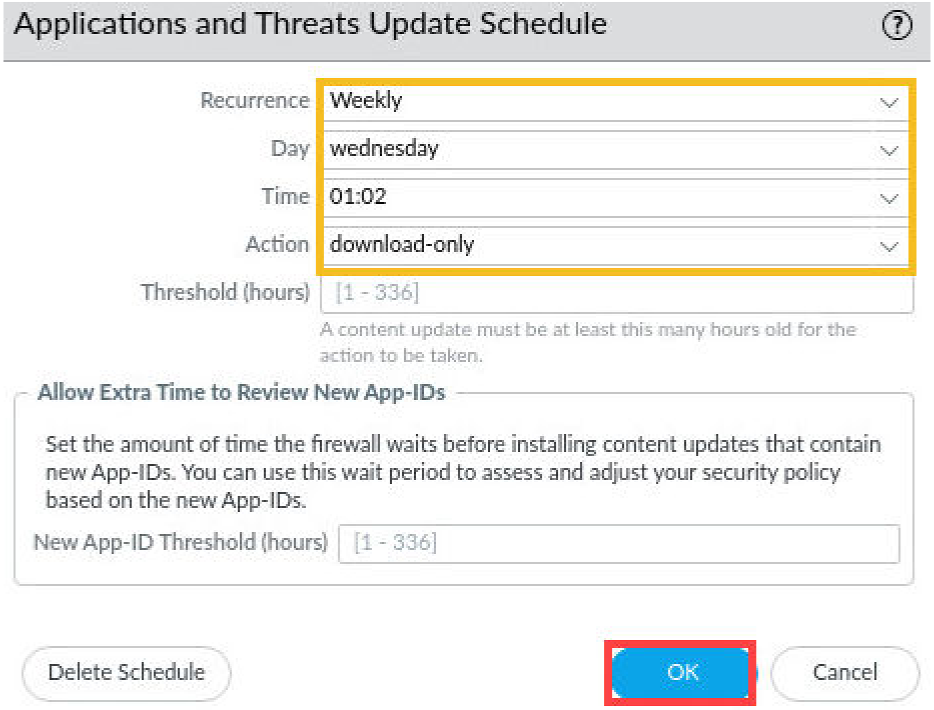
For this lab, you are setting the Action to download-only. This action means that the firewall will check for new signatures and download them but will not install them. In a production environment, you should use download-and-install for the Action.

4. Locate the section for **Applications and Threats**. Click the link for the *existing schedule*.



Applications and Threats   **Last checked:** 2021/08/10 02:07:09 UTC   **Schedule:** Every Wednesday at 01:02 (Download only)

5. In the *Applications and Threats Update Schedule* window, preview the settings. Click **OK**.



Applications and Threats Update Schedule

Recurrence: Weekly

Day: wednesday

Time: 01:02

Action: download-only

Threshold (hours): [1 - 336]

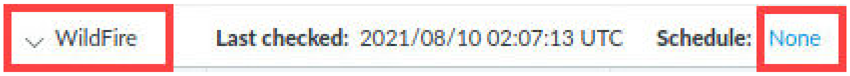
A content update must be at least this many hours old for the action to be taken.

Allow Extra Time to Review New App-IDs

Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.

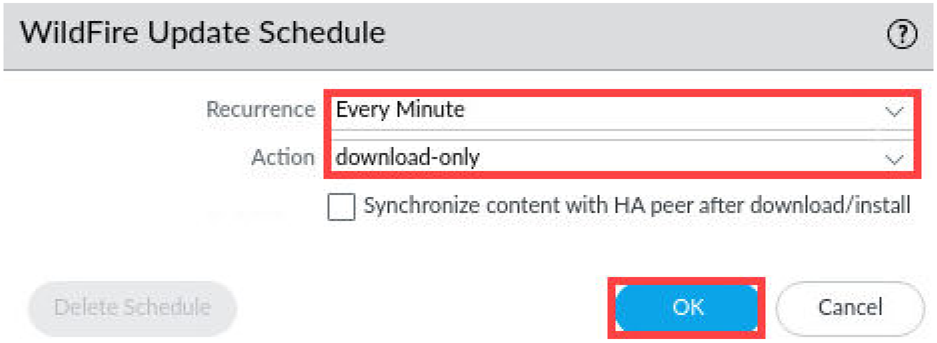
New App-ID Threshold (hours): [1 - 336]

6. Scroll down and locate the section for **WildFire**. Click **None** next to *Schedule***.**



WildFire   **Last checked:** 2021/08/10 02:07:13 UTC   **Schedule:** None

7. In the *Wildfire Update Schedule* window, set the *recurrence* to **Every Minute** and set the *Action* to **download-only**. Click **OK**.



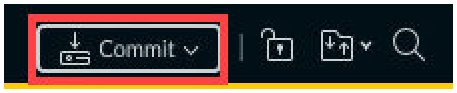
WildFire Update Schedule

Recurrence: Every Minute

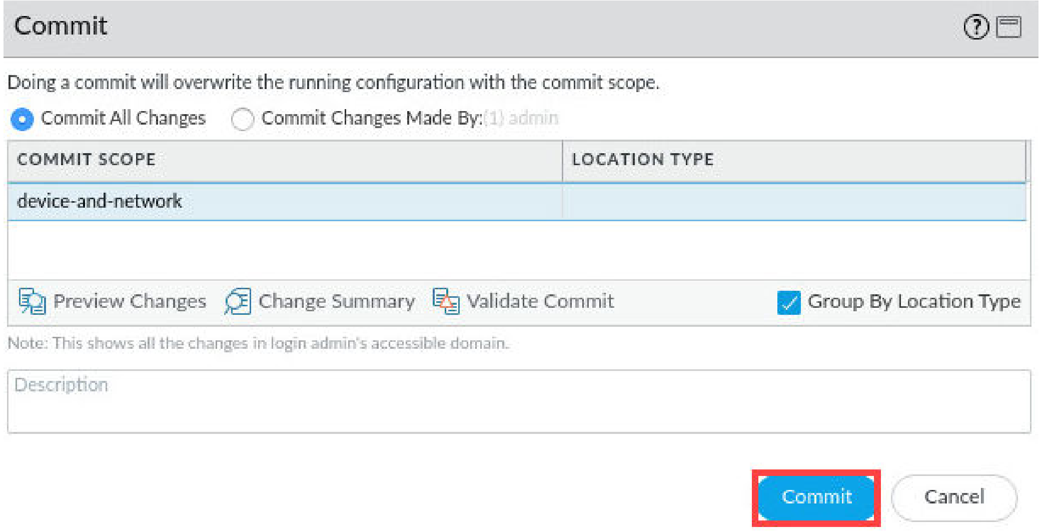
Action: download-only

□ Synchronize content with HA peer after download/install

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.


Commit

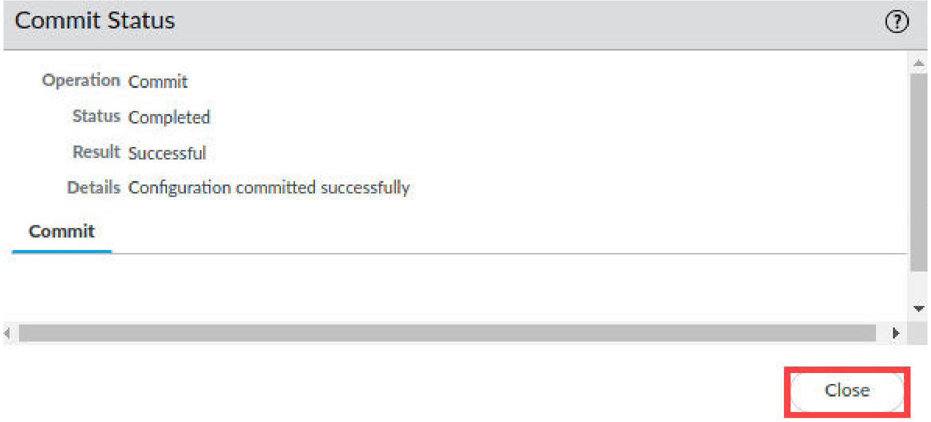
Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
device-and-network	

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

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


Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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