



PALO ALTO NETWORKS EDU 210

Lab 8: Blocking Threats using App-ID

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

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology.....	4
Theoretical Lab Topology.....	4
Lab Settings.....	5
1 Blocking Threats Using App-ID.....	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Create an FTP Service Object and Port-Based Security Policy Rule	10
1.3 Generate Application Traffic	19
1.4 Configure an Application Group.....	21
1.5 Configure a Security Policy to Allow Update Traffic.....	22
1.6 Test the Allow-PANW-Apps Security Policy Rule	27
1.7 Examine the Tasks Lists to See Shadowed Message	28
1.8 Modify the Security Policy to Function Properly.....	30
1.9 Test the Modified Security Policy Rule.....	33

Introduction

The old firewalls in your network only allowed you to block or allow traffic using Layer 3 and Layer 4 characteristics. With the deployment of the new Palo Alto Networks firewall, your control over traffic now includes which applications are allowed or blocked into and out of your network.

Some skeptics on your security team still do not fully believe that the Palo Alto Networks firewall can recognize applications beyond their Layer 4 characteristics.

To illustrate application awareness, you will create a Layer 4 object for FTP and use that in a security policy rule. In a later lab, you will convert this security policy rule to use the FTP application instead of the Layer 4 port-based object.

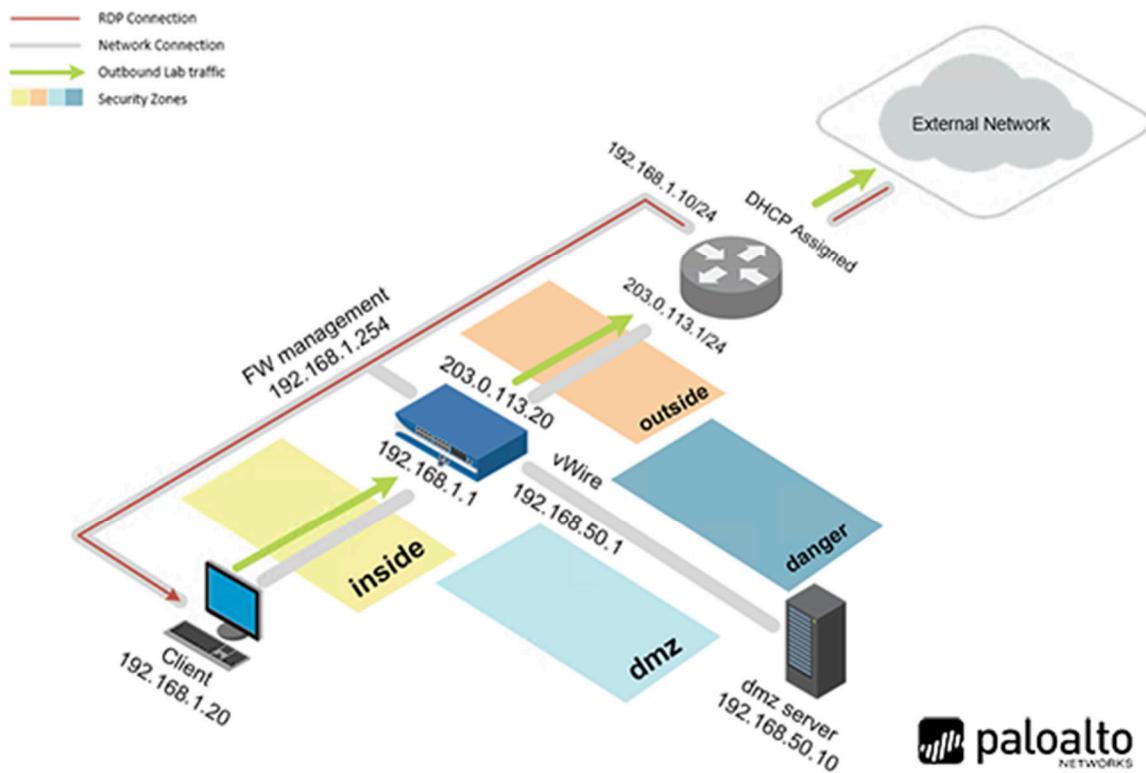
The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this Application Group as part of a security policy rule. This process will give you practice in creating security policy rules that take advantage of applications instead of simply Layer 3 and Layer 4 traffic characteristics.

Objective

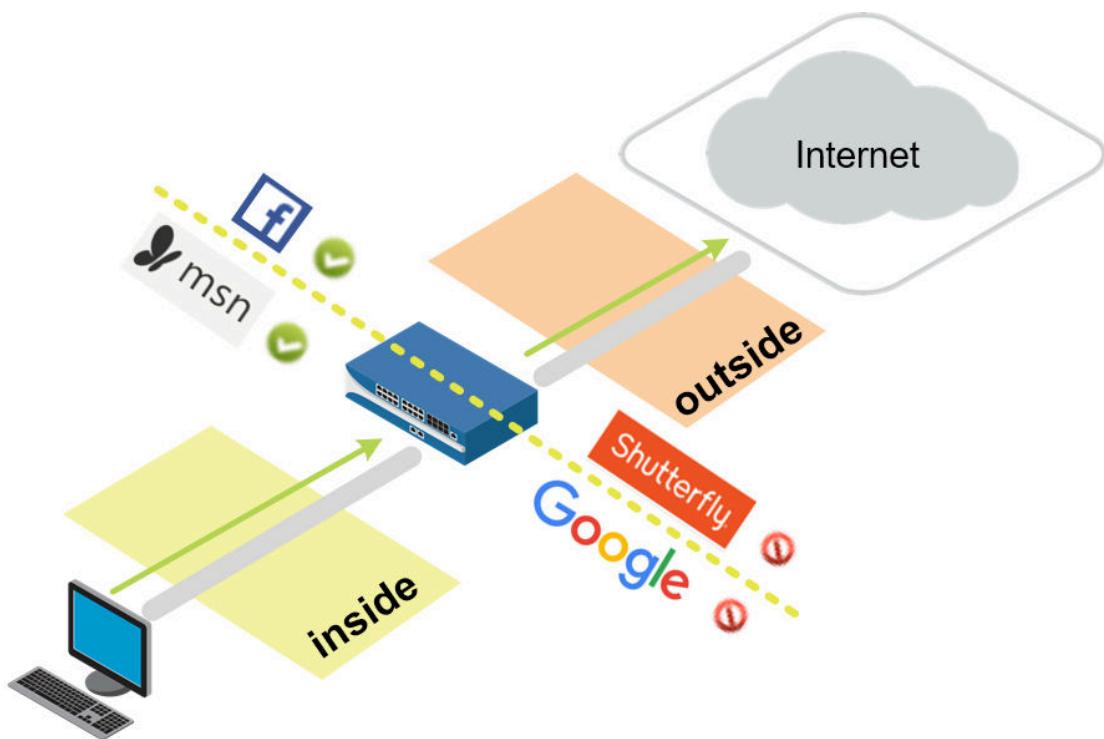
In this lab, you will perform the following tasks:

- Load a baseline configuration
- Create an FTP Service object and an FTP port-based security policy rule
- Test the port-based security policy
- Generate application traffic
- Configure an application group
- Configure a Security policy to allow updated traffic
- Test the Allow-PANW-Apps security policy rule
- Examine the tasks list to see shadowed message
- Modify the security policy to function properly
- Test the modified security policy rule

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	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 App-ID

1.1 Apply a Baseline Configuration to the Firewall

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

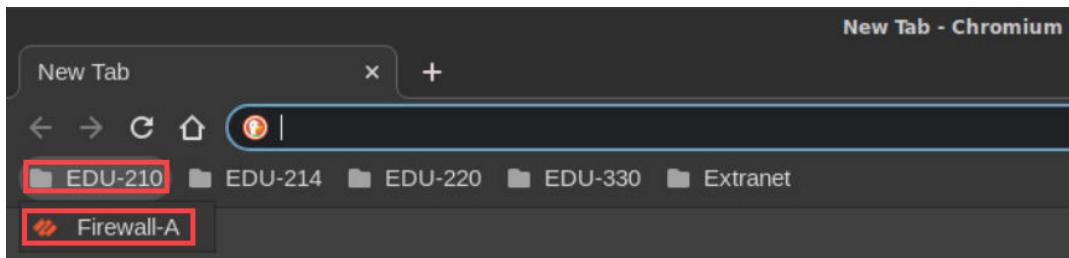
1. Click on the **Client** tab to access the Client PC.



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.



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.

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

[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 \(unsafe\)](#)

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



The screenshot shows a login interface for a Palo Alto Networks device. The page has a yellow border. At the top is the Palo Alto Networks logo. Below the logo is a form with two input fields: one for the username containing "admin" and one for the password containing redacted dots. A blue "Log In" button is at the bottom. The entire form area is highlighted with a red box.

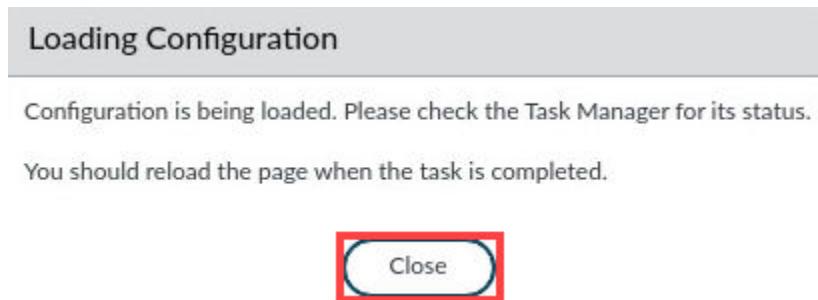
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the 'PA-VM' device interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The 'DEVICE' link is highlighted with a red box. On the left, a sidebar menu is open, showing options like Setup (highlighted with a red box), High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area is titled 'Configuration Management'. It contains several buttons: 'Revert' (links to 'Revert to last saved configuration' and 'Revert to running configuration'), 'Save' (links to 'Save named configuration snapshot' and 'Save candidate configuration'), 'Load' (links to 'Load named configuration snapshot' and 'Load configuration version'), and 'Load named configuration snapshot' (which is explicitly highlighted with a red box).

8. In the *Load Named Configuration* window, select **edu-210-lab-08.xml** from the *Name* dropdown box and click **OK**.



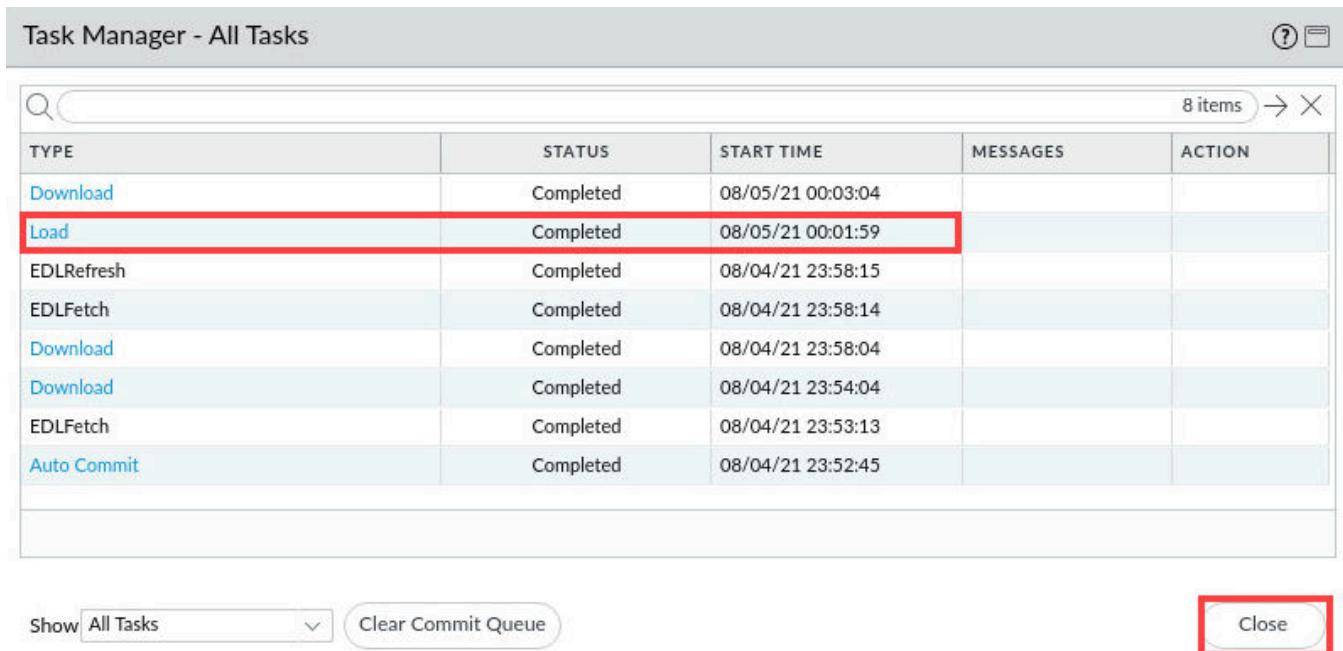
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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**.



The screenshot shows a table titled "Task Manager - All Tasks" with the following data:

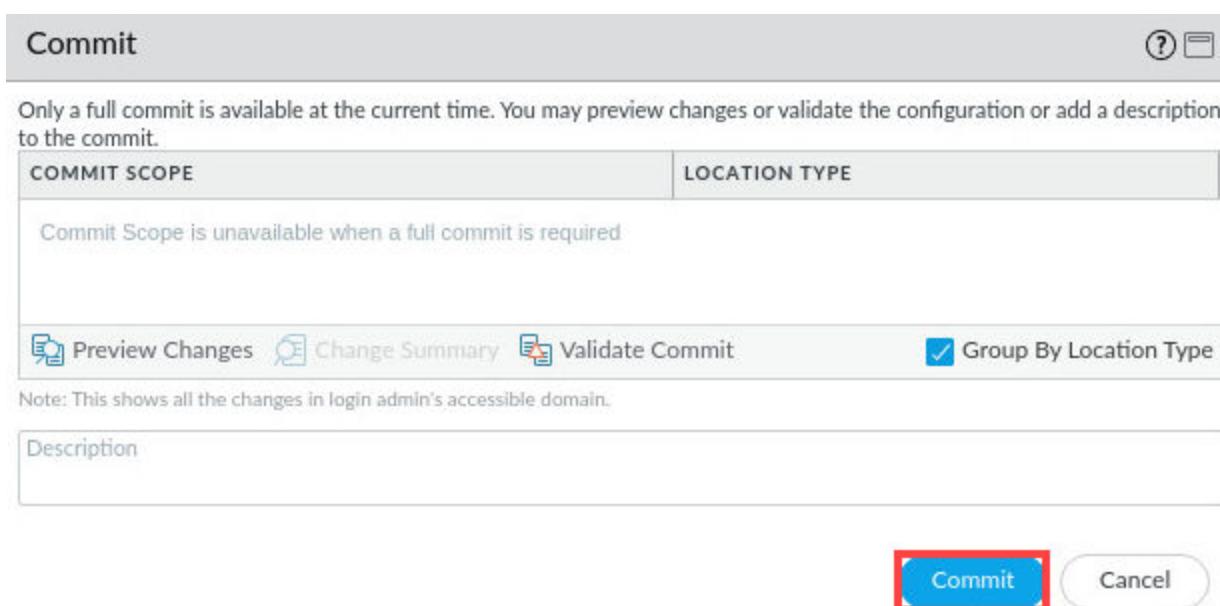
TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13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

Below the table are three buttons: "Show All Tasks" (dropdown), "Clear Commit Queue" (button), and "Close" (button, highlighted with a red box).

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



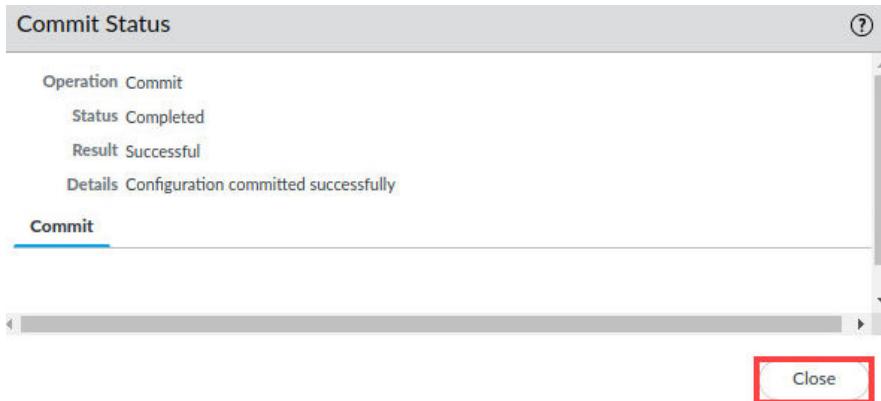
13. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the "Commit" window with the following interface elements:

- Commit Scope:** A note stating "Commit Scope is unavailable when a full commit is required".
- Location Type:** A section for selecting location types.
- Buttons:** "Preview Changes", "Change Summary", "Validate Commit", and "Group By Location Type" (checkbox checked).
- Note:** "Note: This shows all the changes in login admin's accessible domain."
- Description:** A text input field for entering a commit description.
- Buttons:** "Commit" (highlighted with a red box) and "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.

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

1.2 Create an FTP Service Object and Port-Based Security Policy Rule

In this section, you will start by creating an FTP Service object that defines the FTP port. Once you create the FTP Service object, you will create and test a port-based security policy rule that will enable you to simulate part of the process of migrating from a legacy, port-based security policy to a next-generation, application-based security policy.

Lastly, you will generate FTP traffic from the client host to an FTP server in the Extranet zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. After you complete this section, you will move on to other tasks related to App-ID. At the end of this lab, you will return to the task of migrating the FTP port-based rule to an application-based rule.

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

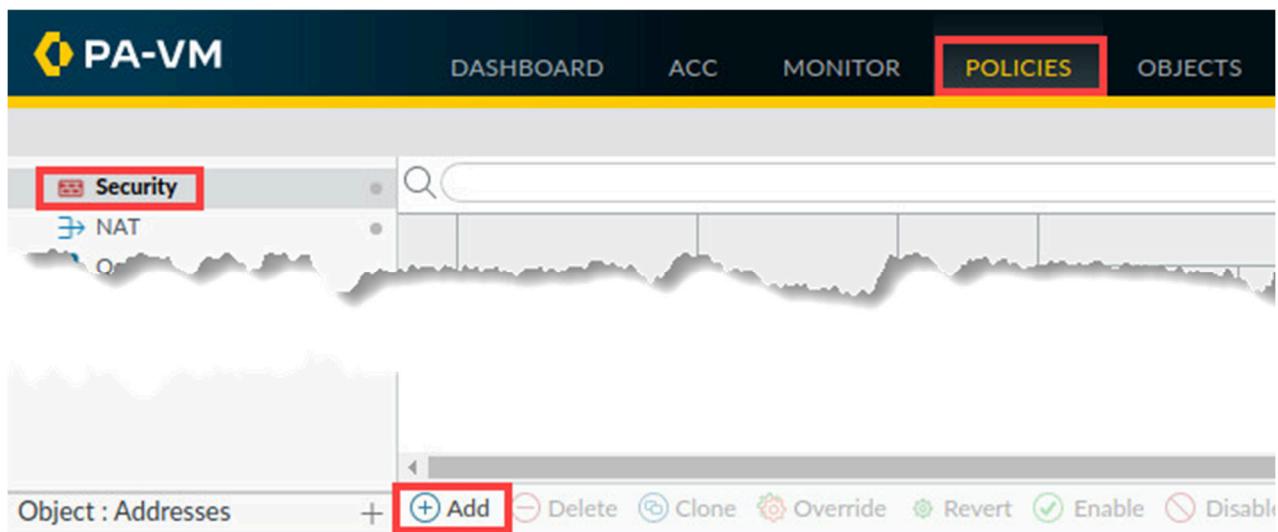
The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. In the left sidebar, the 'Services' option is highlighted with a red box. At the bottom of the main content area, there is a toolbar with several icons: Quality Profile, Traffic Distribution Profile, a search bar, and buttons for Add (+), Delete (-), Clone, and PDF/CSV. The 'Add' button is also highlighted with a red box.

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

Parameter	Value
Name	service-ftp
Protocol	TCP
Destination Port	21

The screenshot shows the 'Service' configuration dialog box. The 'Name' field contains 'service-ftp' (highlighted with a red box). The 'Protocol' section shows 'TCP' selected (radio button highlighted with a red box). The 'Destination Port' field contains '21' (highlighted with a red box). At the bottom right, there are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box.

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



4. On the *General* tab, type **migrated-ftp-port-based** as the *Name*. For *Description*, enter **Migrated from legacy firewall**.

Security Policy Rule	
General	Source Destination Application
Name	<input type="text" value="migrated-ftp-port-based"/>
Rule Type	<input type="text" value="universal (default)"/>
Description	<input type="text" value="Migrated from legacy firewall"/>

Please
Note

You are creating a rule that simulates a port-based rule that was
migrated from another vendor's firewall.

5. 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

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> Users_Net	
+ Add	- Delete

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

Parameter	Value
Destination Zone	Extranet
Destination Address	Any

Security Policy Rule

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

select	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> DESTINATION ZONE ^	<input type="checkbox"/> DESTINATION ADDRESS
<input checked="" type="checkbox"/> Extranet	
+ Add	- Delete

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

Parameter	Value
Applications	Any

The screenshot shows the 'Application' tab of a security policy rule. At the top, there are tabs for General, Source, Destination, and Application. The Application tab is active and highlighted with a red box. Below the tabs, there is a section labeled 'APPLICATIONS' with a dropdown menu. A checkbox labeled 'Any' is checked and highlighted with a red box. The dropdown menu shows other options like 'APPLICATIONS ^'.

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

Parameter	Value
Service	service-ftp

The screenshot shows the 'Service/URL Category' tab of a security policy rule. At the top, there are tabs for General, Source, Destination, Application, and Service/URL Category. The Service/URL Category tab is active and highlighted with a red box. Below the tabs, there is a dropdown menu labeled 'select' with a 'SERVICE' option. Underneath, a list shows 'service-ftp' selected with a checkmark and highlighted with a red box. At the bottom, there are 'Add' and 'Delete' buttons, with the 'Add' button highlighted with a red box.

9. 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
<input type="checkbox"/> Send ICMP Unreachable	

Log Setting

<input type="checkbox"/> Log at Session Start	<input checked="" type="checkbox"/> Log at Session End
Log Forwarding None	

Profile Setting

Profile Type	None
--------------	------

Other Settings

Schedule	None
QoS Marking	None
<input type="checkbox"/> Disable Server Response Inspection	

OK **Cancel**

10. Verify the *migrated-ftp-port-based* security policy is visible.

Sour	NAME	TAGS	TYPE	ZONE	
				ZONE	ADDRESS
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any
2	Users_to_Extranet	none	universal	Users_Net	any
3	Users_to_Internet	none	universal	Users_Net	any
4	Extranet_to_Internet	none	universal	Extranet	any
5	migrated-ftp-port-ba...	none	universal	Users_Net	any
6	intrazone-default	none	intrazone	any	any
7	interzone-default	none	interzone	any	any

11. Use your mouse pointer to drag-and-drop the **migrated-ftp-port-based** rule to just above the **Users_to_Extranet** rule.

	NAME	TAGS	TYPE	Source		
				ZONE	ADDRESS	USER
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any	any
3	Users_to_Extranet	none	universal	Users_Net	any	any

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



13. 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	

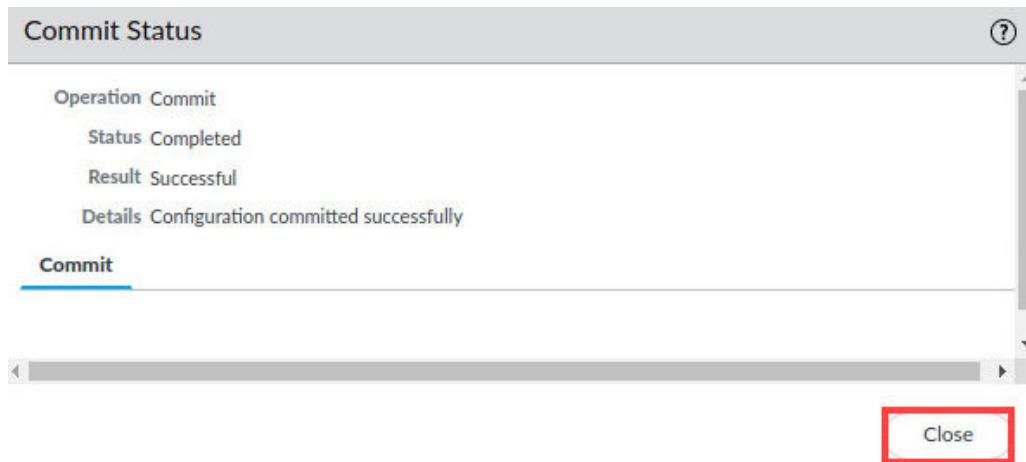
Preview Changes Change Summary Validate Commit Group By Location Type

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

Description

Commit **Cancel**

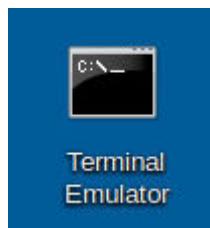
14. Wait until the *Commit* process is complete. Click **Close**.



15. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



16. On the *client desktop*, open **Terminal Emulator**.



17. Enter the command below to connect to the ftp server at 192.168.50.21.

```
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
```

18. Log in with the username **paloalto42** and **Pal0Alt0!** as the password.

```
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: [REDACTED]
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> [REDACTED]
```

19. Type **bye** at the FTP command prompt.

```
ftp> bye
```

```
ftp> bye
221 Goodbye.
C:\home\lab-user\Desktop\Lab-Files>
```

Please Note

This command should end the FTP session. An FTP session will be logged on the firewall even though no file was transferred.

20. Close the *terminal* window by typing **exit**.

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

```
C:\home\lab-user\Desktop\Lab-Files> exit
```

21. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.



22. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following filter (`(addr.src in 192.168.1.20)` and `(app eq ftp)`) in the filter builder.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	08/09 04:23:58	end	Users_Net	Extranet	192.168.1.20	192.168.50.21	21	ftp	allow	migrated-ftp-port-based	tcp-fin

Please Note

Some columns have been hidden to provide all the information needed for this step. If you do not hide or move columns, you can use the scroll bar to view the entire traffic log for the FTP session.

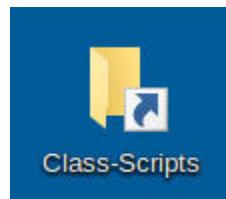
23. Minimize the *Chromium* browser by clicking the minimize icon and continue to the next task.



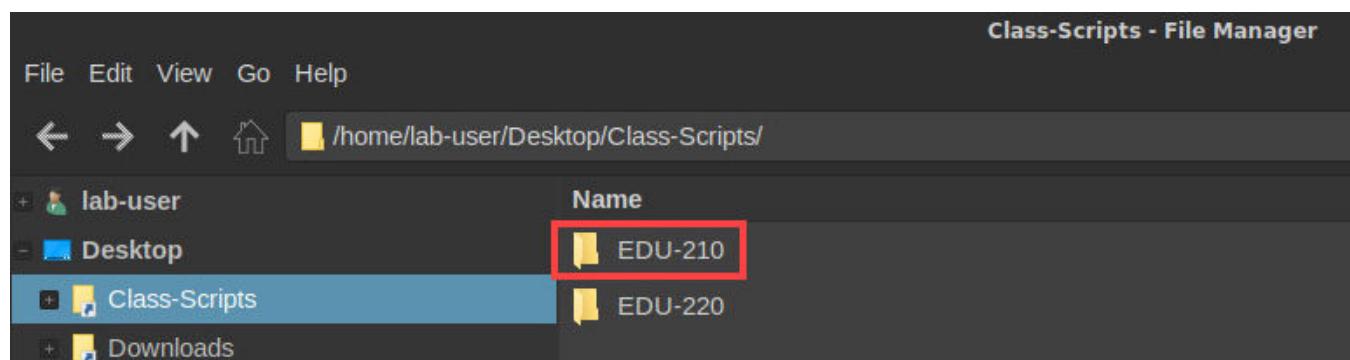
1.3 Generate Application Traffic

In this section, you will run a short script that generates application traffic from your client workstation to hosts against the Internet and Extranet security zones.

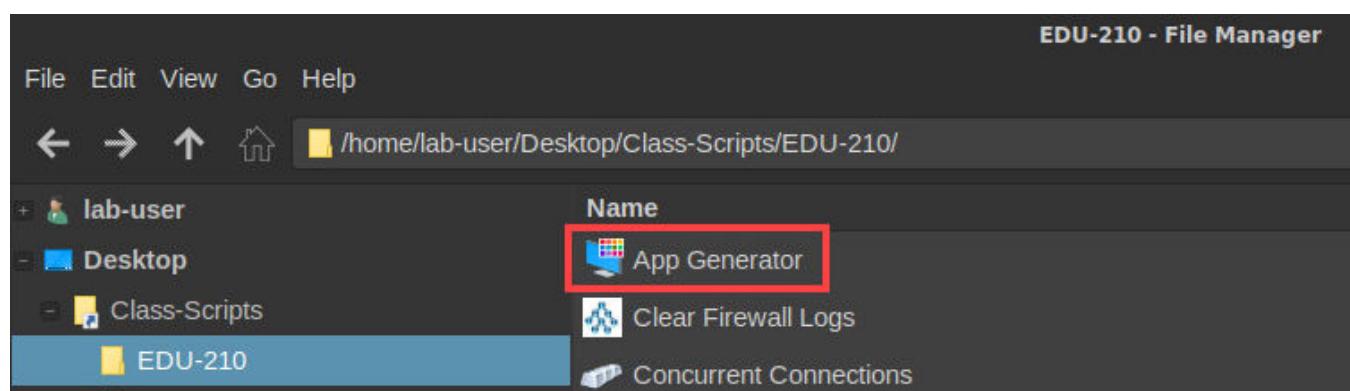
1. On the *client desktop*, double-click the folder for **Class-Scripts**.



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**. Allow the script 30 seconds to 1 minute to complete before proceeding to the next step.

```

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



6. In the web interface, select **Monitor > Logs > Traffic**. Create and apply the following new filter (`addr.src in 192.168.1.20`) in the filter builder. Note the entries in the *Application* column.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
08/10 00:54:39	end	Users_Net	Internet	192.168.1.20	142.251.45.14	80	google-base	allow	Users_to_Internet
08/10 00:54:34	end	Users_Net	Internet	192.168.1.20	17.253.3.206	80	web-browsing	allow	Users_to_Internet
08/10 00:54:13	end	Users_Net	Internet	192.168.1.20	1.1.1.1	53	dns	allow	Users_to_Internet
08/10 00:54:13	end	Users_Net	Extranet	192.168.1.20	192.168.50.53	53	dns	allow	Users_to_Extranet
08/10 00:54:13	end	Users_Net	Internet	192.168.1.20	1.1.1.1	53	dns	allow	Users_to_Internet
08/10 00:54:13	end	Users_Net	Extranet	192.168.1.20	192.168.50.53	53	dns	allow	Users_to_Extranet
08/10 00:54:04	end	Users_Net	Internet	192.168.1.20	91.189.89.199	123	ntp	allow	Users_to_Internet
08/10 00:53:58	end	Users_Net	Internet	192.168.1.20	142.250.31....	443	google-base	allow	Users_to_Internet
08/10 00:53:58	end	Users_Net	Internet	192.168.1.20	157.240.229....	443	facebook-base	allow	Users_to_Internet
08/10 00:53:58	end	Users_Net	Extranet	192.168.1.20	192.168.50.80	80	web-browsing	allow	Users_to_Extranet

Please Note

You may need to scroll the pages in the traffic window to see all the entries.

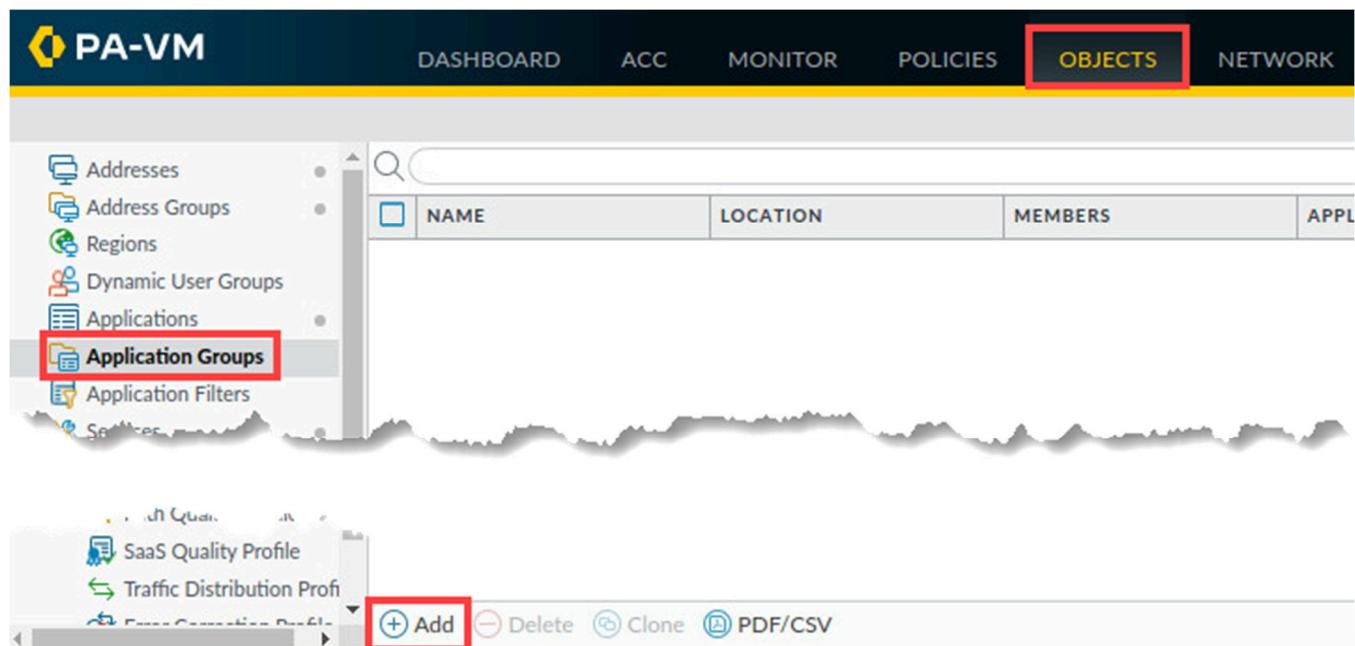
You should see entries for ftp, dns, google-base, ssl, web-browsing, facebook-base and ping. Use the refresh button to update the entries if necessary.

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

1.4 Configure an Application Group

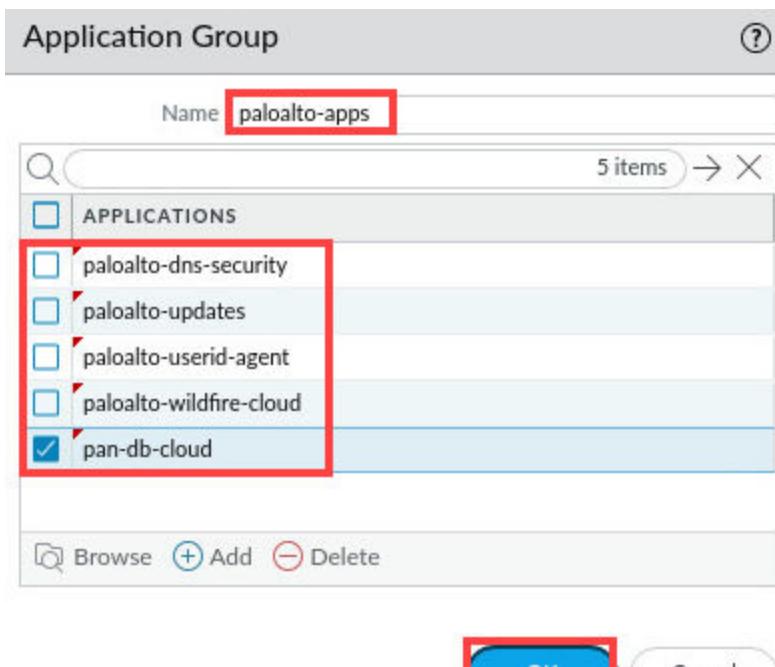
In this section, you will configure an application group called **paloalto-apps** that includes some Palo Alto Networks applications. These applications are used to label and control access to the content update network and other Palo Alto Networks products and features. You will add the application group to a security policy rule later in this lab exercise.

1. Navigate to **Objects > Application Groups**. Click **Add**.



2. In the *Application Group* window, configure the following. Click **OK**.

Parameter	Value
Name	paloalto-apps
Applications	paloalto-dns-security paloalto-updates paloalto-userid-agent paloalto-wildfire-cloud pan-db-cloud

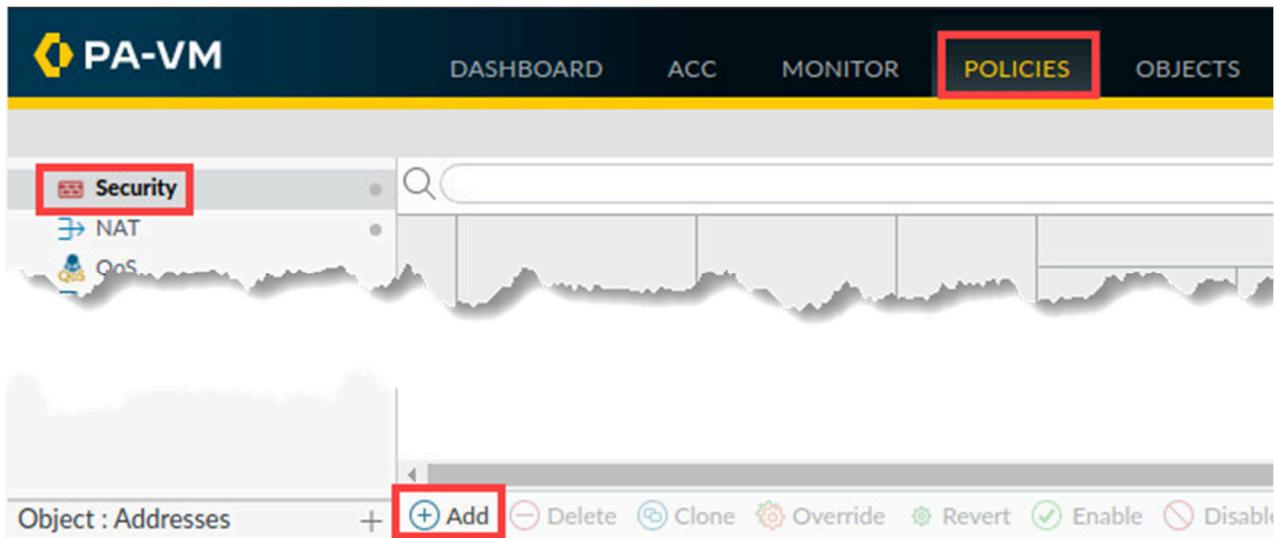


3. Leave the firewall open and continue to the next task.

1.5 Configure a Security Policy to Allow Update Traffic

In this section, you will create a specific security policy rule to enable access to Palo Alto Networks content updates. This configuration is an example of the positive enforcement model where you configure what the firewall should allow rather than only specifying what should be blocked.

- In the web interface, navigate to **Policies > Security**. Click **Add** to configure a new security policy.



- On the *General* tab, type **Allow-PANW-Apps** as the *Name*. For *Description*, enter **Allows PANW apps for firewall**.

Security Policy Rule

General	Source	Destination	Application
Name: Allow-PANW-Apps			
Rule Type: universal (default)			
Description: Allows PANW apps for firewall			

- Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	Users_Net
Source Address	192.168.1.254

General	Source	Destination	Application	Service/URL Category
<input type="checkbox"/> Any <input checked="" type="checkbox"/> SOURCE ZONE ▾ <input checked="" type="checkbox"/> Users_Net	<input type="checkbox"/> Any <input checked="" type="checkbox"/> SOURCE ADDRESS ▾ <input checked="" type="checkbox"/> 192.168.1.254			
<input type="button" value="(+ Add)"/> <input type="button" value="(- Delete)"/>	<input type="button" value="(+ Add)"/> <input type="button" value="(- Delete)"/>			

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

Parameter	Value
Destination Zone	Internet
Destination Address	Any

5. Click the **Application** tab and configure the following.

Parameter	Value
Applications	paloalto-apps

Please
Note

To locate your **paloalto-apps** Application Group, start typing in the first few letters of the group name, and the interface will display only those entries which match. Application Groups appear at the very end of the Application list.

6. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.

The screenshot shows the 'Service/URL Category' tab selected. In the top navigation bar, the tabs are General, Source, Destination, Application, Service/URL Category, and Actions. Below the tabs, there is a dropdown menu set to 'application-default'. To the right of the dropdown, there is a section labeled 'URL CATEGORY' with a checkbox labeled 'Any' which is checked. Both the dropdown and the 'Any' checkbox are highlighted with red boxes.

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

Parameter	Value
Action	Allow
Log Setting	Log at Session End

The screenshot shows the 'Actions' tab selected in a 'Security Policy Rule' dialog. Under 'Action Setting', the 'Action' dropdown is set to 'Allow'. Under 'Log Setting', the 'Log at Session End' checkbox is checked. At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted with a red box.

8. The **Allow PANW-Apps** rule should be listed just above the *intrazone-default* rule in the security policy rule list.

	NAME	TAGS	TYPE	Source	
				ZONE	ADDRESS
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any
3	Users_to_Extranet	none	universal	Users_Net	any
4	Users_to_Internet	none	universal	Users_Net	any
5	Extranet_to_Internet	none	universal	Extranet	any
6	Allow-PANW-Apps	none	universal	Users_Net	192.168.1.254
7	intrazone-default	none	intrazone	any	any
8	interzone-default	none	interzone	any	any

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	

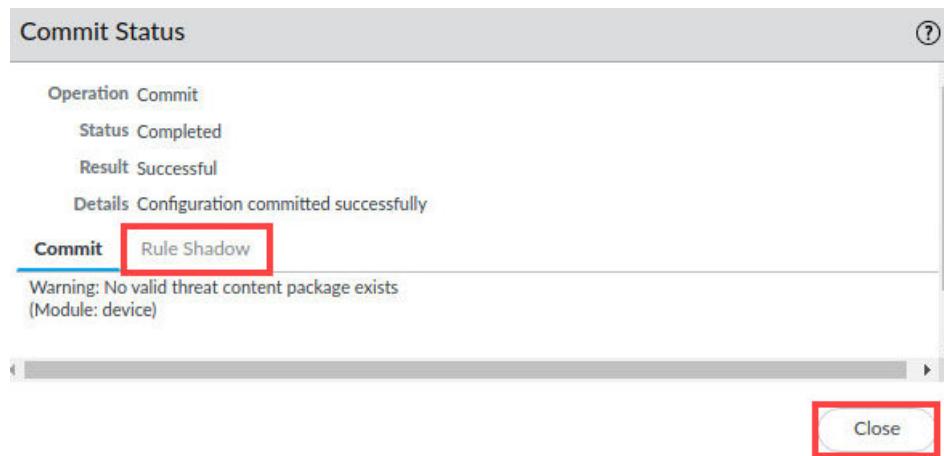
Preview Changes Change Summary Validate Commit Group By Location Type

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

Description

Commit **Cancel**

11. When the *Commit* process completes, notice that there is an additional tab available for *Rule Shadow*. Click **Close**.



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

1.6 Test the Allow-PANW-Apps Security Policy Rule

In this section, you will test the new security policy rule for **Allow-PANW-Apps** to see how it is working.

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

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256
2141-2627	panupv2-all-antivirus-2141-2627	Full		67 MB	b3e19d3d...

Please Note

This action instructs the firewall to check for Dynamic Content updates. The application used by the firewall is called *paloalto-updates* and is one that you included in the Application Group called *paloalto-apps*.

2. Select **Monitor > Logs > Traffic**. Clear any filters you have in place. Create and apply the following filter (`app eq paloalto-updates`) in the filter builder.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
	08/10 01:39:27	end	Users_Net	Internet	192.168.1....	107.178.249....	443	paloalto-updates	allow	Users_to_Internet
	08/10 01:38:50	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet
	08/10 01:38:49	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet
	08/10 01:38:48	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet
	08/10 01:38:47	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet
	08/10 01:38:46	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet



Notice the **Users_to_Internet** rule allowed application traffic to pass through the firewall. The firewall traffic did not hit the **Allow-PANW-Apps** rule because the **Users_to_Internet** rule ‘shadows’ the **Allow-PANW-Apps** rule. Traffic matched the **Users_to_Internet** rule and the firewall carried out the allow action. There is no reason for the firewall to continue comparing packet characteristics to any following rules after it has found a match. Remember: Rule order is important!

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

1.7 Examine the Tasks Lists to See Shadowed Message

The firewall provides notification when you have a rule shadowing one or more other rules. The **Rule Shadow** tab appears at the end of the Commit process.

However, you might not always notice the **Rule Shadow** tab, so in this section, you will use the **Task** list to examine your earlier Commit messages.

1. In the bottom-right corner of the *PA-VM firewall* interface, click the **Tasks** button.



2. In the *Task Manager – All Tasks* window, scroll down and locate the most recent entry for **Commit** under **Type**. Click the link for **Commit**.

Task Manager - All Tasks

TYPE	STATUS	START TIME	MESSAGES	ACTION
EDLFetch	Completed	08/10/21 01:49:23		
EDLFetch	Completed	08/10/21 01:44:22		
EDLRefresh	Completed	08/10/21 01:39:05		
EDLFetch	Completed	08/10/21 01:39:04		
EDLFetch	Completed	08/10/21 01:34:04		
Commit	Completed	08/10/21 01:33:28	Commit Processing By: admin Start Time (Dequeued Time): 08/10/21 01:33:28	
EDLFetch	Completed	08/10/21 01:32:24		

Show All Tasks Clear Commit Queue Close

3. In the *Job Status – Commit* window, select the **Rule Shadow** tab. The interface shows you which rule is shadowing other rules. Click the number under the *Count* (in this example, the value is **1**). Click **Close**.

Job Status - Commit

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit **Rule Shadow**

RULE	TYPE	COUNT
Users_to_Internet	security-rule	1

SHADOWED RULE
Rule 'Users_to_Internet' shadows rule 'Allow-PANW-Apps'.

Close

Please
Note

The value under the **Count** column indicates the number of rules that are shadowed. The **Shadowed Rule** column shows you details about which rule is shadowed.

You can use this detailed information to modify your security policy rule order to make certain traffic hits rules in the correct manner

4. In the *Task Manager – All Tasks* window, click **Close**.

The screenshot shows a table titled "Task Manager - All Tasks" with the following data:

TYPE	STATUS	START TIME	MESSAGES	ACTION
EDLFetch	Completed	08/10/21 01:54:24		
EDLFetch	Completed	08/10/21 01:49:23		
EDLFetch	Completed	08/10/21 01:44:22		
EDLRefresh	Completed	08/10/21 01:39:05		
EDLFetch	Completed	08/10/21 01:39:04		
EDLFetch	Completed	08/10/21 01:34:04		
Commit	Completed	08/10/21 01:33:28	Commit Processing By: admin Start Time (Dequeued Time): 08/10/21 01:33:28	

At the bottom of the window, there are three buttons: "Show All Tasks" with a dropdown arrow, "Clear Commit Queue", and a red-bordered "Close" button.

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

1.8 Modify the Security Policy to Function Properly

In this section, you will modify your security policy to ensure that only the Allow-PANW-Apps rule allows Palo Alto Networks content update traffic. This configuration is another example of the positive enforcement model where you configure what the firewall should allow rather than only specifying what should be blocked.

You will also modify the security policy rule that allows traffic from the Users_Net to the Internet. Instead of allowing any application, the modified rule will allow only a few applications.

- In the web interface, navigate to **Policies > Security**. Click **Users_to_Internet** to edit the rule.

NAME	TAGS	TYPE	ZONE
1			
2			
3			
4 Users_to_Internet	none	universal	Users_Net
5 Extranet_to_Internet	none	universal	Extranet

- In the *Security Policy Rule* window, click the **Application** tab and configure the following. Click **OK**.

Parameter	Value
Applications	dns ping ssl web-browsing

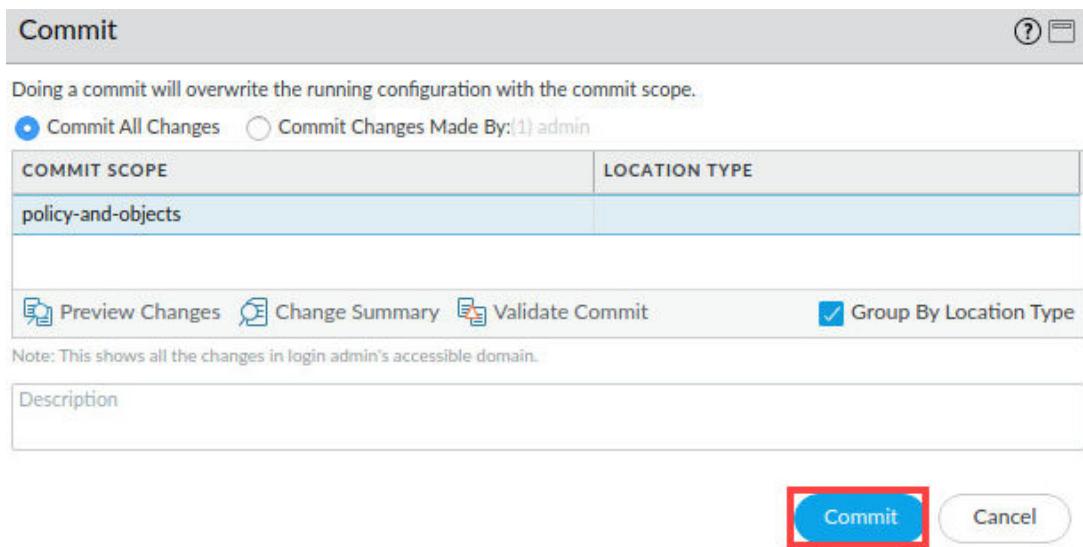
Security Policy Rule

General	Source	Destination	Application	Service/URL Category	Actions	Usage
<input type="checkbox"/> Any			<input type="checkbox"/> APPLICATIONS ^ <input type="checkbox"/> dns <input type="checkbox"/> ping <input type="checkbox"/> ssl <input checked="" type="checkbox"/> web-browsing			
<input type="checkbox"/> Add <input type="checkbox"/> Delete				<input type="checkbox"/> 0 items → X <input type="checkbox"/> DEPENDS ON		
Add To Current Rule						
<input style="background-color: #0070C0; color: white; border-radius: 10px; padding: 5px 10px; border: none; font-weight: bold; font-size: 10pt; margin-right: 10px;" type="button" value="OK"/> <input style="border: 1px solid #0070C0; color: #0070C0; border-radius: 10px; padding: 5px 10px; font-weight: bold; font-size: 10pt;" type="button" value="Cancel"/>						

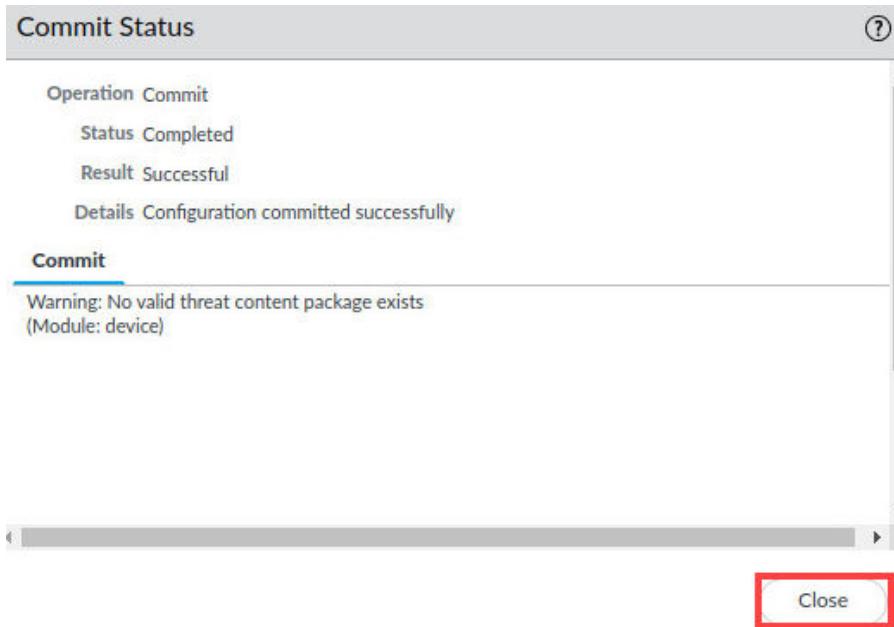
3. Click the **Commit** button at the upper-right of the web interface.



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



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



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

1.9 Test the Modified Security Policy Rule

In this section, you will test the modified security policy to verify that it is working as expected. You want to verify that Dynamic Update traffic from the firewall uses the **Allow-PANW-Apps** rule.

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

The screenshot shows the PA-VM interface with the 'DEVICE' tab selected. On the left, there's a sidebar with various management options like Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, Certificates, and Policy Recommendation. Under 'Dynamic Updates', a sub-menu is open with options: Software, GlobalProtect Client, Dynamic Updates (which is highlighted with a red box), Plugins, VM-Series, Licenses, Support, Master Key and Diagnostics, and Policy Recommendation. At the bottom of the sidebar, there are 'Check Now', 'Upload', and 'Install From File' buttons. The main area displays a table of dynamic update packages:

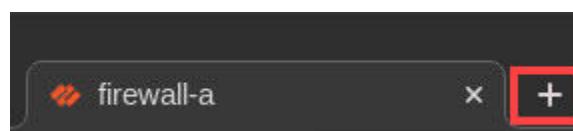
VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256
2141-2627	panup-all-antivirus-2141-2627	Full		67 MB	63e0...3db4747d...
8426-6800	panupv2-all-contents-8426-6800	Apps, Threats	Full	63 MB	45...abc0...
8427-6806	panupv2-all-contents-8427-6806	Apps, Threats	Full	63 MB	3db4747d...
8428-6809	panupv2-all-contents-8428-6809	Apps, Threats	Full	63 MB	bcb9cc1a...
8429-6810	panupv2-all-contents-8429-6810	Apps, Threats	Full	63 MB	547e19d3d...
8430-6813	panupv2-all-contents-8430-6813	Apps, Threats	Full	63 MB	57a70bd1c...
8431-6821	panupv2-all-contents-8431-6821	Apps, Threats	Full	63 MB	4f675fd9e...
8432-6829	panupv2-all-contents-8432-6829	Apps, Threats	Full	63 MB	97e9dd629...

2. Select **Monitor > Logs > Traffic**. Apply the following filter (`app eq paloalto-updates`) in the filter builder. Look for the log entries for the application *paloalto-updates*. It should be the **Allow-PANW_Apps** rule.

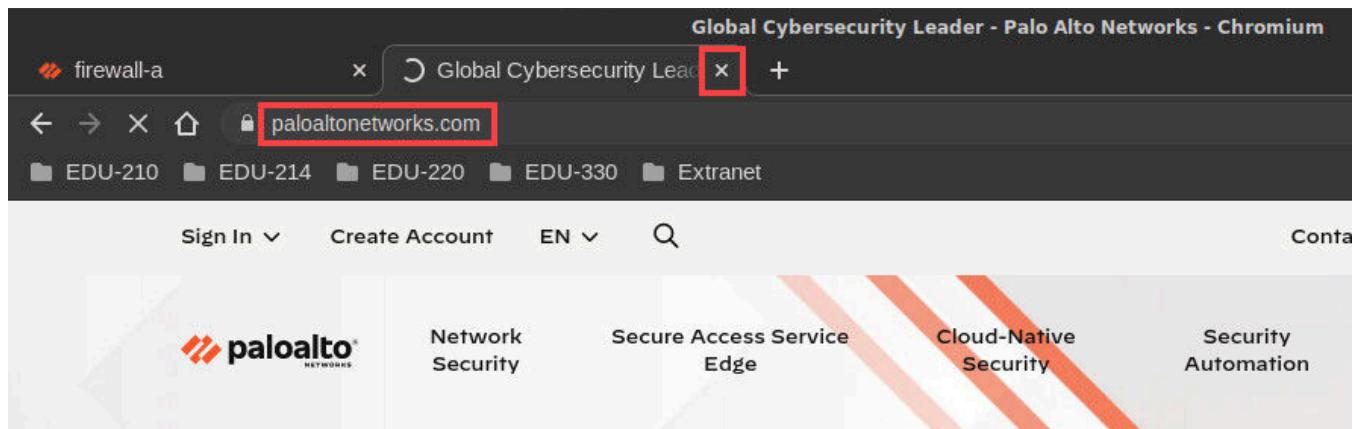
The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, there's a sidebar with 'Logs' and 'Traffic' (which is highlighted with a red box). A search bar at the top has the filter '(app eq paloalto-updates)' applied. The main area displays a table of traffic logs:

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
08/10 02:07:28	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Allow-PANW-Apps
08/10 02:07:27	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Allow-PANW-Apps
08/10 02:07:25	end	Users_Net	Internet	192.168.1....	34.96.84.34	443	paloalto-updates	allow	Allow-PANW-Apps

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



4. Type **www.paloaltonetworks.com** in the address bar and press **Enter**. Once you have verified the website will open, close the *Chromium* tab by clicking on the X icon.



5. Select **Monitor > Logs > Traffic**. Clear any filters you have in place. Create and apply the following filter (`addr.src eq 192.168.1.20`) and (`rule eq Users_to_Internet`) in the filter builder.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATIO...	TO PORT	APPLICATION	ACTION	RULE
	08/10 02:17:20	end	Users_Net	Internet	192.168.1.20	1.1.1.1	53	dns	allow	Users_to_Internet
	08/10 02:17:19	end	Users_Net	Internet	192.168.1.20	1.1.1.1	53	dns	allow	Users_to_Internet
	08/10 02:17:17	end	Users_Net	Internet	192.168.1.20	204.79.197...	443	ssl	allow	Users_to_Internet

Please
Note

Notice the App-ID identified the traffic as dns and ssl. The rule "Users_to_Internet" allowed the traffic for both applications.

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