



PALO ALTO NETWORKS 11.0 FIREWALL ESSENTIALS

Lab 7: Controlling Application Usage with App-ID

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

Contents

Introduction	3
Objective	3
Lab Topology	4
Theoretical Lab Topology	4
Lab Settings	5
Lab Guidance	5
1 Controlling Application Usage with App-ID - High Level Lab Steps	6
1.1 Apply a Baseline Configuration to the Firewall	6
1.2 Configure an Application Group	6
1.3 Configure a Security Policy Rule to Allow Update Traffic.....	6
1.4 Commit the Configuration	6
1.5 Test the Allow-PANW-Apps Security Policy Rule.....	7
1.6 Identify Shadowed Rules	7
1.7 Modify the Security Policy to Function Properly.....	7
1.8 Commit the Configuration	7
1.9 Test the Modified Security Policy Rule	7
1.10 Generate Application Traffic.....	7
1.11 Research Applications.....	8
1.12 Update Security Policy Rules	8
1.13 Commit the Configuration	8
1.14 Test the Updated Security Policy Rules	9
1.15 Enable the Application Block Page	9
1.16 Commit the Configuration	9
1.17 Test the Application Block Page.....	9
2 Controlling Application Usage with App-ID – Detailed Lab Steps	10
2.1 Apply a Baseline Configuration to the Firewall.....	10
2.2 Configure an Application Group	14
2.3 Configure a Security Policy Rule to Allow Firewall Update Traffic.....	16
2.4 Test the Allow-PANW-Apps Security Policy Rule	21
2.5 Identify Shadowed Rules	22
2.6 Modify the Security Policy to Function Properly.....	24
2.7 Test the Modified Security Policy Rule.....	27
2.8 Generate Application Traffic	29
2.9 Research Applications	31
2.10 Update Security Policy Rules	34
2.11 Test the Updated Security Policy Rules.....	39
2.12 Enable the Application Block Page	42
2.13 Test the Application Block Page	44

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.

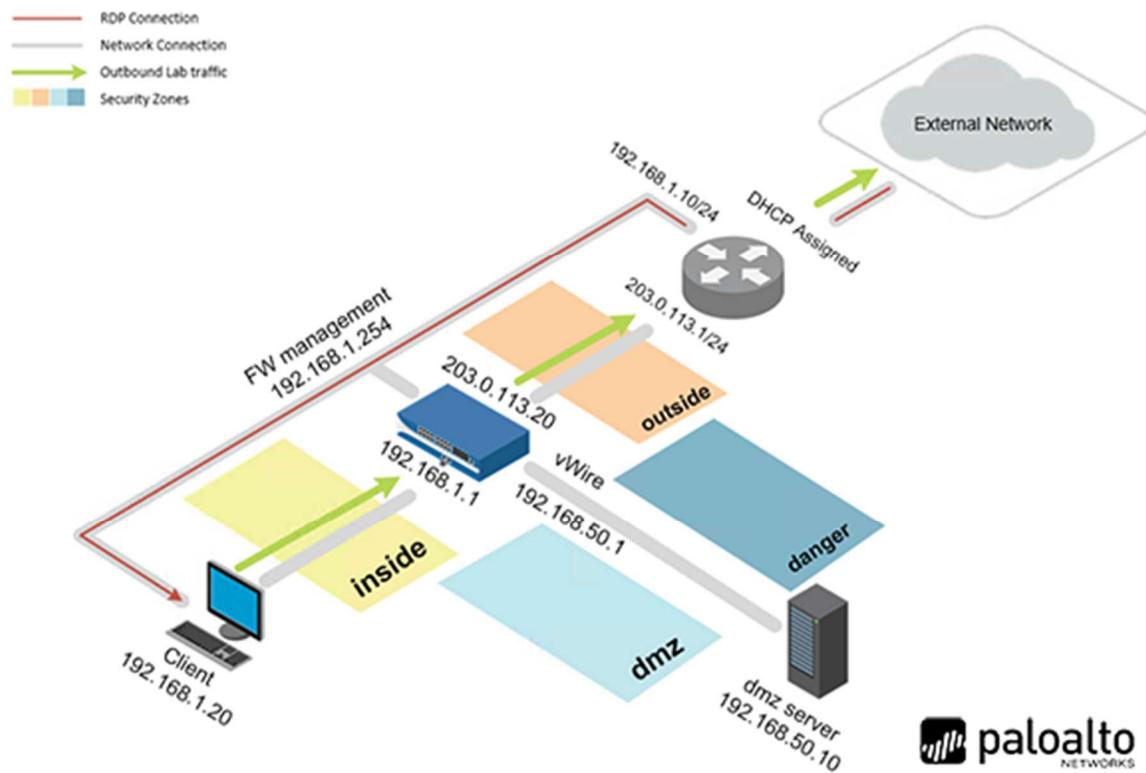
The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications that you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this 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:

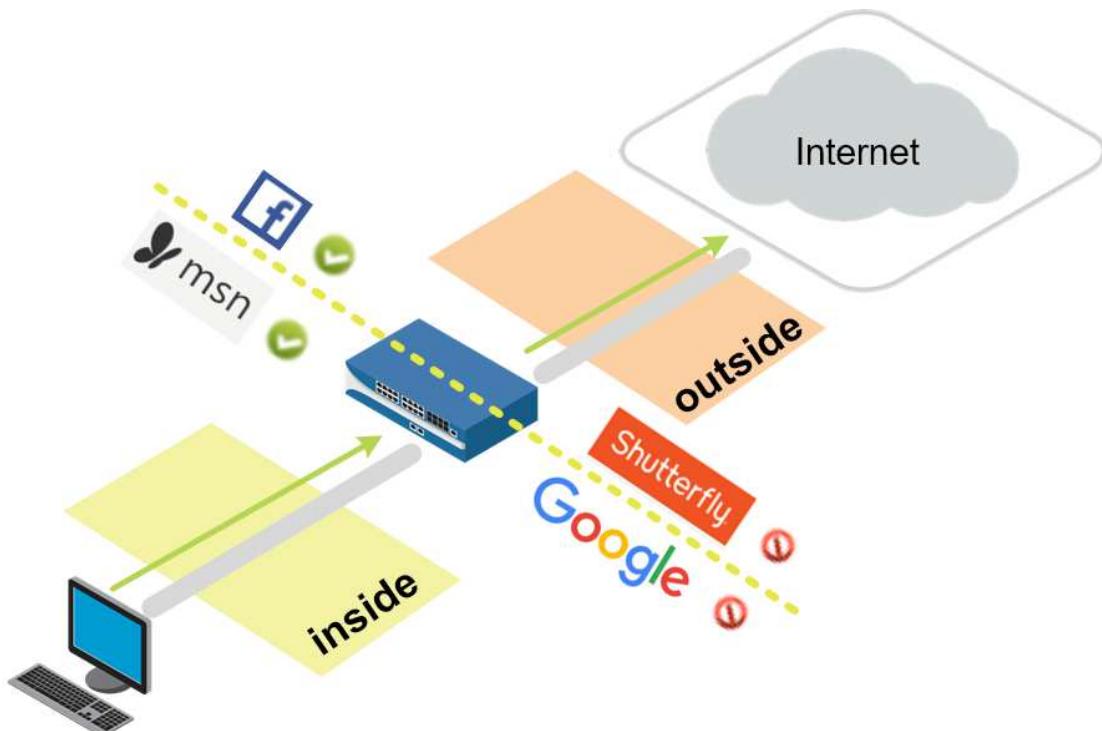
- Load a baseline configuration.
- Generate application traffic.
- Configure an application group.
- Configure a Security policy to allow update traffic.
- Test the Allow-PANW-Apps Security policy rule.
- Identify shadowed rules.
- Modify the Security policy to function properly.
- Test the modified Security policy rule.

Lab Topology



paloaltonetworks

Theoretical Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!
vRouter	192.168.1.10	root	PaloAlt0

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

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

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

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

Please
Note

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

1 Controlling Application Usage with App-ID - High Level Lab Steps

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

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-07.xml** to the Firewall.

1.2 Configure an Application Group

- Use the information below to create an Application Group

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

1.3 Configure a Security Policy Rule to Allow Update Traffic

- Use the information below to create a Security Policy rule to allow Palo Alto Networks update traffic.

Parameter	Value
Name	Allow-PANW-Apps
Description	Allows PANW apps for firewall
Source Zone	Users_Net
Source Address	192.168.1.254
Destination Zone	Internet
Destination Address	Any
Applications	paloalto-apps
Service	application-default
URL Category	Any
Action	Allow
Log At Session End	Enabled

1.4 Commit the Configuration

- Commit the changes before proceeding.

1.5 Test the Allow-PANW-Apps Security Policy Rule

- On the firewall, use the **Check Now** option for Dynamic Updates to test the Security Policy rule – **Allow-PANW-Apps**.
- Create and apply a filter to search for log entries that contain the application **paloalto-updates**.
- Note which rule allowed the application traffic to pass through the firewall.
- Determine why the firewall traffic did not hit the **Allow-PANW-Apps** rule.

1.6 Identify Shadowed Rules

- Use the **Tasks Manager – All Tasks** window to locate the most recent entry for **Commit** under **Type**.
- Use the information in the **Rule Shadow** tab to determine why firewall traffic did not hit the **Allow-PANW-Apps** rule.

1.7 Modify the Security Policy to Function Properly

- Use the information below to update the **Users_to_Internet** Security Policy rule to allow only specific applications (instead of any).

Parameter	Value
Applications	dns ping ssl web-browsing

1.8 Commit the Configuration

- Commit the changes before proceeding.

1.9 Test the Modified Security Policy Rule

- On the firewall, use the **Check Now** option for Dynamic Updates to test the Security Policy rule – **Allow-PANW-Apps**.
- Create and apply a filter to search for log entries that contain the application **paloalto-updates**.
- Note which rule allowed the application traffic to pass through the firewall.

1.10 Generate Application Traffic

- Generate application traffic by double-clicking on the icon for **App Generator**.
- Allow the script to complete.
- Examine the **Traffic Log** and note the entries under the **Application** column for the Client-A host.
- Use the information in the columns for **Application**, **Action** and **Rule** to answer the following questions.
 - Are there any applications that you should not allow from the **Users_Net** zone to the **Extranet** zone?

- Are there any applications being denied from the Users_Net zone that you should allow?

1.11 Research Applications

- Use the Application database on the firewall to research one of the three applications below:
 - dailymotion
 - yammer-base
 - scribd-base
- Answer the following questions about the application you have chosen to research:
 - What category does the application fall into?
 - What risk level has Palo Alto Networks assigned to the application?
 - What are some of the characteristics of this application that might make you want to block its use on your network?
 - Should you allow this application on your company's production network?

1.12 Update Security Policy Rules

- Edit the **Users_to_Extranet** Security Policy rule and allow only the following applications:
 - web-browsing
 - ssl
 - ssh
 - ping
 - dns
 - ldap
 - radius
- Edit the **Users_to_Internet** Security Policy rule and allow only the following applications and their dependencies.
 - dns
 - ping
 - ssl
 - web-browsing
 - yelp
 - dropbox
 - ms-office365

1.13 Commit the Configuration

- Commit the changes before proceeding.

1.14 Test the Updated Security Policy Rules

- Run the Traffic Generator script again on the Client-A desktop.
- Create and apply a filter in the **Traffic** log to display sessions that the firewall has blocked.

Note the applications that are now being blocked.

1.15 Enable the Application Block Page

- To see the kind of behavior a user will experience without the **Application Block Page** enabled, open the Firefox web browser and attempt to connect to <http://www.shutterfly.com>.
- Note how the browser responds.
- Enable the **Application Block Page** under **Device > Response Pages**.

1.16 Commit the Configuration

- Commit the changes before proceeding.

1.17 Test the Application Block Page

- To see the kind of behavior a user will experience with the **Application Block Page** enabled, open the Firefox web browser and attempt to connect to <http://www.shutterfly.com>.
- Note how the browser responds.

2 Controlling Application Usage with App-ID – Detailed Lab Steps

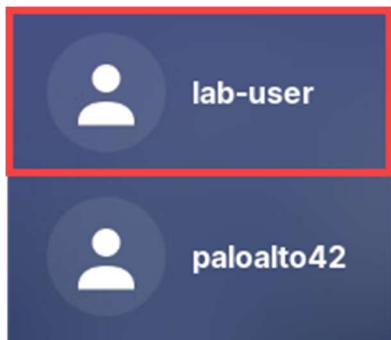
2.1 Apply a Baseline Configuration to the Firewall

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

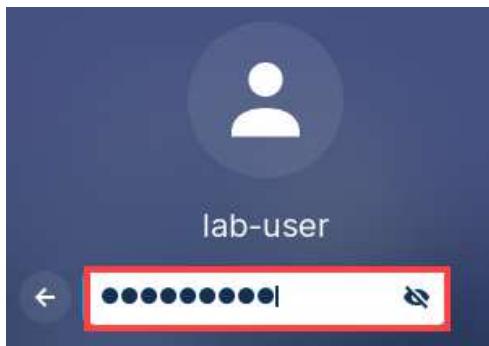
1. Click on the **Client** tab to access the Client PC.



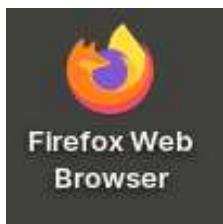
2. On the *Zorin* desktop, click **lab-user**.



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



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



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



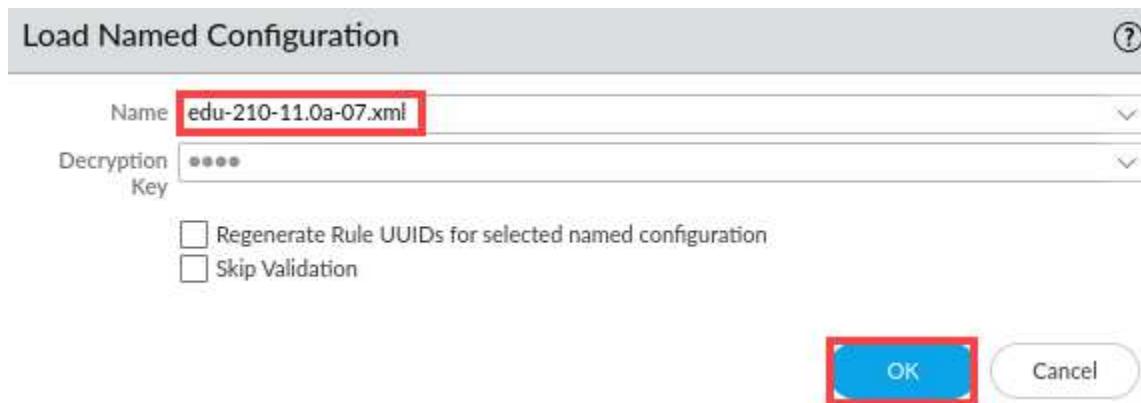
6. Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.



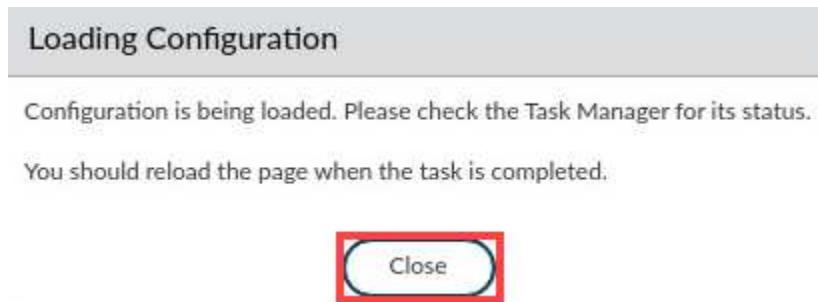
If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

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

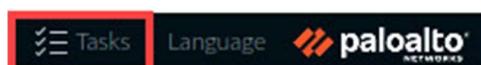
8. In the *Load Named Configuration* window, select **edu-210-11.0a-07.xml** from the *Name* drop-down box and click **OK**.



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 been completed. Click **Close**

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

Show: All Tasks | Close Commit Queue | Close

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



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

Commit

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

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

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

Preview Changes Change Summary Validate Commit

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

Description

Commit **Cancel**

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

Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

Commit

Close

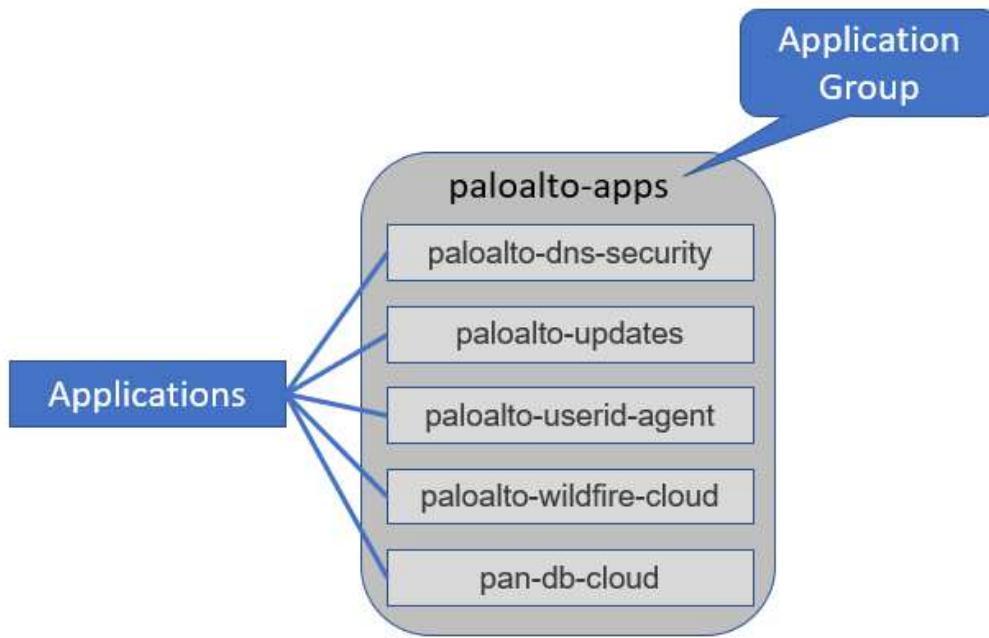


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

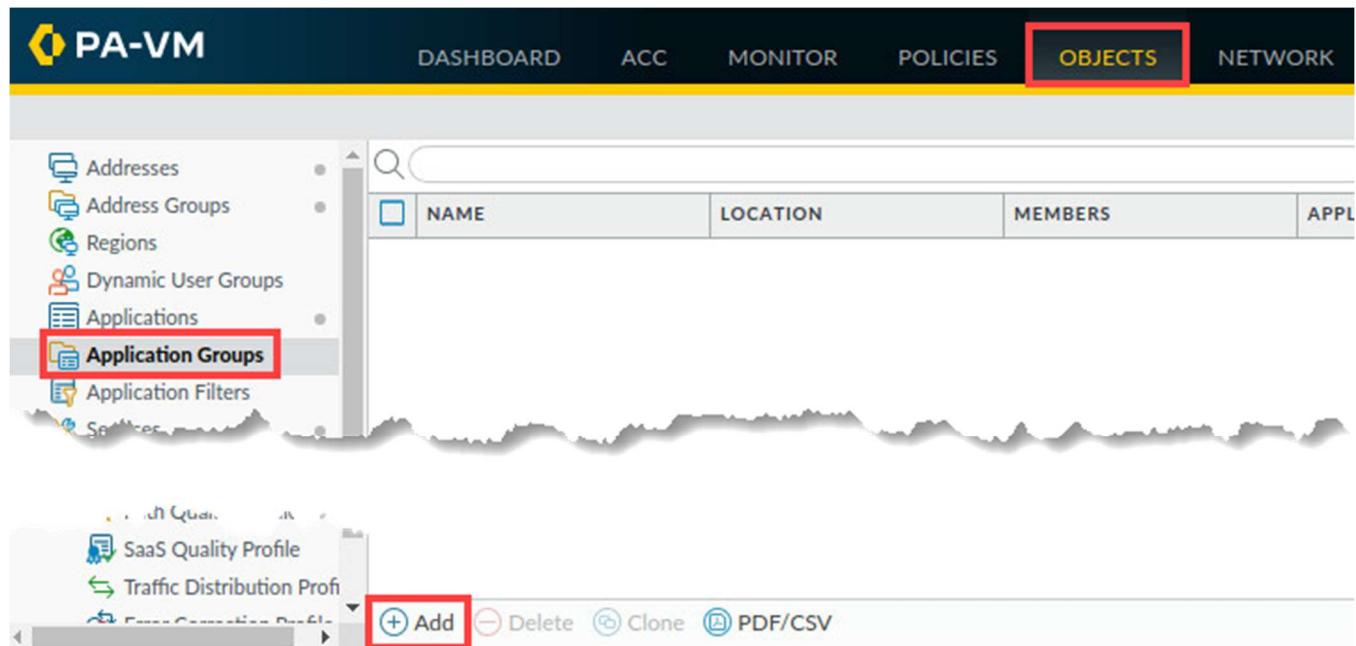
15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.2 Configure an Application Group

In this section, you will configure an application group called `paloalto-apps` that includes some Palo Alto Networks applications. The firewall uses these applications 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.

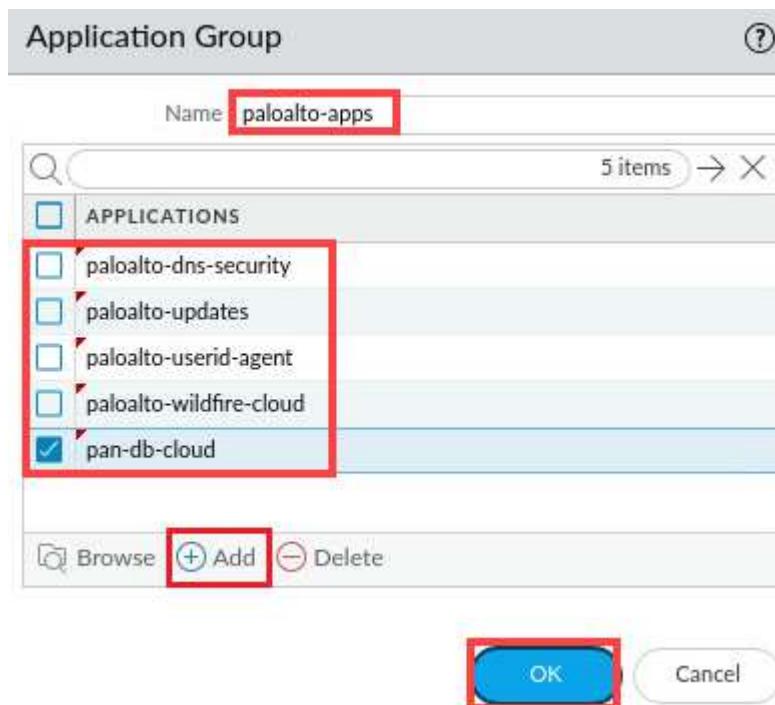


1. Navigate to **Objects > Application Groups**. Click **Add**.



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


Please Note

Note that we are only adding a few of the Palo Alto Networks entries to this group as an example of how to create an Application Group. The list you are building here is not necessarily inclusive of all Palo Alto Networks applications that you might need to allow in a production environment.

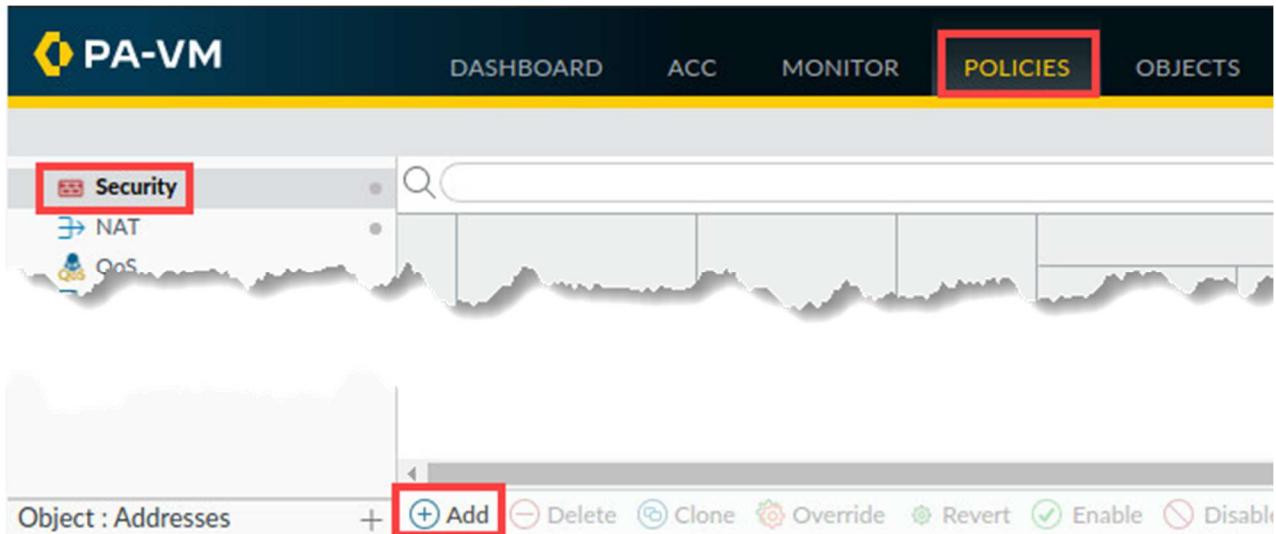
You can also use the Browse button in the Application Group window to add these entries.

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

2.3 Configure a Security Policy Rule to Allow Firewall 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 specify only what should be blocked.

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



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

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

3. 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 type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> Users_Net	<input checked="" type="checkbox"/> 192.168.1.254
(+ Add) (- Delete)	(+ Add) (- Delete)

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

Parameter	Value
Destination Zone	Internet
Destination Address	Any

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"/> Internet	
(+ Add) (- Delete)	(+ Add) (- Delete)

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

Parameter	Value
Applications	paloalto-apps

General | Source | Destination | **Application**

<input type="checkbox"/> Any
<input type="checkbox"/> APPLICATIONS ^
<input checked="" type="checkbox"/> paloalto-apps
(+ Add) (- Delete)

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.

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

The screenshot shows a navigation bar with tabs: General, Source, Destination, Application, Service/URL Category (which is highlighted with a red box), and Actions. Below the tabs is a dropdown menu set to "application-default". To the right of the dropdown is a checkbox labeled "Any" which is checked. There are also "SERVICE" and "URL CATEGORY" dropdowns.

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

Parameter	Value
Action	Allow
Log Setting	Log at Session End

The screenshot shows the "Security Policy Rule" dialog box. The "Actions" tab is selected (highlighted with a red box). In the "Action Setting" section, "Action" is set to "Allow". In the "Log Setting" section, "Log at Session End" is checked (highlighted with a red box). At the bottom right are "OK" and "Cancel" buttons, with "OK" 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-from-Known...	none	universal	Internet	Palo Alto Netw... Palo Alto Netw... Palo Alto Netw...
2	Block-to-Known-Ba...	none	universal	Extranet 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: 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 is complete, notice that there is an additional tab available for **Rule Shadow**. Click **Close**.



Please
Note

This tab only appears when you have a rule that shadows other rules.
You will fix the rule shadow issue in a later section of the lab.

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

2.4 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	RELEASE DATE
Antivirus	Last checked: 2023/07/19 21:07:07 UTC Schedule: None					
8725-8125	panupv2-all-content-8725-8125	Apps, Threats	Full	66 MB	676fa9d...	2023/07/19 21:07:07 UTC
8726-8134	panupv2-all-contents-8726-8134	Apps, Threats	Full	67 MB	6730160...	2023/07/19 21:07:07 UTC
8727-8140	panupv2-all-contents-8727-8140	Apps, Threats	Full	67 MB	0e1fd8c...	2023/07/19 21:07:07 UTC
8728-8146	panupv2-all-contents-8728-8146	Apps, Threats	Full	67 MB	c022dec...	2023/07/19 21:07:07 UTC
8729-8157	panupv2-all-contents-8729-8157	Apps, Threats	Full	67 MB	643f10be...	2023/07/19 21:07:07 UTC
8730-8159	panupv2-all-contents-8730-8159	Apps, Threats	Full	67 MB	d75fa69b...	2023/07/19 21:07:07 UTC
8731-8161	panupv2-all-contents-8731-8161	Apps, Threats	Full	67 MB	15d2a70...	2023/07/19 21:07:07 UTC

Check Now

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.

The screenshot shows the Palo Alto VM interface with the 'MONITOR' tab selected. In the left sidebar, 'Logs' is expanded, and 'Traffic' is selected. A search bar at the top contains the filter `(app eq paloalto-updates)`. The main pane displays a table of traffic logs. The columns are: #, RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, APPLICATION, RULE, ACTION, DESTINATION, SOURCE USER, and DESTIN. GROUP. The table shows multiple entries where the application is 'paloalto-updates' and the rule is 'Users_to_Internet' with an 'allow' action. The destination IP addresses listed are 34.96.84.34, 34.96.84.34, 34.96.84.34, 34.96.84.34, 107.178.249.2..., 107.178.249.2..., 35.190.82.33, and 34.96.84.34.

Please Note

Leave this filter in place for later testing in this lab.

Q1. Which rule allowed the application traffic to pass through the firewall?

- a. Users_to_Internet
- b. egress-inside-content-id
- c. Inside_Nets_to_Internet
- d. Users_to_Extranet

Q2. Once the `Users_to_Internet` rule is matched and the firewall allows traffic, there is no reason for the firewall to continue comparing packet characteristics to any following rules due to the "shadows" effect, highlighting the importance of rule order?

- a. True
- b. False

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

2.5 Identify Shadowed Rules

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.

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



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

JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
19	Commit	Completed	2023/09/13 19:00:23	Commit Processing By: admin Start Time (Dequeued Time): 09/13/23 19:00:23 • Configuration committed successfully		admin
18	EDLFetch	Completed	2023/09/13 18:52:40	• Refresh timer was cancelled due to a commit job		System
17	Commit	Completed	2023/09/13 18:51:30	Commit Processing By: admin Start Time		admin

Show [All Tasks](#) [Clear Commit Queue](#) [Close](#)

- 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**.

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.

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

Task Manager - All Tasks						
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
19	Commit	Completed	2023/09/13 19:00:23	Commit Processing By: admin Start Time (Dequeued Time): 09/13/23 19:00:23 • Configuration committed successfully		admin
18	EDLFetch	Completed	2023/09/13 18:52:40	• Refresh timer was cancelled due to a commit job		System
17	Commit	Completed	2023/09/13 18:51:30	Commit Processing By: admin Start Time		admin

Show

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

2.6 Modify the Security Policy to Function Properly

In this section, you will modify your Security policy to ensure that the firewall update traffic hits the Allow-PANW-Apps rule.

- In the web interface, navigate to **Policies > Security**. Highlight the **Allow-PANW-Apps** but do not open it.

	Source	Destination	Action	Profile	Condition	Target	Order
4	Users_to_Internet	none	universal	Users_Net	any	any	any
5	Extranet_to_Internet	none	universal	Extranet	any	any	any
6	Allow-PANW-Apps	none	universal	Users_Net	192.168.1.254	any	any
7	intrazone-default	none	intrazone	any	any	any	any
8	interzone-default	none	interzone	any	any	any	any

- Drag and drop the **Allow-PANW-Apps** entry to the correct location, or you can use the **Move** button at the bottom to place the rule in the right spot.

1	Block-from-Known-Bad-Addresses	none	universal
2	Block-to-Known-Bad-Addresses	none	universal
3	Users_to_Extranet	none	universal
4	<input checked="" type="checkbox"/> 1 selected row	none	universal
5	Extranet_to_Internet	none	universal
6	Allow-PANW-Apps	none	universal

- Confirm the *Allow-PANW-Apps* security policy is now labeled as the **3rd** security policy.

1	Block-from-Known-Bad-Addresses	none	universal
2	Block-to-Known-Bad-Addresses	none	universal
3	Allow-PANW-Apps	none	universal

- Click the **Commit** button at the upper 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

Commit **Cancel**

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

Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

Commit

Close

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

2.7 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.

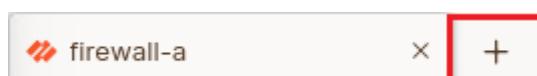
1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE
Antivirus	Last checked: 2023/07/19 21:07:07 UTC Schedule: None					
8725-8125	panupv2-all-contents-8725-8125	Apps, Threats	Full	66 MB	676fa9d...	2023/0 UTC
8726-8134	panupv2-all-contents-8726-8134	Apps, Threats	Full	67 MB	6730160...	2023/0 UTC
8727-8140	panupv2-all-contents-8727-8140	Apps, Threats	Full	67 MB	0e1fd8c1...	2023/0 UTC
8728-8146	panupv2-all-contents-8728-8146	Apps, Threats	Full	67 MB	c022dec...	2023/0 UTC
8729-8157	panupv2-all-contents-8729-8157	Apps, Threats	Full	67 MB	643f10be...	2023/0 UTC
8730-8159	panupv2-all-contents-8730-8159	Apps, Threats	Full	67 MB	d75fa69b...	2023/0 UTC
8731-8161	panupv2-all-contents-8731-8161	Apps, Threats	Full	67 MB	15d2a70...	2023/0 UTC

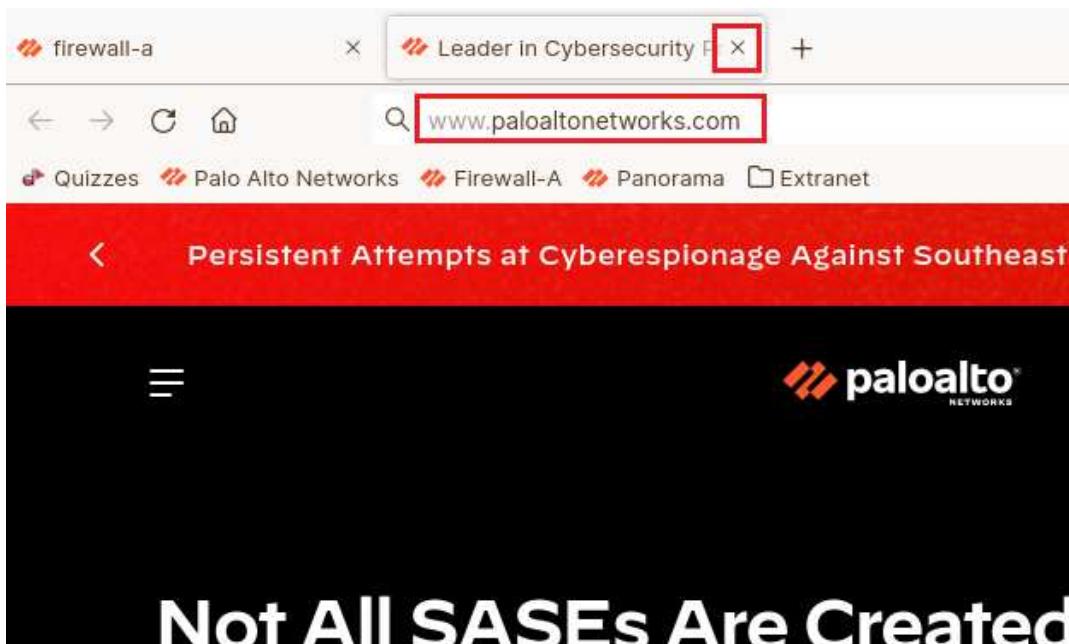
2. Select **Monitor > Logs > Traffic**. Ensure the following filter (`app eq paloalto-updates`) in the filter builder is applied. Refresh the logs by clicking on the **Apply Filter** button. Look for the log entries for the application *paloalto-updates*. It should be the “**Allow-PANW-Apps**” rule.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	APPLICATION	RULE	ACTION
09/13 19:40:51	end	Users_Net	Internet	192.168.1.254	paloalto-updates	Allow-PANW-Apps	allow
09/13 19:36:46	end	Users_Net	Internet	192.168.1.254	paloalto-updates	Users_to_Internet	allow

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



4. Type **www.paloaltonetworks.com** in the address bar and press **Enter**. Once you have verified the website will open, close the *Firefox* 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	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
	10/21 07:03:19	end	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns-base	allow	Users_to_Internet
	10/21 07:03:19	end	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns-base	allow	Users_to_Internet
	10/21 07:03:14	end	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns-base	allow	Users_to_Internet
	10/21 07:03:14	end	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns-base	allow	Users_to_Internet
	10/21 07:03:14	end	Users_Net	Internet	192.168.1.20	8.8.8.8	53	dns-base	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.

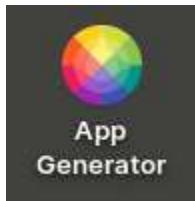
6. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



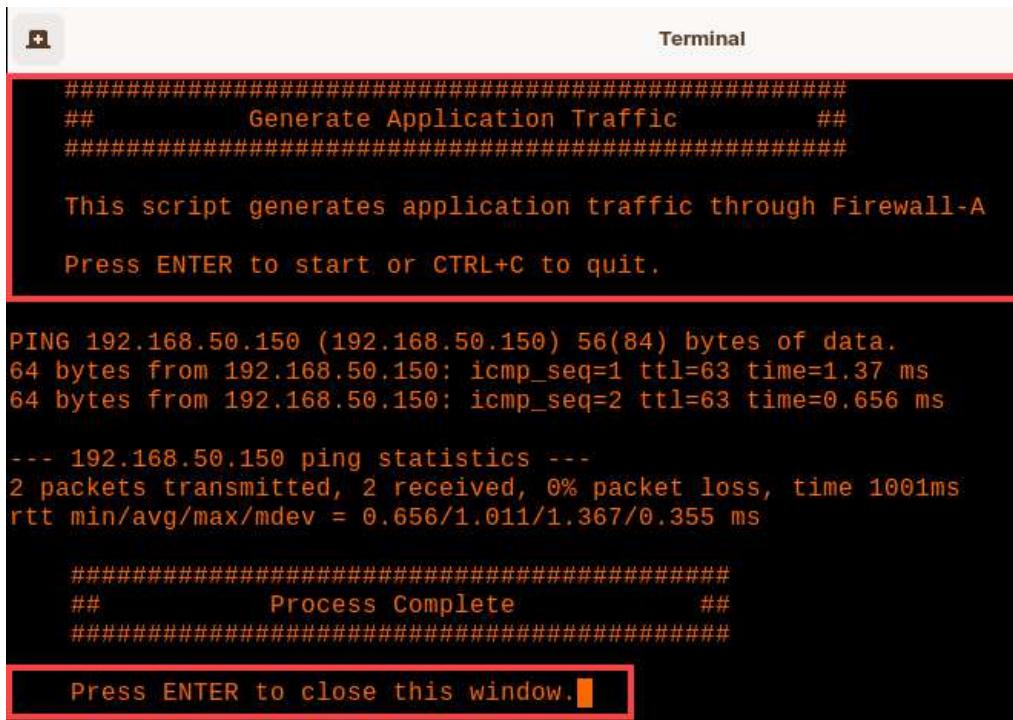
2.8 Generate Application Traffic

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

1. On the *client* desktop, generate application traffic by double-clicking the icon for **App Generator**.



2. 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.

A screenshot of a terminal window titled "Terminal". The window contains the following text:

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

This script generates application traffic through Firewall-A

Press ENTER to start or CTRL+C to quit.

PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=63 time=1.37 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=63 time=0.656 ms

--- 192.168.50.150 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.656/1.011/1.367/0.355 ms

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

Press ENTER to close this window.
```

3. Return to the *firewall-a – Mozilla Firefox* window by clicking on the **Firefox** icon in the taskbar of your client desktop.



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

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	APPLICATION	RULE
	09/13 20:11:01	end	Users_Net	Internet	192.168.1.20	web-browsing	Users_to_Internet
	09/13 20:06:51	end	Users_Net	Internet	192.168.1.20	ssl	Users_to_Internet
	09/13 20:06:26	end	Users_Net	Internet	192.168.1.20	ssl	Users_to_Internet
	09/13 20:06:01	end	Users_Net	Internet	192.168.1.20	web-browsing	Users_to_Internet
	09/13 20:02:39	end	Users_Net	Internet	192.168.1.20	gotomeeting-base	Users_to_Internet
	09/13 20:02:36	end	Users_Net	Extranet	192.168.1.20	web-browsing	Users_to_Extranet
	09/13 20:02:36	end	Users_Net	Internet	192.168.1.20	youku-base	Users_to_Internet
	09/13 20:02:34	end	Users_Net	Internet	192.168.1.20	yelp-base	Users_to_Internet
	09/13 20:02:34	end	Users_Net	Internet	192.168.1.20	yammer-base	Users_to_Internet

Please
Note

You should see entries for a variety of applications. Some of the entries will be recognizable and others will be for applications you may never have heard of.

Q3. Which of the following options best represents the approach to allowing applications from the Users_Net zone to the Extranet zone?

- a. Allow all applications without restriction.
- b. Allow only specific applications based on a defined policy.
- c. Block all applications from the Users_Net zone to the Extranet zone.
- d. Monitor and allow applications on a case-by-case basis.
- e. All of the above.

Q4. Are there any applications being denied from the Users_Net zone that you should allow?

- a. Continue denying all applications to maintain a strict security posture.
- b. Reevaluate and potentially allow specific denied applications based on security needs.
- c. Automatically allow all applications to enhance network flexibility.
- d. Block all applications permanently to minimize security risks.
- e. All of the above.

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

2.9 Research Applications

Now that you have access to detailed information about the applications in use in the network, you can use tools available from Palo Alto Networks to help answer the questions at the end of the last section. In this section, you will locate one application and find out more information about it so you can make an informed decision about whether to allow it onto your network or not.

1. In the **Traffic** log, enter the filter (**addr.src in 192.168.1.20**) and (**app eq dailymotion**) to search for the **dailymotion** application. Click the **Apply** icon.

The screenshot shows the Palo Alto Networks Traffic Log interface. The search bar contains the filter: `(addr.src in 192.168.1.20) and (app eq dailymotion)`. The results table has columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, APPLICATION, and RUM. A row for dailymotion is selected, highlighted with a red box. To the right, there is a toolbar with various icons, and one specific icon (a red box highlights the 'Apply' icon) is highlighted.

2. In the web interface, navigate to **Objects > Applications**. In the **Search** field, enter the name of the application as it appears in the Traffic log. Click the **magnifying glass** icon to search. Click directly on the **dailymotion** application below the **Name** column.

The screenshot shows the Palo Alto Networks Objects > Applications interface. The left sidebar has a tree view with 'Applications' selected and highlighted with a red box. The main area has a search bar with 'dailymotion' entered, and a magnifying glass icon is highlighted with a red box. Below the search bar is a table with columns: CATEGORY, SUBCATEGORY, RISK, and TAGS. Under 'Category' is 'media' and under 'Subcategory' is 'photo-video'. There is one entry with a risk of 4 and a 'Web App' tag. At the bottom, there is a table with columns: NAME, CATEGORY, SUBCATEGORY, RISK, and TAGS. One row is selected, showing 'dailymotion' in the NAME column, 'media' in CATEGORY, 'photo-video' in SUBCATEGORY, a risk of 4, and a 'Web App' tag.

3. The **Applications** database entry will display detailed information about the application.

Application

Name: dailymotion

Standard Ports: tcp/80,443

Depends on: ssl, web-browsing

Implicitly Uses:

Deny Action: drop-reset

Additional Information: [Wikipedia](#) [Google](#) [Yahoo!](#)

Description:

Dailymotion is a video hosting service website, based in Paris, France. Its domain name was registered one month after YouTube (but the site opened one month earlier) with gandi.net, a French internet domain name provider, and at least one name server is based in France with the .fr name extension.

Characteristics

Evasive: yes	Tunnels Other Applications: no
Excessive Bandwidth Use: yes	Prone to Misuse: yes
Used by Malware: no	Widely Used: yes
Capable of File Transfer: yes	
Has Known Vulnerabilities: yes	

Options

TCP Timeout (seconds): 3600	Customize...
TCP Half Closed (seconds): 120	Customize...
TCP Time Wait (seconds): 15	Customize...
App-ID Enabled: yes	

Classification

Category: media
Subcategory: photo-video
Risk: 4 Customize...

Tags

Edit

Close

Q5. What category does the application fall into?

- a. networking
- b. unknown
- c. media
- d. business-systems

Q6. What risk level has Palo Alto Networks assigned to the application?

- a. Level 1
- b. Level 2
- c. Level 3
- d. Level 4
- e. Level 5

Q7. What are some of the characteristics of this application that might make you want to block its use on your network?

- a. Evasive
- b. Widely Used
- c. Prone to Misuse
- d. Capable of File Transfer

e. All of the above.

Q8. What ports does the dailymotion application support?

- a. FTP/ 21
- b. TCP/ 80,443
- c. Telnet/ 23
- d. SMTP/ 25
- e. None of the above.

4. Click **Close** on the Application window.

Application

?

<p>Name: dailymotion</p> <p>Standard Ports: tcp/80,443</p> <p>Depends on: ssl, web-browsing</p> <p>Implicitly Uses:</p> <p>Deny Action: drop-reset</p> <p>Additional Information: Wikipedia Google Yahoo!</p>	<p>Description:</p> <p>Dailymotion is a video hosting service website, based in Paris, France. Its domain name was registered one month after YouTube (but the site opened one month earlier) with gandi.net, a French internet domain name provider, and at least one name server is based in France with the .fr name extension.</p>										
<p>Characteristics</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Evasive: yes</td> <td style="width: 50%;">Tunnels Other Applications: no</td> </tr> <tr> <td>Excessive Bandwidth Use: yes</td> <td>Prone to Misuse: yes</td> </tr> <tr> <td>Used by Malware: no</td> <td>Widely Used: yes</td> </tr> <tr> <td>Capable of File Transfer: yes</td> <td></td> </tr> <tr> <td>Has Known Vulnerabilities: yes</td> <td></td> </tr> </table>		Evasive: yes	Tunnels Other Applications: no	Excessive Bandwidth Use: yes	Prone to Misuse: yes	Used by Malware: no	Widely Used: yes	Capable of File Transfer: yes		Has Known Vulnerabilities: yes	
Evasive: yes	Tunnels Other Applications: no										
Excessive Bandwidth Use: yes	Prone to Misuse: yes										
Used by Malware: no	Widely Used: yes										
Capable of File Transfer: yes											
Has Known Vulnerabilities: yes											
<p>Options</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td>TCP Timeout (seconds): 3600</td> <td>Customize...</td> </tr> <tr> <td>TCP Half Closed (seconds): 120</td> <td>Customize...</td> </tr> <tr> <td>TCP Time Wait (seconds): 15</td> <td>Customize...</td> </tr> <tr> <td>App-ID Enabled: yes</td> <td></td> </tr> </table>		TCP Timeout (seconds): 3600	Customize...	TCP Half Closed (seconds): 120	Customize...	TCP Time Wait (seconds): 15	Customize...	App-ID Enabled: yes			
TCP Timeout (seconds): 3600	Customize...										
TCP Half Closed (seconds): 120	Customize...										
TCP Time Wait (seconds): 15	Customize...										
App-ID Enabled: yes											
<p>Classification</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Category: media</td> <td style="width: 50%;"></td> </tr> <tr> <td>Subcategory: photo-video</td> <td></td> </tr> <tr> <td>Risk: 4</td> <td>Customize...</td> </tr> </table>		Category: media		Subcategory: photo-video		Risk: 4	Customize...				
Category: media											
Subcategory: photo-video											
Risk: 4	Customize...										
<p>Tags</p> <div style="display: flex; align-items: center;"> <input style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;" type="button" value="Web App"/> Edit </div>											
Close											

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

2.10 Update Security Policy Rules

When you created the **Users_to_Extranet** and the **Users_to_Internet** Security Policy rules in an earlier lab, you set the **Application** to Any.

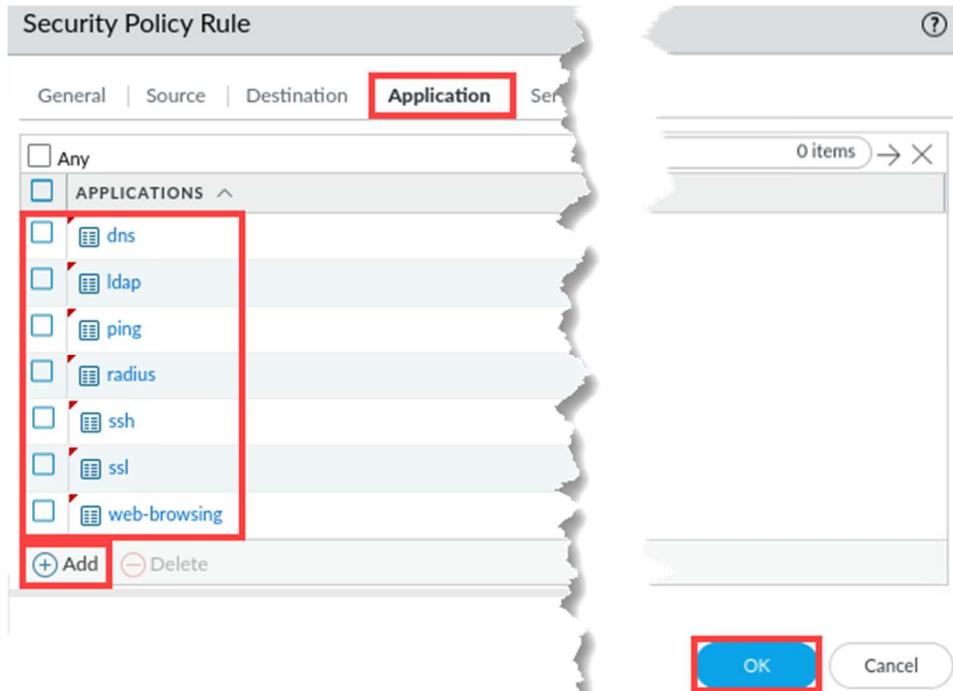
After your research, you can now update both rules to allow only applications that are necessary for your organization.

1. In the web interface, navigate to **Policies > Security**. Select the **Users_to_Extranet** security policy to edit it.

	NAME	TAGS	TYPE	ZONE	AC
1	Block-from-Known-...	none	universal	Internet	
2	Block-to-Known-Ba...	none	universal	Extranet	
3	Allow-PANW-Apps	none	universal	Users_Net	
4	Users_to_Extranet	none	universal	Users_Net	
5	Users_to_Internet	none	universal	Users_Net	
6	Extranet_to_Internet	none	universal	Extranet	
7	intrazone-default	none	intrazone	any	
8	interzone-default	none	interzone	any	

2. In the *Security Policy Rule* window, click the **Application** tab and uncheck the box for **Any**. Configure the following. Click **OK**.

Parameter	Value
Applications	ssl ssh ping dns ldap radius web-browsing

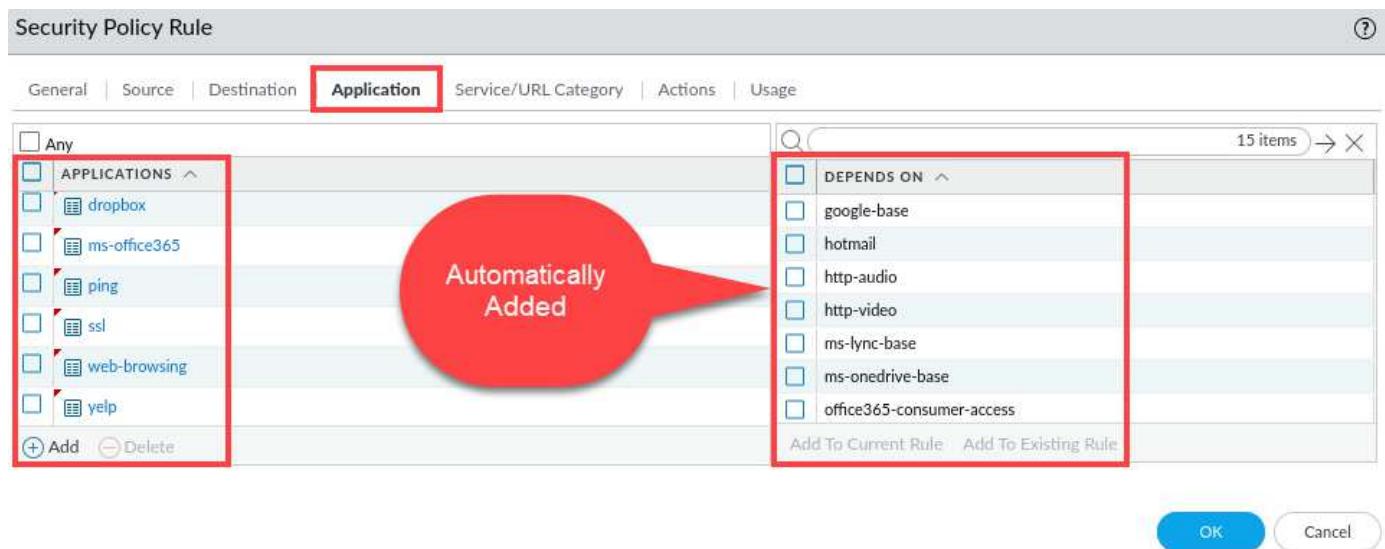


3. Select the **Users_to_Internet** security policy to edit it.

4	Users_to_Extranet	none	universal	Users_Net	any
5	Users_to_Internet	none	universal	Users_Net	any
6	Extranet_to_Internet	none	universal	Extranet	any
7	intrazone-default	none	intrazone	any	any
8	interzone-default	none	interzone	any	any

4. In the *Security Policy Rule* window, click the **Application** tab and uncheck the box for **Any**. Configure the following.

Parameter	Value
Applications	ping dns ssl yelp web-browsing dropbox ms-office365



Please
Note

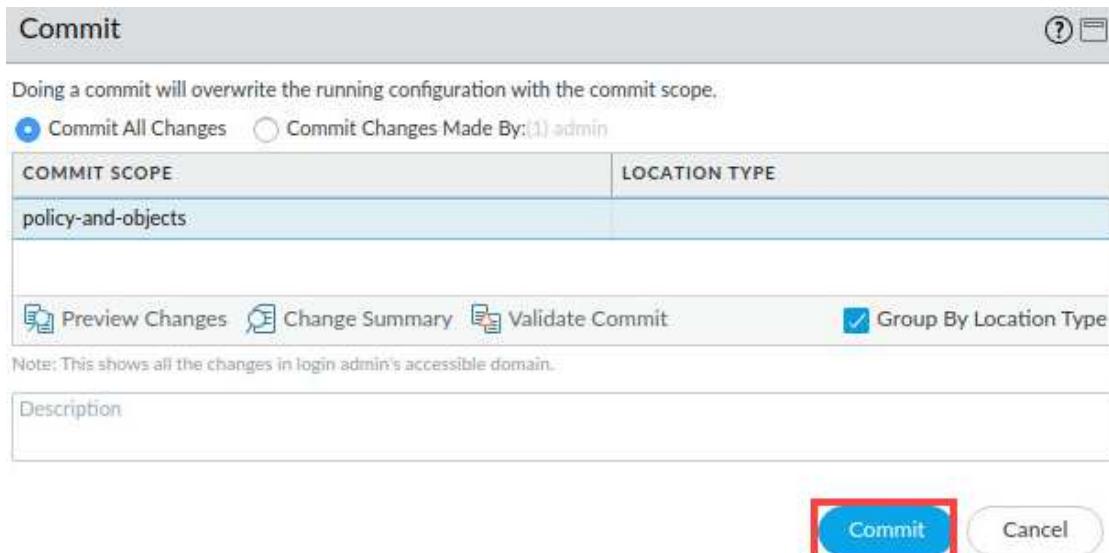
Note that the list of applications in the Depends On column may differ from the example shown here. Palo Alto Networks updates application definitions frequently, and in many cases an existing application will require additional applications to work correctly.

5. Place the check box next to **Depends On** to select all items in that column. Click **Add to Current Rule**.

6. Scan through the list of *Applications* on the left side of the window and note that the dependent applications have been added. Click **OK**.

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

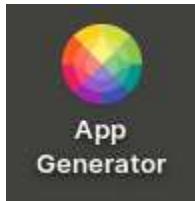


8. In the *Commit* window, click **Commit**.9. Wait until the *Commit* process is complete. Click **Close**.10. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

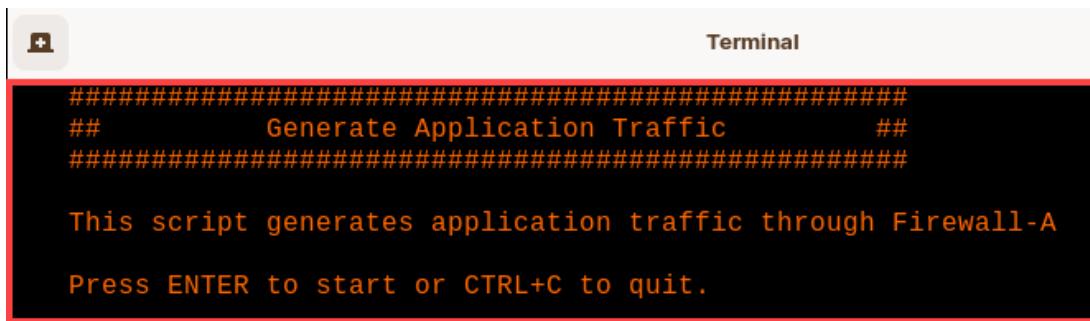
2.11 Test the Updated Security Policy Rules

In this section, you will run a short script and examine the results.

1. On the *client* desktop, generate application traffic by double-clicking the icon for **App Generator**.



2. 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.

A screenshot of a terminal window titled "Terminal". The window contains the following text:

```
#####
##      Generate Application Traffic      ##
#####
This script generates application traffic through Firewall-A
Press ENTER to start or CTRL+C to quit.
```

The text "Generate Application Traffic" is highlighted with a red rectangle.

Ignore any errors that the script generates – these occur because the firewall is blocking various application traffic types. The script may also pause at different points while applications time out because they are being blocked by the firewall.

```

Terminal
":{},"subTitleRichText":{"contentType":"hippostd:html","value":""},"subTitleFlagRichTextEditor":false,"paraGraphFlagRichTextEditor":false,"pricingparagraph":false,"docbaseProductPricing":null,"image":{"$ref":"/page/u5c8b1d6faf6d47089946c2d901c0e5bf"},"paragraph":"","cta":"SHOP WEDDING INVITES >","subtitle":"Effortlessly welcome your guests in signature style. ","imageCta":"","imageCtaUrl":"/t/wedding-invitations/","ctaUrl":null,"flipDirection":false,"ctaButtonDesignOptions":{"name":"brcmsrepo:ctaButtonDesignOptions","displayName":"brcmsrepo:ctaButtonDesignOptions","ctaButtonHoverDesign":"","ctaButtonDesign":"","useCTAButton":false,"contentType":"brcmsrepo:CTAButtonDesignOptions"},"title":"Custom Wedding Invitations","contentType":"brcmsrepo:ContentBlockEntity"}, {"name":"brcmsrepo:elements","displayName":"brcmsrepo:elements","hideBlock":false,"pricingimage":false,"pricingtitle":false,"blobBgProp":null,"paragraphRichTextEditor":{"contentType":"hippostd:html","value":""}}, "subTitleRichText":{"contentType":"hippostd:html","value":""}, "subTitleFlagRichTextEditor":false,"paraGraphFlagRichTextEditor":false,"pricingparagraph":false,"docbaseProductPricing":null,"image":{"$ref":"/page/u0604e9877ada48e3a936edb0fd8dcdf"},"paragraph":"","cta":"SHOP WEDDING GIFTS >","subtitle":"Say thanks with quality gifts they'll always cherish. ","imageCta":"","imageCtaUrl":"/wedding/wedding-gifts/","ctaUrl":null,"flipDirection":false,"ctaButtonDesignOptions":{"name":"brcmsrepo:ctaButtonDesignOptions","displayName":"brcmsrepo:ctaButtonDesignOptions","ctaButtonHoverDesign":"","ctaButtonDesign":"","useCTAButton":false,"contentType":"brcmsrepo:CTAButtonDesignOptions"},"title":"Gifts to Show Gratitude","contentType":"brcmsrepo:ContentBlockEntity"}, {"name":"brcmsrepo:elements","displayName":"brcmsrepo:elements","hideBlock":false,"pricingimage":false,"pricingtitle":false,"blobBgProp":null,"paragraphRichTextEditor":{"contentType":"hippostd:html","value":""}}, "subTitleRichText":{"contentType":"hippostd:html","value":""}, "subTitleFlagRichTextEditor":false,"paraGraphFlagRichTextEditor":false,"pricingparagraph":false,"docbaseProductPricing":null,"image":{"$ref":..

```

<p style="color:#FFF; font-family:arial,helvetica; font-weight:bold; margin-left:30px; margin-bottom:0px; font-size:48px; "> Hello World !

</p>
 <p style="color:#FFF; font-family:arial,helvetica; font-weight:bold; margin-left:30px; margin-bottom:0px; margin-top:2px; font-size:20px; "> My name is www.panw.lab.

</p>
 <p style="color:#FFF; font-family:arial,helvetica; font-weight:bold; margin-left:30px; margin-top:5px; font-size:20px; "> My address is 192.168.50.80.

</p></div>

</body>

</html>

PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.

64 bytes from 192.168.50.150: icmp_seq=1 ttl=63 time=0.436 ms

64 bytes from 192.168.50.150: icmp_seq=2 ttl=63 time=0.740 ms

--- 192.168.50.150 ping statistics ---

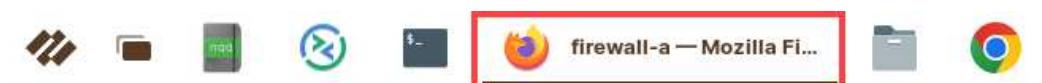
2 packets transmitted, 2 received, 0% packet loss, time 1005ms

rtt min/avg/max/mdev = 0.436/0.588/0.740/0.152 ms

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

Press ENTER to close this window.

3. Return to the *firewall-a – Mozilla Firefox* window by clicking on the **Firefox** icon in the taskbar of your client desktop.



4. In the web interface, select **Monitor > Logs > Traffic**. Clear any filters you may have in place. Create and apply the following new filter (`action neq allow`) in the filter builder. Note the entries in the *Application* column.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	APPLICATION	RULE	ACTION	DESTINATION	TO PORT	SESSION END REASON	BYTES	HTTP/2 CO ID
	09/14 00:41:39	deny	Users_Net	Internet	192.168.1.254	ntp-base	interzone-default	deny	64.79.100.196	123	policy-deny	90	0
	09/14 00:37:49	deny	Users_Net	Internet	192.168.1.254	ntp-base	interzone-default	deny	45.33.59.84	123	policy-deny	90	0
	09/14 00:37:29	deny	Users_Net	Internet	192.168.1.20	youku-base	interzone-default	reset-both	47.246.99.161	443	policy-deny	771	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	webex-base	interzone-default	deny	23.204.253.149	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	wechat-base	interzone-default	reset-both	43.159.18.10	443	policy-deny	771	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	viber-base	interzone-default	deny	104.112.23.13	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	twitter-base	interzone-default	reset-both	104.244.42.65	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	teamdrive-base	interzone-default	reset-both	18.195.149.18	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	tumblr-base	interzone-default	reset-both	192.0.77.40	443	policy-deny	771	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	scribd-base	interzone-default	reset-both	151.101.194.1...	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	sharefile-base	interzone-default	reset-both	104.106.172.95	443	policy-deny	797	0
	09/14 00:37:24	deny	Users_Net	Internet	192.168.1.20	showmax-base	interzone-default	reset-both	18.168.28.22	443	policy-deny	797	0

Please
Note

This filter will allow you to see the applications that have been blocked.

Many of the applications are now being blocked by the interzone-default rule. Remember that any application that is not explicitly allowed in a Security Policy rule will be blocked by the interzone-default rule.

The entries you see will differ from the example shown here.

5. Clear the filter in the Traffic Log. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

ORT	SESSION END REASON	BYTES	HTTP/2 CO ID
	policy-deny	90	0
	policy-deny	90	0

2.12 Enable the Application Block Page

When the firewall denies traffic to a web-based application, many users may assume that the Internet is down or slow or that there is something wrong with their browser settings.

To reduce the number of potential calls to the help desk, you can enable the Application Block Page on the firewall. This setting presents a web page that informs users when the firewall has blocked a web-based application.

By default, the Application Block Page is not enabled.

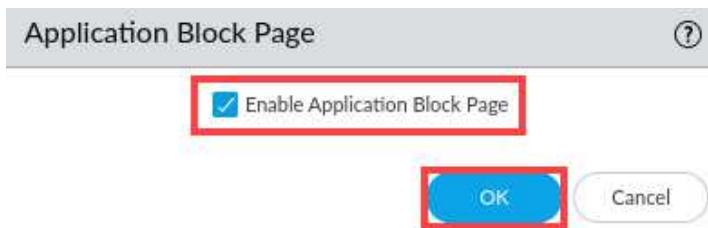
1. To see the kind of behavior a user will experience without the Application Block page enabled, open a new tab in the Firefox web browser. Attempt to connect to <http://www.shutterfly.com>. Close the new **Firefox** tab.



2. In the firewall web interface, navigate to **Device > Response Pages**. Under the **Action** column in the row for **Application Block Page**, click the link for **Disabled**.

TYPE	ACTION	LOCATION
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Disabled	Default
Captive Portal Comfort Page		Default
Data Filtering Block Page		Default

3. In the *Application Block Page* window, place a check in the box for **Enable Application Block Page**. Click **OK**.



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



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

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
device-and-network	Device and Network Configuration			

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

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

2.13 Test the Application Block Page

In this section, you will test the *Application Block Page* when attempting to run a blocked application.

1. To see the kind of behavior a user will experience with the Application Block page enabled, open a new tab in the **Firefox** browser.



2. Attempt to connect to <http://www.shutterfly.com>.

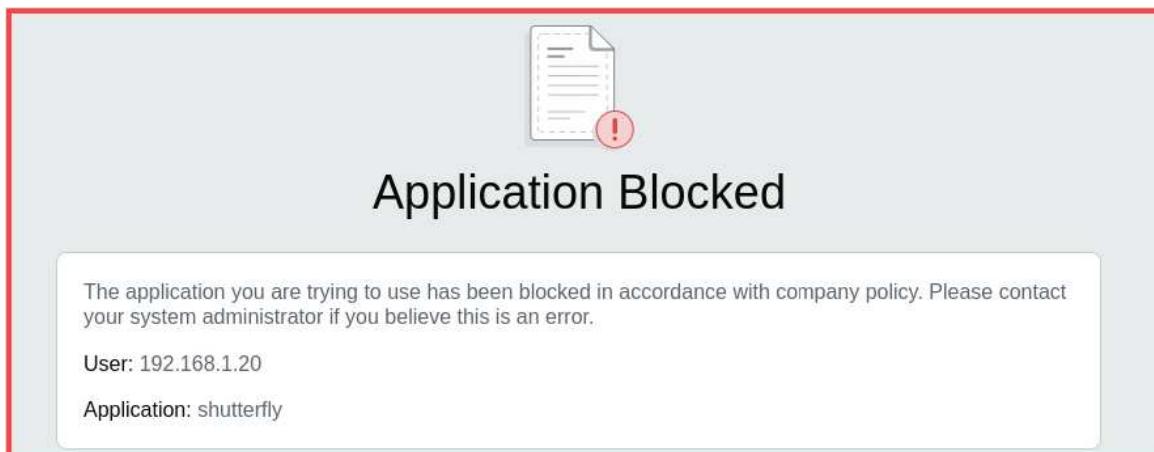


Be sure to use http in the request and be sure to use the Firefox browser for this test.

The number of websites which still support HTTP is dwindling. And, some browsers (such as Chrome) automatically send requests using HTTPS even if you specify HTTP.

This test is only to show you how to enable the block page. In order for the firewall to determine an application inside encrypted web traffic (HTTPS), you need to enable decryption which is covered in a later section of this course.

3. The firewall will present a web page indicating that the application has been blocked.

**Please Note**

You can customize this page to include additional information if necessary. This is the default page that the firewall presents.

Response Pages must also be enabled on the Interface Management Profile assigned to the firewalls interface that is required to respond.

4. Close the *Application Blocked* tab in the **Firefox** browser.

**Please Note**

There are limitations to the Application Block Page. The firewall cannot present the page to a user when the browser session is encrypted using HTTPS. Doing so would interrupt the secure communication between the client and the destination server and violate the rules of encryption.

However, you can configure and enable decryption on the firewall (which we cover in a later module). With decryption enabled, the firewall can present the Application Block Page to a web browser when a user attempts to access a blocked application.

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