PALO ALTO NETWORKS 11.0 FIREWALL ESSENTIALS

Lab 7: Controlling Application Usage with App-ID

Document Version: 2025-10-13

Contents

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.

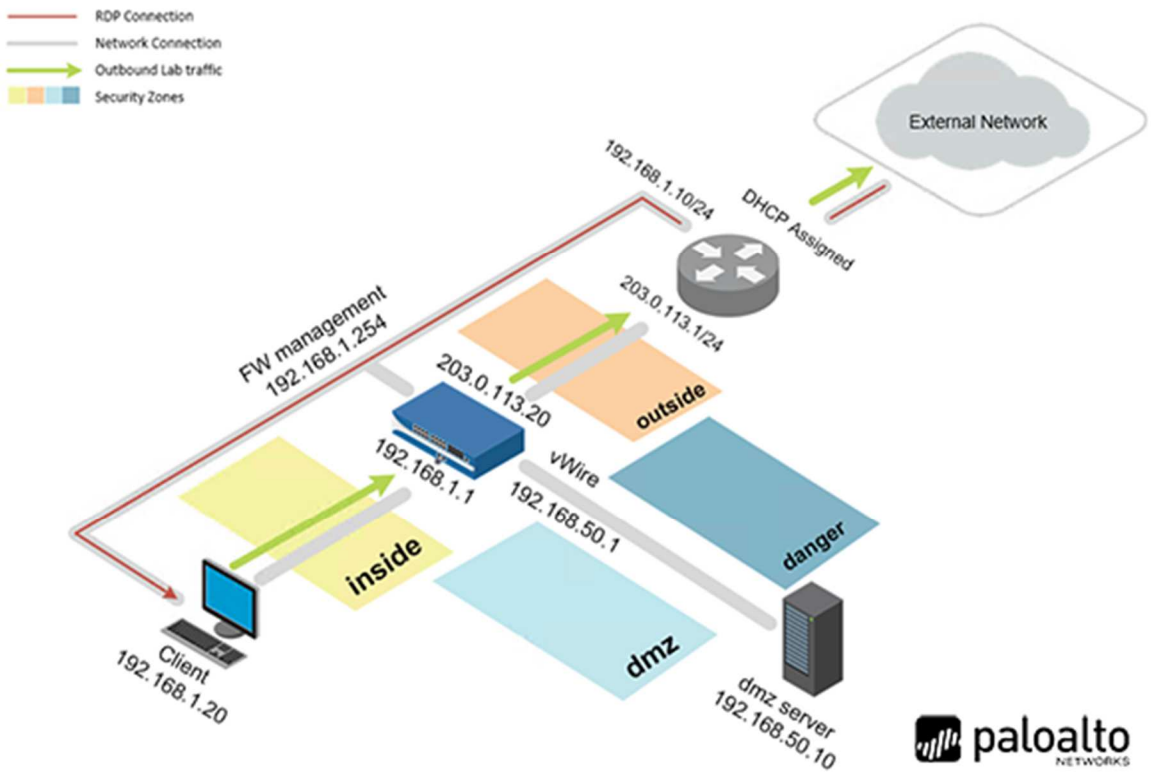
The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications that you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this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

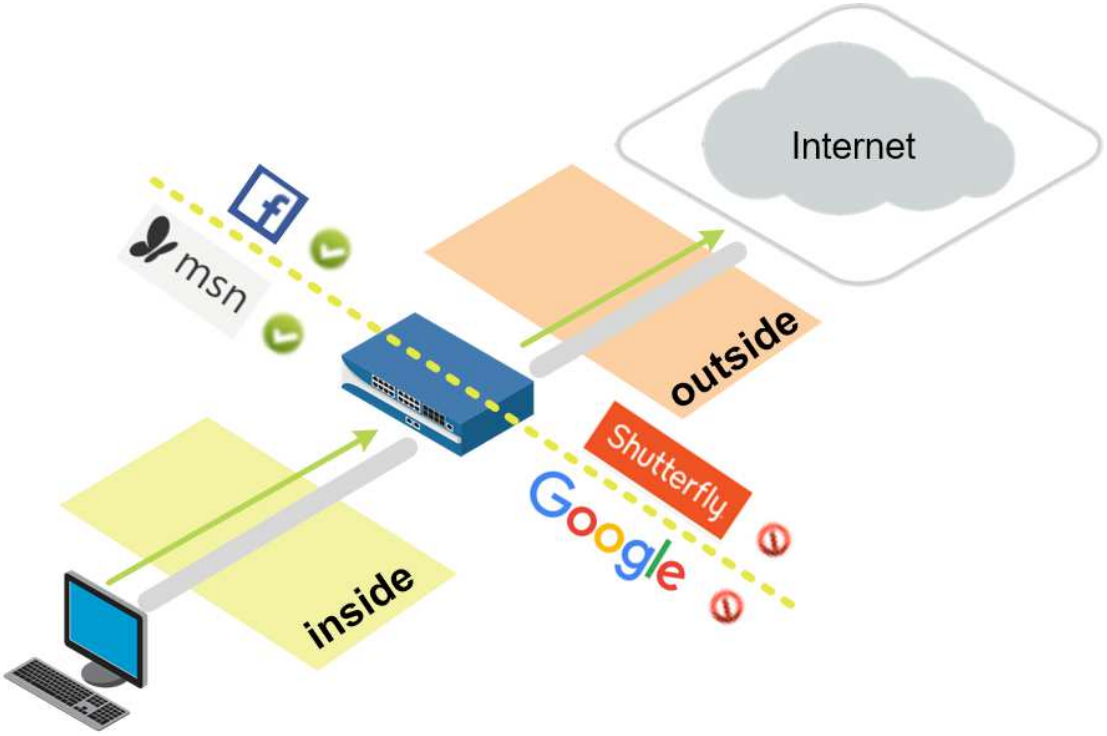
In this lab, you will perform the following tasks:

- 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



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`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

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.

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

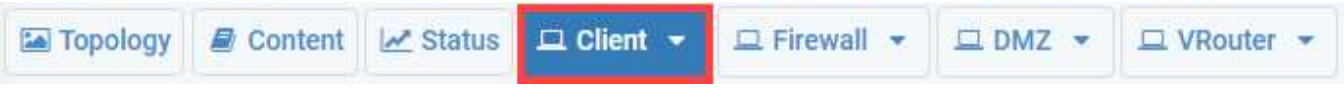
- To see the kind of behavior a user will experience with the **Application Block Page** enabled, open the Firefox web browser and attempt to connect to **http://www.shutterfly.com**.
- Note how the browser responds.

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

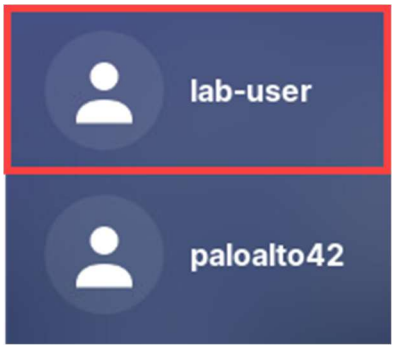
2.1 Apply a Baseline Configuration to the Firewall

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

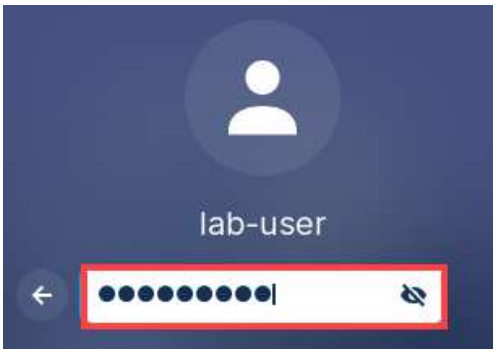
1. Click on the **Client** tab to access the Client PC.



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

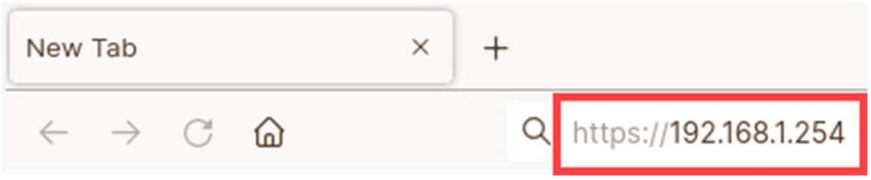


3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



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

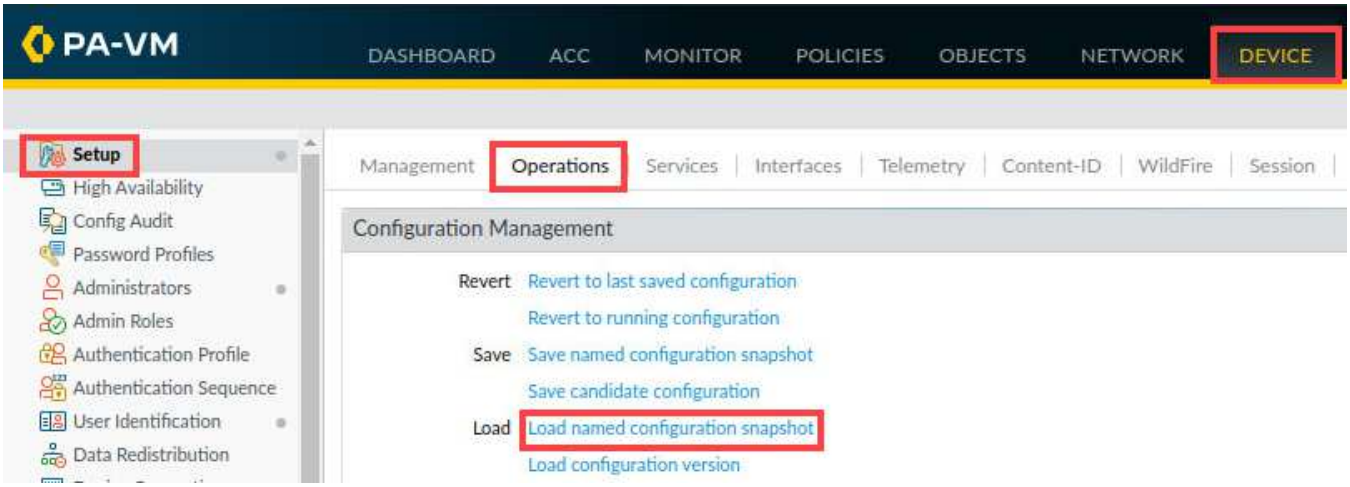
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



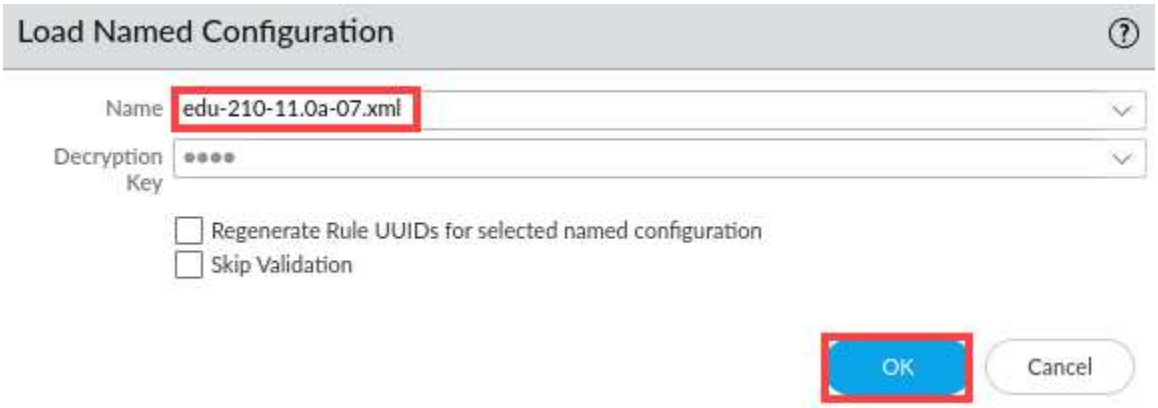
6. Log in to the Firewall web interface as username **admin**, password **`Pal0Alt0!.`**

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.

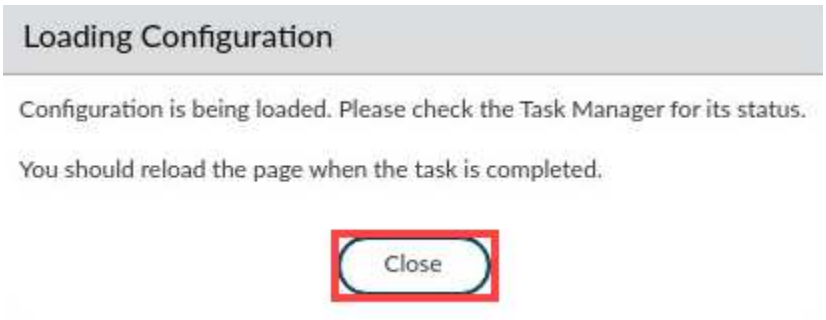
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



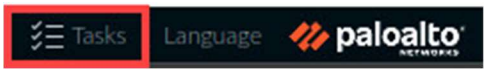
8. In the *Load Named Configuration* window, select **edu-210-11.0a-07.xml** from the *Name* drop-down box and click **OK**.



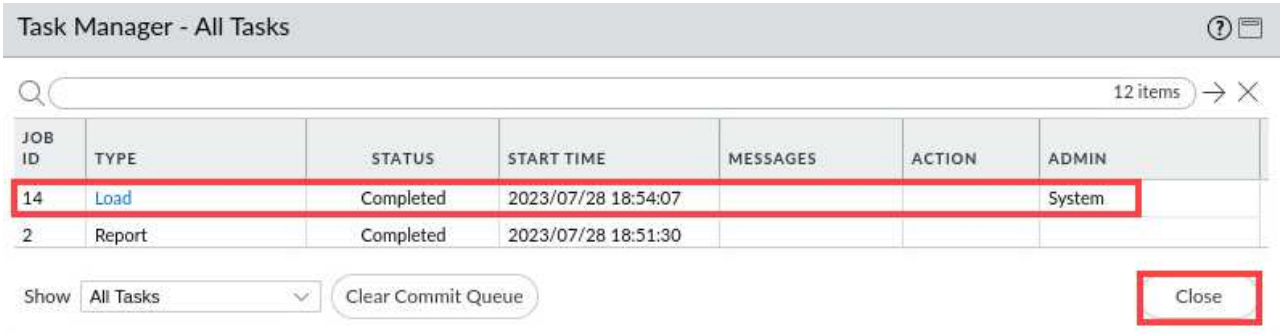
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

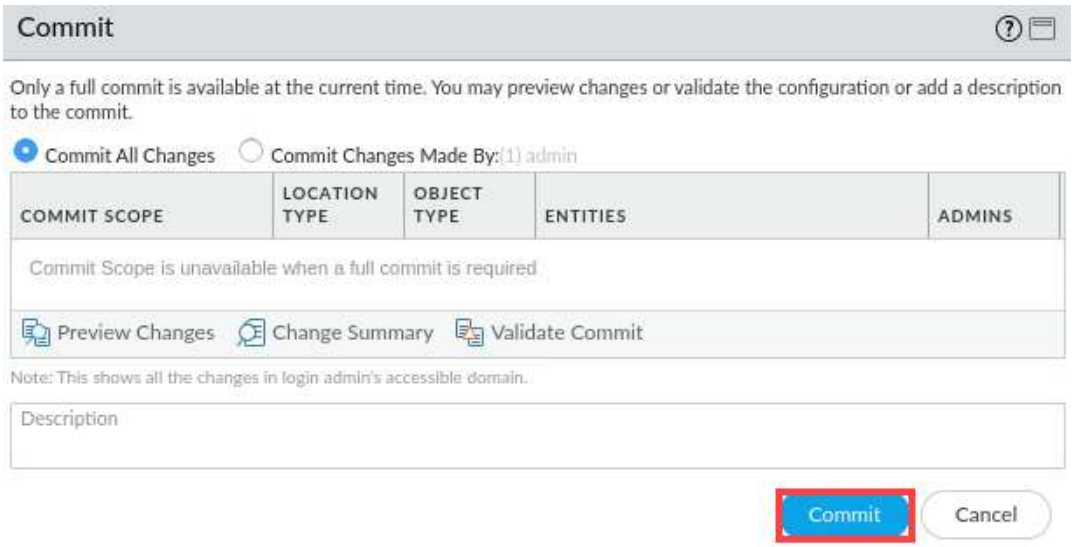


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

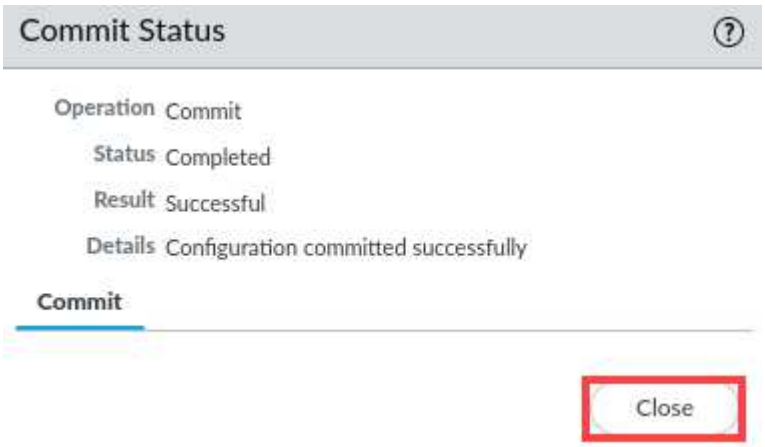


12. Click the **Commit** link located at the top-right of the web interface.

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



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

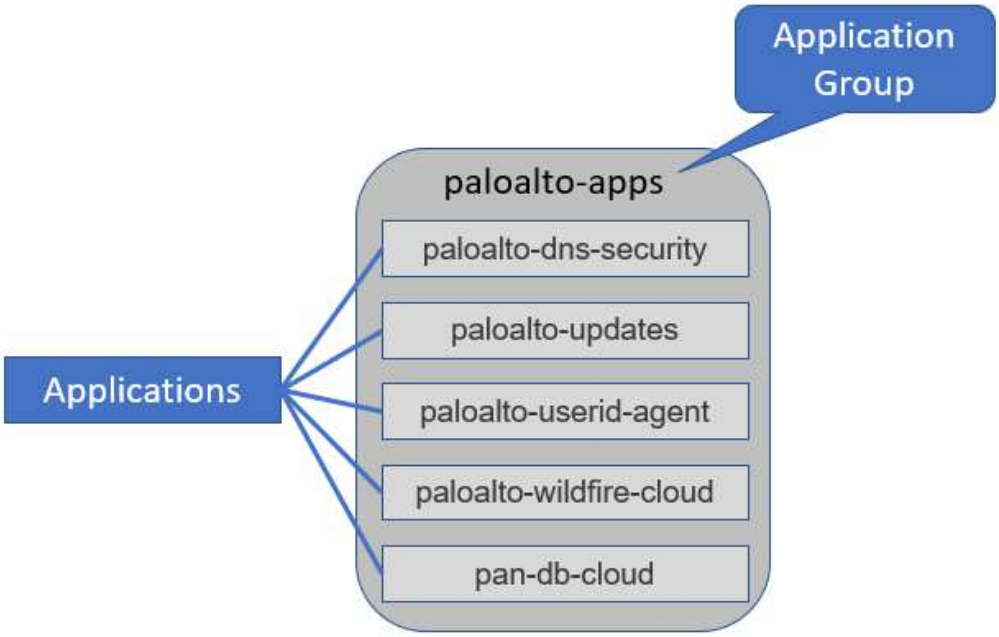


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

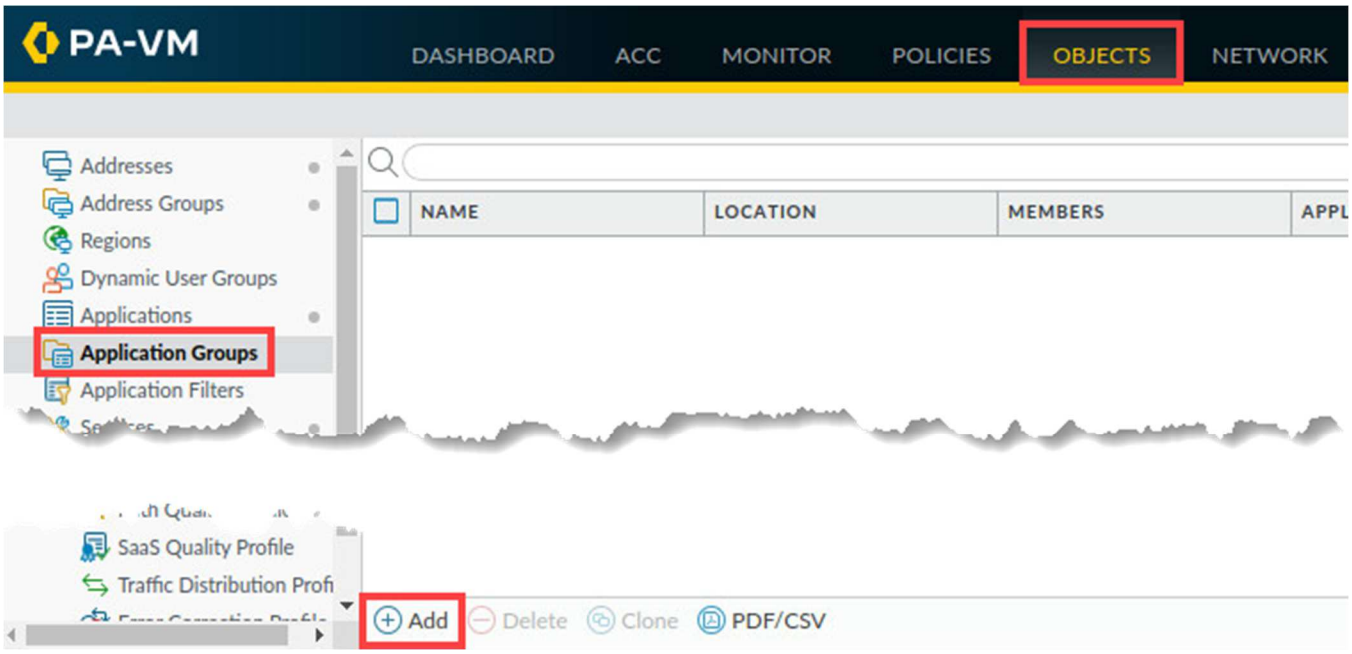
15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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.

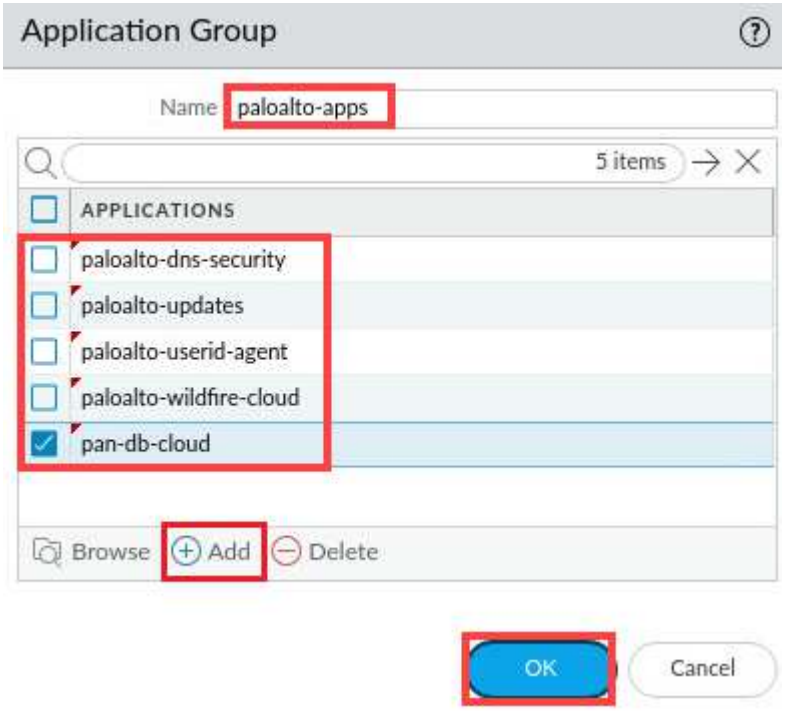


1. Navigate to **Objects > Application Groups**. Click **Add**.



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.

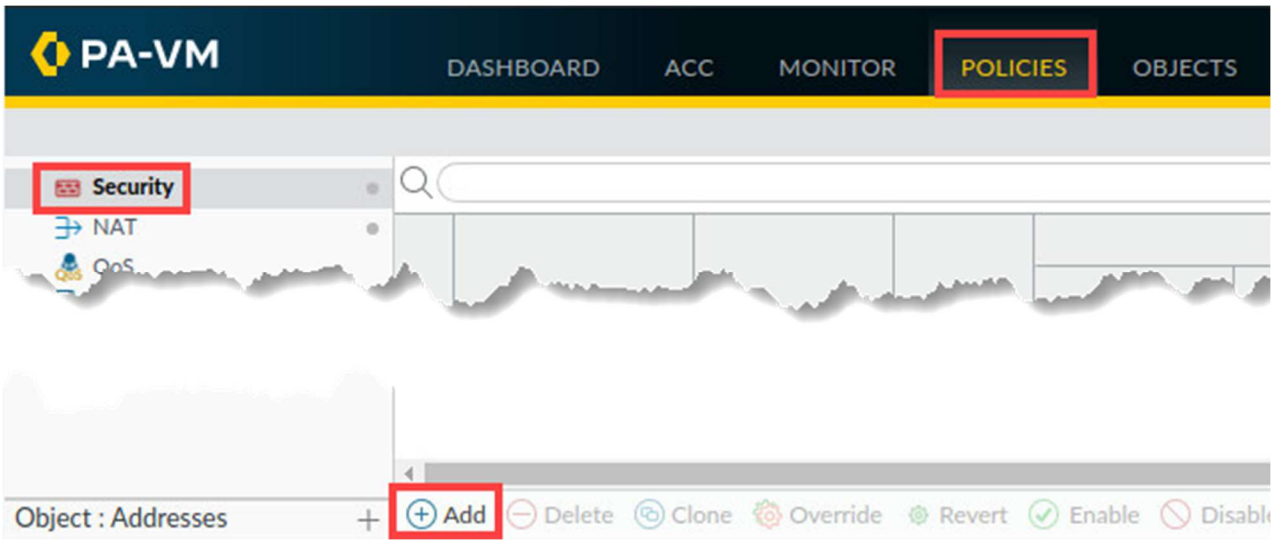
You can also use the Browse button in the Application Group window to add these entries.

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.

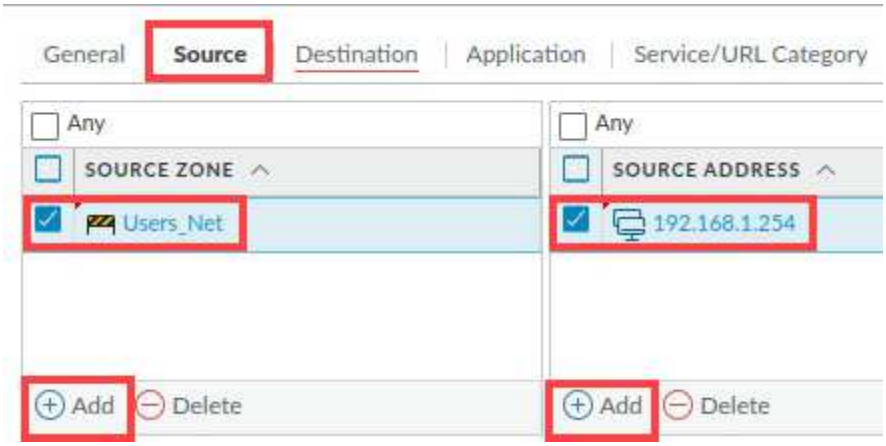
1. In the web interface, navigate to **Policies > Security.** Click **Add** to configure a new security policy.



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

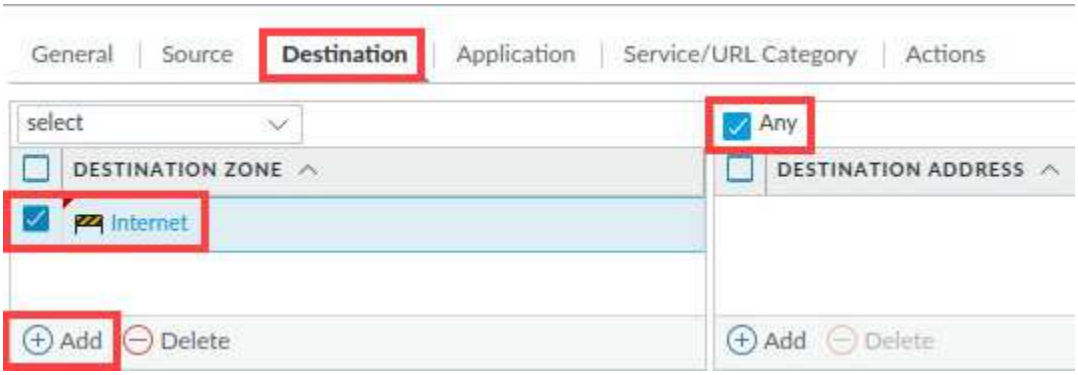
3. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	**Users_Net**
Source Address	**192.168.1.254**



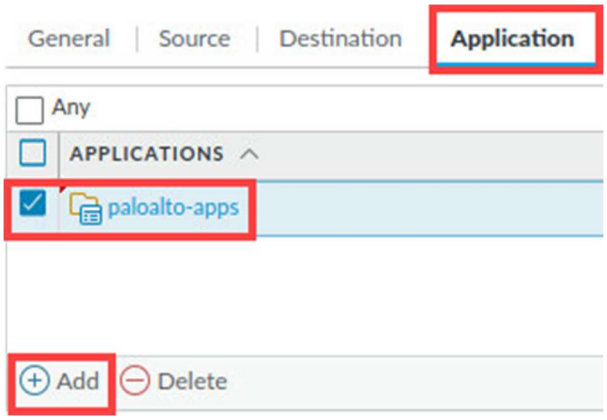
4. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	**Internet**
Destination Address	**Any**



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

Parameter	Value
Applications	**paloalto-apps**



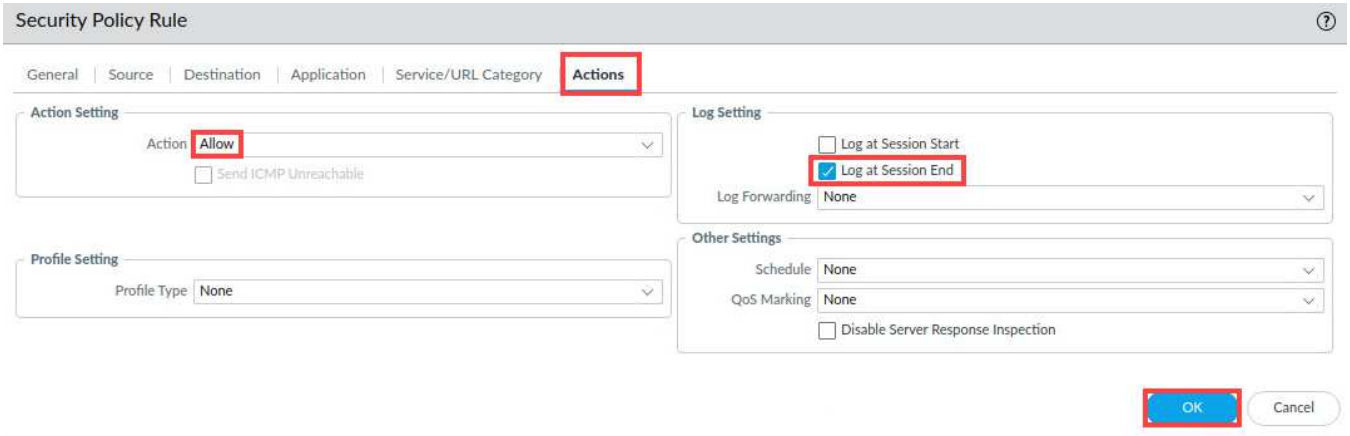
Please Note

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.

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

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

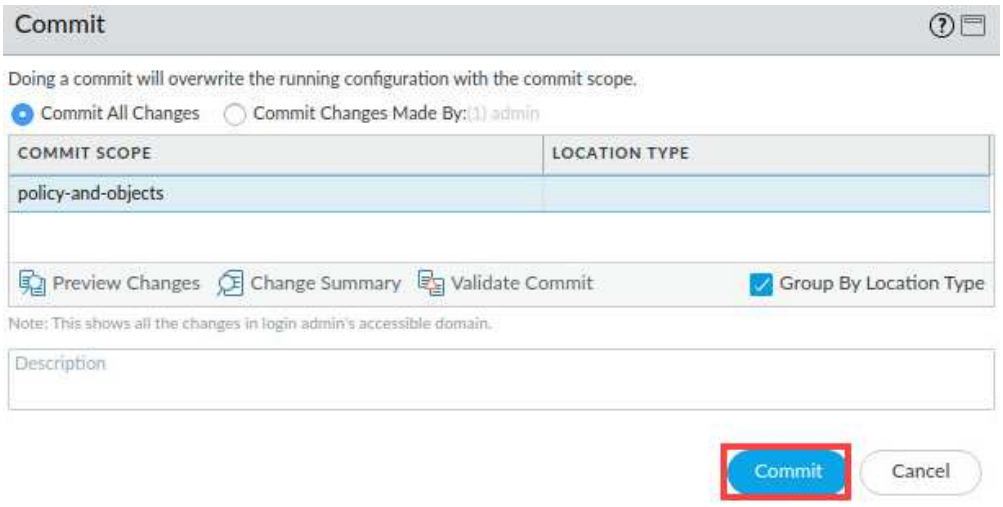


8. The "**Allow PANW-Apps**" rule should be listed just above the "intrazone-default" rule in the Security policy rule list.

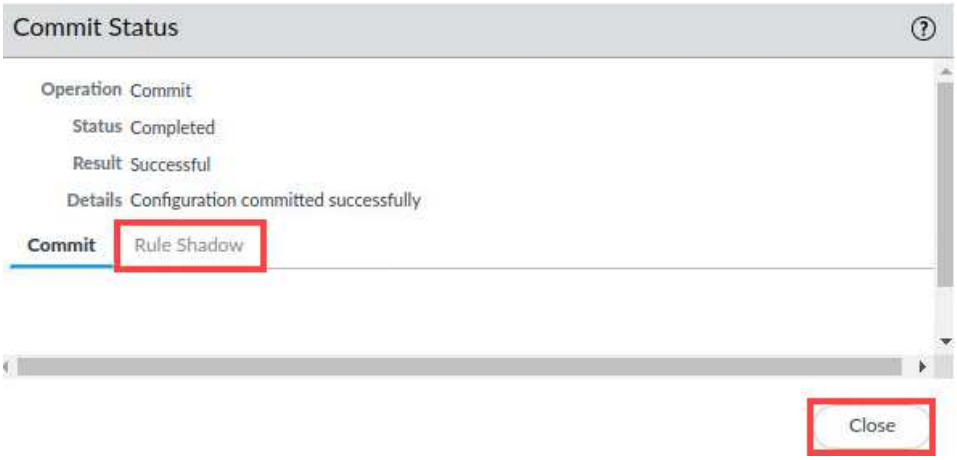
	NAME	TAGS	TYPE	Sour ZONE	ADDRESS
1	Block-from-Known-...	none	universal	Internet	Palo Alto Netw... Palo Alto Netw... Palo Alto Netw...
2	Block-to-Known-Ba...	none	universal	Extranet Users_Net	any
3	Users_to_Extranet	none	universal	Users_Net	any
4	Users_to_Internet	none	universal	Users_Net	any
5	Extranet_to_Internet	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**.



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



Please Note

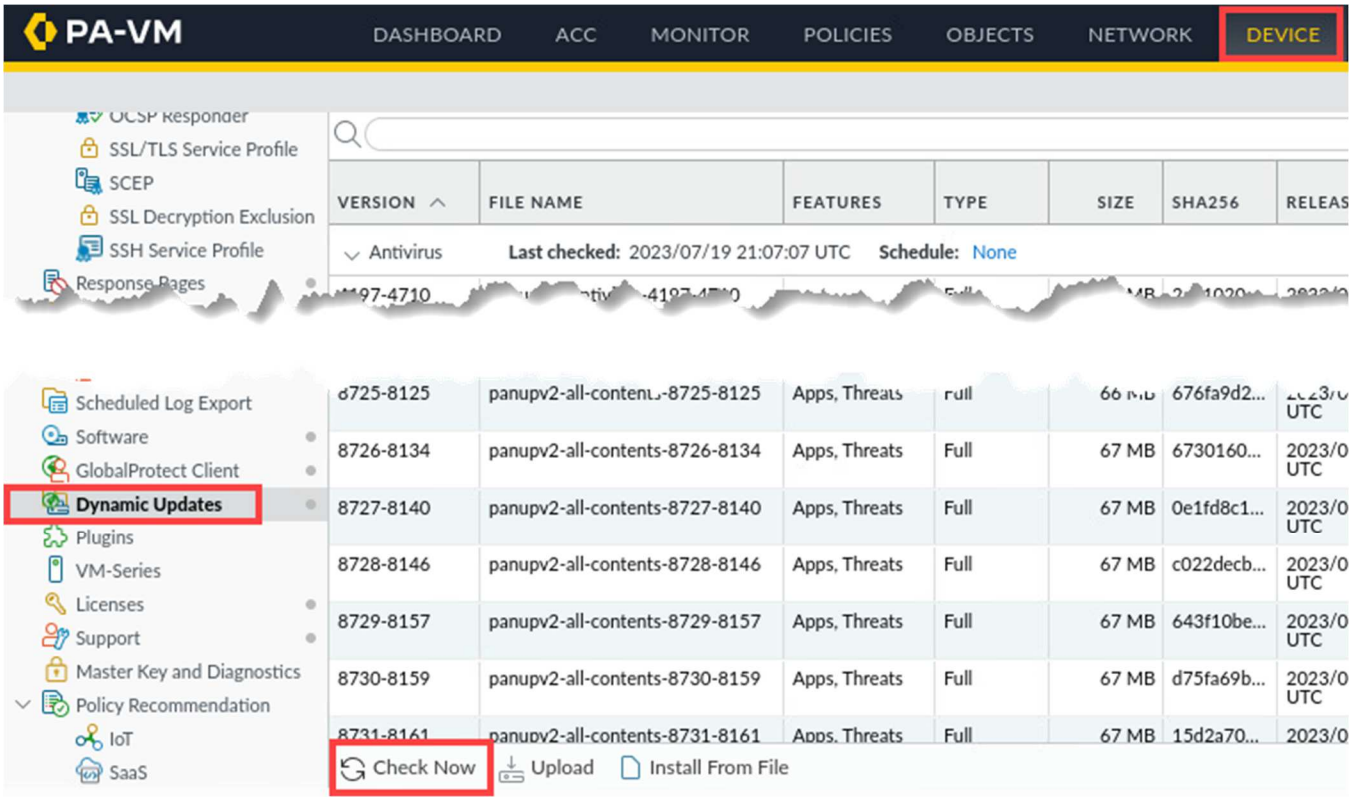
This tab only appears when you have a rule that shadows other rules. You will fix the rule shadow issue in a later section of the lab.

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.

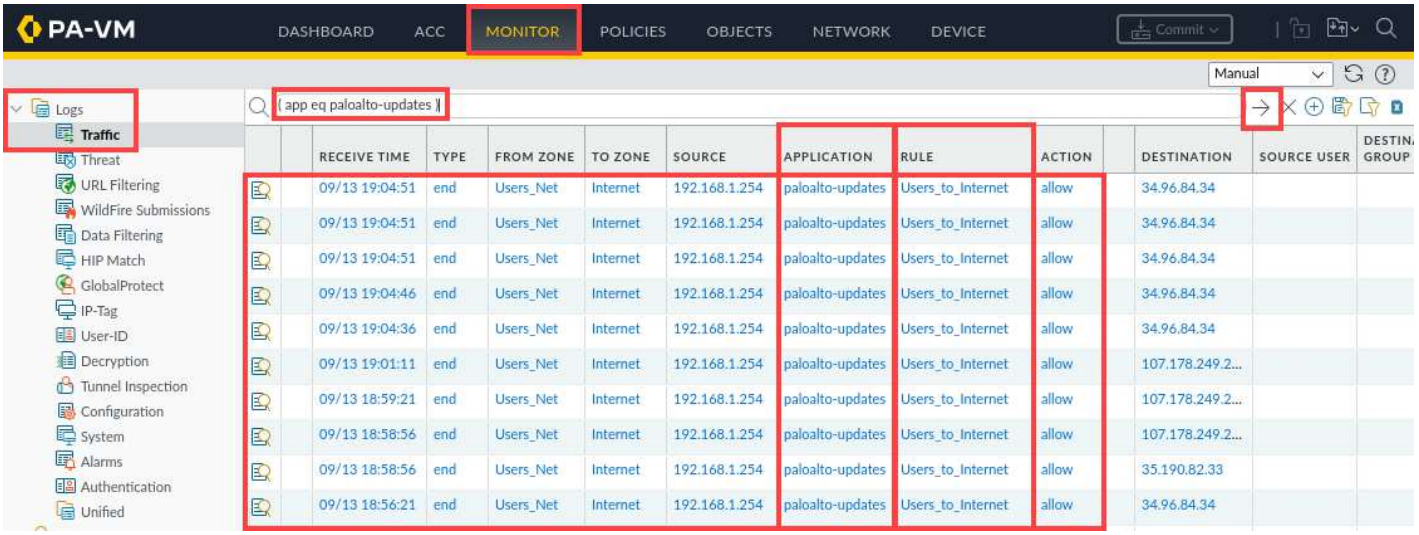
1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.



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.



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.

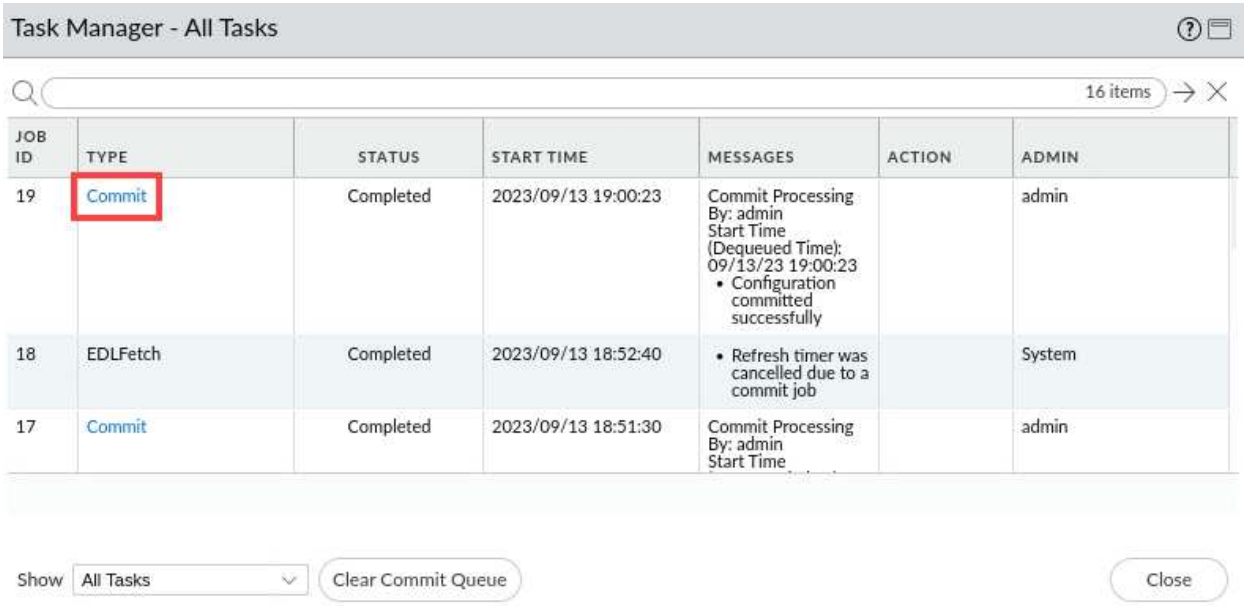
2.5 Identify Shadowed Rules

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.

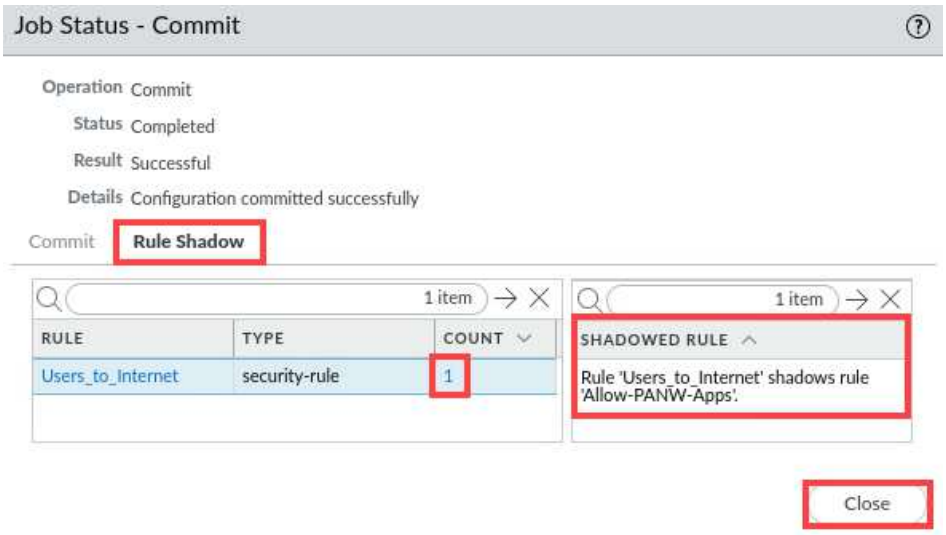
However, you might not always notice the **Rule Shadow** tab, so in this section, you will use the **Task** list to examine your earlier Commit messages.

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**.



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**.

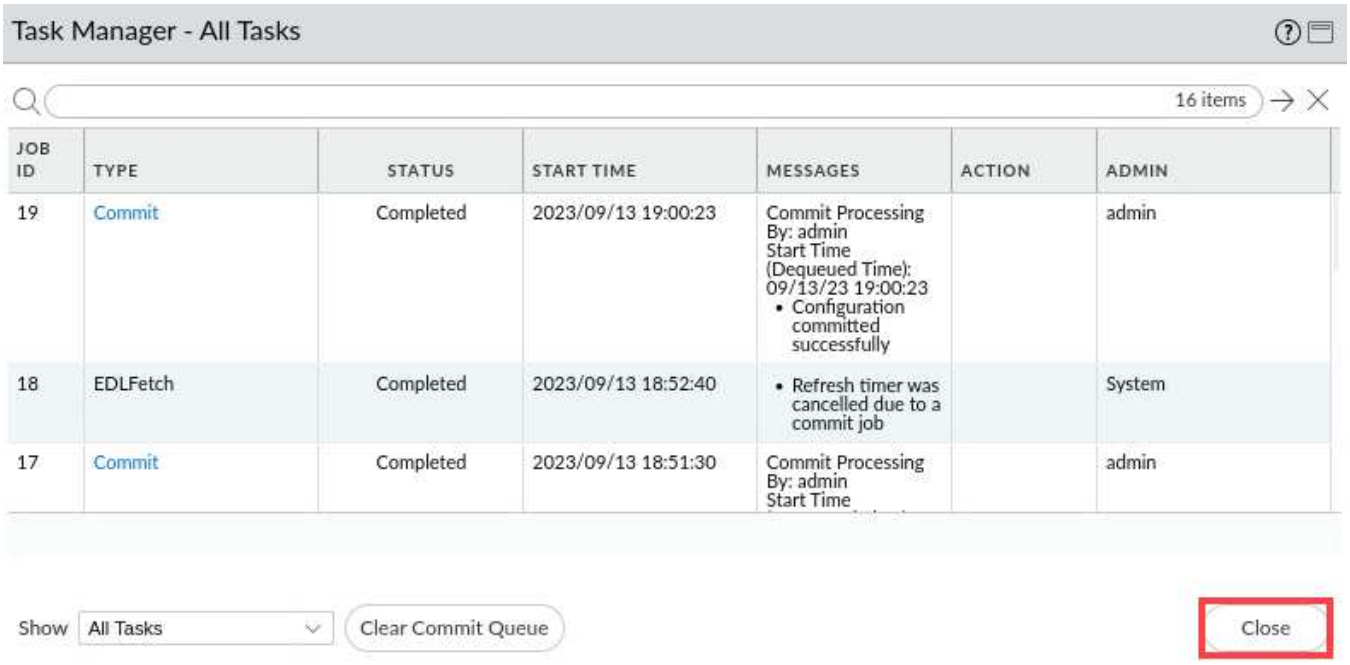


Please Note

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**.

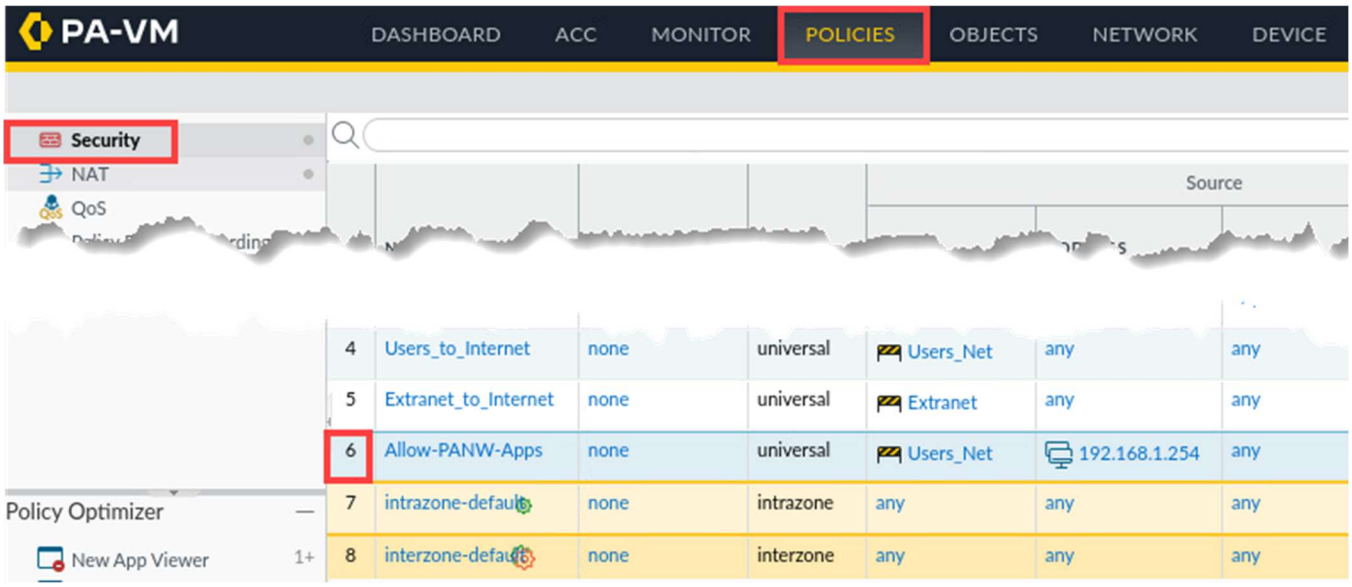


5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

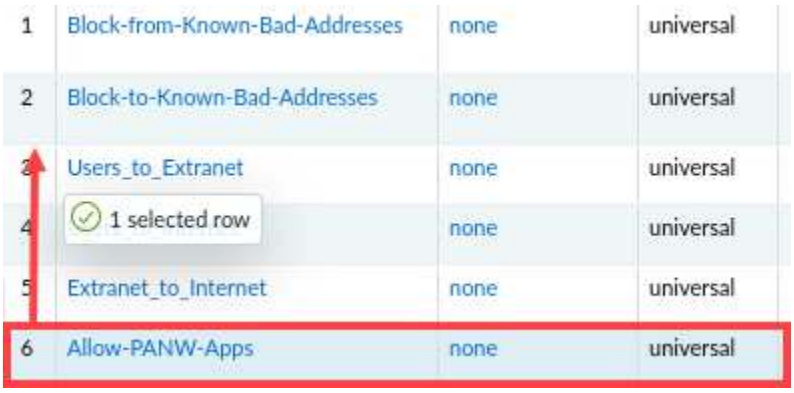
2.6 Modify the Security Policy to Function Properly

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

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



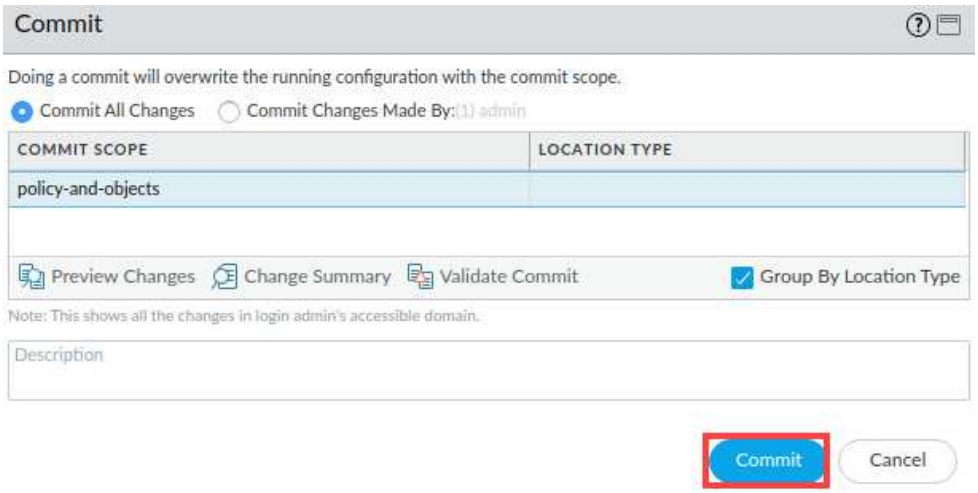
2. Drag and drop the **Allow-PANW-Apps** entry to the correct location, or you can use the **Move** button at the bottom to place the rule in the right spot.



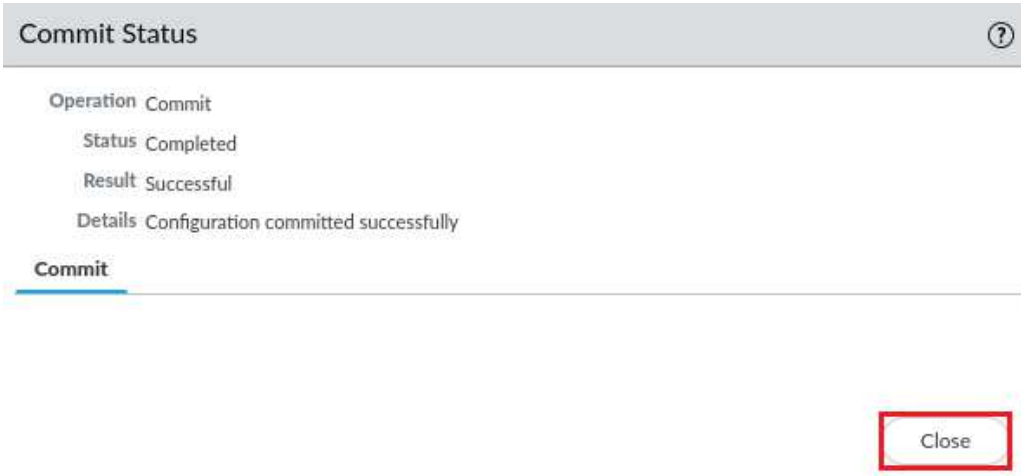
3. Confirm the *Allow-PANW-Apps* security policy is now labeled as the **3rd** security policy.

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

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



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

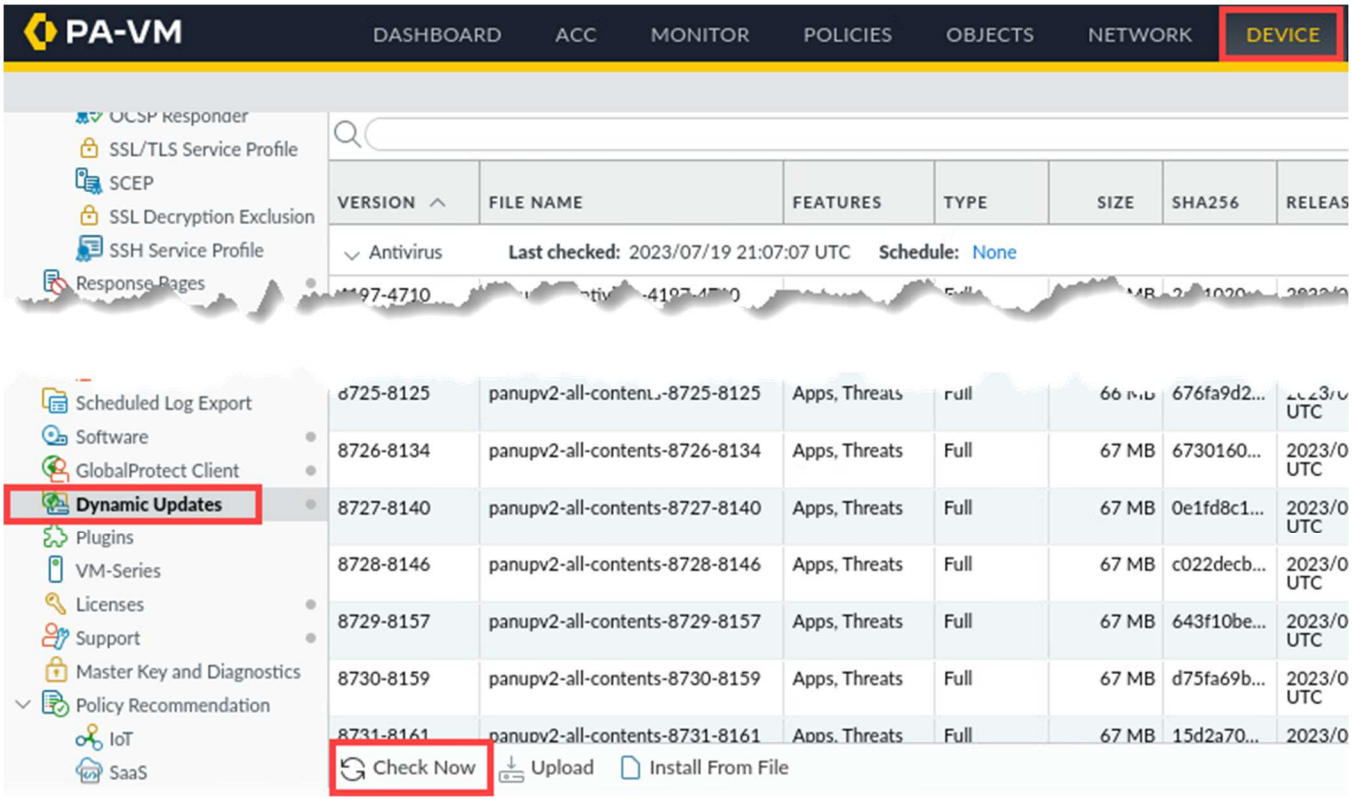


7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

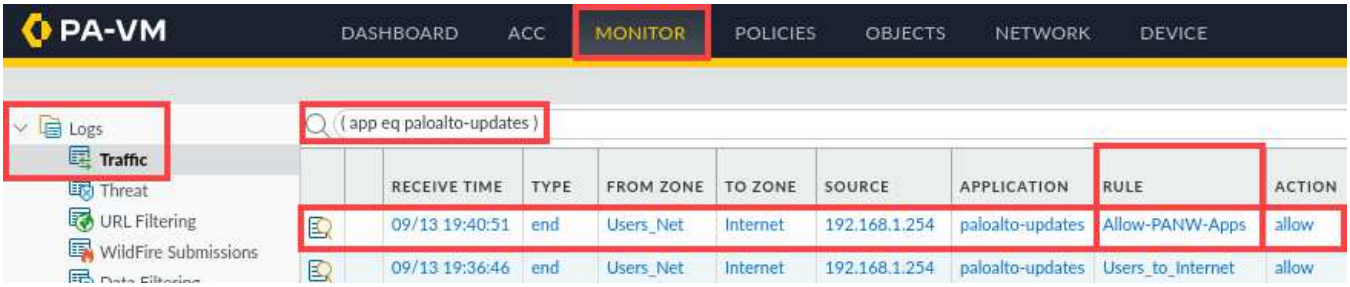
2.7 Test the Modified Security Policy Rule

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.

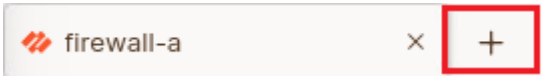
1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.



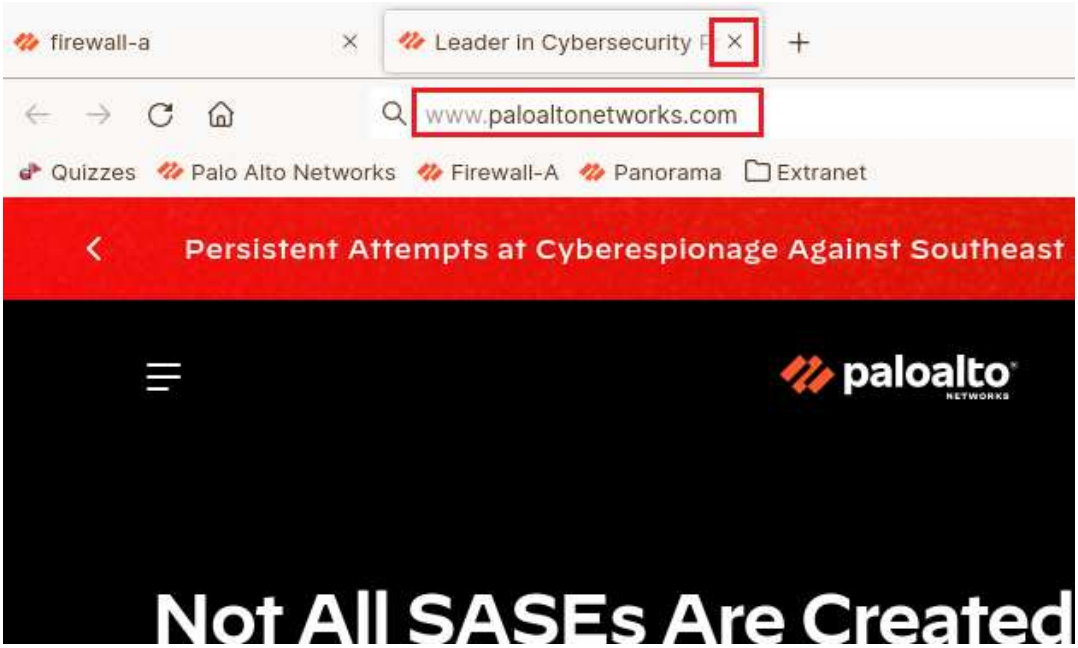
2. Select **Monitor > Logs > Traffic**. Ensure the following filter **(app eq paloalto-updates)** in the filter builder is applied. Refresh the logs by clicking on the **Apply Filter** button. Look for the log entries for the application *paloalto-updates*. It should be the "**Allow-PANW-Apps**" rule.



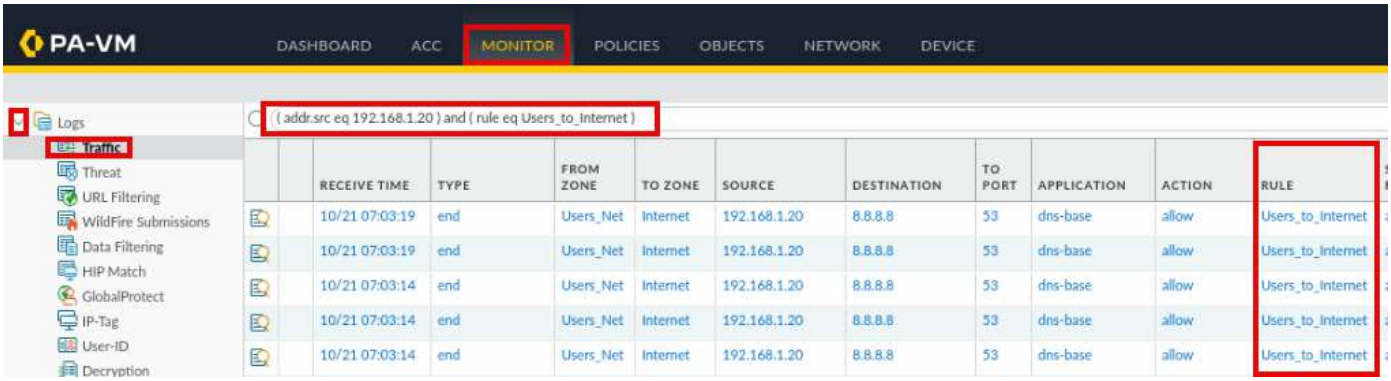
3. Open a new tab in **Firefox**.



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.



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

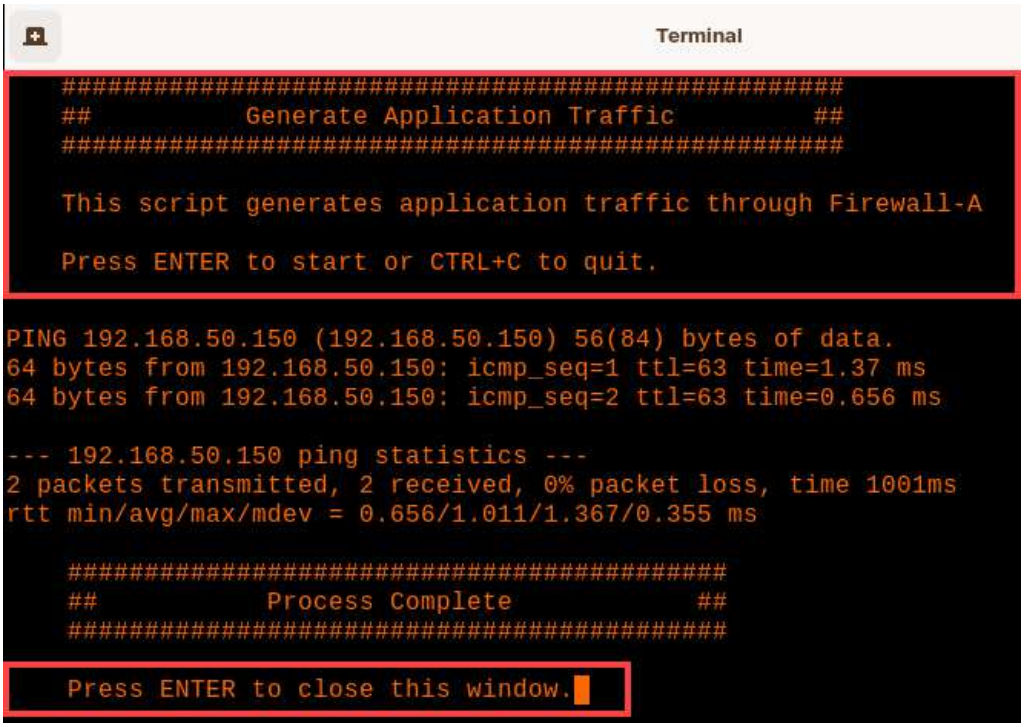
6. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

2.8 Generate Application Traffic

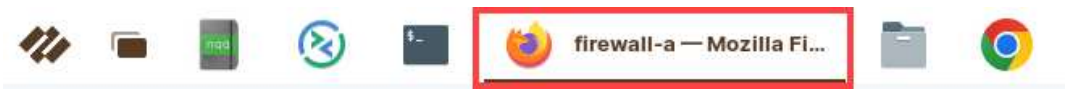
In this section, you will run a short script which generates application traffic from your client workstation to hosts against the Internet and Extranet security zones.

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

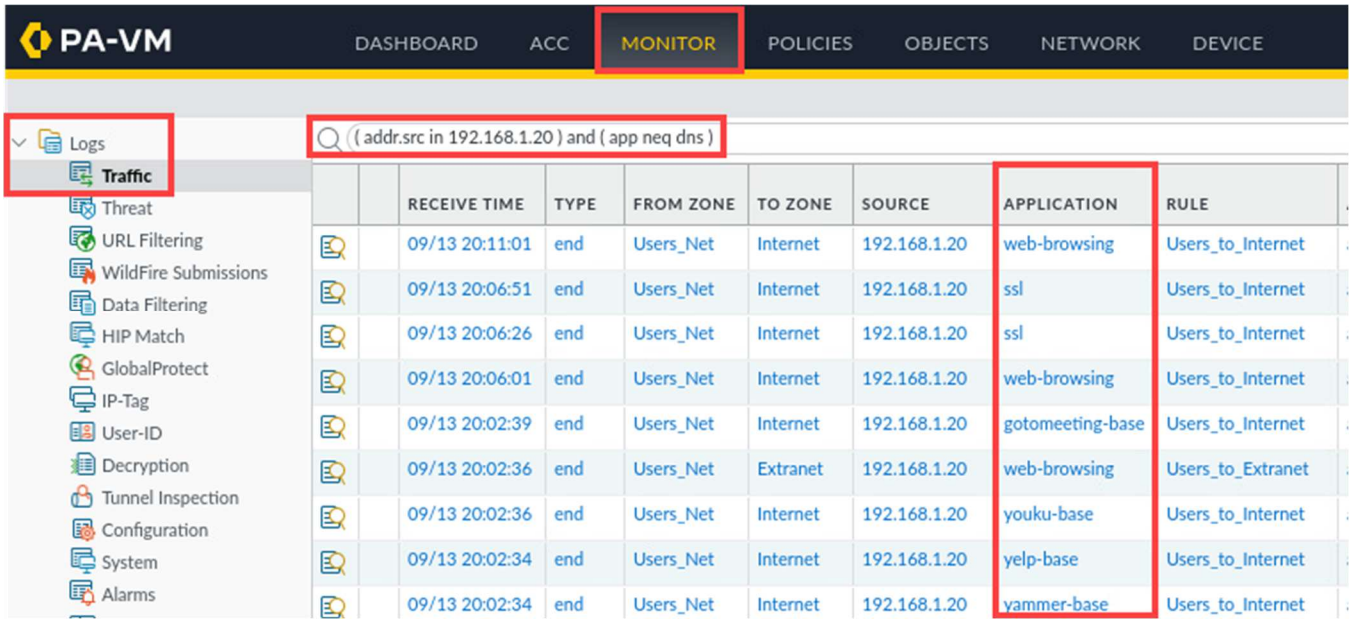
2. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes press **Enter**. Allow the script *30* seconds to *1* minute to complete before proceeding to the next step.



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.



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?

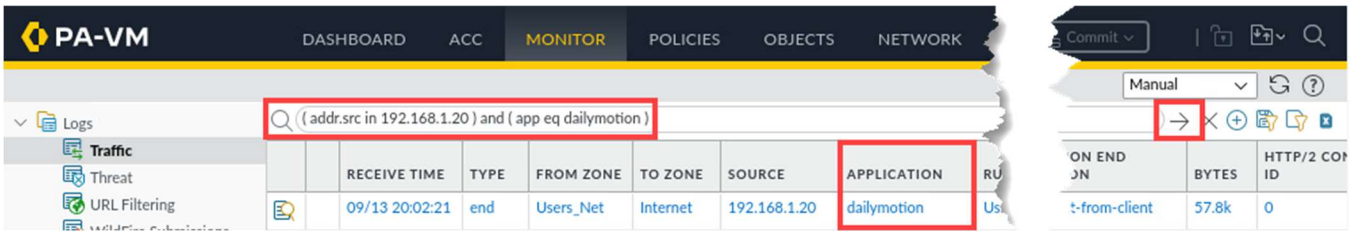
a. Continue denying all applications to maintain a strict security posture.
b. Reevaluate and potentially allow specific denied applications based on security needs.
c. Automatically allow all applications to enhance network flexibility.
d. Block all applications permanently to minimize security risks.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

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

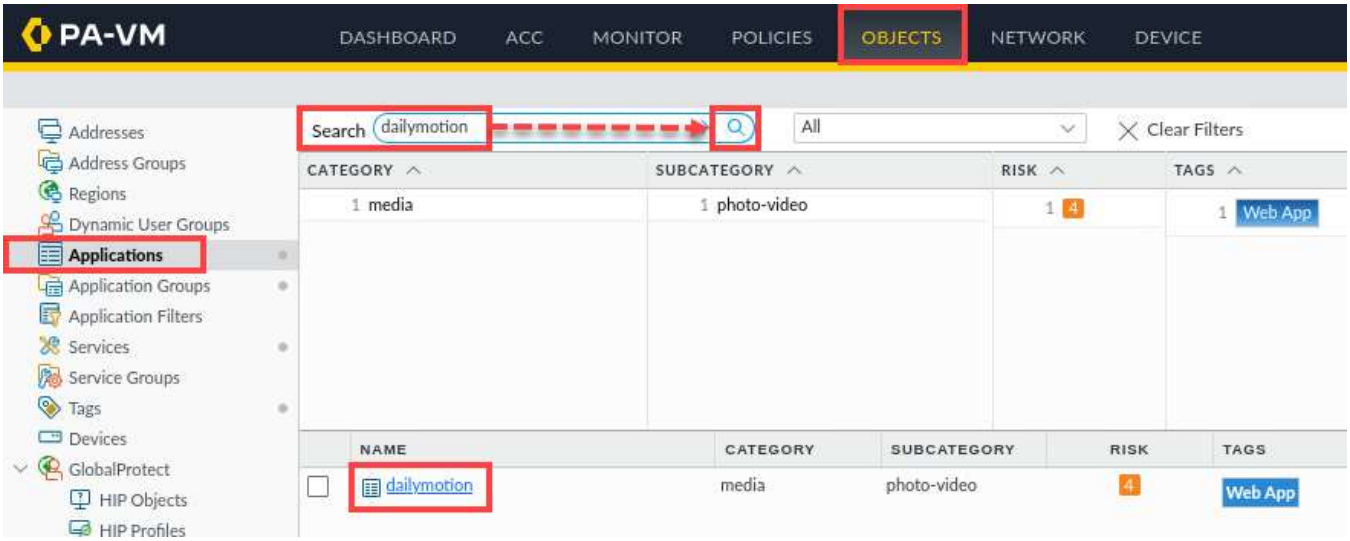
2.9 Research Applications

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.

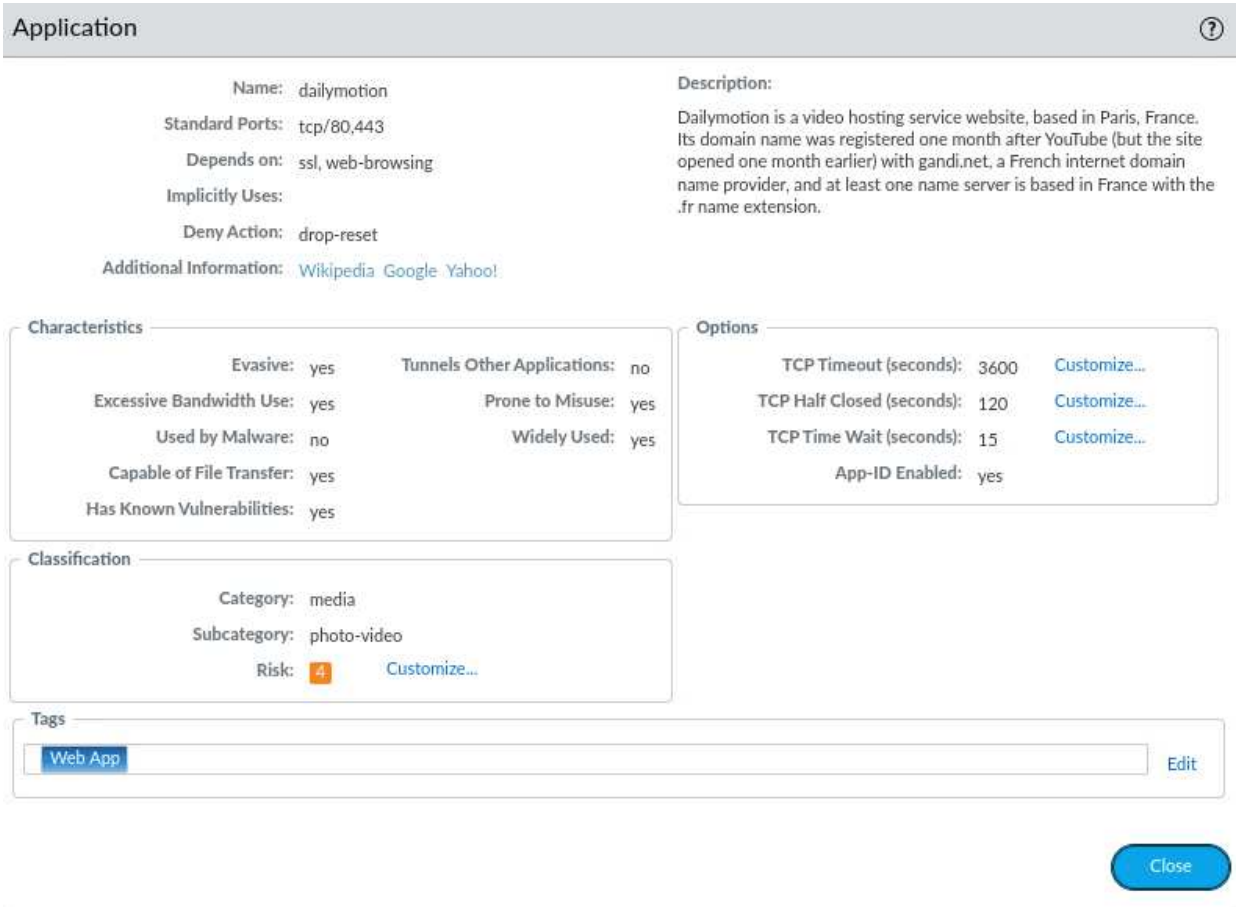
1. In the **Traffic** log, enter the filter **(addr.src in 192.168.1.20) and (app eq dailymotion)** to search for the **dailymotion** application. Click the **Apply** icon.



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.



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



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?

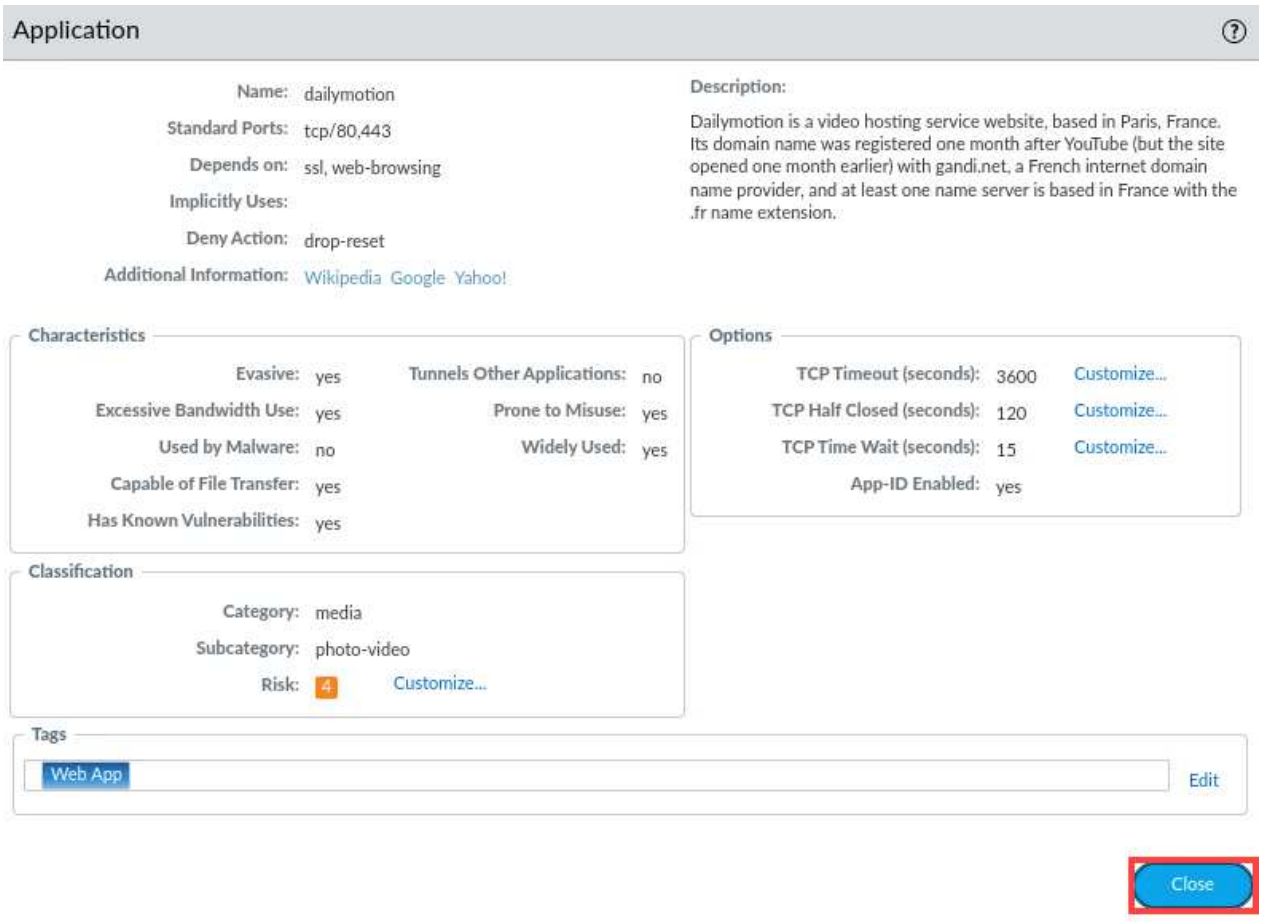
a. Evasive
b. Widely Used
c. Prone to Misuse
d. Capable of File Transfer

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.



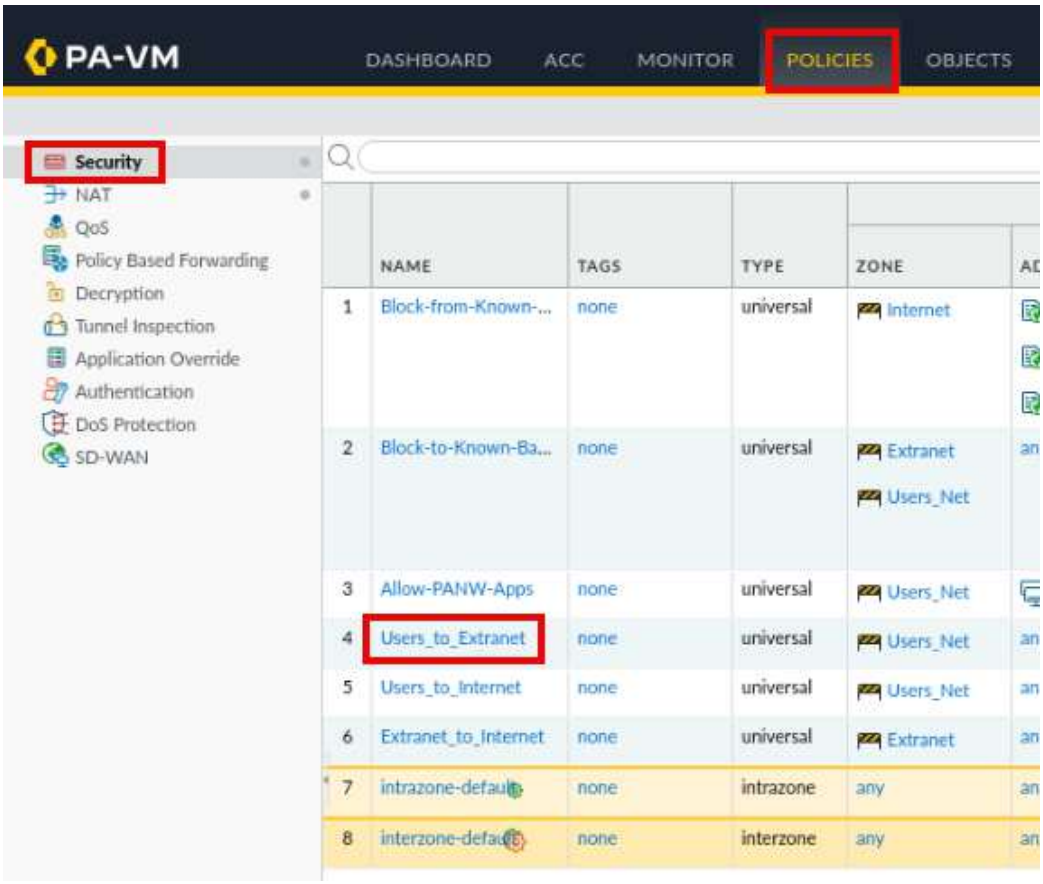
5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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**.

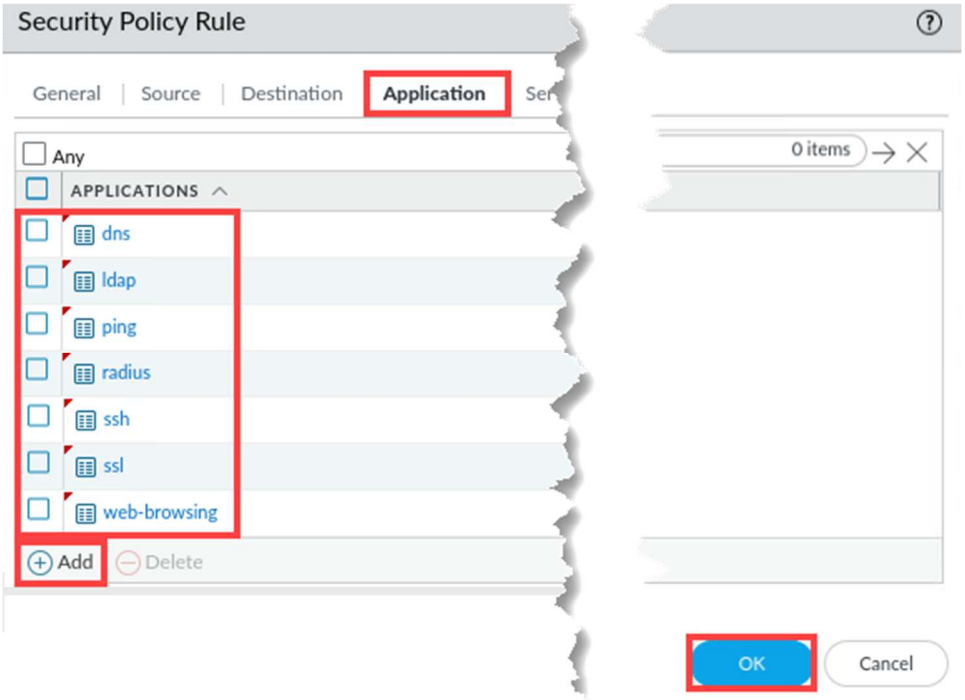
After your research, you can now update both rules to allow only applications that are necessary for your organization.

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



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

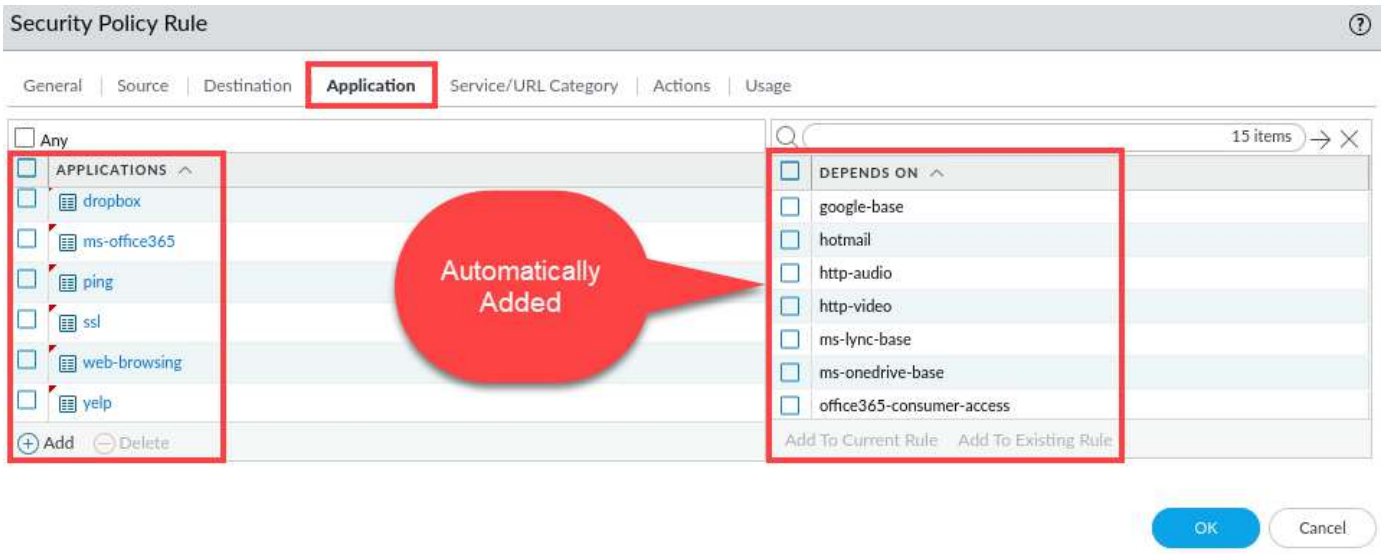
Parameter	Value
Applications	**ssl** **ssh** **ping** **dns** **ldap** **radius** **web-browsing**



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

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

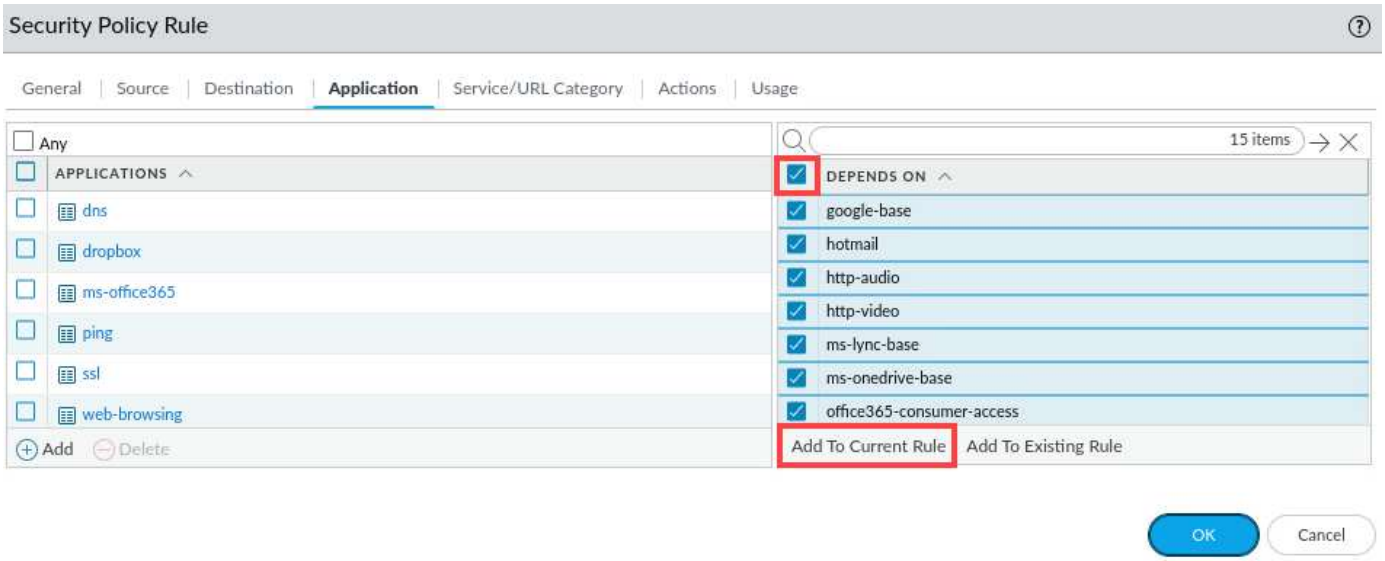
Parameter	Value
Applications	**ping** **dns** **ssl** **yelp** **web-browsing** **dropbox** **ms-office365**



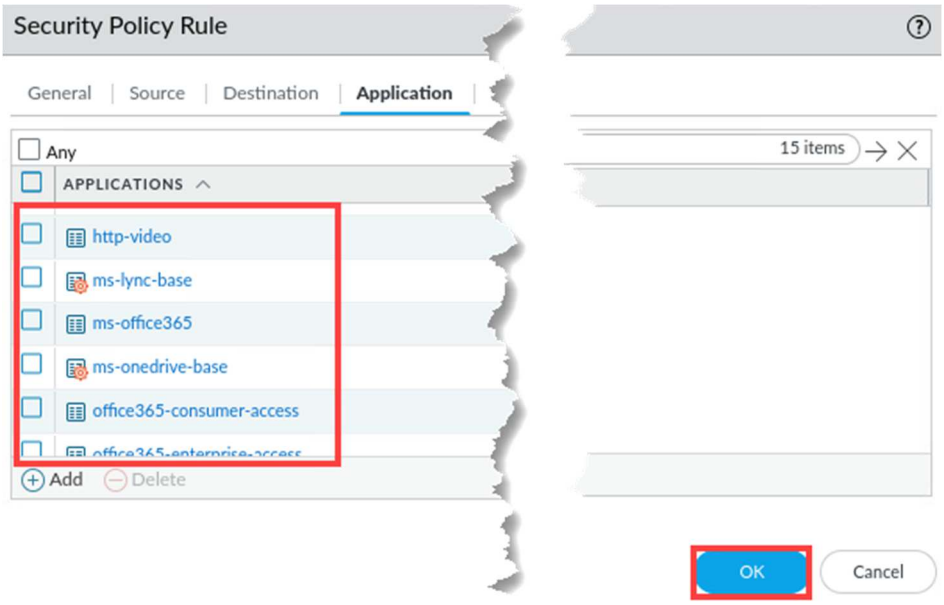
Please Note

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.**

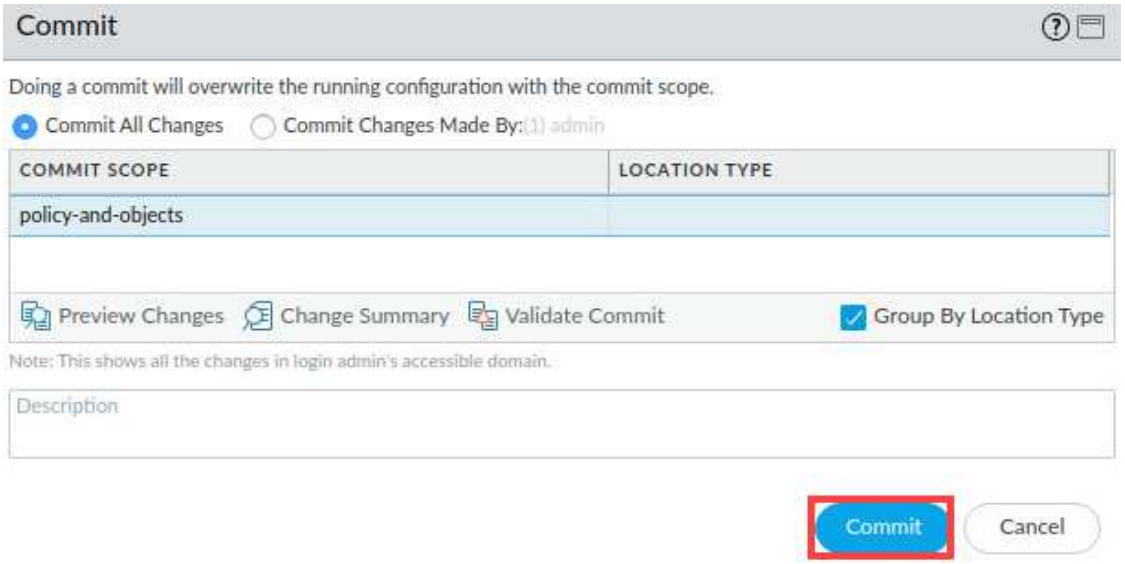


6. Scan through the list of *Applications* on the left side of the window and note that the dependent applications have been added. Click **OK**.

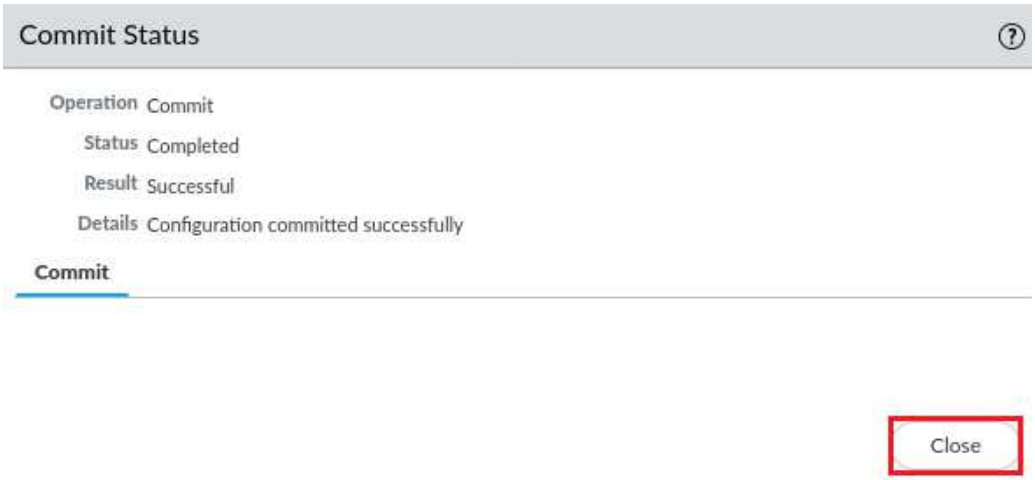


7. Click the **Commit** button at the upper right of the web interface.

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



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



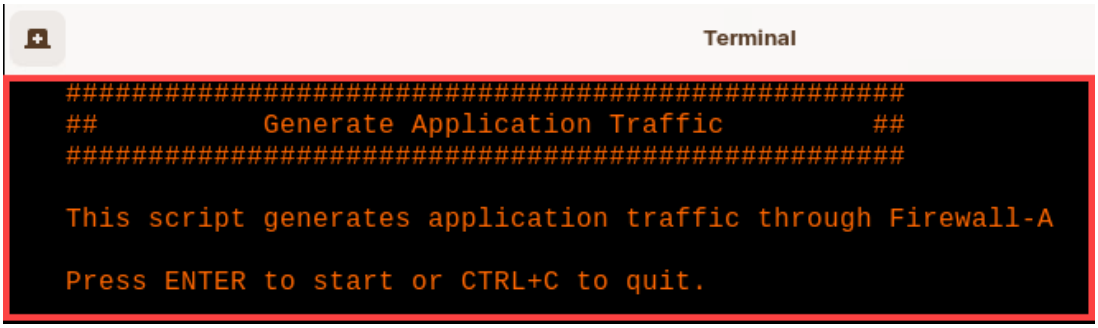
10. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

2.11 Test the Updated Security Policy Rules

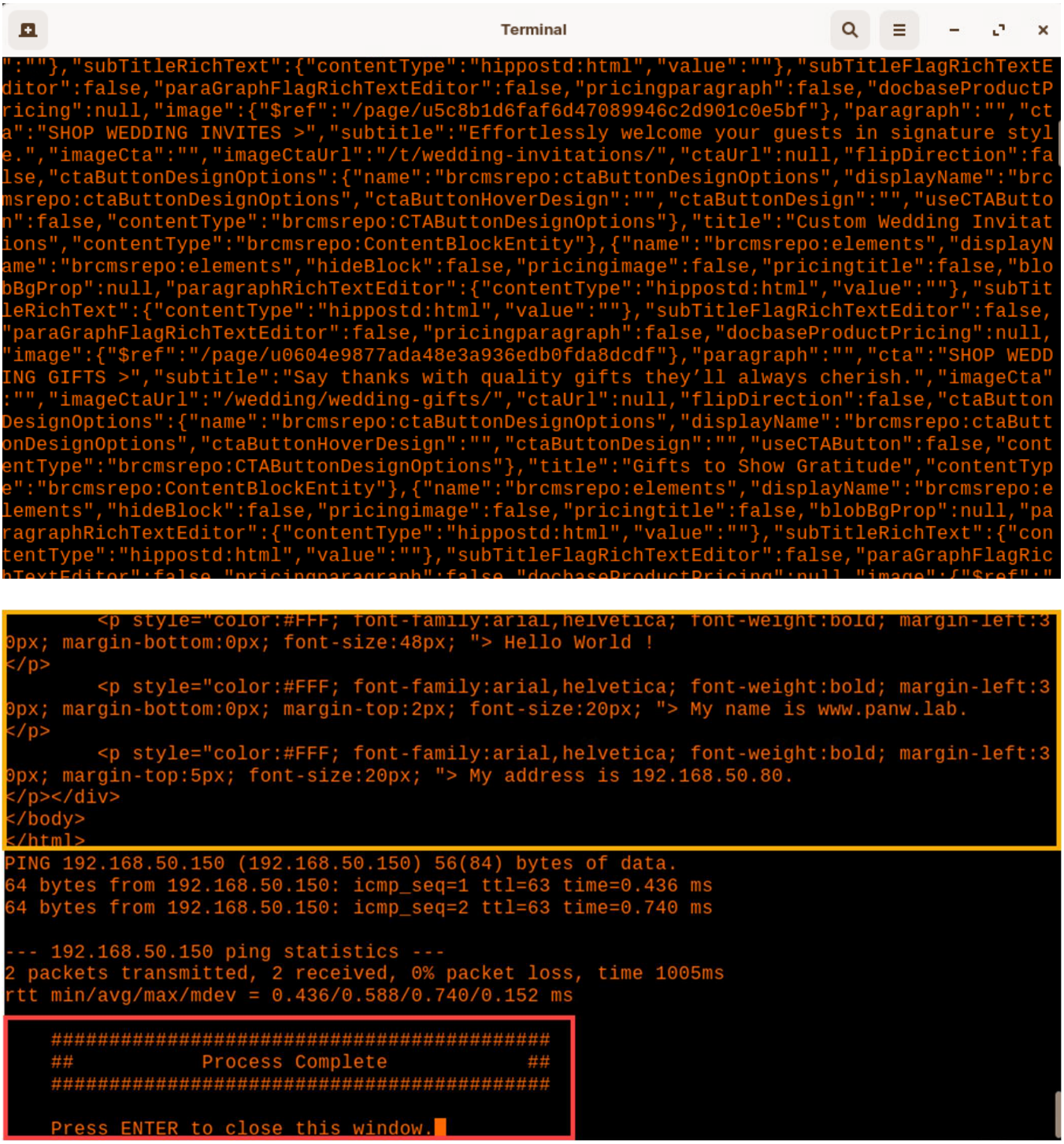
In this section, you will run a short script and examine the results.

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

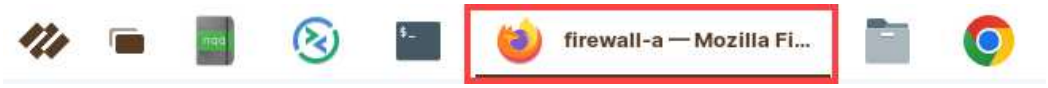
2. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes press **Enter**. Allow the script *30* seconds to *1* minute to complete before proceeding to the next step.



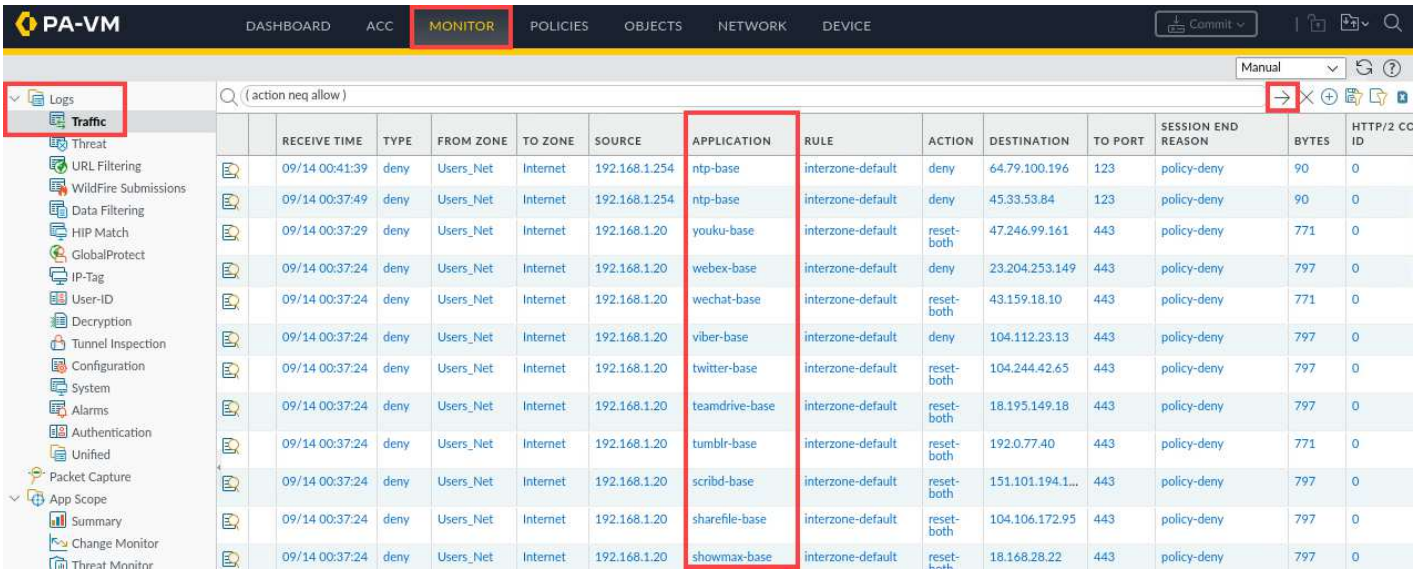
Ignore any errors that the script generates – these occur because the firewall is blocking various application traffic types. The script may also pause at different points while applications time out because they are being blocked by the firewall.



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.



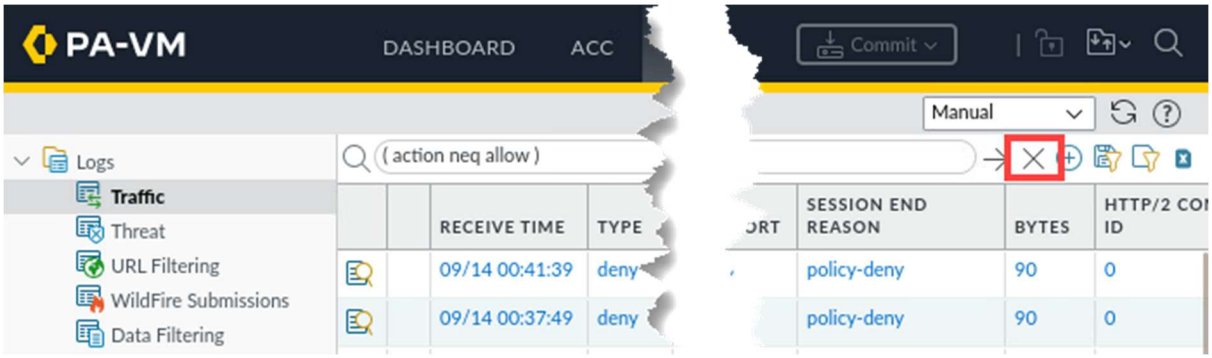
Please Note

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.



2.12 Enable the Application Block Page

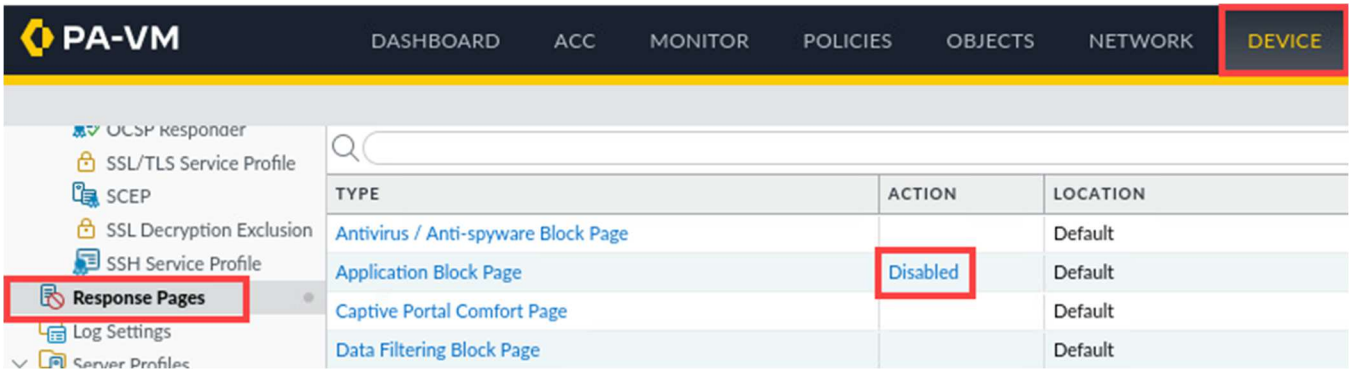
When the firewall denies traffic to a web-based application, many users may assume that the Internet is down or slow or that there is something wrong with their browser settings.

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.

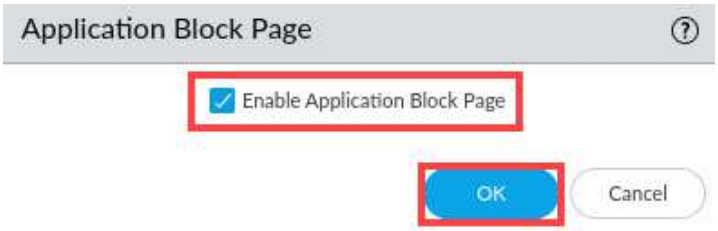
By default, the Application Block Page is not enabled.

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**.

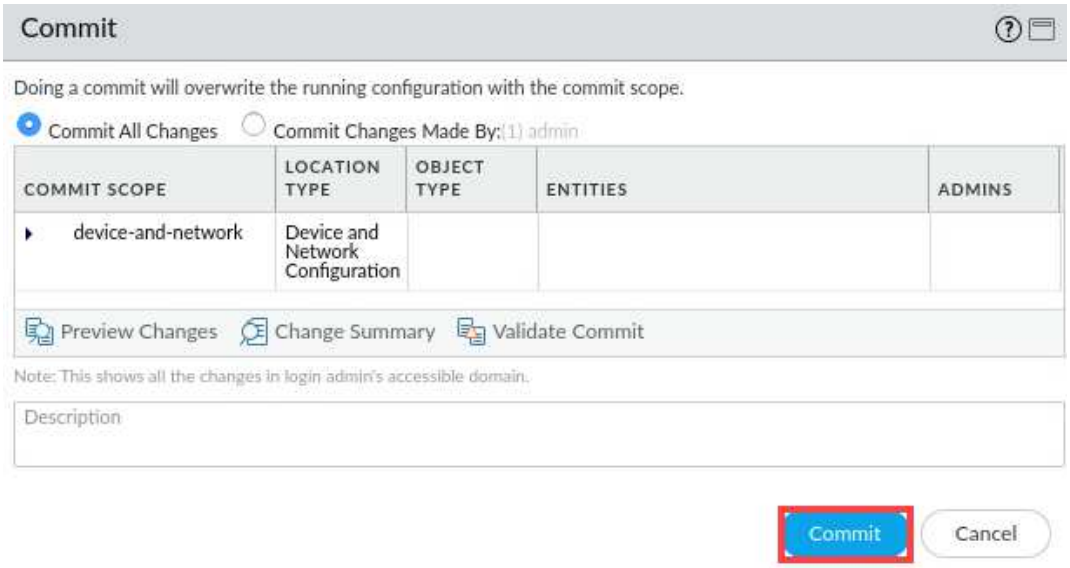


3. In the *Application Block Page* window, place a check in the box for **Enable Application Block Page**. Click **OK**.

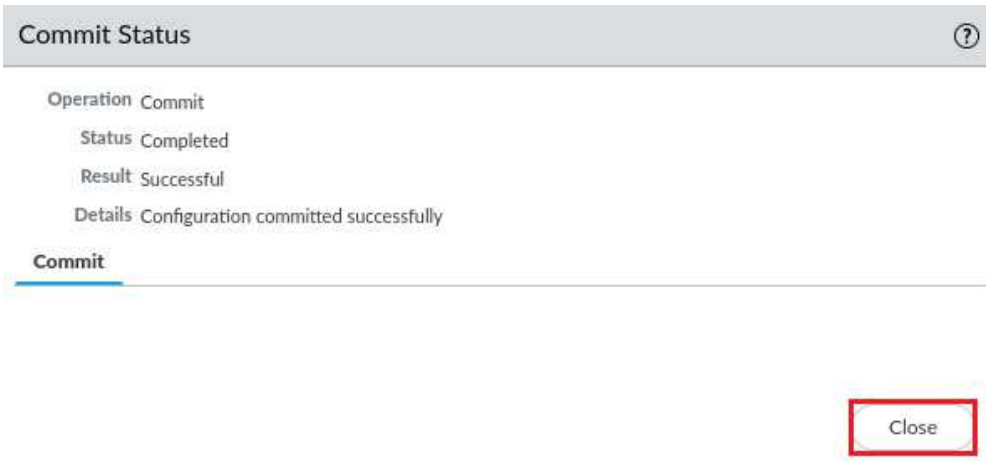


4. Click the **Commit** button at the upper right of the web interface.

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



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

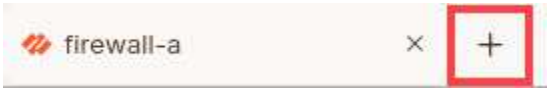


7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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.



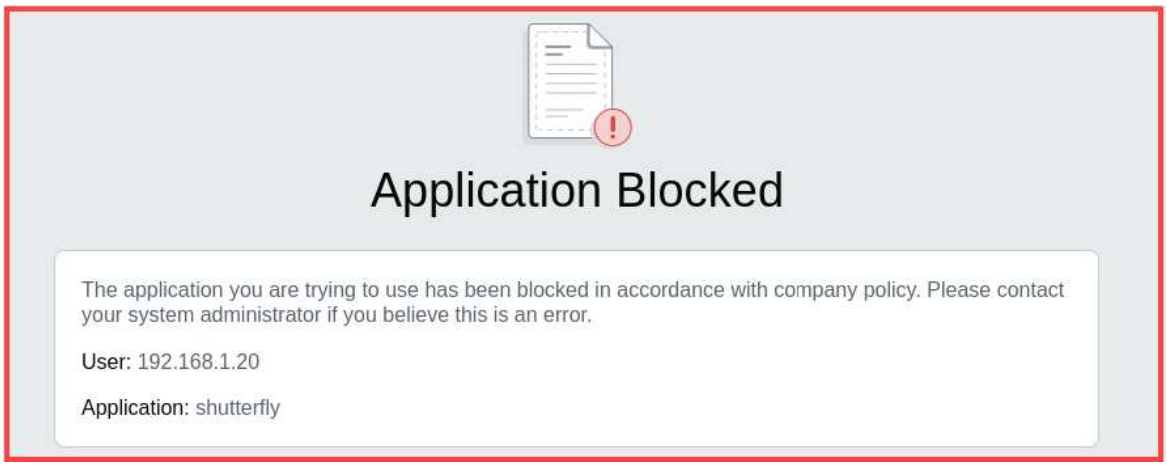
2. Attempt to connect to **http://www.shutterfly.com**.

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.