PALO ALTO NETWORKS EDU 210

Lab 8: Blocking Threats using App-ID

Document Version: 2022-07-18

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.

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

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

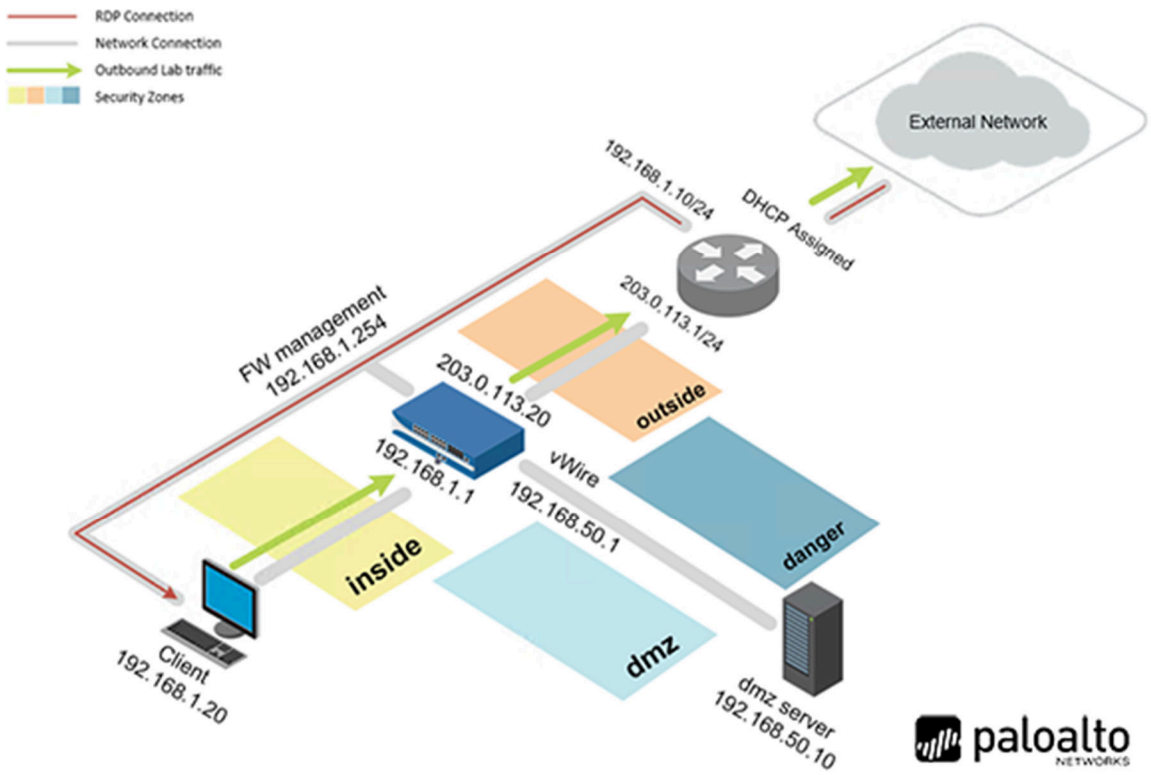
The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this Application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

Objective

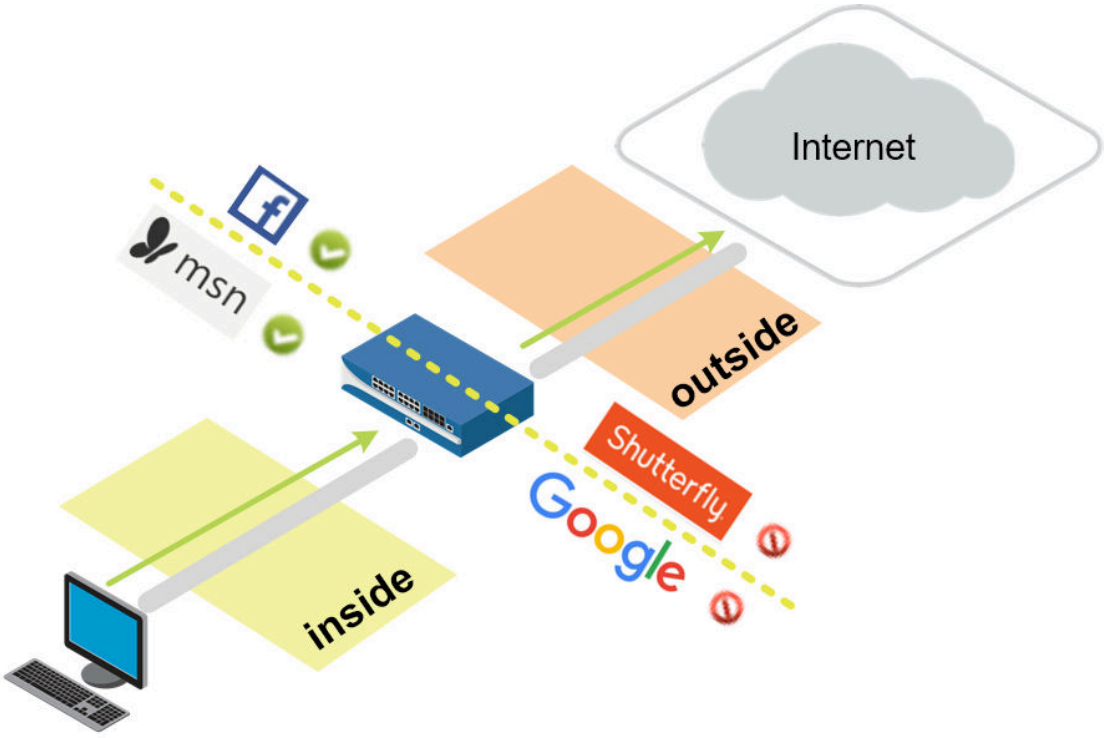
In this lab, you will perform the following tasks:

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

Lab Topology



Theoretical Lab Topology



Lab Settings

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

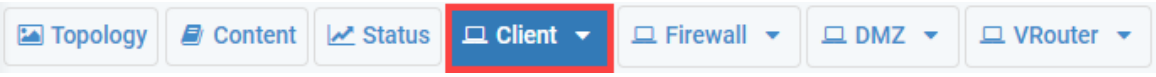
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Blocking Threats Using App-ID

1.1 Apply a Baseline Configuration to the Firewall

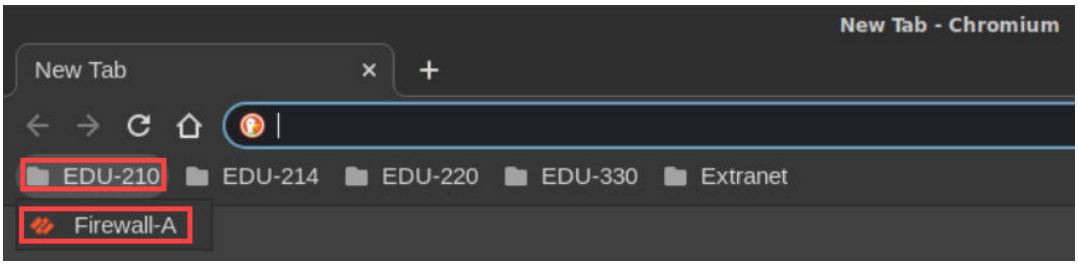
In this section, you will load the Firewall configuration file.

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

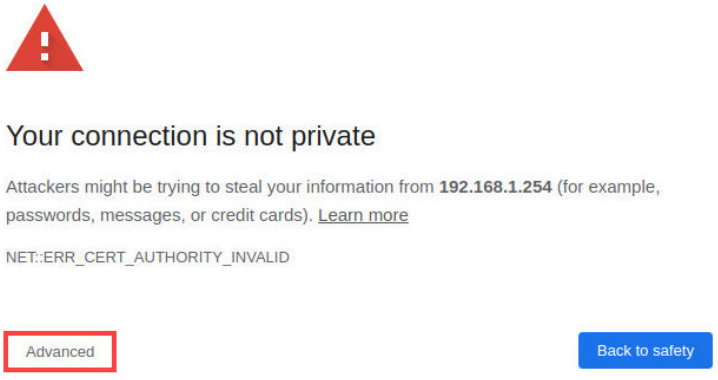


2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

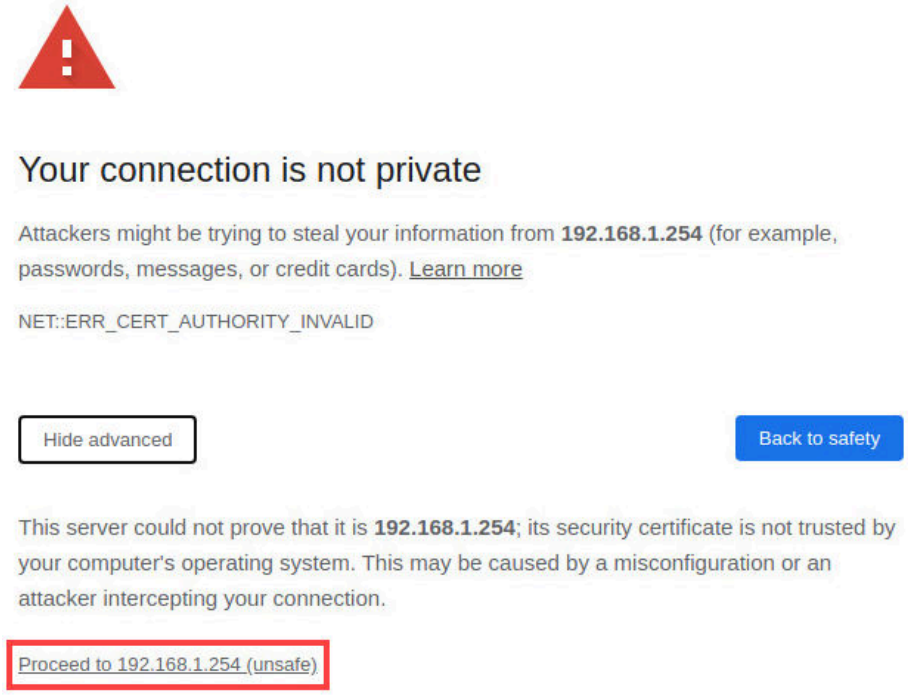


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



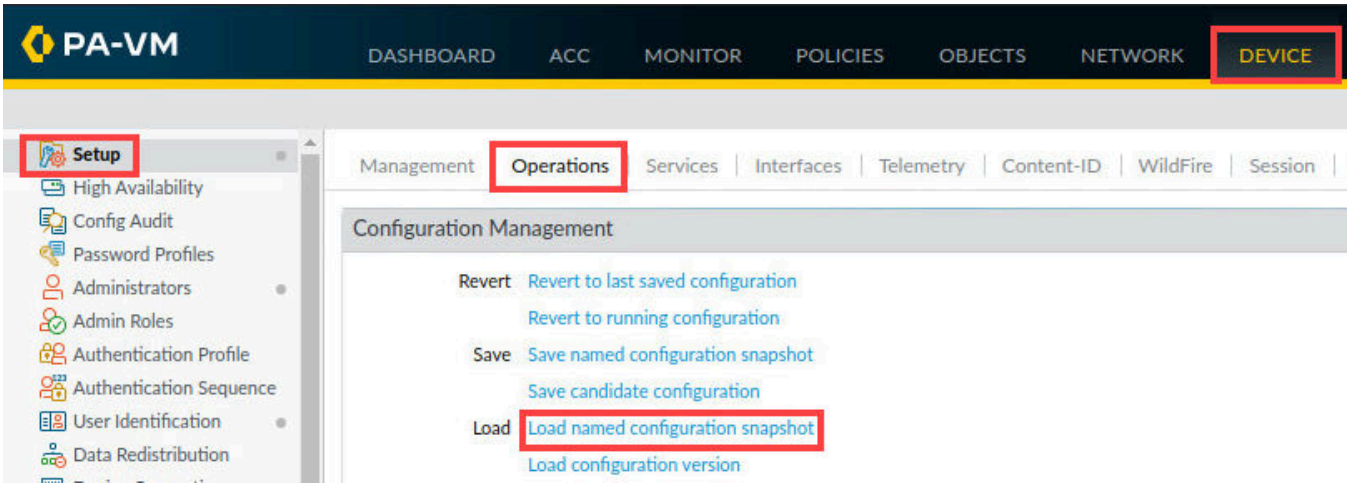
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

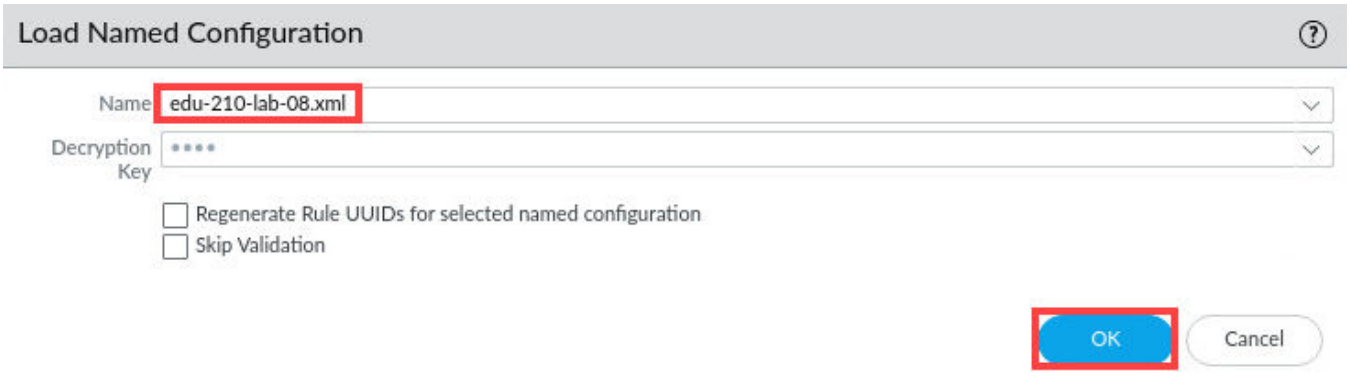


6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

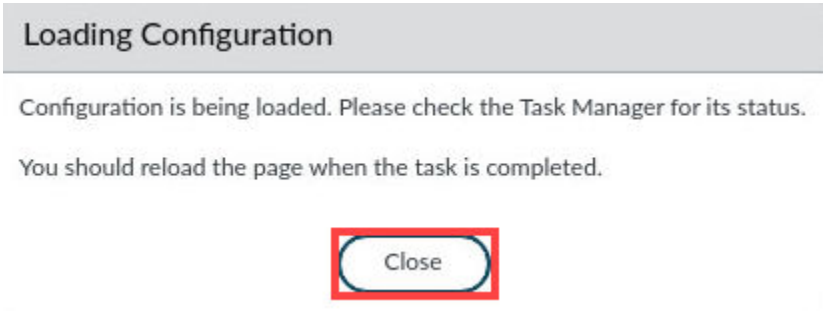
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



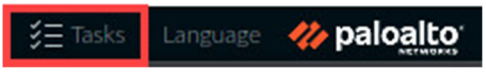
8. In the *Load Named Configuration* window, select **edu-210-lab-08.xml** from the *Name* dropdown box and click **OK**.



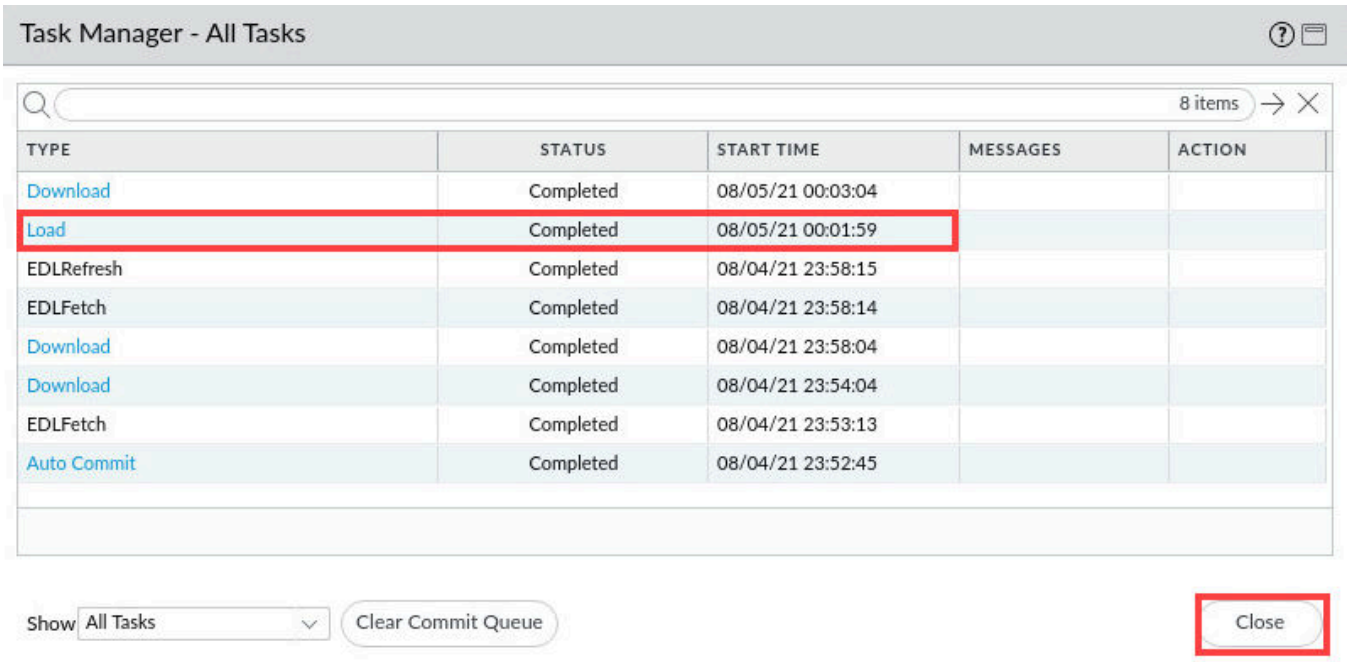
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



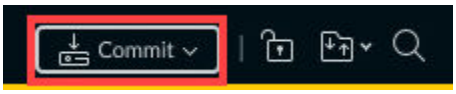
10. Click the **Tasks** icon located at the bottom-right of the web interface.



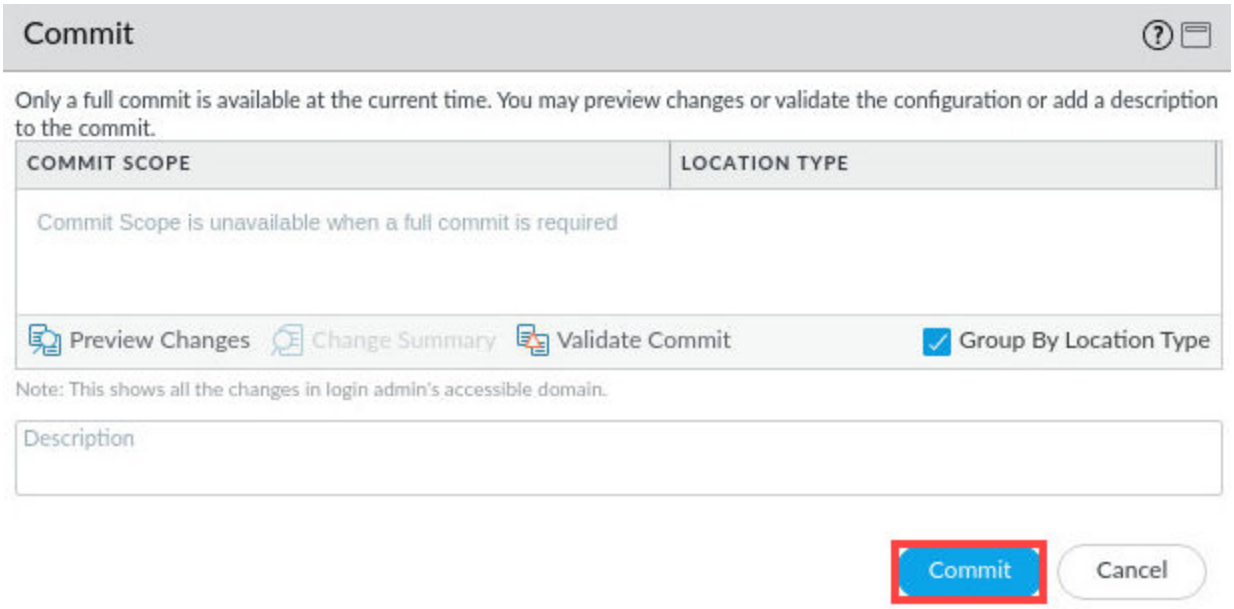
11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



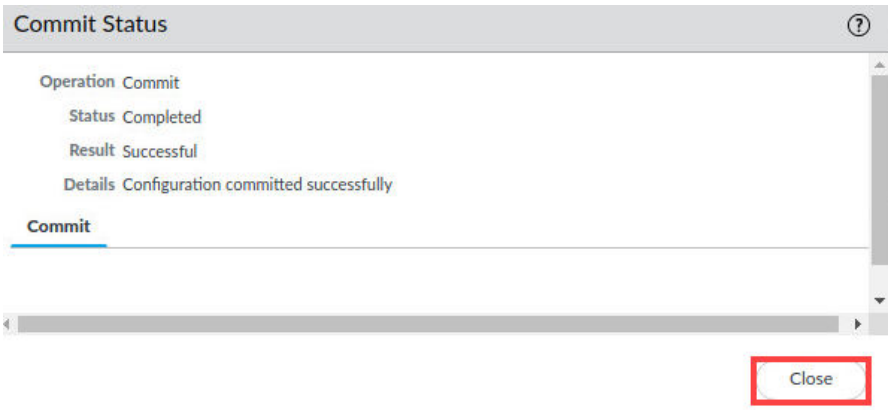
12. Click the **Commit** link located at the top-right of the web interface.



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



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



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

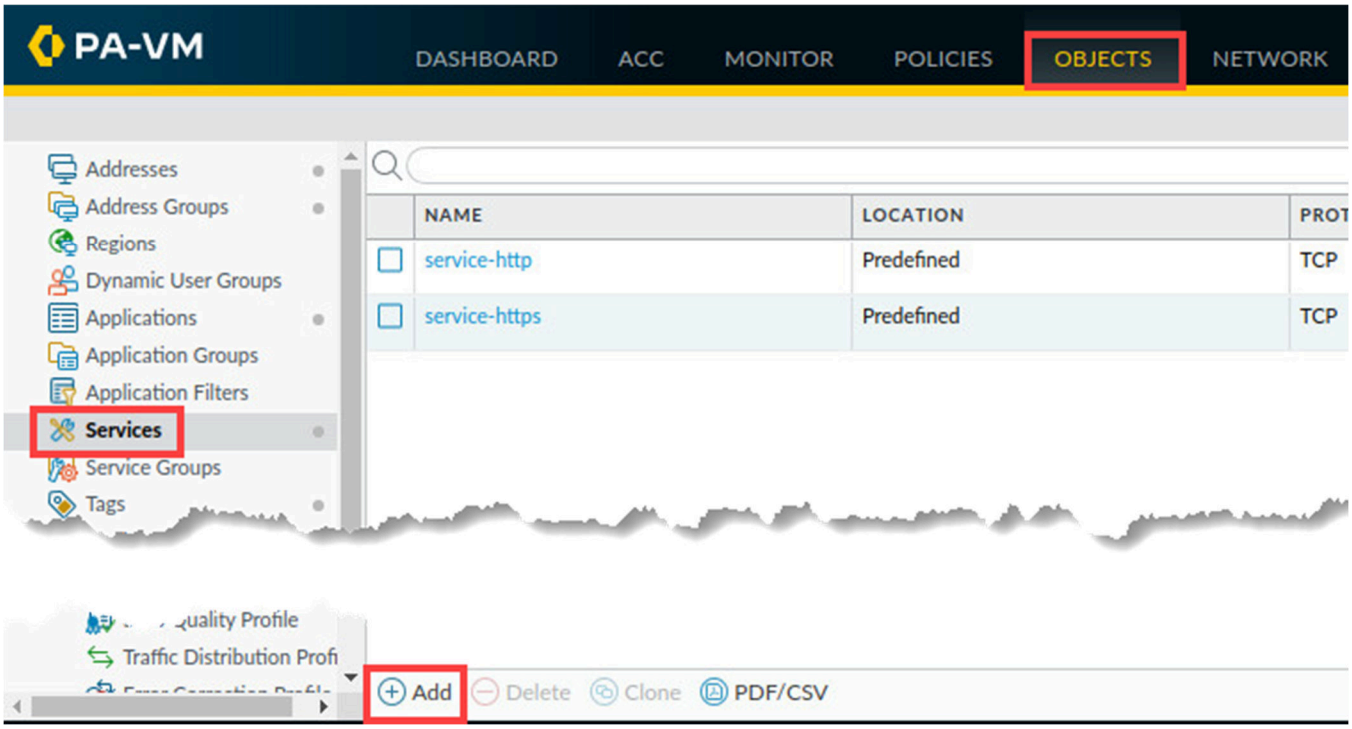
16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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

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

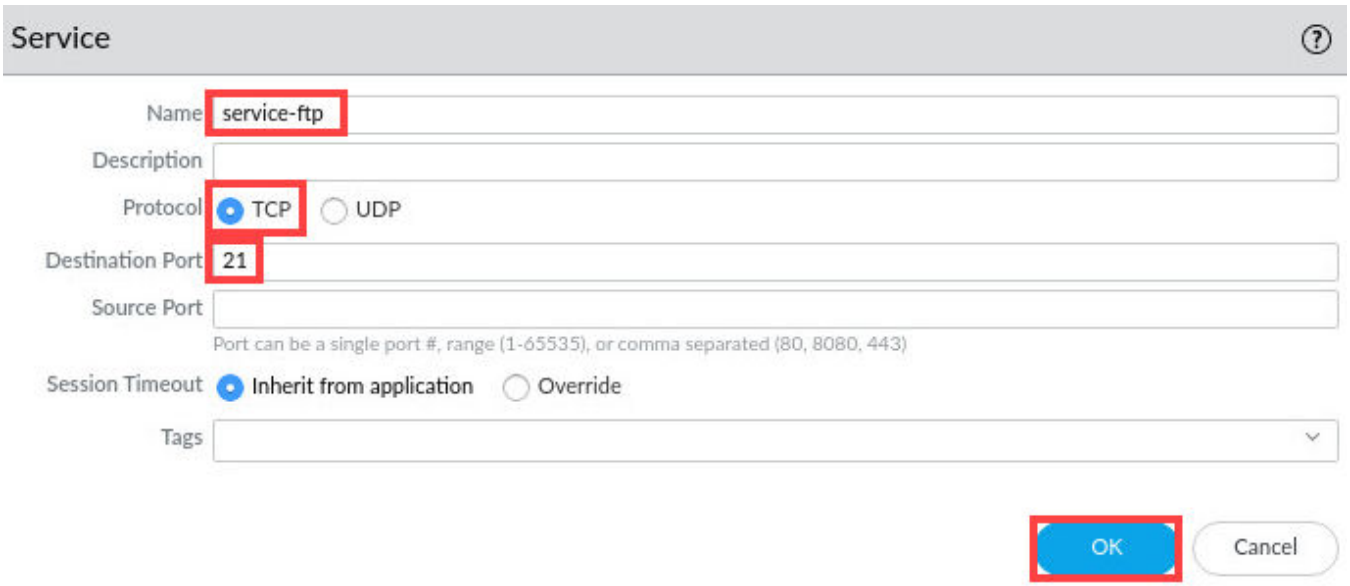
Lastly, you will generate FTP traffic from the client host to an FTP server in the Extranet zone. Then you will examine the Traffic log to view how the firewall processed the FTP traffic. After you complete this section, you will move on to other tasks related to App-ID. At the end of this lab, you will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

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

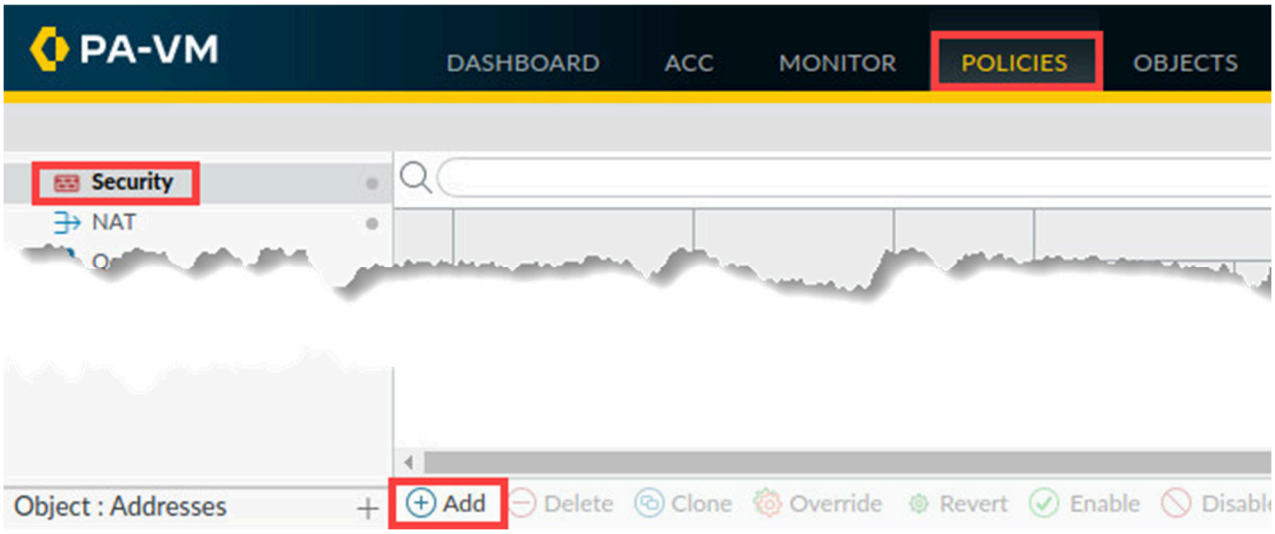


2. In the *Service* window, configure the following. Click **OK**.

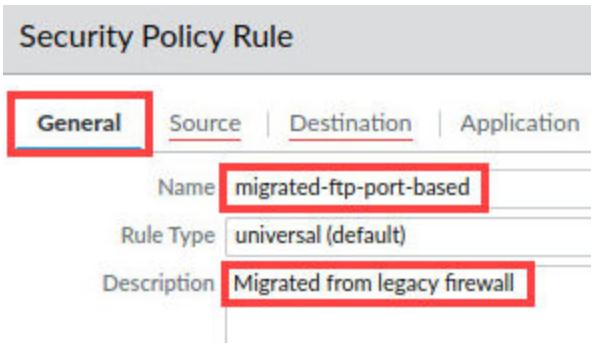
Parameter	Value
Name	**service-ftp**
Protocol	**TCP**
Destination Port	**21**



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



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

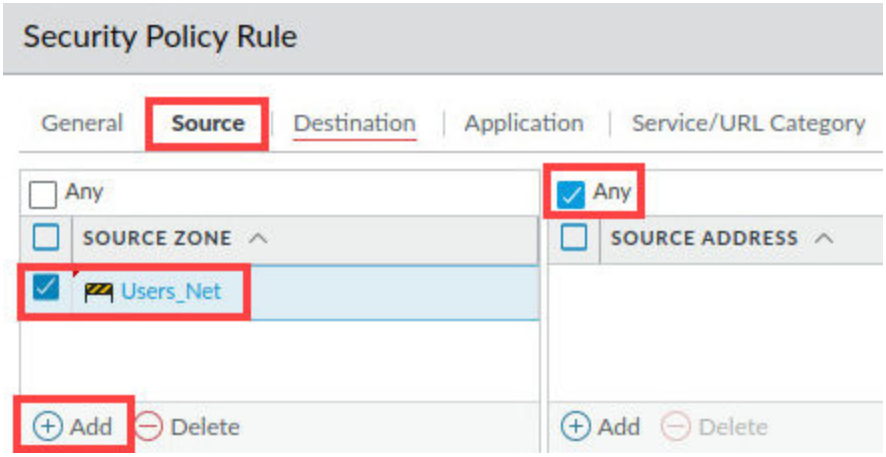


Please Note

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

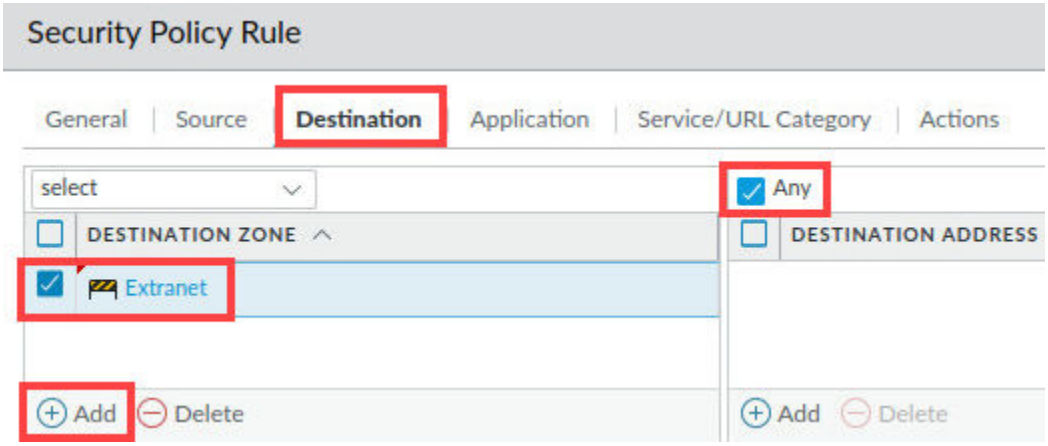
5. Click the **Source** tab and configure the following:

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



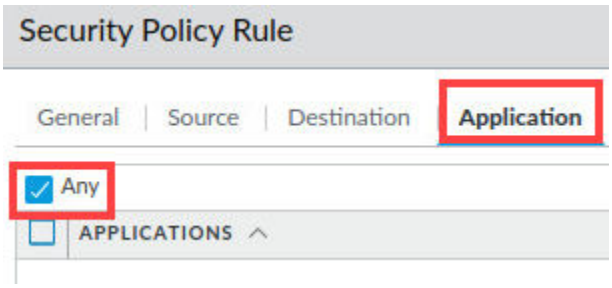
6. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	**Extranet**
Destination Address	**Any**



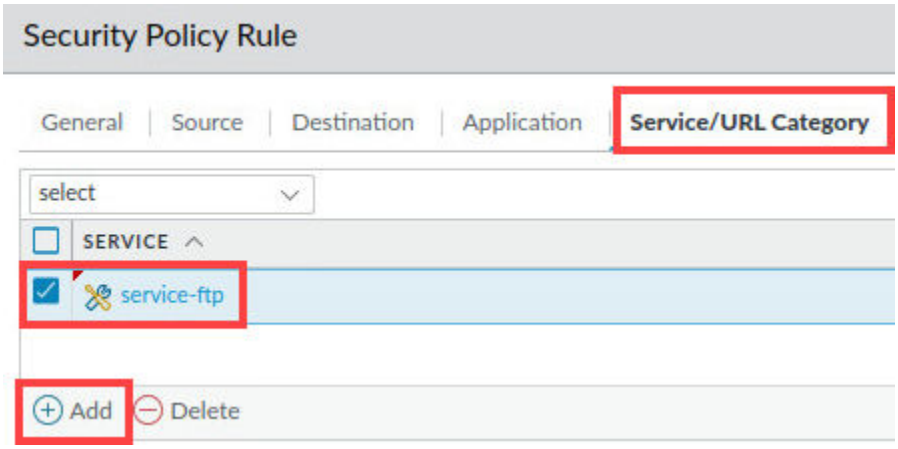
7. Click the **Application** tab and verify the following:

Parameter	Value
Applications	**Any**



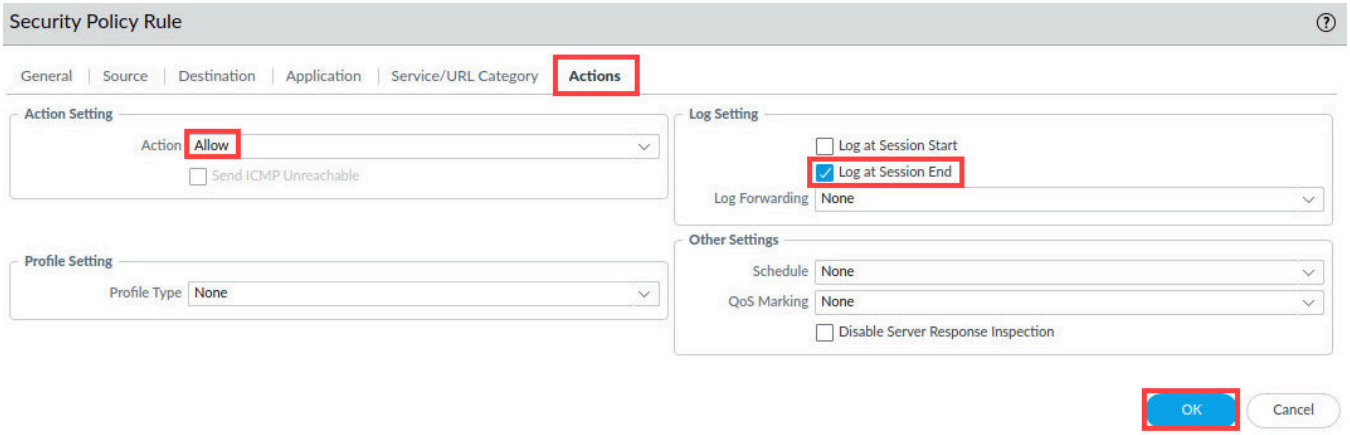
8. Click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	**service-ftp**

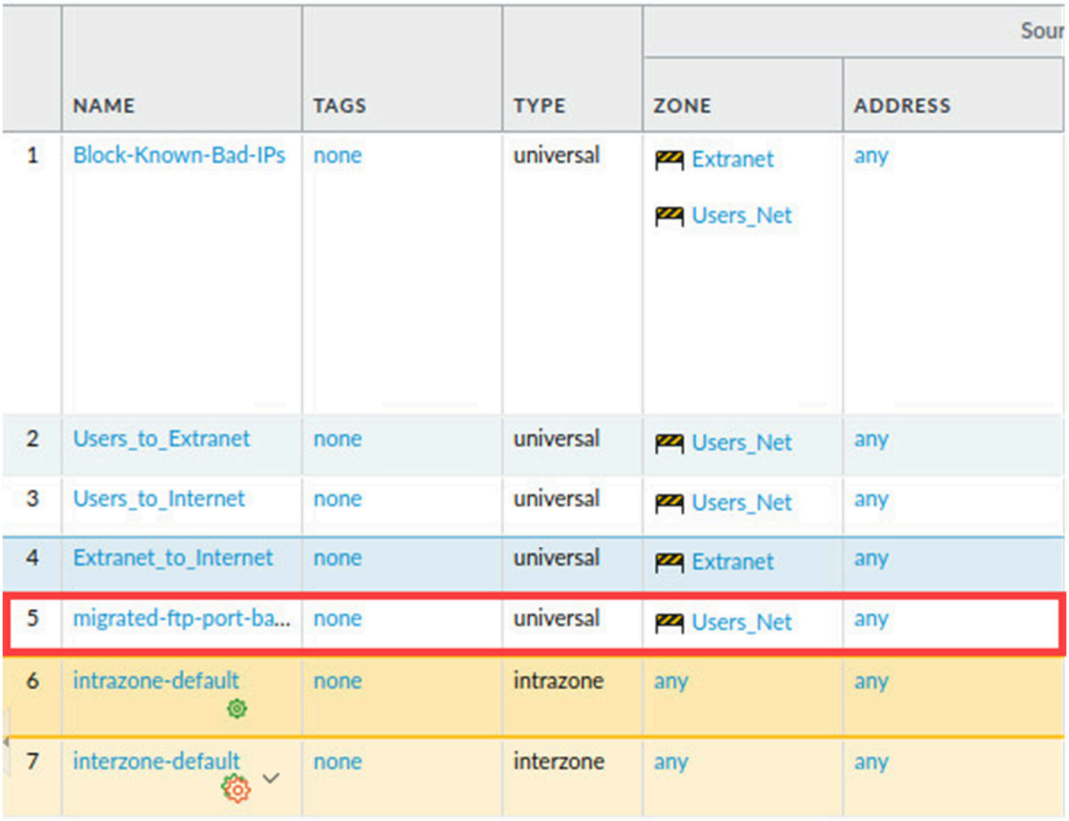


9. Click the **Actions** tab and verify the following. Click **OK**.

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



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

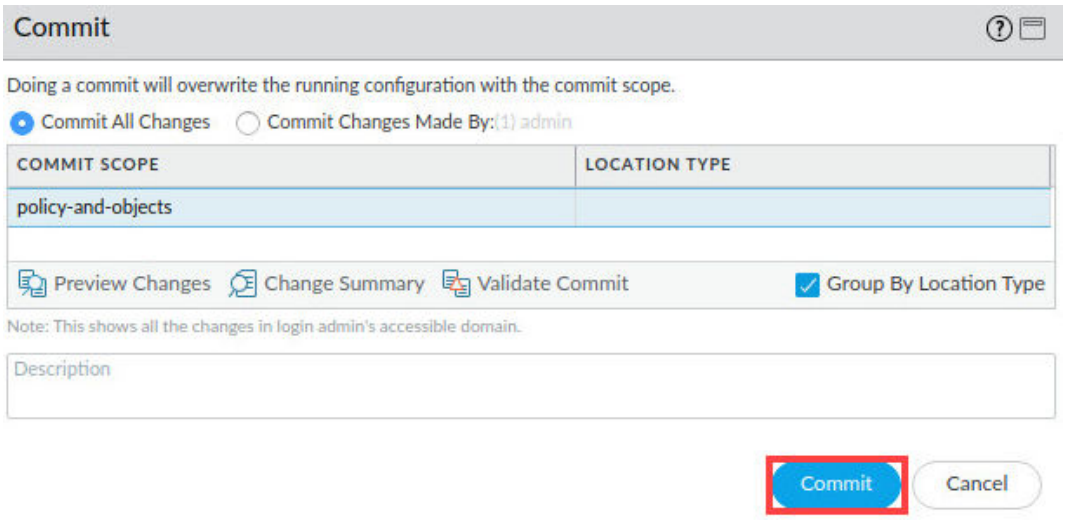


11. Use your mouse pointer to drag-and-drop the **migrated-ftp-port-based** rule to just above the **Users_to_Extranet** rule.

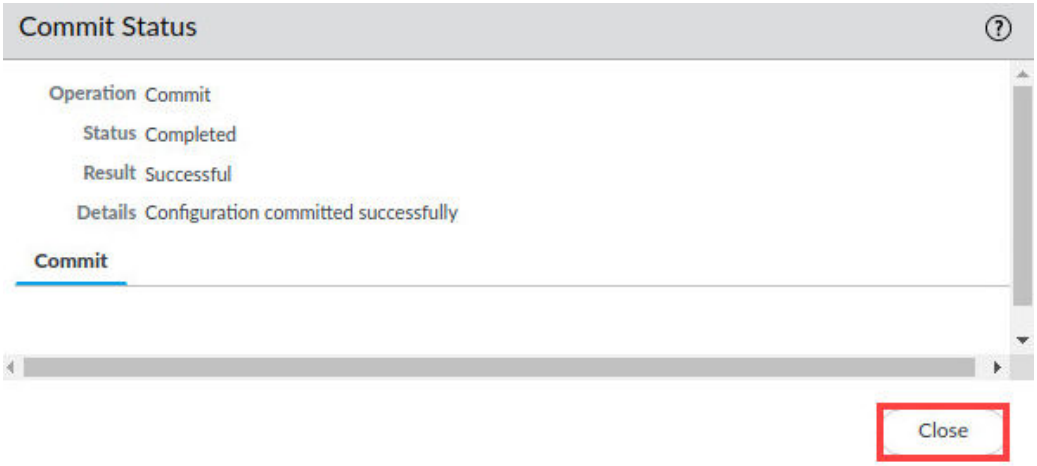
	NAME	TAGS	TYPE	Source		
				ZONE	ADDRESS	USER
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any	any
3	Users_to_Extranet	none	universal	Users_Net	any	any

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

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

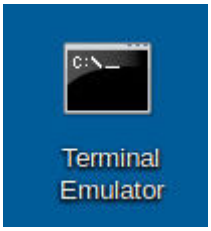


14. Wait until the *Commit* process is complete. Click **Close**.



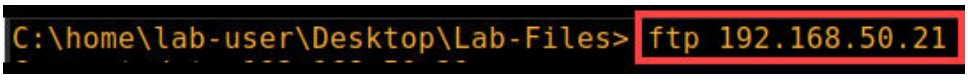
15. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

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

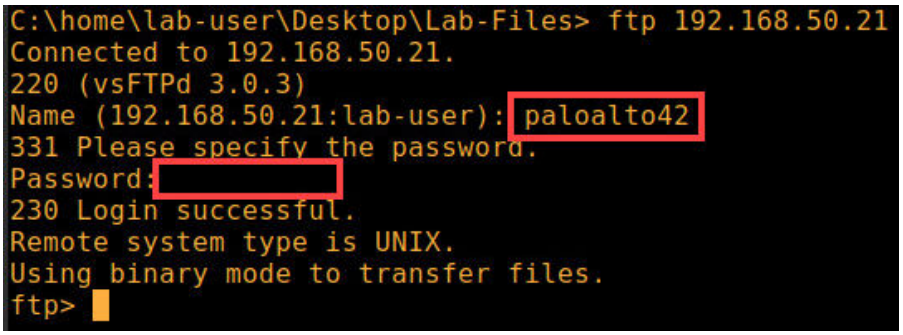


17. Enter the command below to connect to the ftp server at 192.168.50.21.

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

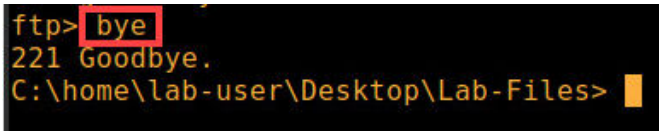


18. Log in with the username **paloalto42** and **Pal0Alt0!** as the password.



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

```
ftp> bye
```

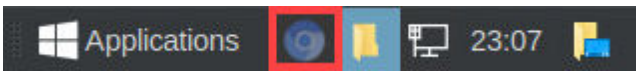


> **Please Note** This command should end the FTP session. An FTP session will be logged on the firewall even though no file was transferred.

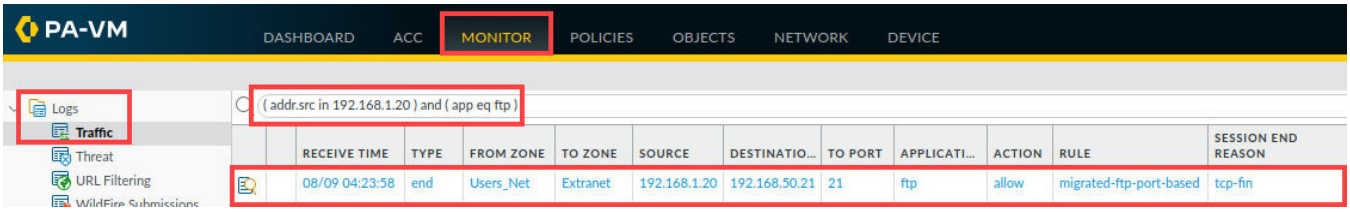
20. Close the *terminal* window by typing **exit**.

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

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



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



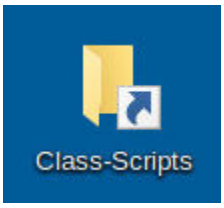
> **Please Note** Some columns have been hidden to provide all the information needed for this step. If you do not hide or move columns, you can use the scroll bar to view the entire traffic log for the FTP session.

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

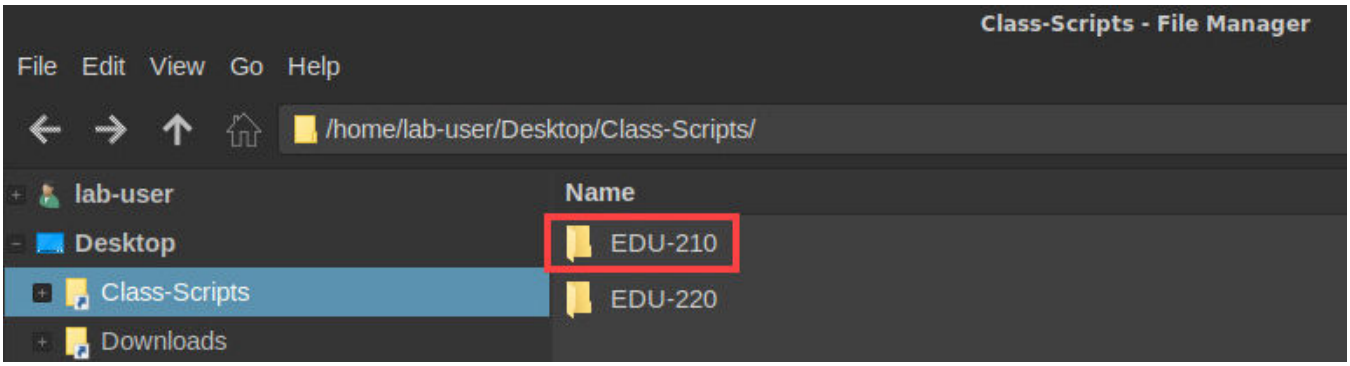
1.3 Generate Application Traffic

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

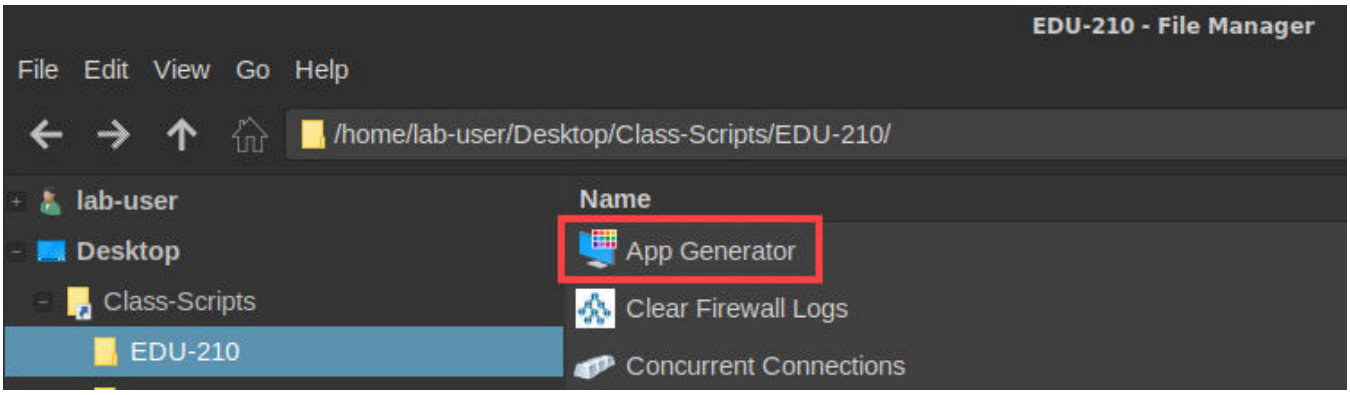
1. On the *client desktop*, double-click the folder for **Class-Scripts**.



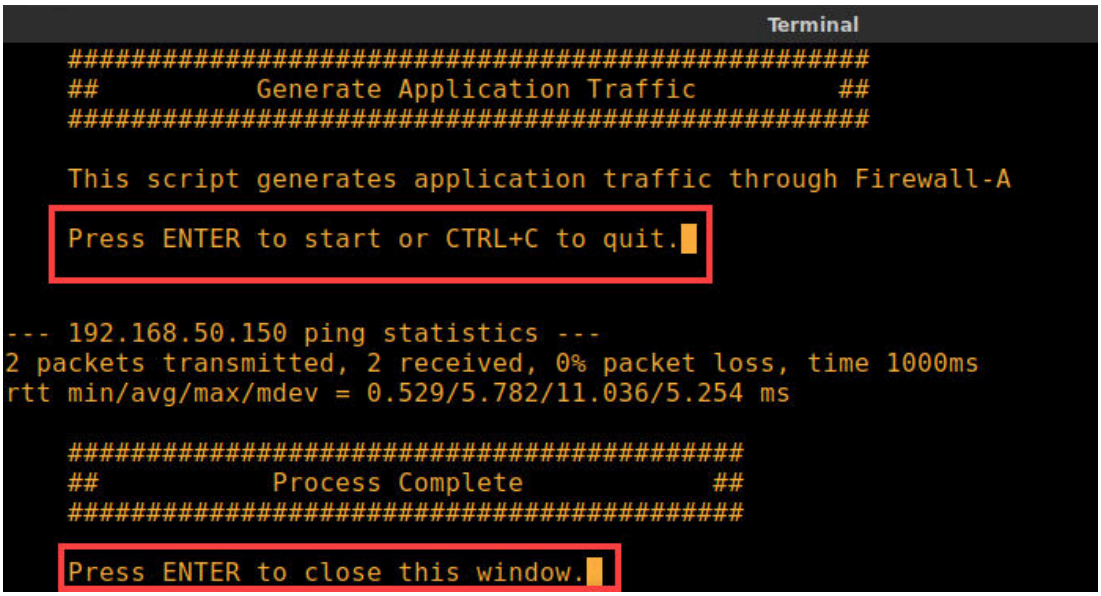
2. Open the **EDU-210** folder.



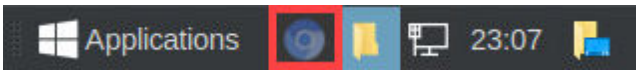
3. Double-click the icon for **App Generator**.



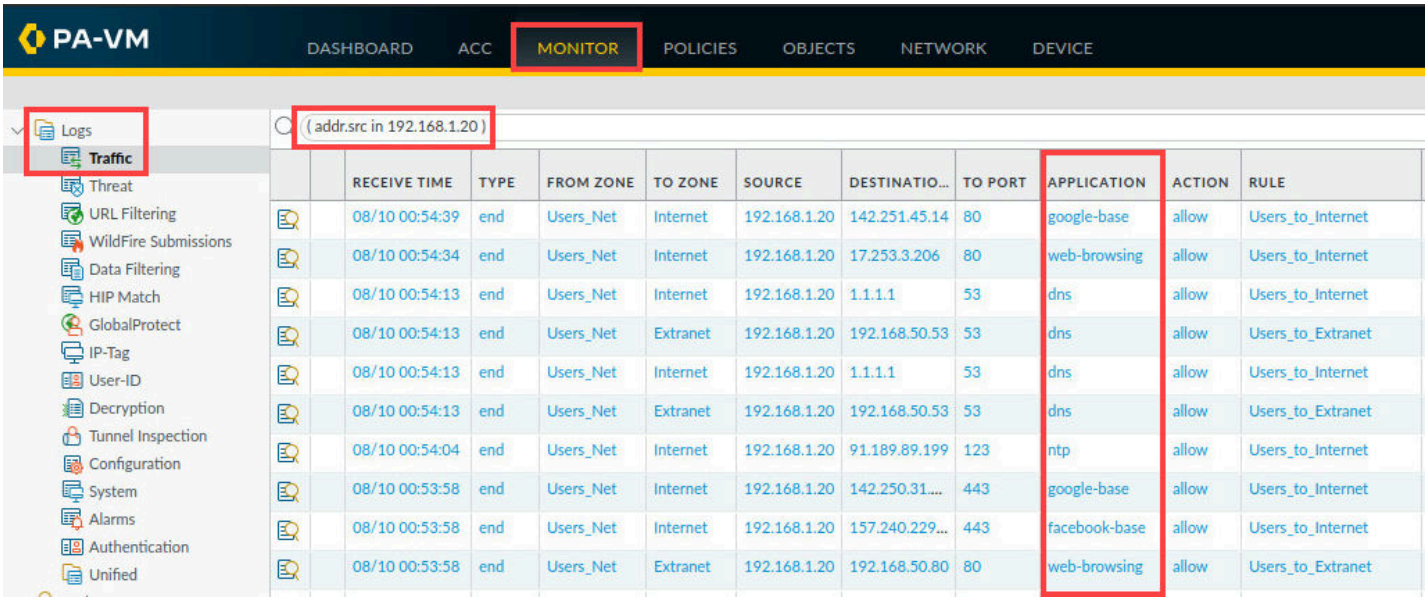
4. Press **Enter** to start the *App Generator* script. Allow the script to complete. Once the *App Generator* script completes, press **Enter**. Allow the script *30* seconds to *1* minute to complete before proceeding to the next step.



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



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



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

Please Note

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

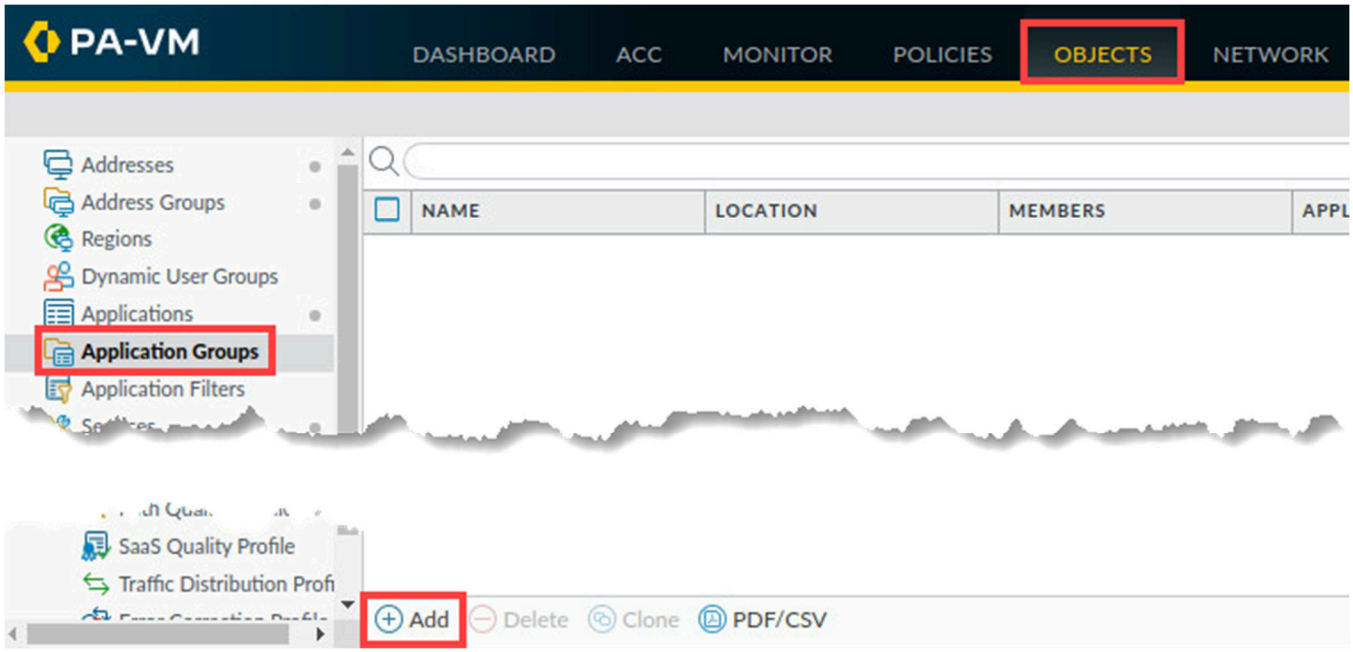
You should see entries for ftp, dns, google-base, ssl, web-browsing, facebook-base and ping. Use the refresh button to update the entries if necessary.

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

1.4 Configure an Application Group

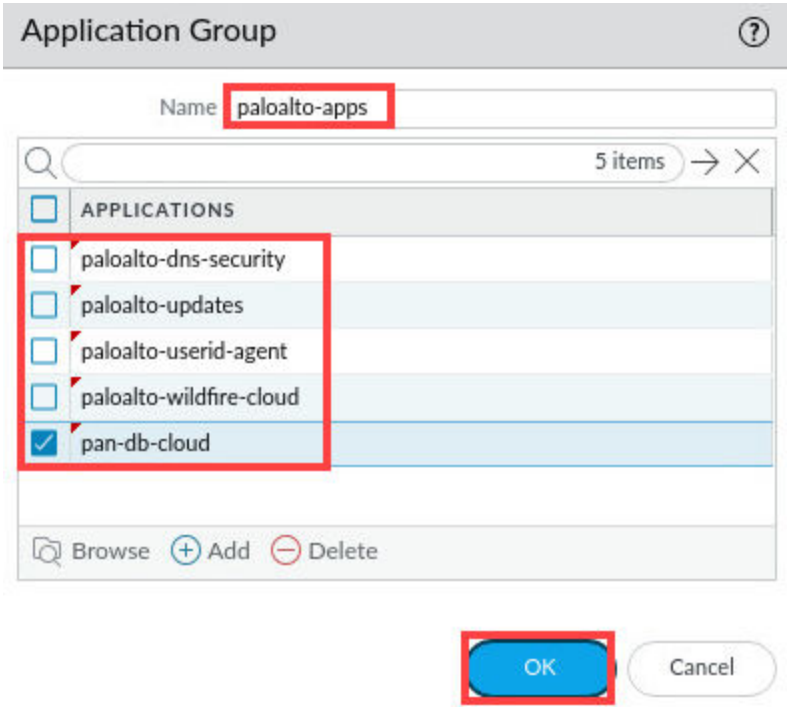
In this section, you will configure an application group called **paloalto-apps** that includes some Palo Alto Networks applications. These applications are used to label and control access to the content update network and other Palo Alto Networks products and features. You will add the application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

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



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

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

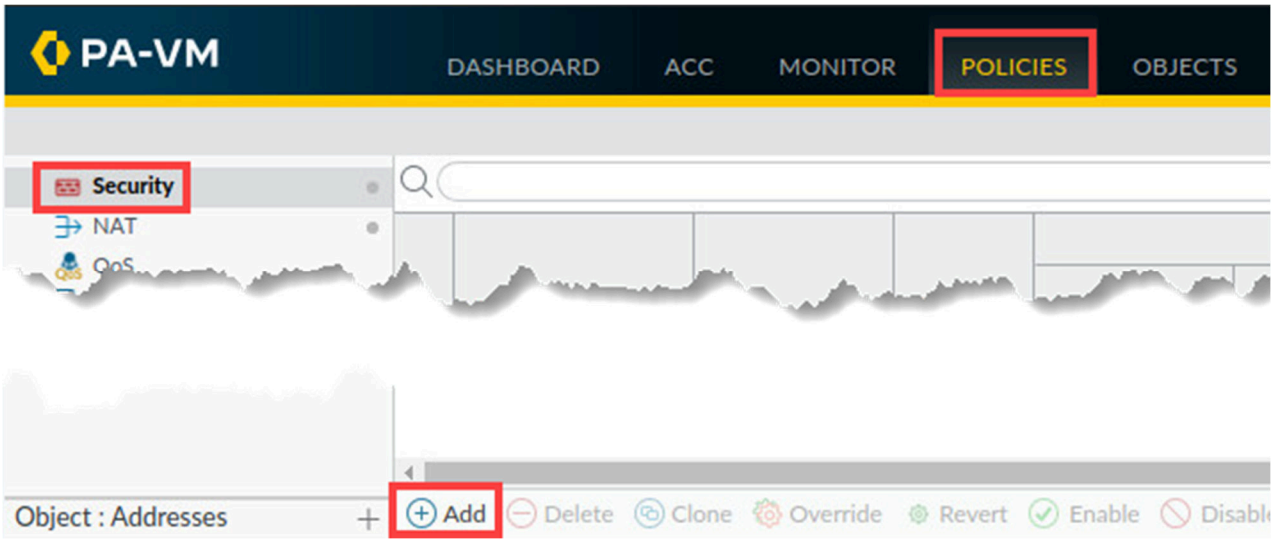


3. Leave the firewall open and continue to the next task.

1.5 Configure a Security Policy to Allow Update Traffic

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

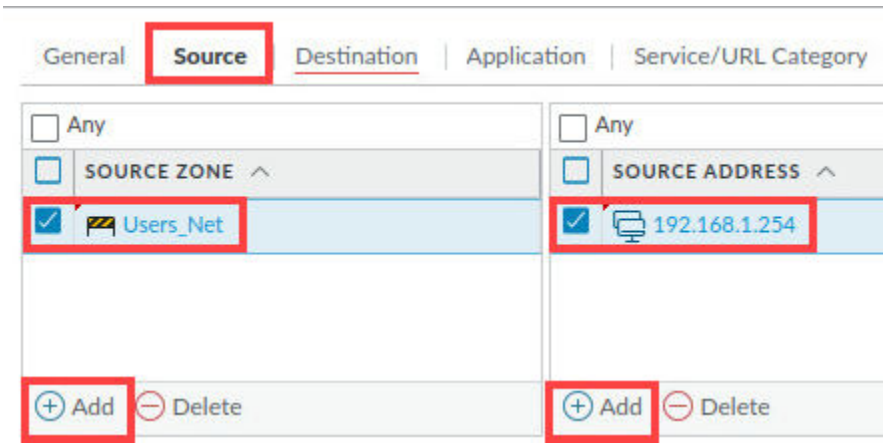
1. In the web interface, navigate to **Policies > Security.** Click **Add** to configure a new security policy.



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

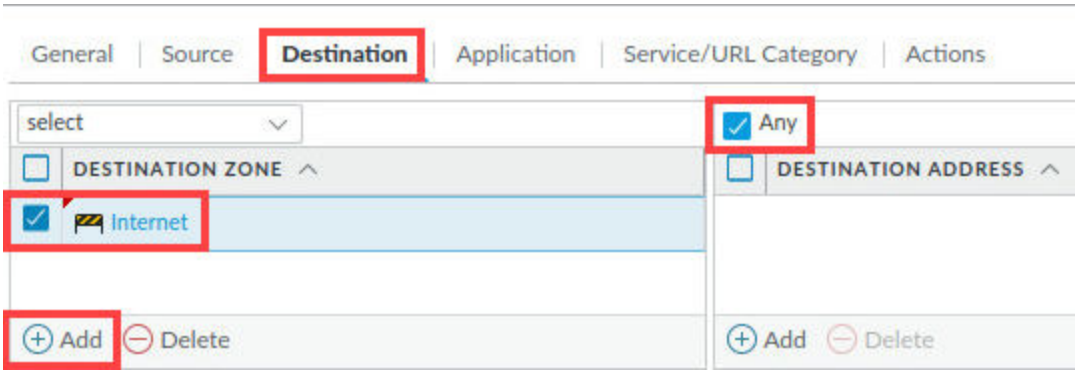
3. Click the **Source** tab and configure the following.

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



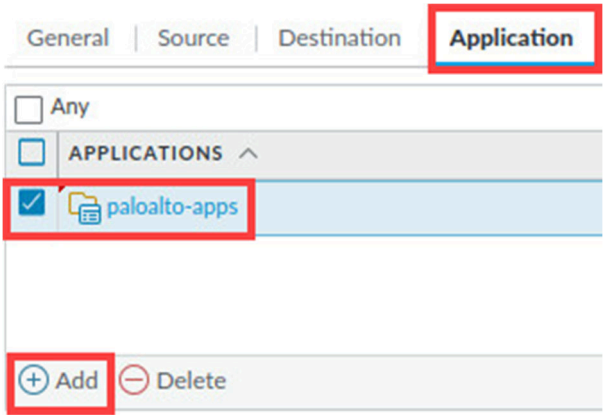
4. Click the **Destination** tab and configure the following.

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



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

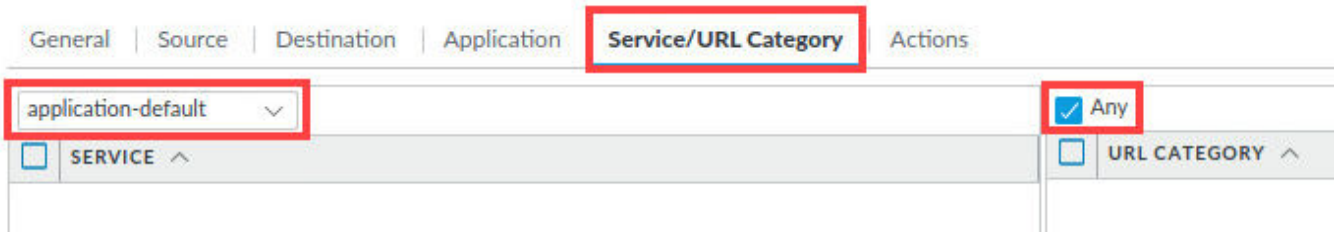
Parameter	Value
Applications	**paloalto-apps**



Please Note

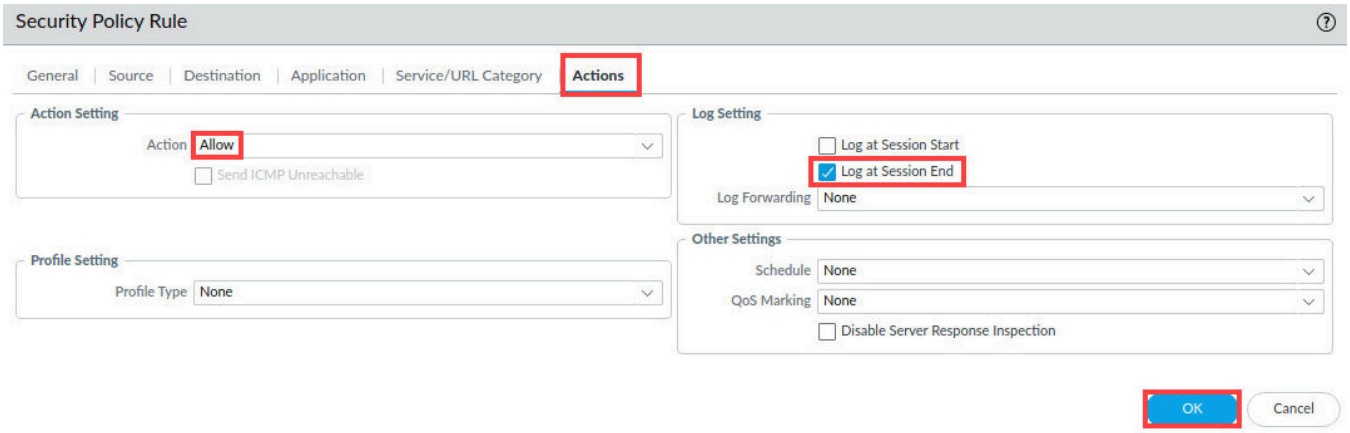
To locate your **paloalto-apps** Application Group, start typing in the first few letters of the group name, and the interface will display only those entries which match. Application Groups appear at the very end of the Application list.

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**

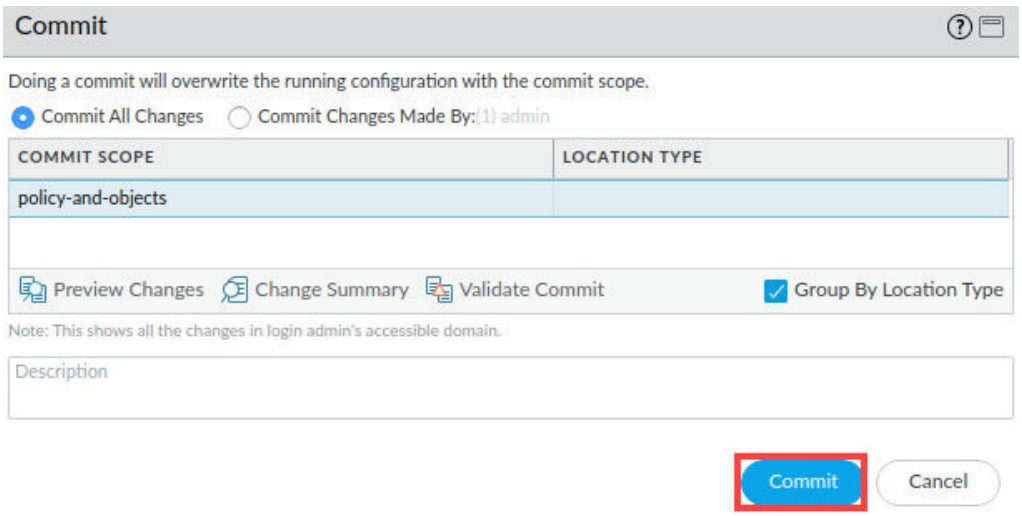


8. The **Allow PANW-Apps** rule should be listed just above the *intrazone-default* rule in the security policy rule list.

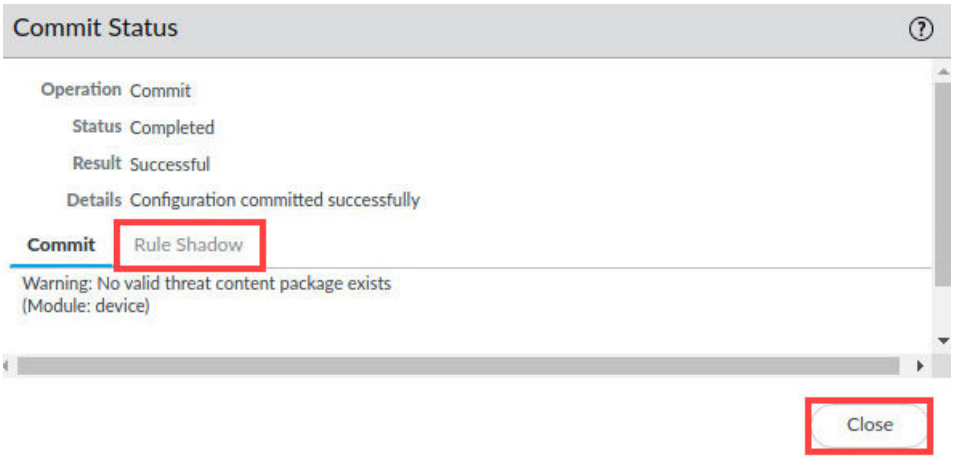
	NAME	TAGS	TYPE	Sour ZONE	ADDRESS
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net	any
2	migrated-ftp-port-ba...	none	universal	Users_Net	any
3	Users_to_Extranet	none	universal	Users_Net	any
4	Users_to_Internet	none	universal	Users_Net	any
5	Extranet_to_Internet	none	universal	Extranet	any
6	Allow-PANW-Apps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

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

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



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

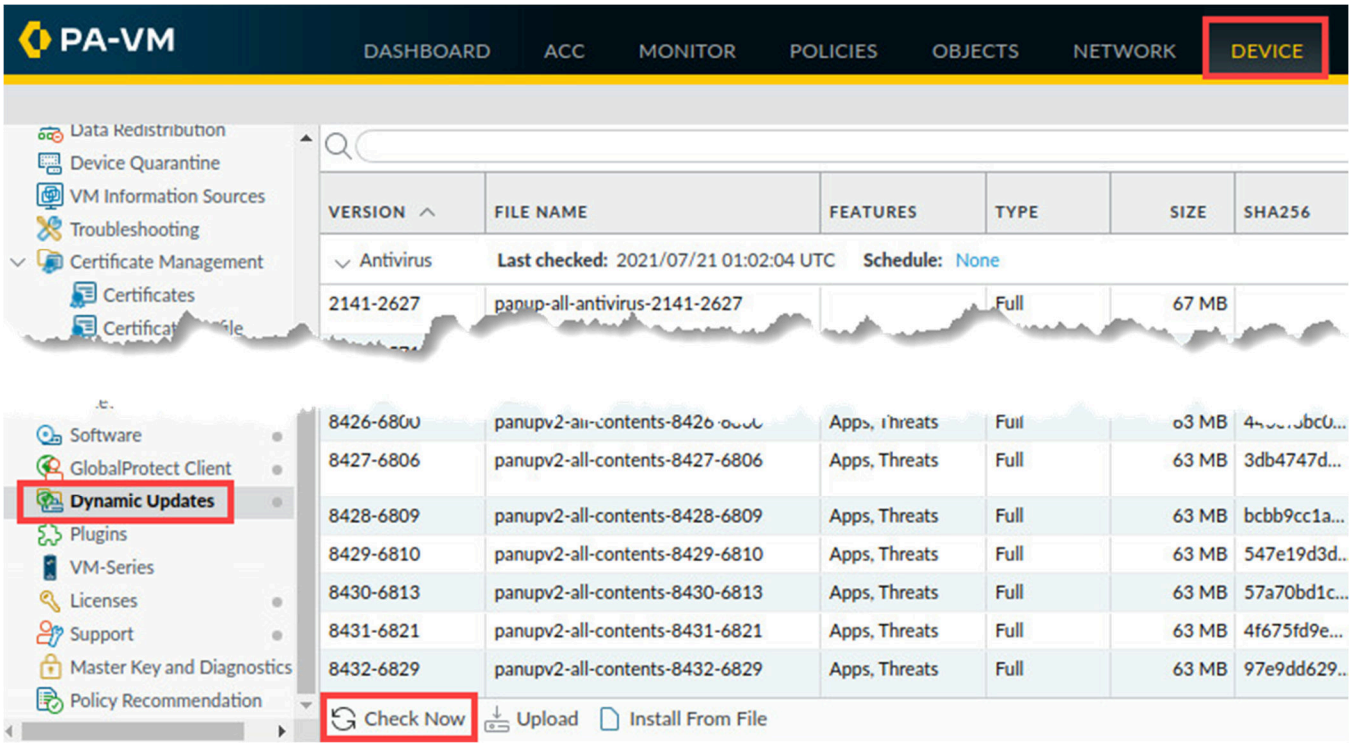


12. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Test the Allow-PANW-Apps Security Policy Rule

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

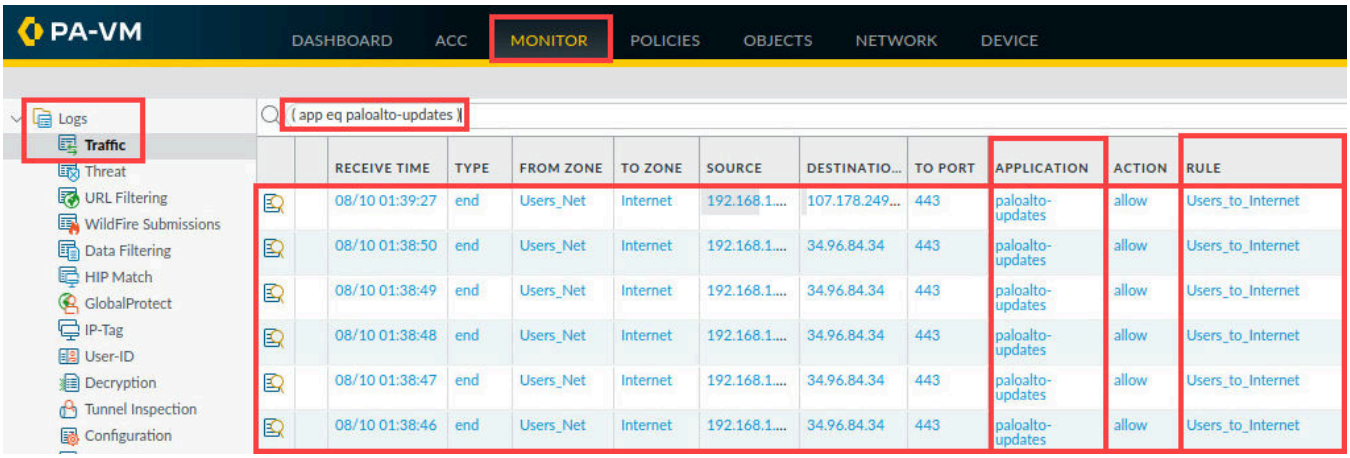
1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.



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.



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

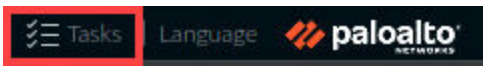
3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.7 Examine the Tasks Lists to See Shadowed Message

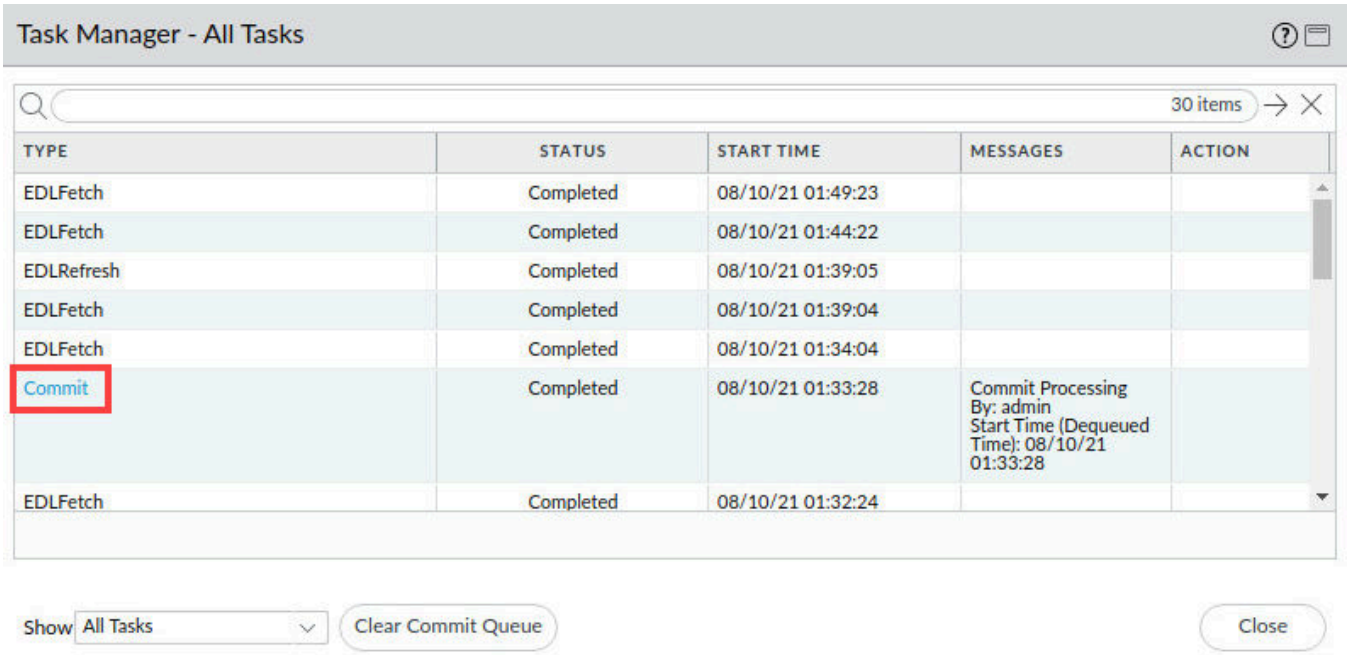
The firewall provides notification when you have a rule shadowing one or more other rules. The **Rule Shadow** tab appears at the end of the Commit process.

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

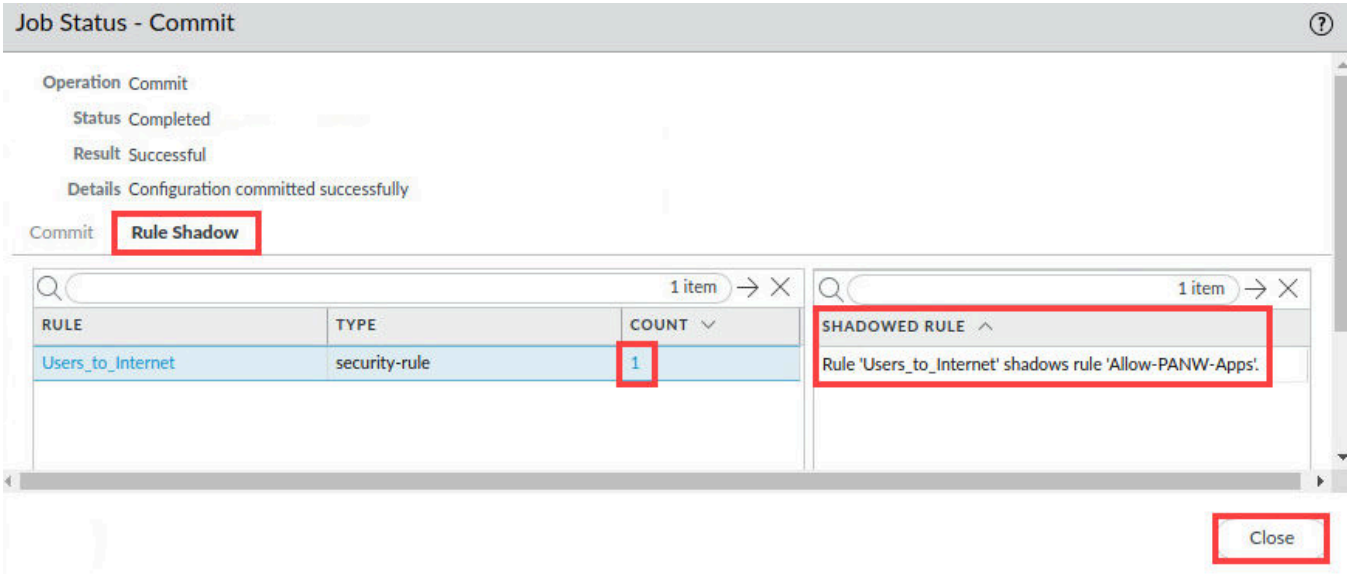
1. In the bottom-right corner of the *PA-VM firewall* interface, click the **Tasks** button.



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



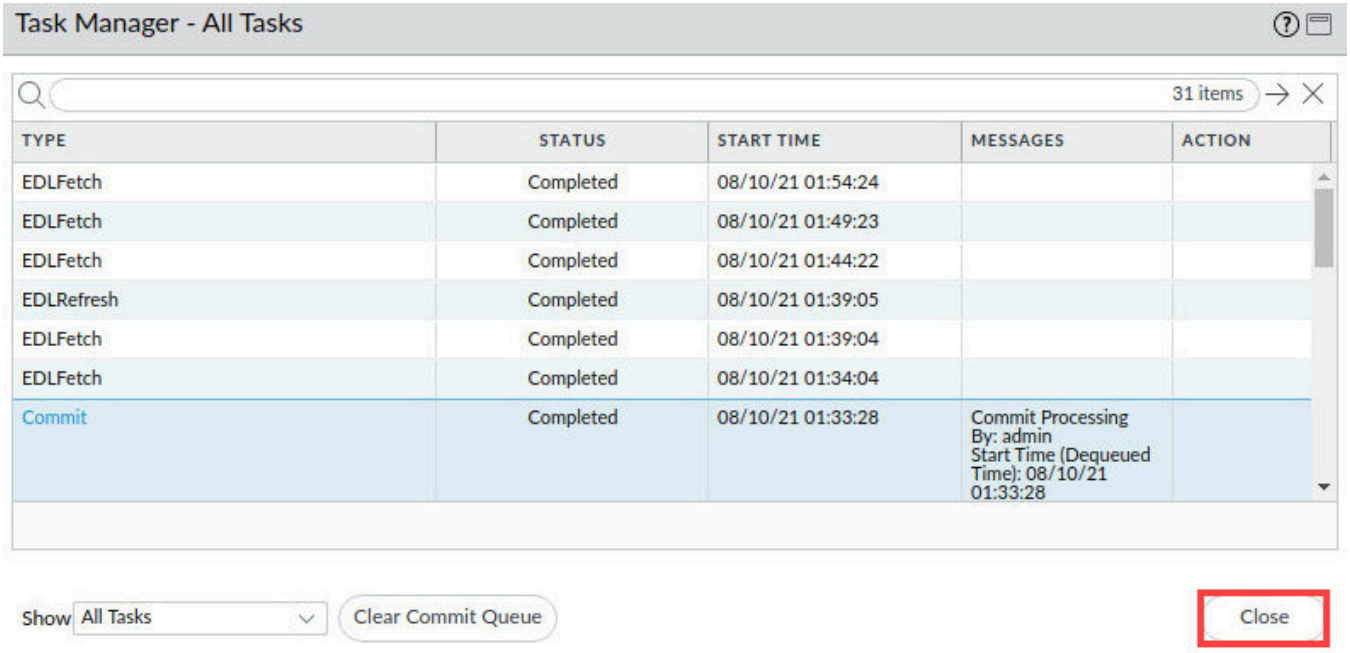
3. In the *Job Status – Commit* window, select the **Rule Shadow** tab. The interface shows you which rule is shadowing other rules. **Click** the number under the *Count* (in this example, the value is **1**). Click **Close**.



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**.



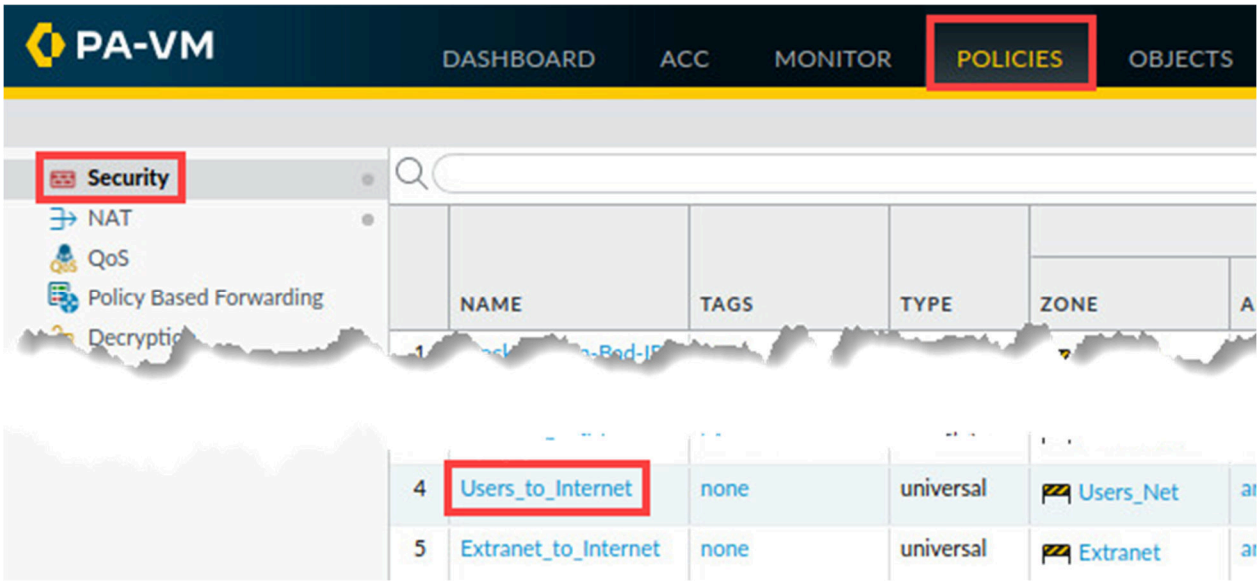
5. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.8 Modify the Security Policy to Function Properly

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

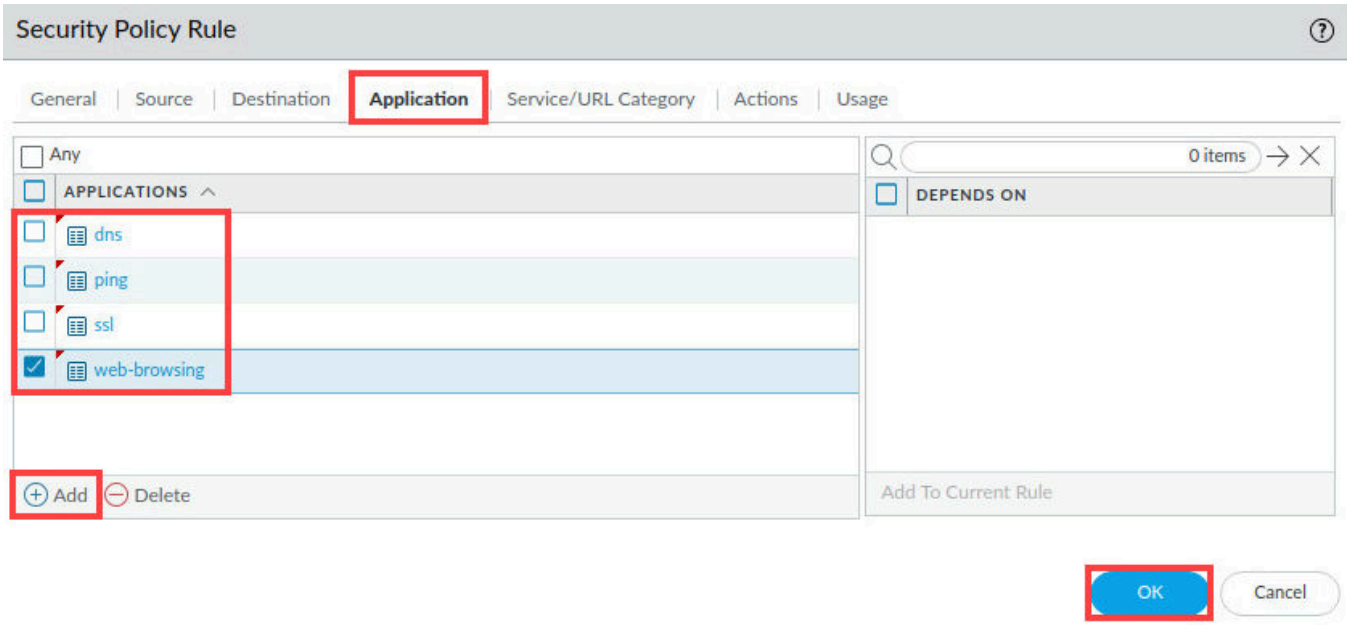
You will also modify the security policy rule that allows traffic from the Users_Net to the Internet. Instead of allowing any application, the modified rule will allow only a few applications.

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



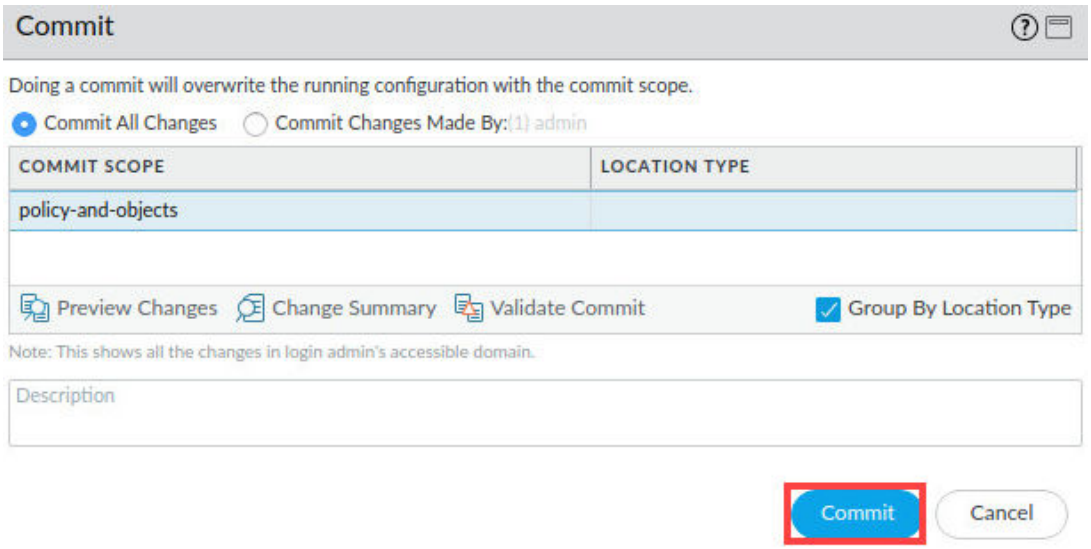
2. In the *Security Policy Rule* window, click the **Application** tab and configure the following. Click **OK**.

Parameter	Value
Applications	**dns** **ping** **ssl** **web-browsing**

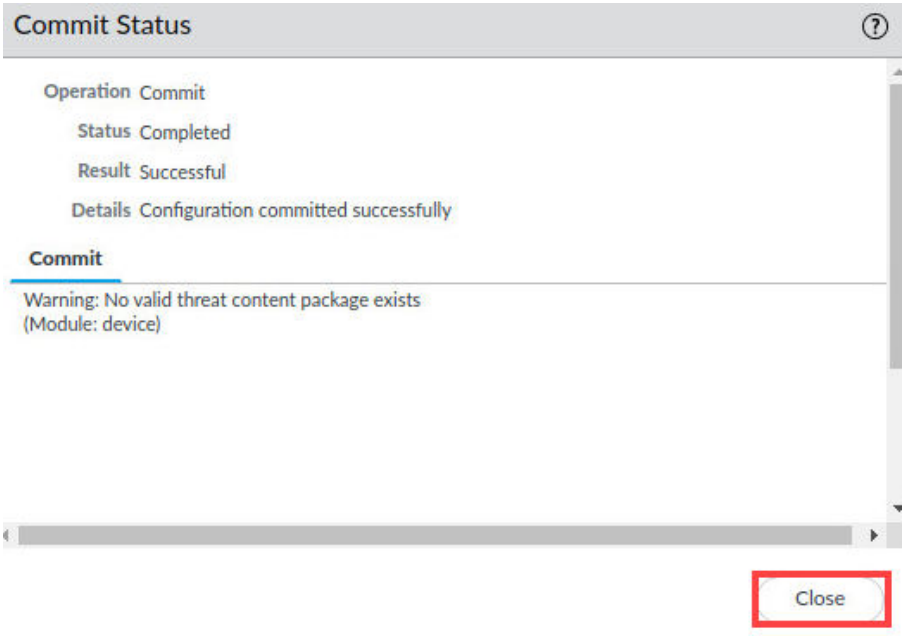


3. Click the **Commit** button at the upper-right of the web interface.

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



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

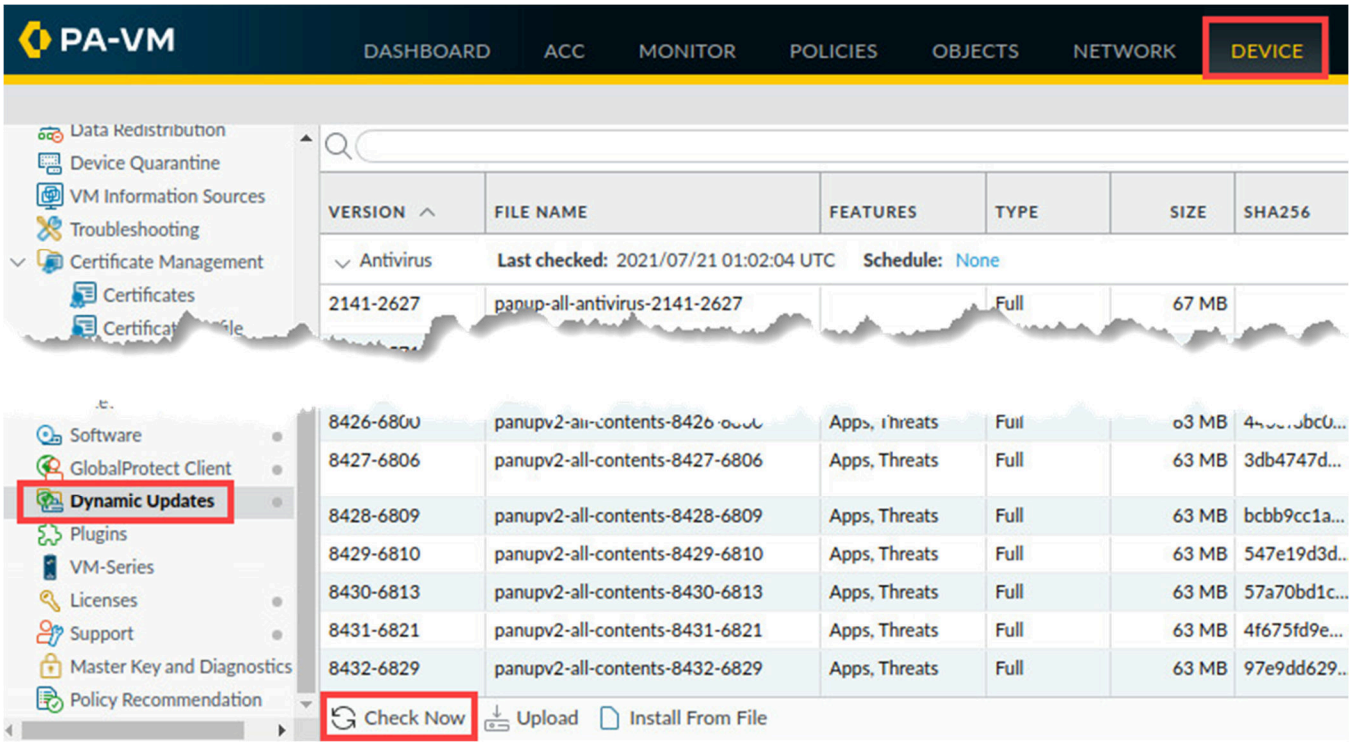


6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

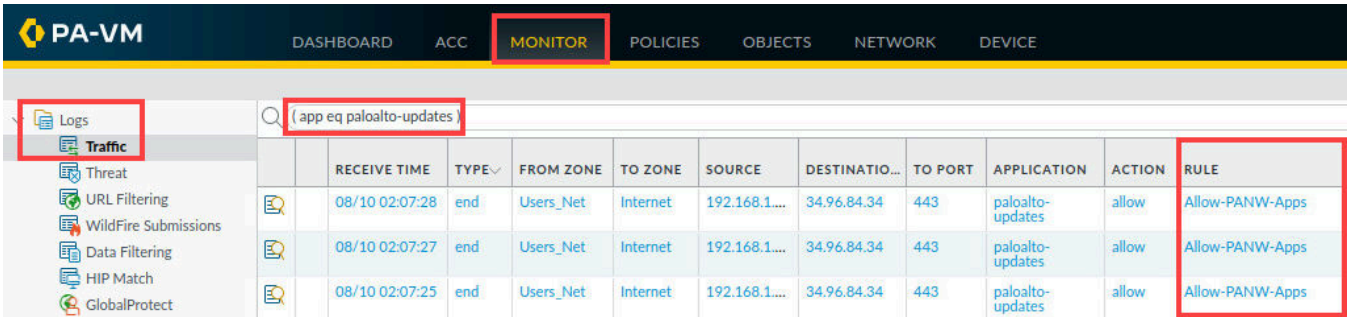
1.9 Test the Modified Security Policy Rule

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

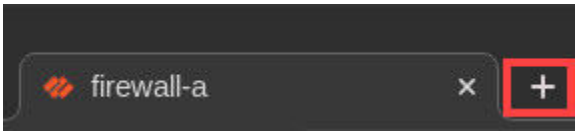
1. In the *firewall* interface, select **Device > Dynamic Updates**. Click **Check Now**.



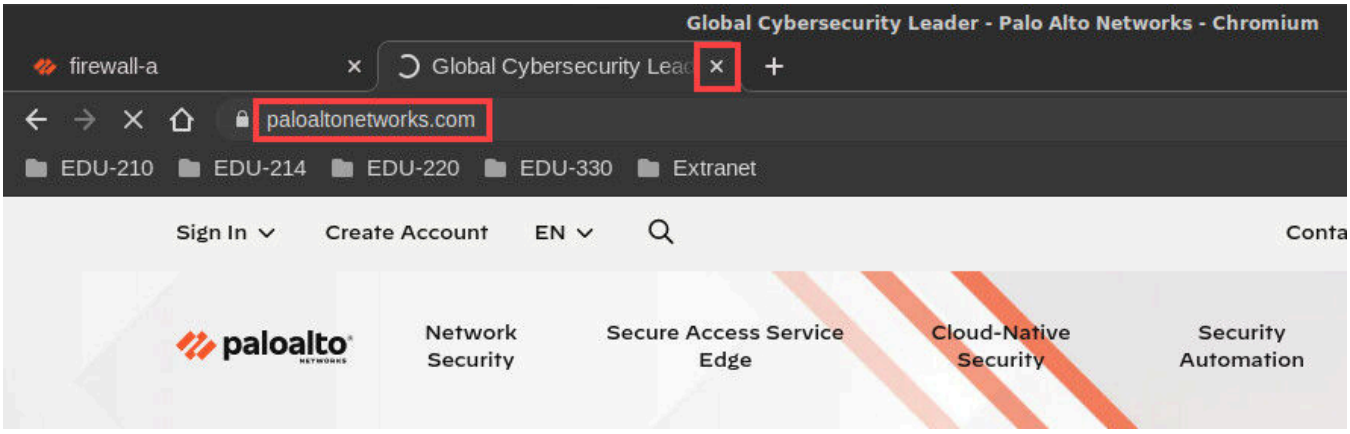
2. Select **Monitor > Logs > Traffic**. Apply the following filter **`( app eq paloalto-updates )`** in the filter builder. Look for the log entries for the application *paloalto-updates*. It should be the **Allow-PANW_Apps** rule.



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



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



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

Please Note

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

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