PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 13: Locating Valuable Information Using Logs and Reports

Document Version: 2025-10-13

Contents

Introduction

Having worked with the new Palo Alto Networks firewall, you have discovered how much information the device provides about traffic that it processes. You have already worked with the Traffic, Threat, URL and System log files and learned how to create filters to locate specific information. But before you roll the firewall into production, you want to spend some time looking at some of the other resources, graphs, reports, and tools that are available.

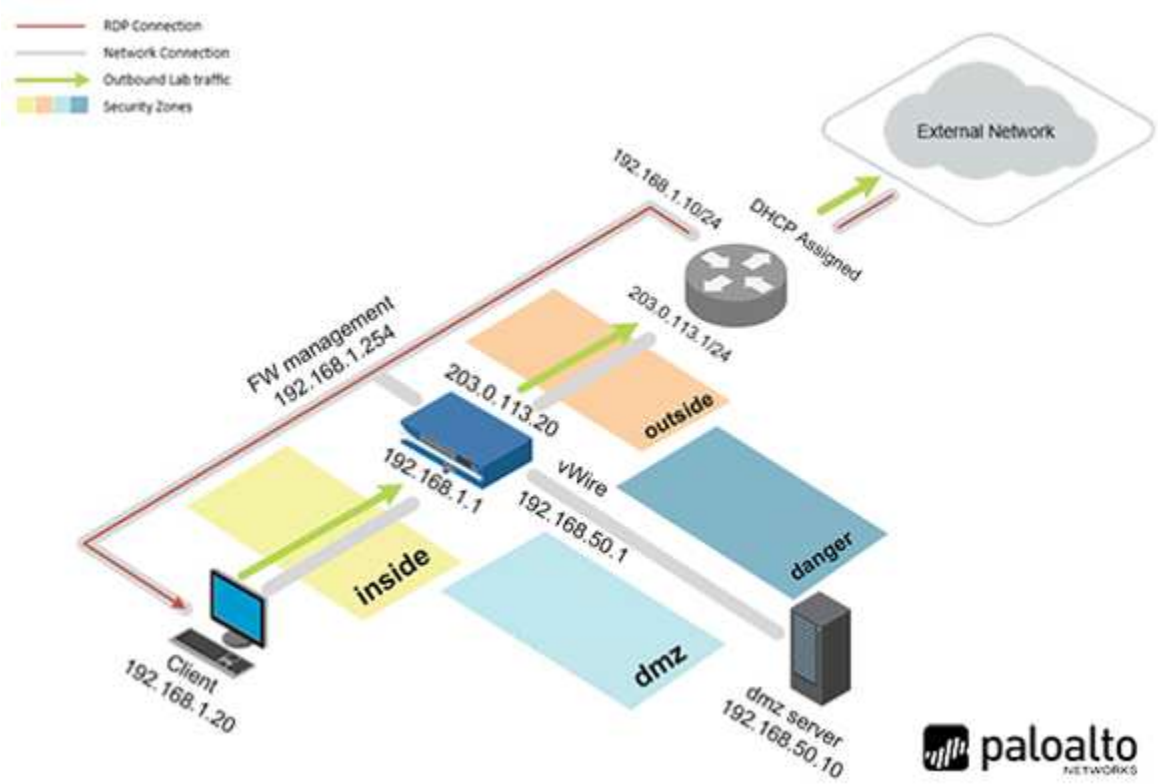
You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

Objective

In this lab, you will perform the following tasks:

- View threat information using the Dashboard.
- View application information using the Dashboard.
- View threat information using the ACC.
- View application information using the ACC.
- View threat information using the Threat log.
- View application information using the Traffic log.
- View threat information using App Scope reports.
- View threat information using predefined reports.
- View application information using predefined reports.
- View threat and application information using custom reports.

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 Locating Valuable Information Using Logs and Reports – 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-13.xml** to the Firewall.

1.2 Generate Traffic

- Use the Remmina application to connect to the **Server-Extranet** host.
- Run the traffic generating script by entering the following commands:
  cd ~ <ENTER>
  ./UsingLogs-V1.sh <Enter>
- Allow the script to run uninterrupted.

1.3 Display Recent Threat Information in the Dashboard

- Add the Threat Logs widget to the Dashboard.
- Use the Threat Log widget to determine what threats the firewall has detected within the last hour.
- Add the URL Filtering Logs widget to the Dashboard.
- Use the URL Filtering Logs widget to examine URL Filtering entries written by the firewall within the last hour.
- Add the Data Filtering Logs widget to the Dashboard.
- Use the Data Filtering Logs widget to examine Data Filtering entries written by the firewall within the last hour.

1.4 Display Recent Application Information in the Dashboard

- Add the Top Applications widget to the Dashboard.
- Note which applications the firewall has detected within the last hour.
- Add the Top High Risk Applications to the Dashboard.
- Note which applications the firewall has detected that are considered high-risk.

  Note: Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks.

1.5 View Threat Information in the ACC

- In the ACC, use the Threat Activity tab to view information for the Last 7 Days.

- In the Threat Activity widget's table below the graph, click the small arrow icon next to one of the critical severity level entries to add critical severity level as a Global filter for the ACC.

  Note that the widget's table changes to display only threats that have a critical severity level.
- In the Global Filters area, click Clear all to remove the global filter.
- On the Threat Activity tab, determine what widgets you would use to see which hosts have either visited or resolved a malicious DNS domain.

1.6 View Application Information in the ACC

- In the Network Activity tab of the ACC, hide the sidebar to make more room for the widgets.
- In the top section of the Application Usage widget, hover your mouse pointer over the web-browsing section in the graph.

  Note the summary window that appears with information about web-browsing.
- In the table below the graph, hover your pointer over the web-browsing application until the global filter Left arrow appears. Then click the Left arrow to promote the web-browsing application to a global filter.
- Unhide the sidebar.
- In the Network Activity tab, locate the Rule Usage widget and change the display to Bytes.

  Use the information displayed to determine which Security Policy rules have allowed web-browsing traffic.
- In the Rule Usage widget, use the Jump to Logs button to open the Traffic Log.

  Note the log filters that have been applied automatically to the Traffic log.
- Clear the filter in the Traffic log.
- In the Global Filters section of the ACC tab, clear all filters.

1.7 View Information in the Threat Log

- In the Threat Log, clear any filters you may have in place.
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	**and**
Attribute	**Severity**
Operator	**greater than or equal**
Value	**high**

  This configuration filters the log to display only critical-severity and high-severity threats.
- Apply the filter to the Threat Log.
- Use the information from the Action column to determine how these threats have been handled by the firewall.
- Clear the existing filter.
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	**and**
Attribute	**Source User**
Operator	**equal**
Value	**chicago\escrooge**

This configuration filters the log to display threats coming from only this user.

- Apply the filter to the Threat log.
- Note what Threats this user has generated. You may need to add the Source User column to the Threat Log display if it is not already present.
- Clear the existing filter.

  Note: URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

1.8 View Application Information in the Traffic Log

- In the **Traffic** Log, remove any existing log filters.
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**equal**
Value	**Acquisition**

This configuration filters the log to display only application traffic that is sourced from the Acquisition zone.

- **Apply** the filter to the Traffic Log.

  Note that the Traffic log has been filtered to display only traffic sourced from the Acquisition zone.
- Use the **Add Log Filter** to modify the existing source zone filter to filter on the Users_Net zone instead of the Acquisition zone.
- Use the Add Log Filter to update the filter to include the following information:

Parameter	Value
Connector	**and**
Attribute	**Application**
Operator	**equal**
Value	**web-browsing**

- **Apply** the filter to the Traffic Log.

  Note that the Traffic log has been filtered to display only web-browsing traffic sourced from the Users_Net zone.

1.9 View Threats Using App Scope Reports

- Select App Scope > Threat Monitor.
- Set the time frame to Last 7 days.
- Set the list of entries to Top 25.
- Filter the list by Source User.
- Set the display to Show all threat types.
- Hover your pointer over the top section of any bar on the bar chart and note the popup window that shows the threat name and number of detections.

1.10 View Threat Information Using Predefined Reports

- Under Monitor > Reports, expand the list of Traffic Reports.
- Select the entry for Sources.
- Note the Sources report that is displayed in the web interface.
- In the calendar below the report column, click various dates from the past week to see information about traffic logged by the firewall on other days.

  Note that days that are grayed out do not have any data available.

1.11 View Application Information Using Predefined Reports

- Under Monitor > Reports, expand the list of Application Reports.
- Select the entry for Applications.

  Note the Applications report that is displayed in the web interface.
- Expand the list of URL Filtering Reports and select the entry for Web Sites.

  Note that you may need to click different dates until you see a report with data.

1.12 View Threat and Application Information Using Custom Reports

- Select **Monitor > Manage Custom Reports**, and use the following information to create a **Custom Report**:

Parameter	Value
Name	**Apps Used by Internal Zones**
Database	**Traffic Summary**
Scheduled check box	Select it
Time Frame	**Last 7 Days**
Sort By	Select **Sessions** and **Top 100**
Group By	Select **Source Zone** and **5 Groups**
Selected Columns	In top-down order, select **Source Zone**, **Application**, **Bytes**, and **Action**

- The report will list each internal zone along with the applications seen coming from each zone. Because only four zones are available in the lab environment, grouping of the data into a maximum of five groups is enough to display all zones. Sorting the applications list in each zone by the top 100 sessions should display all applications associated with a source zone.

- Use the Filter Builder button to create a filter with the following characteristics:

Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**not equal**
Value	**Internet**

- **Apply** the filter.
- Click **OK** to close the **Custom Report** window and to see a new entry in the list of custom reports.
- Open the custom report and use **Run Now** to see report information.

  Note that the report provides details for applications used by the Extranet and the Acquisition zones.

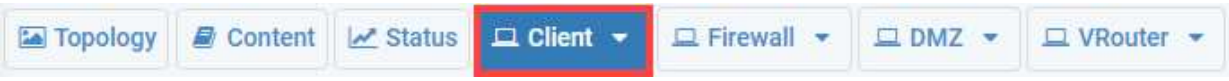
2 Locating Valuable Information Using Logs and Reports – Detailed Lab Steps

It is recommended to use this section if you prefer detailed guidance to complete the objectives for this lab. It is strongly recommended that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

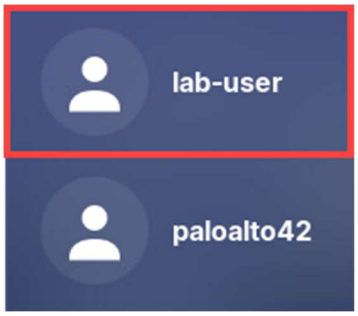
2.1 Apply a Baseline Configuration to the Firewall

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.



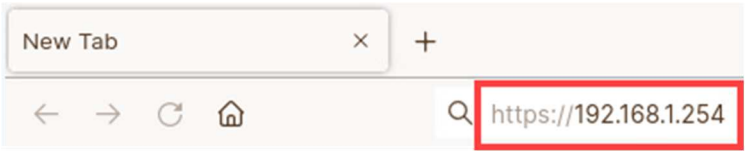
2. On the *Zorin* desktop, click **lab-user.**



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

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

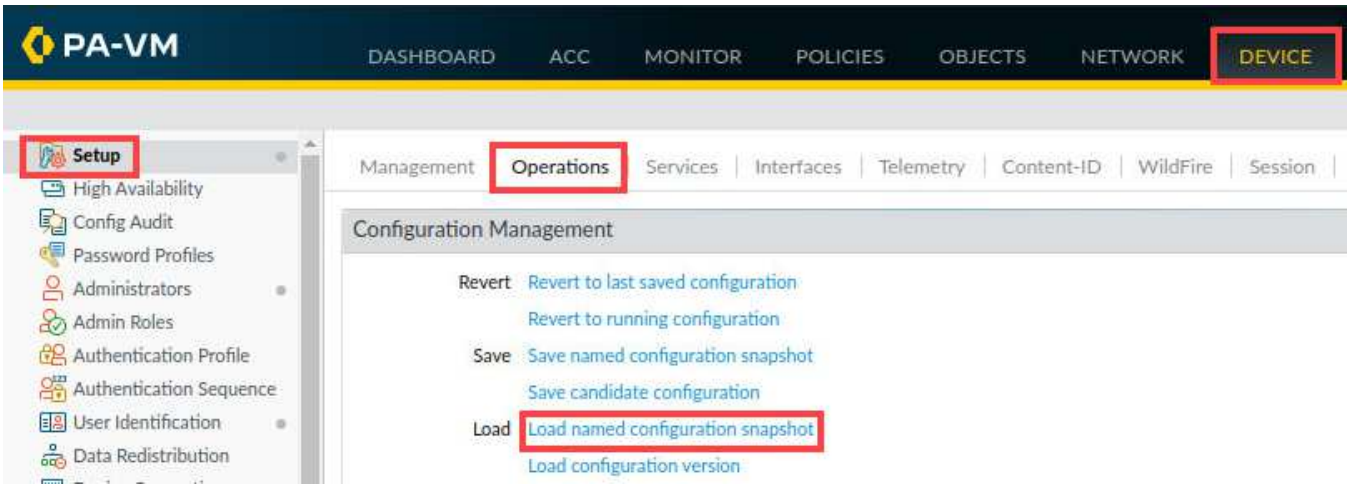
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



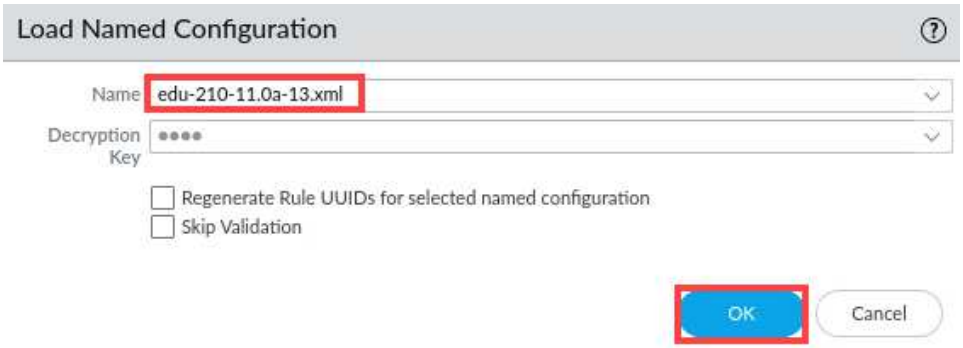
6. Log in to the Firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

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.

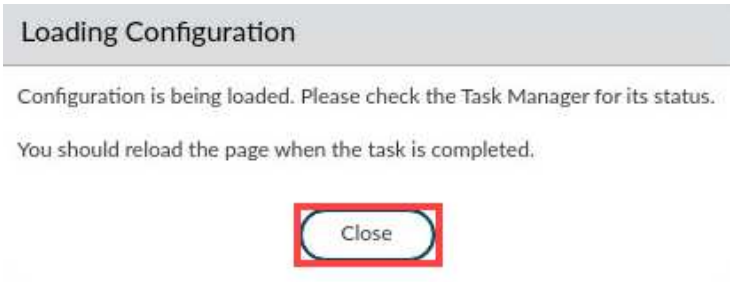
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



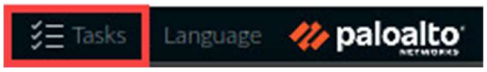
8. In the *Load Named Configuration* window, select **edu-210-11.0a-13.xml** from the *Name* drop-down box and click **OK**.



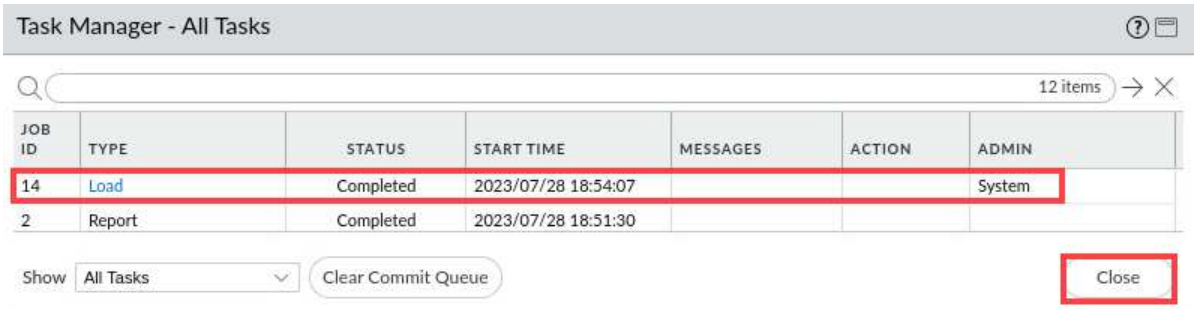
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

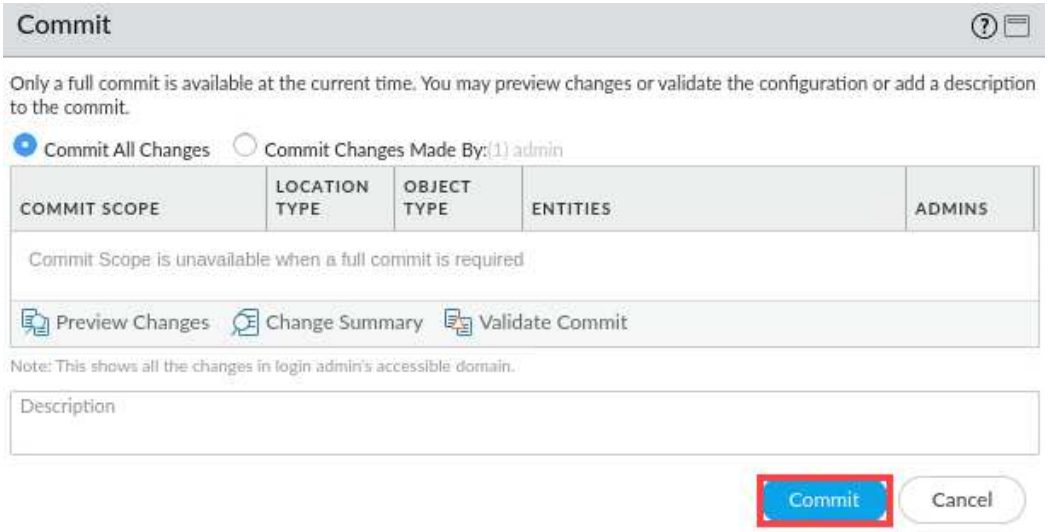


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

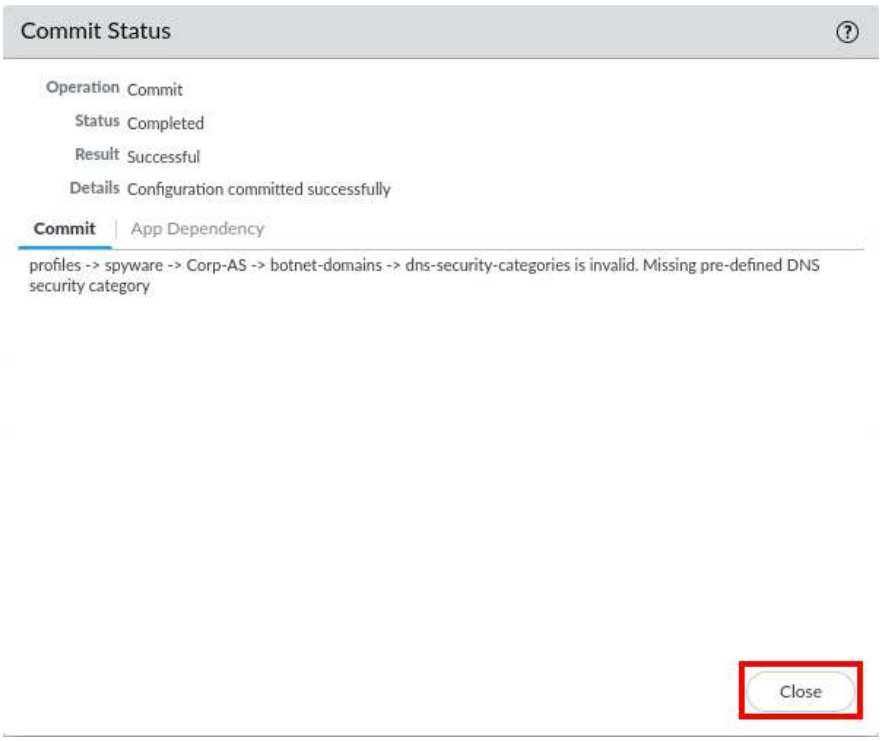


12. Click the **Commit** link located at the top-right of the web interface.

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* window open and continue to the next task.

2.2 Generate Traffic

In this section, you will generate simulated attacks, web browsing and application traffic to populate firewall logs.

1. On the client taskbar, open the **Remmina** application.

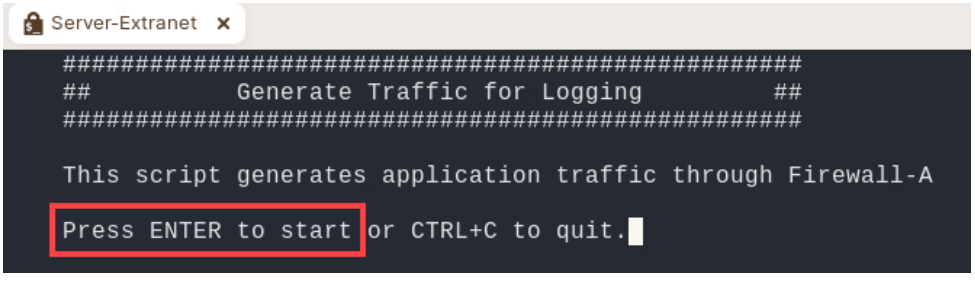
2. Double-click the entry for **Server-Extranet**.

> **Please Note** This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

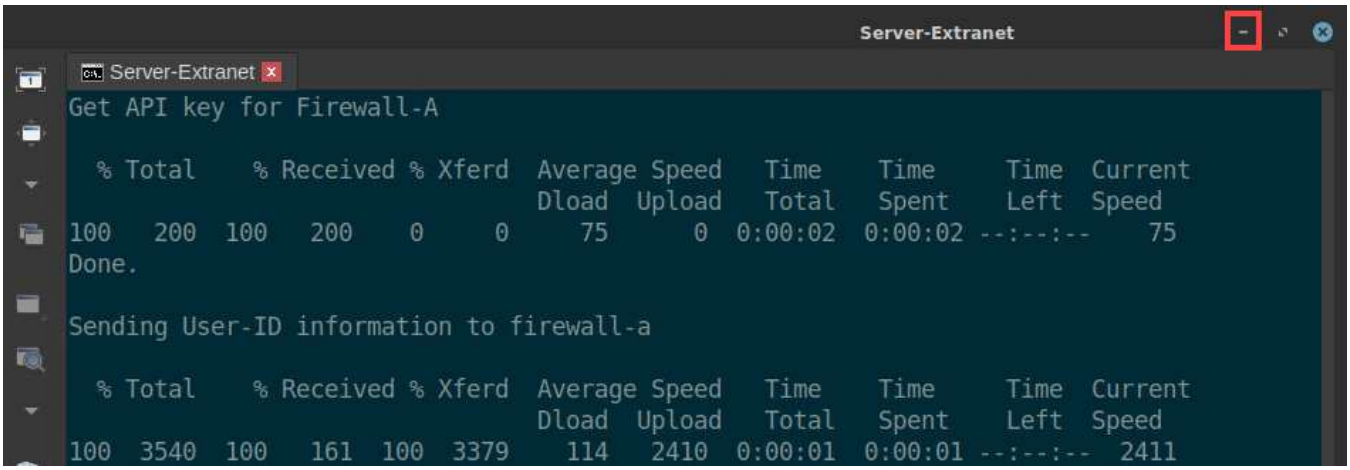
3. In the CLI connection enter the following command to generate traffic for logging.

```
paloalto42@extranet1:~$ ./UsingLogs-V1.sh <Enter>
```

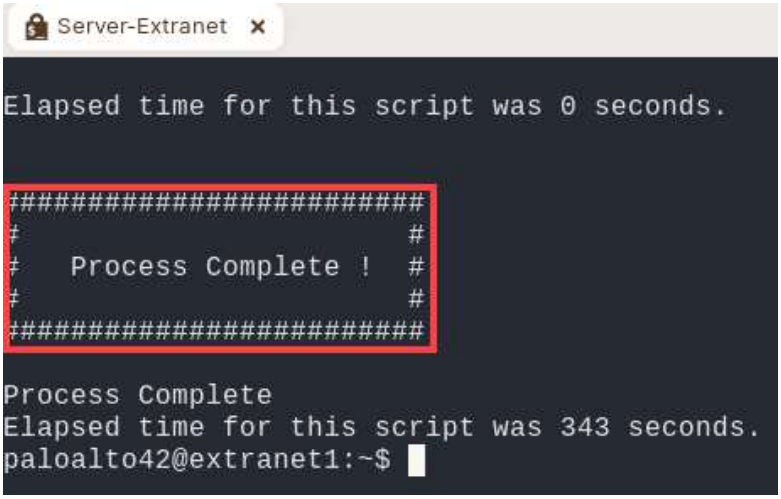
4. Press **Enter** to start the *UsingLogs-V1.sh* script.



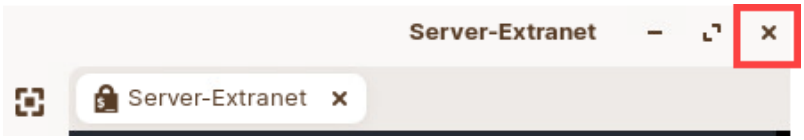
5. Allow 5 to 7 minutes for the script to run uninterrupted.



Do not continue until the **UsingLogs-V1** script completes.



6. Once complete, close the **Server-Extranet** window.

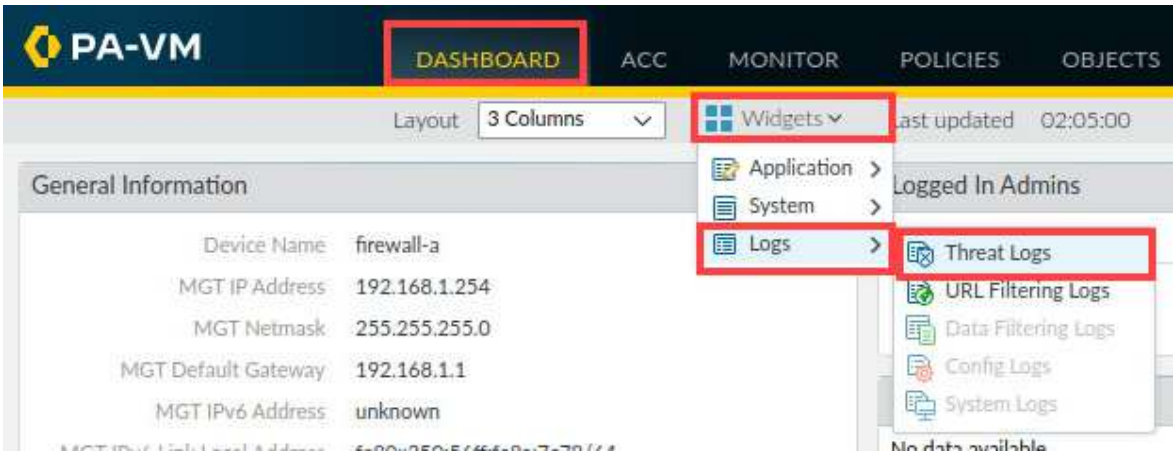


7. Close the **Remmina Remote Desktop Client** window and continue to the next task.

2.3 Display Recent Threat Information in the Dashboard

You will use the Dashboard to view threats detected by the firewall in the last hour. Because you can configure the Dashboard to periodically refresh, the displayed threats will change, depending on the most recent information available. The Dashboard information is sourced from the Threat, URL Filtering, and Data Filtering logs.

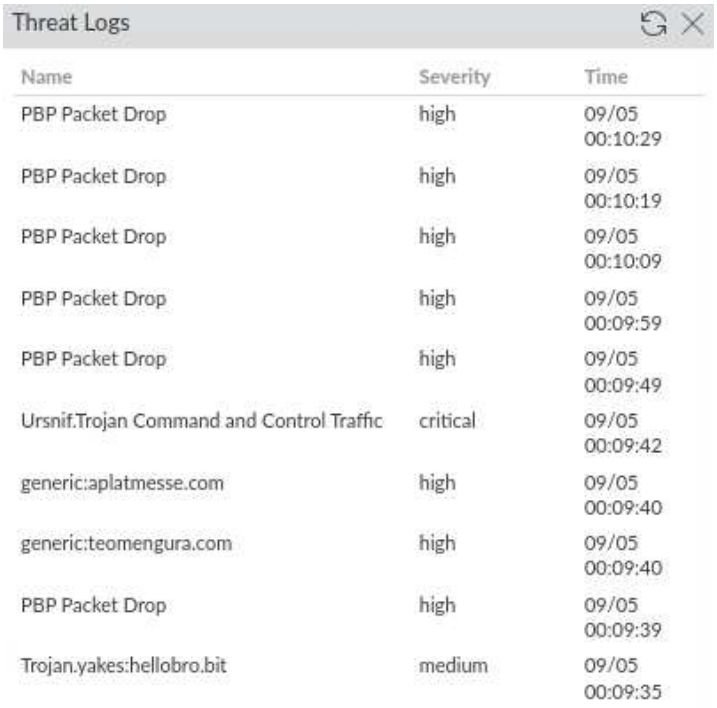
1. In the web interface, click the **Dashboard** tab**.** Click **Widgets** and select **Logs > Threat Logs.**



Please Note

Note that if Threat Logs is greyed out, it means that the widget is already displayed on the Dashboard.

2. The *Threat* Logs window will display the 10 most recent threats detected by the firewall in the last hour.

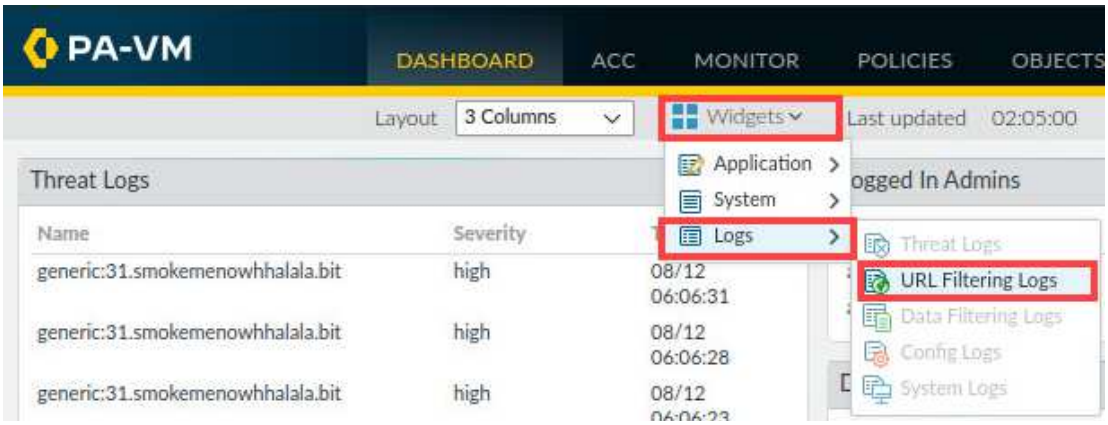


This widget is useful for viewing only the most recent threats detected by the firewall.

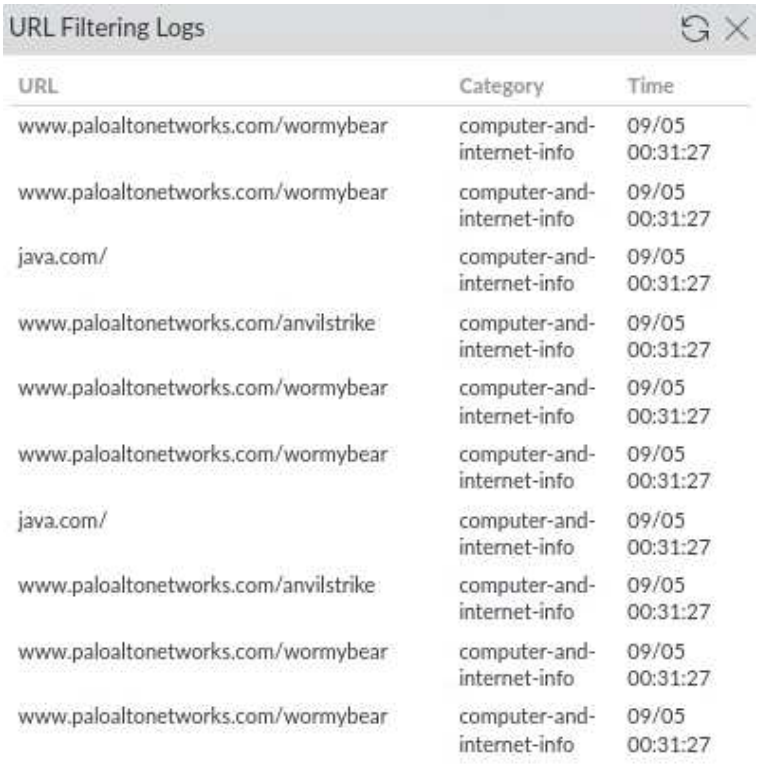
Q1. Are any threats displayed in the **Threats Logs** widget? It can display the 10 most recent threats detected by the firewall in the last hour.

a. Yes
b. No

3. Click **Widgets** and select **Logs > URL Filtering Logs**.



4. The *URL Filtering Logs* window will display the 10 most recent threats detected by the firewall in the last hour.



URL Filtering Logs

URL	Category	Time
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27
java.com/	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/anvilstrike	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27
java.com/	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/anvilstrike	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27
www.paloaltonetworks.com/wormybear	computer-and-internet-info	09/05 00:31:27

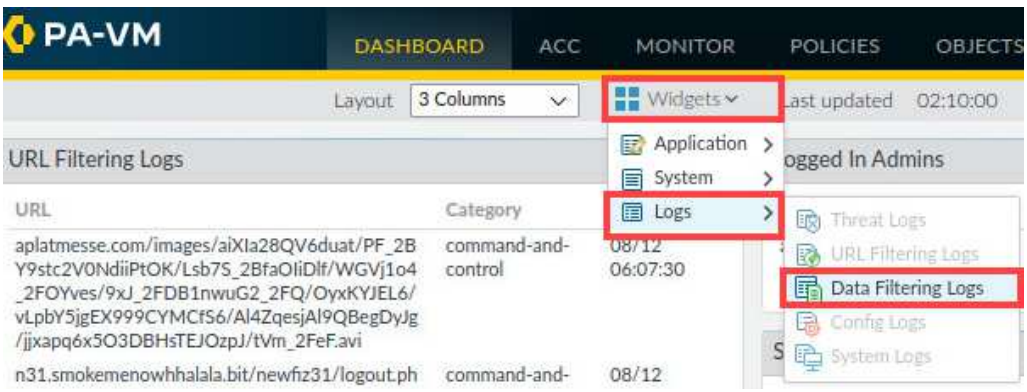
Please Note

This widget is useful for viewing only the most recent threats detected by the firewall.

Q2. Are any URLs displayed in the **URL Filtering Logs** widget? It can display the 10 most recent URLs seen by the firewall in the last hour.

a. Yes
b. No

5. Click **Widgets** and select **Logs > Data Filtering Logs** if it is not already selected.



Please Note

This widget is useful for viewing only the most recent threats detected by the firewall.

Q3. Are any files displayed in the **Data Logs** widget? It can display the 10 most recent files detected by the firewall in the last hour.

a. Yes
b. No

6. The *Data Logs* window will display the 10 most recent threats detected by the firewall in the last hour**.** For this step, you may or may not see the file entries in the *Data Logs* window. This is due to no activity being logged in the last hour in the *Data Logs*.

Data Logs

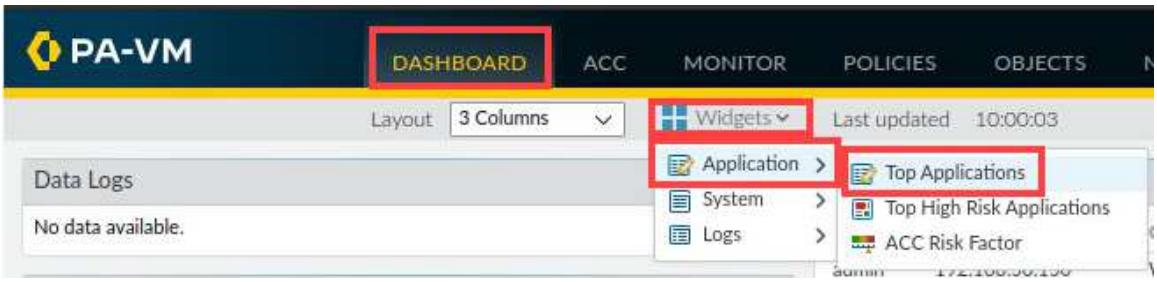
File Name	Name	Time
CSPCA.crl	Certificate Revocation List File	09/10 22:31:25
CSPCA.crl	DER Encoded X509 Certificate	09/10 22:31:25
CSPCA.crl	Certificate Revocation List File	09/10 22:31:25
CSPCA.crl	DER Encoded X509 Certificate	09/10 22:31:25
CSPCA.crl	Certificate Revocation List File	09/10 22:31:19
CSPCA.crl	DER Encoded X509 Certificate	09/10 22:31:19
CSPCA.crl	Certificate Revocation List File	09/10 22:31:19
CSPCA.crl	DER Encoded X509 Certificate	09/10 22:31:19
CSPCA.crl	Certificate Revocation List File	09/10 22:31:14
CSPCA.crl	DER Encoded X509 Certificate	09/10 22:31:14

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

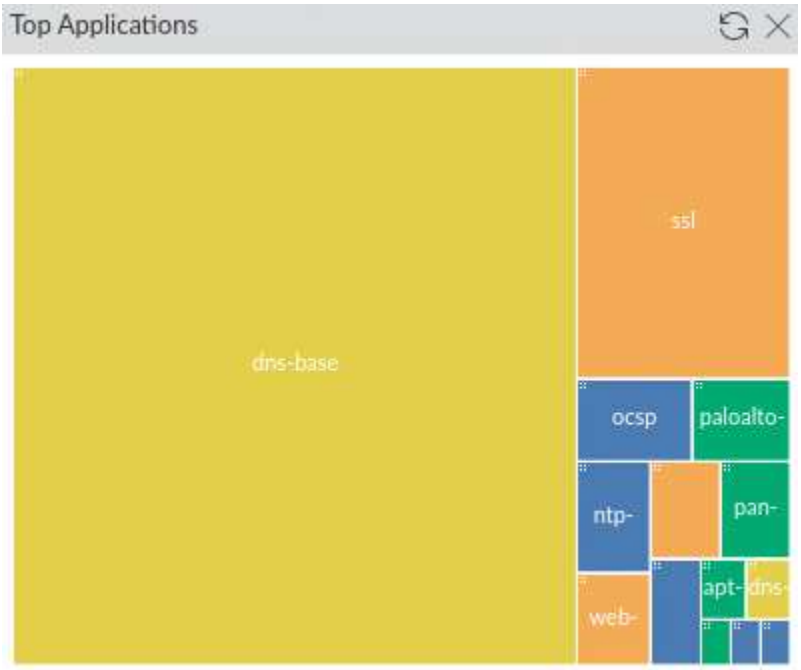
2.4 Display Recent Application Information in the Dashboard

In this section, you will display the Dashboard and view applications identified by the firewall in the last hour. Because you can configure the Dashboard to periodically refresh, the displayed applications will change depending on the most recent information available. You also will use the Dashboard to display those applications identified by the firewall in the last hour that have the most risk associated with them.

1. In the web interface, verify you are still located on the **Dashboard** tab. Click **Widgets** and select **Application > Top Applications.**



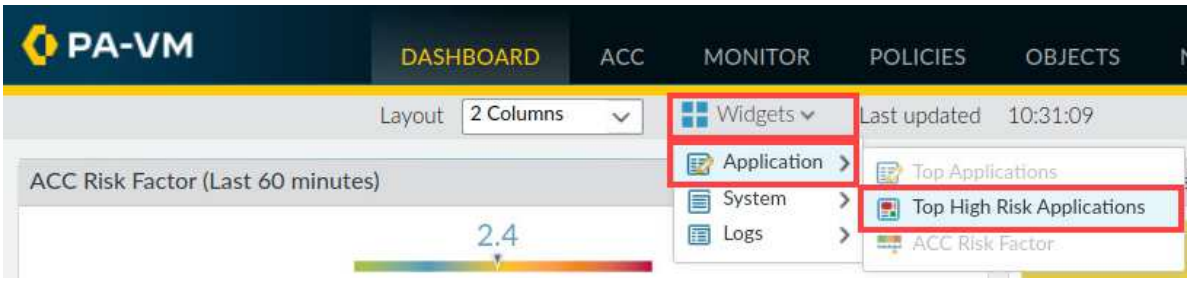
2. Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour. The screen shot below may differ than the actual lab environment.



Please Note

Some applications should be listed because some "housekeeping" traffic nearly always traverses the network, even in the lab environment. This widget is useful for viewing only the recent application traffic seen in the last hour by the firewall.

3. Click **Widgets** and select **Application** > **Top High Risk Applications**.



4. Notice the applications displayed in the **Top High Risk Applications** widget. It displays the high-risk applications seen by the firewall in the last hour. The screen shot below may differ than the actual lab environment.

Please Note

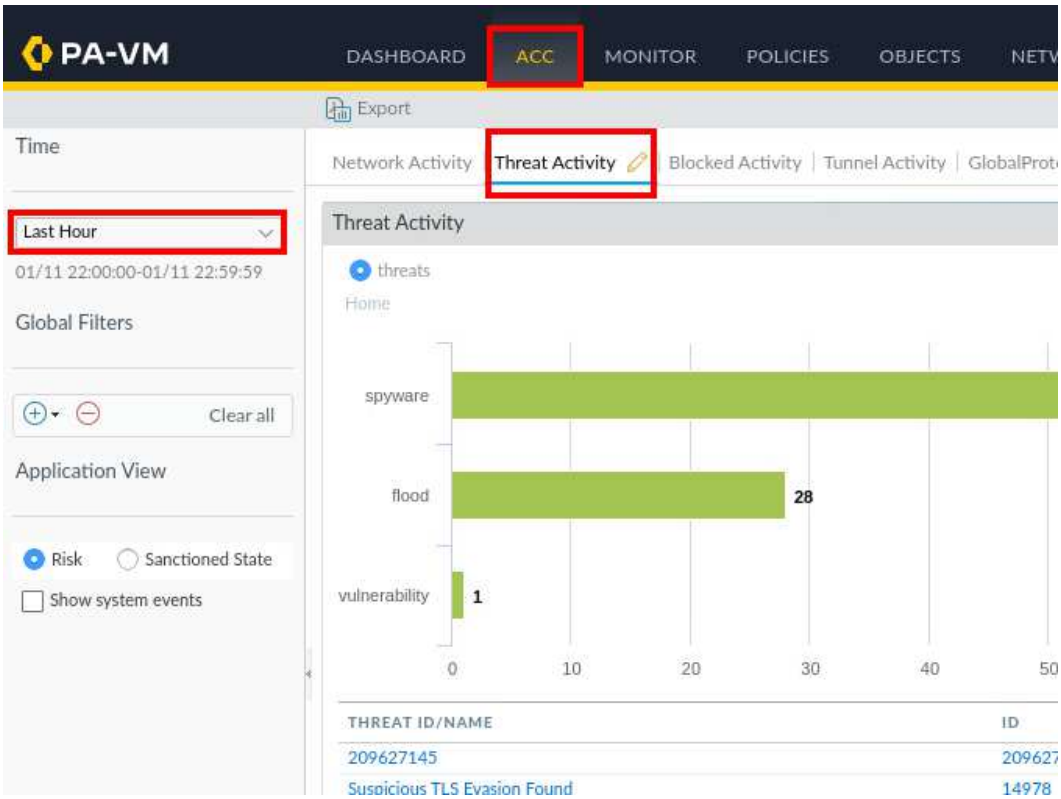
Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. If the Top High Risk and Top Applications have not updated, please allow 3 to 5 minutes for the widgets to update.

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

2.5 View Threat Information in the ACC

In this section, you will view a few ACC widgets on the Threat Activity tab to become familiar with widgets that display threats against your environment. Spend time examining each widget so that you can determine which information is presented that might be most useful to you back in your environment.

1. In the web interface, click the **ACC** tab. On the left side of the *ACC* page, look at **Global Filters** for any configured global filters. If there are filters, click **Clear all**. Change the Time to **Last Hour** and select the **Threat Activity** tab.



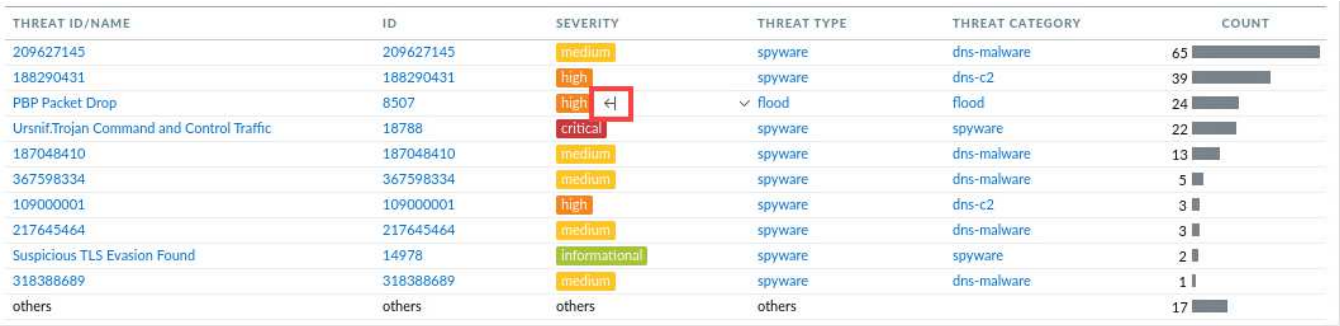
Q4. Do you see any threats listed in the **Threat Activity** widget?

a. No threats are listed.
b. Yes multiple threats are listed.

Please Note

You should see some combination of flood, scan, spyware, packet, vulnerability, and virus threats displayed in a graph. Next to each entry should be the number of occurrences of these threat types that the firewall has seen in the last seven days. More detail about the threats should be displayed in a table below the graph.

2. In the **Threat Activity** widget's table below the graph, hover the mouse over a **high** severity level item. You should see a small arrow appear to the side, click the **small arrow icon**. If you do not see any high severity level items, run the *UsingLogs-V1.sh* script once more.



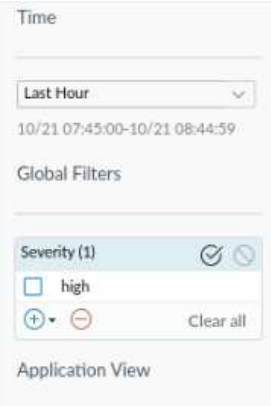
THREAT ID/NAME	ID	SEVERITY	THREAT TYPE	THREAT CATEGORY	COUNT
209627145	209627145	medium	spyware	dns-malware	65
188290431	188290431	high	spyware	dns-c2	39
PBP Packet Drop	8507	high	flood	flood	24
Ursnif.Trojan Command and Control Traffic	18788	critical	spyware	spyware	22
187048410	187048410	medium	spyware	dns-malware	13
367598334	367598334	medium	spyware	dns-malware	5
109000001	109000001	high	spyware	dns-c2	3
217645464	217645464	medium	spyware	dns-malware	3
Suspicious TLS Evasion Found	14978	informational	spyware	spyware	2
318388689	318388689	medium	spyware	dns-malware	1
others	others	others	others		17

Q5. Did the widget's table change to display only threats that have a **high** severity level?

a. Yes, the widget should have changed to display only high severity level threats.
b. No, the widget should not have changed to display only critical severity level threats.
c. Yes, the widget should have changed to display only critical severity level threats.
d. No, the widget should not have changed to display only high severity level threats.

Based on the Severity level you choose, this action adds the severity level as a Global filter for the ACC. Global filters are applied to every widget on the ACC. Global filters are useful for quickly pivoting your search on a specific piece of information, thus causing all widgets to display only information that is relevant to a specific object or threat.

3. Find the global filter on the left side of the **ACC** window.



Q6. Is the high severity listed in the Global Filter condition box?

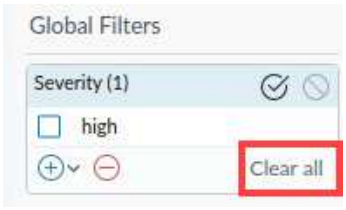
a. No the critical severity is listed.
b. Yes the high severity is listed.
c. No the low severity is listed.
d. Yes the medium severity is listed.

4. Note that the Threat Activity graph and the table of Threat Names are updated to reflect only items with a Severity level of **high**.

THREAT ID/NAME	ID	SEVERITY	THREAT TYPE	THREAT CATEGORY	COUNT
188290431	188290431	high	spyware	dns-c2	39
PBP Packet Drop	8507	high	flood	flood	24
109000001	109000001	high	spyware	dns-c2	3
217501578	217501578	high	spyware	dns-c2	1
187533357	187533357	high	spyware	dns-c2	1
217500861	217500861	high	spyware	dns-c2	1

Please Note The entries you see will differ from the examples shown here.

5. In the *Global Filters* area, click **Clear all** to remove the global filter.



Please Note The global filter should be removed, and all widgets should be refreshed to include all threats detected in the last seven days.

Q7. On the **Threat Activity** tab, scroll through the widgets. Which widgets would you use to see which hosts have either visited or resolved a malicious DNS domain? Make a guess based on the widget names. (Choose all that apply)

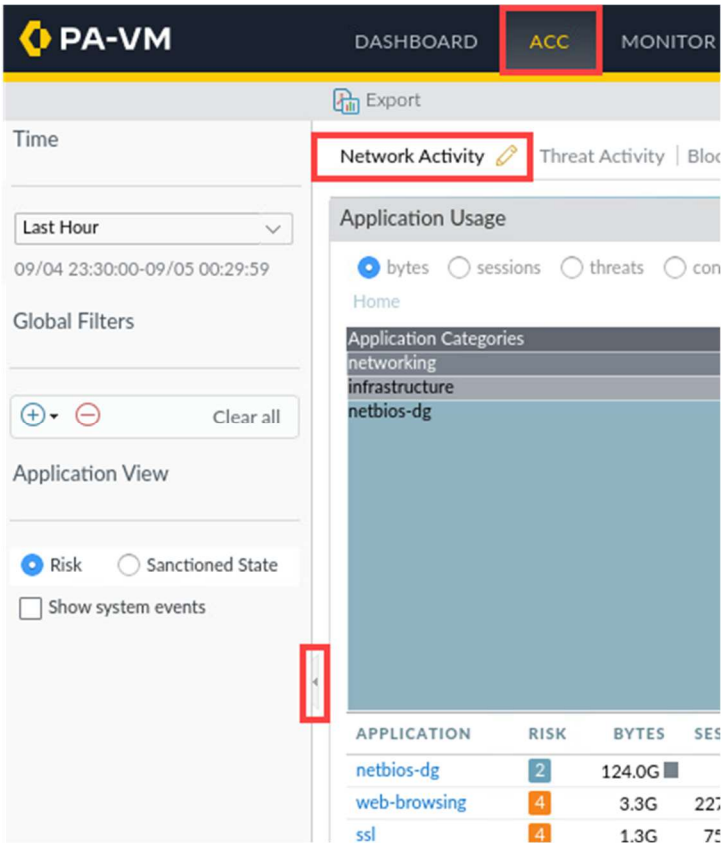
a. Hosts Visiting Malicious URLs
b. Rules Allowing Apps on Non-Standard Ports
c. Content Activity
d. Hosts Resolving Malicious Domains

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

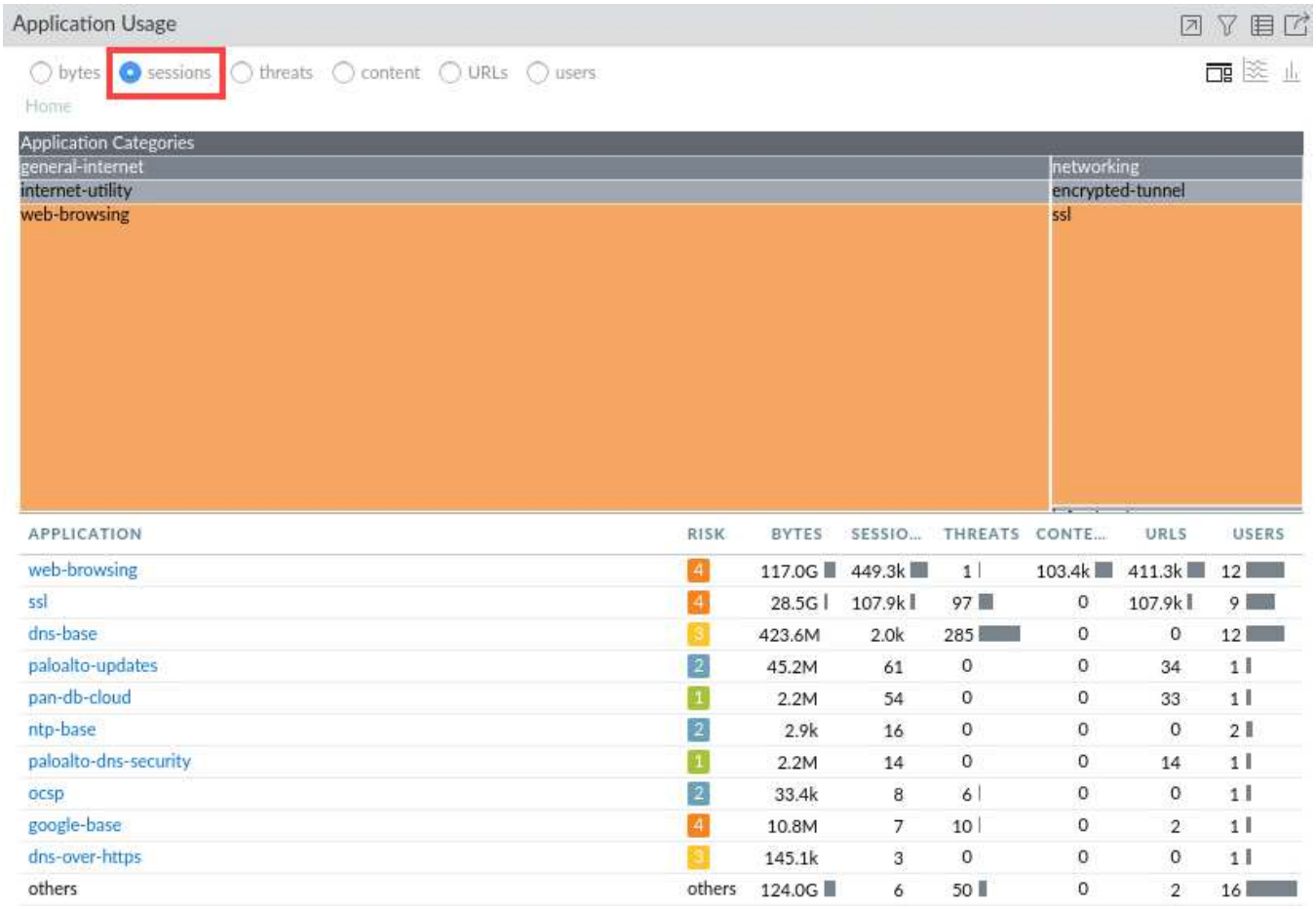
2.6 View Application Information in the ACC

In this section, you will view two widgets on the Network Activity tab. The goal is for you to gain familiarity with some of the widgets available for viewing application and traffic information.

1. In the web interface, click the **ACC** tab and then the **Network Activity** tab. Hide the sidebar to make more room for the widgets by clicking the very small arrow shown.



2. The top section of the **Application Usage** widget is a graph that illustrates how much traffic a specific application represents. Select the **sessions** radio button.

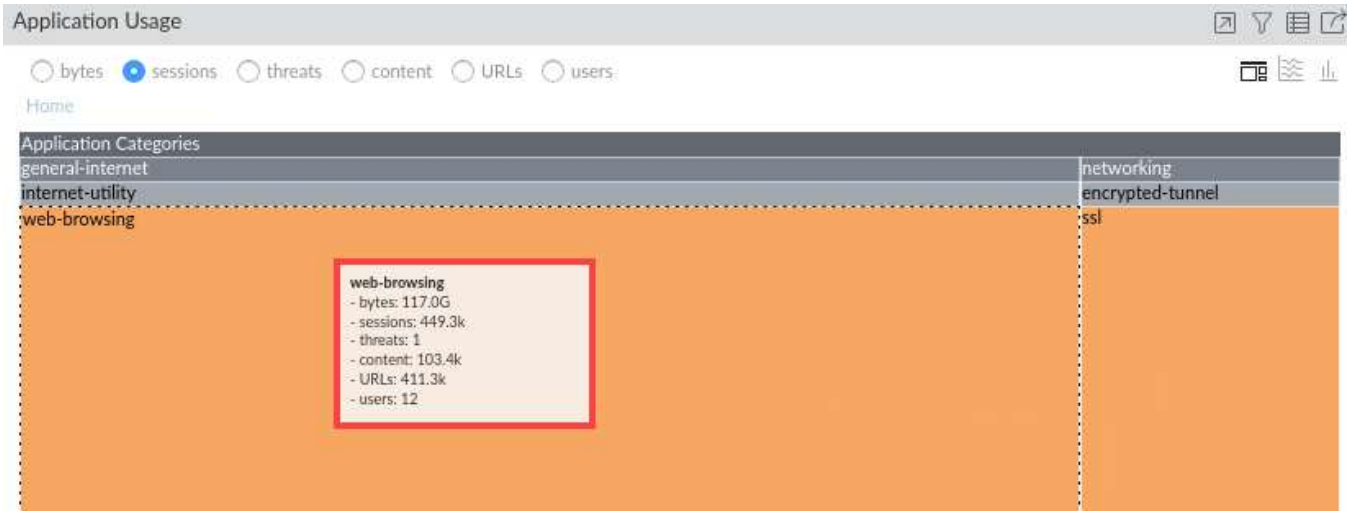


APPLICATION	RISK	BYTES	SESSIO...	THREATS	CONTE...	URLS	USERS
web-browsing	4	117.0G	449.3k	1	103.4k	411.3k	12
ssl	4	28.5G	107.9k	97	0	107.9k	9
dns-base	3	423.6M	2.0k	285	0	0	12
paloalto-updates	2	45.2M	61	0	0	34	1
pan-db-cloud	1	2.2M	54	0	0	33	1
ntp-base	2	2.9k	16	0	0	0	2
paloalto-dns-security	1	2.2M	14	0	0	14	1
ocsp	2	33.4k	8	6	0	0	1
google-base	4	10.8M	7	10	0	2	1
dns-over-https	3	145.1k	3	0	0	0	1
others	others	124.0G	6	50	0	2	16

Please Note

Think of this as a sort of square pie-chart. The entries you see will differ from the examples shown here.

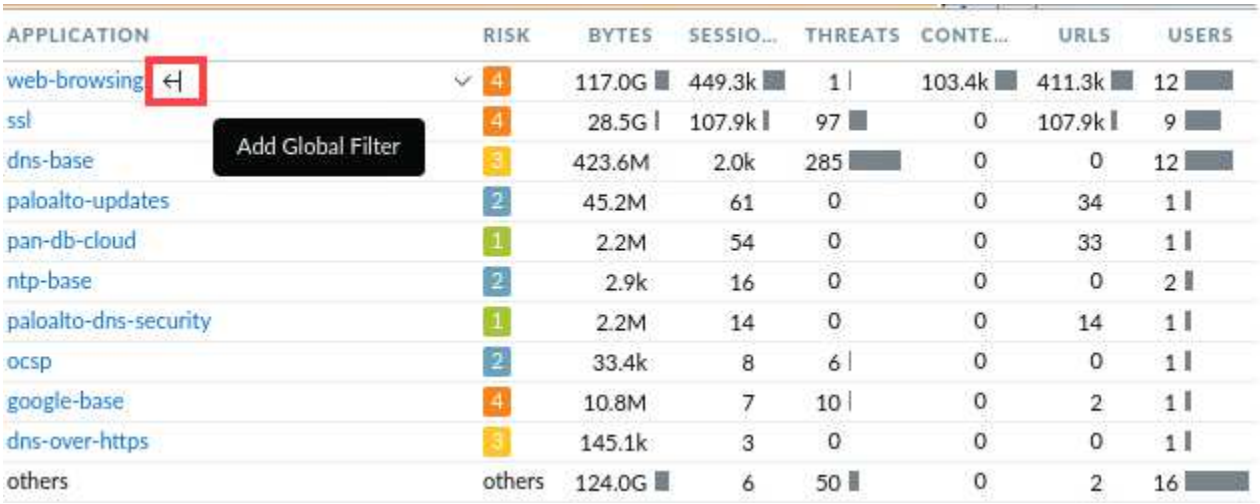
3. Hover your pointer over the section for **web-browsing**. This action displays a summary window with information about that application.



Please Note

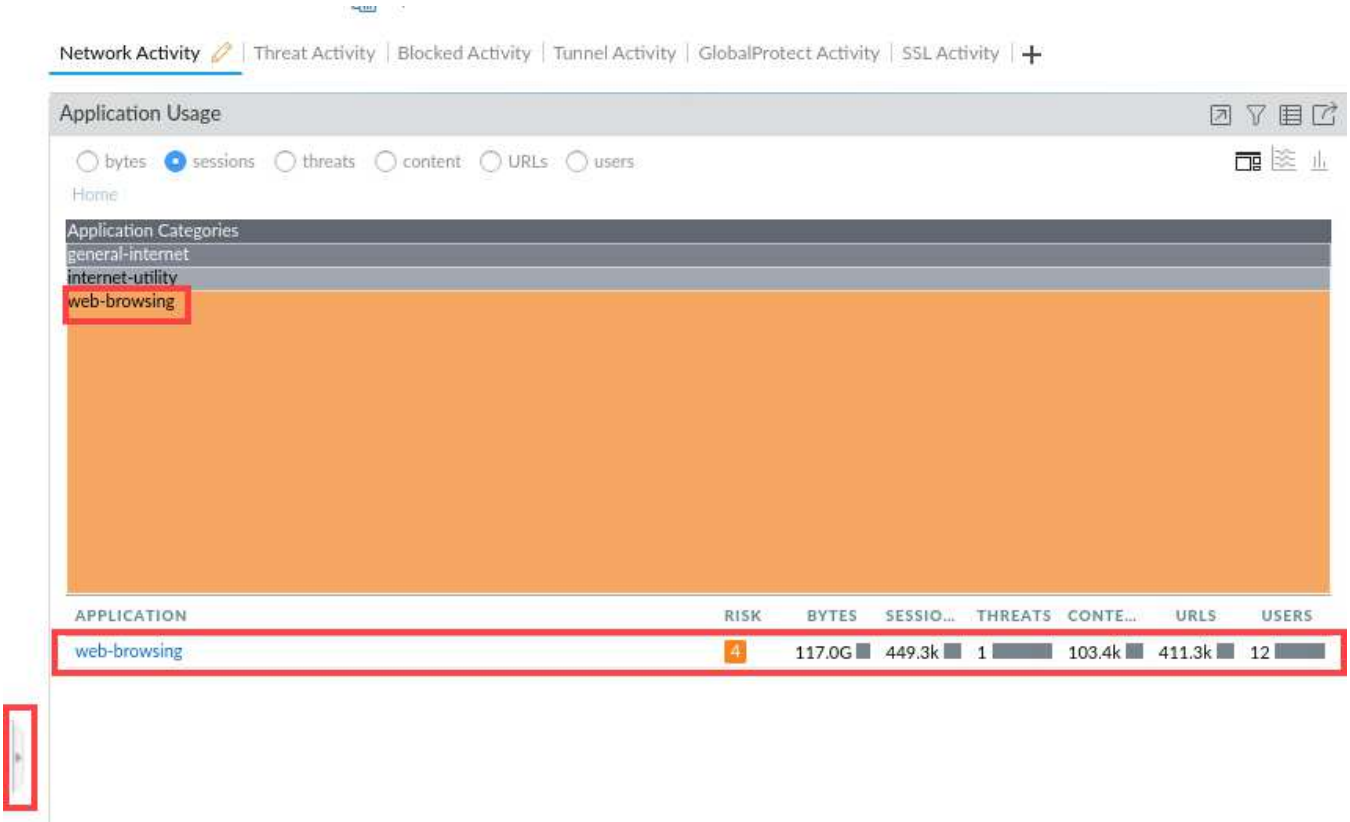
This action displays a summary window with information about that application. The information you see will differ from the examples shown here.

4. In the table below the graph, hover your pointer over the **web-browsing** application until the global filter **Left arrow** appears. Then click the **Left arrow** to promote the **web-browsing** application to a global filter.

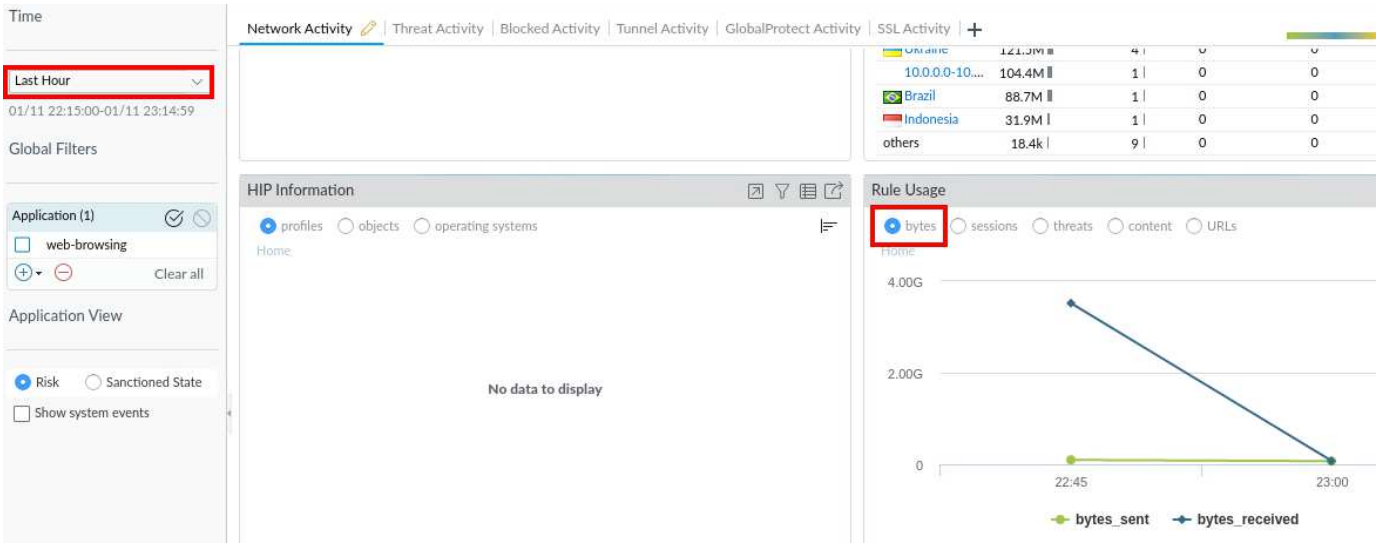


APPLICATION	RISK	BYTES	SESSIO...	THREATS	CONTE...	URLS	USERS
web-browsing	4	117.0G	449.3k	1	103.4k	411.3k	12
ssl	4	28.5G	107.9k	97	0	107.9k	9
dns-base	3	423.6M	2.0k	285	0	0	12
paloalto-updates	2	45.2M	61	0	0	34	1
pan-db-cloud	1	2.2M	54	0	0	33	1
ntp-base	2	2.9k	16	0	0	0	2
paloalto-dns-security	1	2.2M	14	0	0	14	1
ocsp	2	33.4k	8	6	0	0	1
google-base	4	10.8M	7	10	0	2	1
dns-over-https	3	145.1k	3	0	0	0	1
others	others	124.0G	6	50	0	2	16

5. Unhide the sidebar by clicking the *tiny* arrow again**.** Notice the *Application Usage* chart has been upgraded to show the **web-browsing** application.



6. Scroll down in the **Network Activity** tab until you reach the **Rule Usage** widget**.** Select the radio button at the top for **bytes.** In the *Time* column, make sure **Last Hour** is selected.

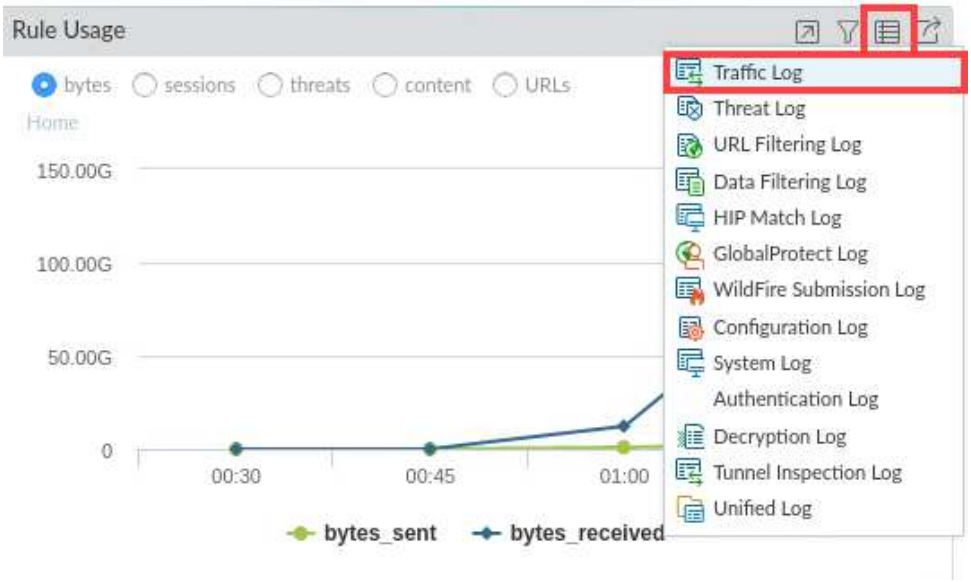


Q8. Which Security Policy rules have allowed web-browsing traffic?

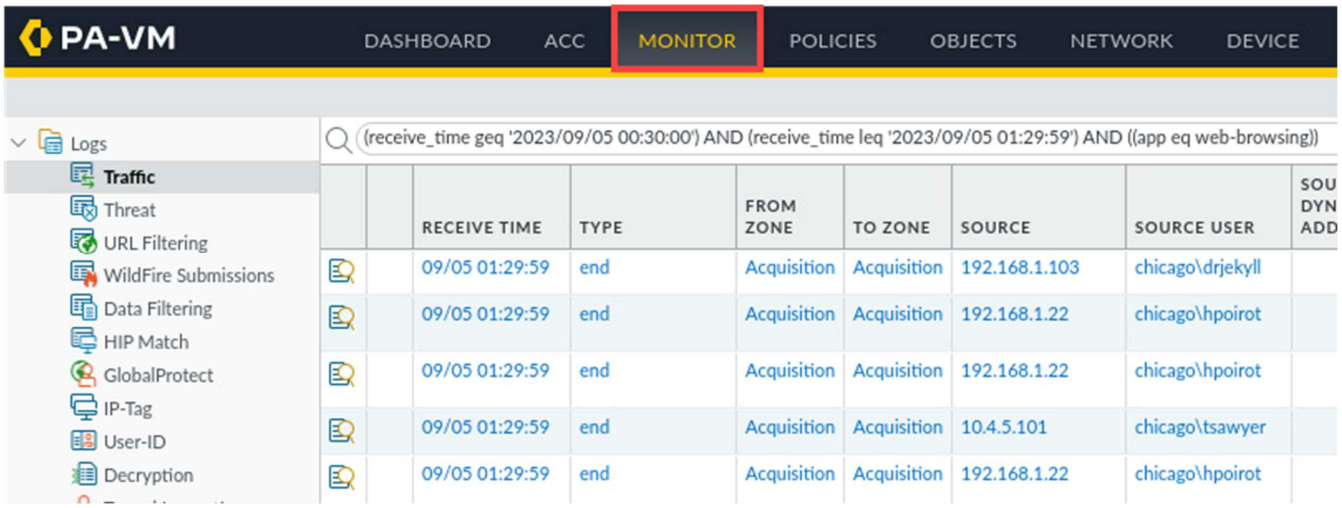
a. Allow-Corp-Apps
b. Users_to_Internet

c. Users_to_DMZ
d. Users_to_Extranet

7. In the upper right corner of the **Rule Usage** widget, click the **Jump to Logs** button and select **Traffic Log** icon to open the logs menu.



8. Notice the Logs it navigated you to on the **Monitor** tab. Note that the entries displayed in the Traffic log match the filter.



Q9. Which log is displayed in the web interface?

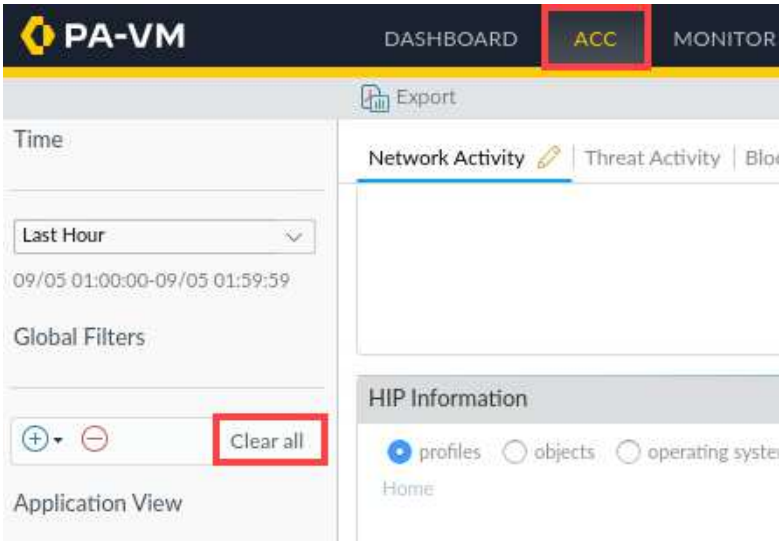
a. Traffic
b. Threat
c. User-ID
d. URL Filtering

Q10. Which log filters have been applied automatically to the Traffic log? (Choose all that apply)

a. Range filter
b. Application filter
c. Device filter
d. Port filter

9. Clear the filter in the Traffic log.

10. Click the **ACC** tab. In the *Global Filters* area, click **Clear all** to remove the global filter.

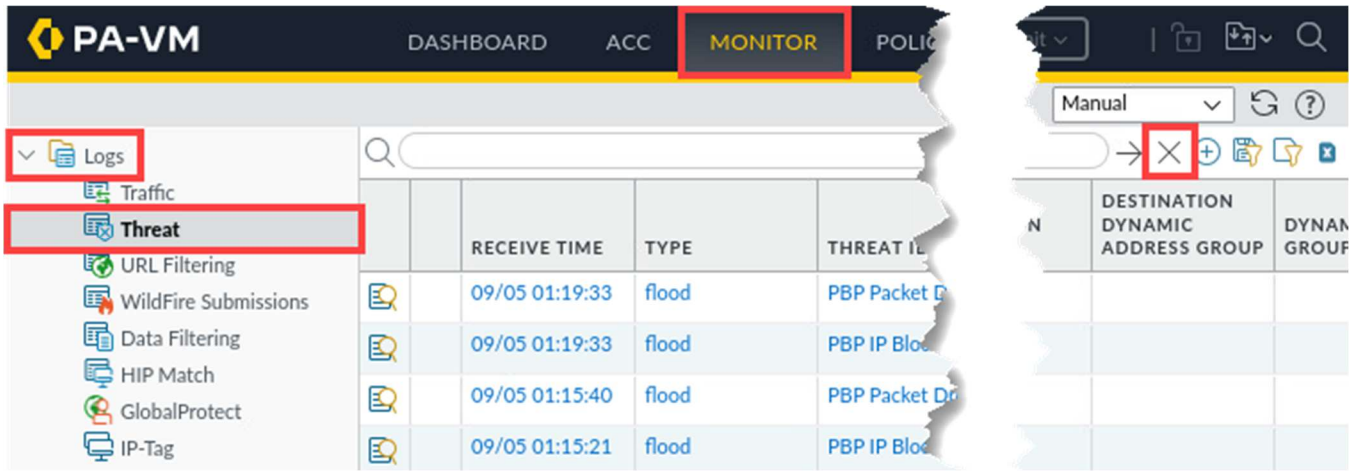


11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

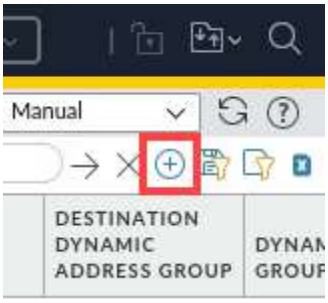
2.7 View Threat Information in the Threat Log

In this section, you will apply different filters to the Threat log. You will use the filters to determine whether all critical-severity and high-severity threats detected by the firewall have been blocked. You also will use a log filter to determine which threats have been detected that come from a specific security zone.

1. Select **Monitor > Logs > Threat.** In the upper right corner of the window, click the **X** icon in the filter area to remove any existing log filter.

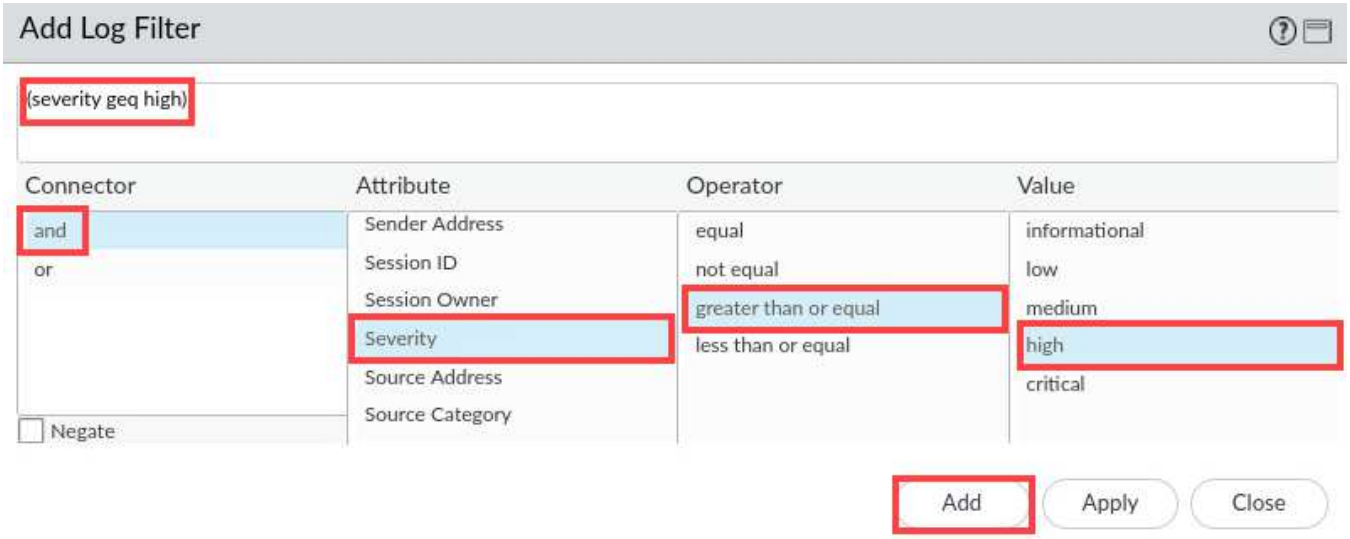


2. Click the **+** icon in the filter area to open the **Add Log Filter** window.



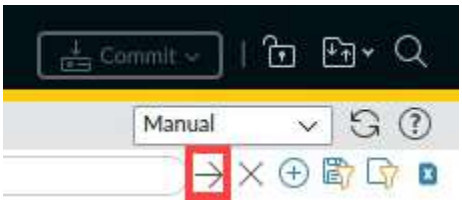
3. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Severity**
Operator	**greater than or equal**
Value	**high**



4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

5. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



Q11. Is the Threat log filtered to display only threats of high severity or greater?

a. True
b. False

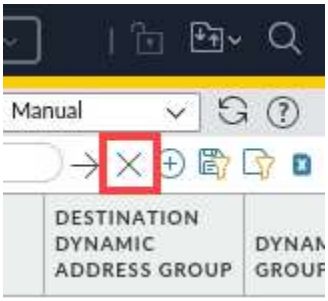
6. Notice the threat log has been filtered to display only threats of high severity or greater. Some columns have been adjusted to reflect the *Severity* column.

(severity geq high)

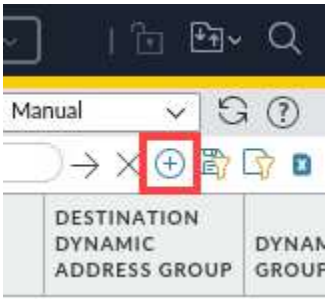
		RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SEVERITY
		09/05 01:19:33	flood	PBP Packet Drop	Acquisition		10.11.2.102	chicago\escrooge	high
		09/05 01:19:33	flood	PBP IP Blocked	Acquisition		10.11.2.102	chicago\escrooge	high
		09/05 01:15:40	flood	PBP Packet Drop	Acquisition		10.9.3.101	chicago\aoakley	high
		09/05 01:15:21	flood	PBP IP Blocked	Acquisition		10.10.17.1		high
		09/05 01:15:18	flood	PBP Packet Drop	Acquisition		10.4.5.101	chicago\tsawyer	high

Please Note Note that several columns have been hidden or rearranged in the example shown here. The entries you see will differ from the ones shown here.

7. Click the **X** icon in the filter area to remove any existing log filter.

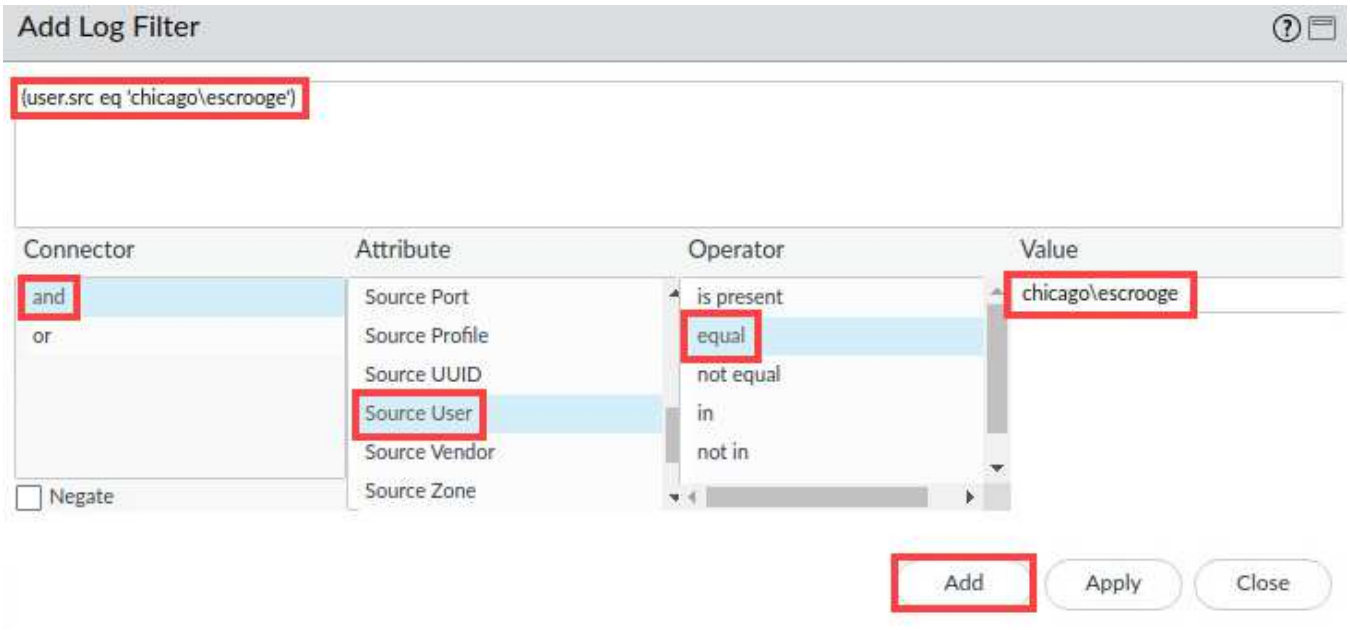


8. Click the **+** icon in the filter area to re-open the **Add Log Filter** window.



9. In the *Add Log Filter* window, select the following. Click **Add**.

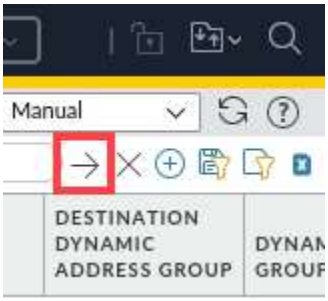
Parameter	Value
Connector	**and**
Attribute	**Source User**
Operator	**equal**
Value	**chicago\escrooge**



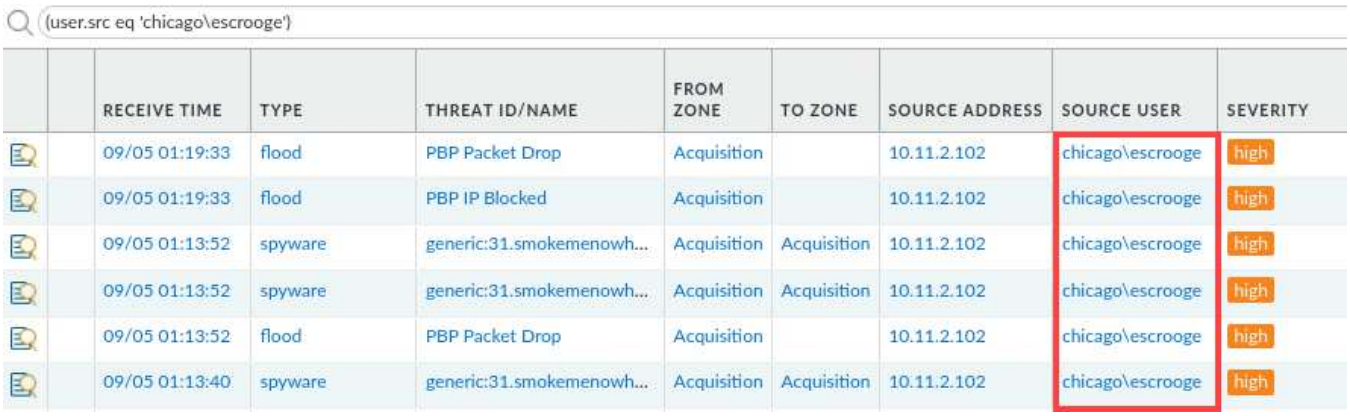
Please Note This configuration filters the log to display threats coming from only this user.

10. In the *Add Log Filter* window, click **Apply**.

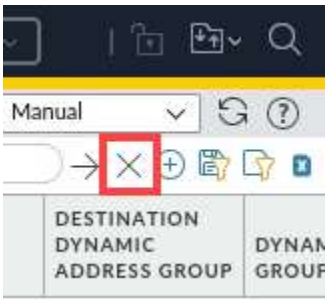
11. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



12. Notice the threat log has been filtered to display only threats from the Source User **chicago\escrooge**.



13. Click the **X** icon to clear the filter from the log filter text box.



Please Note URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

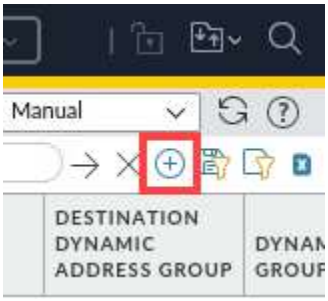
14. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.8 View Application Information in the Traffic Log

In this section, you will apply different filters to the Traffic log. You will use a filter to determine which applications are being seen in a specific zone.

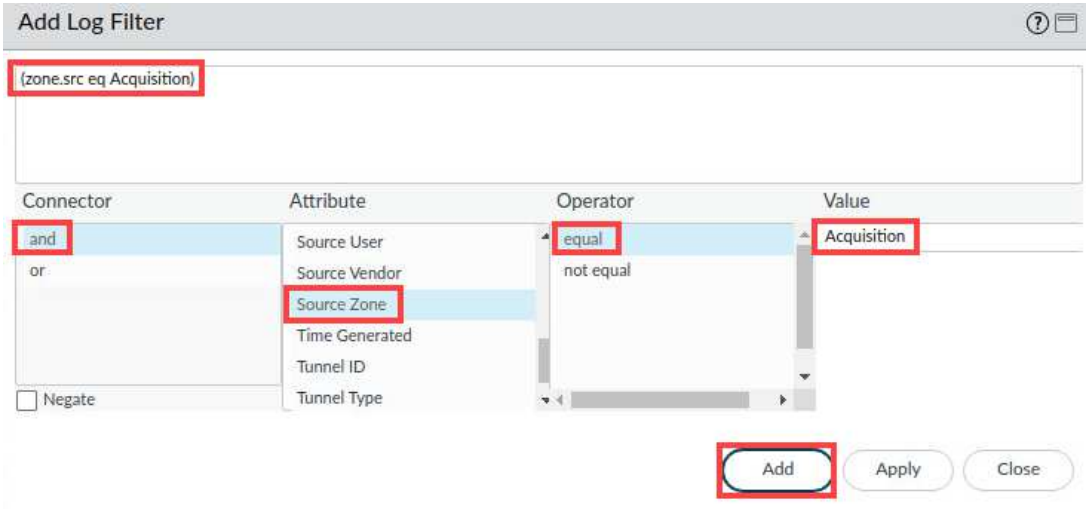
1. Select **Monitor > Logs > Traffic.** Click the **X** icon in the filter area to remove any existing log filter.

2. Click the **+** icon in the filter area to open the **Add Log Filter** window.



3. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**equal**
Value	**Acquisition**

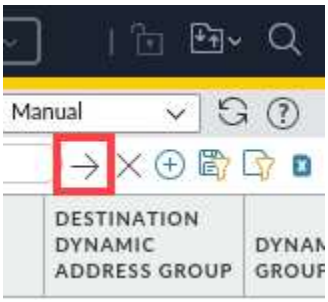


Please Note

This configuration filters the log to display only application traffic that is sourced from the Acquisition zone. You could use this information, for example, to help you to determine how to configure your Security policy rules. You easily could modify the filter to display application traffic sourced from any zone and use that information to help you improve your Security policy configuration.

4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.

5. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



Q12. Has the Traffic log been filtered to display only traffic sourced from the Acquisition zone?

a. True

b. False

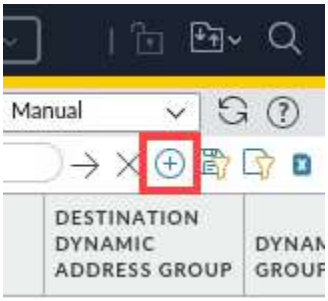
6. Notice the traffic log has been filtered to display only threats from the *From Zone* **Acquisition**. Some columns have been adjusted to reflect the *Severity* column.

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER
		09/05 02:21:10	end	Acquisition	Acquisition	10.10.17.102	chicago\wearp
		09/05 02:21:10	end	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot
		09/05 02:21:10	end	Acquisition	Acquisition	10.4.5.101	chicago\tsawyer
		09/05 02:21:10	end	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot
		09/05 02:21:10	end	Acquisition	Acquisition	10.4.5.101	chicago\tsawyer

Please Note

You could use this information to help you determine the Security policy rules required to control legitimate traffic sourced from devices in the dmz zone.

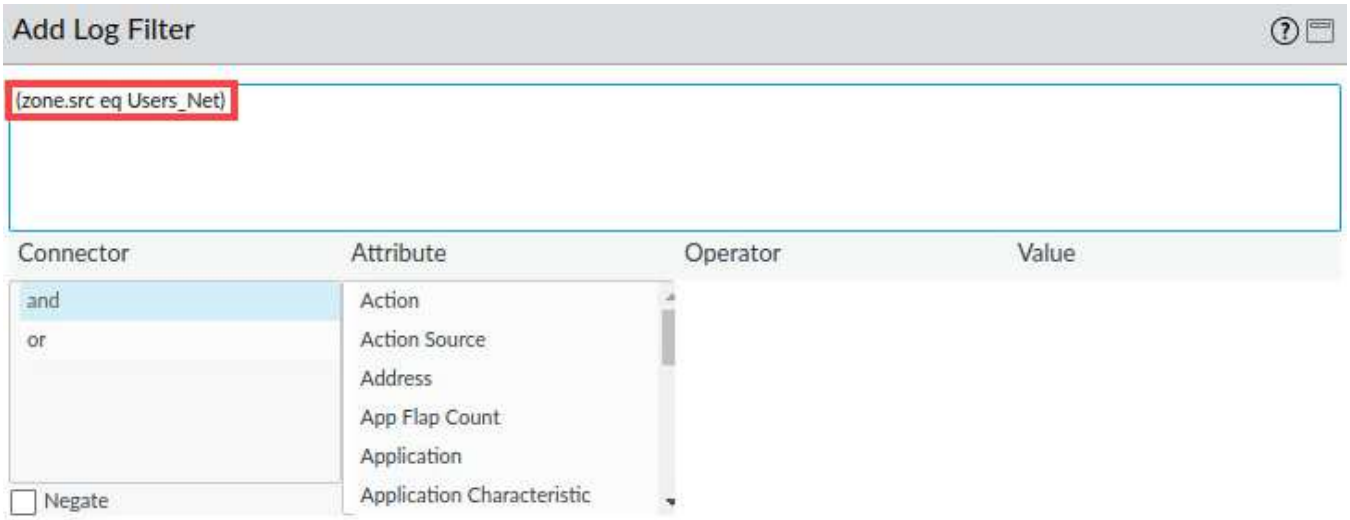
7. Click the **+** icon in the filter area to open the *Add Log Filter* window again.



Please Note

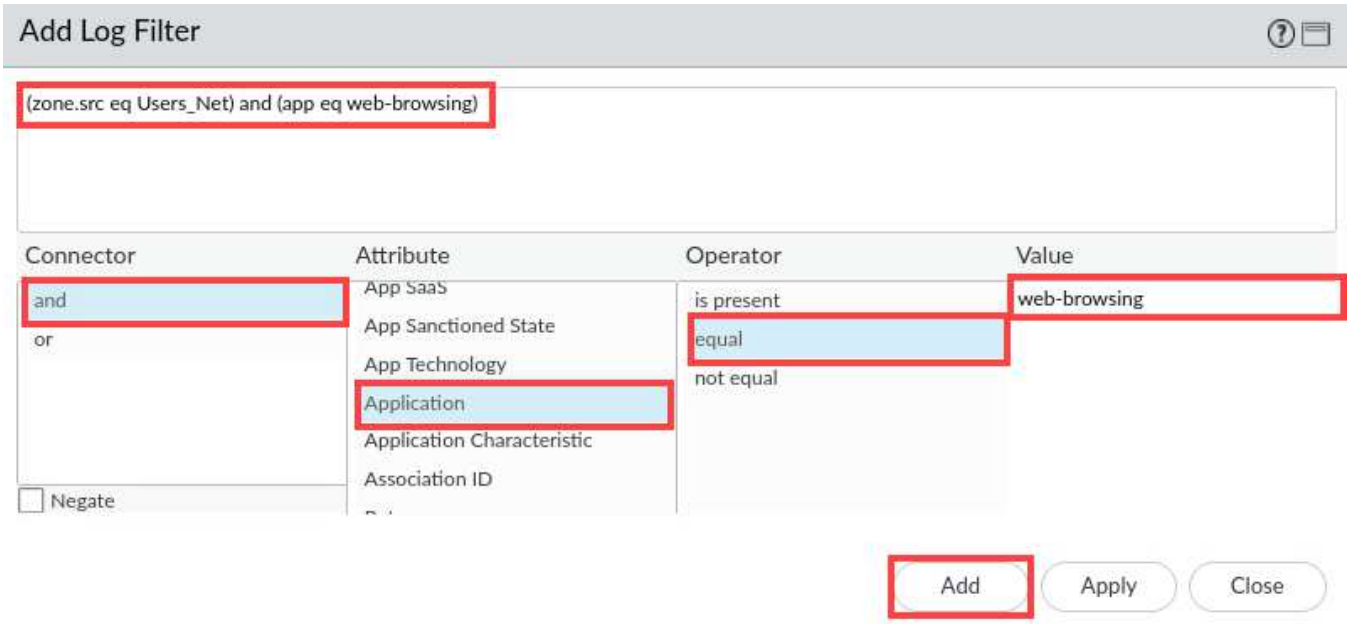
The Acquisition source zone filter still should appear in the open **Add Log Filter** window.

8. In the *Add Log Filter* window in the top pane, modify the existing source zone filter to filter on the *Users_Net* zone instead of the *Acquisition* zone. The completed filter should read **`(zone.src eq Users_Net)`**.



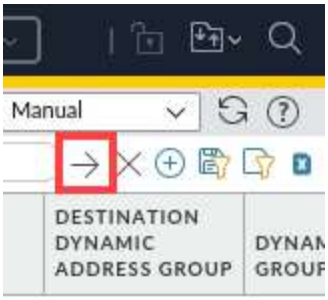
9. In the *Add Log Filter* window, select the following. Click **Add**. It should add the additional filter.

Parameter	Value
Connector	**and**
Attribute	**Application**
Operator	**equal**
Value	**web-browsing**



10. In the *Add Log Filter* window, click **Apply**.

11. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



Q13. Has the Traffic log been filtered to display only web-browsing traffic sourced from the Users_Net zone?

a. True

b. False

12. Notice the traffic log has been filtered to display only threats from the *From Zone* **Users_Net** and the *Application* **web-browsing**. Some columns have been adjusted to reflect the *Application* column.

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DYNAMIC USER GROUP	APPLICATION
		09/05 02:28:32	end	Users_Net	Internet	192.168.1.20		web-browsing
		09/05 02:28:31	end	Users_Net	Internet	192.168.1.20		web-browsing
		09/05 02:27:29	end	Users_Net	Extranet	192.168.1.254		web-browsing
		09/05 02:26:53	end	Users_Net	Internet	192.168.1.20		web-browsing

Please Note

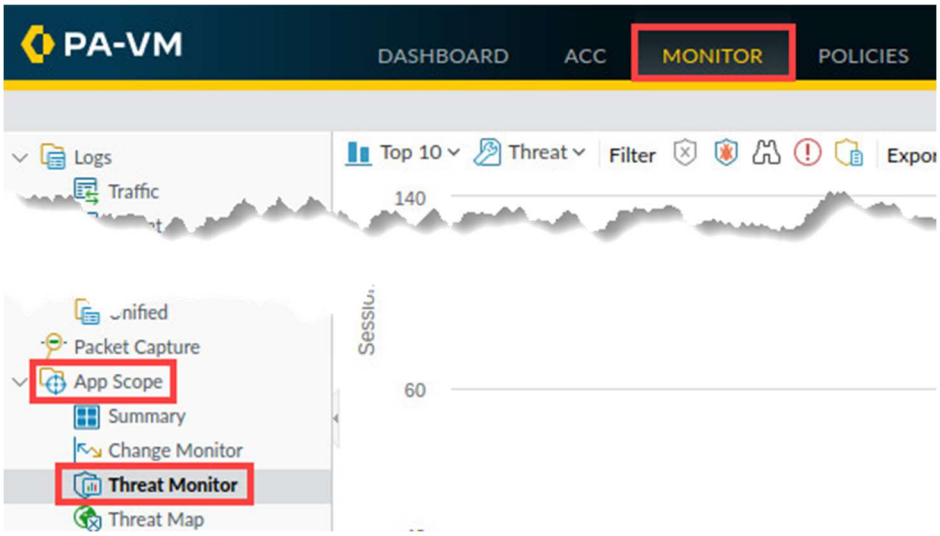
Note that several columns have been hidden or rearranged in the example shown here.

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

2.9 View Threats Using App Scope Reports

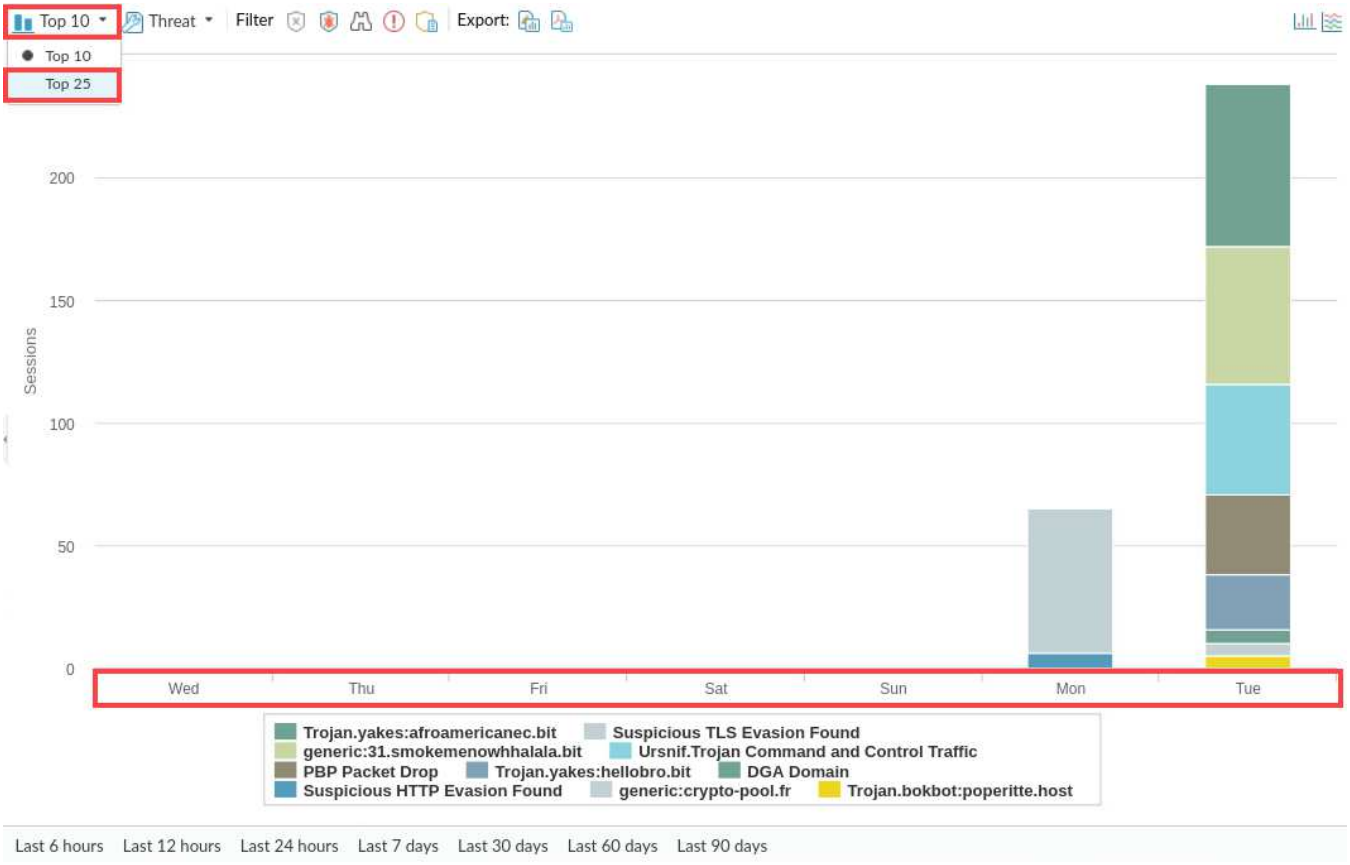
In this section, you will view threat information using App Scope's Threat Monitor and Threat Map reports.

1. Select **Monitor > App Scope > Threat Monitor**.



2. At the bottom of the window, click **Last 7 days**.

3. The window should be updated to display the *top 10 threats* detected by the firewall in the last seven days. At the top of the window, click **Top 10** and select **Top 25** from the menu.



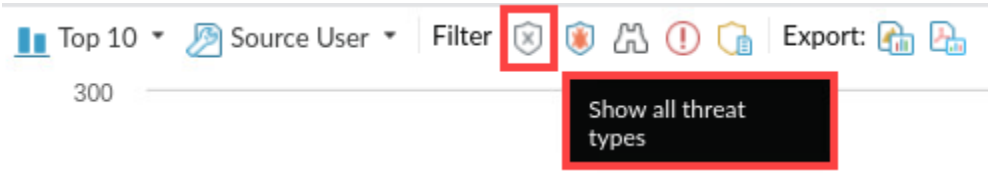
Please Note

Note that the image you see will differ from the example shown here.

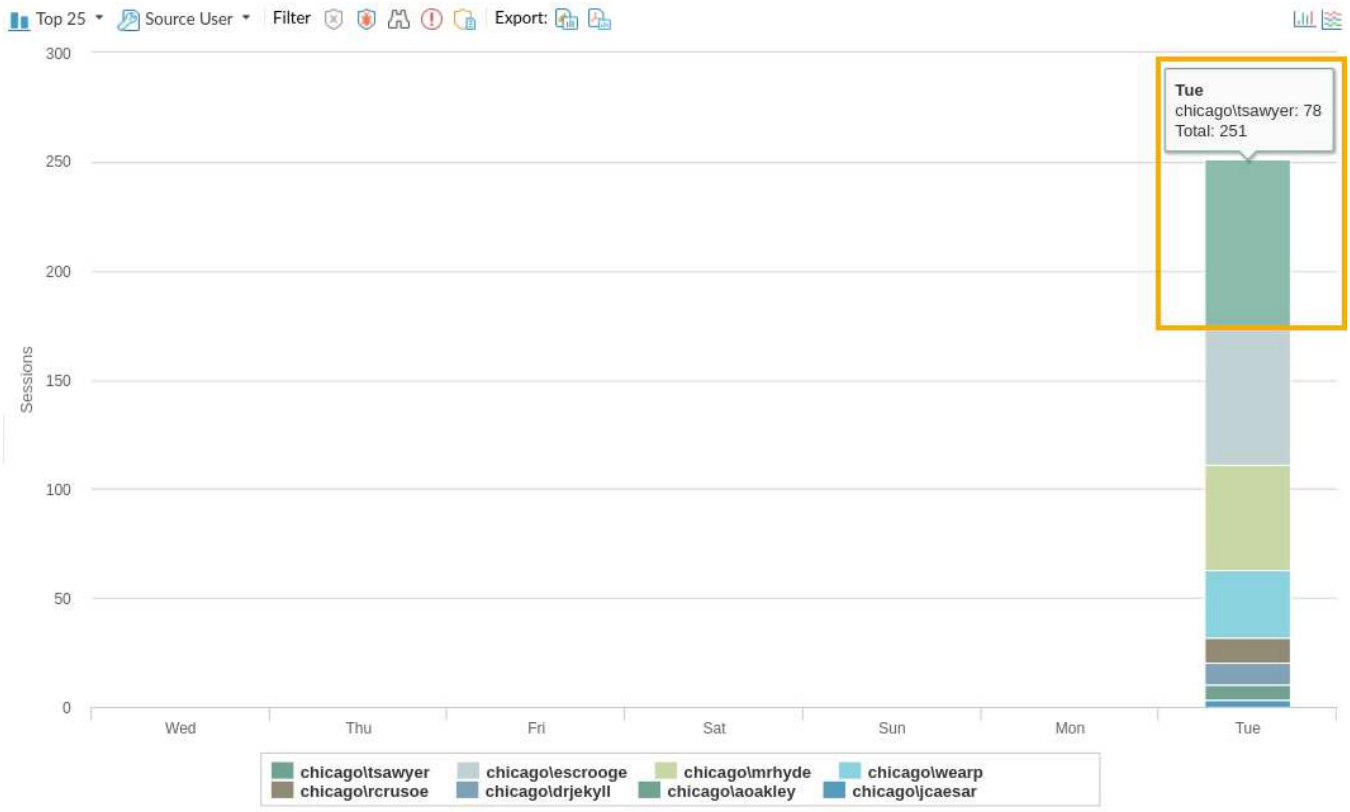
4. At the top of the window, click **Threat** and choose **Source User**.

5. At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats.

6. Select **Show all threat types**.



7. Hover your pointer over the top section of any bar on the bar chart**.** You should see a popup window that shows the source User Name and number of detections**.**



Please Note The information you see may differ from the example here.

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

2.10 View Threat Information Using Reports

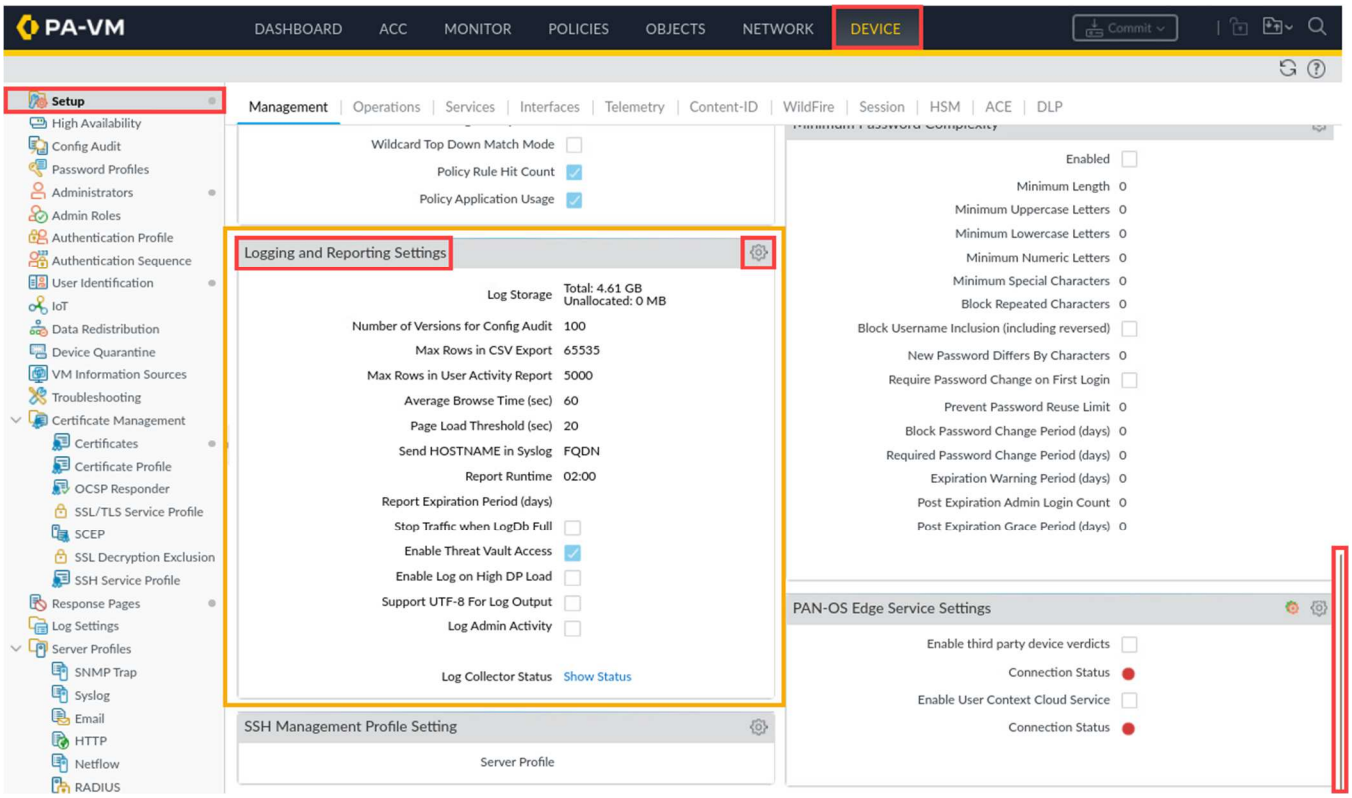
In this section, you will enable and view more than 40 predefined reports available on the firewall. Your efficient use of the predefined reports depends on your spending time with each report, discovering and determining which information might be useful to you in your own environment. Your familiarity with the reports will help you to find the reports that are most useful to you. For this lab, you only utilize Custom Reports and build a Custom Report.

The firewall offers a comprehensive reporting system that caters to various user needs and preferences. Users have the flexibility to leverage both predefined reports or create customized reports tailored to their specific data requirements and actionable tasks. Furthermore, it is possible to amalgamate predefined and custom reports to consolidate the desired information.

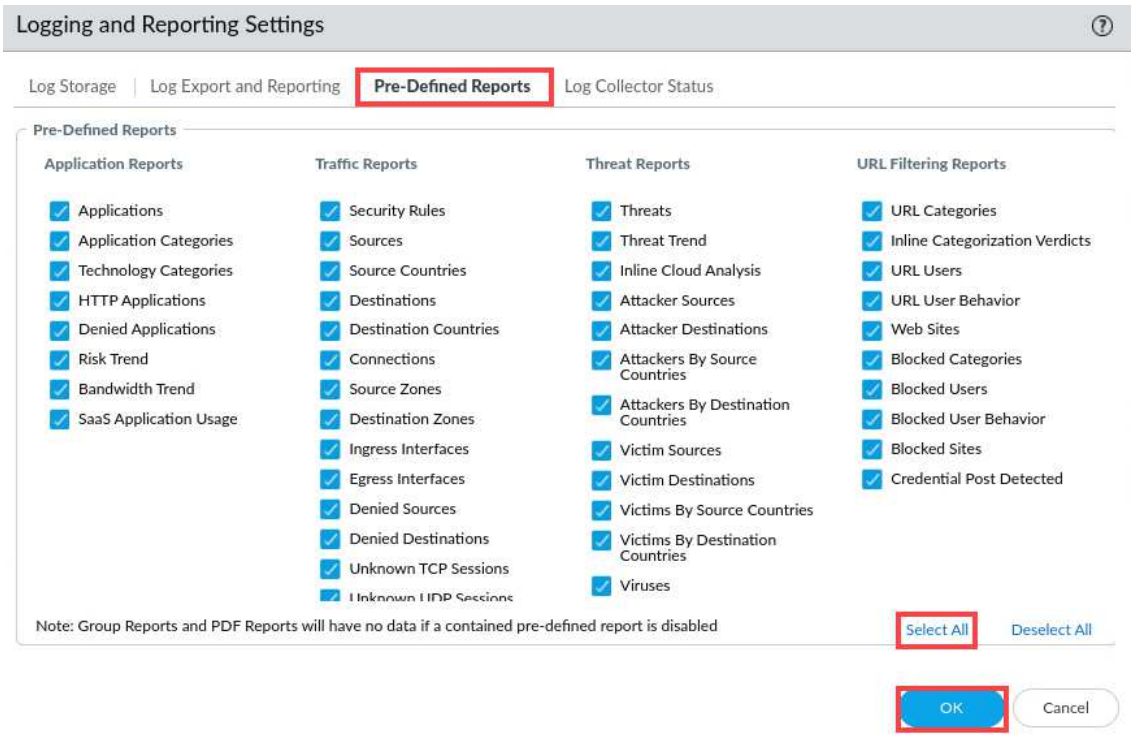
The reporting capabilities of the firewall encompass the following categories:

- **Predefined Reports**: These reports provide users with succinct overviews of network traffic. They are available in four distinct categories, namely Applications, Traffic, Threat, and URL Filtering.
- **User or Group Activity Reports**: This feature enables users to either schedule or generate on-demand reports pertaining to application usage and URL activities for individual users or user groups. These reports include detailed information such as URL categories and estimated browse time calculations for individual users.
- **Custom Reports**: Users have the ability to create and schedule reports that specifically display the information they require. This customization involves applying filters based on conditions and columns, with the option to utilize query builders for more precise drilling down into report data.
- **PDF Summary Reports**: Users can compile up to 18 predefined or custom reports/graphs from various categories, including Threat, Application, Trend, Traffic, and URL Filtering, into a single PDF document. This feature also incorporates behavior-based mechanisms to identify potential botnet-infected hosts within the network.
- **Report Groups**: To streamline reporting processes, users can aggregate custom and predefined reports into report groups, resulting in a consolidated PDF report. This report can be conveniently emailed to one or more designated recipients.

1. Navigate to **Device > Setup > Management**. Scroll and locate the *Logging and Reporting Settings* in the Management pane. Click the **Gear** icon.

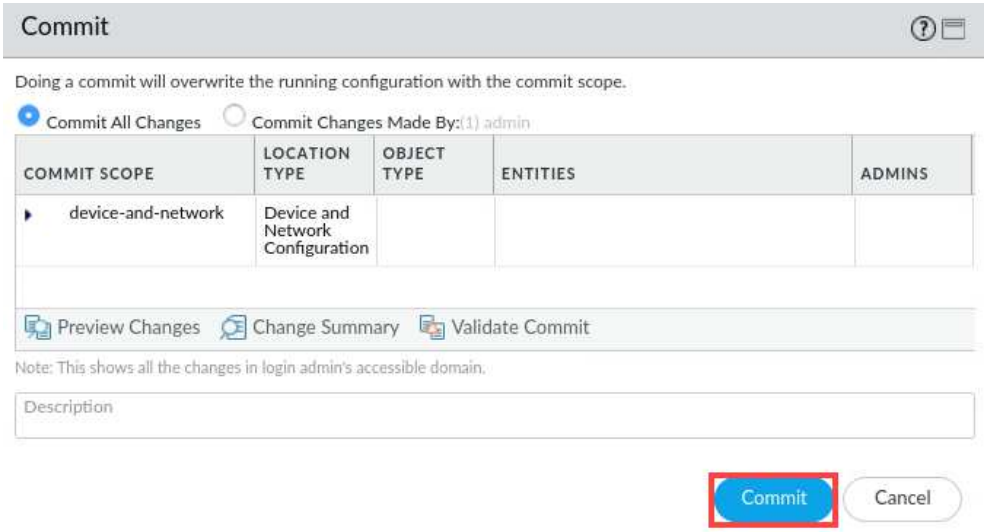


2. In the *Logging and Reporting Settings* window, select the **Pre-Defined Reports** tab. Enable all the pre-defined reports by choosing **Select All** and click **OK.** For this task, you will enable all the pre-defined reports. In your capacity as an administrator, you have the flexibility to align your organization's requirements with the specific reports that are necessary by choosing only the reports needed.

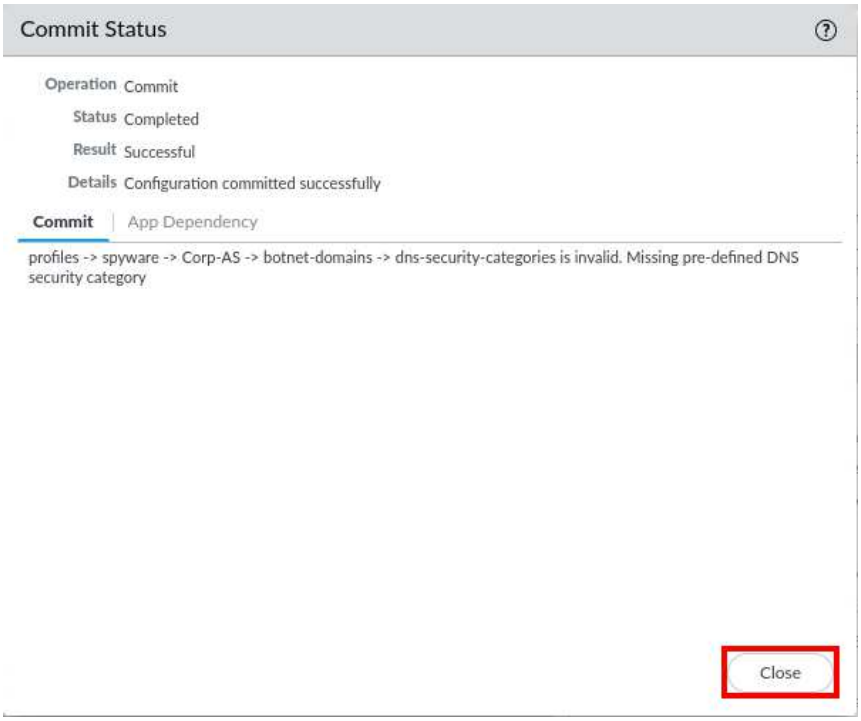


3. Click the **Commit** link located at the top-right of the web interface**.**

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



5. When the commit operation successfully completes, click **Close** to continue**.**

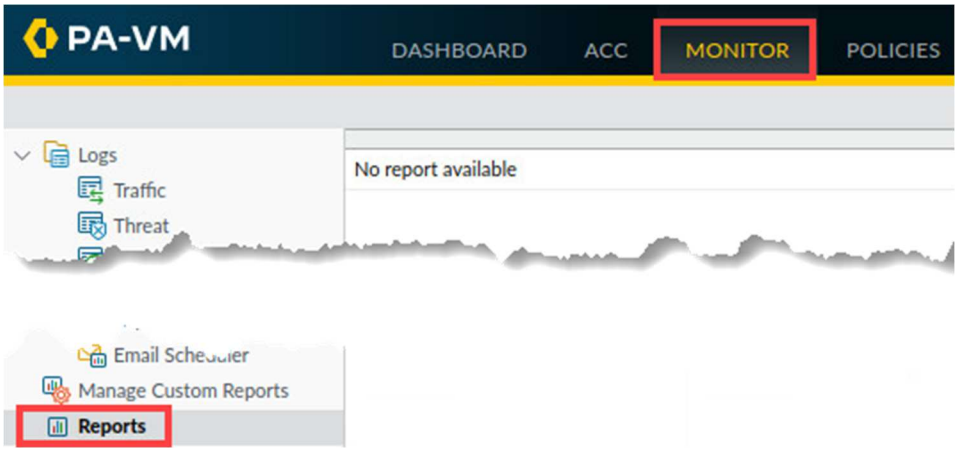


6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

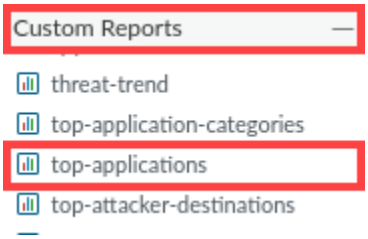
2.11 View Application Information Using Predefined Reports

In this section, you will open and view two reports from the more than 40 predefined reports available on the firewall. After you have learned to open and view a single report, you have the knowledge to open and view any report. Your efficient use of the predefined reports depends on your spending time with each report, discovering and determining which information in which reports might be most useful to you.

1. Navigate to **Monitor > Reports**.



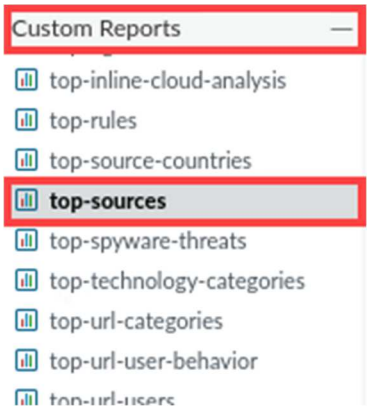
2. In **Custom Reports**, expand the list of available application reports. Scroll and click **top-applications**.



3. A **top-applications** report should be displayed in the web interface. The report displays the top applications that were detected by your firewall on the previous day. It should have a format like the following example, but your application data will be different. You can use this information to update your Security policy rules, as necessary.

	APPLICATION NAME	BYTES	SESSIONS
1	dns	190.9k	514
2	paloalto-updates	208.2M	130
3	web-browsing	14.2M	30
4	insufficient-data	6.6k	23
5	pan-db-cloud	282.5k	21
6	google-base	395.4k	13

5. At the far right of the report window, click **Custom Reports** to expand the list of available Reports. Scroll and click **top-sources** to view a report.



6. A *Sources* report should be displayed in the web interface. The report displays which source IP addresses were detected by your firewall on the previous day. It should have a format like the following example, but your data will be different.

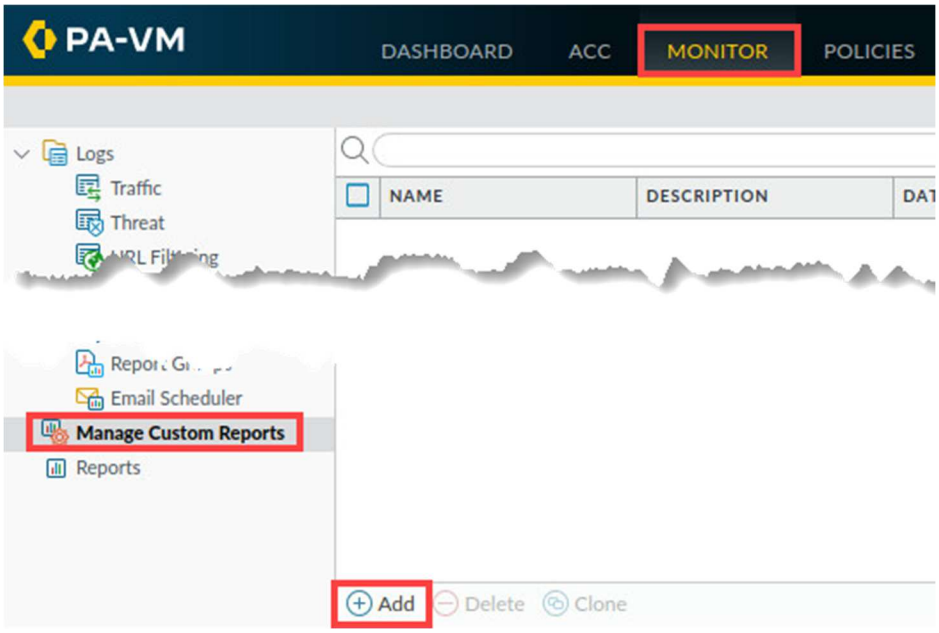
	SOURCE ADDRESS	SOURCE HOST NAME	SOURCE USER	BYTES	SESSIONS
1	192.168.1.254	192.168.1.254		208.6M	672
2	192.168.1.20	192.168.1.20		16.3M	73

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

2.12 View Threat and Application Information Using Custom Reports

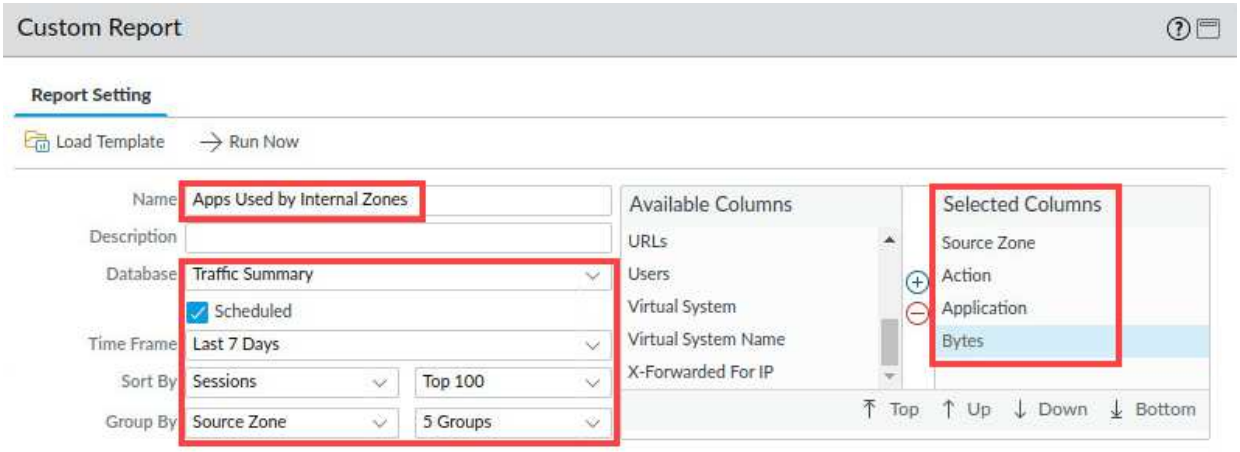
In this section, you will create a custom report. The custom reports feature enables you to build reports that include only the information that you consider useful to you in your environment. The first custom report will list the applications that the firewall has detected in each of your internal security zones. The second custom report will list the applications that the firewall has detected in the outside zone, which in the lab environment is associated with the internet. Such information can help you to improve the configuration of your Security policy.

1. Select **Monitor > Manage Custom Reports**. Click **Add**.

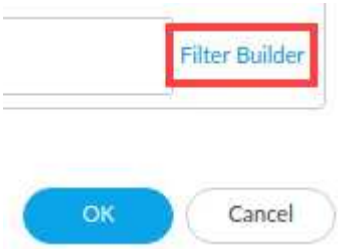


2. In the *Custom Report* window, configure the following.

Parameter	Value
Name	**Apps Used by Internal Zones**
Database	**Summary Databases > Traffic**
Scheduled	Select **check box**
Time Frame	**Last 7 Days**
Sort By	**Sessions** and **Top 100**
Group By	**Source Zone** and **5 Groups**
Selected Columns	**Source Zone**, **Action, Application**, and **Bytes**

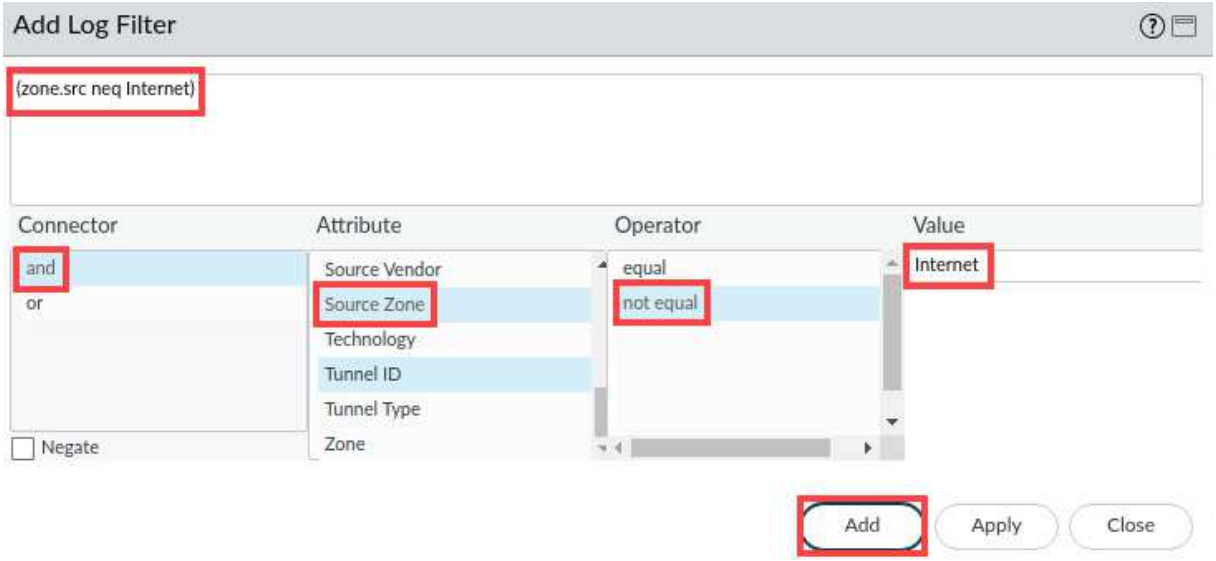


3. In the bottom right corner of the *Custom Report* window, click the **Filter Builder** link.



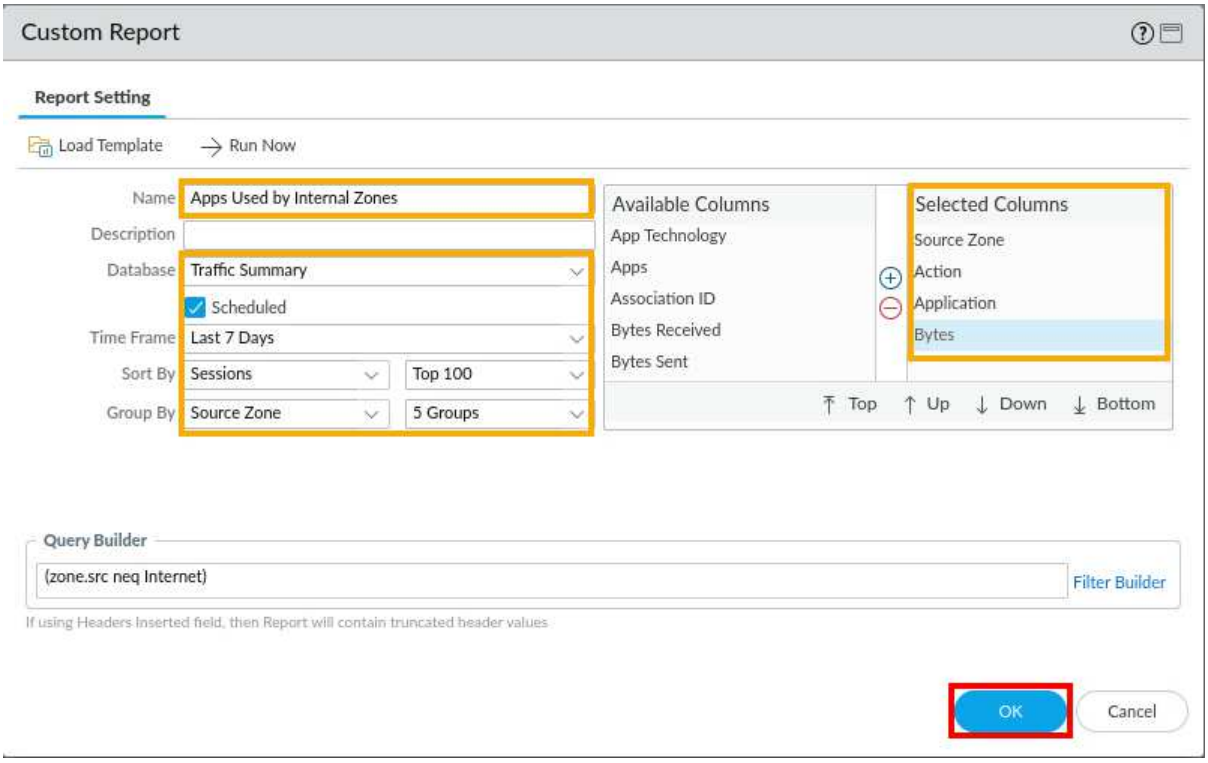
4. In the *Add Log Filter* window, configure the following. Click **Add**.

Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**not equal**
Value	**`Internet`**

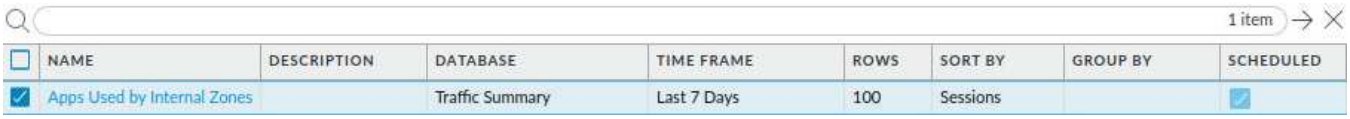


5. Click **Apply**.

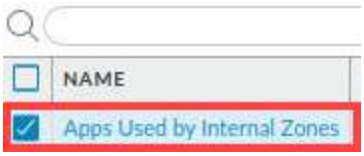
6. Click **OK** to close the **Custom Report** window.



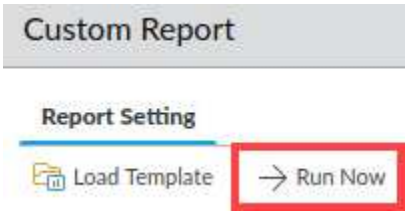
7. The new custom report should be added to the list of custom reports in the web interface.



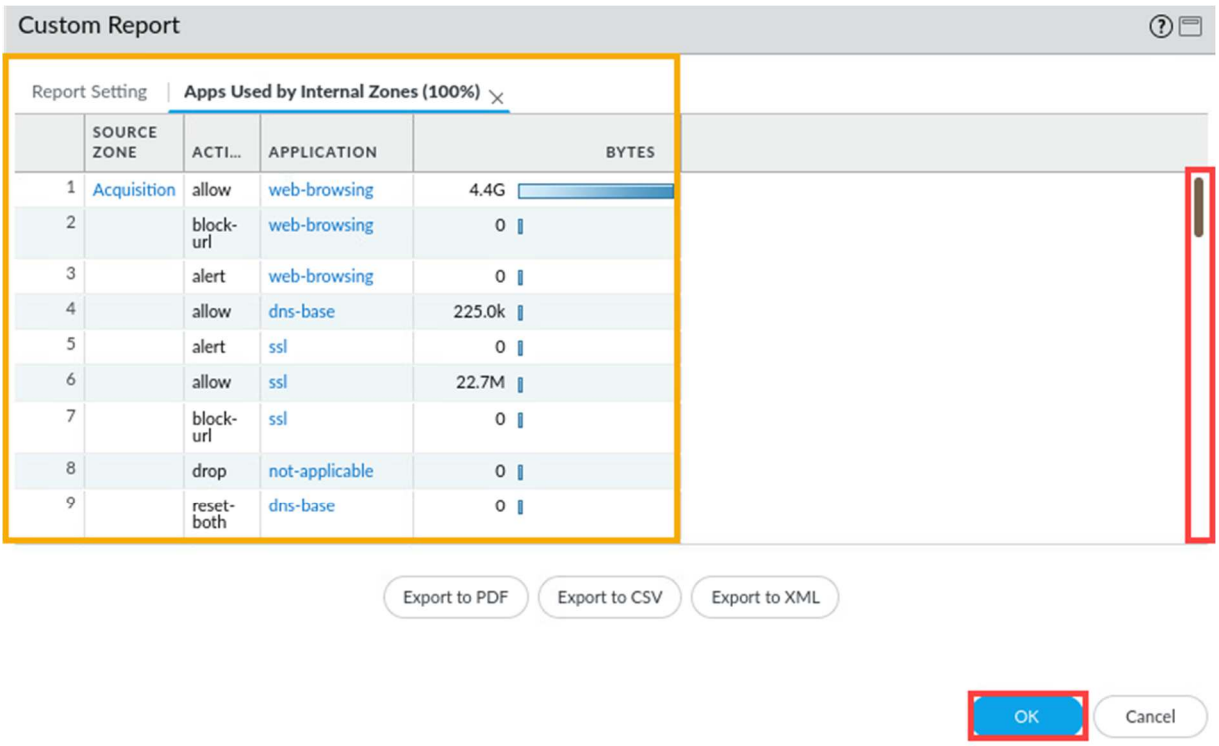
8. Click **Apps Used by Internal Zones** to open the custom report.



9. Click **Run Now** to run the custom report. The report should run, and the results should be displayed in a tab that is added and opened in the **Custom Report** window.



10. View the results of the custom report. You can scroll down through the report to see information about the Extranet and the Acquisition zones along with details about the applications which the firewall processed in each one.



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