



PALO ALTO NETWORKS EDU 210

Lab 16: Viewing Threat and Application Information

Document Version: 2022-07-19

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Blocking Threats in Encrypted Traffic	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Generate Traffic	10
1.3 Display Recent Threat Information in the Dashboard	13
1.4 Display Recent Application Information in the Dashboard	16
1.5 View Threat Information in the ACC	18
1.6 View Application Information in the ACC	22
1.7 View Threat Information in the Threat Log	26
1.8 View Application Information in the Traffic Log	31
1.9 View Threats Using App Scope Reports	36

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.

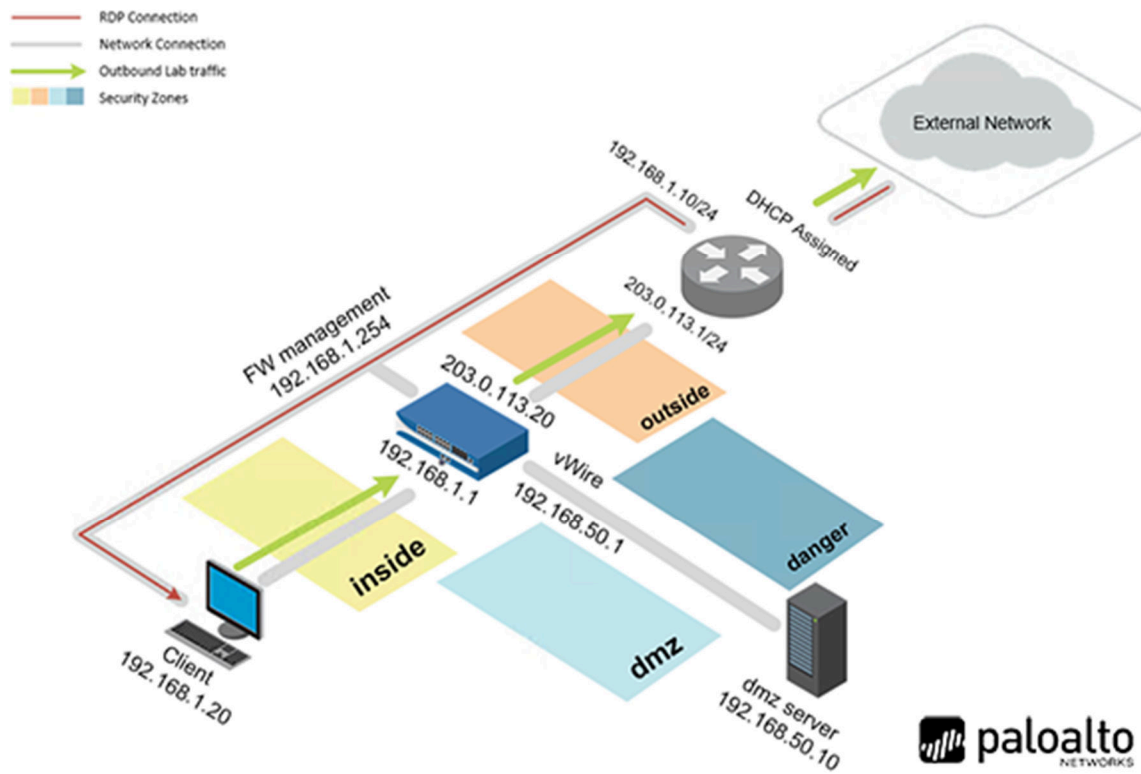
You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

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

Lab Topology



Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

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

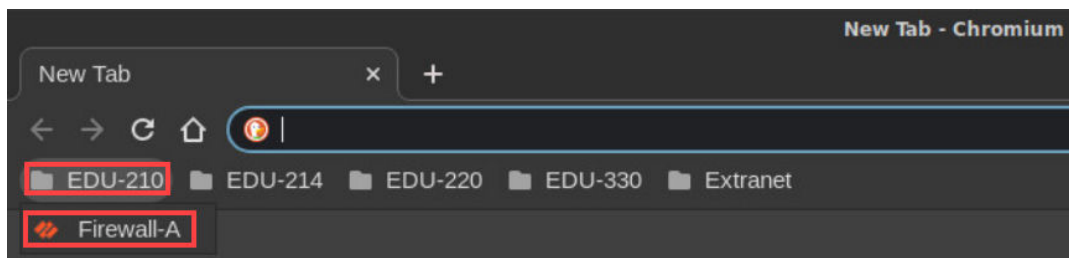
1. Click on the **Client** tab to access the Client PC.



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



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



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



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Advanced

Back to safety



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

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



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

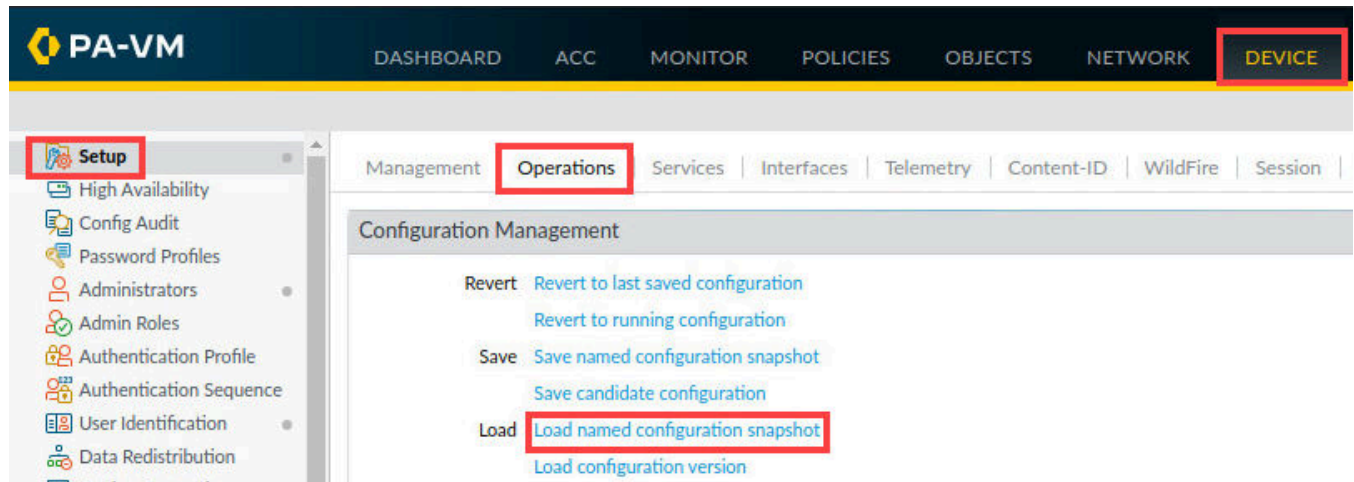
[Proceed to 192.168.1.254 \(unsafe\)](#)

- Log in to the firewall web interface as username **admin**, password **Pa10Alt0!**.



The image shows the Palo Alto Networks login page. It features the Palo Alto Networks logo at the top. Below the logo, there is a username field containing the text "admin" and a password field filled with dots. A blue "Log In" button is positioned below the password field. The entire login form is enclosed in a yellow rectangular border.

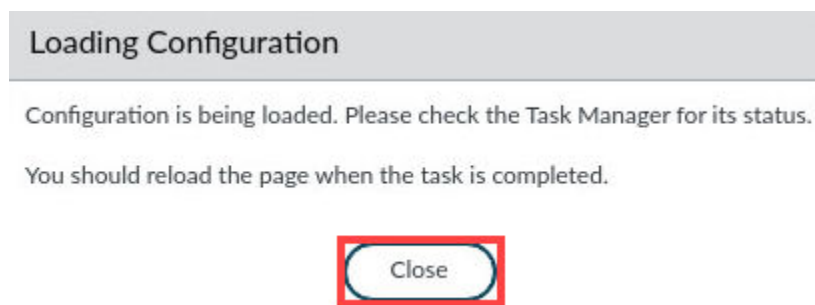
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named **configuration snapshot** underneath the *Configuration Management* section.



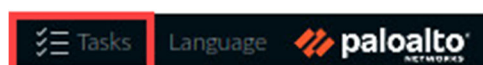
- In the *Load Named Configuration* window, select **edu-210-lab-16.xml** from the *Name* dropdown box and click **OK**.



- 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.



- 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**.

Task Manager - All Tasks ? ☰

8 items → ×

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

Show All Tasks Clear Commit Queue Close

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



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

Commit ? ☰

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

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

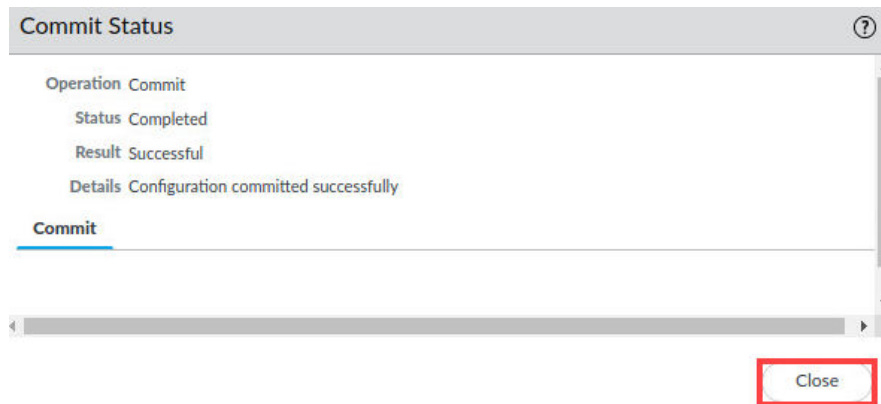
Preview Changes
Change Summary
Validate Commit
☒ Group By Location Type

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

Description

Commit Cancel

14. 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.

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



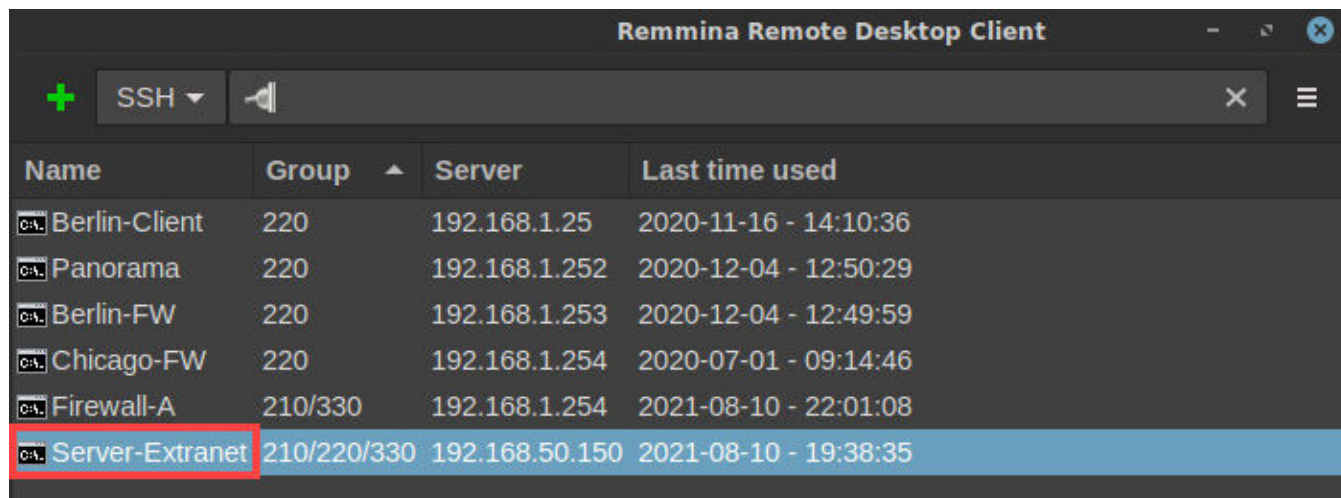
1.2 Generate Traffic

In this section, you will create a new Security policy rule and attempt to leave out the Description. This will let you see what happens when an administrator does not provide adequate information when creating a rule.

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



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



Name	Group	Server	Last time used
Berlin-Client	220	192.168.1.25	2020-11-16 - 14:10:36
Panorama	220	192.168.1.252	2020-12-04 - 12:50:29
Berlin-FW	220	192.168.1.253	2020-12-04 - 12:49:59
Chicago-FW	220	192.168.1.254	2020-07-01 - 09:14:46
Firewall-A	210/330	192.168.1.254	2021-08-10 - 22:01:08
Server-Extranet	210/220/330	192.168.50.150	2021-08-10 - 19:38:35

Please
Note

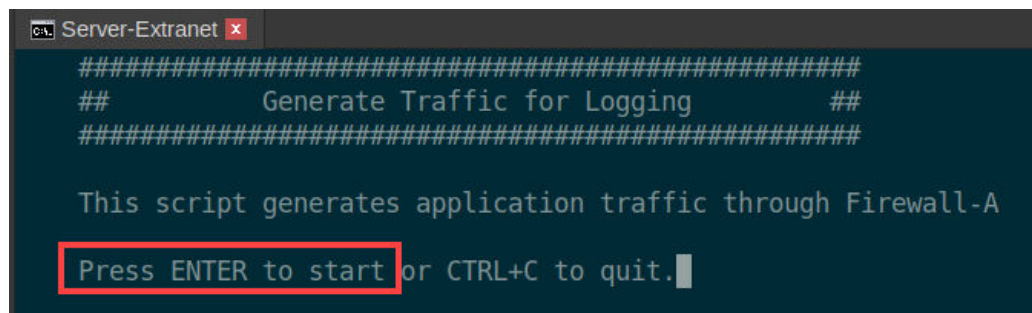
This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

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

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

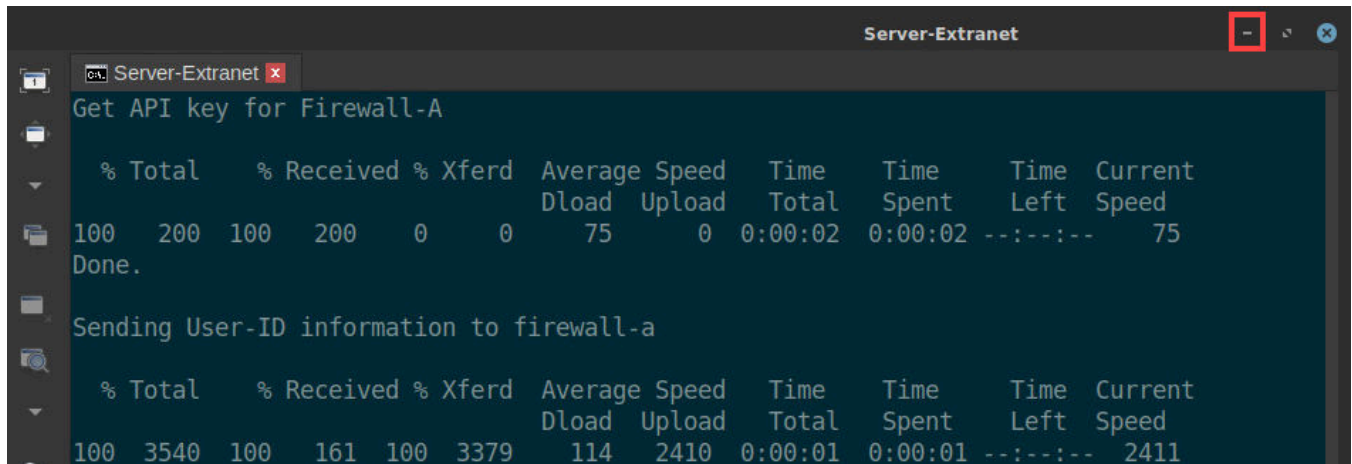
```
paloalto42@extranet1:~$ ./UsingLogs-V1.sh
```

4. Press **Enter** to start the *UsingLogsV1.sh* script.



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

- Allow 5 to 7 minutes for the script to run uninterrupted. Once the **UsingLogsV1** script completes, minimize the *Remmina* connection window.



```

Server-Extranet
Get API key for Firewall-A

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload   Total             0          0       0      75
100  200    100    200     0     0    75     0  0:00:02  0:00:02  --:--:--    75
Done.

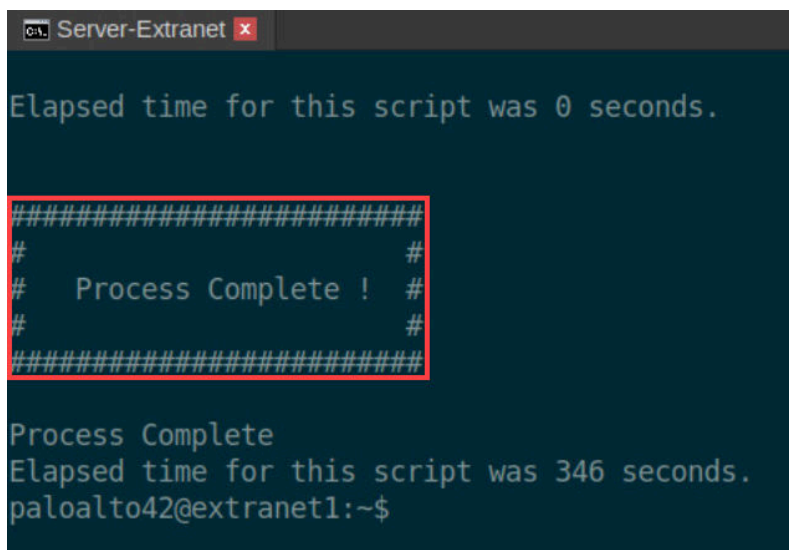
Sending User-ID information to firewall-a

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload   Total             0          0       0     2411
100  3540    100    161    100    3379    114    2410  0:00:01  0:00:01  --:--:--   2411

```



Do not continue until the **UsingLogsV1** script completes.



```

Server-Extranet
Elapsed time for this script was 0 seconds.

#####
# Process Complete ! #
#####

Process Complete
Elapsed time for this script was 346 seconds.
paloalto42@extranet1:~$

```

- Re-open the *PA-VM firewall* by clicking on the **Chromium** icon in the *Taskbar*.

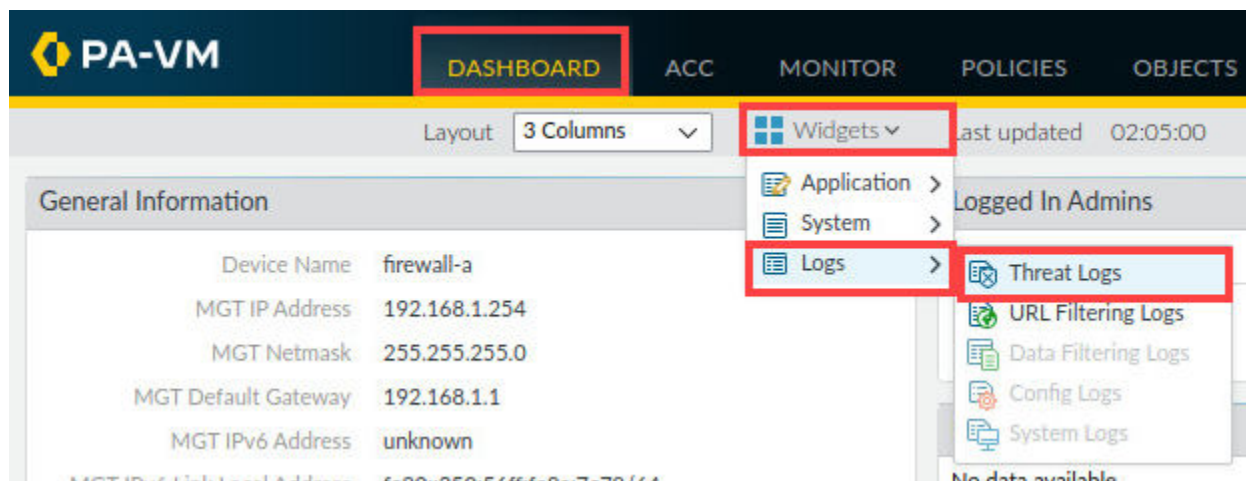


- Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 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.

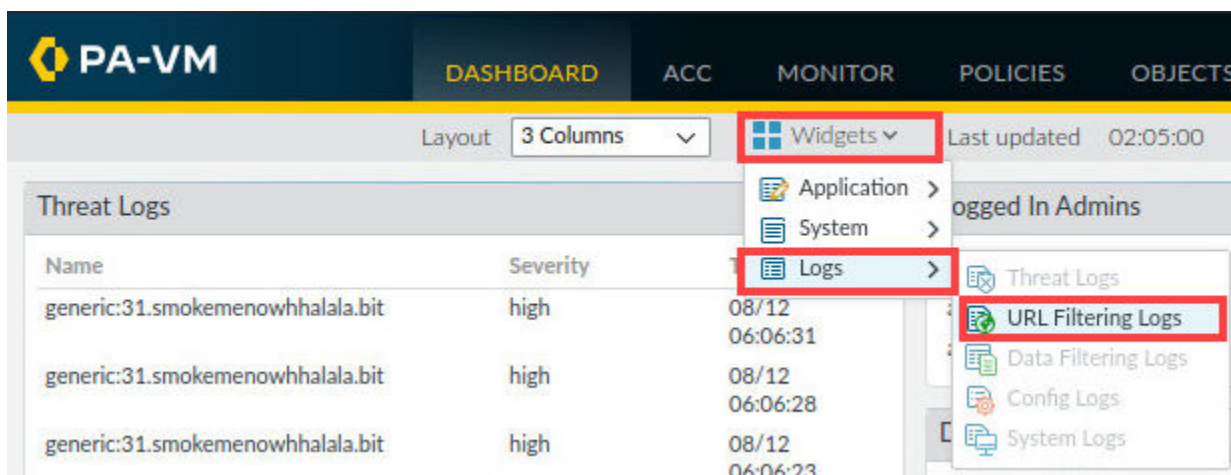
- The *Threat Logs* window will display the 10 most recent threats detected by the firewall in the last hour.

Name	Severity	Time
generic:31.smokemenowhhalala.bit	high	08/12 06:06:31
generic:31.smokemenowhhalala.bit	high	08/12 06:06:28
generic:31.smokemenowhhalala.bit	high	08/12 06:06:23
generic:31.smokemenowhhalala.bit	high	08/12 06:06:21
Trojan-Banker.neutrinopos.gdiscoun.org	high	08/12 06:06:19
generic:transmercasa.com	medium	08/12 06:06:19
generic:poperitte.host	high	08/12 06:05:50
generic:annamount.pw	medium	08/12 06:05:36
generic:againston.pw	medium	08/12 06:05:36
generic:packals.pw	medium	08/12 06:05:35

Please Note

Depending on activity in your lab environment in the last hour, you might not see threat entries. This widget is useful for viewing only the most recent threats detected by the firewall.

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



The screenshot shows the PA-VM dashboard with the 'DASHBOARD' tab selected. The 'Widgets' menu is open, and the 'Logs' option is selected, which has opened a sub-menu. In this sub-menu, the 'URL Filtering Logs' option is highlighted with a red box. The 'Threat Logs' widget is visible in the background, showing a list of threats.

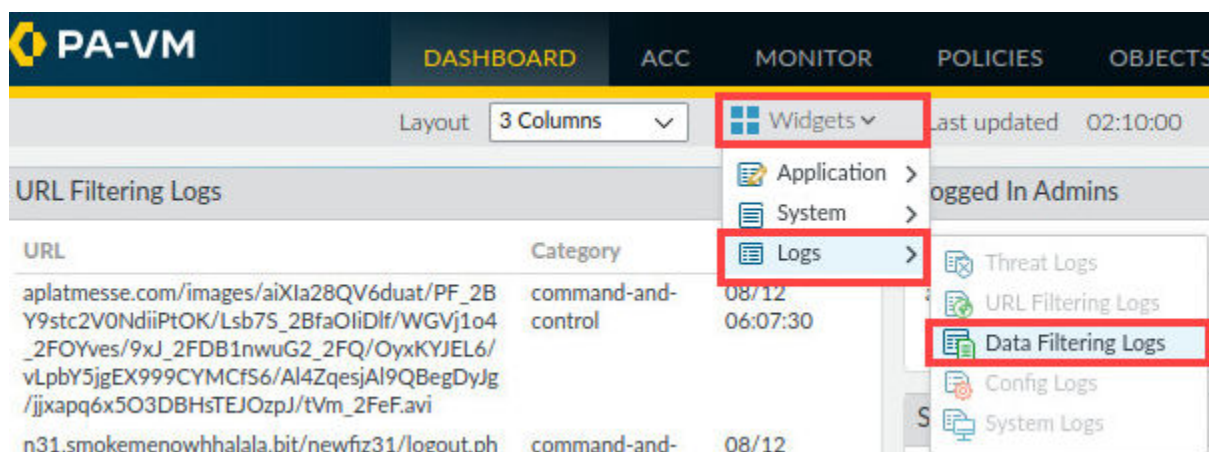
4. The *URL Filtering Logs* window will display the 10 most recent threats detected by the firewall in the last hour.

URL	Category	Time
aplatmesse.com/images/aiXla28QV6duat/PF_2B_Y9stc2V0NdiiPtOK/Lsb7S_2BfaOliDlf/WGVj1o4_2FOYves/9xJ_2FDB1nwwG2_2FQ/OyxKYJEL6/vLpbY5jgEX999CYMCfS6/Al4ZqesjAl9QBegDyJg/jjxapq6x5O3DBHsTEJOzpJ/tVm_2FeF.avi	command-and-control	08/12 06:07:30
n31.smokemenowhhalala.bit/newfiz31/logout.php	command-and-control	08/12 06:06:26
n31.smokemenowhhalala.bit/newfiz31/logout.php	command-and-control	08/12 06:06:23
poperitte.host/data2.php?79504E1137D96CED	command-and-control	08/12 06:05:38
82.146.42.174/sin.png	malware	08/12 06:05:33
againston.pw/	malware	08/12 06:05:31
46.249.62.199/Tinx86_14.exe	malware	08/12 06:05:31
wodjfdhhen2dsads.info/	adult	08/12 06:05:25
wodjfdhhen1ndhd.online/	command-and-control	08/12 06:05:23
wodjfdhhen1ndhd.online/	command-and-control	08/12 06:05:22

Please Note

Depending on activity in your lab environment in the last hour, you might not see threat entries. This widget is useful for viewing only the most recent threats detected by the firewall.

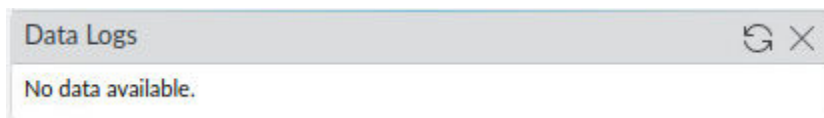
5. Click **Widgets** and select **Logs > Data Filtering Logs** if it is not already selected.



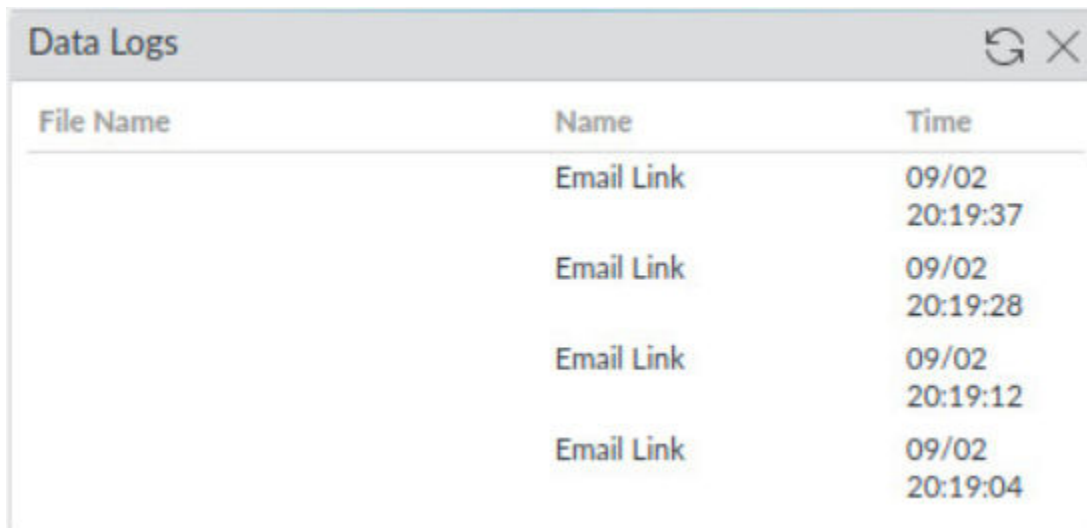
The screenshot shows the PA-VM dashboard with the following elements:

- Navigation Bar:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS.
- Layout:** 3 Columns.
- Widgets Menu:** A dropdown menu is open, showing:
 - Application >
 - System >
 - Logs >** (highlighted with a red box)
- Logs Sub-menu:** A secondary dropdown menu is open from the 'Logs' option, showing:
 - Threat Logs
 - URL Filtering Logs
 - Data Filtering Logs** (highlighted with a red box)
 - Config Logs
 - System Logs
- URL Filtering Logs Widget:** A table displaying the 10 most recent threats detected by the firewall in the last hour, as shown in the previous table.

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



When logs are present, you will be presented with the following below.



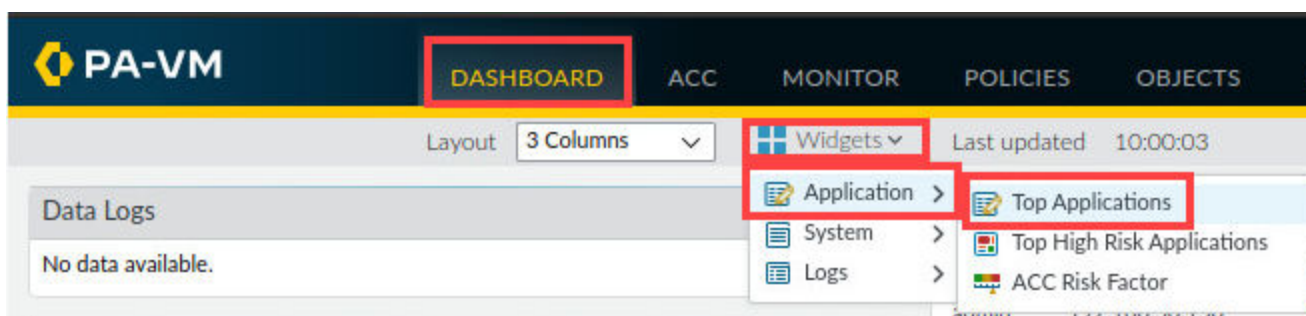
File Name	Name	Time
	Email Link	09/02 20:19:37
	Email Link	09/02 20:19:28
	Email Link	09/02 20:19:12
	Email Link	09/02 20:19:04

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

1.4 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.

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



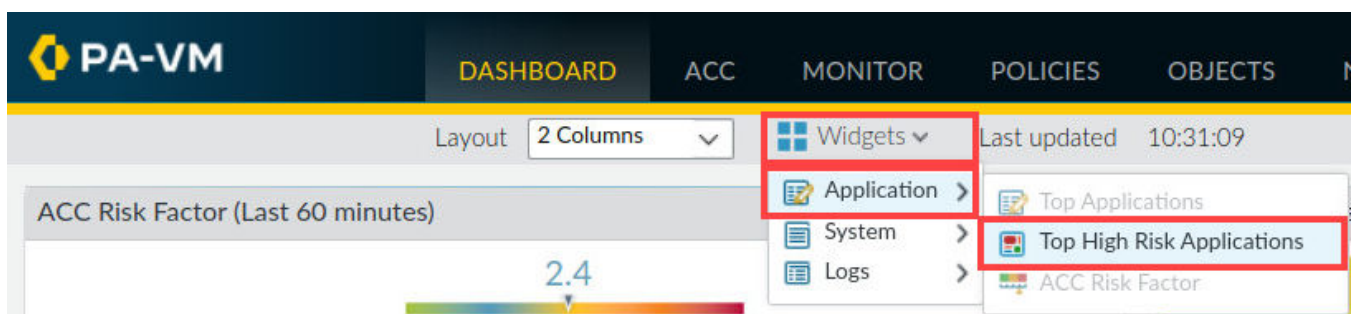
- Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour.



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.

- 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.

**Please Note**

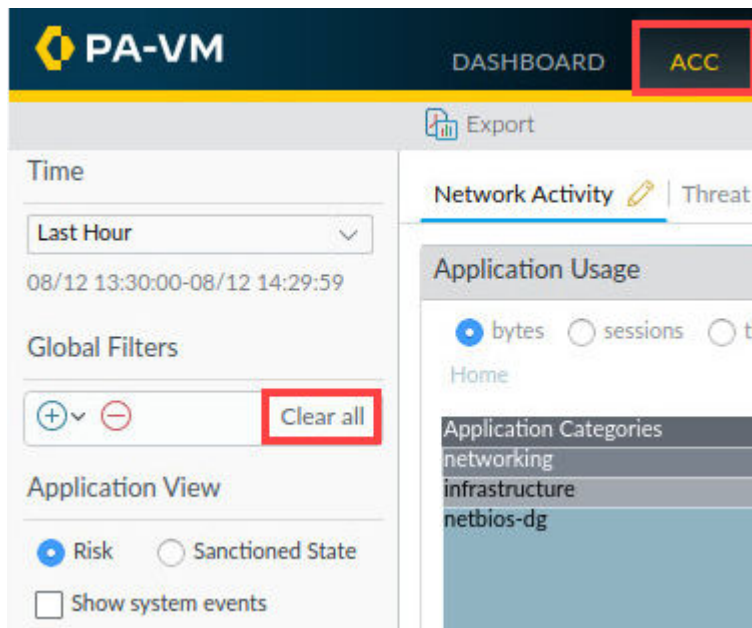
Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. If the Top High Risk and Top Applications have not updated, please allow 3 to 5 minutes for the widgets to update.

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

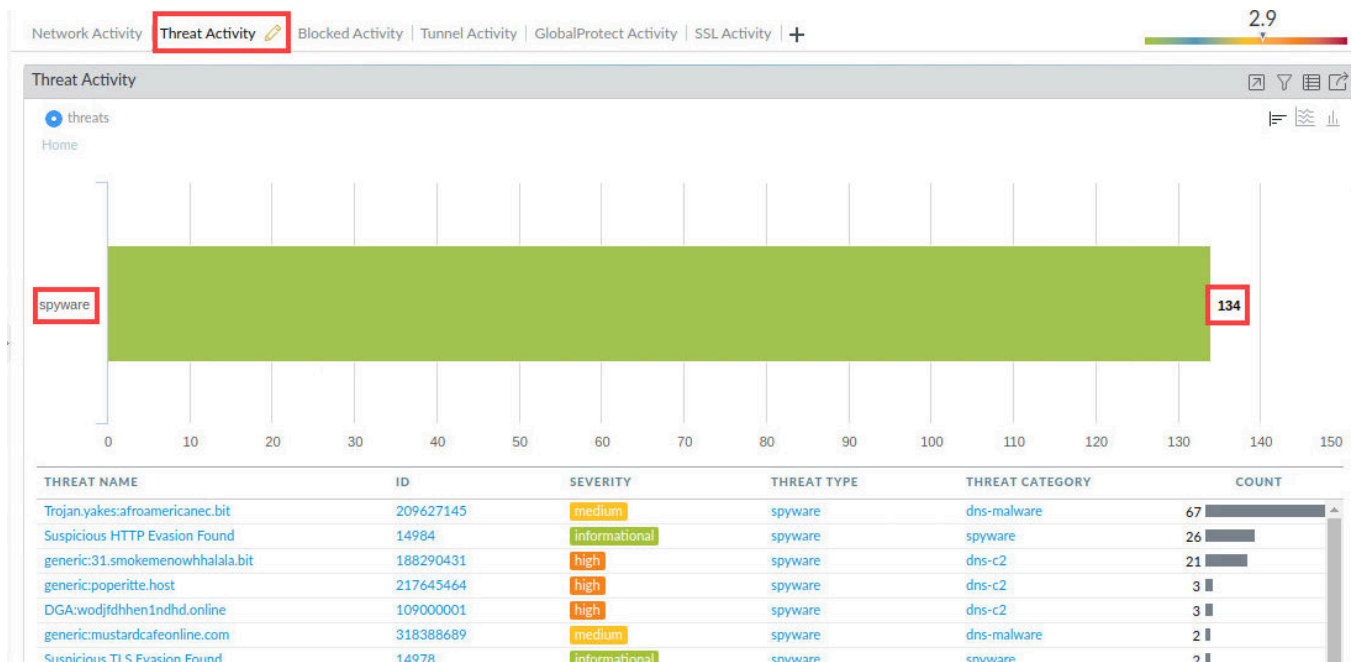
1.5 View Threat Information in the ACC

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**.




2. Click the **Threat Activity** tab. On the left side of the **ACC** window, click the **Time** dropdown menu and select **Last 7 Days**. This value configures all the widgets to display threat information for the last seven days.



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.

- In the **Threat Activity** widget's table below the graph, click the small arrow icon next to one of the **Severity** level entries. For this step, we chose to use the **high** Severity level.

THREAT NAME	ID	SEVERITY	THREAT TYPE
Trojan.yakes:afroamericanec.bit	209627145	medium	spyware
generic:31.smokemenowhhalala.bit	188290431	high 	spyware
Suspicious HTTP Evasion Found	14984	informational	spyware
Trojan.yakes:hellbro.bit	187048410	medium	spyware
generic:crypto-pool.fr	367598334	medium	spyware
generic:poperitte.host	217645464	high	spyware
DGA:wodjfdhhen1ndhd.online	109000001	high	spyware
Suspicious TLS Evasion Found	14978	informational	spyware
generic:mustardcafeonline.com	318388689	medium	spyware
generic:toptoptop1.online	262789992	medium	spyware

Please Note

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.



- Find the global filter on the left side of the ACC window. Notice **high** was added as a global filter condition.

Time



Last 7 Days

08/05 14:45:00-08/12 14:44:59

Global Filters

Severity (1)  

☒ high

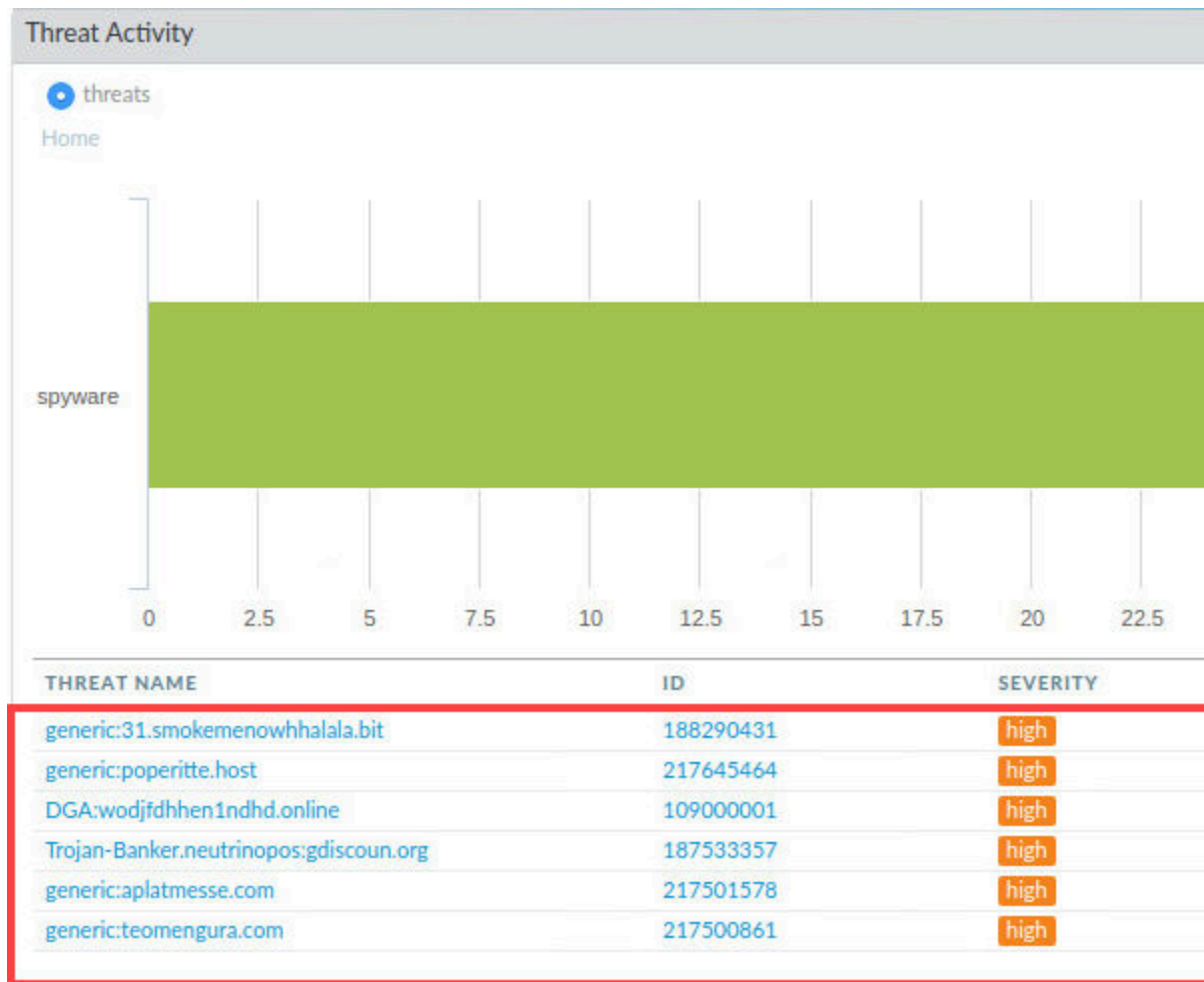
  Clear all

Application View

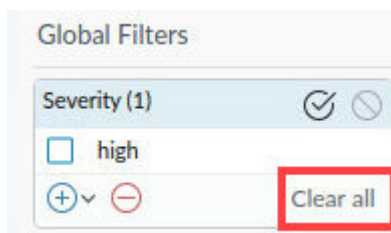
☒ Risk ☐ Sanctioned State

☐ Show system events

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



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

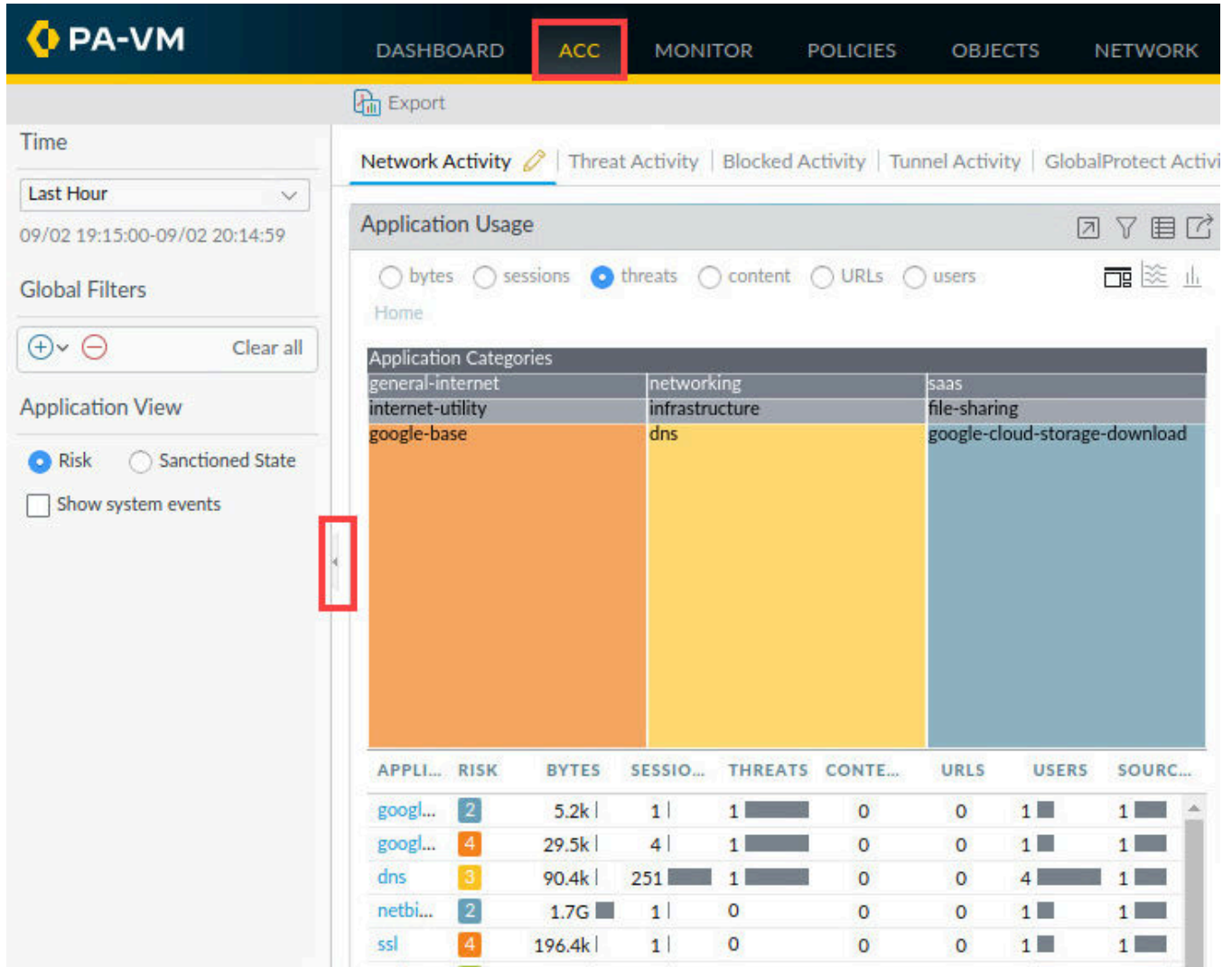


- Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 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.



The screenshot shows the PA-VM web interface. The top navigation bar includes tabs for DASHBOARD, ACC (highlighted with a red box), MONITOR, POLICIES, OBJECTS, and NETWORK. Below the navigation bar, the 'Network Activity' tab is selected, and the 'Application Usage' widget is displayed. The widget shows a heatmap of application categories and a table of application data. A small arrow icon in the sidebar is highlighted with a red box, indicating how to hide the sidebar.

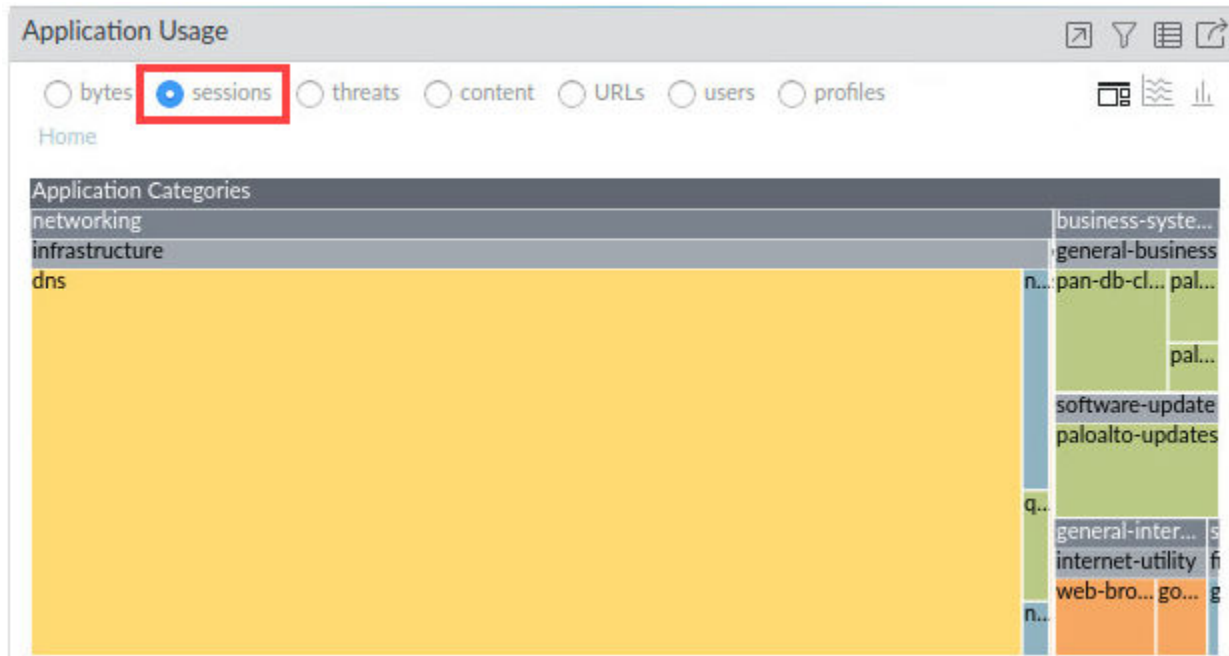
Application Categories

Category	Sub-category	Color
general-internet	networking	Orange
internet-utility	infrastructure	Yellow
google-base	dns	Blue
	saas	Light Blue
	file-sharing	Light Blue
	google-cloud-storage-download	Light Blue

Application Data Table

APPLI...	RISK	BYTES	SESSIO...	THREATS	CONTE...	URLS	USERS	SOURC...
googl...	2	5.2k	1	1	0	0	1	1
googl...	4	29.5k	4	1	0	0	1	1
dns	3	90.4k	251	1	0	0	4	1
netbi...	2	1.7G	1	0	0	0	1	1
ssl	4	196.4k	1	0	0	0	1	1

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



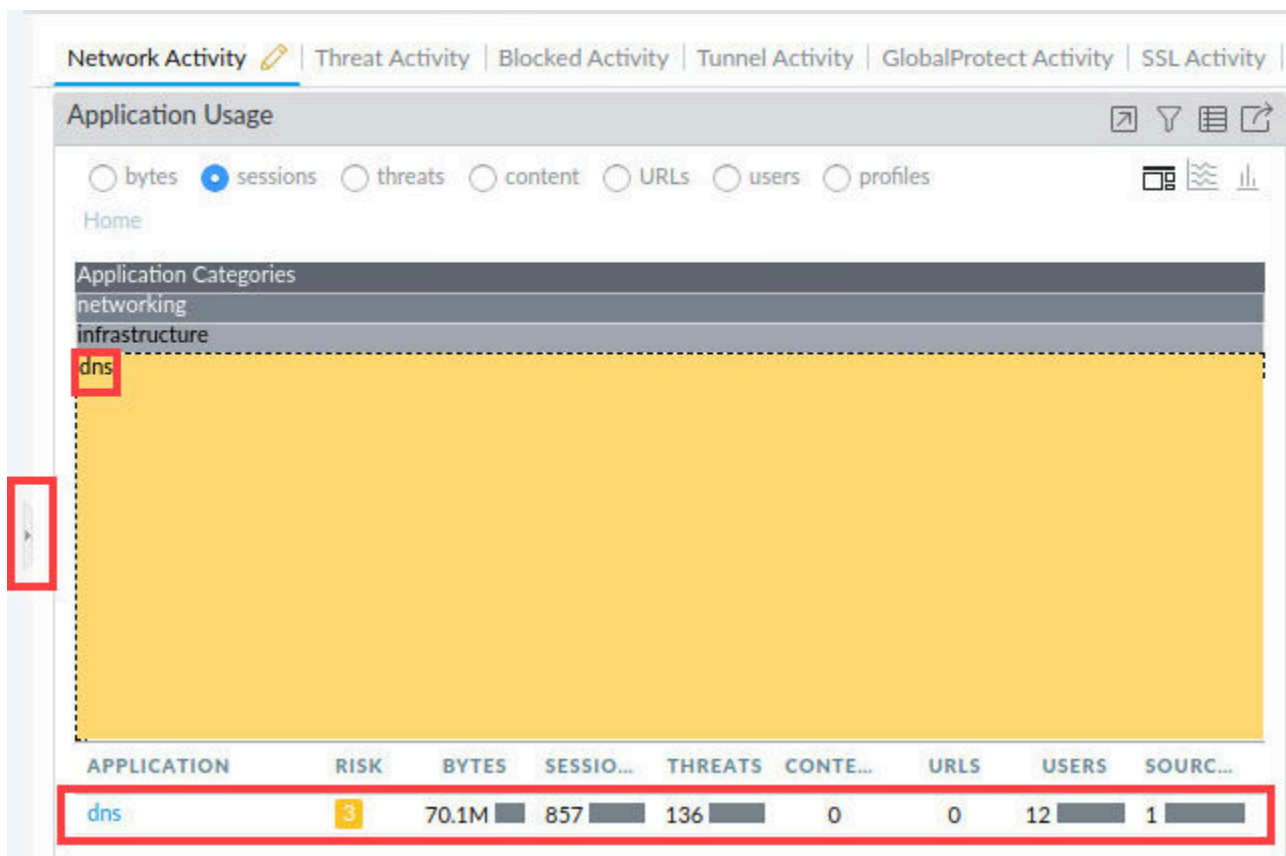
- Hover your pointer over the section for **dns**. This action displays a summary window with information about that application.



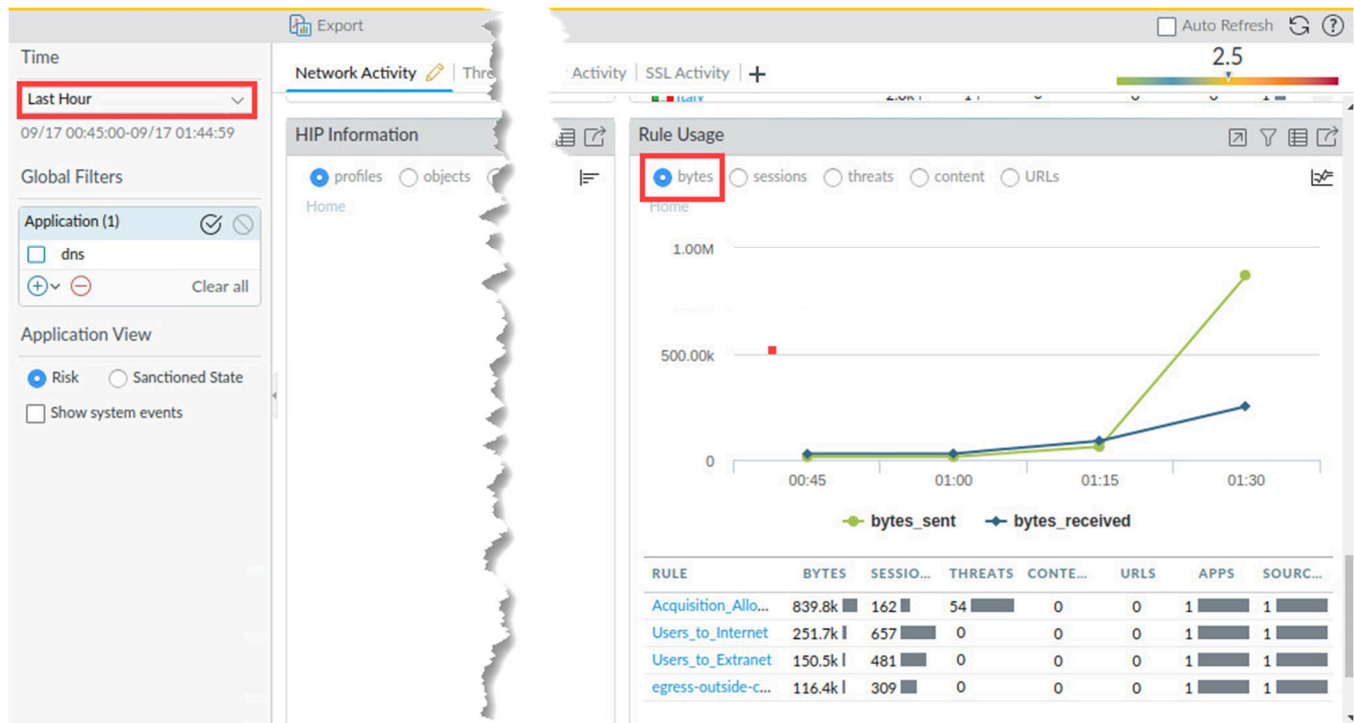
4. In the table below the graph, hover your pointer over the **dns** application until the global filter **left arrow** appears. Then click the **Left arrow** to promote the **dns** application to a global filter.

APPLICATION	RISK	BYTES	SE
web-browsing	4	689.4M	2.7
dns	3	70.1M	85
ssl		491.4M	5
paloalto-u		50.8M	3
pan-db-cloud	1	233.5k	1
insufficient data			

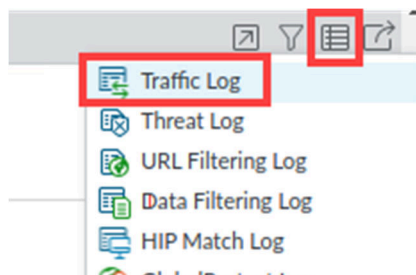
5. Unhide the sidebar by clicking the *tiny* arrow again. Notice the *Application Usage* chart has been upgraded to show the **dns** application.



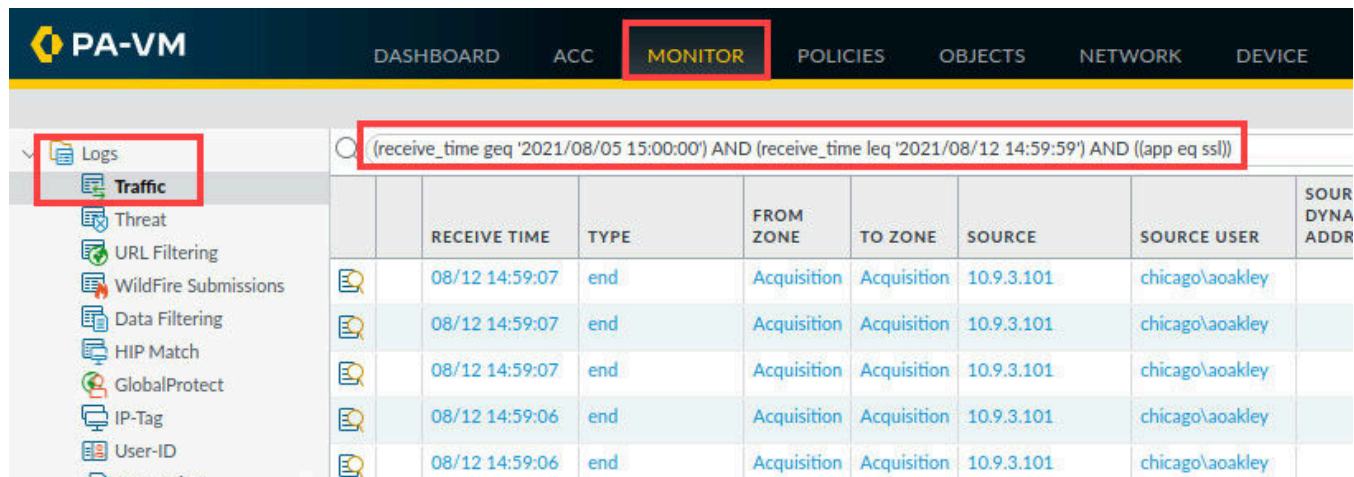
6. Scroll down in the **Network Activity** tab until you reach the **Rule Usage** widget. Select the radio button at the top for **Bytes**. In the *Time* column, select **Last Hour**.



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 it navigated you to **Monitor > Logs > Traffic**. There should be a time range filter and an application filter for web browsing. The time range filter is derived from the time specified in the ACC. Note that the entries displayed in the Traffic log match the filter

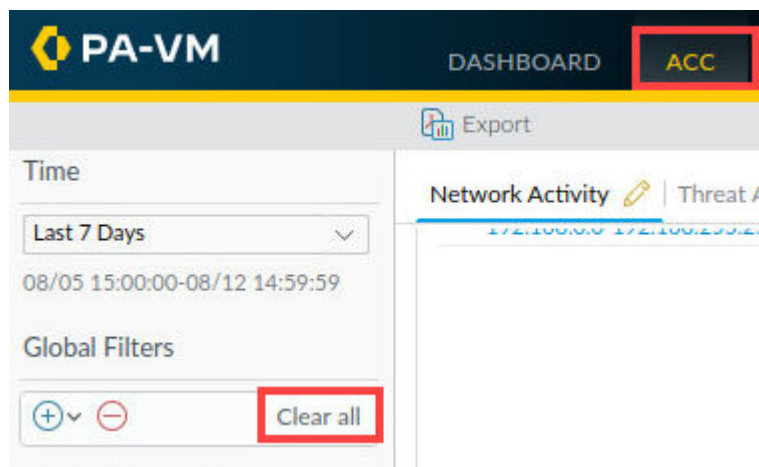


RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOUR DYN ADDR
08/12 14:59:07	end	Acquisition	Acquisition	10.9.3.101	chicago\aoakley	
08/12 14:59:07	end	Acquisition	Acquisition	10.9.3.101	chicago\aoakley	
08/12 14:59:07	end	Acquisition	Acquisition	10.9.3.101	chicago\aoakley	
08/12 14:59:06	end	Acquisition	Acquisition	10.9.3.101	chicago\aoakley	
08/12 14:59:06	end	Acquisition	Acquisition	10.9.3.101	chicago\aoakley	

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.

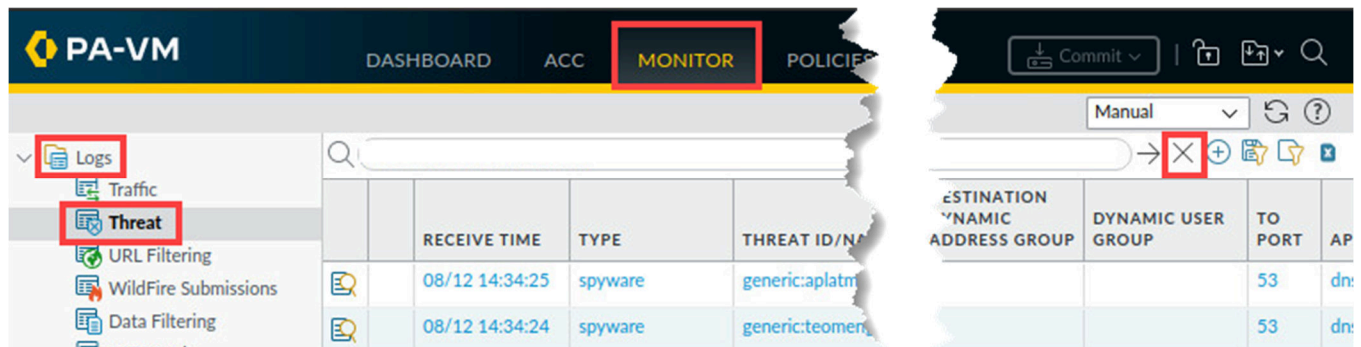


11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

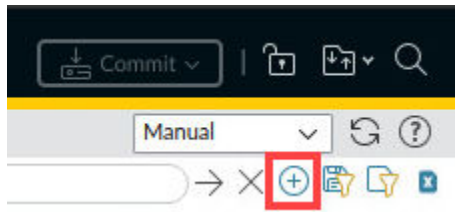
1.7 View Threat Information in the Threat Log

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

Add Log Filter ?

(severity geq high)

Connector	Attribute	Operator	Value
and	Sender Address	equal	informational
or	Session ID	not equal	low
	Session Owner	greater than or equal	medium
	Severity	less than or equal	high
	Source Address		critical
	Source Category		

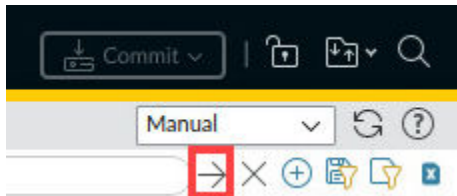
☐ Negate

Add
Apply
Close



- 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.



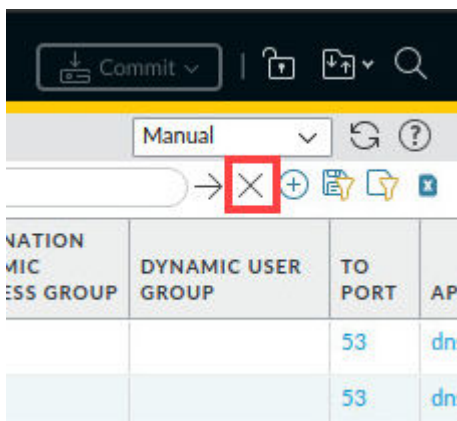
- With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



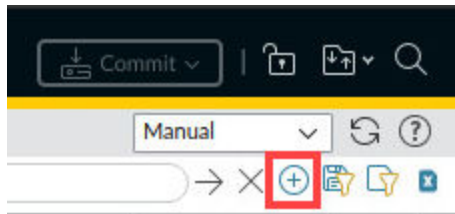
- Notice the Threat log has been filtered to display only threats of high severity or greater. Some columns have been adjusted to reflect the *Severity* column.

<input type="text" value="(severity geq high)"/>					
		RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME
		08/12 14:34:25	high	spyware	generic:aplatmesse.com
		08/12 14:34:24	high	spyware	generic:teomengura.com
		08/12 14:33:54	high	spyware	generic:31.smokemenowh...
		08/12 14:33:40	high	spyware	generic:31.smokemenowh...
		08/12 14:33:40	high	spyware	generic:31.smokemenowh...

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

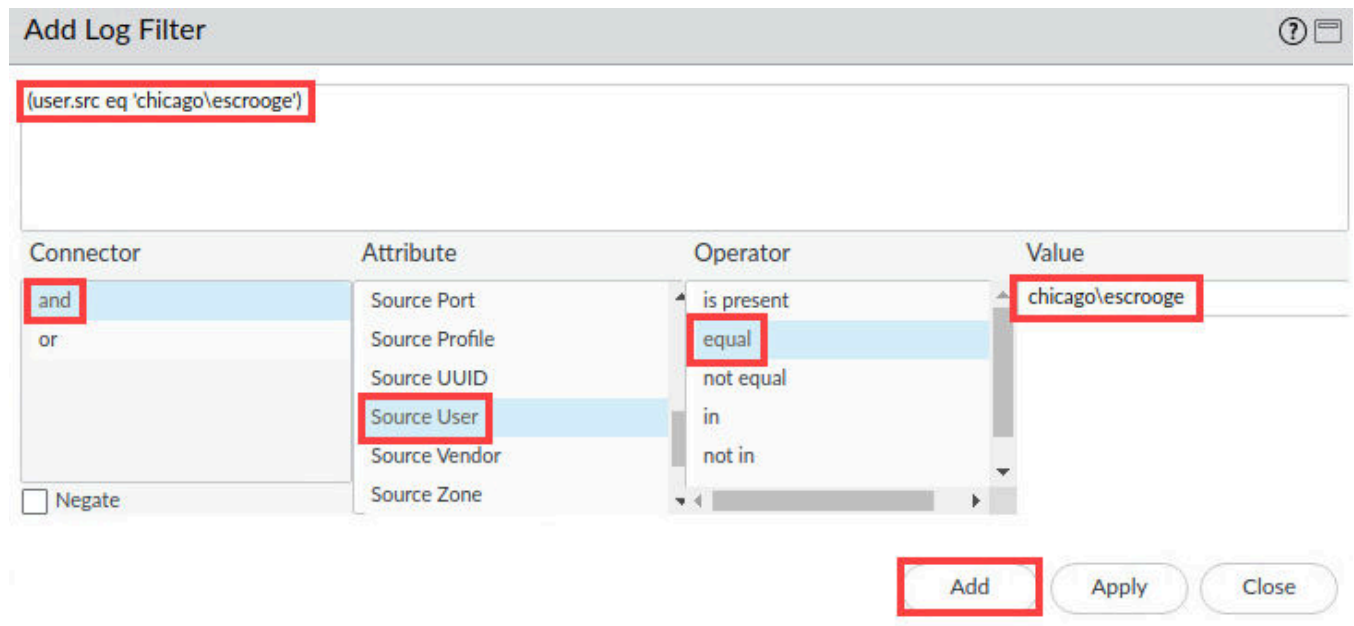


8. Click the **+** icon in the filter area to re-open the **Add Log Filter** window.

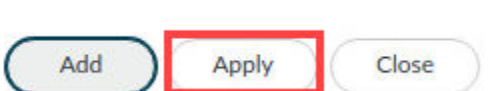


9. In the *Add Log Filter* window, select the following. Click **Add**.

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



10. 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.



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

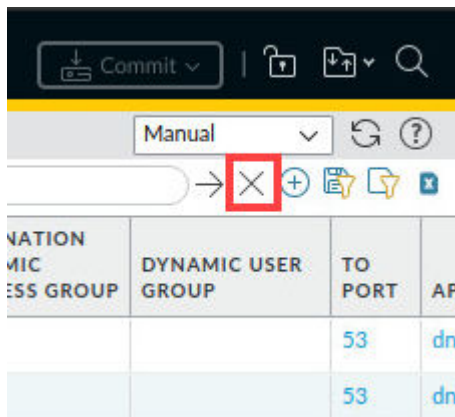


12. Notice the Threat log has been filtered to display only threats from the Source User **Chicago\escrooge**. Some columns have been adjusted to reflect the *Severity* column.

Search: (user.src eq 'chicago\escrooge')

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER
	08/12 14:33:54	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:40	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:40	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:18	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:18	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:12	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge
	08/12 14:33:12	high	spyware	generic:31.smokemenowh...	Acquisition	Acquisition	10.11.2.102	chicago\escrooge

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



Please Note

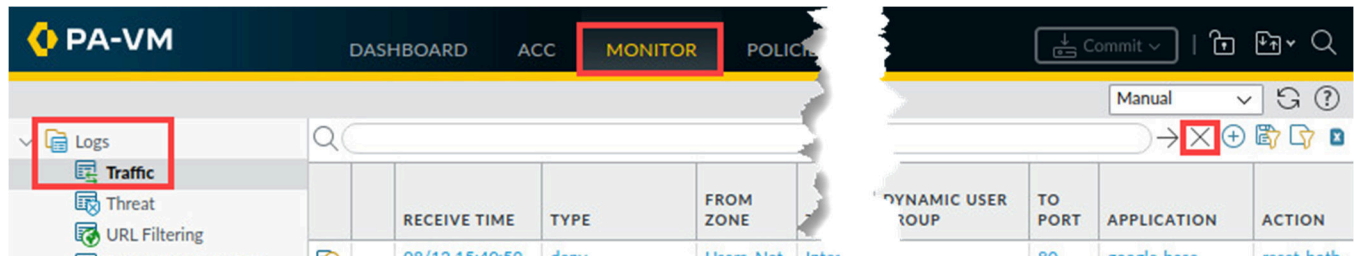
URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

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

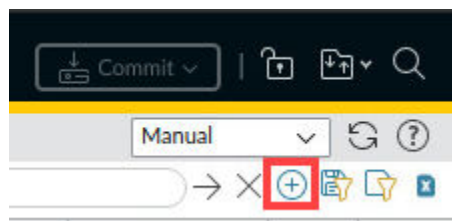
1.8 View Application Information in the Traffic Log

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.

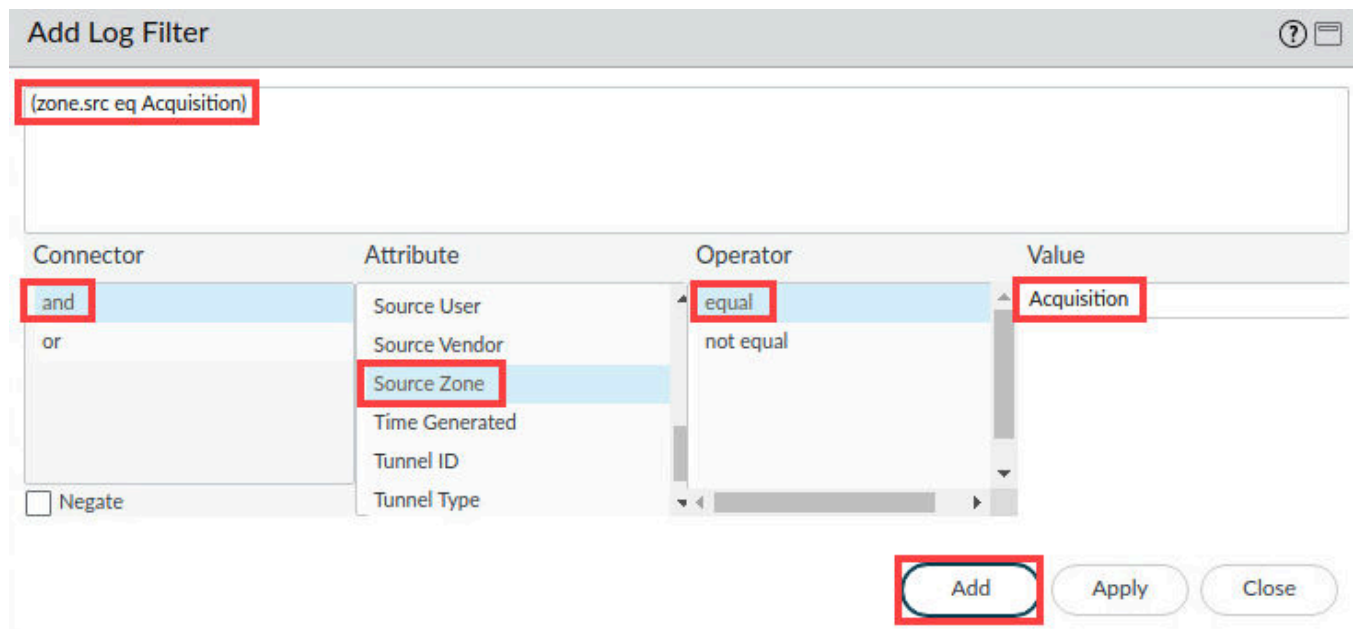


2. Click the **+** icon in the filter area to open the *Add Log Filter* window.



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

Parameter	Value
Connector	and
Attribute	Source Zone
Operator	equal
Value	Acquisition



Add Log Filter

(zone.src eq Acquisition)

Connector	Attribute	Operator	Value
and	Source User	equal	Acquisition
or	Source Vendor	not equal	
	Source Zone		
	Time Generated		
	Tunnel ID		
	Tunnel Type		

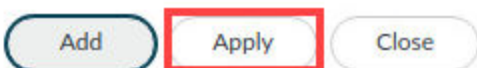
☐ Negate

Add Apply Close

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.



Add **Apply** Close

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



- 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.

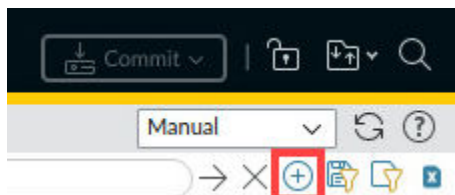
Q (zone.src eq Acquisition)

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER
	08/12 15:37:16	end	Acquisition	Acquisition	192.168.1.104	chicago\mrhyde
	08/12 15:37:16	end	Acquisition	Acquisition	192.168.1.20	chicago\sholmes
	08/12 15:35:43	end	Acquisition	Acquisition	192.168.1.104	chicago\mrhyde
	08/12 15:35:00	end	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot

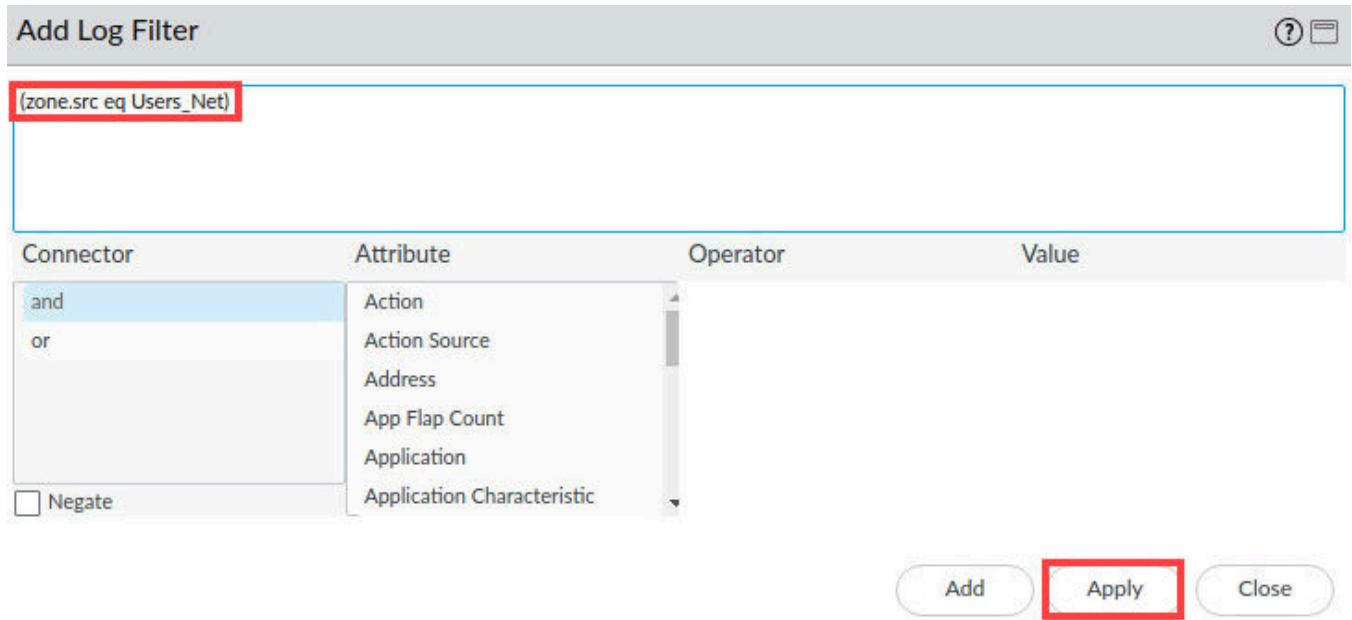
Please Note

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.

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



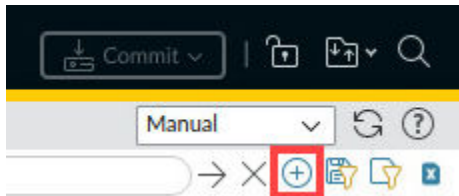
8. In the *Add Log Filter* window in the top pane, modify the existing source zone filter to filter on the *User_Net* zone instead of the *Acquisition* zone. The completed filter should read **(zone.src eq Users_Net)**. Click **Apply**.



The *Add Log Filter* window is shown. The filter text **(zone.src eq Users_Net)** is entered in the top text box. Below the text box is a table with four columns: Connector, Attribute, Operator, and Value. The *Connector* column has a dropdown menu with *and* and *or* options. The *Attribute* column has a dropdown menu with options: *Action*, *Action Source*, *Address*, *App Flap Count*, *Application*, and *Application Characteristic*. There is a *Negate* checkbox. At the bottom right are three buttons: *Add*, *Apply* (highlighted with a red box), and *Close*.

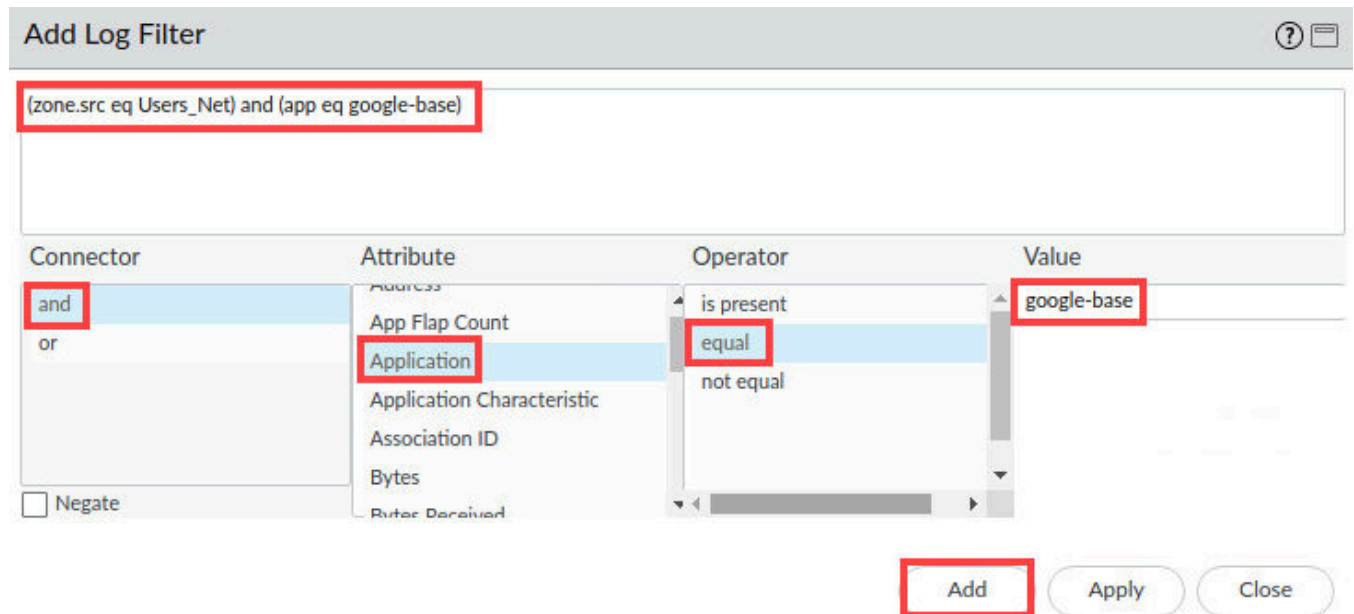
Connector	Attribute	Operator	Value
and	Action		
or	Action Source		
	Address		
	App Flap Count		
	Application		
	Application Characteristic		

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

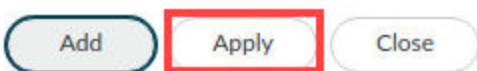


10. In the *Add Log Filter* window, select the following. Click **Add**.

Parameter	Value
Connector	and
Attribute	Application
Operator	equal
Value	google-base



11. 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.



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



13. Notice the Traffic log has been filtered to display only threats from the *From Zone* **Users_Net** and the *Application* **google-base**. Some columns have been adjusted to reflect the *Application* column.

Search: (zone.src eq Users_Net) and (app eq google-base)

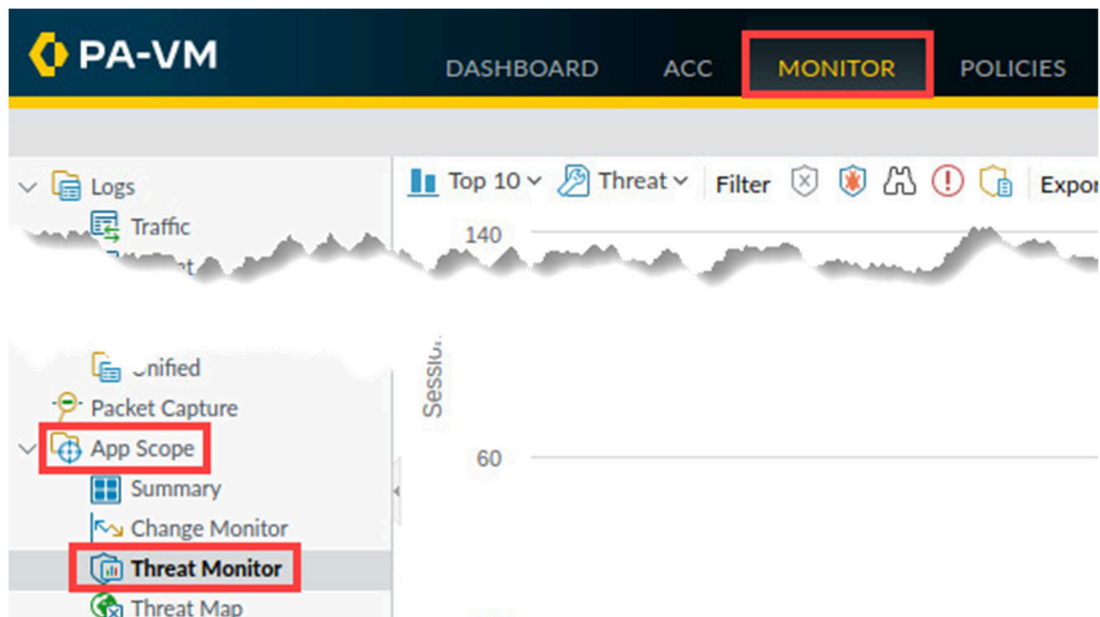
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION
	08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
	08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
	08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	142.250.188.46	80	google-base
	08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
	08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base

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

1.9 View Threats Using App Scope Reports

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

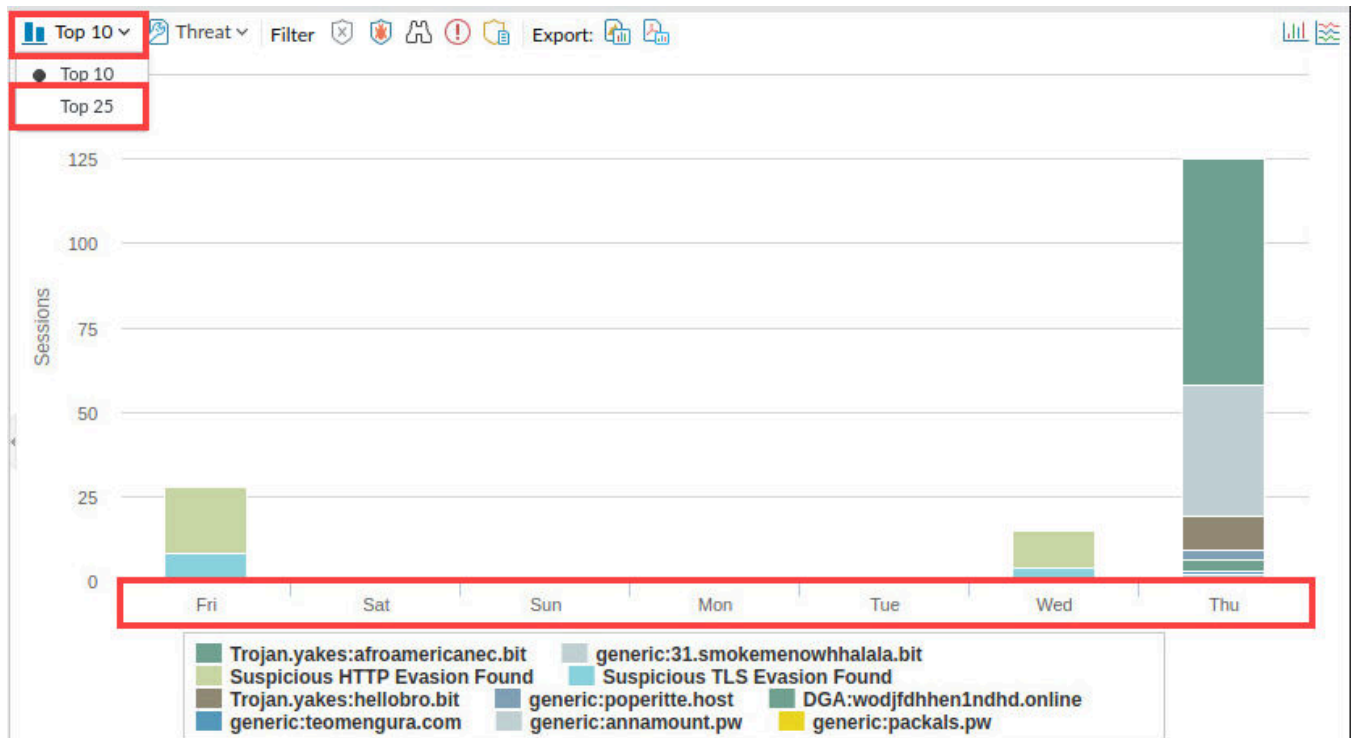
1. Select **Monitor > App Scope > Threat Monitor**.



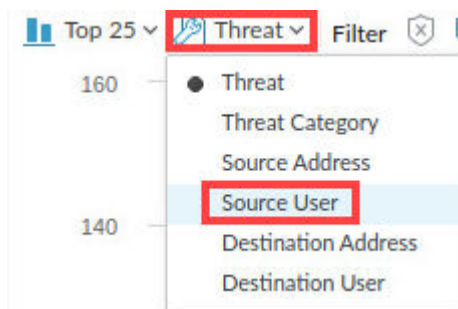
2. At the bottom of the window, click **Last 7 days**.



- The window should update 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.



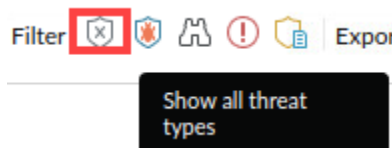
- At the top of the window, click **Threat** and choose **Source User**.



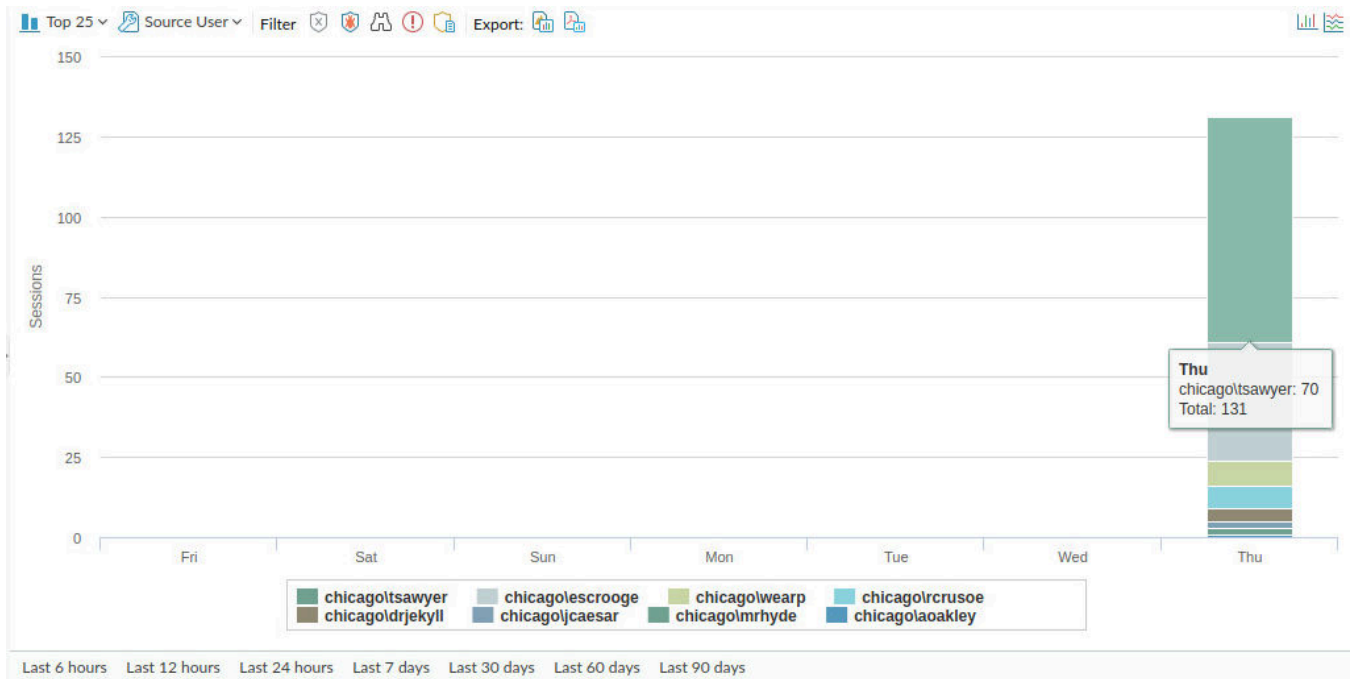
- At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats.



- Select **Show all threat types**.



7. Hover your pointer over the top section of any bar on the bar chart. You should see a pop-up window that shows the threat name and number of detections.



Please
Note

The information you see may differ from the example here.

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