PALO ALTO NETWORKS EDU 210

Lab 16: Viewing Threat and Application Information

Document Version: 2022-07-19

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.

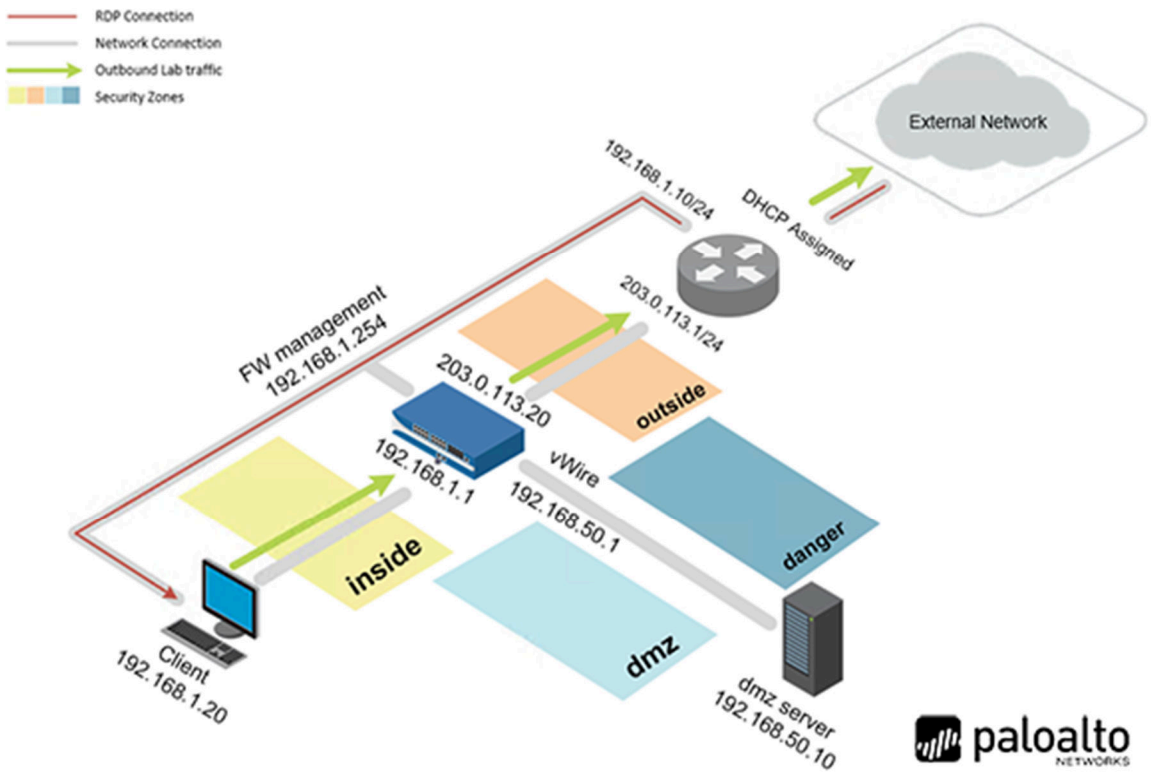
You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

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

Lab Topology



Lab Settings

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

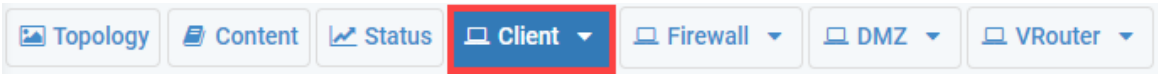
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Blocking Threats in Encrypted Traffic

1.1 Apply a Baseline Configuration to the Firewall

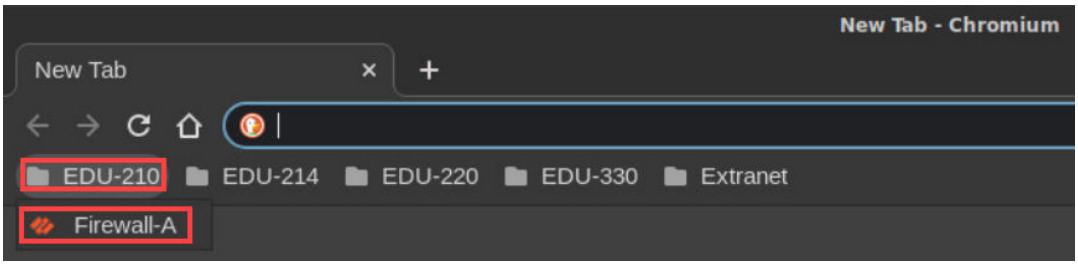
In this section, you will load the Firewall configuration file.

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

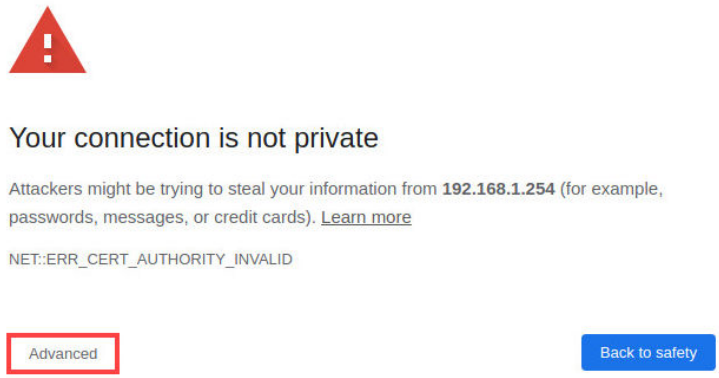


2. Double-click the **Chromium Web Browser** icon located on the desktop.

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

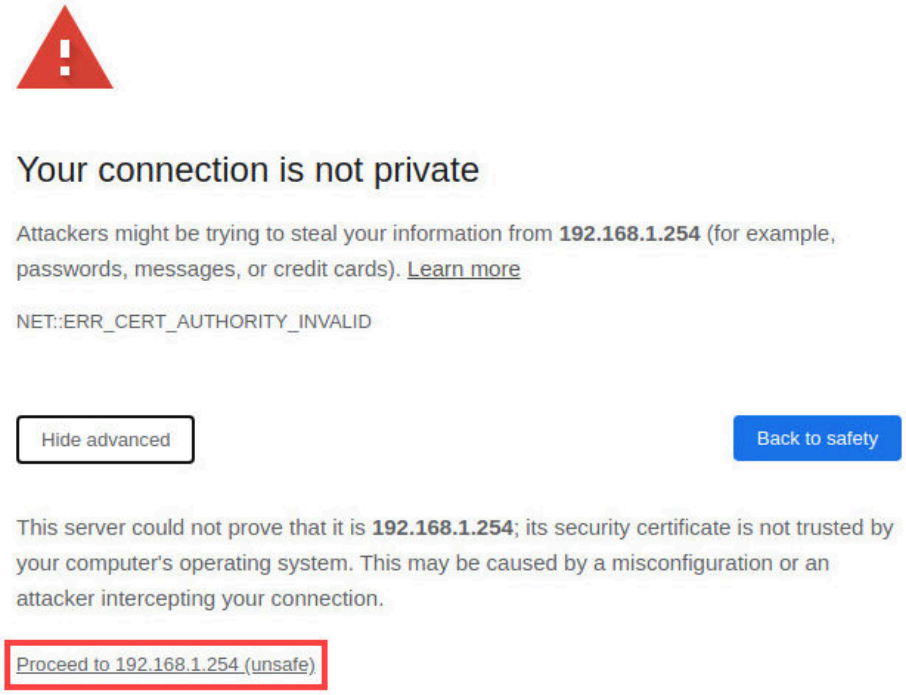


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



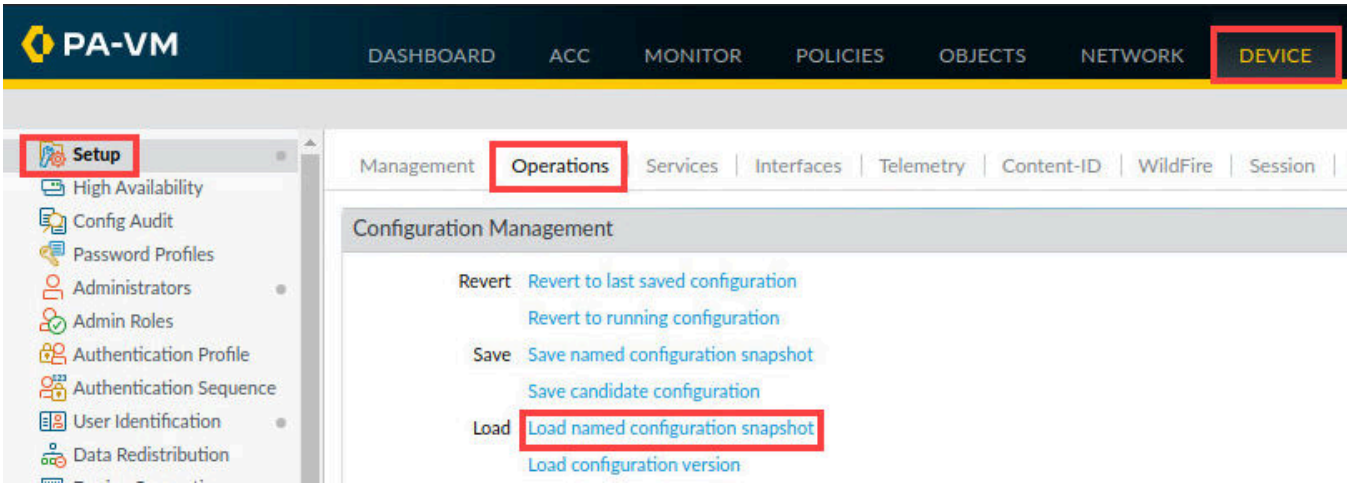
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

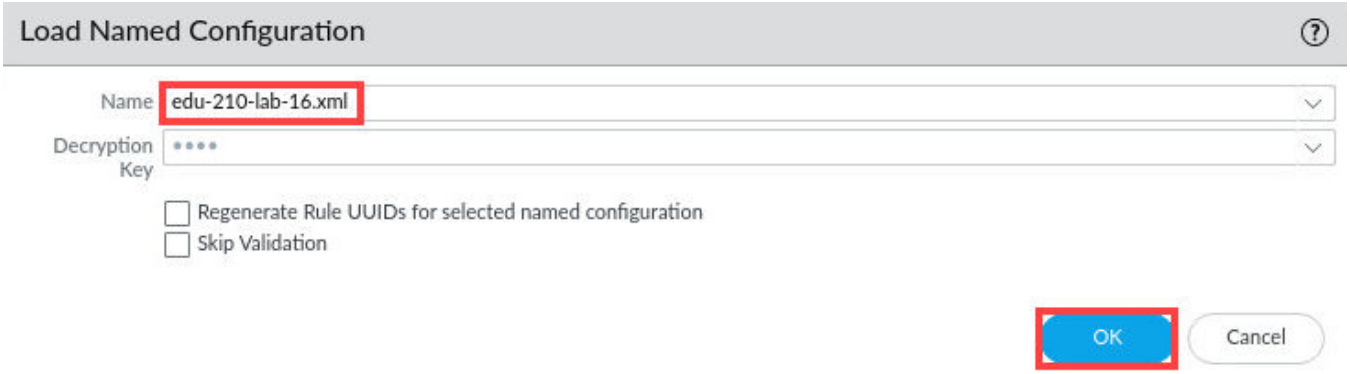


6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

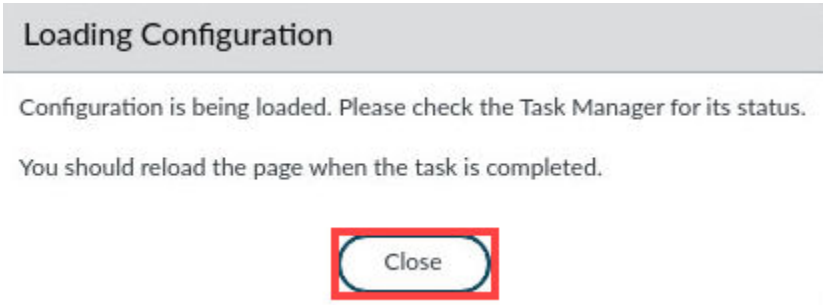
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



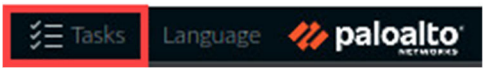
8. In the *Load Named Configuration* window, select **edu-210-lab-16.xml** from the *Name* dropdown box and click **OK**.



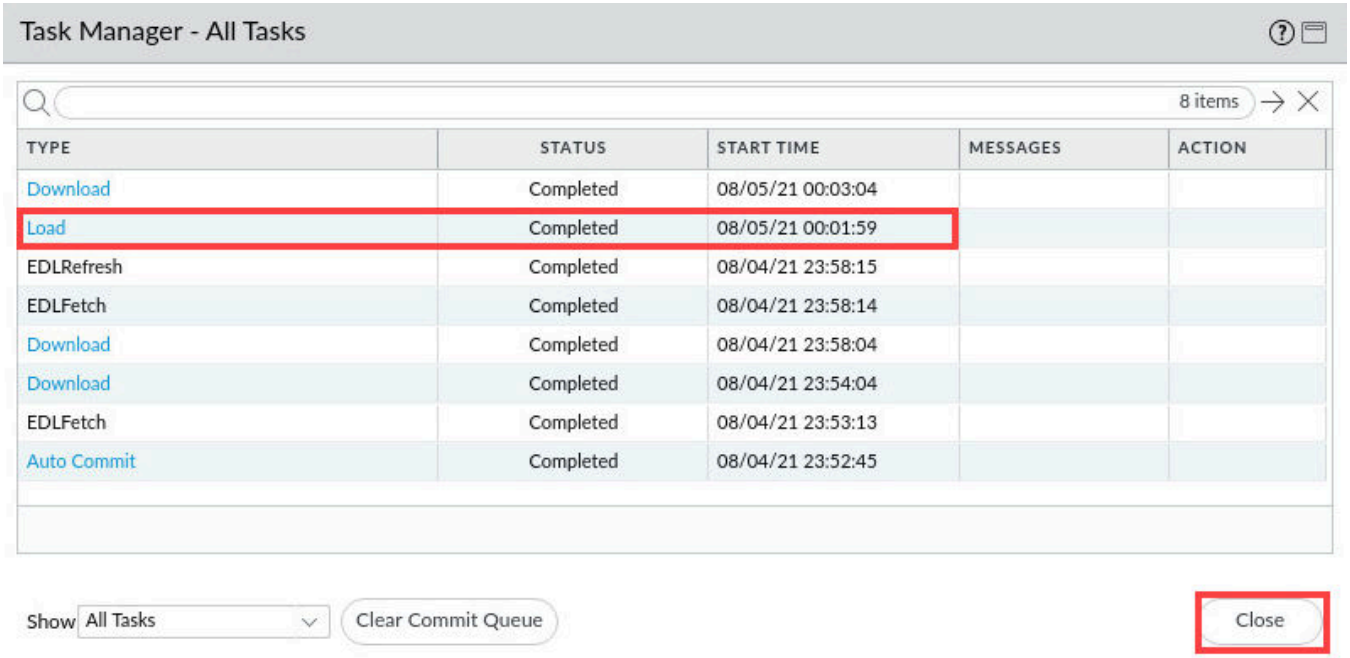
9. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



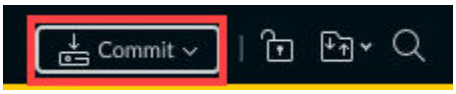
10. Click the **Tasks** icon located at the bottom-right of the web interface.



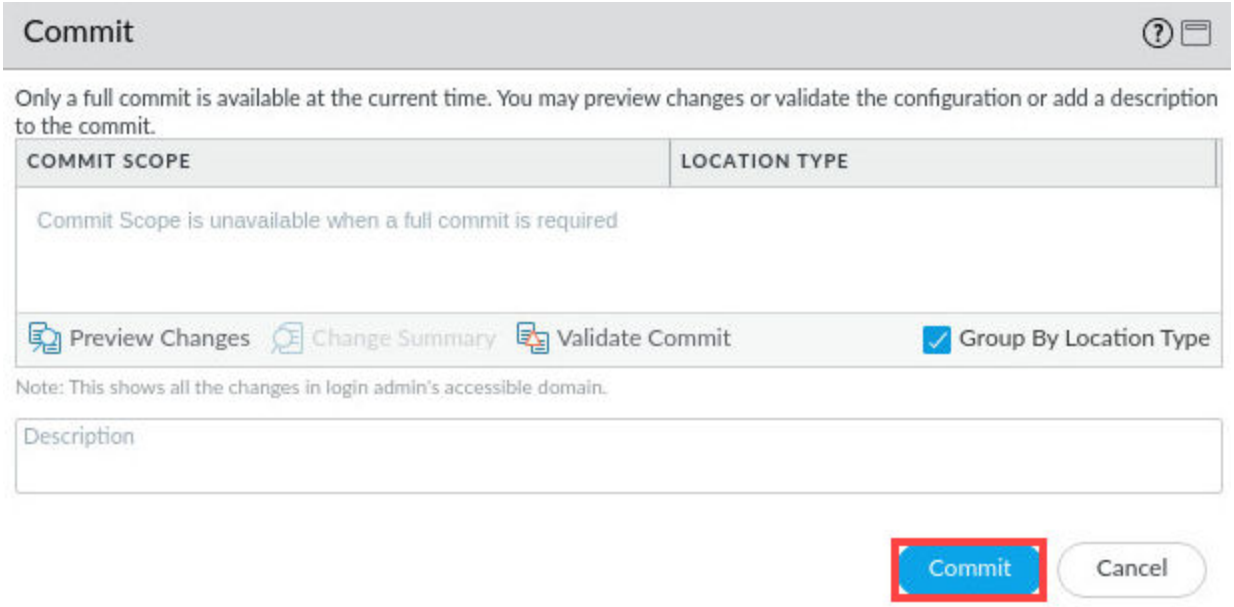
11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



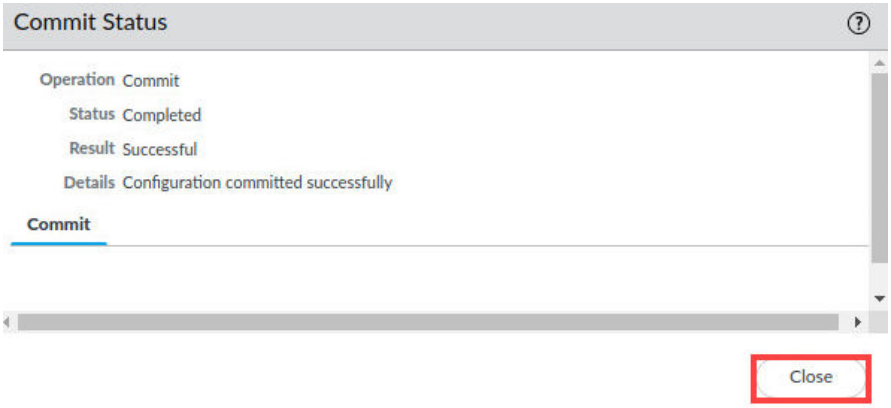
12. Click the **Commit** link located at the top-right of the web interface.



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

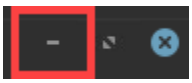


14. When the commit operation successfully completes, click **Close** to continue.



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

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

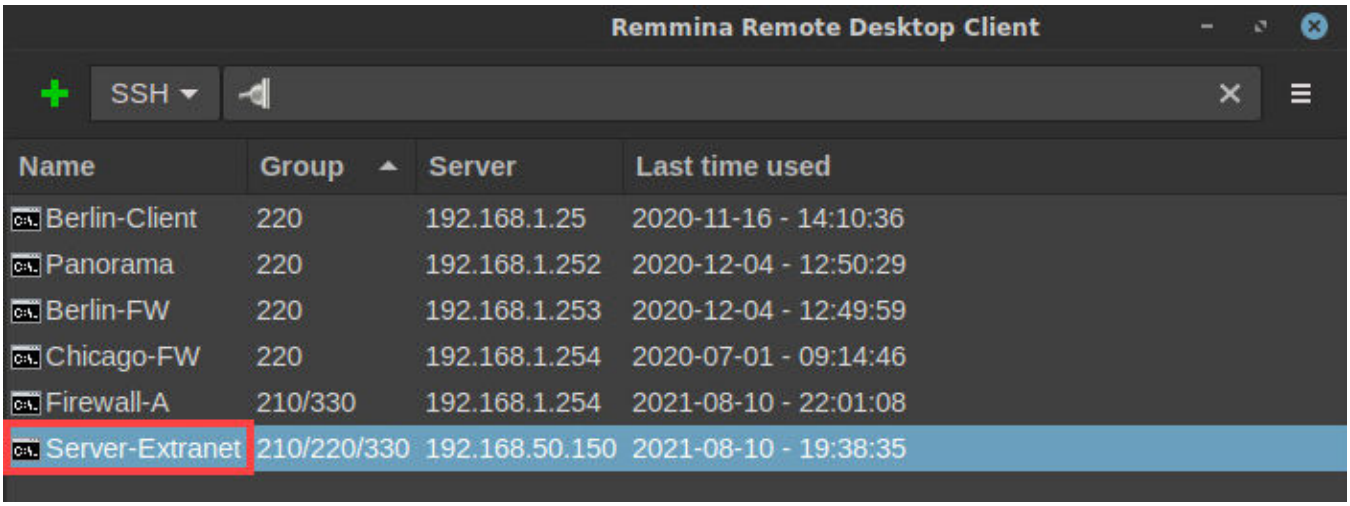


1.2 Generate Traffic

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.

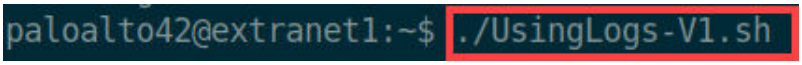
2. Double-click the entry for **Server-Extranet**.



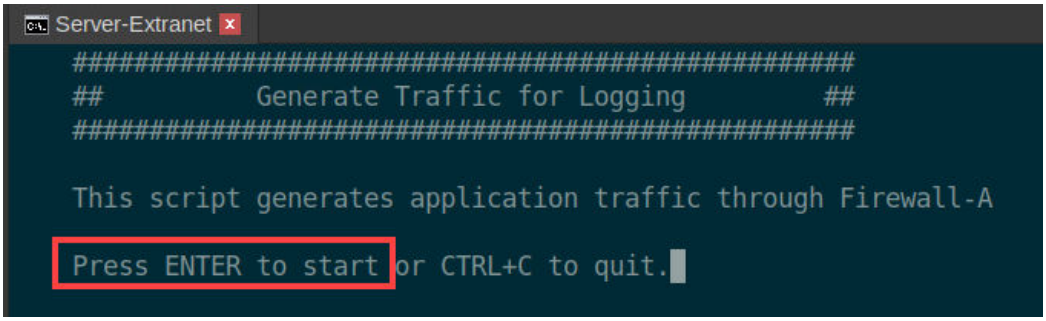
> **Please Note**
> This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

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

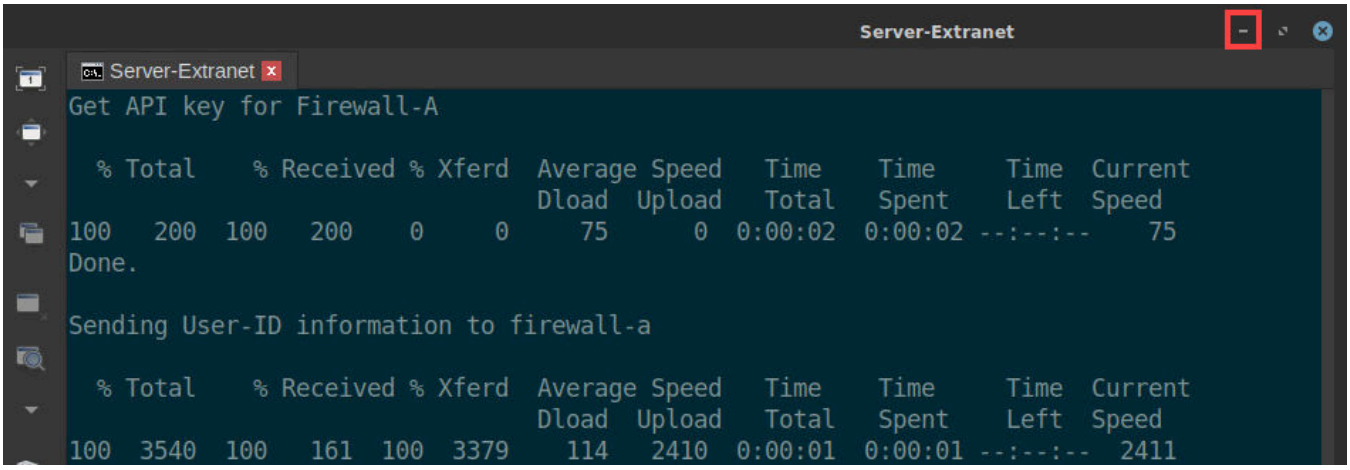
```
paloalto42@extranet1:~$ ./UsingLogs-V1.sh <Enter>
```



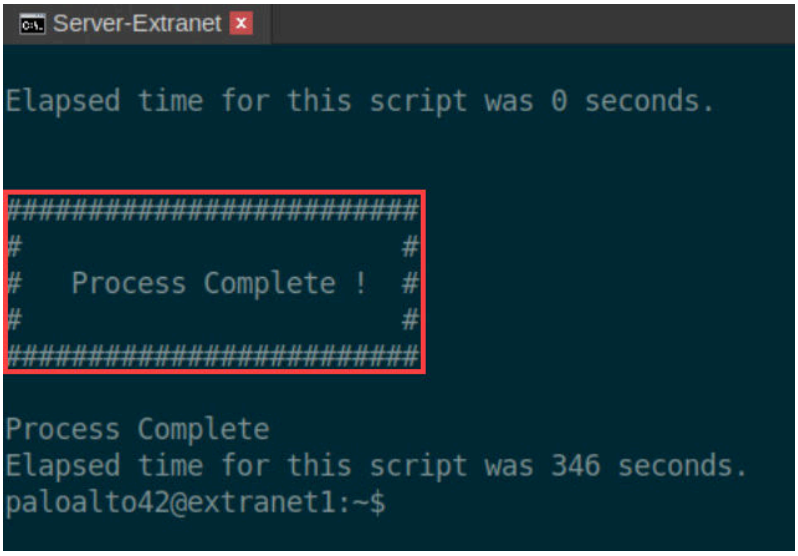
4. Press **Enter** to start the *UsingLogsV1.sh* script.



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



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



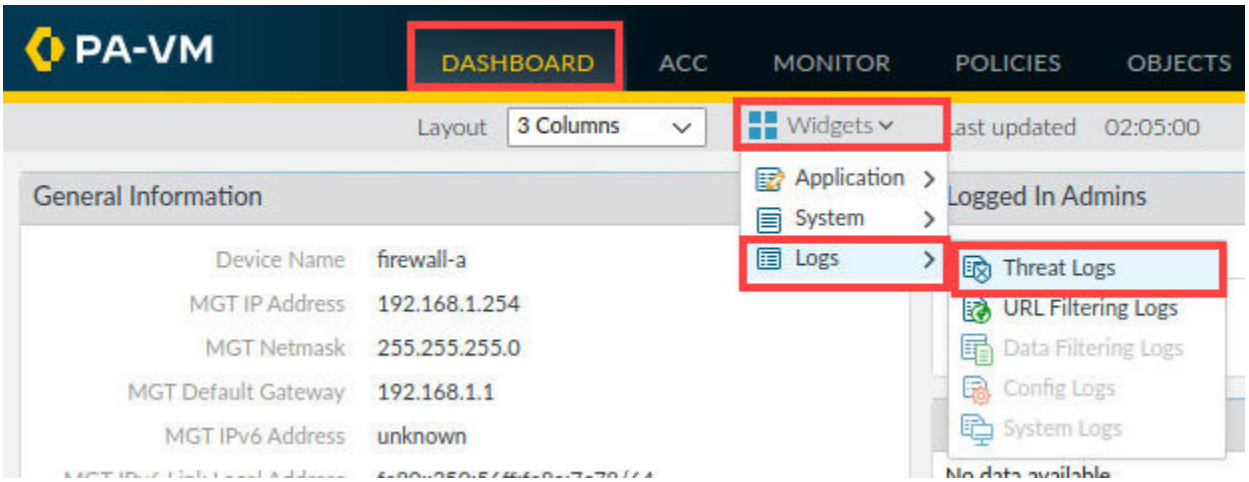
6. Re-open the *PA-VM firewall* by clicking on the **Chromium** icon in the *Taskbar*.

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

1.3 Display Recent Threat Information in the Dashboard

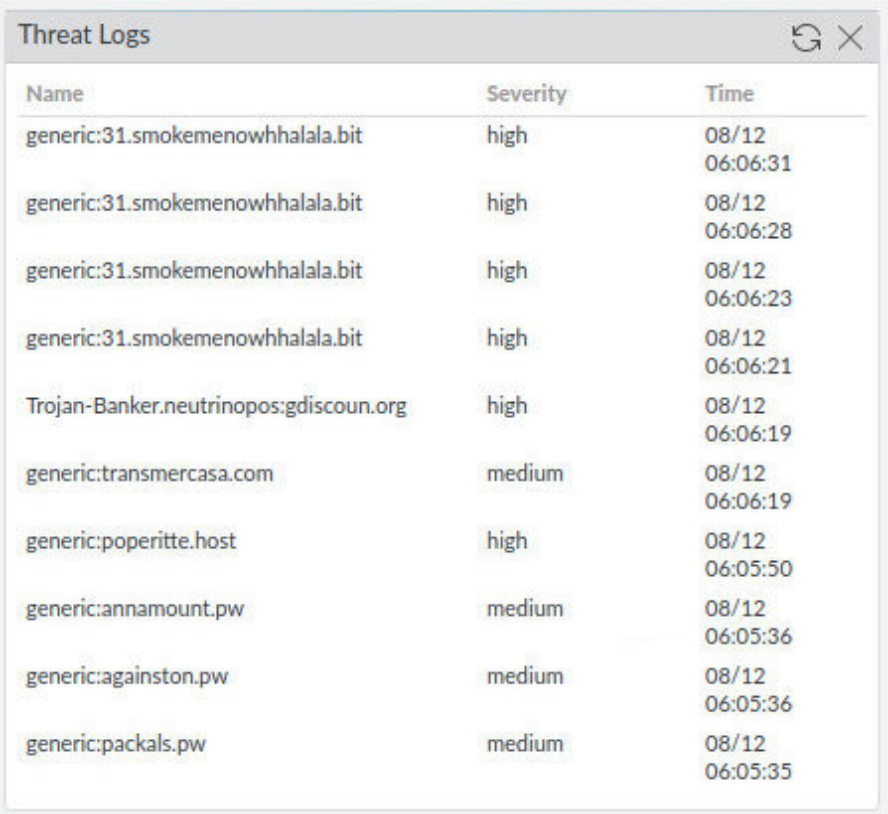
You will use the Dashboard to view threats detected by the firewall in the last hour. Because you can configure the Dashboard to periodically refresh, the displayed threats will change, depending on the most recent information available. The Dashboard information is sourced from the Threat, URL Filtering,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

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



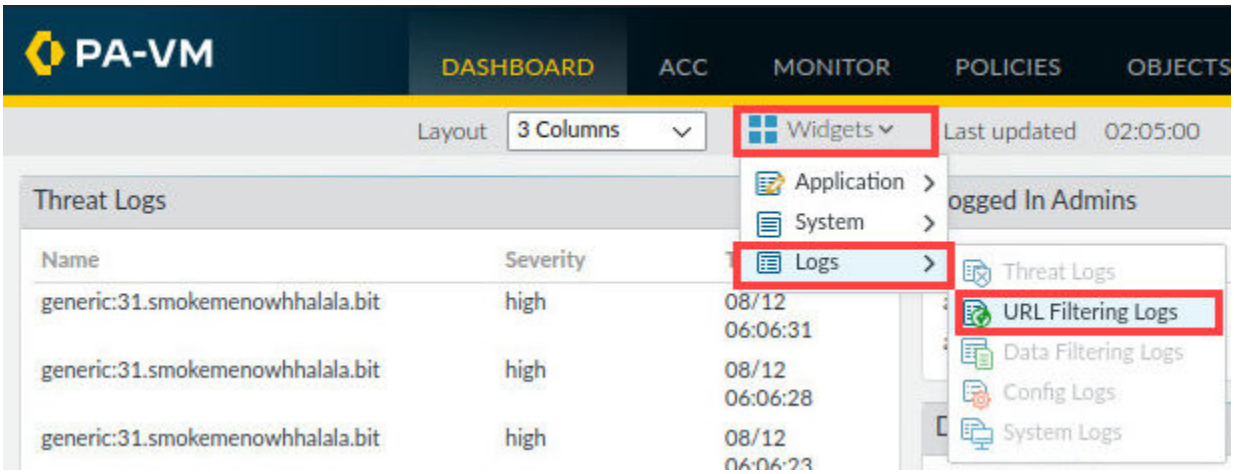
Threat Logs

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:against on.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.

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.

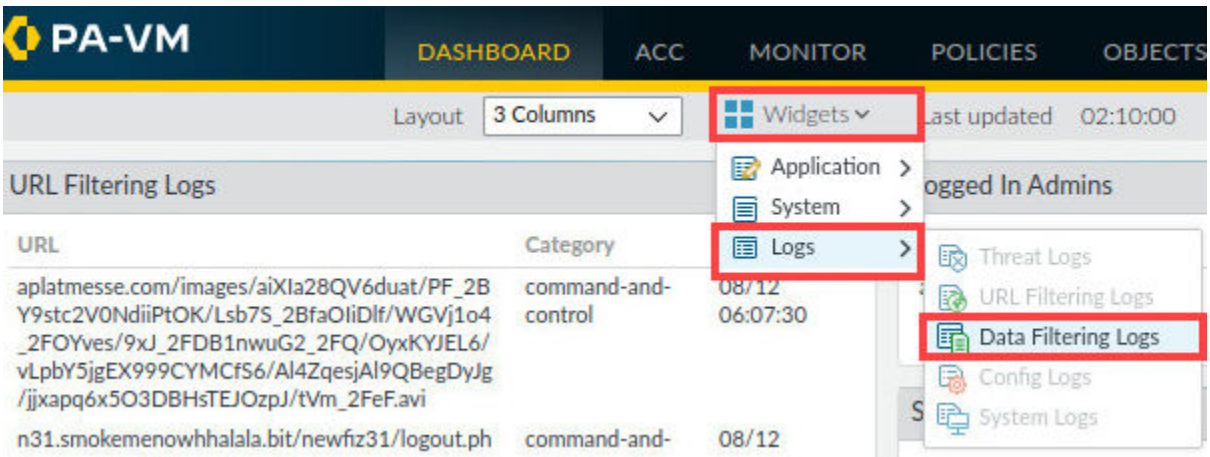
URL Filtering Logs

URL	Category	Time
aplatmesse.com/images/aiXIa28QV6duat/PF_2BY9stc2V0NdiiPtOK/Lsb7S_2BfaOIiDlf/WGVj1o4_2FOYves/9xJ_2FDB1nwuG2_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
against on.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

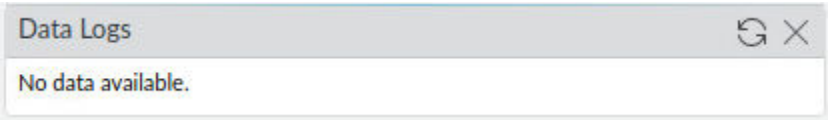
Please Note

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.

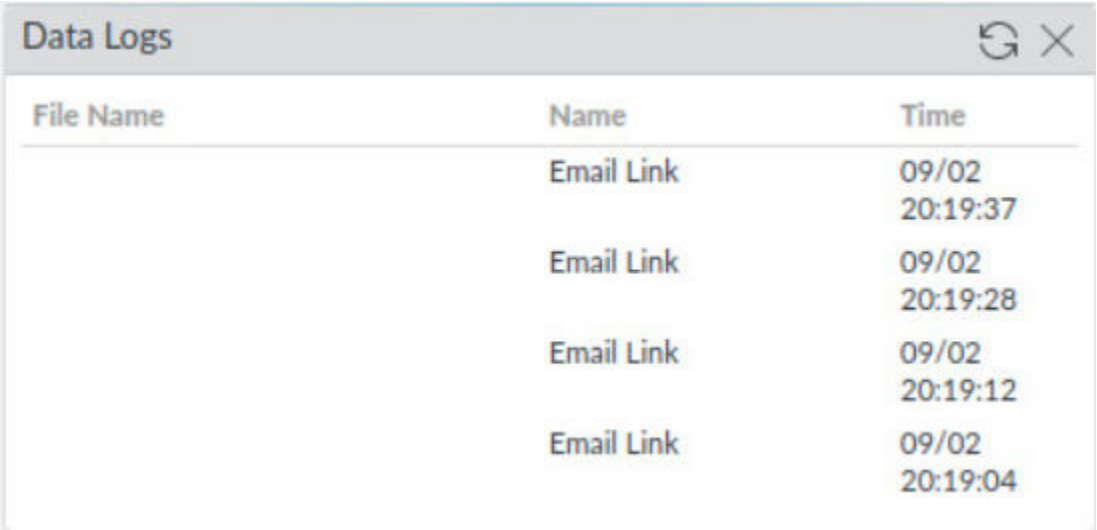
5. Click **Widgets** and select **Logs > Data Filtering Logs** if it is not already selected.



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 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.

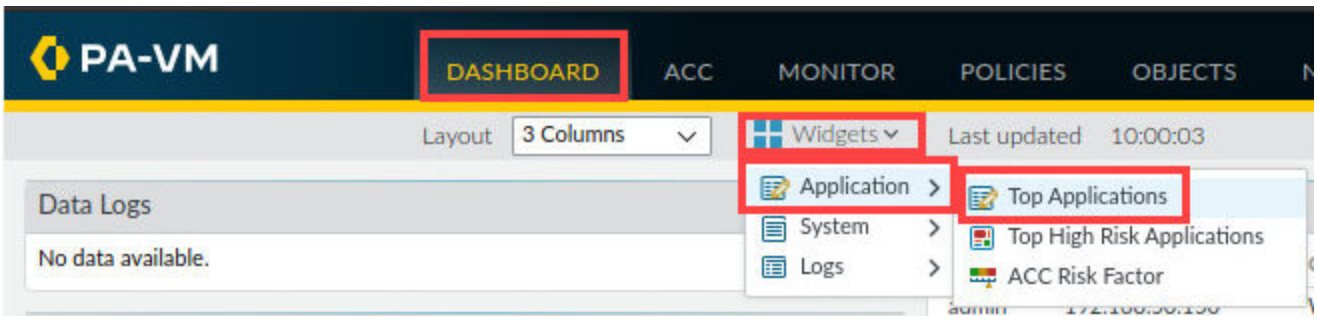


7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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.

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

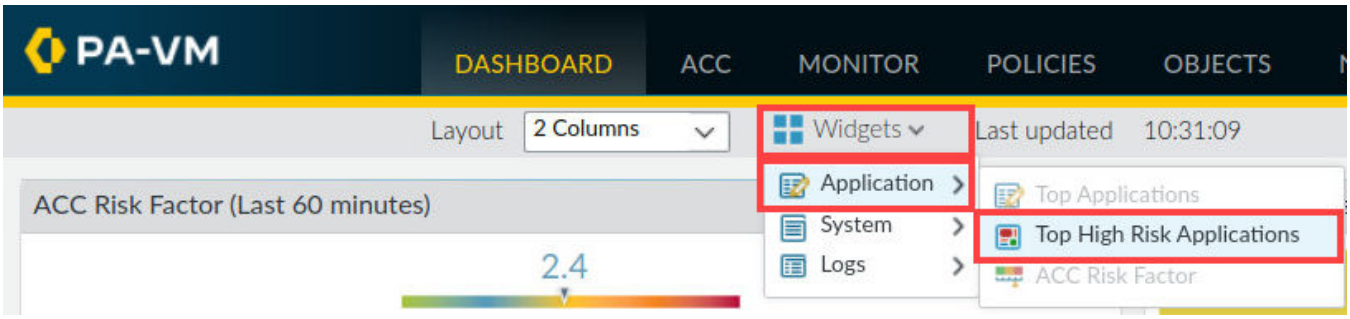


2. Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour.

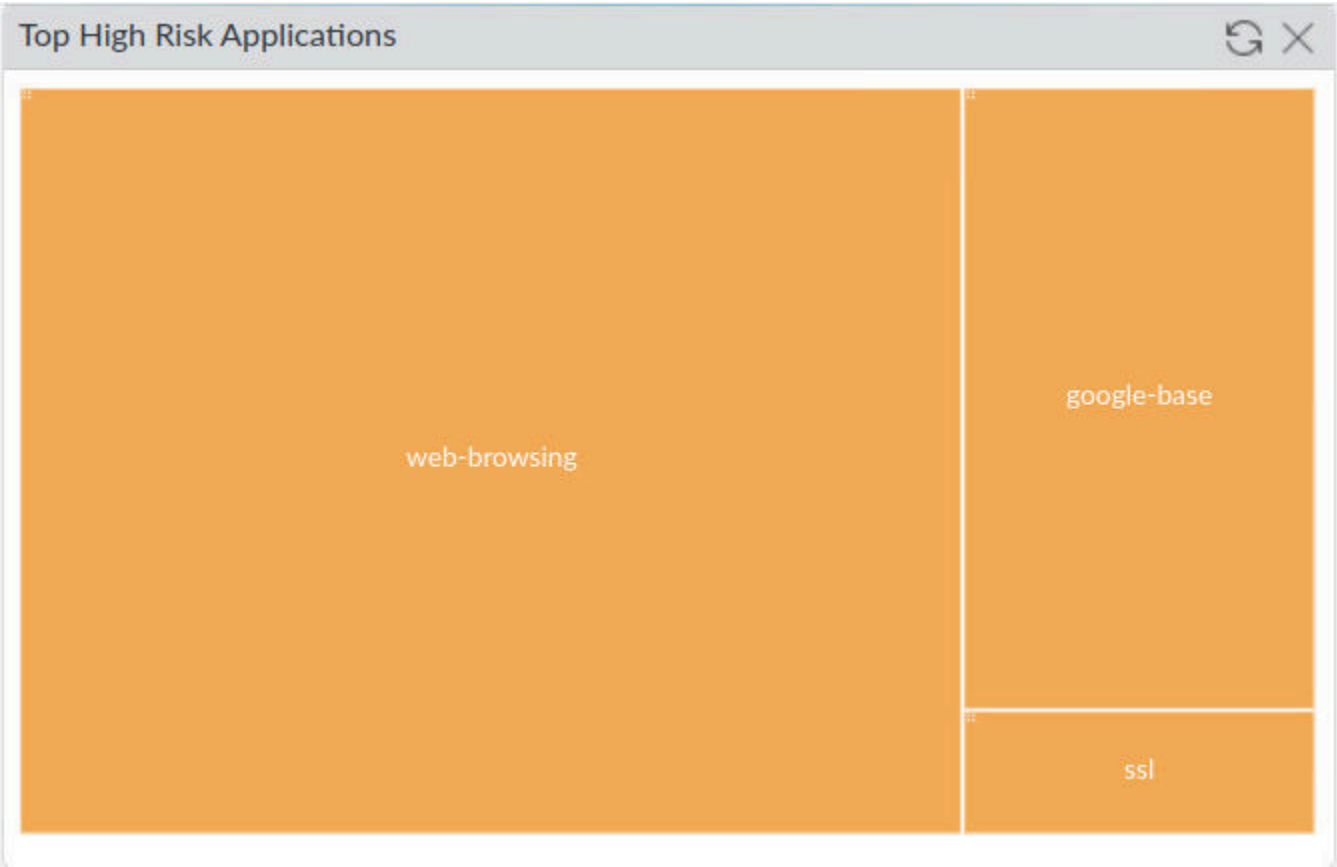
Please Note

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.



Please Note

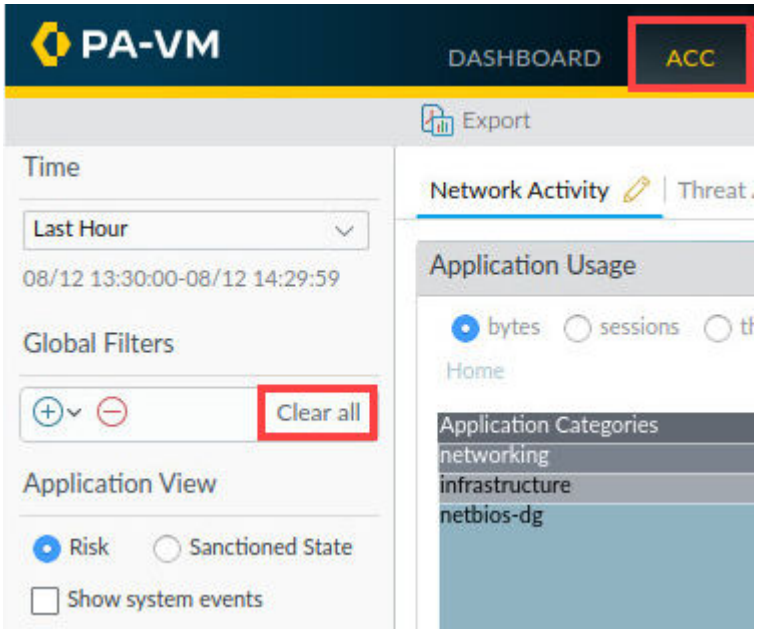
Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. If the Top High Risk and Top Applications have not updated, please allow 3 to 5 minutes for the widgets to update.

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

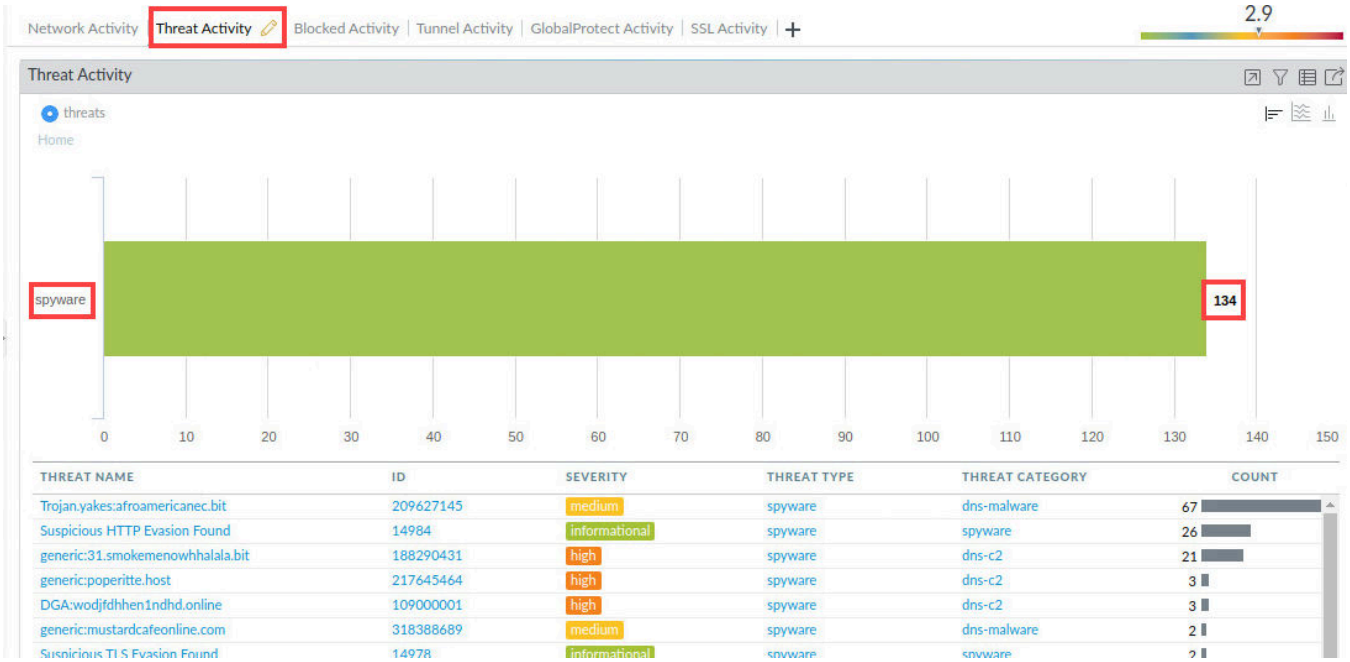
1.5 View Threat Information in the ACC

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.

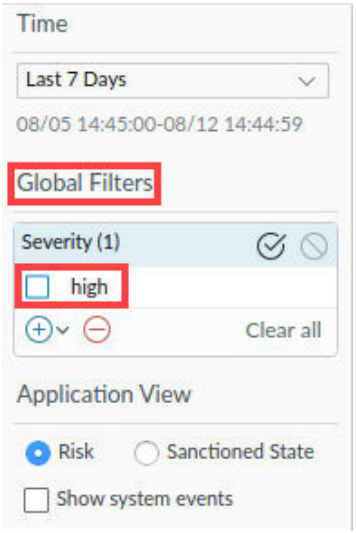
3. In the **Threat Activity** widget's table below the graph, click the small arrow icon next to one of the *Severity* level entries. For this step, we chose to use the **high** *Severity* level.

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:hellobro.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

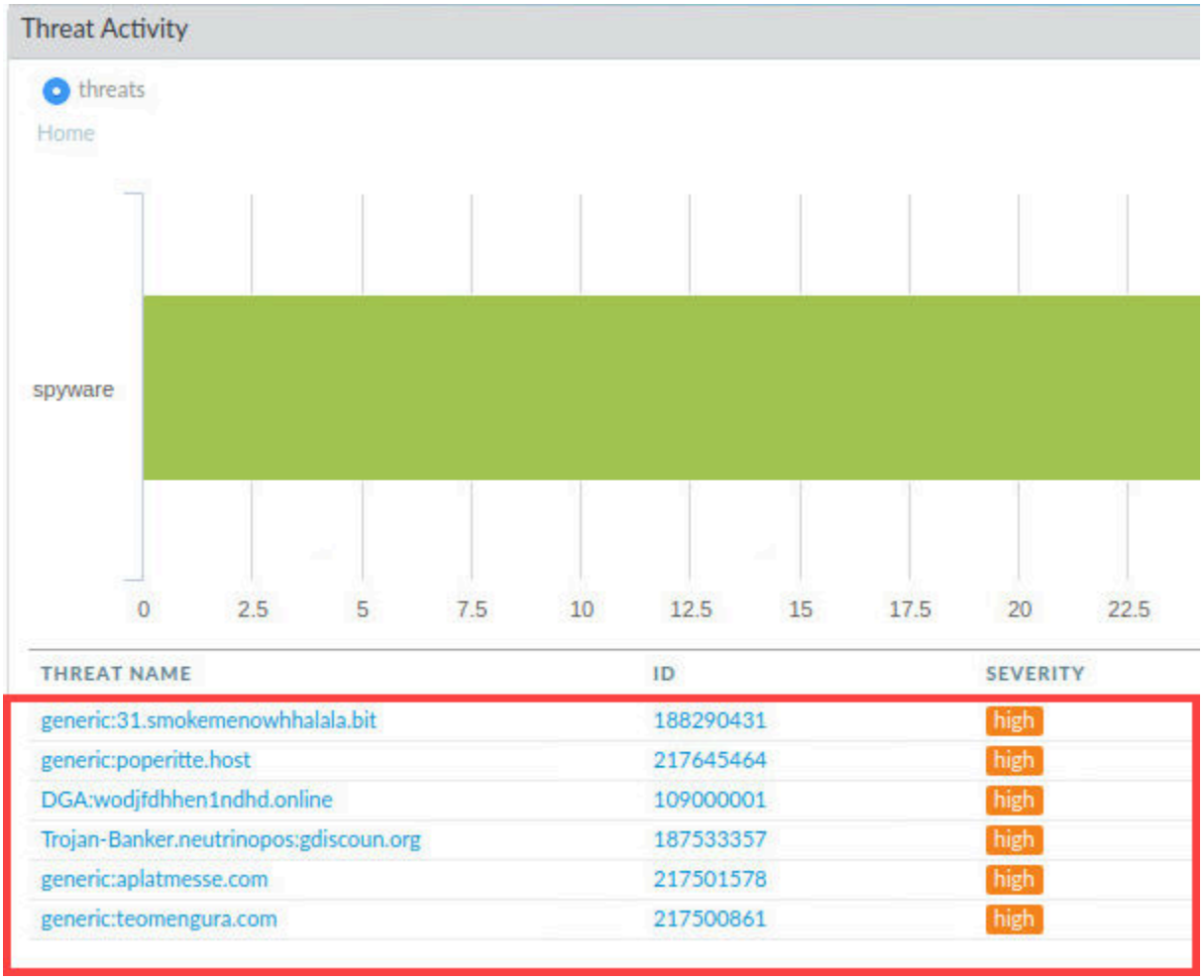
Please Note

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.

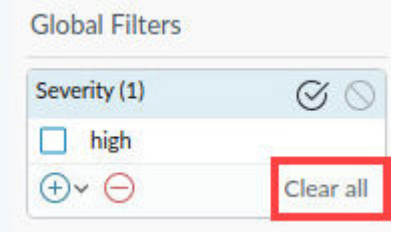
4. Find the global filter on the left side of the *ACC* window. Notice **high** was added as a global filter condition.



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



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

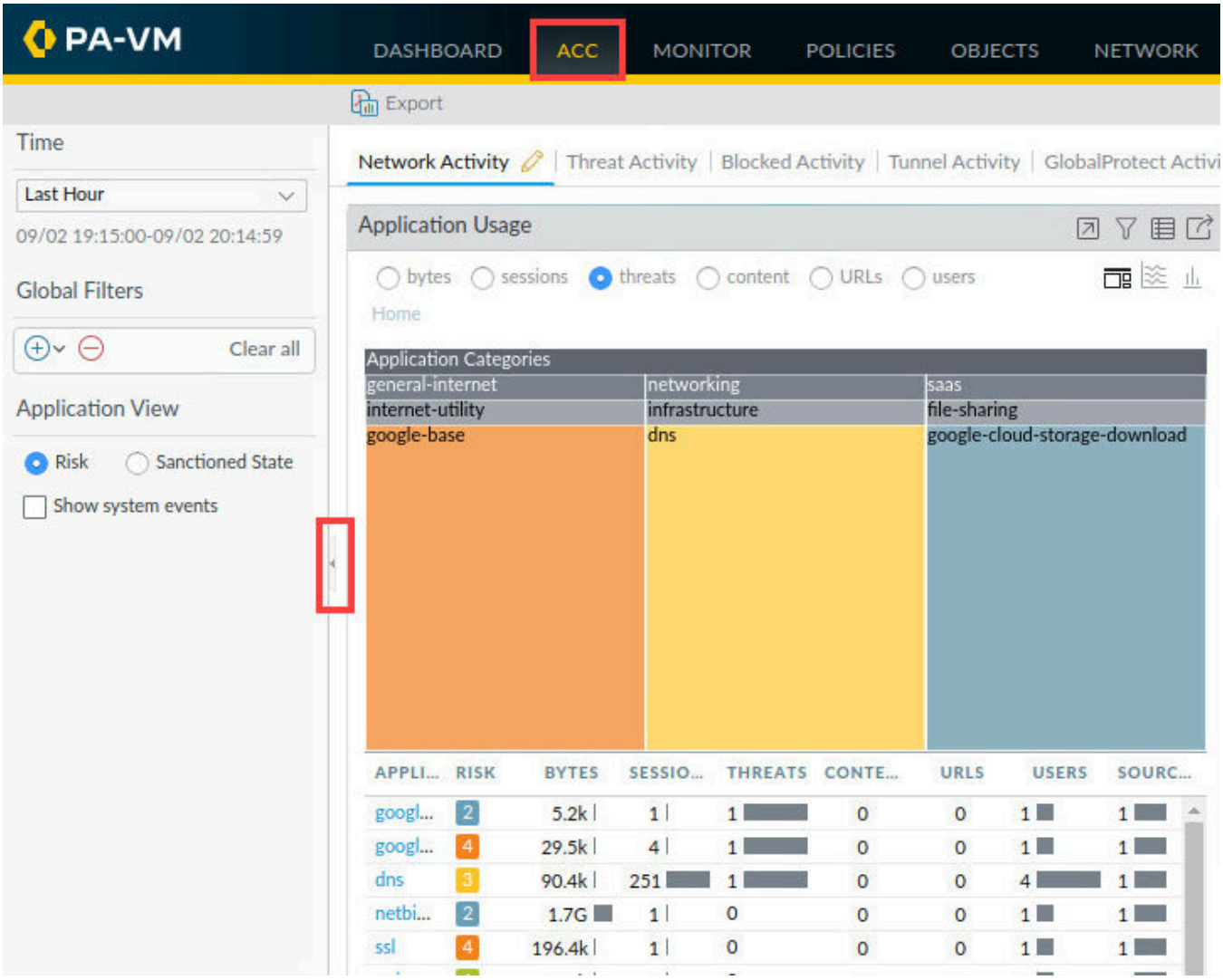


7. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

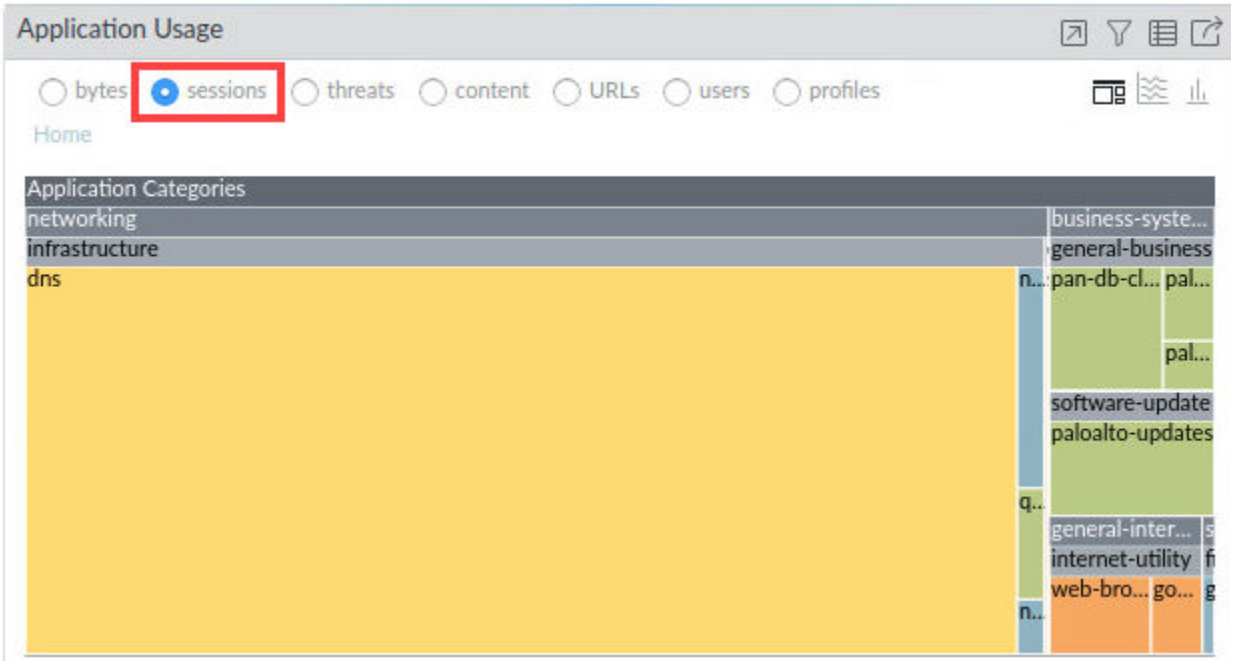
1.6 View Application Information in the ACC

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.

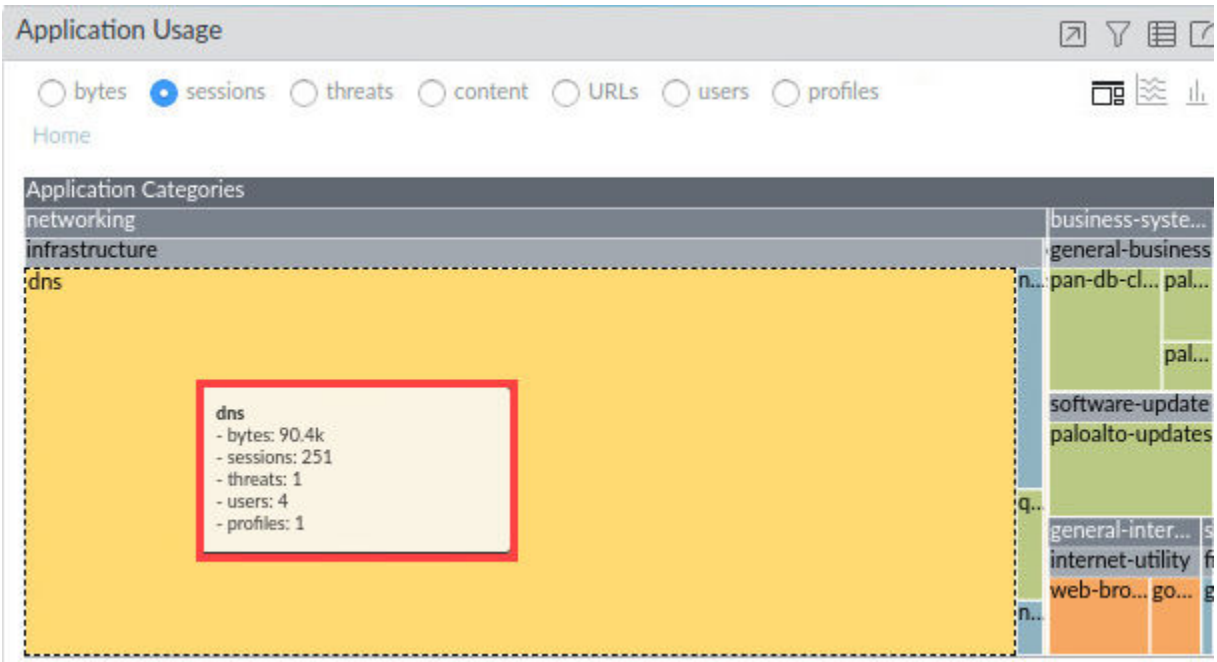
1. In the web interface, click the **ACC** tab and then the **Network Activity** tab. Hide the sidebar to make more room for the widgets by clicking the very small arrow shown.



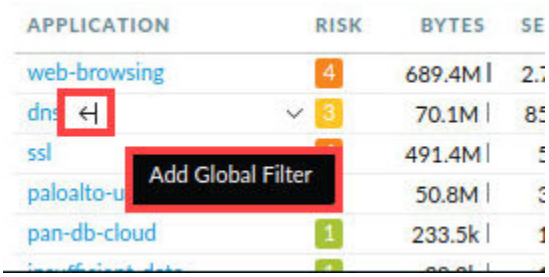
2. The top section of the **Application Usage** widget is a graph that illustrates how much of the traffic a specific application represents. Select the **sessions** radio button.



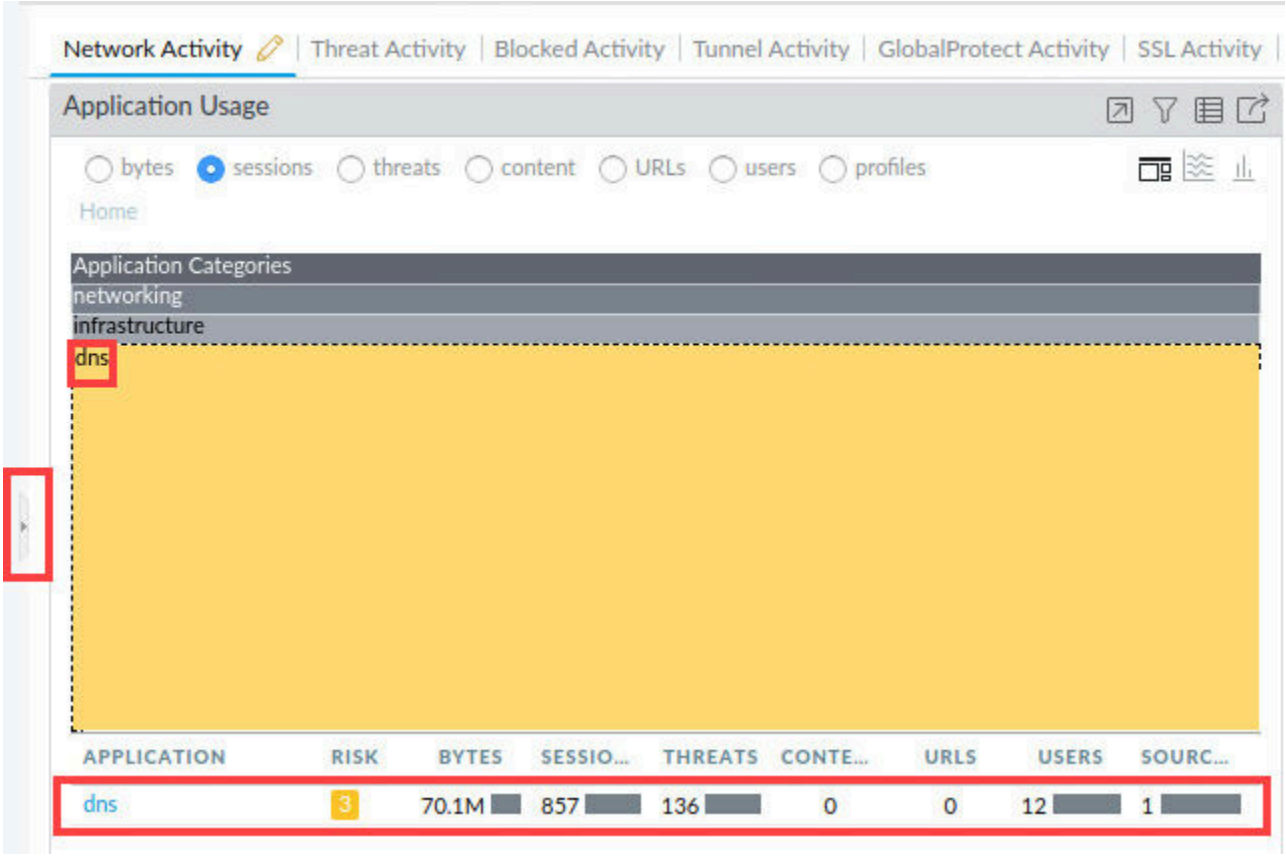
3. Hover your pointer over the section for **dns**. This action displays a summary window with information about that application.



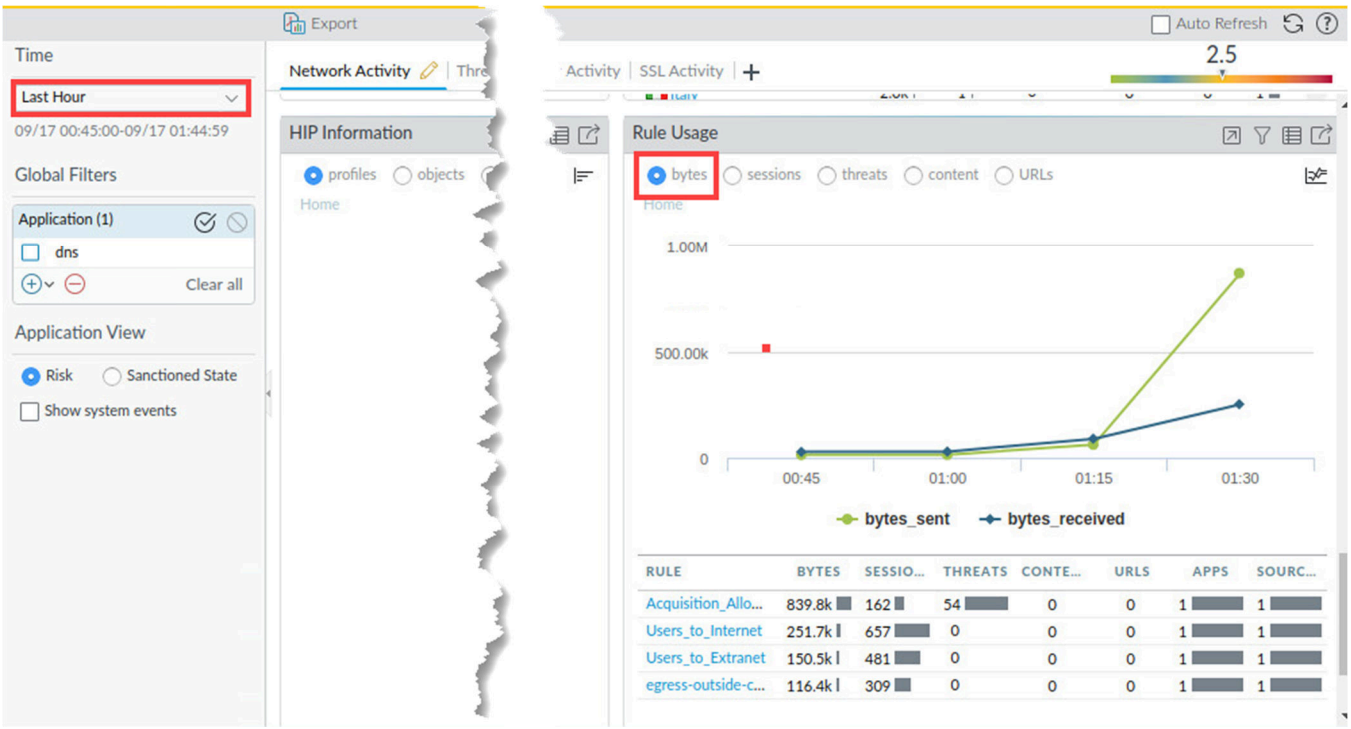
4. In the table below the graph, hover your pointer over the **dns** application until the global filter **left arrow** appears. Then click the **Left arrow** to promote the **dns** application to a global filter.



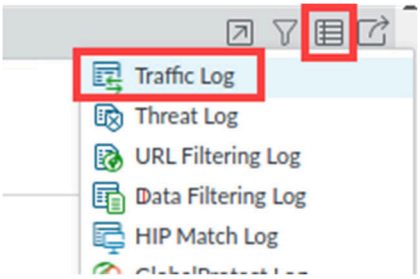
5. Unhide the sidebar by clicking the *tiny* arrow again**.** Notice the *Application Usage* chart has been upgraded to show the **dns** application.



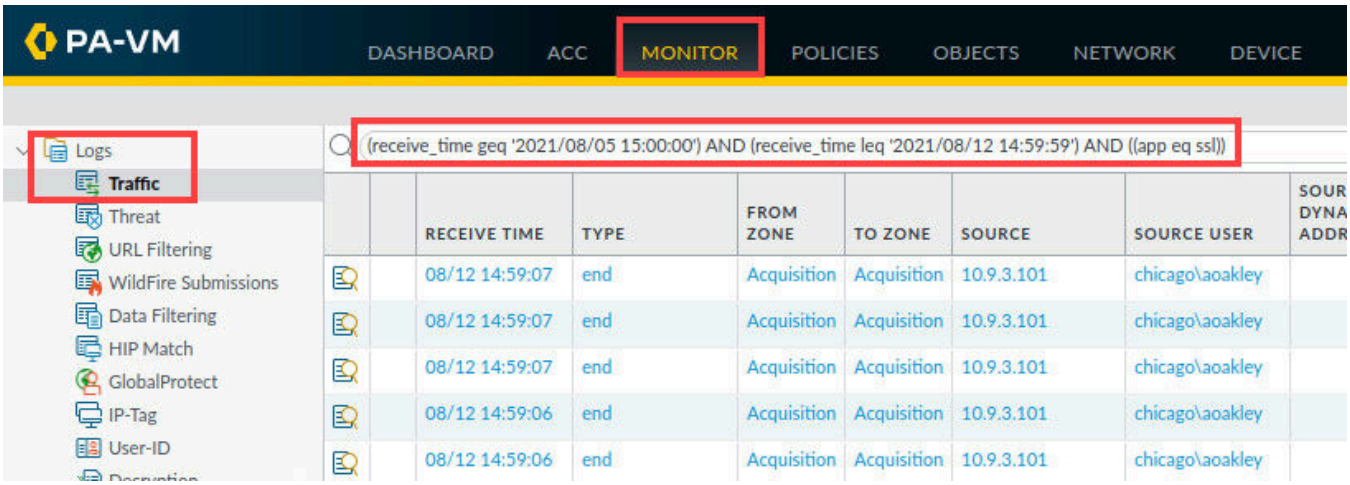
6. Scroll down in the **Network Activity** tab until you reach the **Rule Usage** widget**.** Select the radio button at the top for **Bytes.** In the *Time* column, select **Last Hour**.



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.

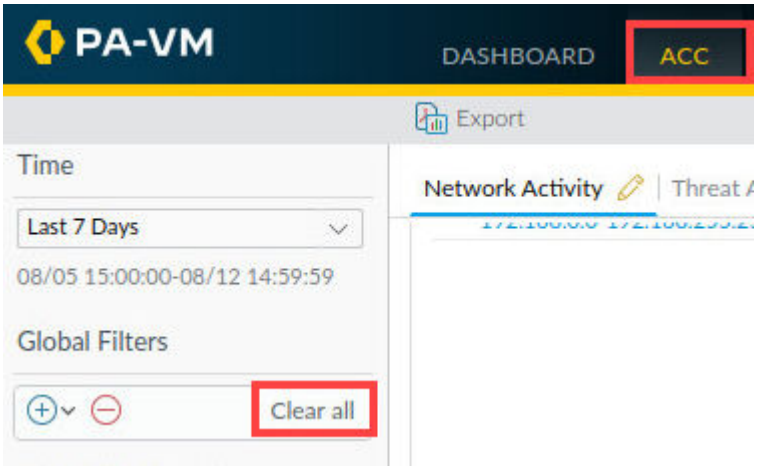


8. Notice it navigated you to **Monitor > Logs > Traffic**. There should be a time range filter and an application filter for web browsing. The time range filter is derived from the time specified in the ACC. Note that the entries displayed in the Traffic log match the filter



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.

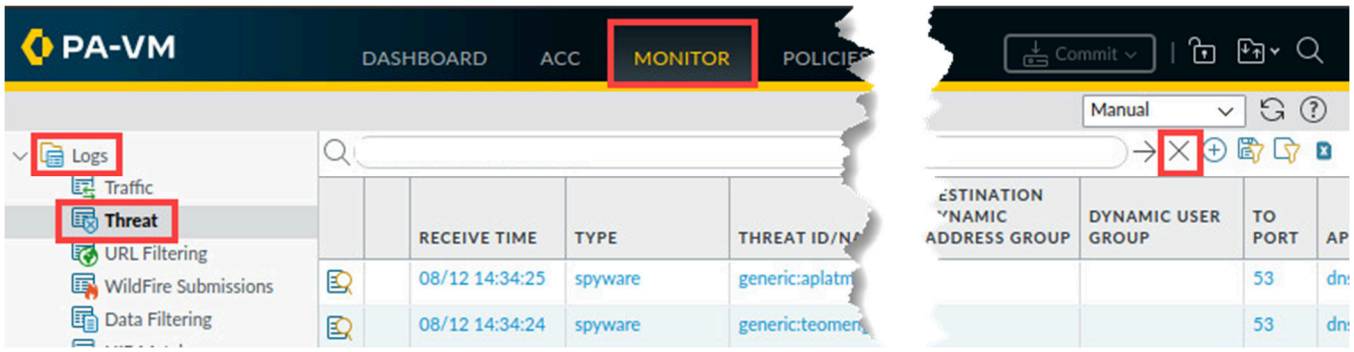


11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

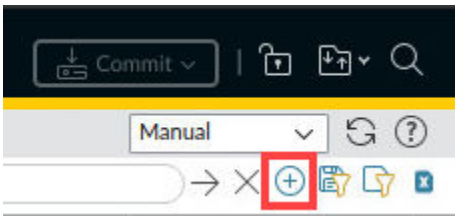
1.7 View Threat Information in the Threat Log

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.

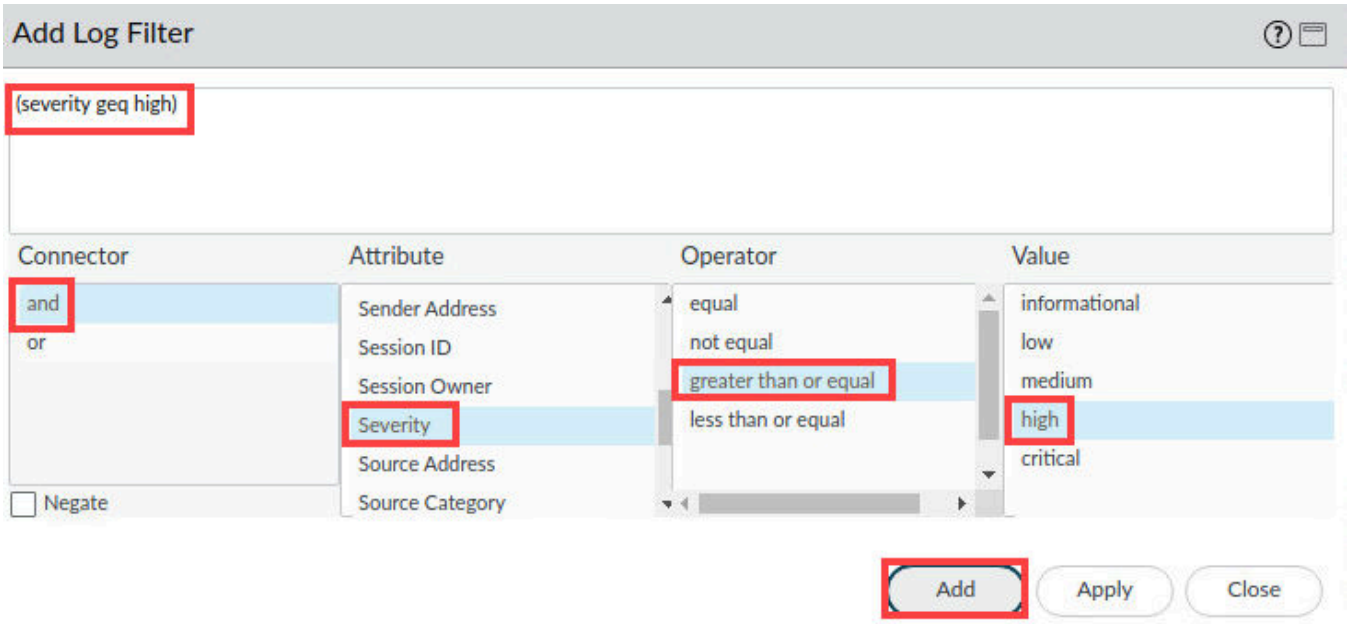


2. Click the **+** icon in the filter area to open the *Add Log Filter* window.

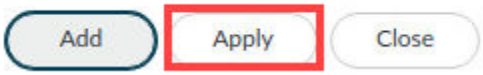


3. In the *Add Log Filter* window, select the following. Click **Add**.

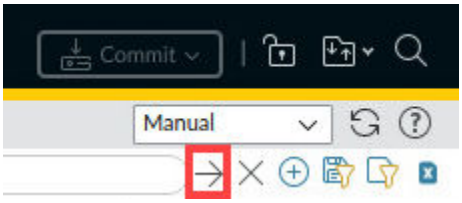
Parameter	Value
Connector	**and**
Attribute	**Severity**
Operator	**greater than or equal**
Value	**high**



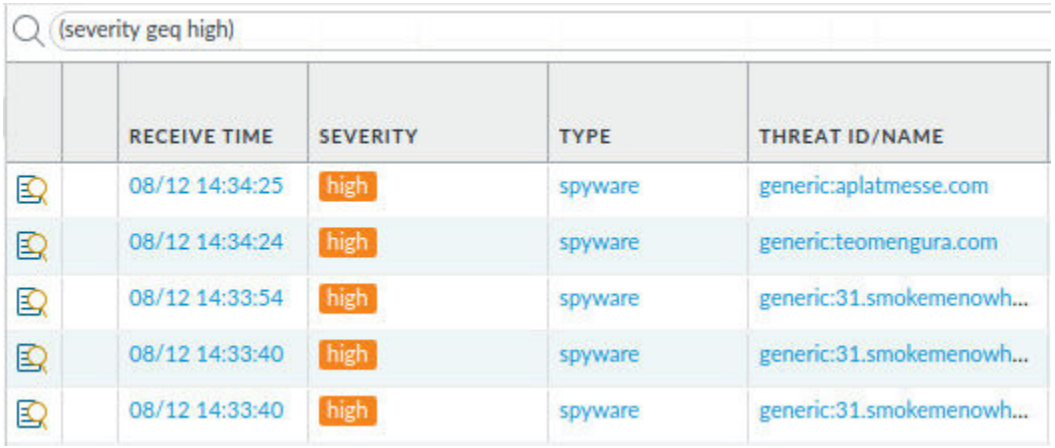
4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.



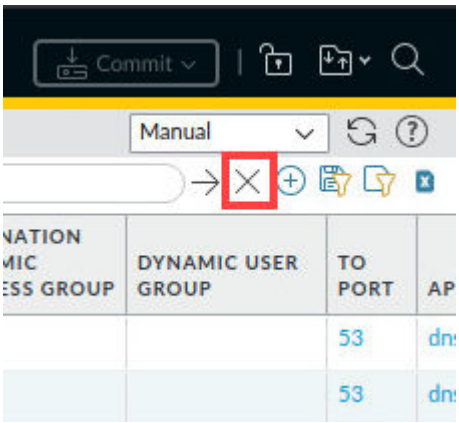
5. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.



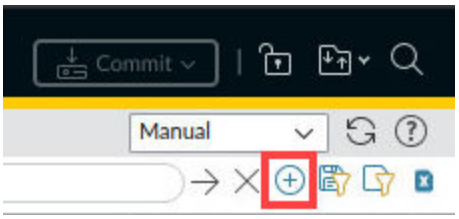
6. Notice the Threat log has been filtered to display only threats of high severity or greater. Some columns have been adjusted to reflect the *Severity* column.



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

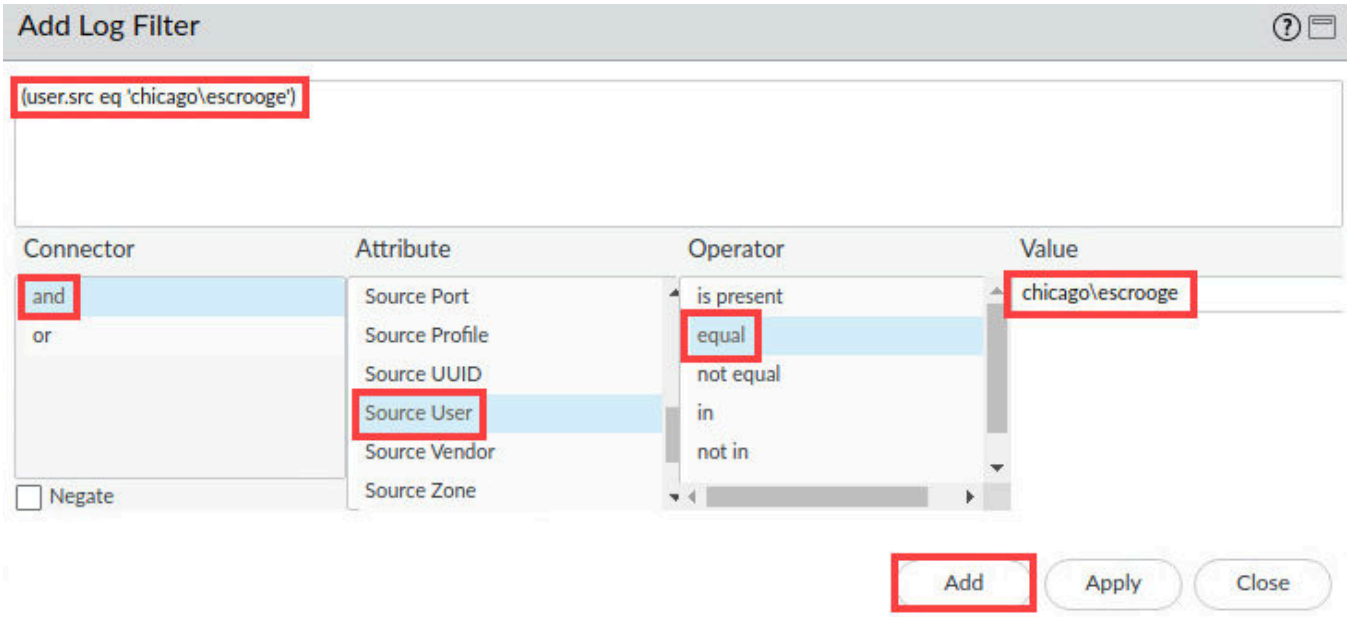


8. Click the **+** icon in the filter area to re-open the **Add Log Filter** window.

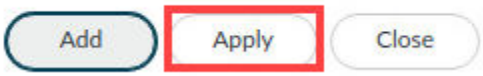


9. In the *Add Log Filter* window, select the following. Click **Add**.

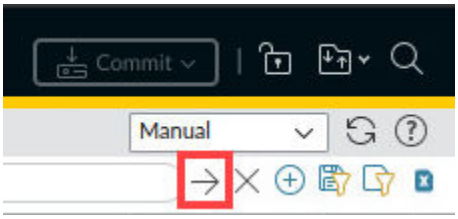
Parameter	Value
Connector	**and**
Attribute	**Source User**
Operator	**equal**
Value	**`chicago\escrooge`**



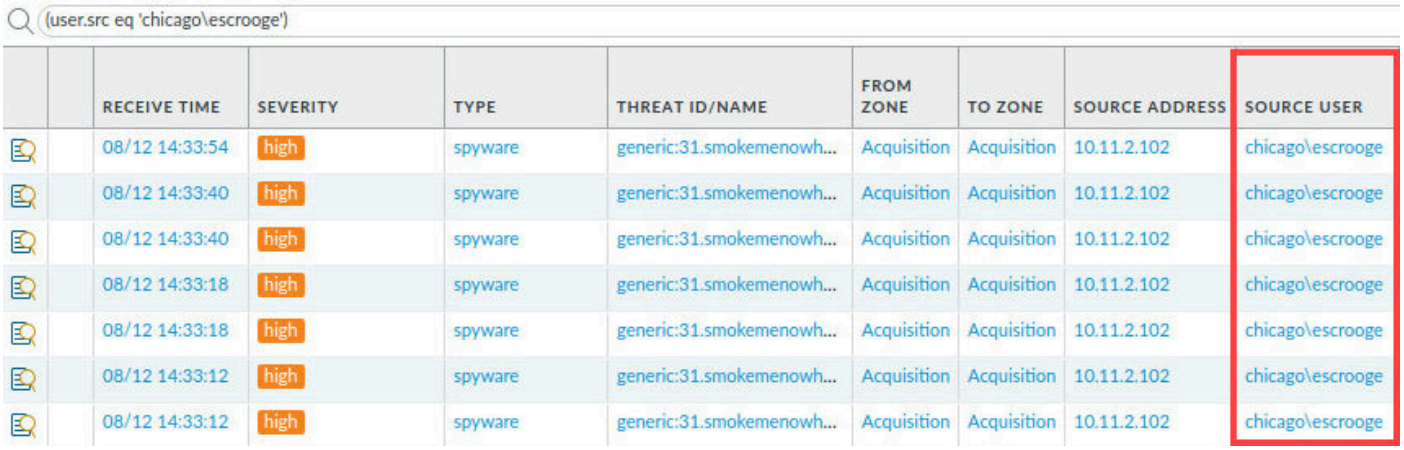
10. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.



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

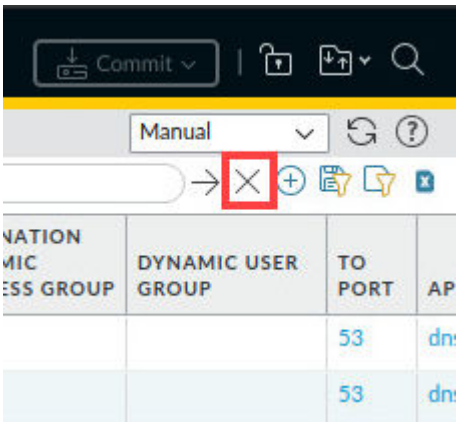


12. Notice the Threat log has been filtered to display only threats from the Source User **Chicago\escrooge**. Some columns have been adjusted to reflect the *Severity* column.



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

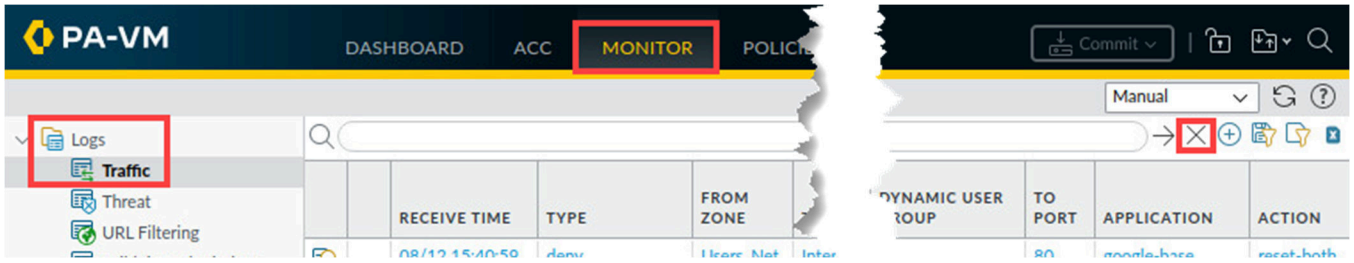
URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

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.

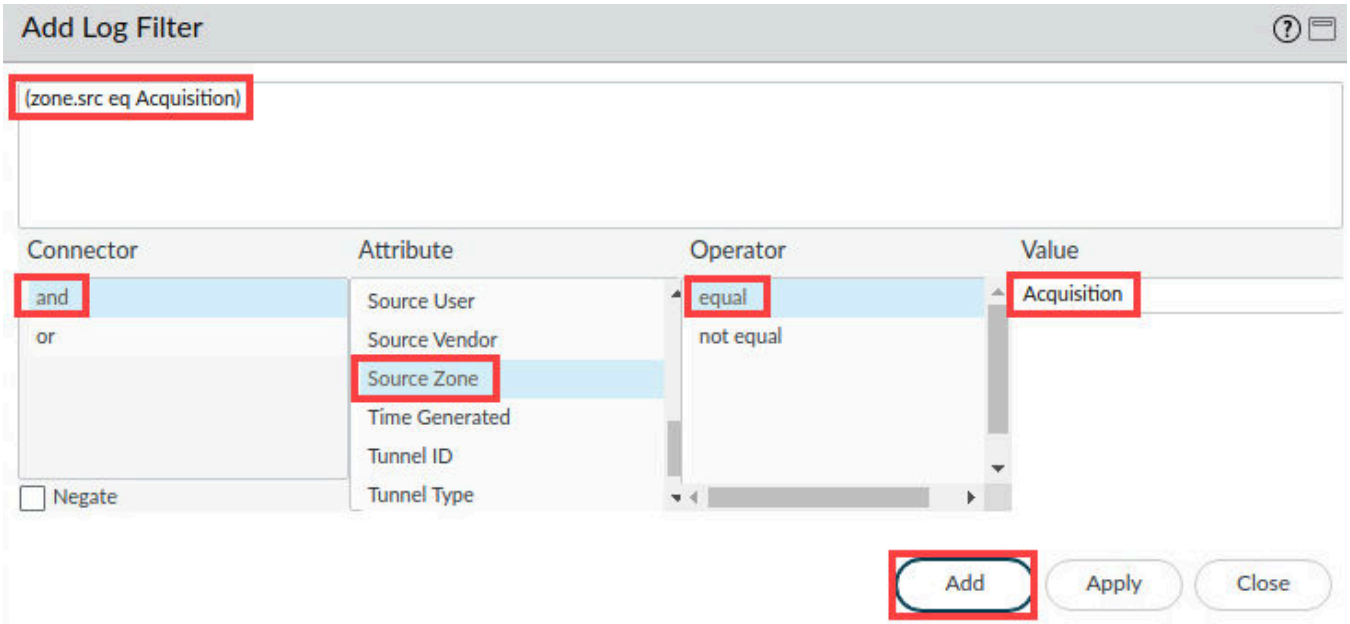
1. Select **Monitor > Logs > Traffic.** Click the **X** icon in the filter area to remove any existing log filter.



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**.

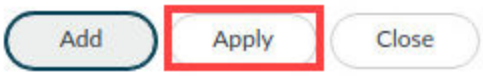
Parameter	Value
Connector	**and**
Attribute	**Source Zone**
Operator	**equal**
Value	**`Acquisition`**



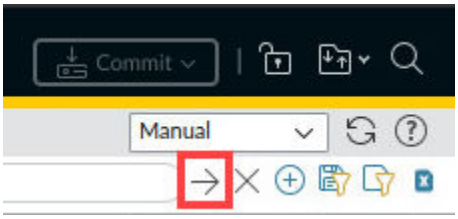
Please Note

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.

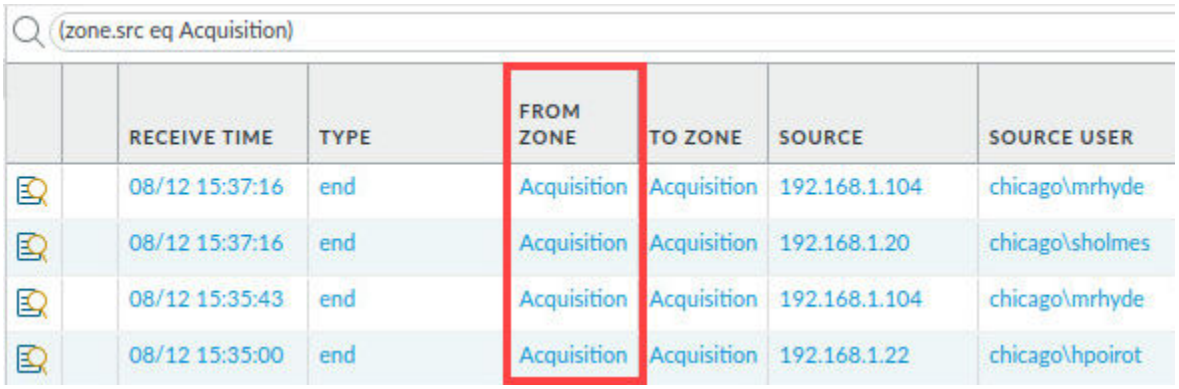
4. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.



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



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.



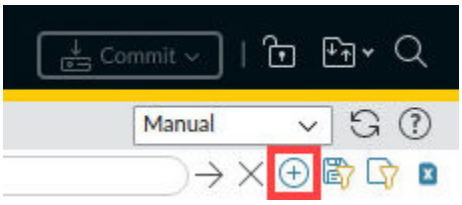
(zone.src eq Acquisition)

		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

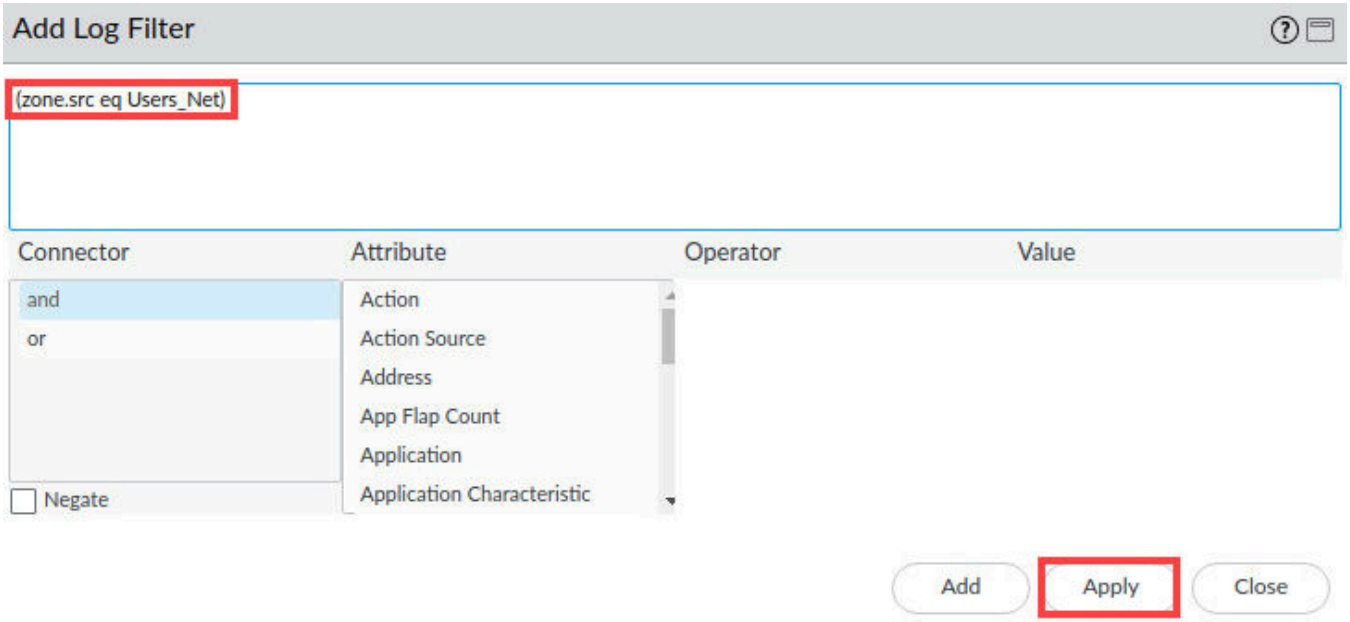
Please Note

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.

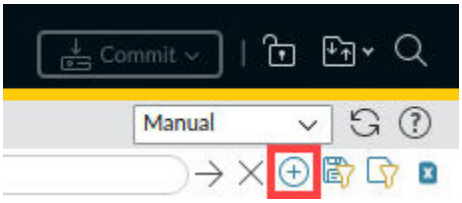
7. Click the **+** icon in the filter area to again open the *Add Log Filter* window.



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**.

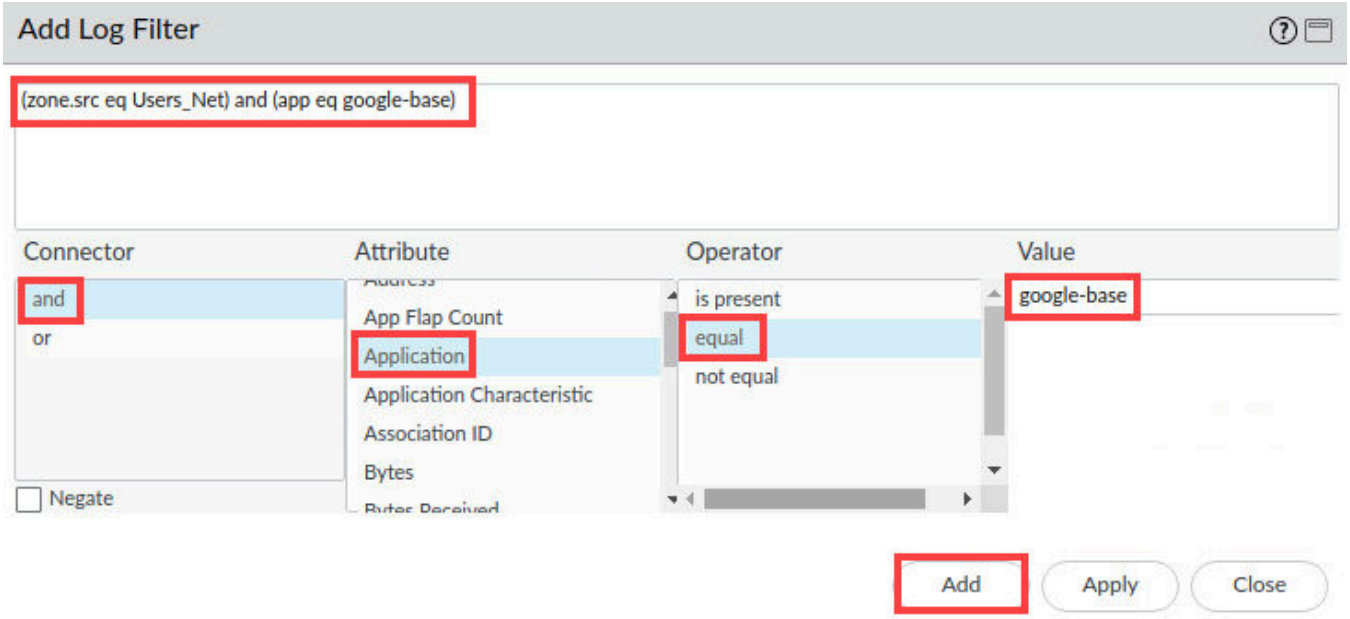


9. Click the **+** icon in the filter area to again open the *Add Log Filter* window.

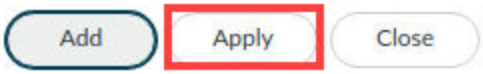


10. In the *Add Log Filter* window, select the following. Click **Add**.

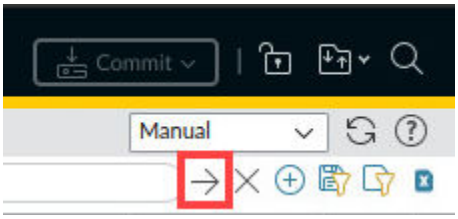
Parameter	Value
Connector	**and**
Attribute	**Application**
Operator	**equal**
Value	**google-base**



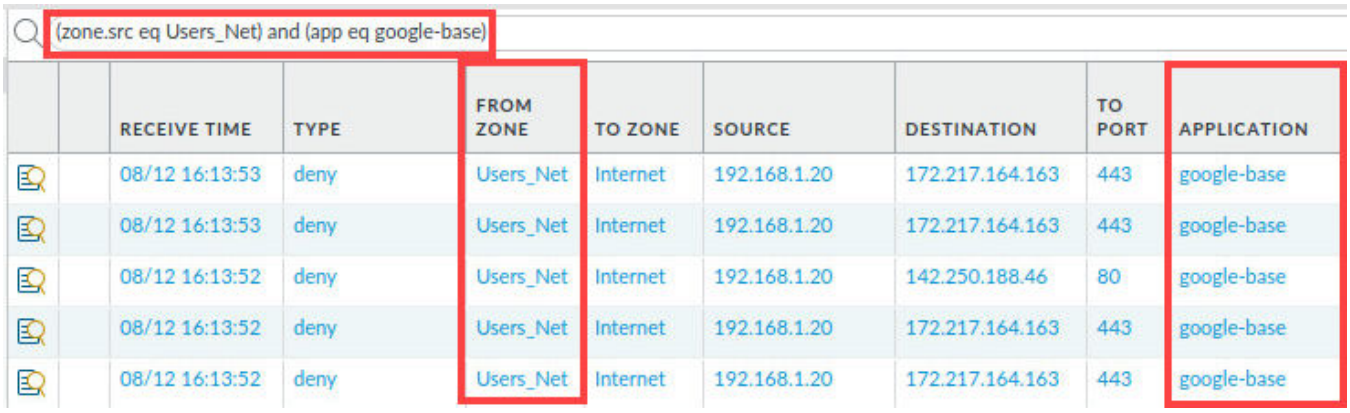
11. In the *Add Log Filter* window, click **Apply**. As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forgo using the filter builder.



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.



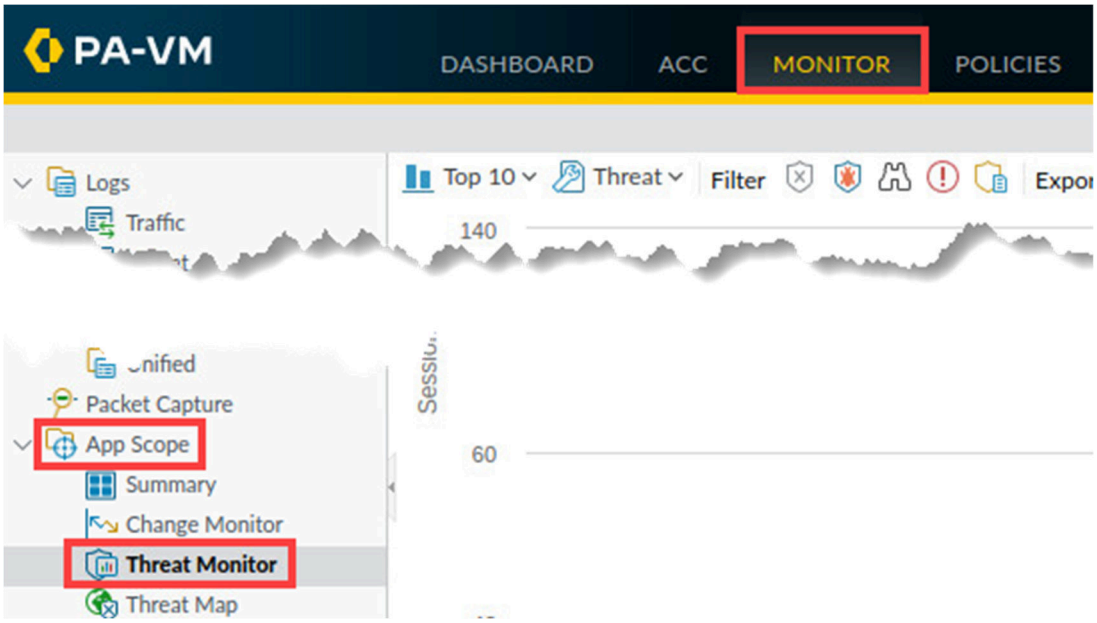
RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION
08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
08/12 16:13:53	deny	Users_Net	Internet	192.168.1.20	172.217.164.163	443	google-base
08/12 16:13:52	deny	Users_Net	Internet	192.168.1.20	142.250.188.46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

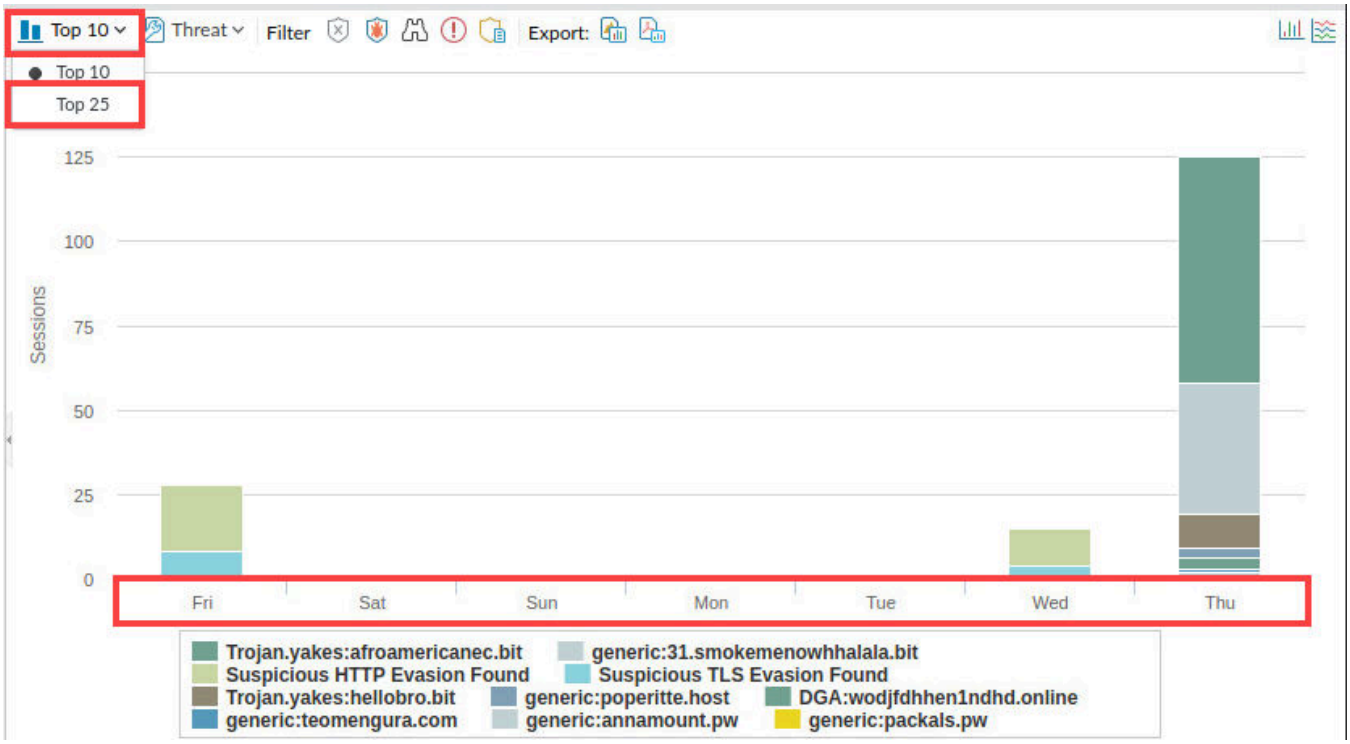
In this section, you will view threat information using App Scope's Threat Monitor and Threat Map reports.

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

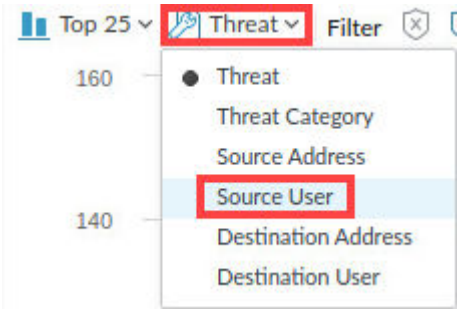


2. At the bottom of the window, click **Last 7 days**.

3. 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.

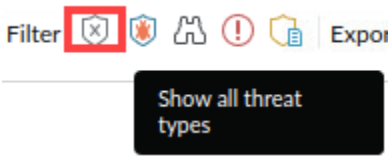


4. At the top of the window, click **Threat** and choose **Source User**.

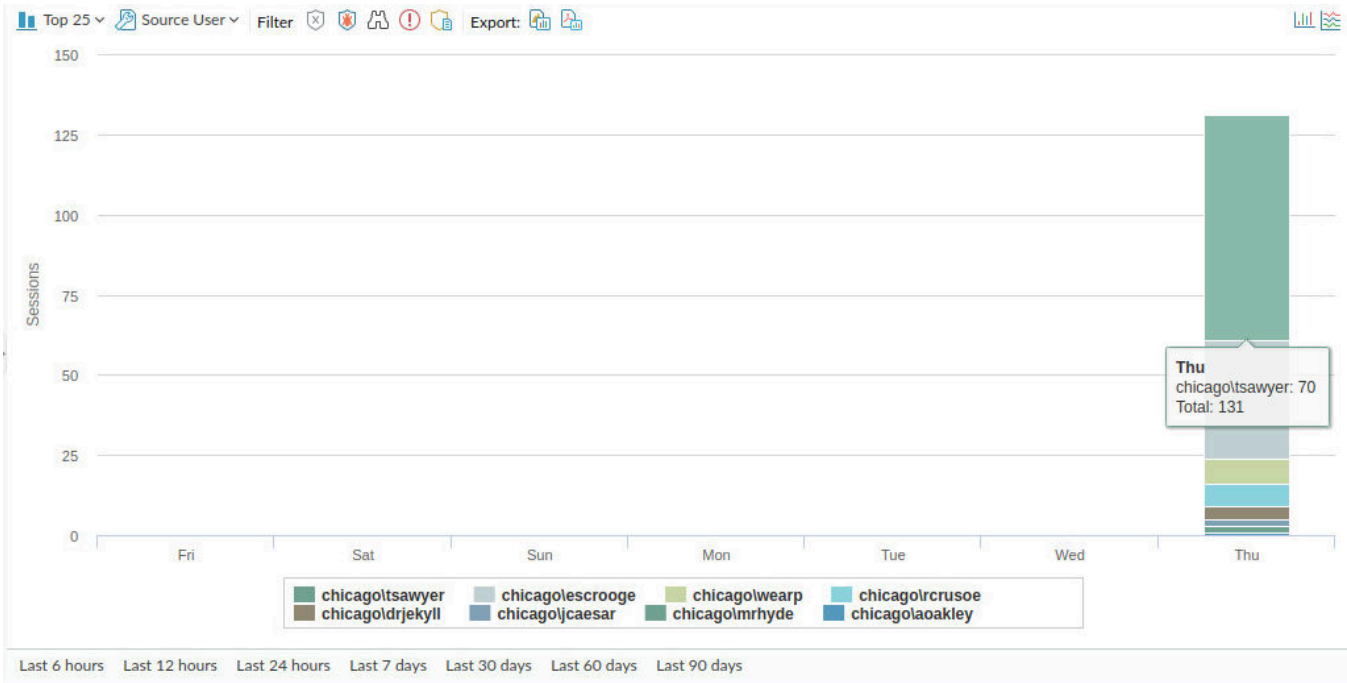


5. At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats.

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 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.