



## PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

### Lab 13: Locating Valuable Information Using Logs and Reports

Document Version: **2025-10-13**

Copyright © 2025 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are registered trademarks of Palo Alto Networks, Inc. All other marks mentioned herein may be trademarks of their respective companies.

## Contents

|  |           |
|--|-----------|
| Introduction .....   | 3         |
| Objective .....  | 3         |
| Lab Topology .....   | 4         |
| Lab Settings .....   | 5         |
| Lab Guidance.....  | 5         |
| <b>1 Locating Valuable Information Using Logs and Reports – High Level Lab Steps .....</b> | <b>6</b>  |
| 1.1 Apply a Baseline Configuration to the Firewall .....                                   | 6         |
| 1.2 Generate Traffic .....   | 6         |
| 1.3 Display Recent Threat Information in the Dashboard.....                                | 6         |
| 1.4 Display Recent Application Information in the Dashboard .....                          | 6         |
| 1.5 View Threat Information in the ACC.....  | 6         |
| 1.6 View Application Information in the ACC .....  | 7         |
| 1.7 View Information in the Threat Log.....  | 7         |
| 1.8 View Application Information in the Traffic Log.....                                   | 8         |
| 1.9 View Threats Using App Scope Reports.....  | 9         |
| 1.10 View Threat Information Using Predefined Reports .....                                | 9         |
| 1.11 View Application Information Using Predefined Reports .....                           | 9         |
| 1.12 View Threat and Application Information Using Custom Reports .....                    | 9         |
| <b>2 Locating Valuable Information Using Logs and Reports – Detailed Lab Steps .....</b>   | <b>11</b> |
| 2.1 Apply a Baseline Configuration to the Firewall .....                                   | 11        |
| 2.2 Generate Traffic.....  | 15        |
| 2.3 Display Recent Threat Information in the Dashboard.....                                | 17        |
| 2.4 Display Recent Application Information in the Dashboard .....                          | 21        |
| 2.5 View Threat Information in the ACC.....  | 22        |
| 2.6 View Application Information in the ACC .....  | 26        |
| 2.7 View Threat Information in the Threat Log .....  | 31        |
| 2.8 View Application Information in the Traffic Log.....                                   | 37        |
| 2.9 View Threats Using App Scope Reports.....  | 41        |
| 2.10 View Threat Information Using Reports .....   | 44        |
| 2.11 View Application Information Using Predefined Reports .....                           | 47        |
| 2.12 View Threat and Application Information Using Custom Reports .....                    | 49        |

## 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.

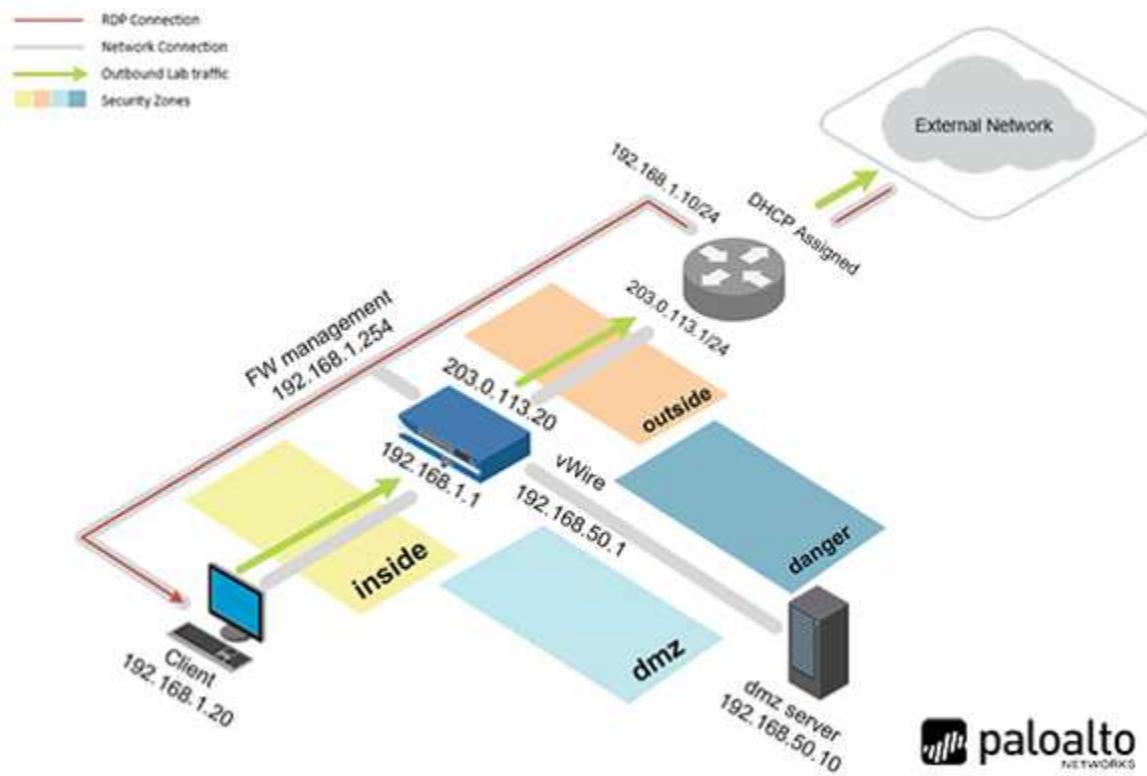
You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

## 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<br>(if needed) | Password<br>(if needed) |
|-----------------|----------------------|------------------------|-------------------------|
| Client          | <b>192.168.1.20</b>  | lab-user               | PaloAlt0!               |
| DMZ             | <b>192.168.50.10</b> | root                   | PaloAlt0!               |
| Firewall        | <b>192.168.1.254</b> | admin                  | PaloAlt0!               |
| vRouter         | <b>192.168.1.10</b>  | root                   | PaloAlt0                |

## 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.

Please  
Note

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\escooge |

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

- 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.

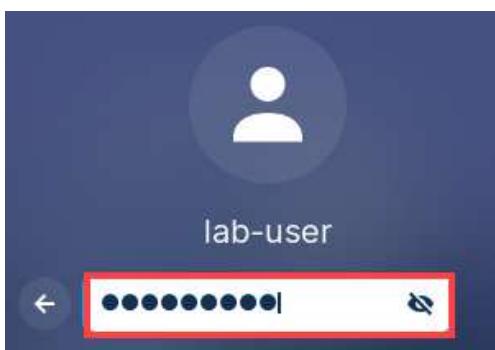
1. Click on the **Client** tab to access the Client PC.



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



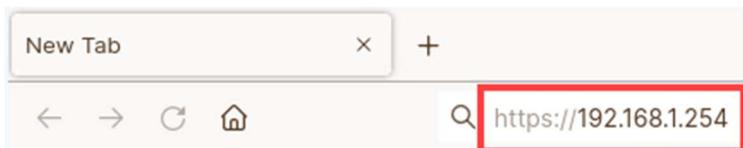
3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



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 **Pa10Alt0!**.

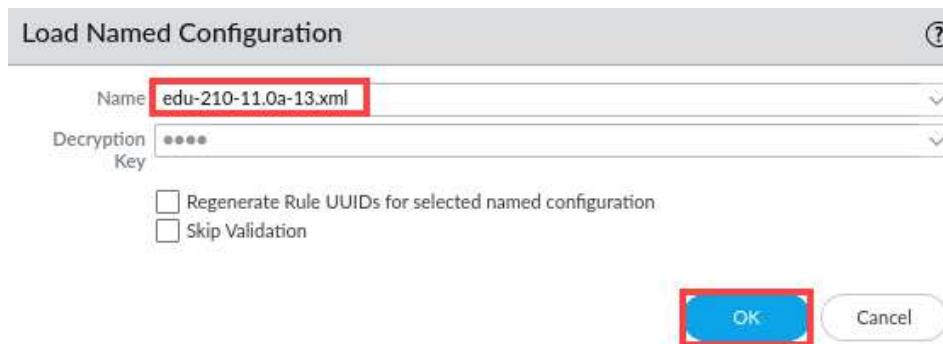


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

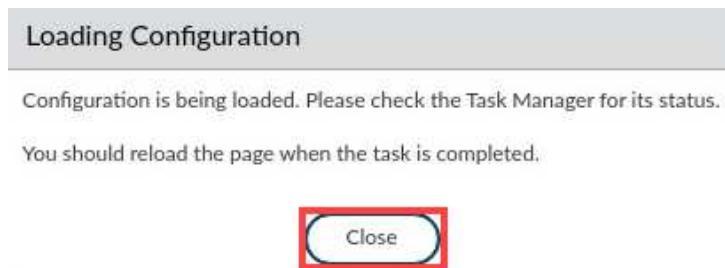
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE (which is highlighted). On the left, a sidebar under the 'Setup' heading lists: High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area has tabs for Management, Operations (which is highlighted), Services, Interfaces, Telemetry, Content-ID, WildFire, and Session. Under the Configuration Management section, there are options for Revert, Save, Load, and Load named configuration snapshot. The 'Load named configuration snapshot' option is specifically highlighted with a red box.

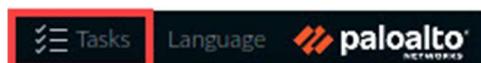
8. In the *Load Named Configuration* window, select **edu-210-11.0a-13.xml** from the *Name* drop-down box and click **OK**.



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**

| Task Manager - All Tasks                                      |        |           |                     |          |        |        |
|---|--------|-----------|---------------------|----------|--------|--------|
| <input type="text"/> <span>12 items</span> <span>Close</span> |        |           |                     |          |        |        |
| JOB ID  | TYPE   | STATUS    | START TIME          | MESSAGES | ACTION | ADMIN  |
| 14  | Load   | Completed | 2023/07/28 18:54:07 |          |        | System |
| 2   | Report | Completed | 2023/07/28 18:51:30 |          |        |        |

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 All Changes  Commit Changes Made By:(1) admin

| COMMIT SCOPE  | LOCATION TYPE | OBJECT TYPE | ENTITIES | ADMINS |
|---|---------------|-------------|----------|--------|
| Commit Scope is unavailable when a full commit is required  |               |             |          |        |
| <a href="#">Preview Changes</a> <a href="#">Change Summary</a> <a href="#">Validate Commit</a>  |               |             |          |        |
| Note: This shows all the changes in login admin's accessible domain.  |               |             |          |        |
| <input type="text" value="Description"/>  |               |             |          |        |
| <div style="text-align: right;"> <input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px; border-radius: 5px; margin-right: 10px;" type="button" value="Commit"/> <input style="border: 1px solid #ccc; padding: 5px; border-radius: 5px;" type="button" value="Cancel"/> </div> |               |             |          |        |

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

**Commit Status**

Operation Commit  
 Status Completed  
 Result Successful  
 Details Configuration committed successfully

**Commit** | App Dependency

profiles -> spyware -> Corp-AS -> botnet-domains -> dns-security-categories is invalid. Missing pre-defined DNS security category



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**.

| Name                   | Group | Server        | Plugin | Last used             |
|------------------------|-------|---------------|--------|-----------------------|
| Berlin-Client          |       | 192.168.1.25  | SSH    | 2022-11-21 - 09:01:12 |
| Firewall-A             |       | 192.168.1.254 | SSH    | 2022-12-16 - 07:51:14 |
| Firewall-B             |       | 192.168.1.253 | SSH    | 2022-11-21 - 08:51:34 |
| Panorama               |       | 192.168.1.252 | SSH    | 2022-12-14 - 10:34:19 |
| <b>Server-Extranet</b> |       | 192.168.50.10 | SSH    | 2022-12-16 - 09:27:14 |

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
```

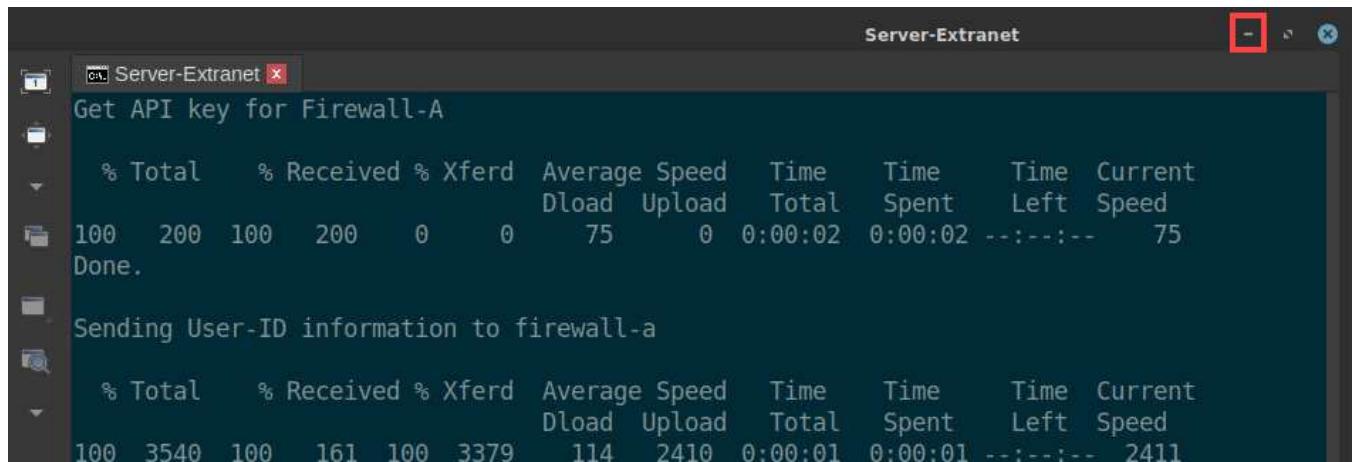
4. Press **Enter** to start the *UsingLogs-V1.sh* script.

```
#####
##      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.

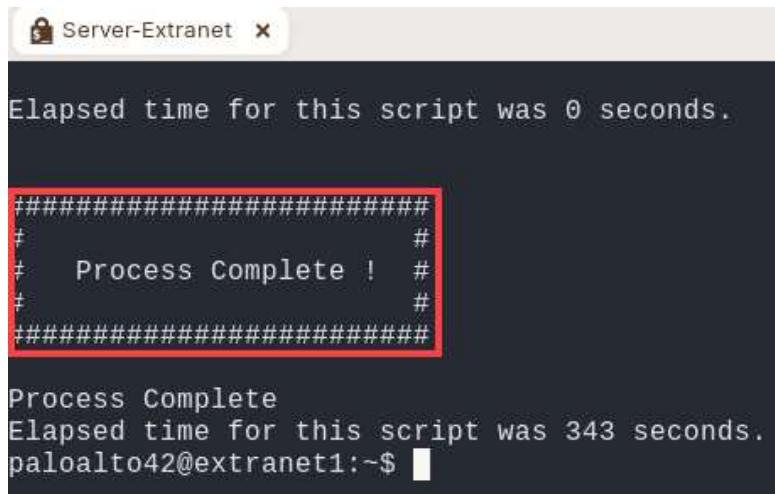


```
Server-Extranet
Get API key for Firewall-A
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
100  200  100  200    0     0      75      0  0:00:02  0:00:02 --::--  75
Done.

Sending User-ID information to firewall-a
% Total % Received % Xferd Average Speed Time Time Time Current
          Dload Upload Total Spent Left Speed
100 3540  100   161  100  3379    114   2410  0:00:01  0:00:01 --::--  2411
```



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

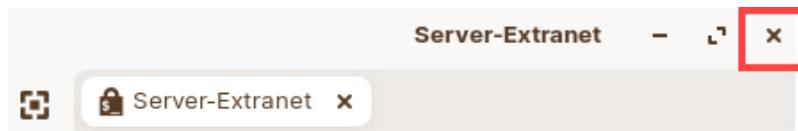


```
Server-Extranet
Elapsed time for this script was 0 seconds.

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

Process Complete
Elapsed time for this script was 343 seconds.
paloalto42@extranet1:~$
```

- 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**.

The screenshot shows the PA-VM dashboard interface. At the top, there's a navigation bar with tabs: DASHBOARD (highlighted with a red box), ACC, MONITOR, POLICIES, and OBJECTS. Below the navigation bar, there's a 'General Information' section with device details: Device Name (firewall-a), MGT IP Address (192.168.1.254), MGT Netmask (255.255.255.0), MGT Default Gateway (192.168.1.1), and MGT IPv6 Address (unknown). To the right of this section is a 'Widgets' dropdown menu. The 'Logs' option is expanded, showing sub-options: Application, System, Logs, and Threat Logs. The 'Threat Logs' option is highlighted with a red box. A note at the bottom right of the dashboard area says 'No data available'.

**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.

| Name                                      | Severity | Time              |
|---|----------|-------------------|
| PBP Packet Drop                           | high     | 09/05<br>00:10:29 |
| PBP Packet Drop                           | high     | 09/05<br>00:10:19 |
| PBP Packet Drop                           | high     | 09/05<br>00:10:09 |
| PBP Packet Drop                           | high     | 09/05<br>00:09:59 |
| PBP Packet Drop                           | high     | 09/05<br>00:09:49 |
| Ursnif.Trojan Command and Control Traffic | critical | 09/05<br>00:09:42 |
| generic:aplatmesse.com                    | high     | 09/05<br>00:09:40 |
| generic:teomengura.com                    | high     | 09/05<br>00:09:40 |
| PBP Packet Drop                           | high     | 09/05<br>00:09:39 |
| Trojan.yakes:hellobro.bit                 | medium   | 09/05<br>00:09:35 |

Please Note

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**.

The screenshot shows the PA-VM dashboard interface. At the top, there are tabs for DASHBOARD, ACC, MONITOR, POLICIES, and OBJECTS. Below the tabs, there's a "Layout" dropdown set to "3 Columns". A "Widgets" button is highlighted with a red box. To its right, a dropdown menu is open, showing categories: Application, System, and Logs. The "Logs" category is also highlighted with a red box. Under "Logs", the "URL Filtering Logs" option is highlighted with a red box. The main content area displays a table titled "Threat Logs" with three entries:

| Name                             | Severity | Time              |
|----------------------------------|----------|-------------------|
| generic:31.smokemenowhhalala.bit | high     | 08/12<br>06:06:31 |
| generic:31.smokemenowhhalala.bit | high     | 08/12<br>06:06:28 |
| generic:31.smokemenowhhalala.bit | high     | 08/12<br>06:06:23 |

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

| 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.

The screenshot shows the PA-VM dashboard with the 'Widgets' menu open. The 'Logs' option under 'Widgets' is highlighted with a red box. Within the 'Logs' dropdown, the 'Data Filtering Logs' option is also highlighted with a red box. The main pane displays a table of URL filtering logs.

| URL  | Category            | Time           |
|--|---------------------|----------------|
| aplatmesse.com/images/aiXla28QV6duat/PF_2B<br>Y9stc2V0NdiiPtOK/Lsb7S_2BfaOliDlf/WGVj1o4<br>_2FOYves/9xJ_2FDB1nwuG2_2FQ/OyxKYJEL6/<br>vLpbY5gEX999CYMCf56/AI4ZqesjAI9QBegDyJg<br>/jjxapq6x5O3DBHsTEJOzpJ/tVm_2FeF.avi | command-and-control | 08/12 06:07:30 |
| n31.smokemenowhhala.bit/newfz31/logout.ph  | command-and-        | 08/12          |

**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*.



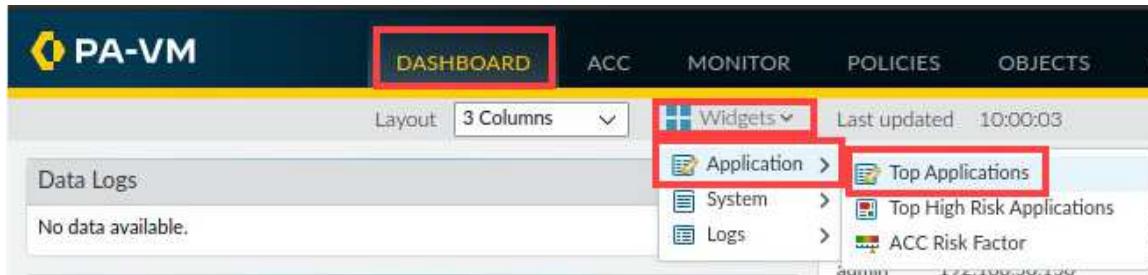
| File Name | Name                             | Time           |
|-----------|----------------------------------|----------------|
| CSPCA.crl | Certificate Revocation List File | 09/10 22:31:25 |
| CSPCA.crl | DER Encoded X509 Certificate     | 09/10 22:31:25 |
| CSPCA.crl | Certificate Revocation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

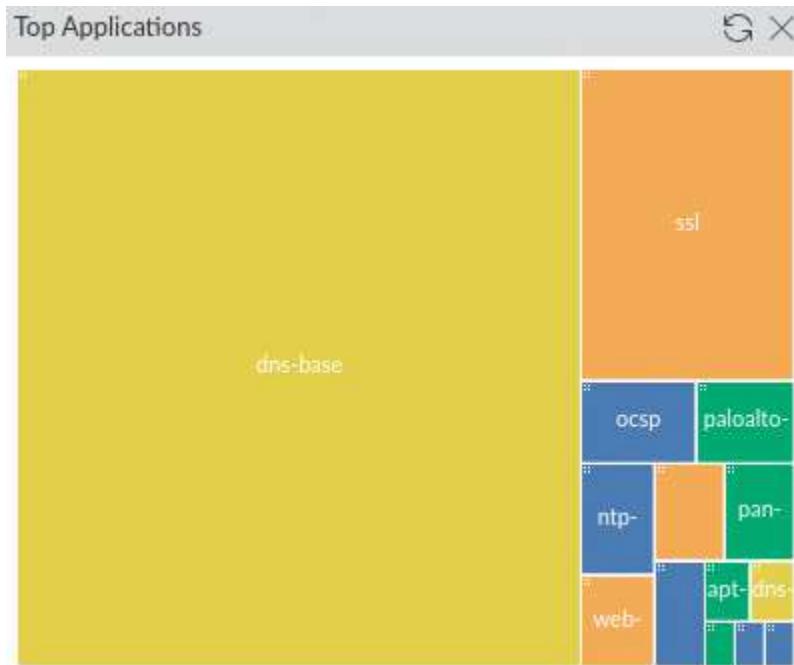
## 2.4 Display Recent Application Information in the Dashboard

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**.

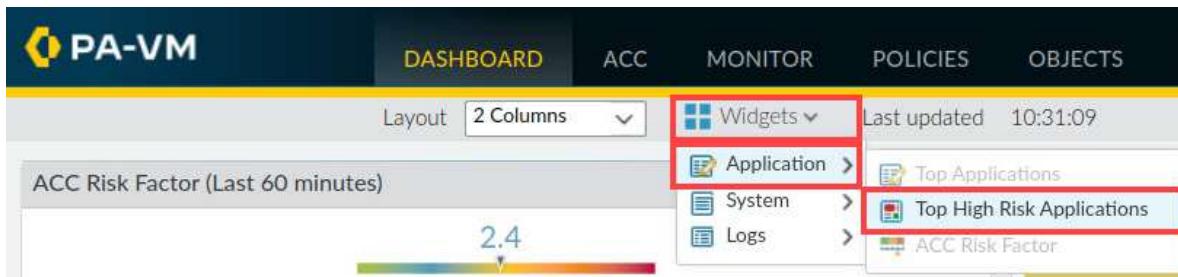


2. Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour. The screen shot below may differ than the actual lab environment.

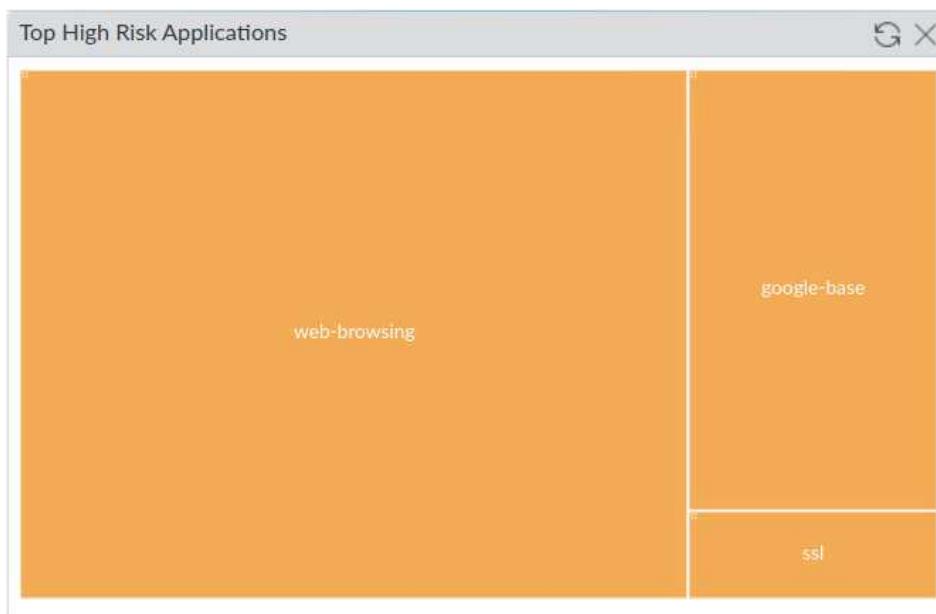


Some applications should be listed because some “housekeeping” traffic nearly always traverses the network, even in the lab environment. This widget is useful for viewing only the recent application traffic seen in the last hour by the firewall.

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**

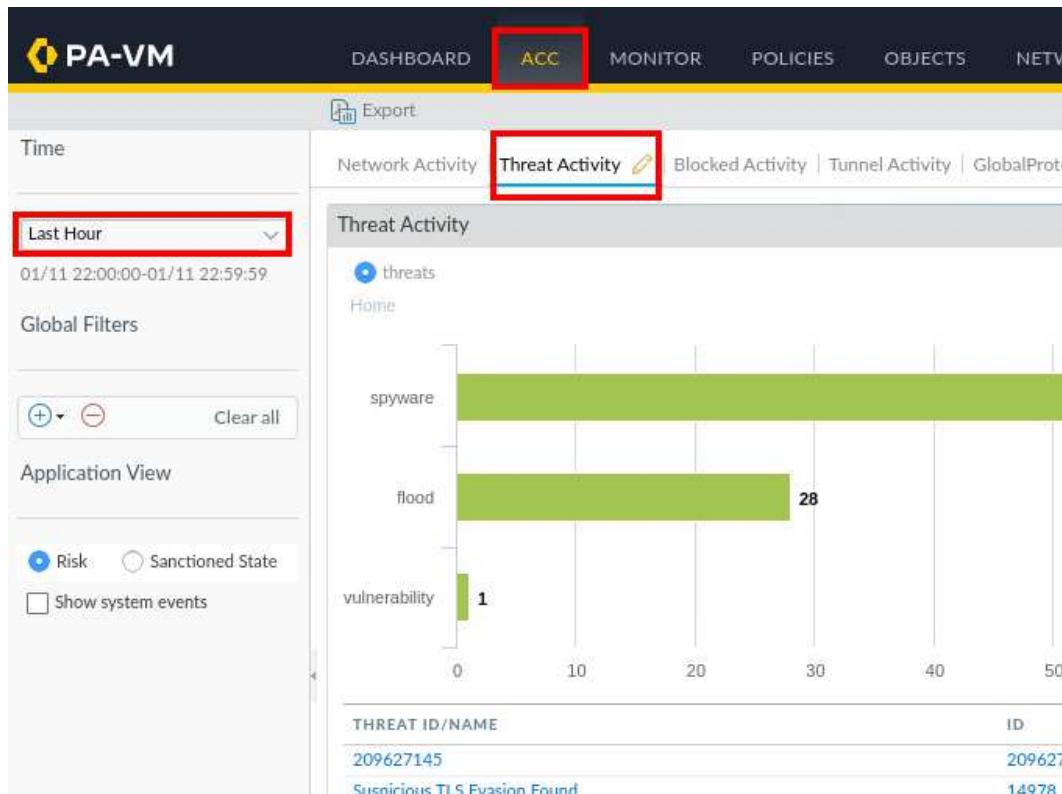
Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. If the Top High Risk and Top Applications have not updated, please allow 3 to 5 minutes for the widgets to update.

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.

- 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    |
| PPP 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.

**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.

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

The screenshot shows the ACC interface with the following details:

- Time: Last Hour
- Date Range: 10/21 07:45:00-10/21 08:44:59
- Global Filters:
  - Severity (1):  high
  - Buttons: +, -, Clear all
- Application View

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.

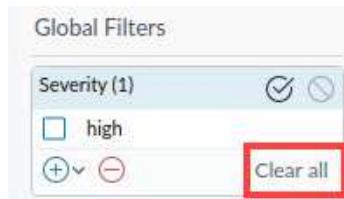
4. Note that the Threat Activity graph and the table of Threat Names are updated to reflect only items with a Severity level of **high**.



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

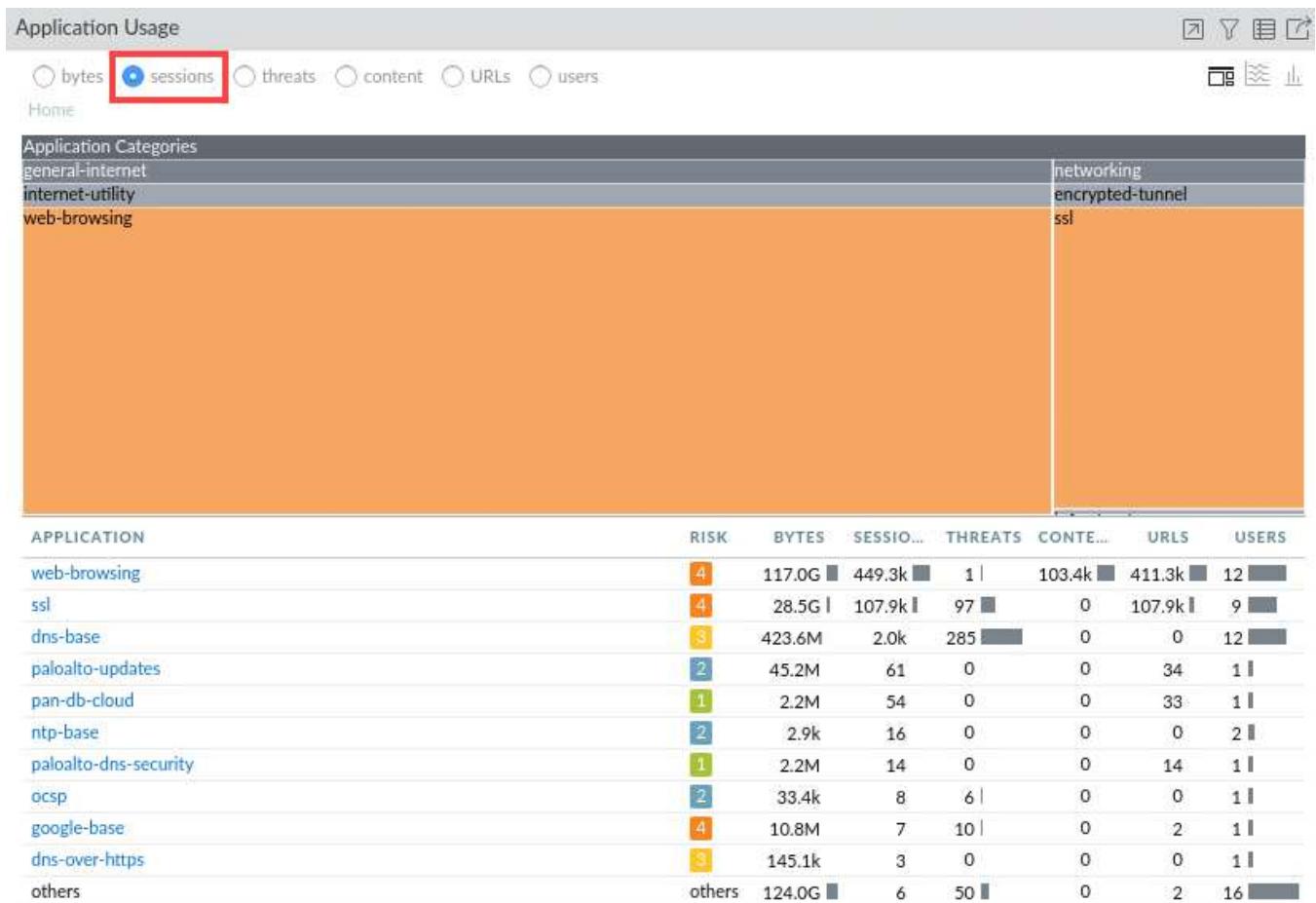
In this section, you will view two widgets on the Network Activity tab. The goal is for you to gain familiarity with some of the widgets available for viewing application and traffic information.

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.

The screenshot shows the Palo Alto Networks Firewall's Application Control Center (ACC) interface. At the top, there are three tabs: DASHBOARD, ACC (which is highlighted with a red box), and MONITOR. Below the tabs, there is a sidebar on the left containing various filters and settings. The main area is titled "Network Activity" and includes a "Threat Activity" tab. Under "Network Activity", there is a section for "Application Usage" where users can choose between "bytes" (selected), "sessions", "threats", and "connections". Below this is a "Home" section showing "Application Categories" with networking, infrastructure, and netbios-dg listed. At the bottom, there is a table showing application usage statistics:

| APPLICATION  | RISK | BYTES  | SES |
|--------------|------|--------|-----|
| netbios-dg   | 2    | 124.0G |     |
| web-browsing | 4    | 3.3G   | 22  |
| ssl          | 4    | 1.3G   | 7   |

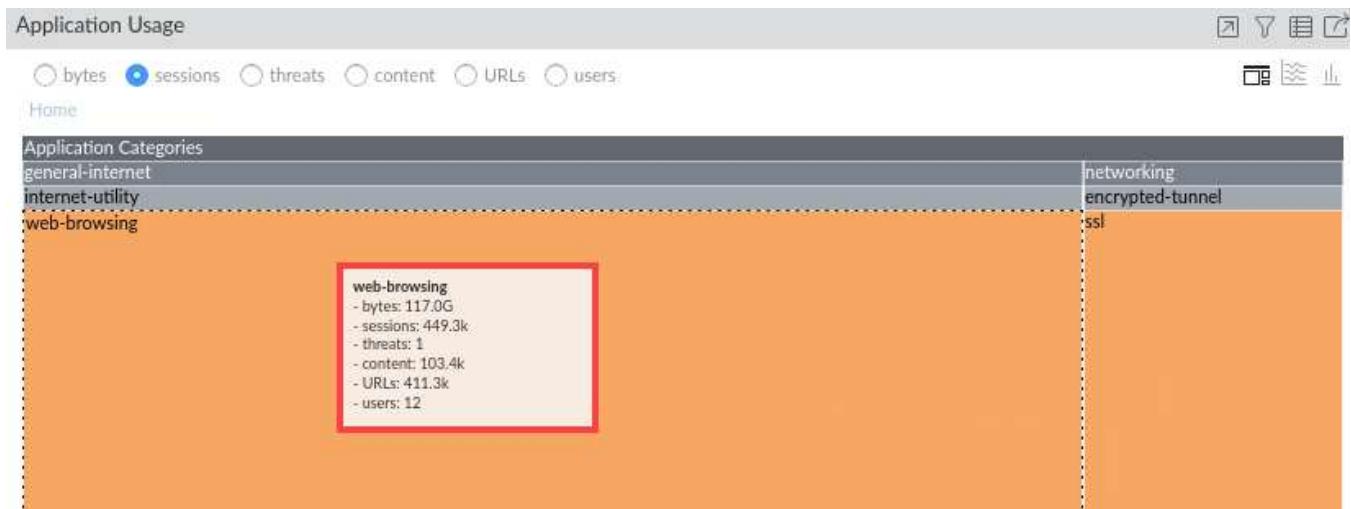
2. The top section of the **Application Usage** widget is a graph that illustrates how much traffic a specific application represents. Select the **sessions** radio button.



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.

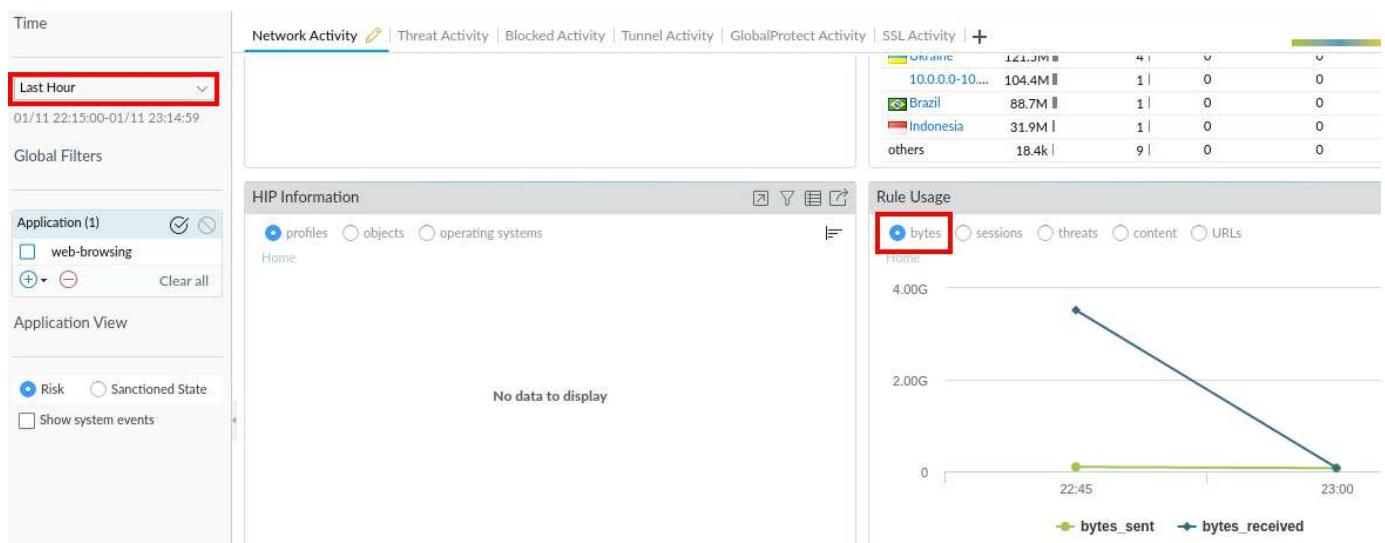
4. In the table below the graph, hover your pointer over the **web-browsing** application until the global filter **Left arrow** appears. Then click the **Left arrow** to promote the **web-browsing** application to a global filter.

| APPLICATION           | RISK   | BYTES  | SESSIONS | THREATS | CONTENT | 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.



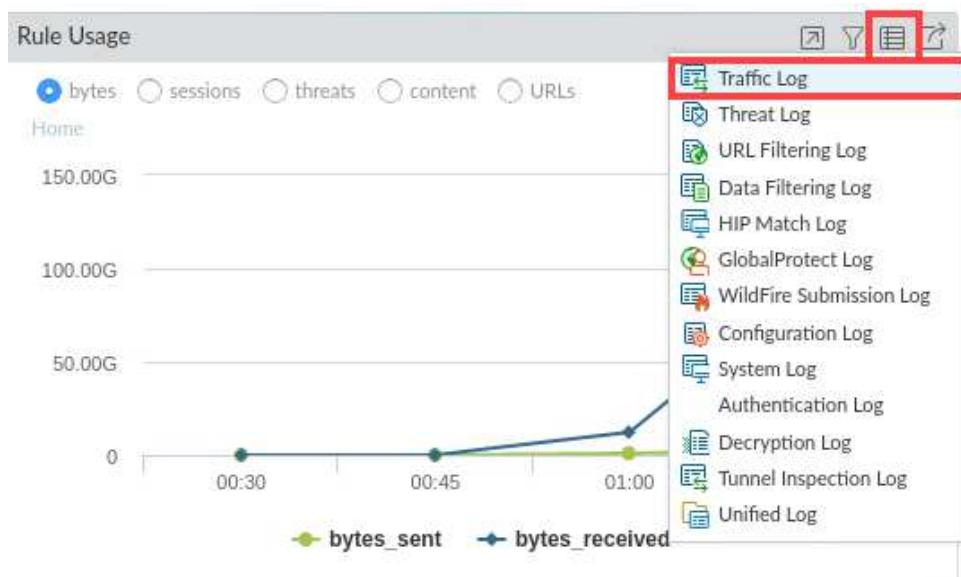
6. Scroll down in the **Network Activity** tab until you reach the **Rule Usage** widget. Select the radio button at the top for **bytes**. In the *Time* column, make sure **Last Hour** is selected.



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

- Allow-Corp-Apps
- 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.

The figure shows the PA-VM web interface with the 'MONITOR' tab selected. On the left, there's a sidebar with a 'Logs' section containing various log categories like Traffic, Threat, URL Filtering, etc. The 'Traffic' category is currently selected and highlighted. The main content area shows a table of traffic log entries. The table has columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, and SOU DYN ADD. The table data is as follows:

|  | RECEIVE TIME   | TYPE | FROM ZONE   | TO ZONE     | SOURCE        | SOURCE USER      | SOU DYN ADD |
|--|----------------|------|-------------|-------------|---------------|------------------|-------------|
|  | 09/05 01:29:59 | end  | Acquisition | Acquisition | 192.168.1.103 | chicago\drjekyll |             |
|  | 09/05 01:29:59 | end  | Acquisition | Acquisition | 192.168.1.22  | chicago\hpoirot  |             |
|  | 09/05 01:29:59 | end  | Acquisition | Acquisition | 192.168.1.22  | chicago\hpoirot  |             |
|  | 09/05 01:29:59 | end  | Acquisition | Acquisition | 10.4.5.101    | chicago\tsawyer  |             |
|  | 09/05 01:29:59 | end  | Acquisition | Acquisition | 192.168.1.22  | chicago\hpoirot  |             |

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.

A screenshot of the Palo Alto Networks Firewall interface. The top navigation bar has tabs: DASHBOARD, ACC (which is highlighted with a red box), and MONITOR. Below the tabs is a toolbar with an 'Export' button and a 'Network Activity' tab (which is underlined). On the left, there's a sidebar with 'Time' set to 'Last Hour' (09/05 01:00:00-09/05 01:59:59) and a 'Global Filters' section. In the 'Global Filters' section, there are '+' and '-' buttons and a 'Clear all' button, which is also highlighted with a red box. The main pane shows 'HIP Information' with radio buttons for 'profiles' (selected), 'objects', and 'operating system'. At the bottom of the sidebar is an 'Application View' link.

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

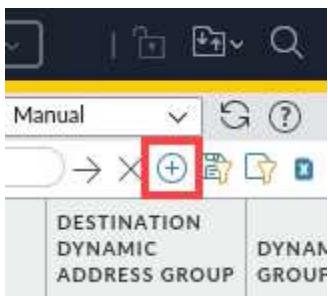
## 2.7 View Threat Information in the Threat Log

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.

- 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.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. In the left sidebar, under 'Logs', the 'Threat' link is highlighted with a red box. In the top right corner, there is a filter area with a search bar and several icons. One of the icons, which is a red X, is also highlighted with a red box. Below the filter area, there is a table with columns: RECEIVE TIME, TYPE, and THREAT ID. The table contains four rows of threat log entries.

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



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

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

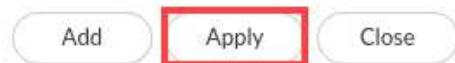
Add Log Filter

(severity geq high)

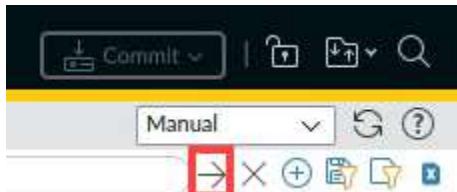
| Connector                       | Attribute       | Operator              | Value         |
|---------------------------------|-----------------|-----------------------|---------------|
| and                             | Sender Address  | equal                 | informational |
|                                 | Session ID      | not equal             | low           |
| or                              | Session Owner   | greater than or equal | medium        |
|                                 | Severity        | less than or equal    | high          |
|                                 | Source Address  |                       | critical      |
|                                 | Source Category |                       |               |
| <input type="checkbox"/> Negate |                 |                       |               |

Add      Apply      Close

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.

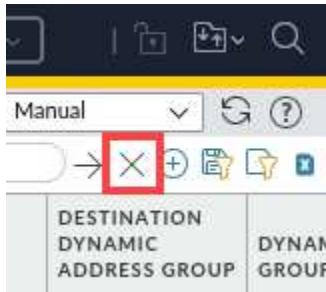
severity geq high

|  | 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     |

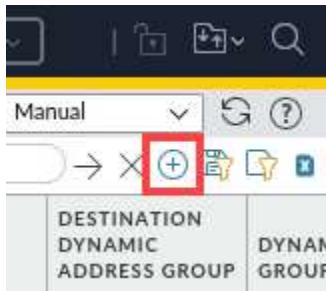
Please  
Note

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.

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



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



- In the Add Log Filter window, select the following. Click Add.

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

Add Log Filter

(user.src eq 'chicago\escrooge')

| Connector | Attribute      | Operator   | Value            |
|-----------|----------------|------------|------------------|
| and       | Source Port    | is present |                  |
| or        | Source Profile | equal      | chicago\escrooge |
|           | Source UUID    | not equal  |                  |
|           | Source User    | in         |                  |
|           | Source Vendor  | not in     |                  |
|           | Source Zone    |            |                  |

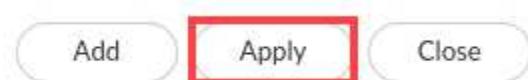
Negate

Add    Apply    Close

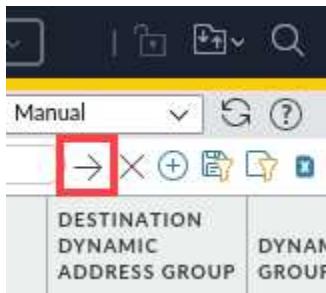
**Please Note**

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.

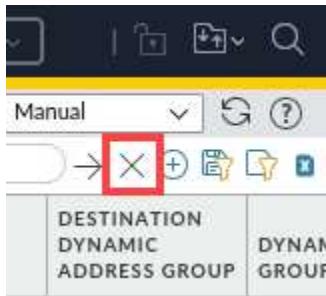


12. Notice the threat log has been filtered to display only threats from the Source User **chicago\escrooge**.

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

|  | 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 01:13:52 | spyware | generic:31.smokemenowh... | Acquisition | Acquisition | 10.11.2.102    | chicago\escrooge | high     |
|  | 09/05 01:13:52 | spyware | generic:31.smokemenowh... | Acquisition | Acquisition | 10.11.2.102    | chicago\escrooge | high     |
|  | 09/05 01:13:52 | flood   | PBP Packet Drop           | Acquisition |             | 10.11.2.102    | chicago\escrooge | high     |
|  | 09/05 01:13:40 | spyware | generic:31.smokemenowh... | Acquisition | Acquisition | 10.11.2.102    | chicago\escrooge | high     |

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 |

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

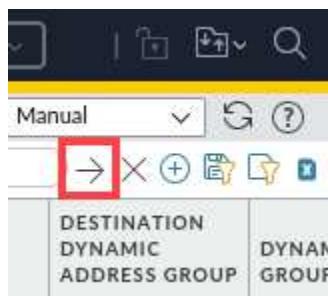
**Please Note**

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.

- 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.



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

- a. True
  - b. False
- 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.

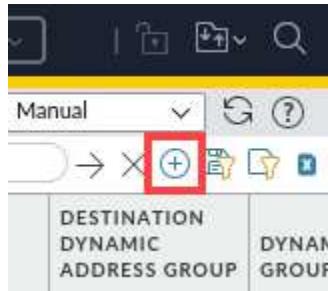
(zone,src eq Acquisition)

|  | RECEIVE TIME   | TYPE | FROM ZONE   | TO ZONE     | SOURCE       | SOURCE USER     |
|--|----------------|------|-------------|-------------|--------------|-----------------|
|  | 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**

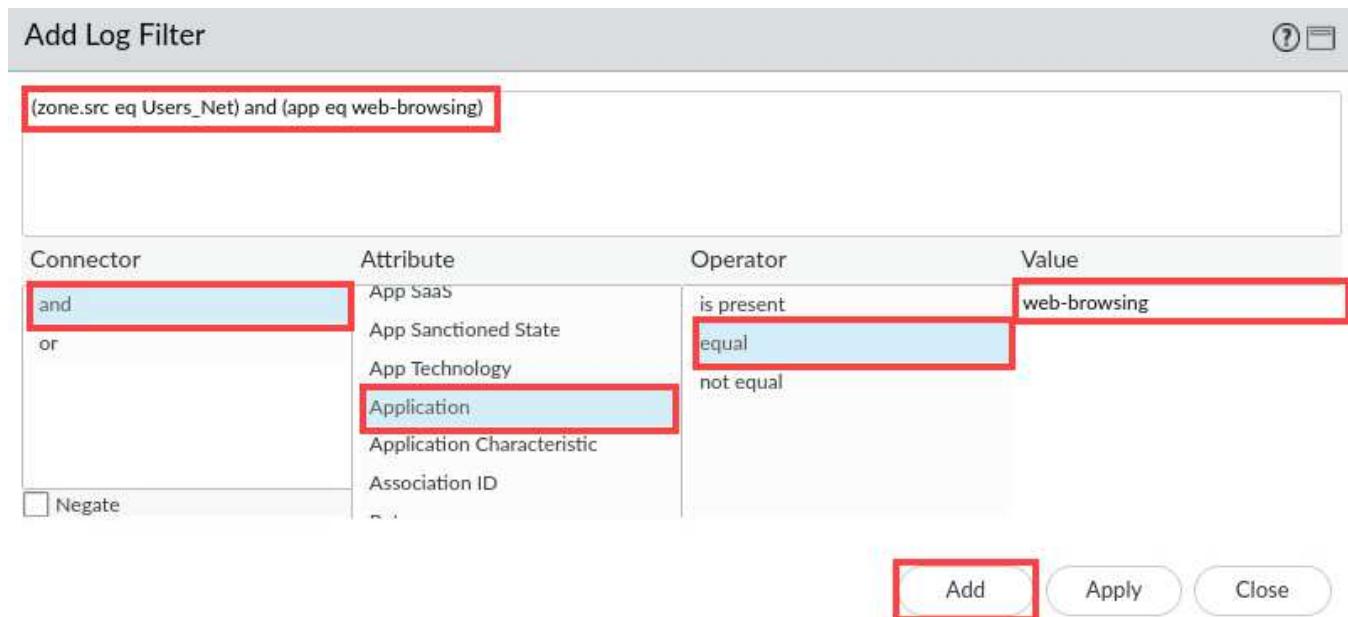
The Acquisition source zone filter still should appear in the open **Add Log Filter** window.

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**).

A screenshot of the 'Add Log Filter' dialog box. The title bar says 'Add Log Filter'. The main area contains the filter expression '(zone.src eq Users\_Net)' which is highlighted with a red box. Below this is a large empty text area. At the bottom is a table with four columns: 'Connector', 'Attribute', 'Operator', and 'Value'. The 'Connector' column has rows for 'and' and 'or'. The 'Attribute' column lists various network attributes like Action, Action Source, Address, App Flap Count, Application, and Application Characteristic. The 'Operator' and 'Value' columns are currently empty.

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

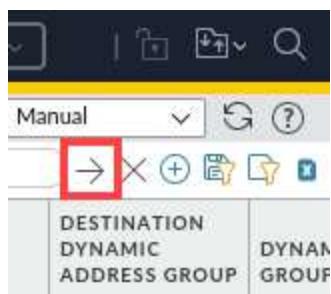
| Parameter | Value        |
|-----------|--------------|
| Connector | and          |
| Attribute | Application  |
| Operator  | equal        |
| Value     | web-browsing |



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

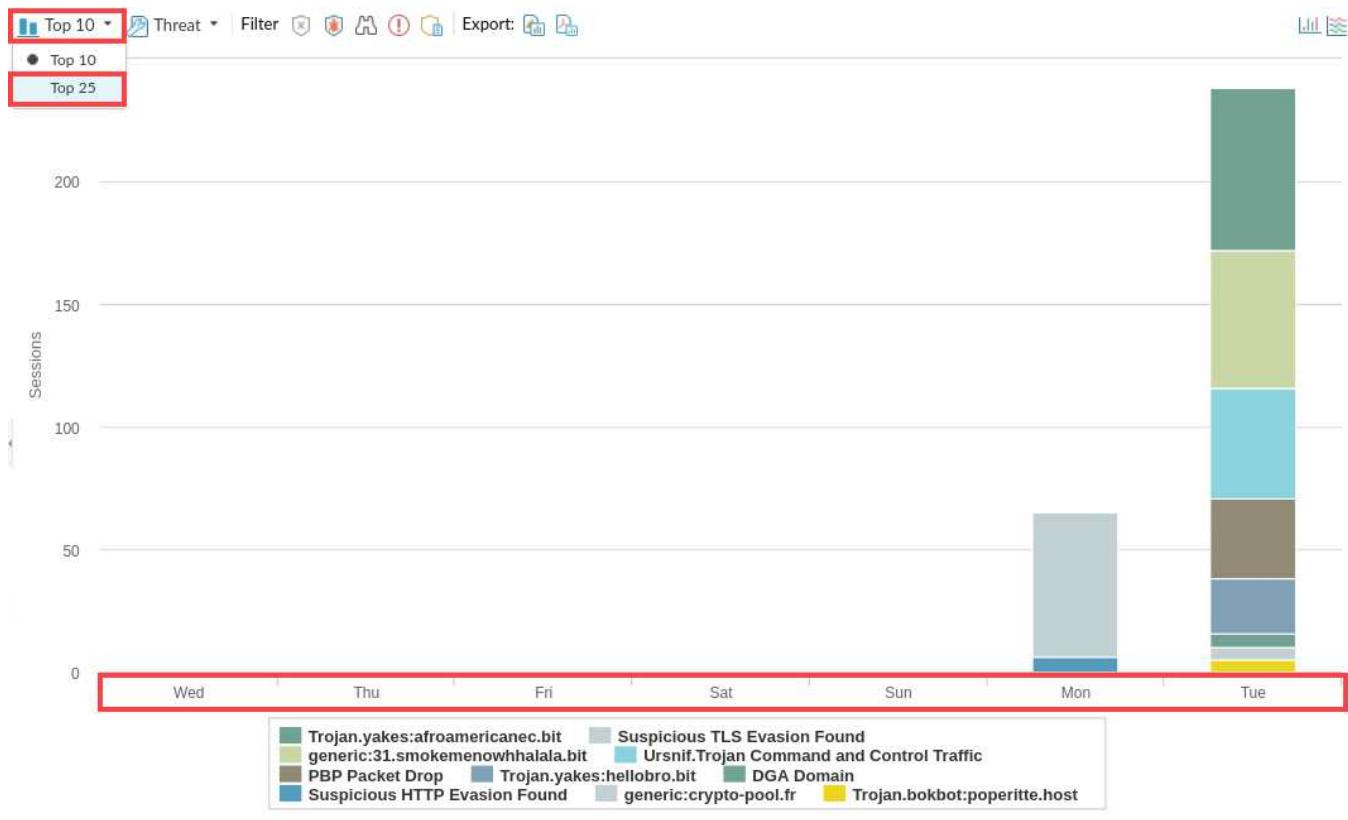
In this section, you will view threat information using App Scope's Threat Monitor and Threat Map reports.

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

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

Last 6 hours Last 12 hours Last 24 hours **Last 7 days** Last 30 days Last 60 days Last 90 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.

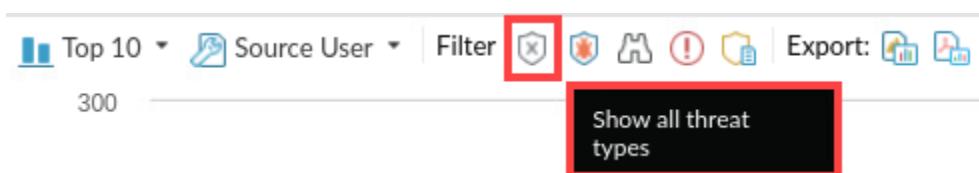
- At the top of the window, click **Threat** and choose **Source User**.



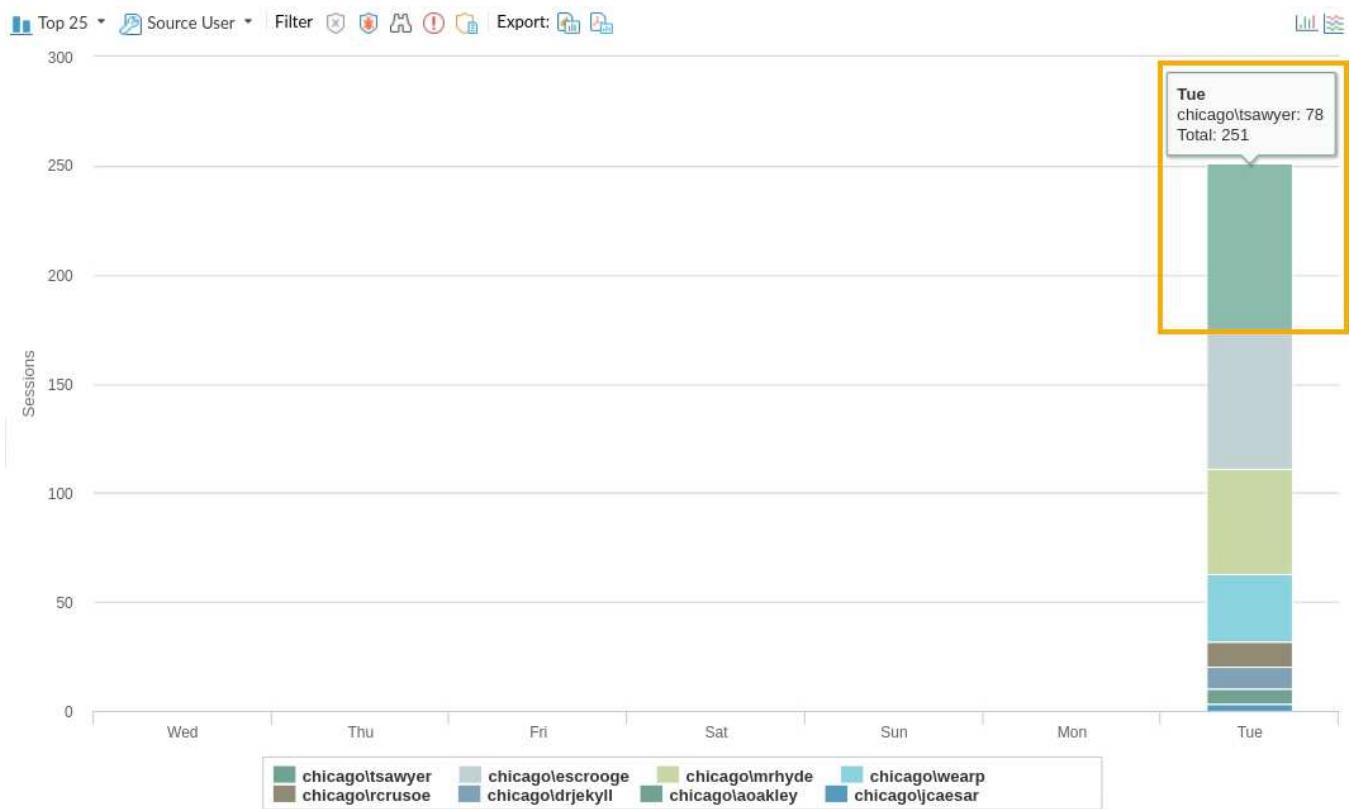
- At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats.



- Select **Show all threat types**.



7. Hover your pointer over the top section of any bar on the bar chart. You should see a 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

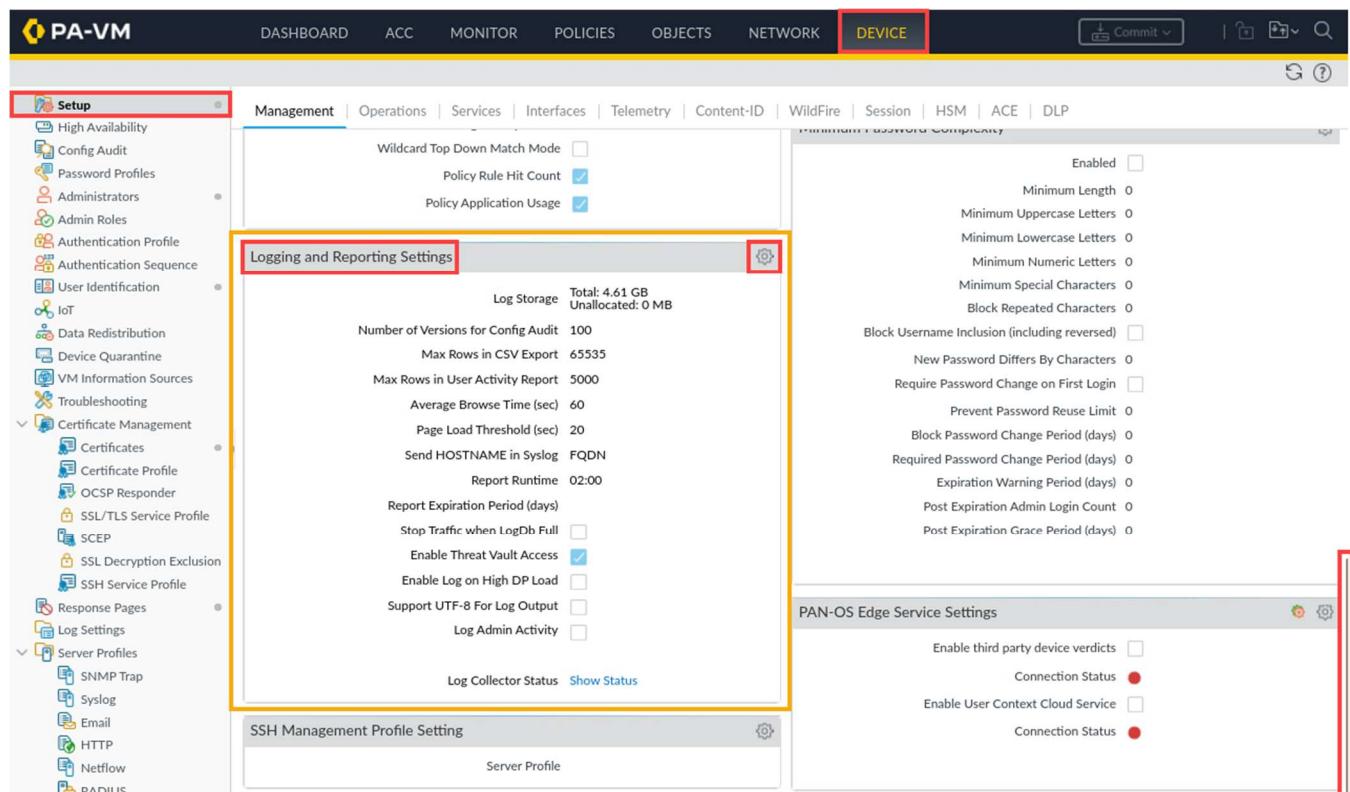
In this section, you will enable and view more than 40 predefined reports available on the firewall. Your efficient use of the predefined reports depends on your spending time with each report, discovering and determining which information might be useful to you in your own environment. Your familiarity 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.



The screenshot shows the PAN-OS Management interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is highlighted with a red box. On the left, a sidebar menu under the 'Setup' heading lists various configuration options like High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, IoT, Data Redistribution, Device Quarantine, VM Information Sources, Troubleshooting, Certificate Management, Response Pages, Log Settings, Server Profiles, and RADIUS. The 'Management' tab is selected in the main content area. A specific section titled 'Logging and Reporting Settings' is highlighted with a yellow box and contains the following details:

- Log Storage: Total: 4.61 GB Unallocated: 0 MB
- Number of Versions for Config Audit: 100
- Max Rows in CSV Export: 65535
- Max Rows in User Activity Report: 5000
- Average Browse Time (sec): 60
- Page Load Threshold (sec): 20
- Send HOSTNAME in Syslog: FQDN
- Report Runtime: 02:00
- Report Expiration Period (days):
- Stop Traffic when LogDb Full:
- Enable Threat Vault Access:
- Enable Log on High DP Load:
- Support UTF-8 For Log Output:
- Log Admin Activity:
- Log Collector Status: Show Status

To the right of this section, there are two other panels:

- Common Password Complexity:** Contains fields for Enabled (checkbox), Minimum Length (0), Minimum Uppercase Letters (0), Minimum Lowercase Letters (0), Minimum Numeric Letters (0), Minimum Special Characters (0), and Block Repeated Characters (checkbox).
- PAN-OS Edge Service Settings:** Contains fields for Enable third party device verdicts (checkbox), Connection Status (red dot), Enable User Context Cloud Service (checkbox), and Connection Status (red dot).

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.

The screenshot shows the 'Logging and Reporting Settings' interface. The 'Pre-Defined Reports' tab is active. Under 'Application Reports', all items are checked. Under 'Traffic Reports', all items are checked. Under 'Threat Reports', all items are checked. Under 'URL Filtering Reports', all items are checked. At the bottom, there is a note: 'Note: Group Reports and PDF Reports will have no data if a contained pre-defined report is disabled'. Below the note are 'Select All' and 'Deselect All' buttons, both highlighted with red boxes. At the bottom right are 'OK' and 'Cancel' buttons, also highlighted with red boxes.

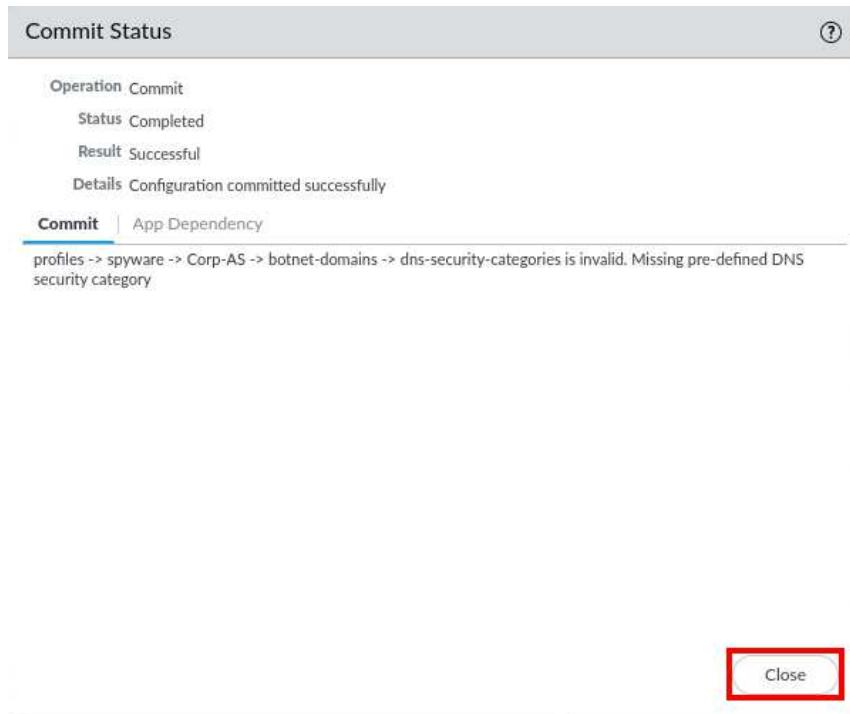
3. Click the **Commit** link located at the top-right of the web interface.



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

The screenshot shows the 'Commit' window. It says 'Doing a commit will overwrite the running configuration with the commit scope.' There are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. A table shows a single row for 'device-and-network' with 'Device and Network Configuration' under 'LOCATION TYPE'. At the bottom, there are 'Preview Changes', 'Change Summary', and 'Validate Commit' buttons, and a note: 'Note: This shows all the changes in login admin's accessible domain.' Below that is a 'Description' input field and 'Commit' and 'Cancel' buttons, both highlighted with red boxes.

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

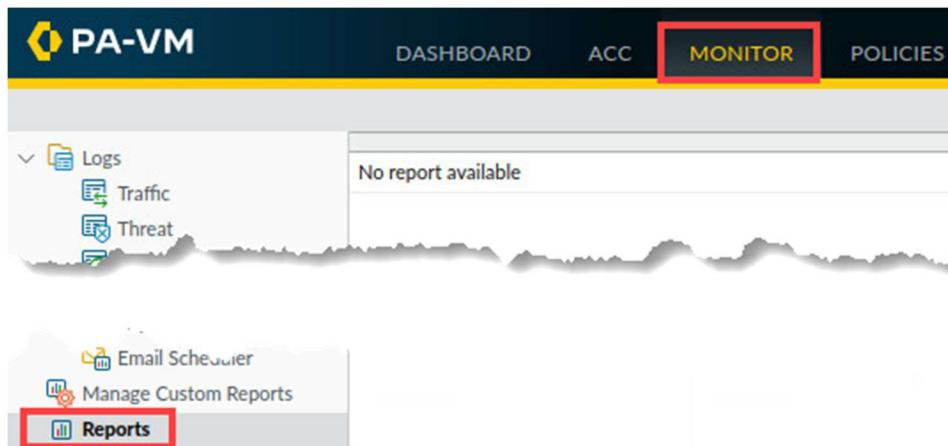


6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 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**.

Custom Reports

- threat-trend
- top-application-categories
- top-applications
- top-attacker-destinations

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.

Custom Reports

- top-inline-cloud-analysis
- top-rules
- top-source-countries
- top-sources
- top-spyware-threats
- top-technology-categories
- top-url-categories
- top-url-user-behavior
- top-url-views

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.

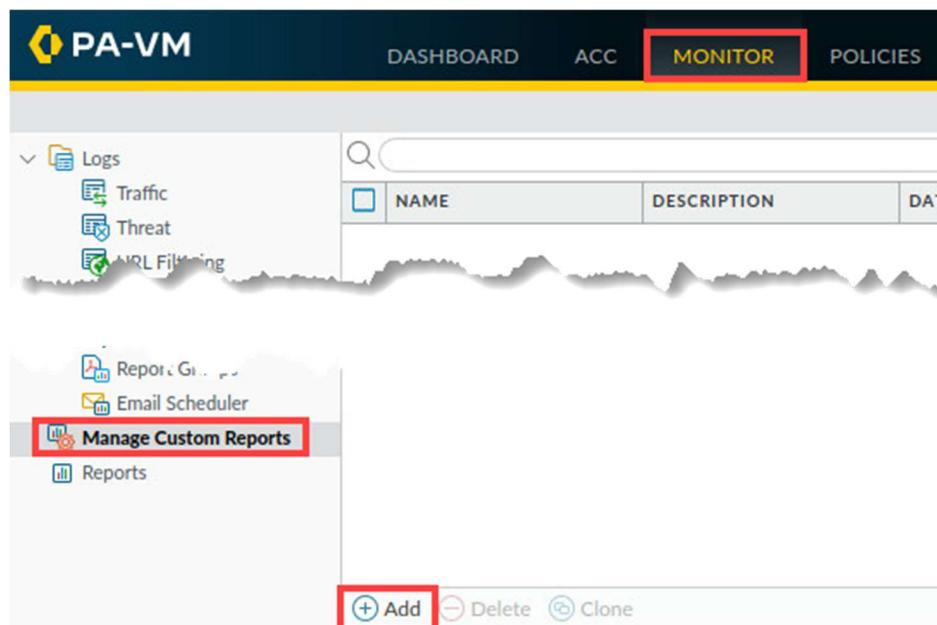
|   | SOURCE ADDRESS | SOURCE HOST NAME | SOURCE USER | BYTES  | SESSIONS |
|---|----------------|------------------|-------------|--------|----------|
| 1 | 192.168.1.254  | 192.168.1.254    |             | 208.6M | 672      |
| 2 | 192.168.1.20   | 192.168.1.20     |             | 16.3M  | 73     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

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**.

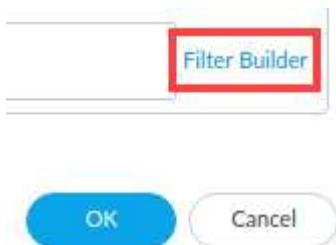


2. In the *Custom Report* window, configure the following.

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

The screenshot shows the 'Custom Report' window. On the left, there's a 'Report Setting' section with fields for 'Name' (set to 'Apps Used by Internal Zones'), 'Description', 'Database' (set to 'Traffic Summary'), 'Scheduled' (checkbox checked), 'Time Frame' (set to 'Last 7 Days'), 'Sort By' (set to 'Sessions Top 100'), and 'Group By' (set to 'Source Zone 5 Groups'). To the right is a 'Available Columns' list (URLs, Users, Virtual System, Virtual System Name, X-Forwarded For IP) and a 'Selected Columns' list (Source Zone, Action, Application, Bytes). A red box highlights the 'Name' field and the 'Selected Columns' list.

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



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

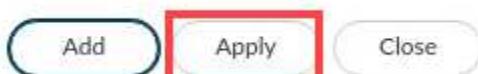
| Parameter | Value       |
|-----------|-------------|
| Connector | and         |
| Attribute | Source Zone |
| Operator  | not equal   |
| Value     | Internet    |

The screenshot shows the 'Add Log Filter' window. At the top, there's a search bar containing '(zone.src neq Internet)' with a red box around it. Below is a table for defining the filter rules:

| Connector | Attribute   | Operator  | Value    |
|-----------|-------------|-----------|----------|
| and       | Source Zone | not equal | Internet |
| or        |             |           |          |

At the bottom, there are three buttons: 'Add' (highlighted with a red box), 'Apply', and 'Close'.

5. Click **Apply**.



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

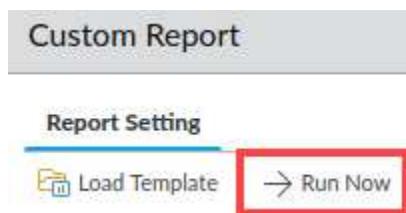
7. The new custom report should be added to the list of custom reports in the web interface.

|                                     | NAME                        | DESCRIPTION | DATABASE        | TIME FRAME  | ROWS | SORT BY  | GROUP BY | SCHEDULED                           |
|-------------------------------------|-----------------------------|-------------|-----------------|-------------|------|----------|----------|-------------------------------------|
| <input checked="" type="checkbox"/> | Apps Used by Internal Zones |             | Traffic Summary | Last 7 Days | 100  | Sessions |          | <input checked="" type="checkbox"/> |

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

|                                     | NAME                        |
|-------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> | Apps Used by Internal Zones |

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.

The screenshot shows the 'Custom Report' window with the title 'Custom Report'. At the top, there's a 'Report Setting' tab and a 'Help' icon. Below it is a table titled 'Apps Used by Internal Zones (100%)'. The table has columns: SOURCE ZONE, ACTI..., APPLICATION, and BYTES. The first row shows 'Acquisition' with 'allow' and 'web-browsing' under 'APPLICATION', and '4.4G' under 'BYTES'. Rows 2 through 9 show various other configurations like 'block-url', 'alert', and 'ssl'. The entire table is highlighted with a yellow border. To the right of the table is a vertical scroll bar, which is also highlighted with a red border. At the bottom of the report area are three export buttons: 'Export to PDF', 'Export to CSV', and 'Export to XML'. At the very bottom are 'OK' and 'Cancel' buttons, with 'OK' being highlighted by a red box.

| SOURCE ZONE | ACTI...     | APPLICATION | BYTES                |
|-------------|-------------|-------------|----------------------|
| 1           | Acquisition | allow       | web-browsing<br>4.4G |
| 2           |             | block-url   | web-browsing<br>0    |
| 3           |             | alert       | web-browsing<br>0    |
| 4           |             | allow       | dns-base<br>225.0k   |
| 5           |             | alert       | ssl<br>0             |
| 6           |             | allow       | ssl<br>22.7M         |
| 7           |             | block-url   | ssl<br>0             |
| 8           |             | drop        | not-applicable<br>0  |
| 9           |             | reset-both  | dns-base<br>0        |

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