

## **VIEW THREAT AND TRAFFIC INFORMATION**



**EDU-210 Version B  
PAN-OS® 10.0**

### *KEEP YOUR EYES ON THE ROAD*

---

- View threat and traffic information:
  - In the Dashboard
  - In the ACC
  - In the logs
  - In App Scope reports
  - In the botnet report
  - In predefined reports
  - In custom reports
- Forward threat and traffic information to external services

**paloalto**  
NETWORKS

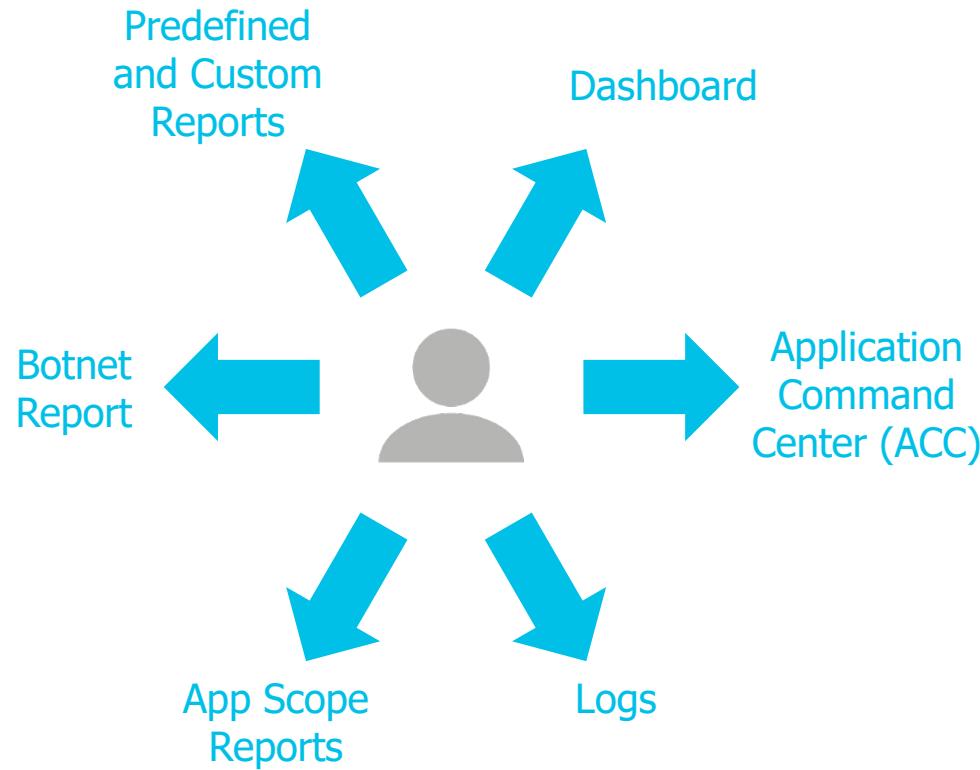
## Learning Objectives

After you complete this module,  
you should be able to:

- Monitor threat and traffic information using the Dashboard and the ACC
- Monitor threat and traffic information using the logs
- Monitor threat and traffic information using App Scope reports
- Monitor threat and traffic information using the botnet report
- Monitor threat and traffic information using predefined and custom reports
- Configure firewall log forwarding to external services



# View Threat and Traffic Information



- Information is viewable in graphical and textual formats.
- Most information is viewable in the web interface.
- Some information is exportable and viewable outside the firewall.

**View threat and traffic information:**



**In the Dashboard**

In the ACC

In the logs

In App Scope reports

In the botnet report

In predefined reports

In custom reports

**Forward threat and traffic information to external services**

An abstract graphic at the bottom of the slide features several curved, translucent bands in shades of orange and red, set against a white background with faint gray X-shaped patterns.

# The Dashboard

- The **Dashboard** consists of a customizable set of widgets.
- A widget is a tool that displays firewall information in a pane.

The screenshot shows the Palo Alto Networks Dashboard interface. At the top, there's a navigation bar with tabs: DASHBOARD (which is selected), ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. Below the navigation bar, there's a toolbar with buttons for Commit, Undo, Redo, and Search. The main area is divided into several sections, each containing a different type of dashboard widget:

- General Information** (Widget A): Shows device details like Device (firewall-a), MGT IP Address (192.168.1.254), and MGT Netmask (255.255.255.0).
- Widgets** (Widget B): A dropdown menu for managing widgets.
- Interfaces** (Widget A): Displays a grid of interface icons numbered 1 through 9.
- Logged In Admins** (Widget A): Shows a table of logged-in administrators, including admin from 192.168.1.20 via Web at 07/27 15:44:42.
- System Logs** (Widget A): Shows log entries related to EDL files.
- System Resources** (Widget A): Shows CPU usage: Manager CPU at 14% and Data Plane CPU at 2%.
- ACC Risk Factor** (Widget A): A gauge showing a risk factor of 2.8 minutes.
- Locks**: Shows "No locks found".
- Config Logs**: Shows "No data available".

A callout box on the left side contains the following text:

A: Example widgets.  
B: Add a widget.  
C: Remove a widget.  
D: Drag and drop to rearrange widgets.

Annotations with yellow circles and letters A, B, C, and D point to specific elements: A points to the General Information and Interface widgets; B points to the Widgets dropdown; C points to the close button of the Logged In Admins widget; D points to the Config Logs section.

# Widgets for Viewing Threat Information

Three **Dashboard** widgets are used to display threat information.

The screenshot shows a Palo Alto Networks PA-VM dashboard with three columns of log entries:

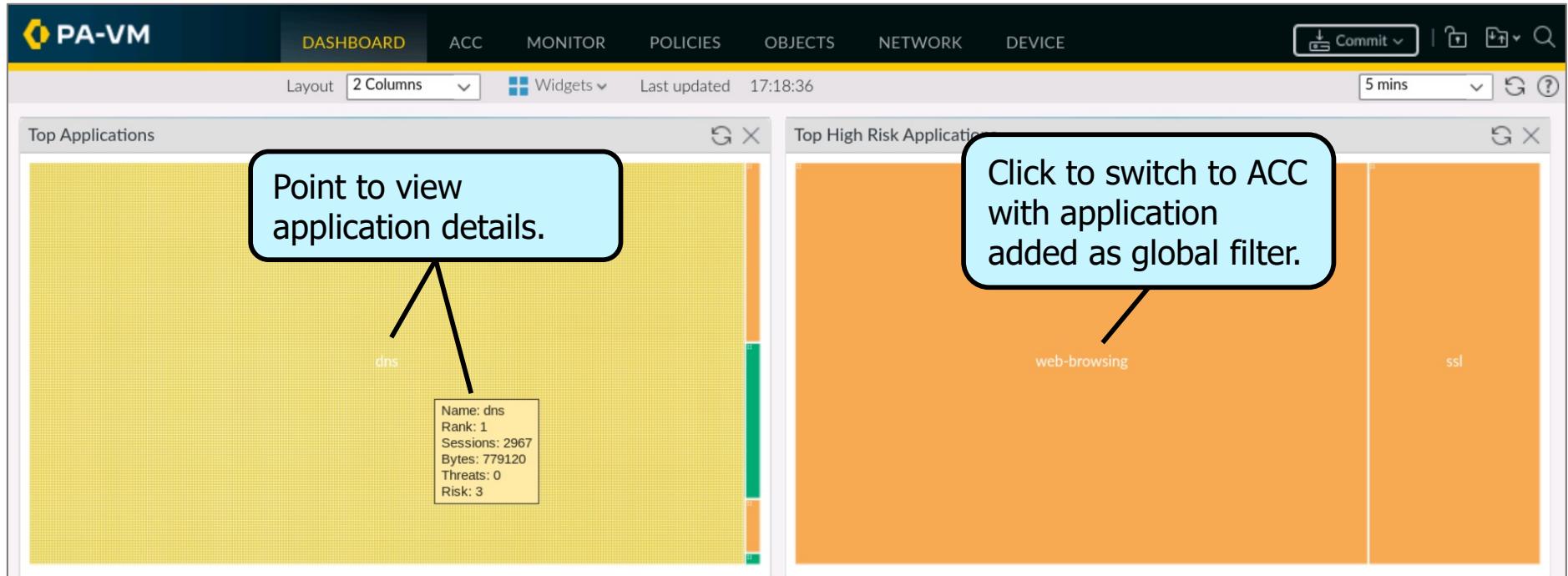
- Data Logs:** Shows log entries for file names, names, and times. Callout: "Last 10 Data Filtering log entries in the last hour".
- URL Filtering Logs:** Shows log entries for URLs, categories, and times. Callout: "Last 10 URL Filtering log entries in the last hour".
- Threat Logs:** Shows log entries for names, severities, and times. Callout: "Last 10 Threat log entries in the last hour".

Dashboard navigation and status:

- Top navigation: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE.
- Header: PA-VM, Commit, Widgets, Last updated: 17:34:42, 5 mins.

# Widgets for Viewing Application Information

Two **Dashboard** widgets are used to display application information.



## **View threat and traffic information:**

**In the Dashboard**



**In the ACC**

**In the logs**

**In App Scope reports**

**In the botnet report**

**In predefined reports**

**In custom reports**

**Forward threat and traffic information to external services**

# Application Command Center (ACC)

The screenshot displays the ACC interface with several key components highlighted:

- Activity tabs**: A callout points to the top navigation bar where "Network Activity" is selected, along with other tabs like Threat Activity, Blocked Activity, Tunnel Activity, GlobalProtect Activity, and SSL Activity.
- Sorts widget data**: A callout points to the sorting dropdown menu located at the top right of the Application Usage and User Activity sections.
- Jumps to logs**: A callout points to the log icon in the top right corner of the User Activity section.
- Applied to all widgets**: A callout points to the global filters on the left side of the screen, which affect all visible widgets.
- Example widgets**: A callout points to the Application Categories heatmap and the detailed application usage table below it.

**Application Categories Heatmap Data:**

Category	Sub-Categories	Applications
business-systems		paloalto-updates, general-business, paloalto-wildfire-cloud, paloalto-dns-security, office-programs, google-docs, apt-get
networking	infrastructure	dns, ssl
general	inter...	googl...
web	web...	file-s...

**Detailed Application Usage Table Data:**

APPLICATION	RISK	BYTES	SESSIONS	THREATS	CONTENT	URLS	USERS	SOURCE...
paloalto-updates	1	86.8M	534	0	0	0	1	1
dns	3	78.0M	272.7k	40	0	0	5	1

**User Activity Graph Data:**

Graph showing bytes sent (green line with circles) and bytes received (blue line with diamonds) over time (17 to 27). The Y-axis ranges from 0 to 100.00M.

Time	bytes_sent	bytes_received
17	~10M	~50M
21	~15M	~15M
24	~10M	~10M
25	~5M	~5M
26	~5M	~5M
27	~5M	~10M

# Widgets on the ACC Network Activity and Threat Activity Tabs

These tabs typically are the most frequently used to view and analyze traffic and threat information.

**Primarily used to view *application* and *traffic* information**

#### **Available Widgets**

- Application Usage
- User Activity
- Source IP Activity
- Destination IP Activity
- Source Regions
- Destination Regions
- GlobalProtect Host Information
- Rule Usage



**Primarily used to view *threat* information**

#### **Available Widgets**

- Threat Activity
- WildFire Activity By File Type
- WildFire Activity By Application
- Host Visiting Malicious URLs
- Host Resolving Malicious Domains
- Applications Visiting Non Standard Ports
- Rules Allowing Apps On Non Standard Ports
- Compromised Hosts

The **Blocked Activity** widgets are useful to show what has been prevented by the firewall.

# Example: Threat Activity Widget

ACC



## **View threat and traffic information:**

In the Dashboard

In the ACC

**In the logs**

In App Scope reports

In the botnet report

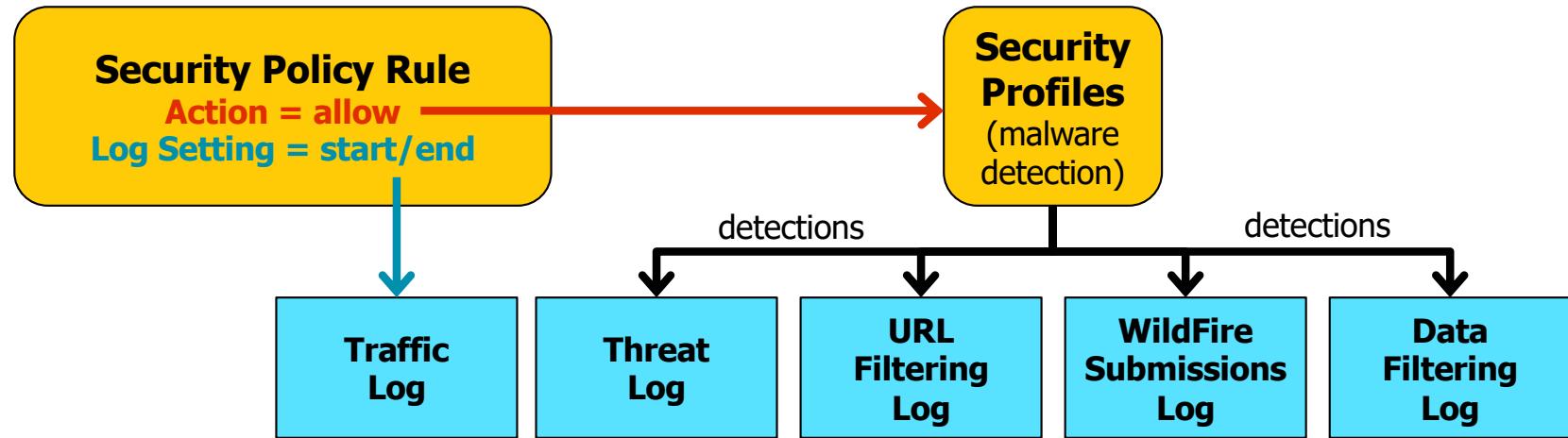
In predefined reports

In custom reports

**Forward threat and traffic information to external services**



# Firewall Logging Overview



- A log contains timestamped information that provides a record of events:
  - Each entry contains a list of artifacts arranged in columns.
- Security policy rules determine what is logged to the Traffic log:
  - Log at session start or session end (end is recommended).
- Security policy and Security Profiles determine what is logged to the other logs.

# Example: Traffic Log

## Monitor > Logs > Traffic

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
Q		07/27 17:34:13	deny	Users_Net	Internet	192.168.1.254	34.96.84.34	443	ssl	allow	Users_to_Internet	decrypt-error	6.7k
Q		07/27 17:34:07	deny	Users_Net	Internet	192.168.1.20	172.217.6.174	80	google-base	reset-both	interzone-default	policy-deny	433
Q		07/27 17:34:00	deny	Users_Net	Internet	192.168.1.20	172.217.6.174	80	google-base	reset-both	interzone-default	policy-deny	433
Q		07/27 17:33:58	deny	Users_Net	Internet	192.168.1.20	172.217.6.174	80	google-base	reset-both	interzone-default	policy-deny	433
Q		07/27 17:33:57	end	Users_Net	Extranet	192.168.1.254	192.168.50.80	80	web-browsing	allow	Users_to_Extranet	tcp-fin	999
Q		07/27 17:33:57	end	Users_Net	Extranet	192.168.1.254	192.168.50.80	80	web-browsing	allow	Users_to_Extranet	tcp-fin	1.0k
Q		07/27 17:33:51	deny	Users_Net	Internet	192.168.1.20	172.217.6.174	80	google-base	reset-both	interzone-default	policy-deny	433
Q		07/27 17:33:49	deny	Users_Net	Internet	192.168.1.20	172.217.6.174	80	google-base	reset-both	interzone-default	policy-deny	433

- Displays an entry for each firewall session:
  - No entry for *in-progress* sessions if **Log Setting = Log at Session End**
- Useful to determine applications seen by the firewall and to improve Security policy

# Example: Threat Log

## Monitor > Logs > Threat

		RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME
1	07/23 16:43:24	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
2	07/23 16:43:05	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
3	07/23 16:42:57	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
4	07/23 16:42:48	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
5	07/23 16:42:42	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
6	07/23 16:42:35	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	
7	07/23 16:42:04	ml-virus	Malicious Windows Executable	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	reset-both	medium	wildfire-test-pe-file.exe	

- Displays entries when threats are detected in allowed traffic.
- *Critical*-severity and *high*-severity threats always should be blocked.
- *Medium*-severity threats might need to be blocked.
- *Low*-severity and *informational*-severity threats should generate an alert.

# Example: URL Filtering Log

## Monitor > Logs > URL Filtering

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
1	07/27 17:22:02	block-per-company-policy	block-per-company-policy,news,low-risk	www.theguardian.com/favicon.ico	Users_Net	Internet	192.168.1.20	151.101.129.111	web-browsing	block-url
2	07/27 17:22:01	block-per-company-policy	block-per-company-policy,news,low-risk	www.theguardian.com/login/css/latofonts....	Users_Net	Internet	192.168.1.20	151.101.129.111	web-browsing	block-url
3	07/27 17:22:01	block-per-company-policy	block-per-company-policy,news,low-risk	www.theguardian.com/	Users_Net	Internet	192.168.1.20	151.101.129.111	web-browsing	block-url
4	07/27 17:21:11	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/favicon.ico	Users_Net	Internet	192.168.1.20	23.64.169.49	web-browsing	block-url
5	07/27 17:21:11	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/login/css/latofonts.css	Users_Net	Internet	192.168.1.20	23.64.169.49	web-browsing	block-url
6	07/27 17:21:11	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/	Users_Net	Internet	192.168.1.20	23.64.169.49	web-browsing	block-url
7	07/27 17:21:05	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/favicon.ico	Users_Net	Internet	192.168.1.20	23.64.169.49	web-browsing	block-url

- Displays entries for URLs or URL categories configured in URL Filtering Profiles:
  - Configure the website or URL category with at least the “alert” action.
- Use the information to improve your Security policy and URL Filtering Profiles.

# Example: WildFire Submissions Log

## Monitor > Logs > WildFire Submissions

	RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	RULE	VERDICT	ACTION	SEVERITY	FILE TYPE
1	07/23 21:08:22	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
2	07/23 20:44:54	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
3	07/23 20:10:31	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
4	07/23 20:10:31	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
5	07/23 19:52:18	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
6	07/23 19:36:17	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
7	07/23 18:49:32	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe
8	07/23 18:41:32	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20	35.222.124.72	80	web-browsing	Users_to_Internet	malicious	allow	high	pe

- Displays submissions by the firewall to WildFire
- Use to determine:
  - Who sent the malware (can it be blocked?)
  - Who received the malware (who potentially is infected?)
  - The filename or URL link used to deliver the malware (what to remove or block)

# Example: Data Filtering Log

## Monitor > Logs > Data Filtering

	RECEIVE TIME	CATEGORY	FILE NAME	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
1	07/17 17:55:24	private-ip-addresses	webmail.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	squirrelmail	alert
2	07/17 17:55:16	private-ip-addresses	login.php	Hypertext Preprocessor PHP File	Users_Net	Extranet	192.168.1.20	192.168.50.150	80	web-browsing	alert
3	07/17 17:51:58	computer-and-internet-info	04457f5911080bb0...	Unknown Binary File	Extranet	Internet	192.168.50.150	91.189.91.38	80	apt-get	alert
4	07/17 17:51:44	computer-and-internet-info	Packages.gz	GZIP	Extranet	Internet	192.168.50.150	104.207.151.13	80	apt-get	alert
5	07/17 17:51:34	computer-and-internet-info	ec430cd4d2899367...	Unknown Binary File	Extranet	Internet	192.168.50.150	91.189.91.39	80	apt-get	alert

- Displays entries when sensitive files or data are seen by the firewall:
  - Configure the File Blocking or Data Filtering Profile with at least the “alert” action.
- Use the information:
  - To improve the security configuration
  - In incident response

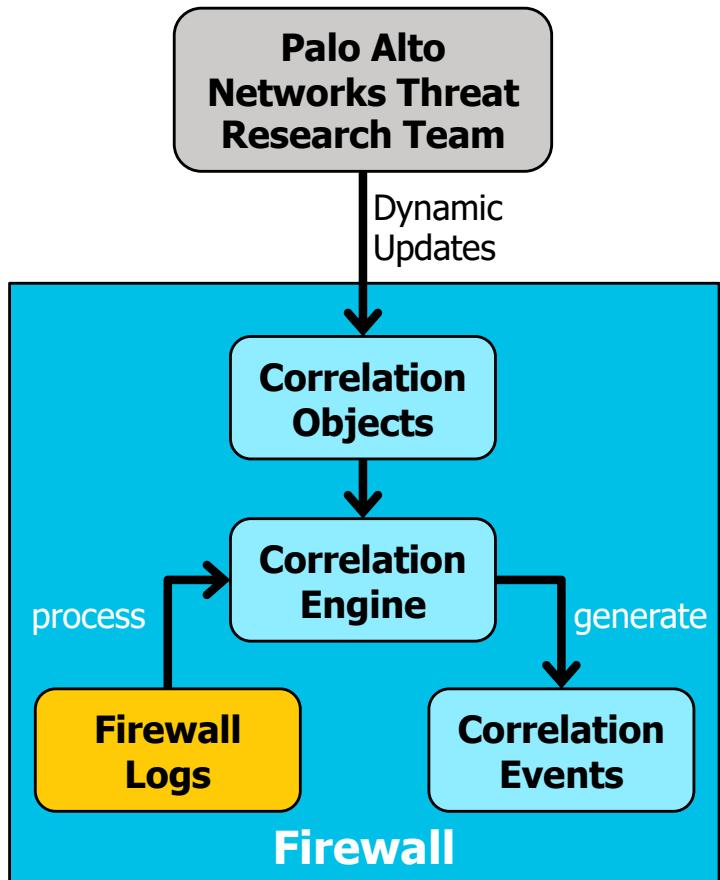
# Example: Unified Log

Monitor > Logs > Unified

The screenshot shows the 'Unified Log' page in the Palo Alto Networks interface. At the top left, there is a search bar with a magnifying glass icon and a dropdown menu icon. To the right of the search bar are icons for refresh, close, and add. Below the search bar is a table with columns: LOG TYPE, RECEIVE TIME, LOG SUBTYPE, SESSION ID, SOURCE ZONE, DESTINA..., SOURCE ADDRESS, DESTINATION ADDRESS, DEST... PORT, APPLICATION, ACTION, RULE, and BYTES. The table contains several log entries, including traffic logs for 'deny' and 'end' events, and dns logs. A large black arrow points from the text 'Show Effective Queries' down to the sidebar. The sidebar has a title 'Show Effective Queries' with a help icon. It includes a 'LOG TYPE' section with checkboxes for 'traffic' (which is checked), 'threat', 'url', 'data', 'wildfire', 'tunnel', 'auth', 'iptag', 'globalprotect', and 'decryption', all of which have 'N/A' next to them. There is also a 'FILTER' section.

- View several log types from a single location:
  - Can modify the list of included log types
- Simplifies threat and traffic investigation and analysis

# Correlation Engine, Objects, and Events



- Automated utility to detect and report possibly infected hosts
- The automated *correlation engine*:
  - Is an analytics tool
  - Examines firewall logs
  - Looks for behavior patterns that match criteria defined in *correlation objects*:
    - Objects define:
      - Pattern to match
      - Logs to reference
      - Time period to look at
    - Generates *correlation events*:
      - Notices of possible infection

## **View threat and traffic information:**

In the Dashboard

In the ACC

In the logs

**In App Scope reports**

In the botnet report

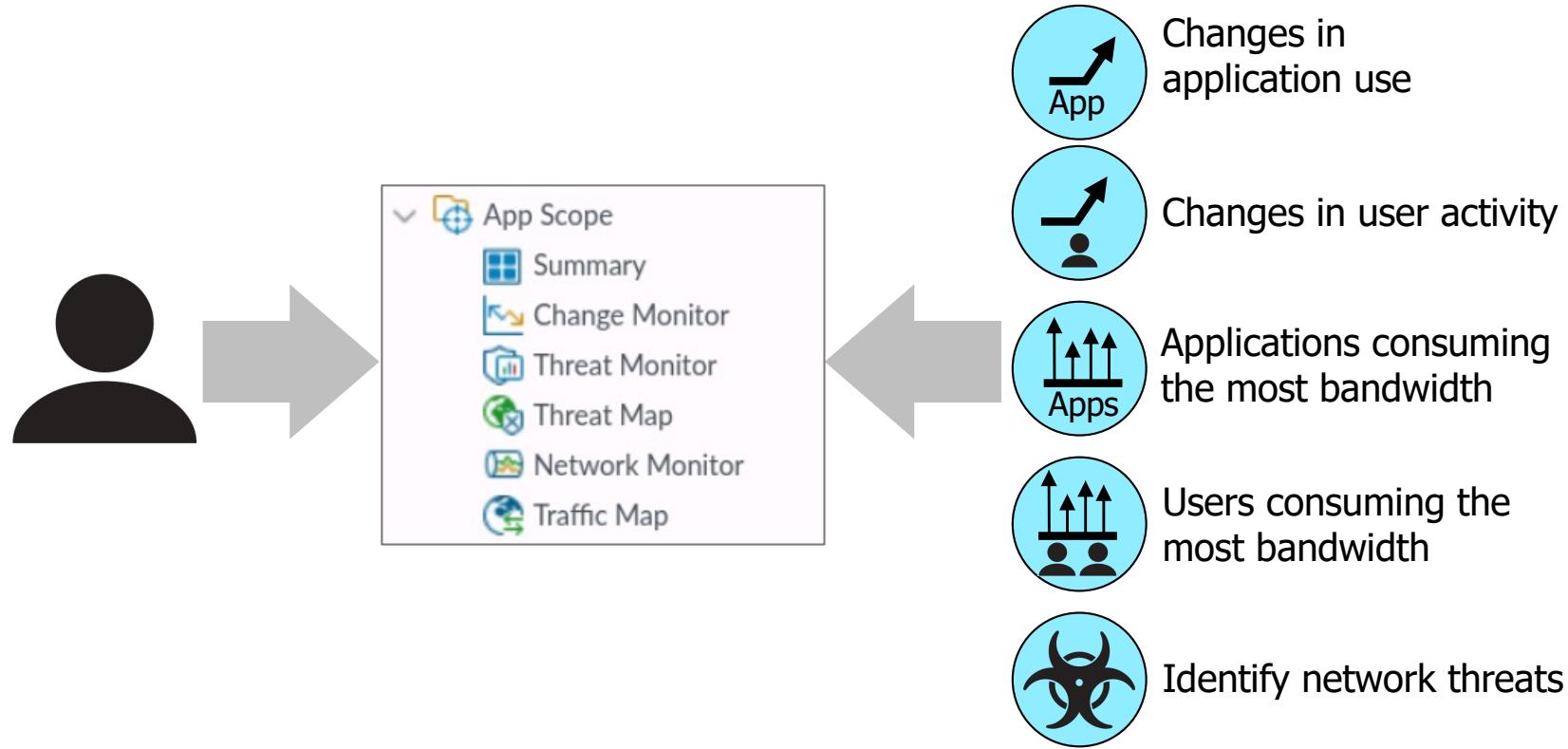
In predefined reports

In custom reports

**Forward threat and traffic information to external services**



# App Scope Reports



# App Scope Reports: What's Available?

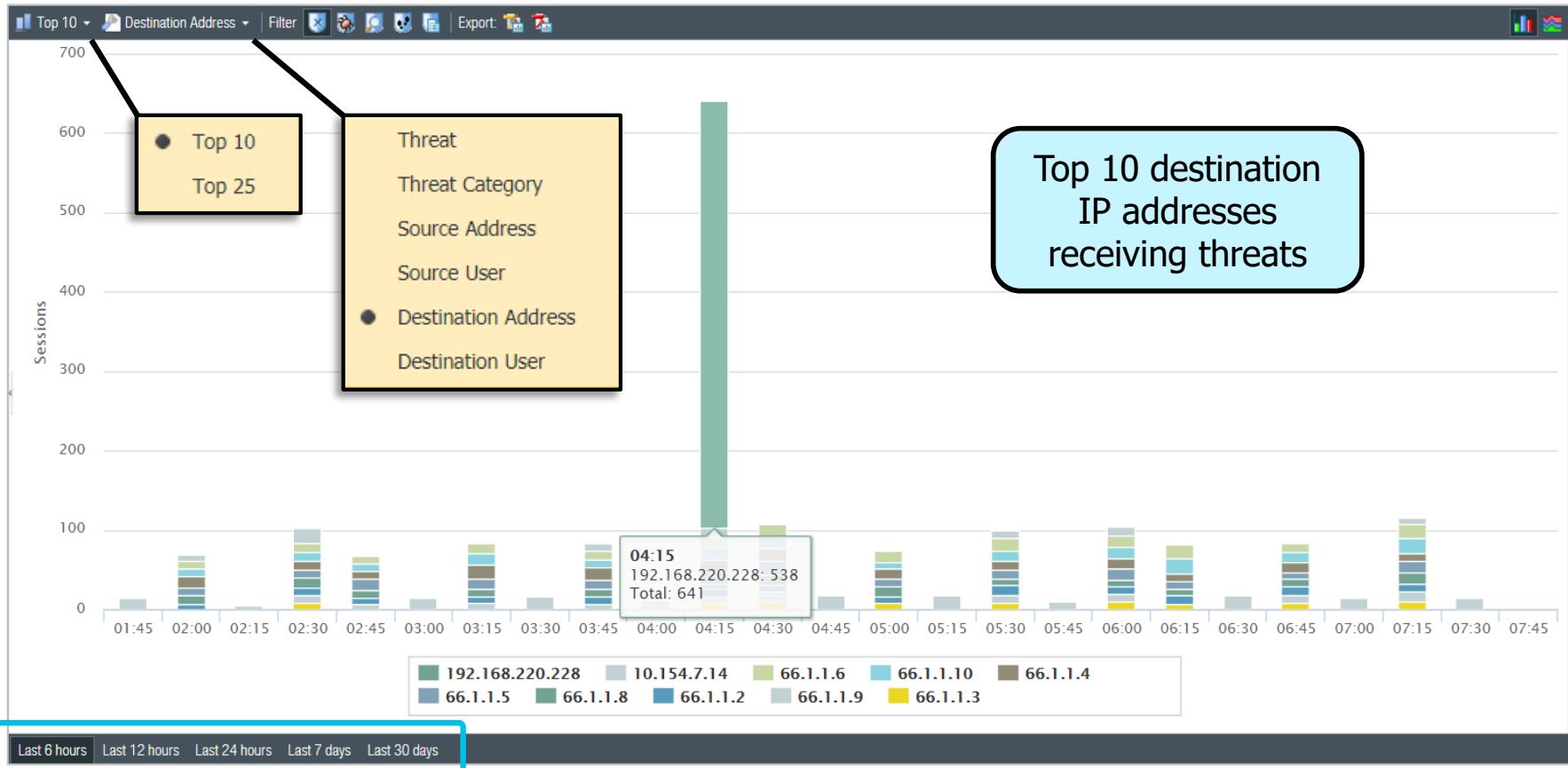
Report Name	Description
Summary Report	Set of six graphical reports displayed in a single browser pane
Top 5 Gainers	Applications showing largest increase in number of sessions (last 60 minutes)
Top 5 Losers	Applications showing largest decrease in number of sessions (last 60 minutes)
Top 5 Bandwidth Consuming Source	Devices sending the most bytes of data (last 60 minutes.)
Top 5 Bandwidth Consuming Apps	Applications sending the most bytes of data (last 24 hours)
Top 5 Bandwidth Consuming App categories	Application categories sending the most bytes of data (last 24 hours)
Top 5 Threats	Threats encountered the most often (last 24 hours)

## App Scope Reports: What's Available? (Cont.)

Report Name	Description
Change Monitor	Applications, users, sources, and destinations showing the largest increase in the number of sessions over the selected time period
Threat Monitor	Threats appearing in the largest number of sessions over the selected time period (by threat name, category, source, or destination)
Threat Map	World map showing sources and destinations of threats (by country)
Network Monitor	Applications, users, sources, and destinations showing the largest network bandwidth consumption over the selected time period
Traffic Map	World map showing sources and destinations of traffic (by country)

# Example: App Scope Report

Monitor > App Scope > Threat Monitor



## **View threat and traffic information:**

In the Dashboard

In the ACC

In the logs

In App Scope reports

**In the botnet report**

In predefined reports

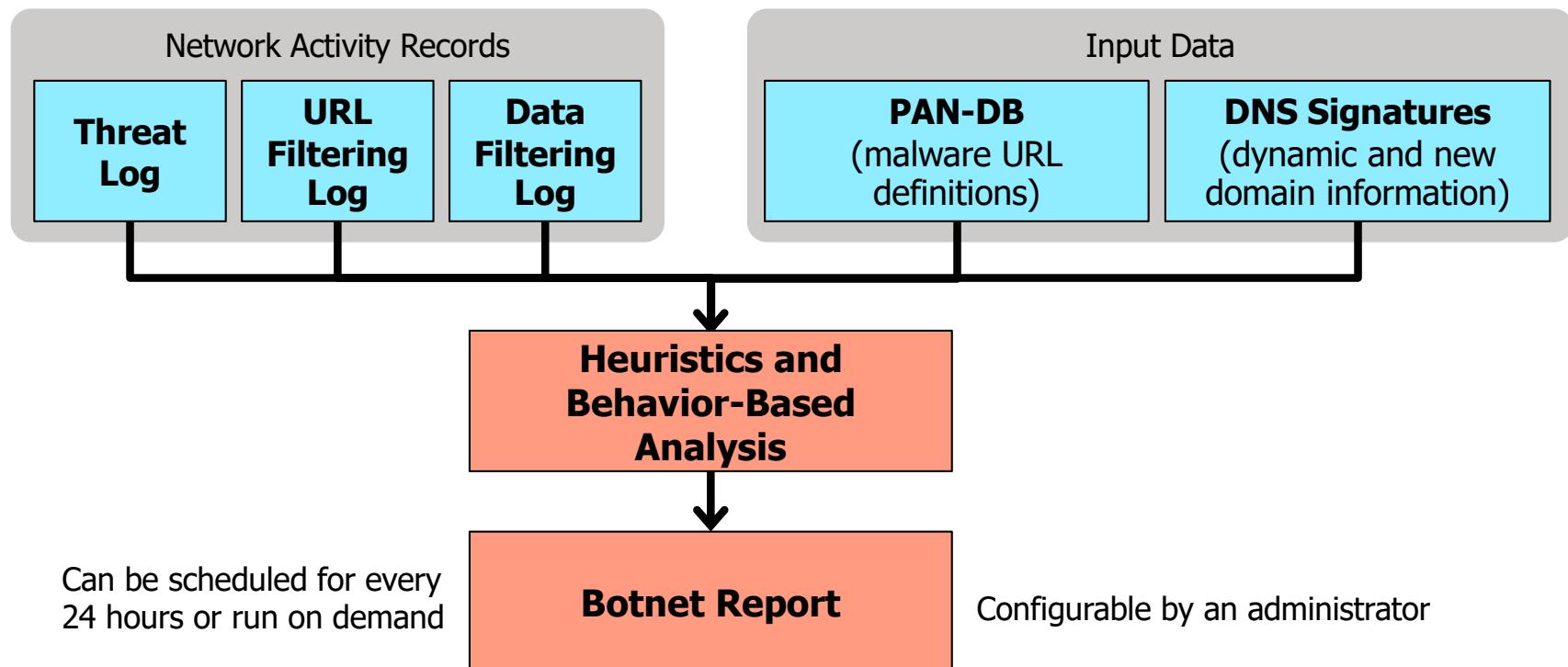
In custom reports

**Forward threat and traffic information to external services**



# Botnet Report

Enables you to identify potential botnet-infected hosts



## **View threat and traffic information:**

In the Dashboard

In the ACC

In the logs

In App Scope reports

In the botnet report

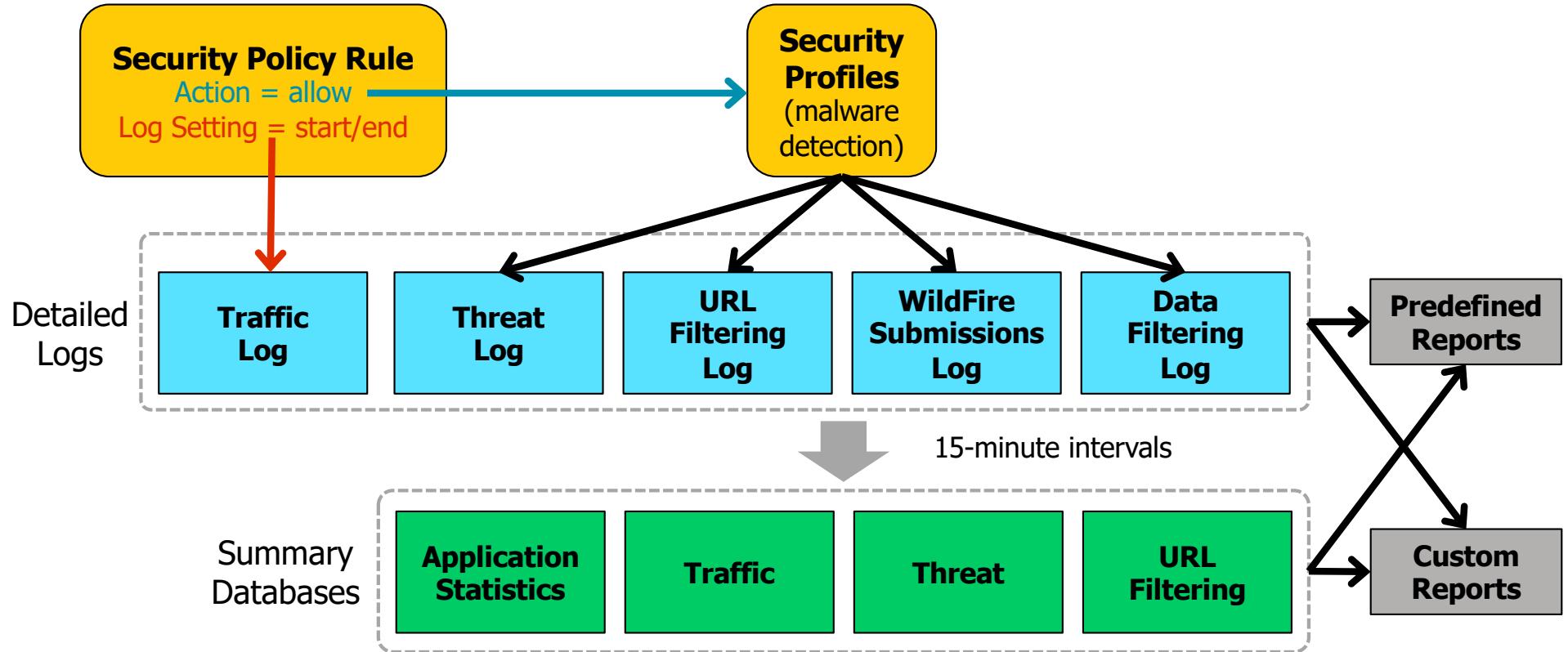
**In predefined reports**

In custom reports



**Forward threat and traffic information to external services**

# Firewall Logging and Reporting Overview



# Predefined Reports

## Monitor > Reports

Application Reports

- New Applications
- Applications
- Application Categories
- Technology Categories
- HTTP Applications
- SaaS Application Usage
- Denied Applications

Traffic Reports

- Security Rules
- Sources
- Source Countries
- Destinations
- Destination Countries
- Connections
- Source Zones
- Destination Zones

Threat Reports

- Botnet
- Threats
- Attacker Sources
- Attacker Destinations
- Attackers By Source Countries
- Attackers By Destination Countries
- Victim Sources
- Victim Destinations

URL Filtering Reports

- URL Categories
- URL Users
- URL User Behavior
- Web Sites
- Blocked Categories
- Blocked Users
- Blocked User Behavior
- Blocked Sites

PDF Summary Reports

- predefined

Click report to view in web interface.

Click to download as a PDF.

- More than 40 predefined reports.
- Arranged in five categories.
- Firewall generates a new report each day.
- To display a report:
  - Click a date.
  - Click a report.

# Example: Threats Report

## Monitor > Reports

	THREAT ID/NAME	ID	THREAT/CONTENT TYPE	COUNT
1	Suspicious TLS Evasion Found	14978	spyware	380
2	Suspicious Domain	12000000	spyware	236
3	Suspicious HTTP Evasion Found	14984	spyware	174
4	41101	41101	vulnerability	1
5	41100	41100	vulnerability	1

Application Reports +  
Traffic Reports +  
Threat Reports -  
Botnet  
**Threats** Select. 26  
Attacker Sources  
Attacker Destinations  
Attackers By Source Countries  
Attackers By Destination Countries  
Victims  
Victim Destinations  
URL Filtering Reports +  
PDF Summary Reports +  
June 2020 27  
S M T W T F S  
31 1 2 3 4 5 6  
7 8 9 10 11 12 13  
14 15 16 17 18 19 20  
21 22 23 24 25 26 27  
28 29 30 1 2 3 4  
5 6 7 8 9 10 11

Export to PDFExport to CSVExport to XML

## **View threat and traffic information:**

In the Dashboard

In the ACC

In the logs

In App Scope reports

In the botnet report

In predefined reports

**In custom reports**



**Forward threat and traffic information to external services**

# Custom Reports

- Custom reports show only the information you want:
  - You choose the logs and log columns to view.
- Schedule reports or run on demand.
- View a report:
  - In the web interface
  - By exporting a PDF, CSV, or XML file

## Monitor > Manage Custom Reports

NAME	DESCRIPTION	DATABASE	TIME FRAME	ROWS	SORT BY	GROUP BY	SCHEDULED
<input type="checkbox"/> Test Report	Test Report for Application Statistics	Application Statistics	Last 30 Days	10	Sessions	category-of-name	<input type="checkbox"/>

**Add** **Delete** **Clone**

Display a custom report.

Create, delete, or clone a report.

# Custom Report Example

## Monitor > Manage Custom Reports

Custom Report

Report Setting | Test Report (100%) X

APP CATEGORY	APP CONTAINER	APPLICATION NAME	DAY RECEIVED	RISK	SESSIONS	THREATS
1 networking		dns	Sun, Jul 26, 2020	3	72.1k	0
2 networking		dns	Sat, Jul 25, 2020	3	68.2k	0
3 networking		dns	Fri, Jul 24, 2020	3	65.8k	0
4 networking		dns	Mon, Jul 27, 2020	3	53.9k	0
5 networking		dns	Thu, Jul 23, 2020	3	18.0k	0
6 networking		dns	Fri, Jul 17, 2020	3	2.3k	0
7 unknown		insufficient-data	Fri, Jul 24, 2020	1	1.4k	0
8 unknown		insufficient-data	Sat, Jul 25, 2020	1	1.4k	0
9 unknown		insufficient-data	Sun, Jul 26, 2020	1	1.4k	0
10 unknown		insufficient-data	Mon, Jul 27, 2020	1	1.2k	0

Selected Columns

- App Category
- App Container
- Application Name
- Day
- Risk

Time Frame | Last 30 Days

Database | Application Statistics

Sort By Sessions | Top 10

Group By App Category | 10 Groups

The screenshot shows a 'Custom Report' window with a table of data. The table has columns: APP CATEGORY, APP CONTAINER, APPLICATION NAME, DAY RECEIVED, RISK, SESSIONS, and THREATS. A red box highlights the first ten rows of the table. A yellow box highlights the 'Group By' dropdown set to 'App Category' and '10 Groups'. A black box highlights the 'Sort By' dropdown set to 'Sessions' and 'Top 10'. A red box highlights the 'Selected Columns' sidebar with items: App Category, App Container, Application Name, Day, and Risk. A yellow box highlights the 'Time Frame' dropdown set to 'Last 30 Days'. A black box highlights the 'Database' dropdown set to 'Application Statistics'. A red box highlights the top navigation bar with 'Report Setting' and 'Test Report (100%) X'.

# Custom Report with a Query Builder Filter

Monitor > Manage Custom Reports > Add

The screenshot shows the 'Report Setting' tab of the 'Custom Report' configuration. On the left, there are fields for Name (Test Report), Description (Test Report for Application Statistics), Database (Application Statistics), and various sorting and grouping options. On the right, there are two columns: 'Available Columns' (App Category, App Sub Category, App Technology, Bytes, Device Name) and 'Selected Columns' (App Container, Application Name, Day, Risk, Sessions). Below these is a toolbar with arrows for Top, Up, Down, and Bottom. At the bottom left is the 'Query Builder' section, which contains the filter '(category-of-name eq networking)'.

Include only log entries where **networking** is the category of name.

- **QueryBuilder** applies filters to source log.
- Only log entries matching the filter are included in the report.
- Filters match only if a specific *value* is in a column.
- This example reports only applications where the category of name equals networking.

# Query Builder Report Example

## Monitor > Manage Custom Reports

Custom Report

Report Setting | Test Report (100%) X

	APP CATEGORY	APPLICATION NAME	DAY RECEIVED	RISK	SESSIONS	THREATS
1	networking	dns	Sun, Jul 26, 2020	3	72.1k	0
2		dns	Sat, Jul 25, 2020	3	68.2k	0
3		dns	Fri, Jul 24, 2020	3	65.8k	0
4		dns	Mon, Jul 27, 2020			0
5		dns	Thu, Jul 23, 2020			0
6		dns	Fri, Jul 17, 2020			0
7		ssl	Thu, Jul 23, 2020	4	601	0
8		netbios-dg	Fri, Jul 17, 2020	2	66	0
9		ssl	Fri, Jul 17, 2020	4	33	0
10		ntp	Fri, Jul 17, 2020	2	32	0

Export to PDF Export to CSV Export to XML

Applications with the App Category of networking

- Report provides intelligence to configure your perimeter Security policy rules.
- Modify the app category name in the filter to see applications from other application categories.

**View threat and traffic information:**

**In the Dashboard**

**In the ACC**

**In the logs**

**In App Scope reports**

**In the botnet report**

**In predefined reports**

**In custom reports**



**Forward threat and traffic information to external services**

# Device Telemetry

- Shared data with Palo Alto Networks.
- Data is used to improve visibility into device health, performance, capacity planning, and configuration.
- Requires a Cortex Data Lake license.

## Device > Setup > Telemetry

Management | Operations | Services | Interfaces | **Telemetry** | Content-ID | WildFire | Session | HSM

**Telemetry**

- Threat Prevention
- Device Health and Performance
- Product Usage

**device-health-performance**

Status success  
Reason  
Last Attempt Thu Jan 23 15:19:04 PST 2020  
Last Success Thu Jan 23 15:19:04 PST 2020  
No. of Failed Attempts 0

**product-usage**

Status success  
Reason

**threat-prevention**

Status success

# Configure Device Telemetry

Device > Setup > Telemetry

The screenshot shows the 'Telemetry' configuration page. At the top, there's a section titled 'Telemetry Sharing' with a descriptive text about the analysis of telemetry data. Below this, under 'Settings', there's a list of data categories with checkboxes. A callout box points to this list with the text: 'Select which categories of data to share.' The categories listed are:

- Enable Telemetry
- Threat Prevention  
Includes URL Filtering and Threat Prevention summaries
- Device Health and Performance  
Includes resource utilization (CPU/Memory/Sessions etc.)
- Product Usage  
Includes configuration

Below the settings, there's a 'Telemetry Region' dropdown set to 'Americas' with a note 'Select Region to enable telemetry'. A callout box points to this region with the text: 'Select Region to enable sharing of device telemetry data.' At the bottom, there's a 'Generate Telemetry File' button, and a callout box points to it with the text: 'Download a live example of data collected and shared.'

# Monitor Device Telemetry

## Device > Setup > Telemetry

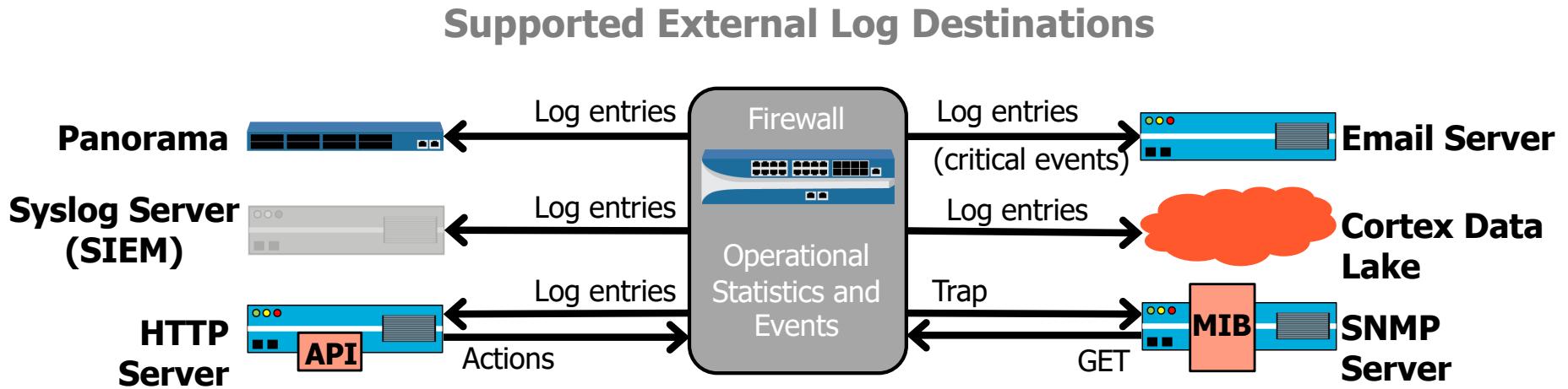
The screenshot shows the 'Telemetry' section of the Device Setup interface. Three categories are selected: Threat Prevention, Device Health and Performance, and Product Usage. Each selection has a corresponding widget on the right side of the screen.

- Threat Prevention:** Status: success, Last Attempt: Thu Jan 23 15:19:04 PST 2020, Last Success: Thu Jan 23 15:19:04 PST 2020, No. of Failed Attempts: 0
- Device Health and Performance:** Status: success, Last Attempt: Thu Jan 23 15:19:04 PST 2020, Last Success: Thu Jan 23 15:19:04 PST 2020, No. of Failed Attempts: 0
- Product Usage:** Status: success, Last Attempt: Thu Jan 23 15:19:04 PST 2020, Last Success: Thu Jan 23 15:19:04 PST 2020, No. of Failed Attempts: 0

A callout box points to the Threat Prevention category with the text: "Widgets display Status for each category selected."

A callout box points to the Product Usage category with the text: "If transmission fails, firewall waits 10 minutes before attempting to resend the data."

# Firewall Log Forwarding Review



- Benefits of log forwarding and centralized logging:
  - Better log availability (off-firewall backup)
  - Centralized log analysis (PAN-OS software or third-party applications)
  - Longer log retention
  - Alerts for critical events
  - Automated responses (via Web API)

# Configure a Server Profile: Syslog Example

- Create a Server Profile:
  - Defines where and how the firewall should connect to an external service

Device > Server Profiles > Syslog > Add

Syslog Server Profile

Name

Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
Syslog1	192.168.50.10	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

How to format forwarded log entries

Facility Options:

- UDP
- TCP
- SSL

Format Options:

- BSD
- IETF

Facility Legend (highlighted in blue):

- LOG\_USER
- LOG\_LOCAL0
- LOG\_LOCAL1
- LOG\_LOCAL2
- LOG\_LOCAL3
- LOG\_LOCAL4
- LOG\_LOCAL5
- LOG\_LOCAL6
- LOG\_LOCAL7

# Configure Logs to Forward: Example

Defines which logs or log entries to forward to which external services

Objects > Log Forwarding > Add

Log Forwarding Profile

Name	Forwarding-Threat-Information	Description	Forwarding Threat Log Information to the Syslog Server
NAME	LOG TYPE	FILTER	FORWARD METHOD
Forwarding-Traffic-Logs	threat	All Logs	SysLog • Syslog-Log-Forwarding
Forwarding-Threat-Logs	threat	(severity eq high)	SysLog • Syslog-Log-Forwarding
Forwarding-WildFire-Logs	wildfire	All Logs	SysLog • Syslog-Log-Forwarding
Forwarding-URL-Logs	url	All Logs	SysLog • Syslog-Log-Forwarding

4 items → X

Add Delete Clone

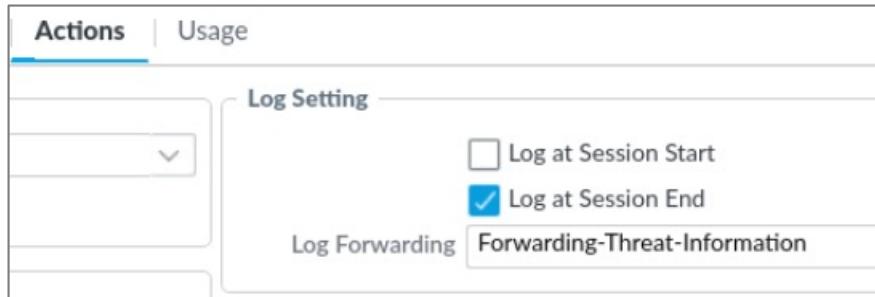
Means all log *entries* (logs are *not* filtered)

Server Profile

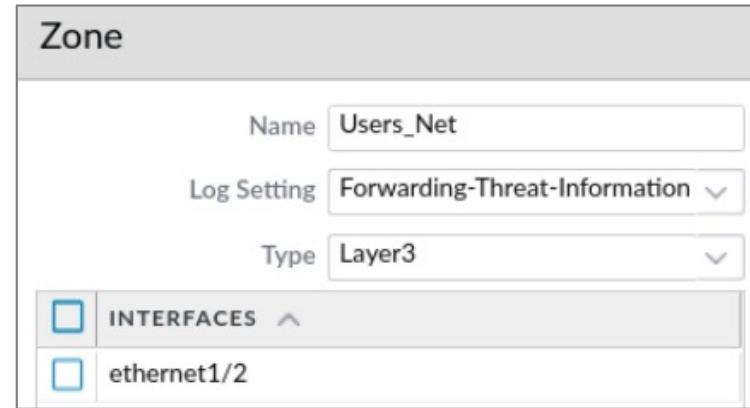
Name	Forwarding-Threat-Information	Description	Forwarding Threat Log Information to the Syslog Server
NAME	LOG TYPE	FILTER	FORWARD METHOD
Forwarding-Traffic-Logs	threat	All Logs	SysLog • Syslog-Log-Forwarding
Forwarding-Threat-Logs	threat	(severity eq high)	SysLog • Syslog-Log-Forwarding
Forwarding-WildFire-Logs	wildfire	All Logs	SysLog • Syslog-Log-Forwarding
Forwarding-URL-Logs	url	All Logs	SysLog • Syslog-Log-Forwarding

# Apply Log Forwarding

Policies > Security > <rule>



Network > Zones > <zone>



- Log forwarding applied per Security policy rule
- Forwards logs for traffic matching:
  - Security policy rule
  - Log Forwarding Profile settings

- Log forwarding applied per security zone
- Forwards threats detected by the Zone Protection Profile

## Module Summary

Now that you have completed this module,  
you should be able to:

- Monitor threat and traffic information using the Dashboard and the ACC
- Monitor threat and traffic information using the logs
- Monitor threat and traffic information using App Scope reports
- Monitor threat and traffic information using the botnet report
- Monitor threat and traffic information using predefined and custom reports
- Configure firewall log forwarding to external services



# Questions



## Lab 19: Viewing Threat and Application Information

- Generate Traffic
- Display Recent Threat and Application Information in the Dashboard
- View Threat and Application Information in the ACC
- View Threat Information in the Threat Log
- View Application Information in the Traffic Log
- View Threats Using App Scope Reports
- View Threat and Application Information Using Predefined Reports
- View Threat and Application Information Using Custom Reports



**Protecting our  
digital way  
of life.**

This page intentionally left blank.