VIEW THREAT AND TRAFFIC INFORMATION

KEEP YOUR EYES ON THE ROAD

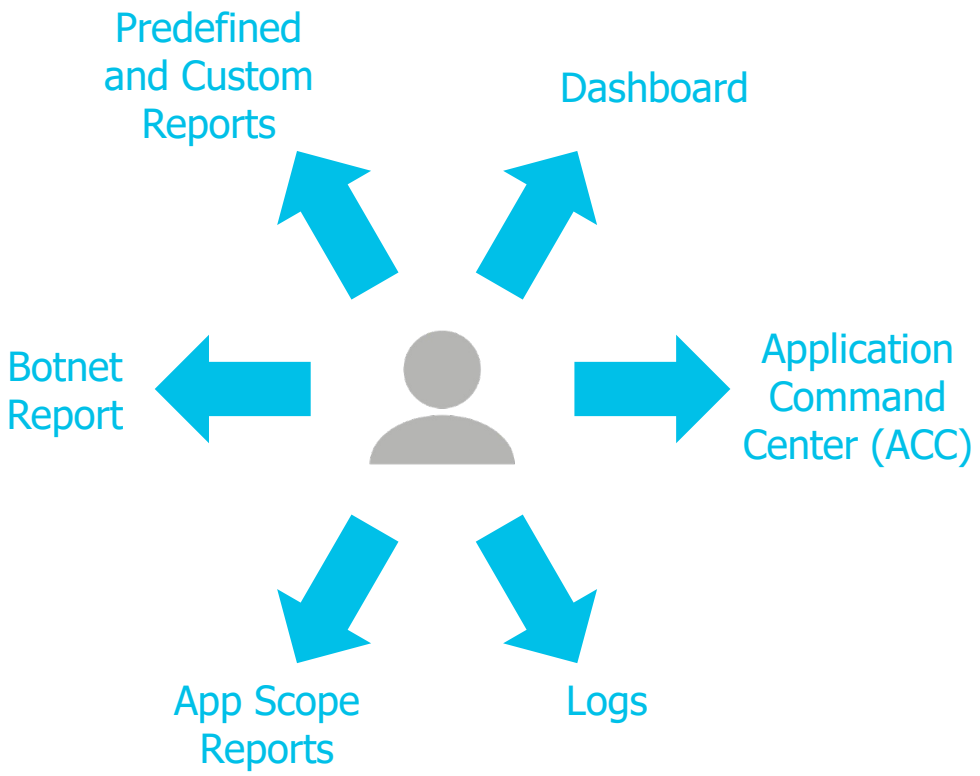
- View threat and traffic information:
  - In the Dashboard
  - In the ACC
  - In the logs
  - In App Scope reports
  - In the botnet report
  - In predefined reports
  - In custom reports
- Forward threat and traffic information to external services

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:

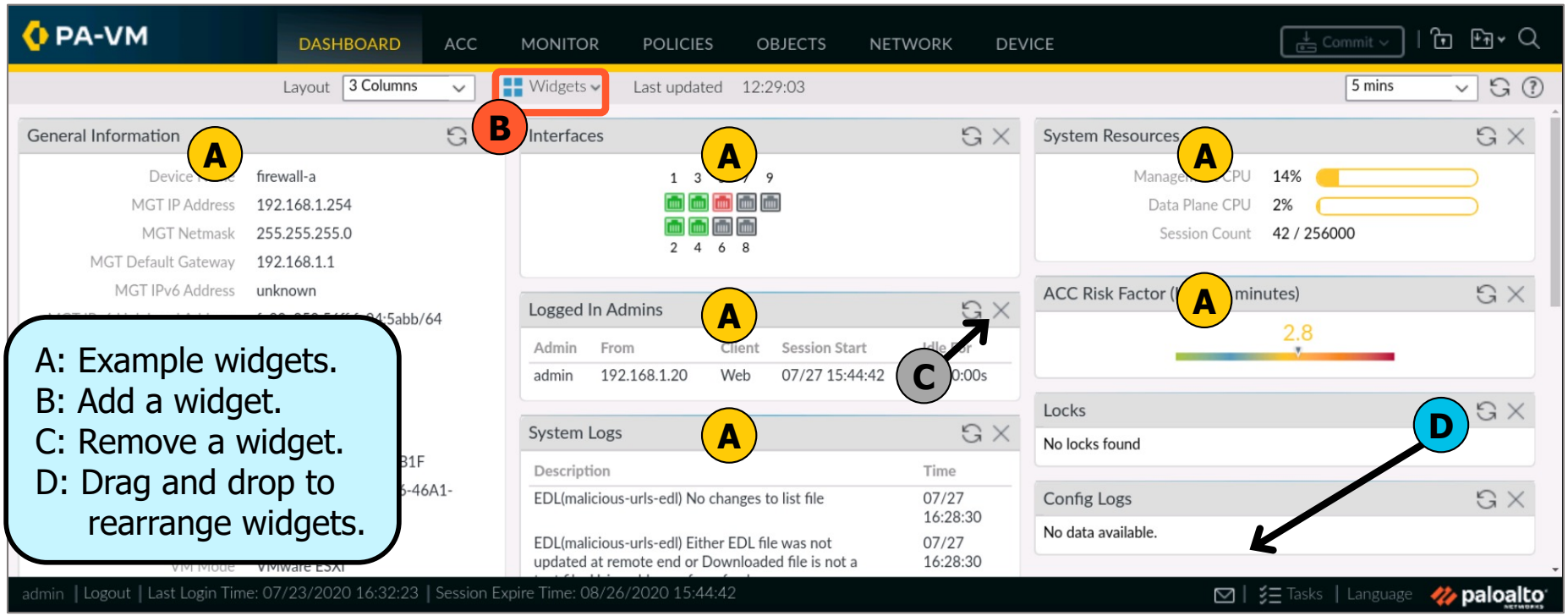
- **In the Dashboard**
- In the ACC
- In the logs
- In App Scope reports
- In the botnet report
- In predefined reports
- In custom reports

Forward threat and traffic information to external services

paloalto NETWORKS

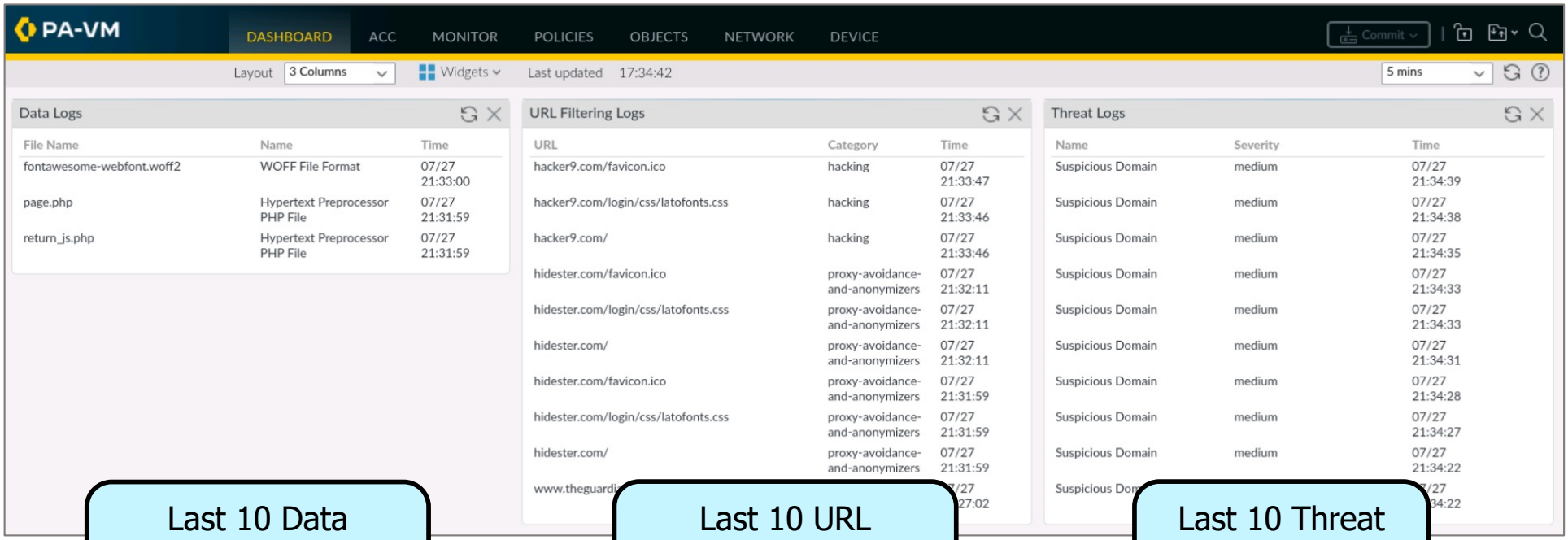
The Dashboard

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



Widgets for Viewing Threat Information

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



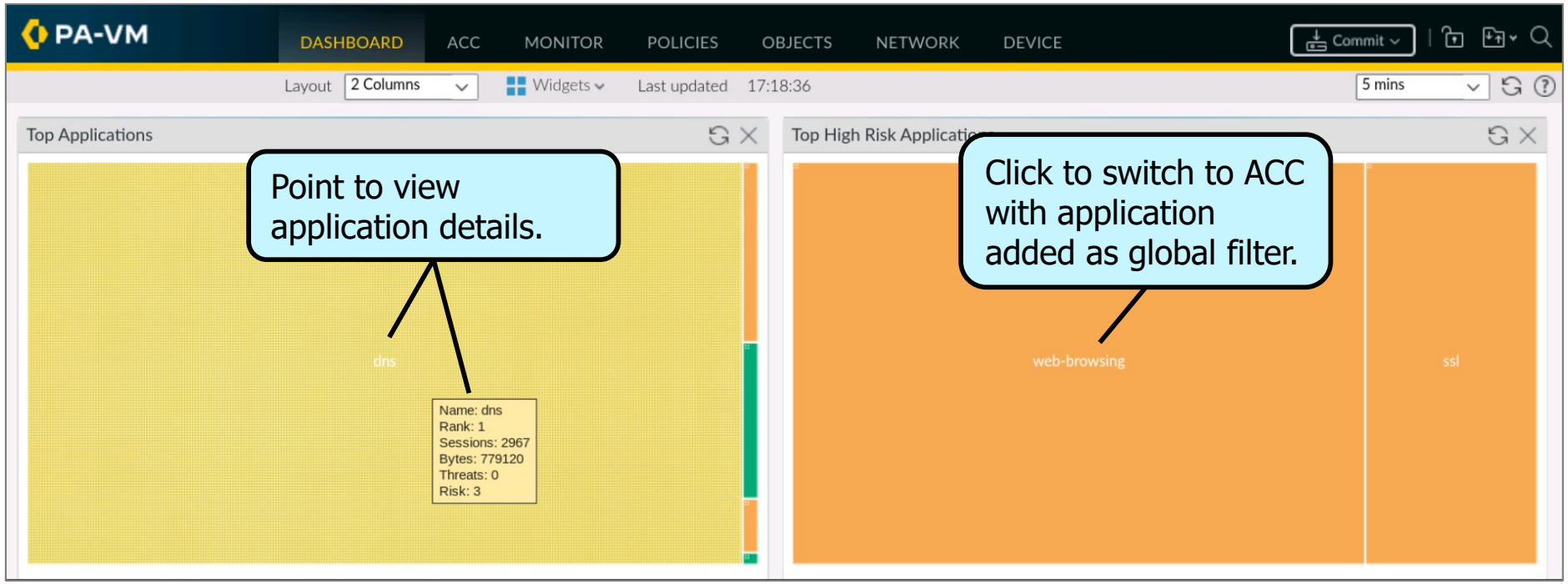
Last 10 Data Filtering log entries in the last hour

Last 10 URL Filtering log entries in the last hour

Last 10 Threat log entries in the last hour

Widgets for Viewing Application Information

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



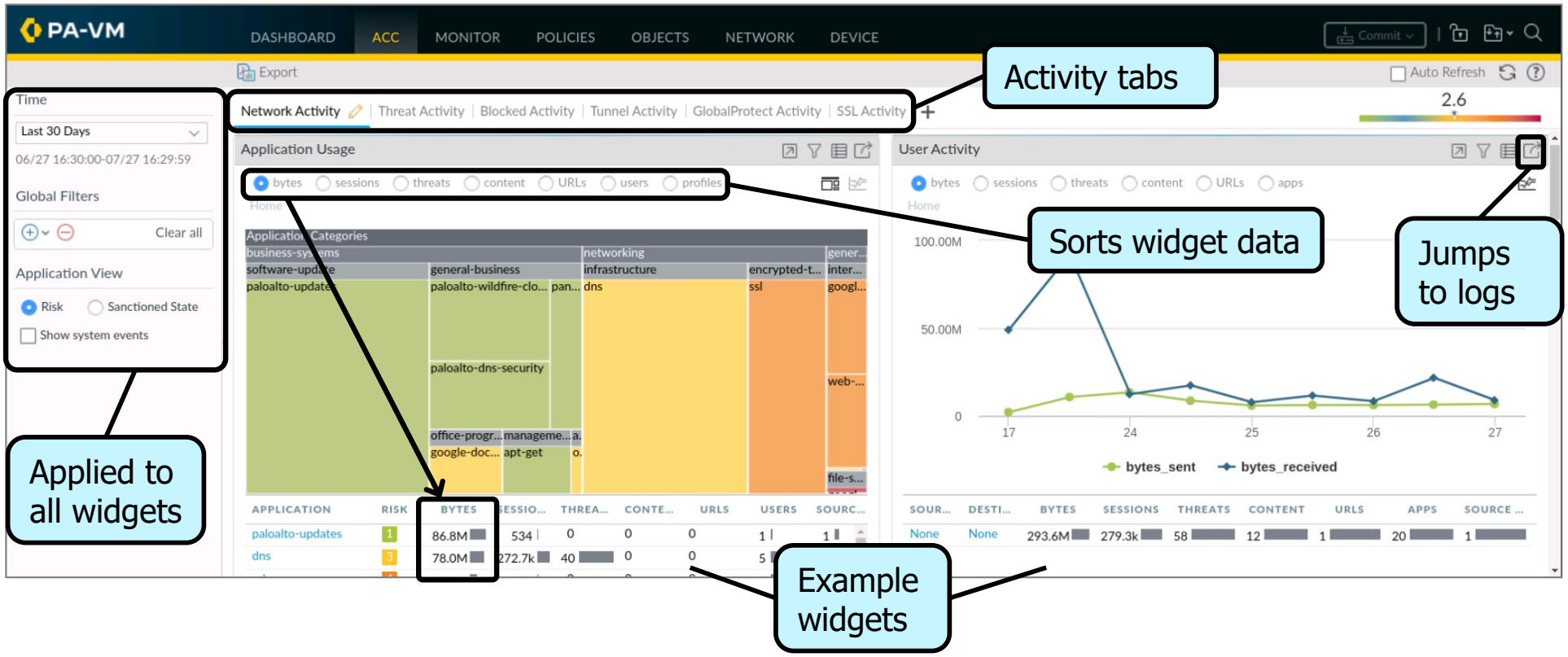
View threat and traffic information:

- 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

paloalto NETWORKS

Application Command Center (ACC)



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

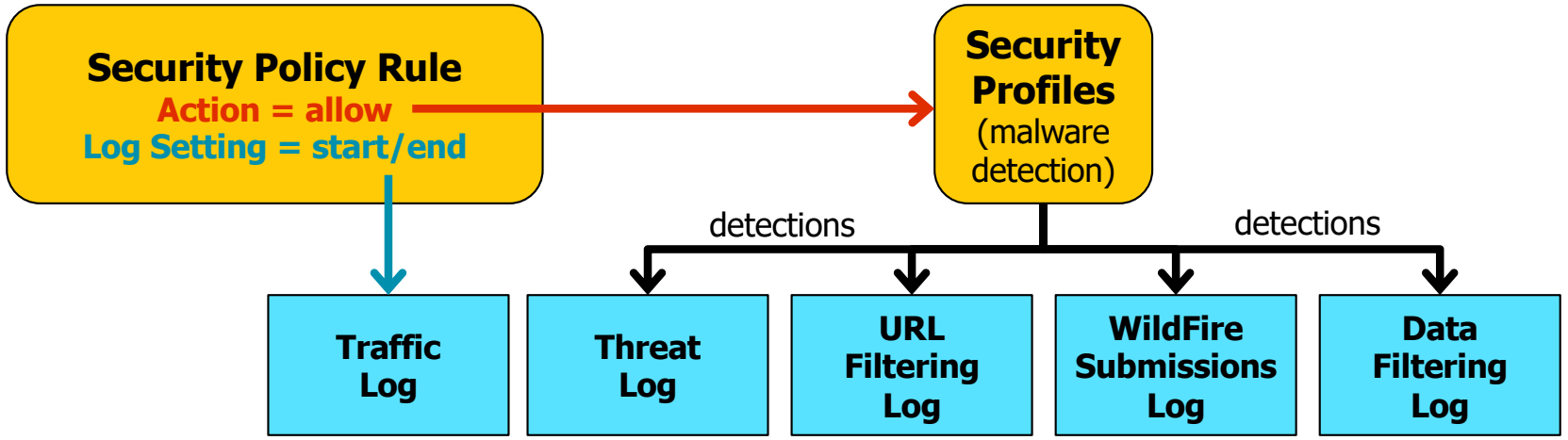
View threat and traffic information:

- 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

paloalto NETWORKS

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
	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
	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
	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
	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
	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
	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
	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
	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
		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.ex
		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.ex
		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.ex
		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.ex
		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.ex
		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.ex
		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.ex

- 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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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

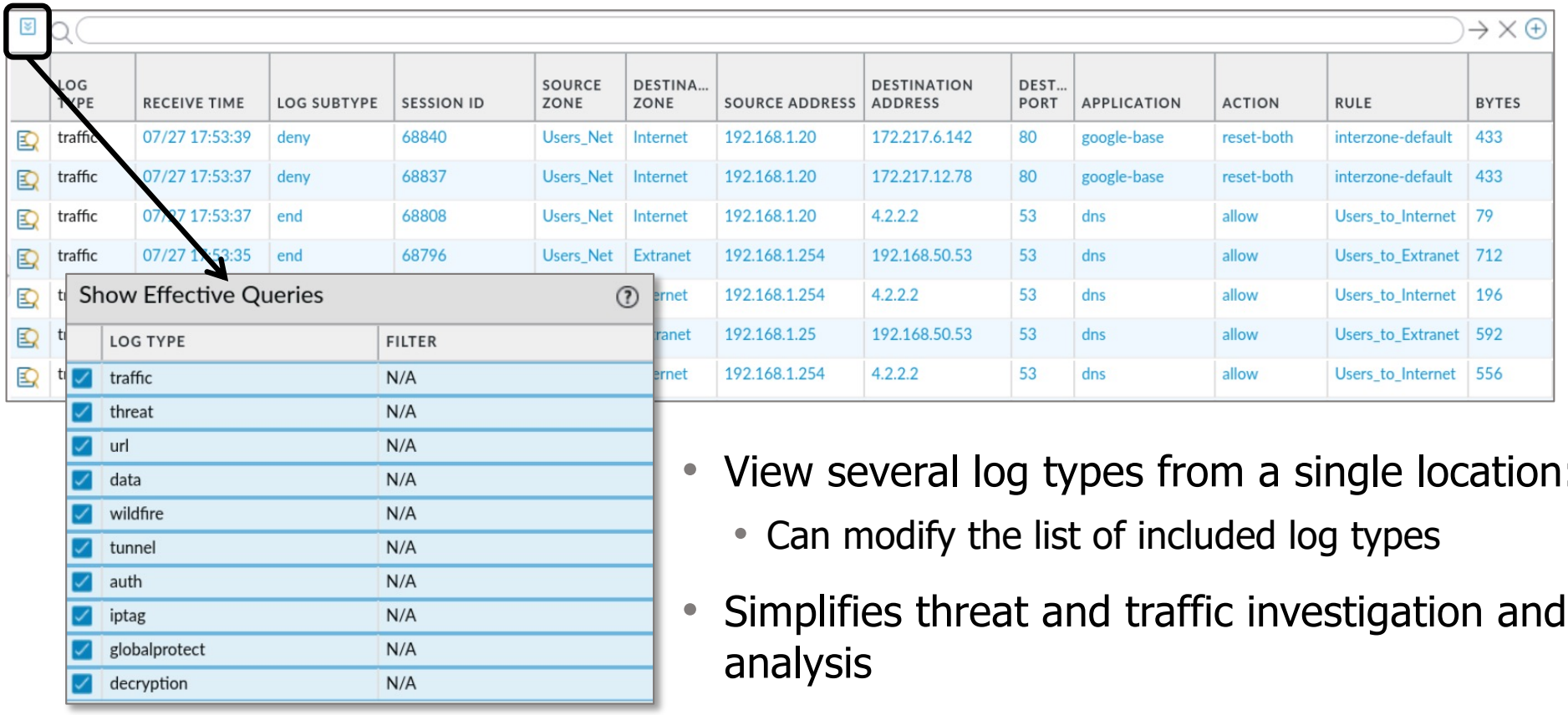
Monitor > Logs > Data Filtering

	RECEIVE TIME	CATEGORY	FILE NAME	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
	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
	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
	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
	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
	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



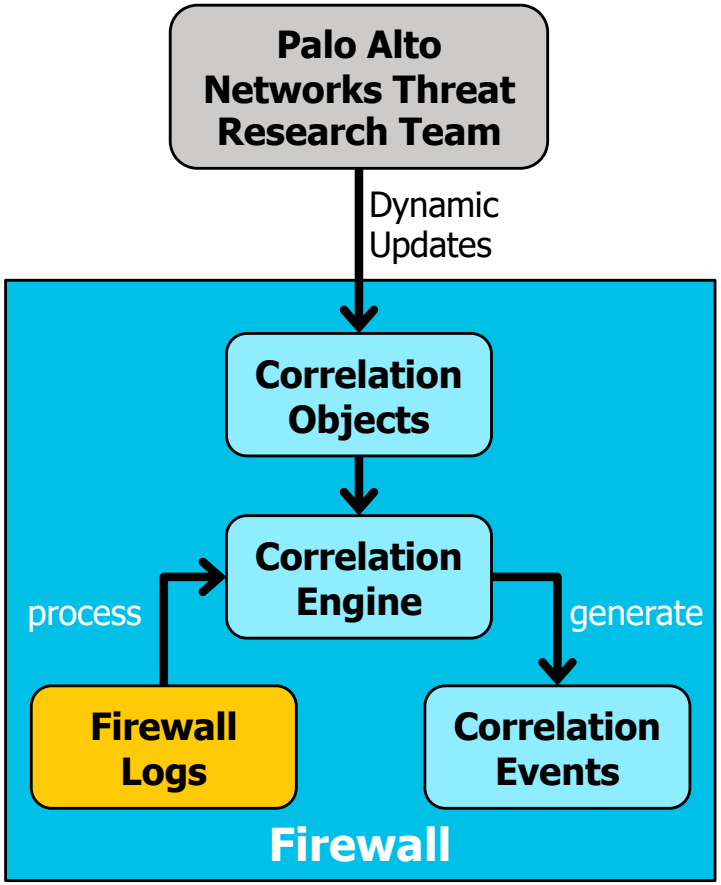
LOG TYPE	RECEIVE TIME	LOG SUBTYPE	SESSION ID	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	ACTION	RULE	BYTES
traffic	07/27 17:53:39	deny	68840	Users_Net	Internet	192.168.1.20	172.217.6.142	80	google-base	reset-both	interzone-default	433
traffic	07/27 17:53:37	deny	68837	Users_Net	Internet	192.168.1.20	172.217.12.78	80	google-base	reset-both	interzone-default	433
traffic	07/27 17:53:37	end	68808	Users_Net	Internet	192.168.1.20	4.2.2.2	53	dns	allow	Users_to_Internet	79
traffic	07/27 17:53:35	end	68796	Users_Net	Extranet	192.168.1.254	192.168.50.53	53	dns	allow	Users_to_Extranet	712
t					ernet	192.168.1.254	4.2.2.2	53	dns	allow	Users_to_Internet	196
t					ranet	192.168.1.25	192.168.50.53	53	dns	allow	Users_to_Extranet	592
t					ernet	192.168.1.254	4.2.2.2	53	dns	allow	Users_to_Internet	556

Show Effective Queries

LOG TYPE	FILTER
traffic	N/A
threat	N/A
url	N/A
data	N/A
wildfire	N/A
tunnel	N/A
auth	N/A
iptag	N/A
globalprotect	N/A
decryption	N/A

- 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

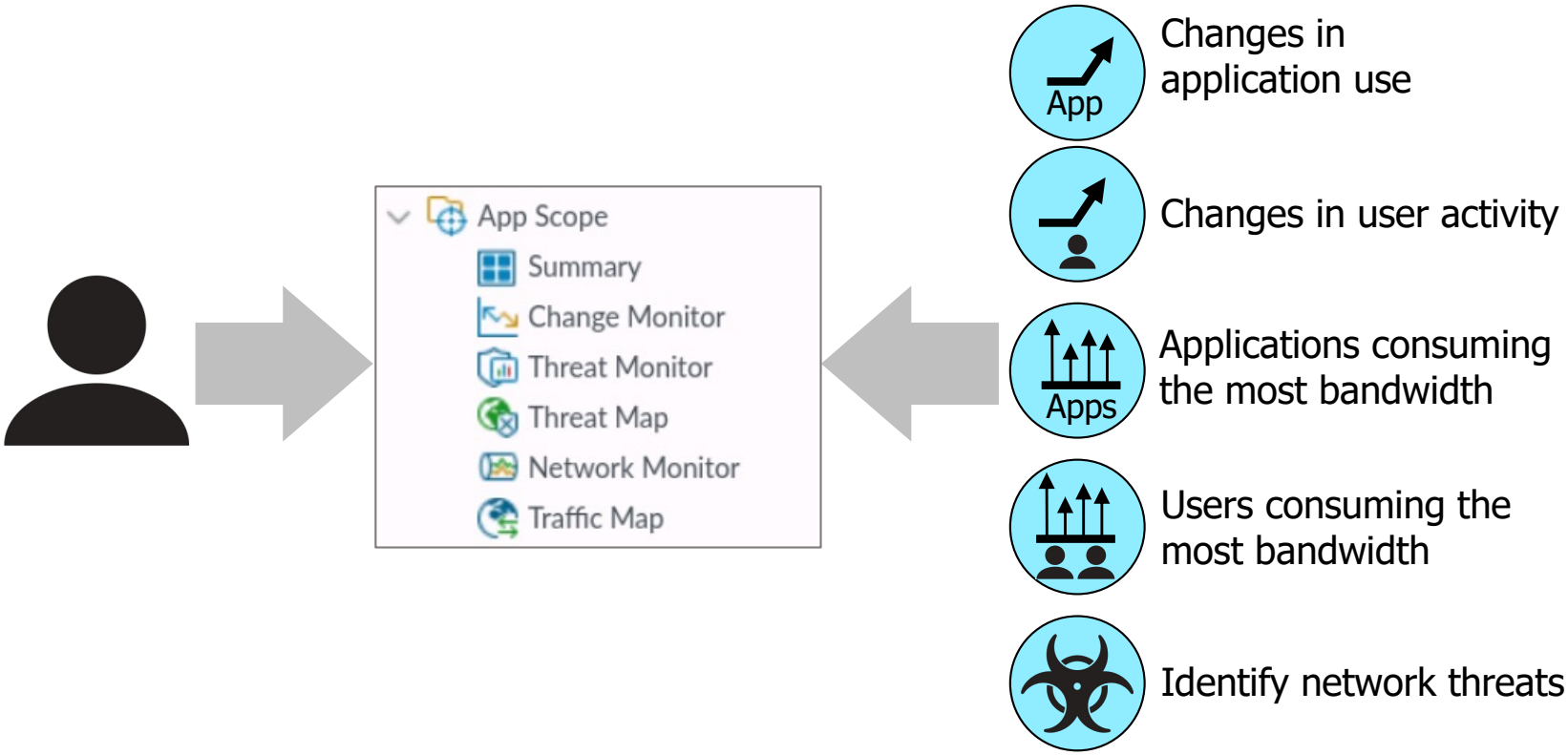
View threat and traffic information:

- 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

paloalto NETWORKS

App Scope Reports



App Scope Reports: What's Available?

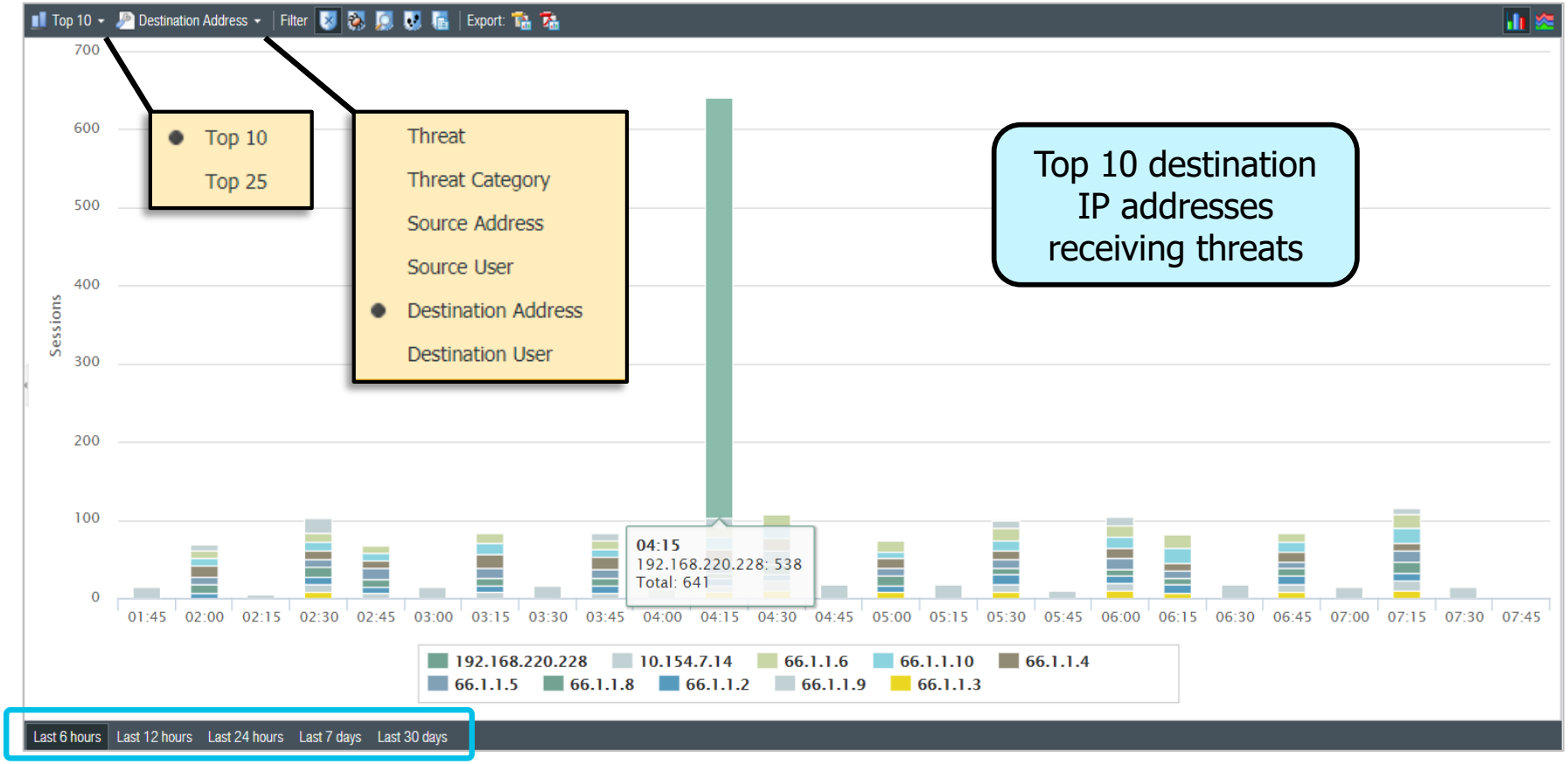
Report Name	Description
Summary Report	Set of six graphical reports displayed in a single browser pane
Top 5 Gainers	Applications showing largest increase in number of sessions (last 60 minutes)
Top 5 Losers	Applications showing largest decrease in number of sessions (last 60 minutes)
Top 5 Bandwidth 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:

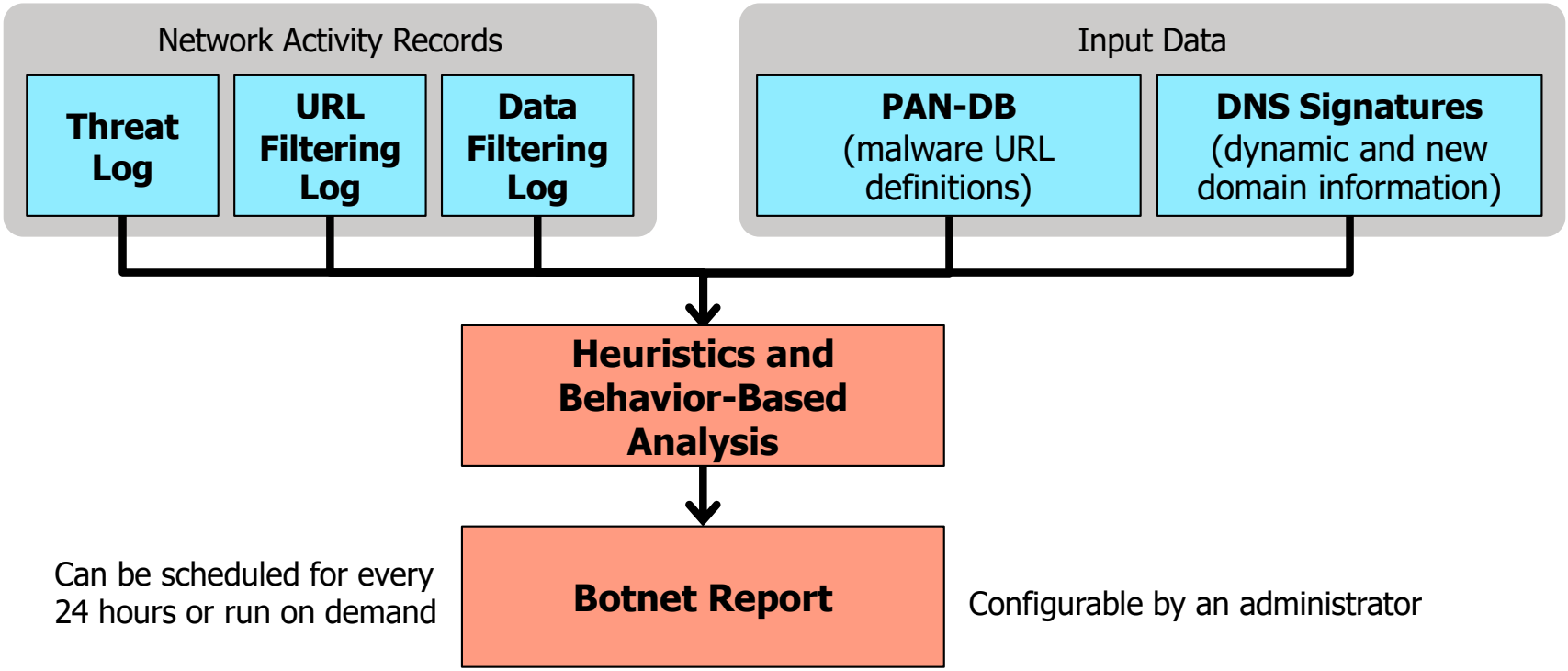
- In the Dashboard
- In the ACC
- In the logs
- In App Scope reports
- **In the botnet report**
- In predefined reports
- In custom reports

Forward threat and traffic information to external services

paloalto NETWORKS

Botnet Report

Enables you to identify potential botnet-infected hosts



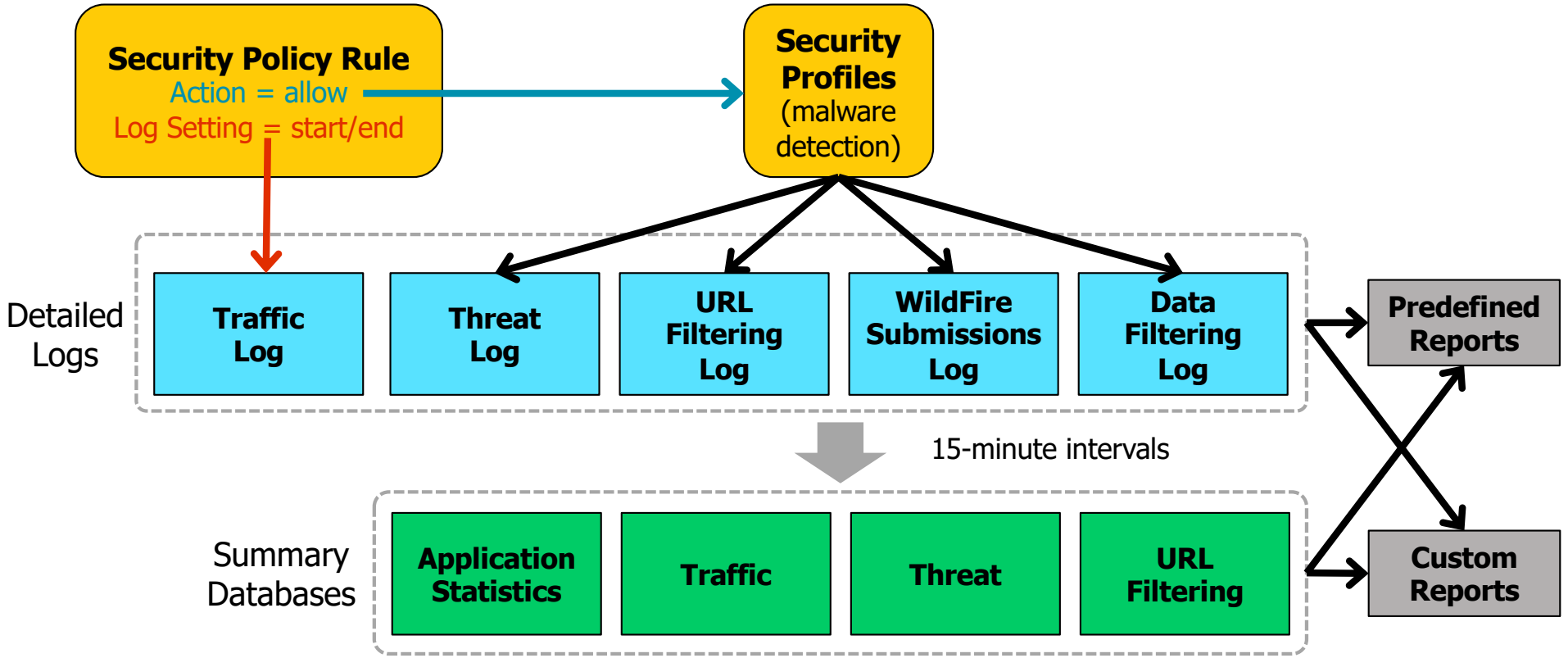
View threat and traffic information:

- 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

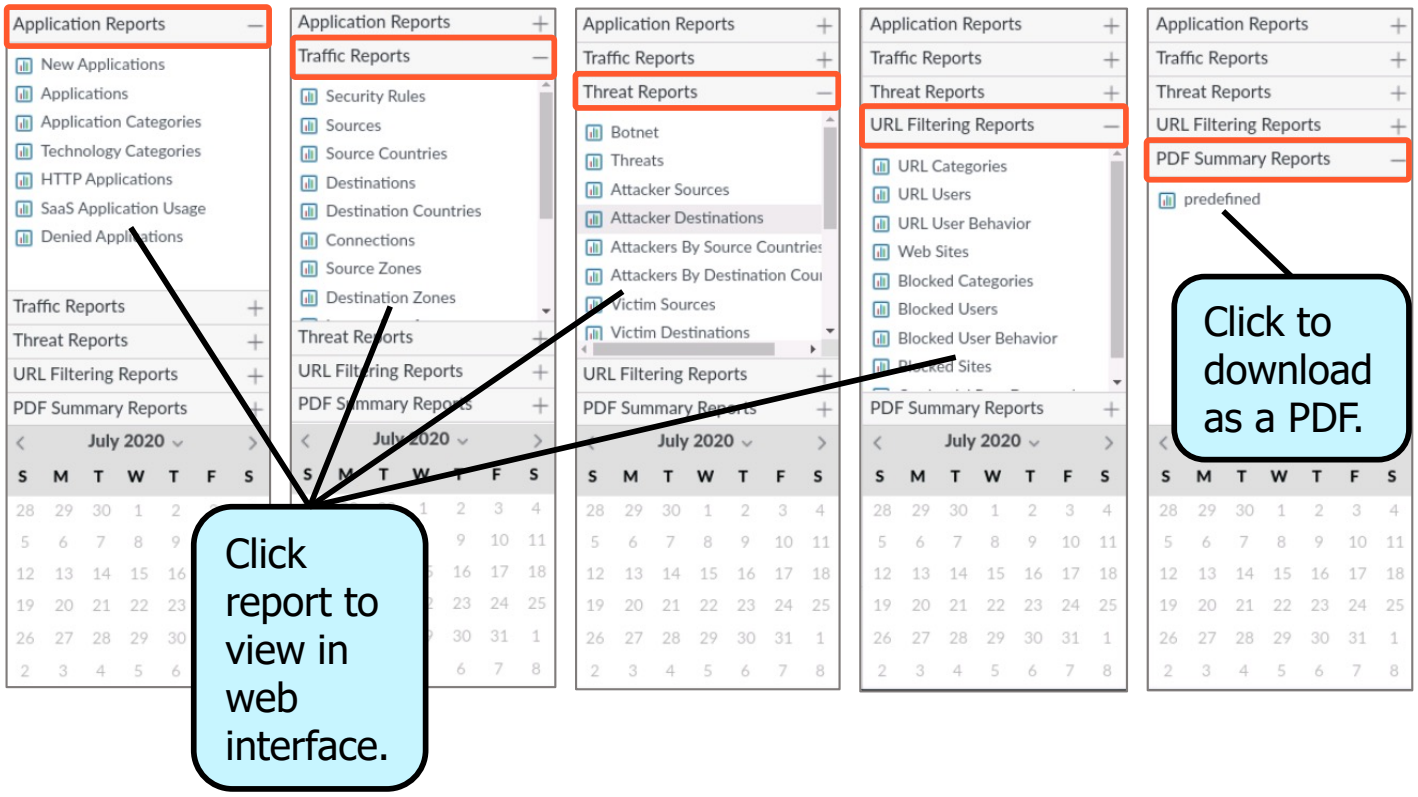
paloalto NETWORKS

Firewall Logging and Reporting Overview



Predefined Reports

Monitor > Reports



- 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

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**

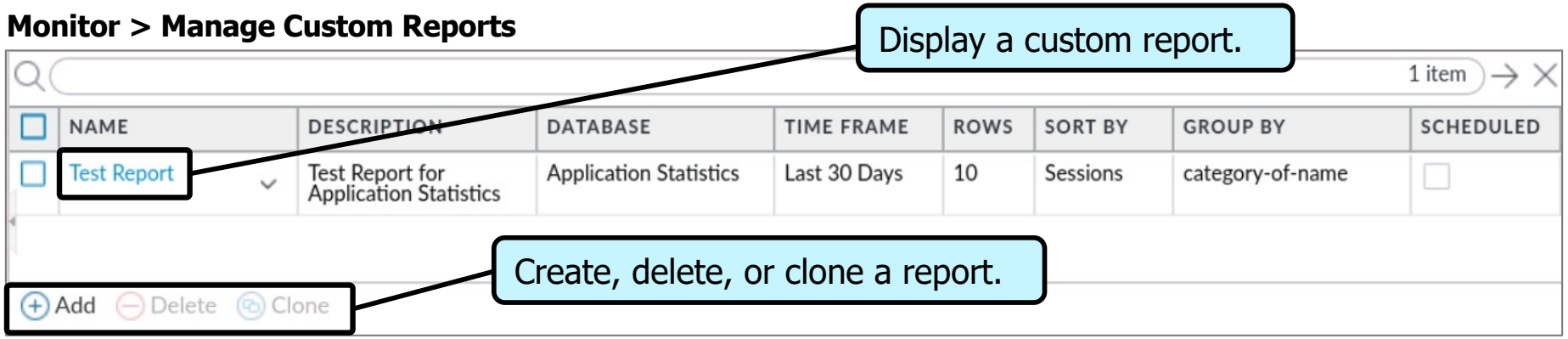
Forward threat and traffic information to external services

paloalto NETWORKS

Custom Reports

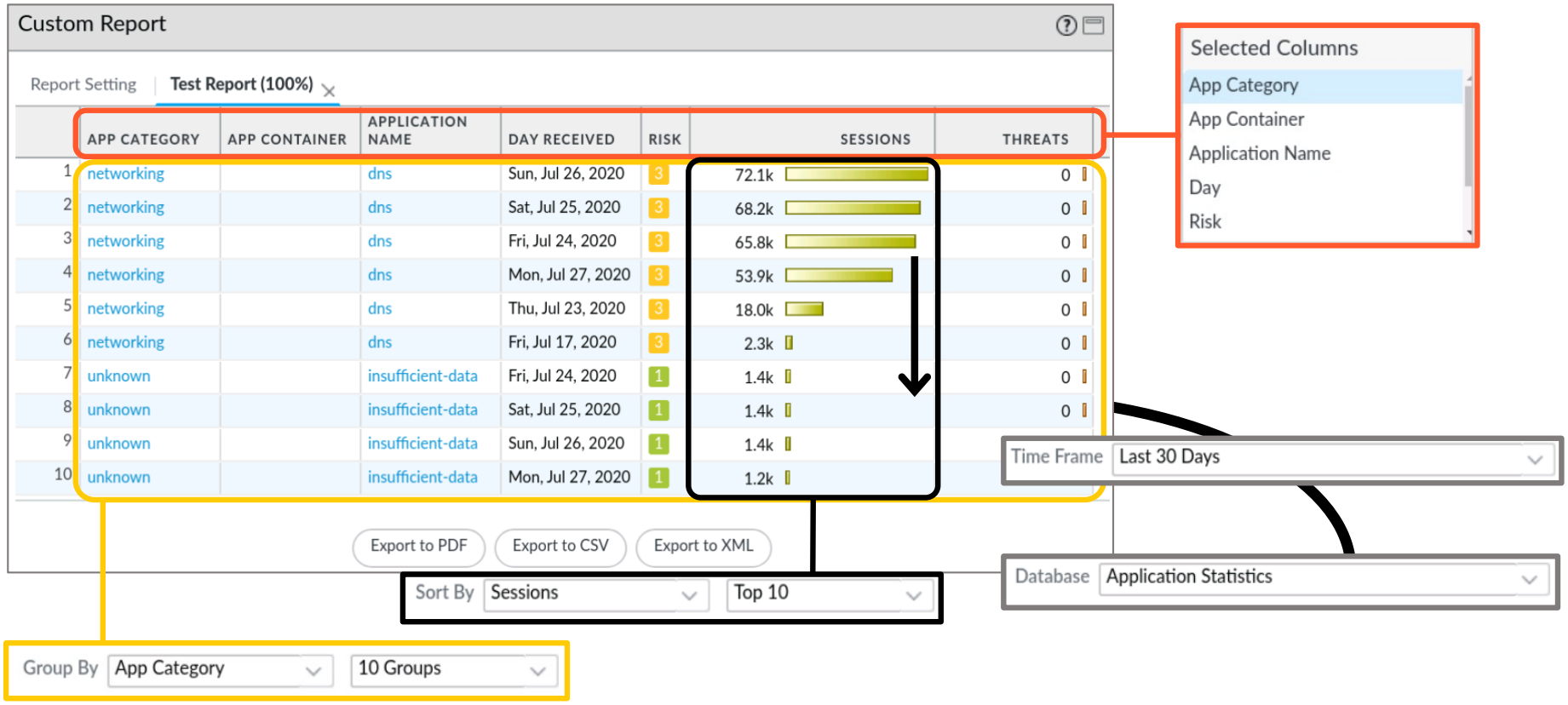
- Custom reports show only the information you want:
  - You choose the logs and log columns to view.
- Schedule reports or run on demand.
- View a report:
  - In the web interface
  - By exporting a PDF, CSV, or XML file

Monitor > Manage Custom Reports



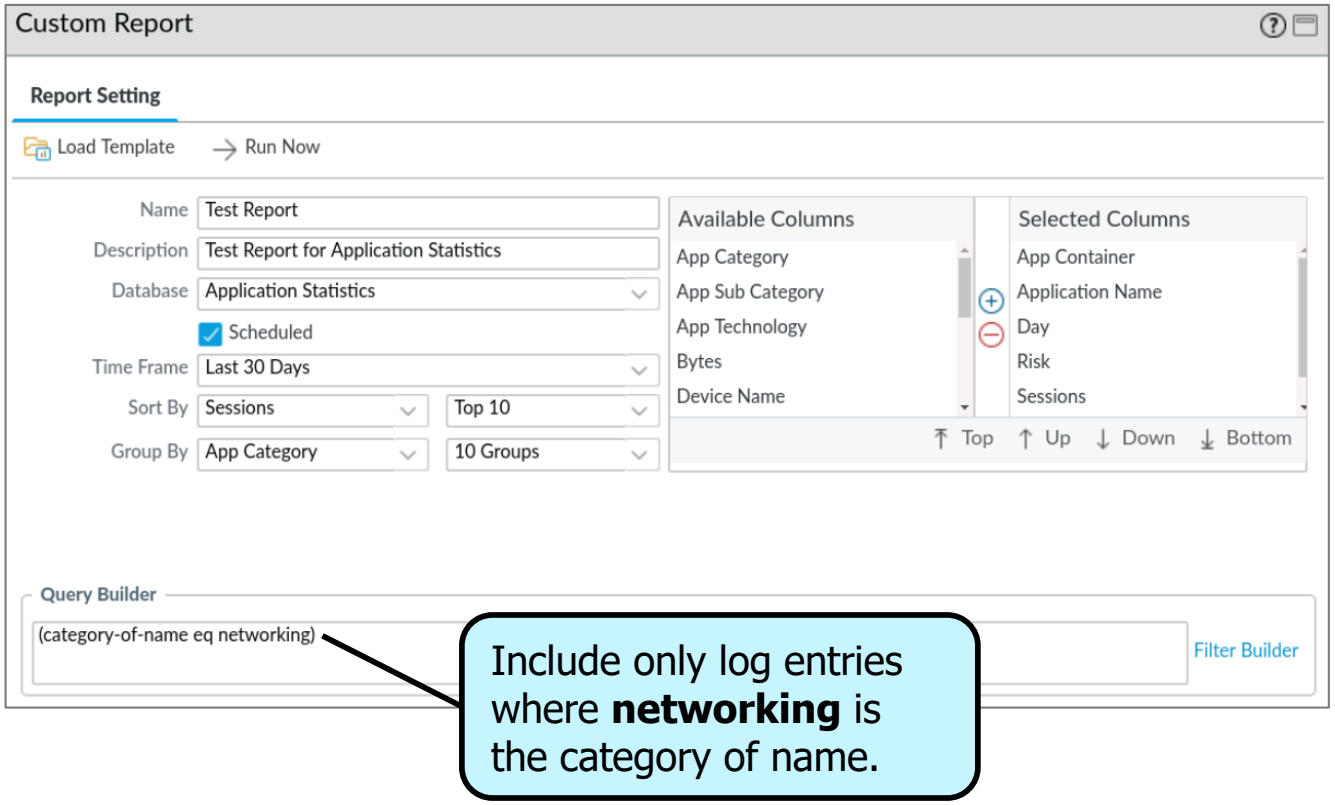
Custom Report Example

Monitor > Manage Custom Reports



Custom Report with a Query Builder Filter

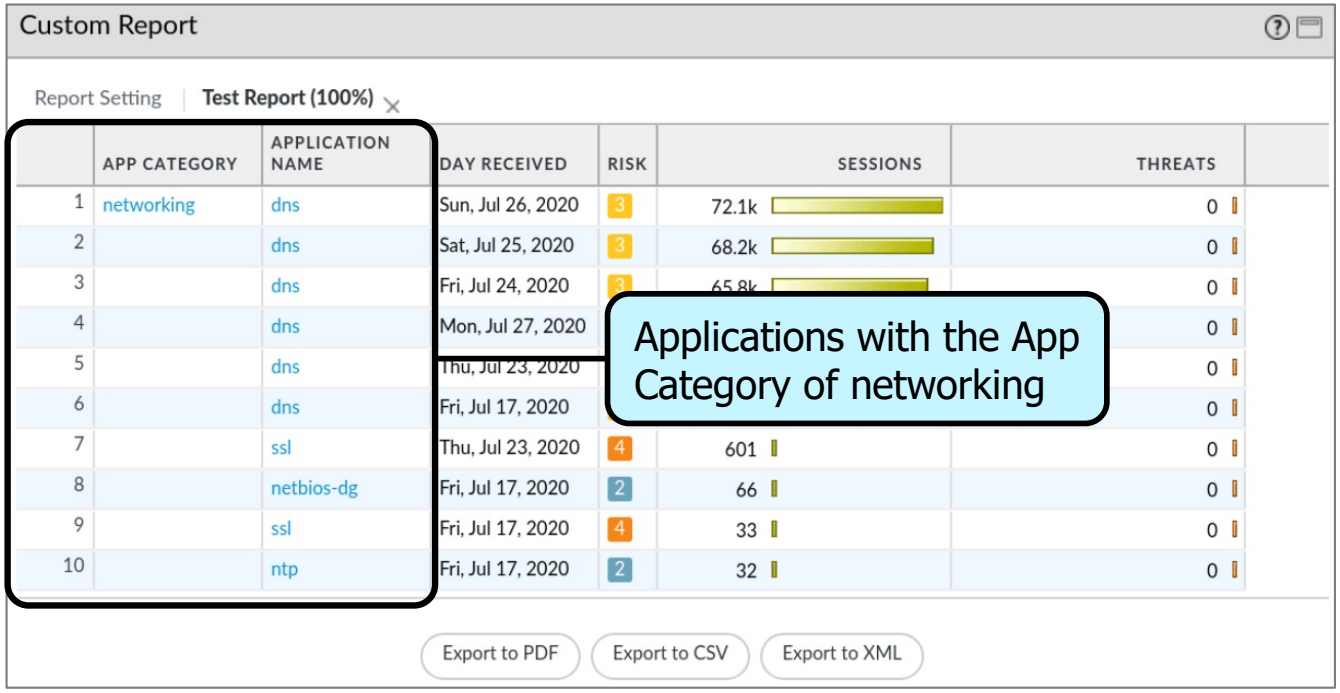
Monitor > Manage Custom Reports > Add



- **Query Builder** 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



	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

- 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

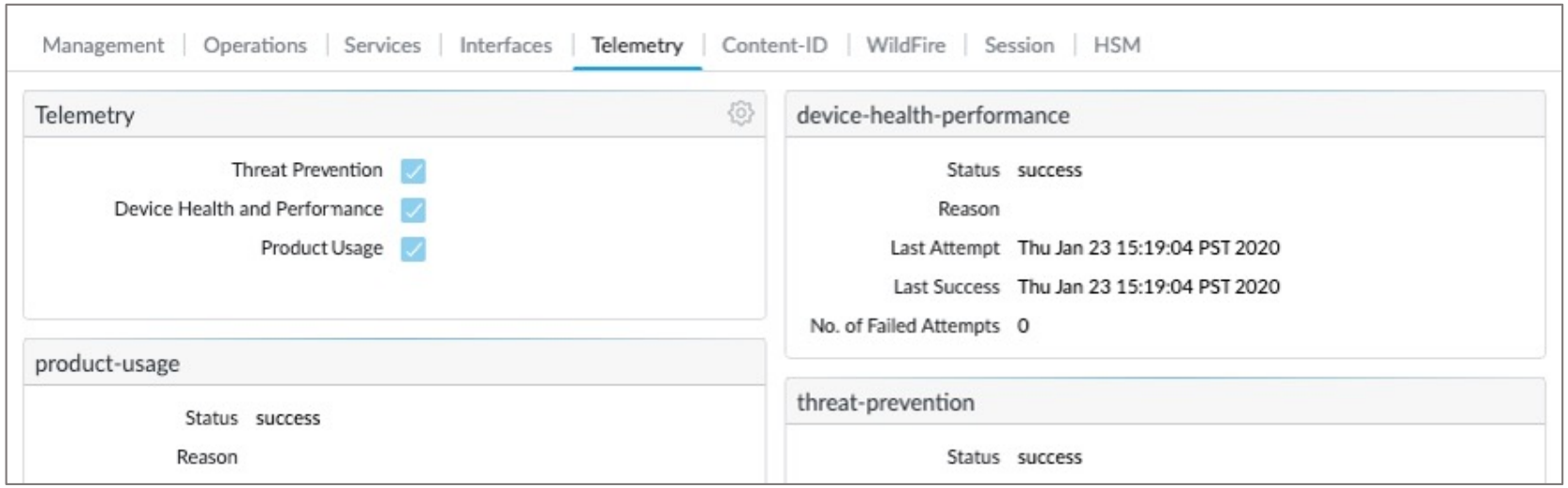
Forward threat and traffic information to external services

paloalto NETWORKS

Device Telemetry

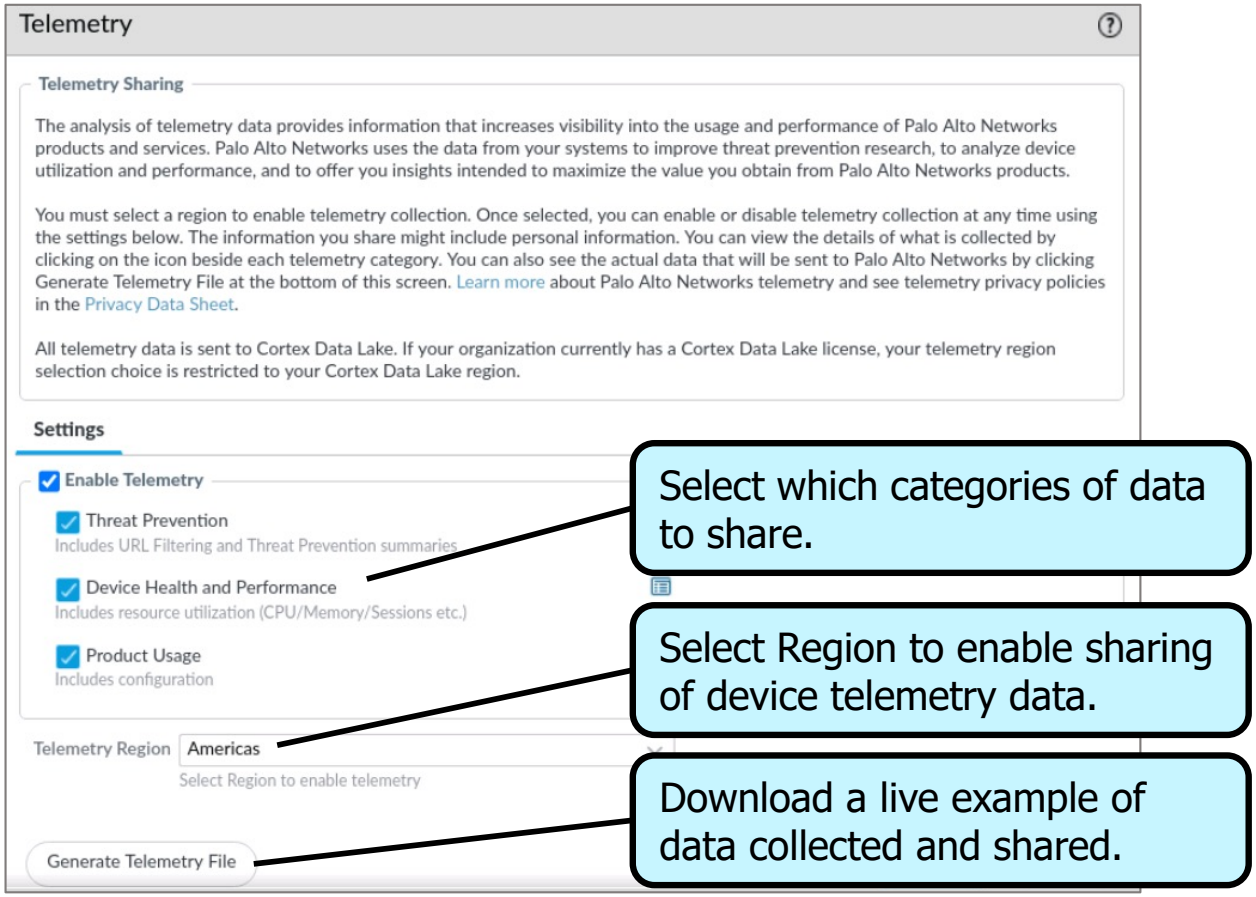
- Shared data with Palo Alto Networks.
- Data is used to improve visibility into device health, performance, capacity planning, and configuration.
- Requires a Cortex Data Lake license.

Device > Setup > Telemetry



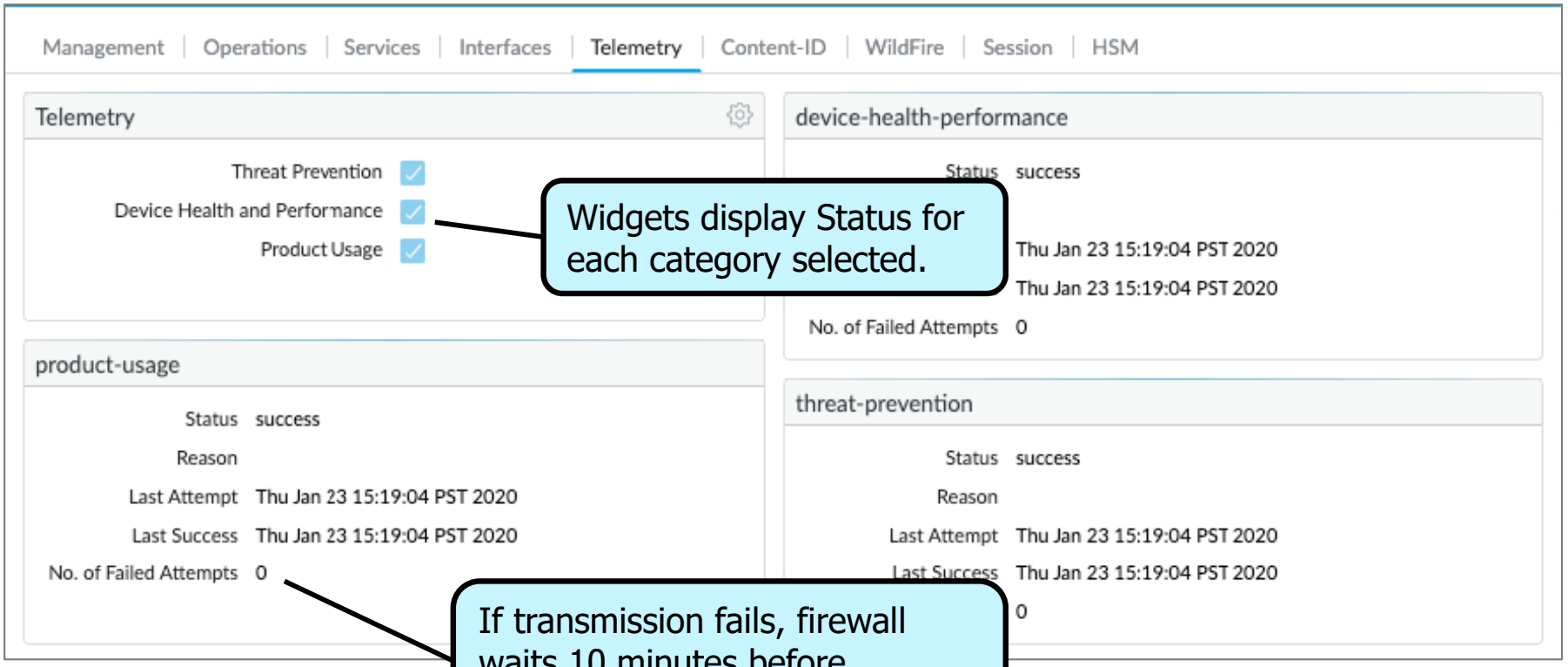
Configure Device Telemetry

Device > Setup > Telemetry

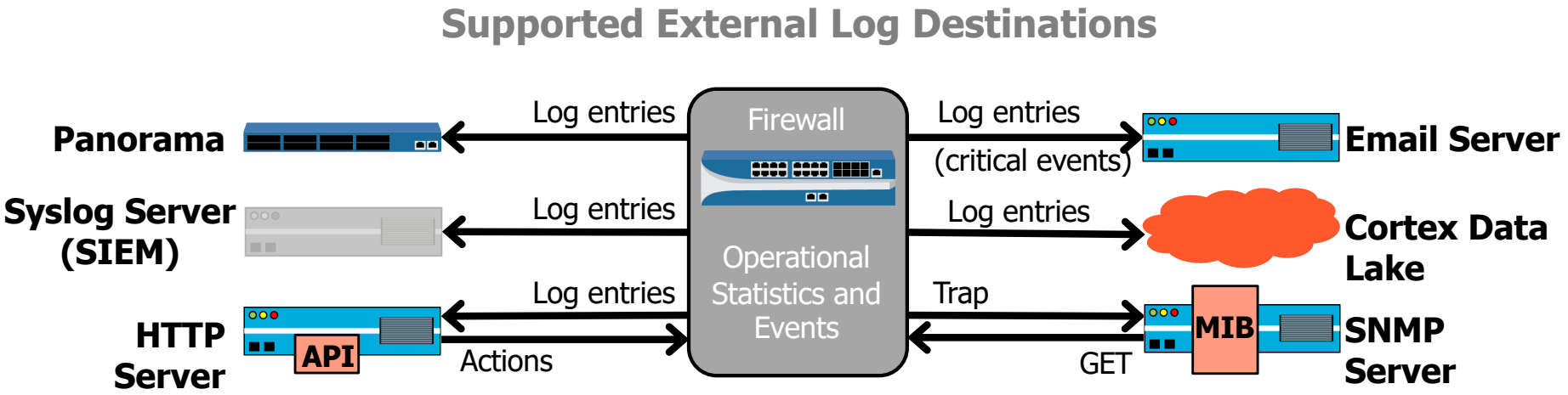


Monitor Device Telemetry

Device > Setup > Telemetry



Firewall Log Forwarding Review

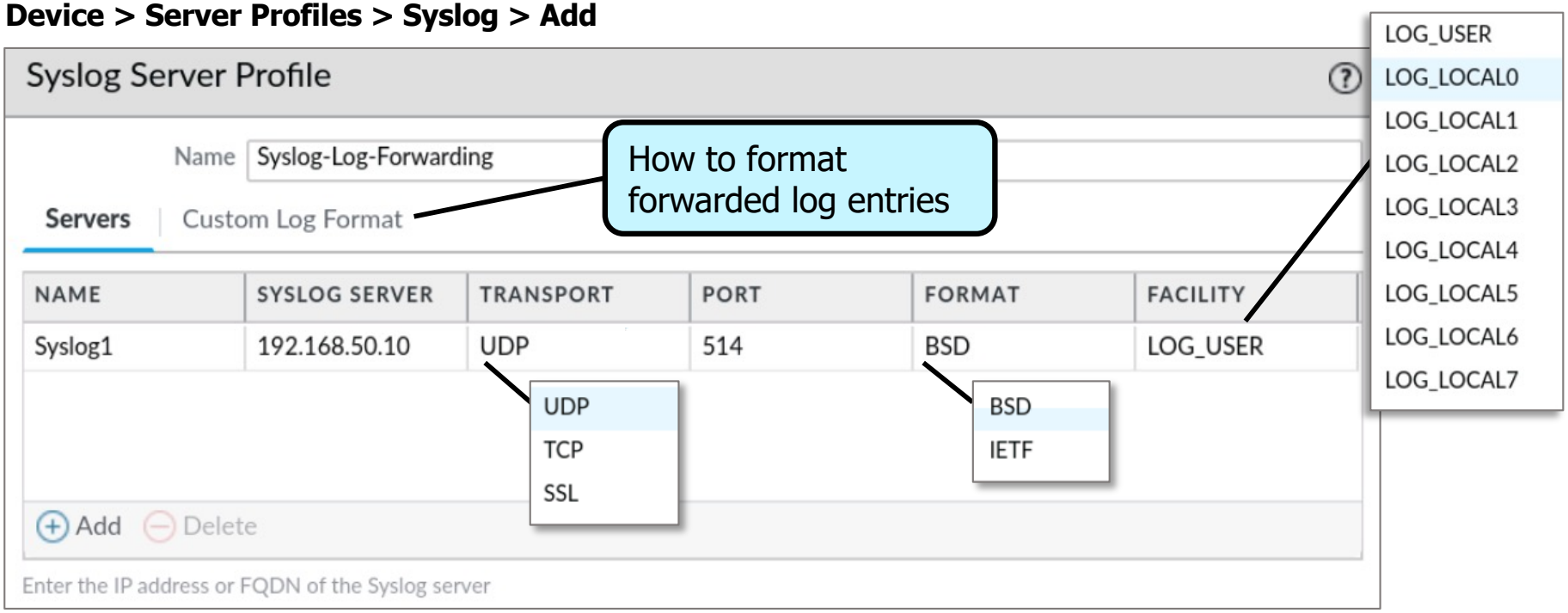


- Benefits of log forwarding and centralized logging:
  - Better log availability (off-firewall backup)
  - Centralized log analysis (PAN-OS software or third-party applications)
  - Longer log retention
  - Alerts for critical events
  - Automated responses (via Web API)

Configure a Server Profile: Syslog Example

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

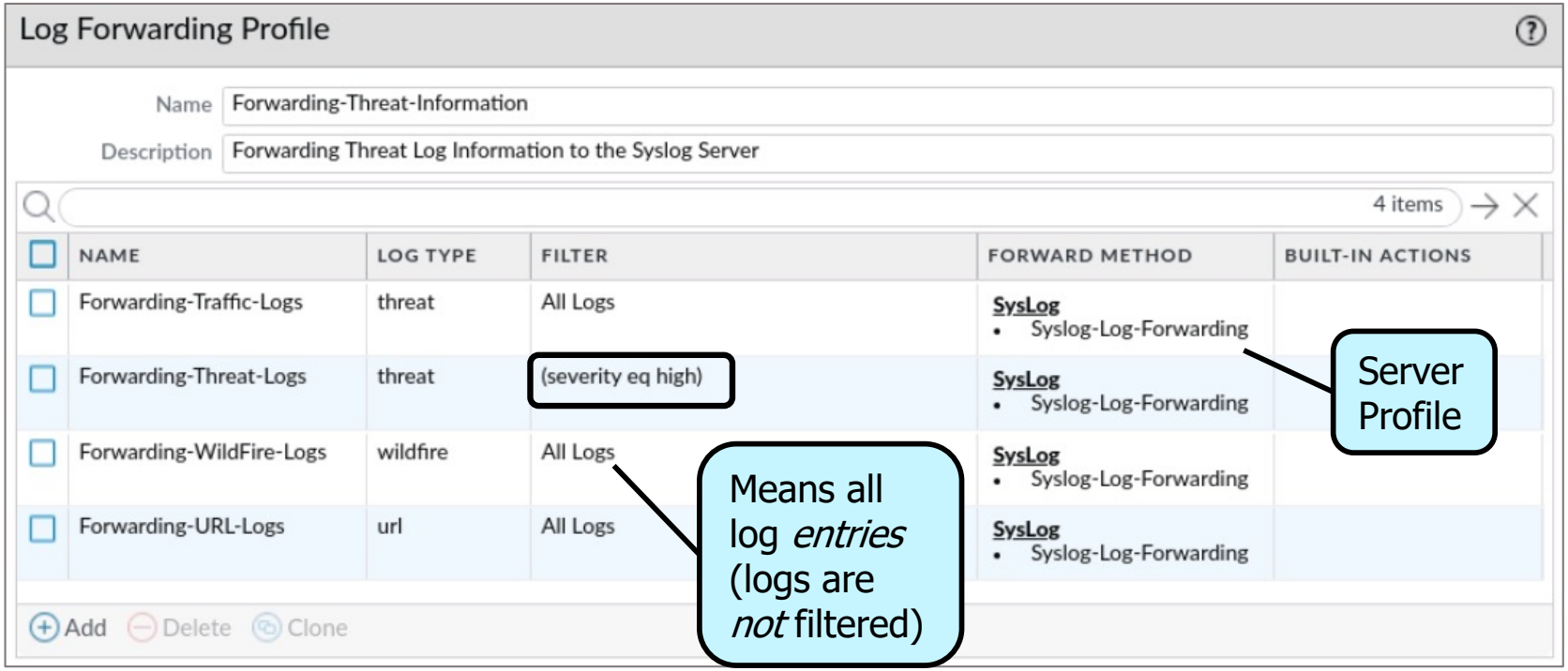
Device > Server Profiles > Syslog > Add



Configure Logs to Forward: Example

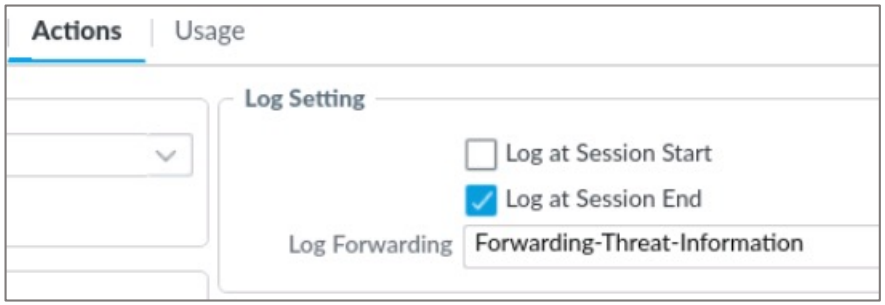
Defines which logs or log entries to forward to which external services

Objects > Log Forwarding > Add



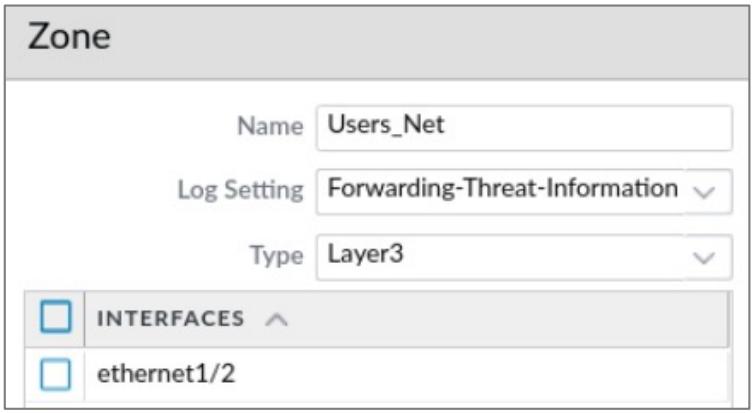
Apply Log Forwarding

Policies > Security > <rule>



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

Network > Zones > <zone>



- 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.