LOCATING VALUABLE INFORMATION USING LOGS AND REPORTS

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 predefined reports
  - In custom reports
- Forward threat and traffic information to external services

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

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

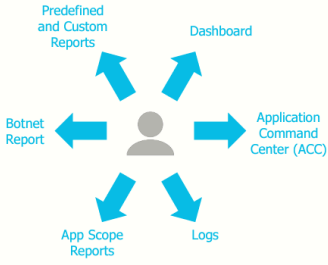
- Monitor threat and traffic information using the Dashboard and the ACC
- Monitor threat and traffic information using the logs
- Monitor threat and traffic information using App Scope reports
- Monitor threat and traffic information using predefined and custom reports
- Configure firewall log forwarding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

This module covers the topics listed here. Read through the list before proceeding.

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

- Monitor threat and traffic information using the Dashboard and ACC
- Monitor threat and traffic information using the logs
- Monitor threat and traffic information using App Scope reports
- 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.

The firewall web interface provides threat and traffic information in various formats. Use the information provided in the Dashboard, Application Command Center, logs, App Scope reports, botnet reports, and predefined and custom reports to maintain a secure network and to accelerate incident response when needed.

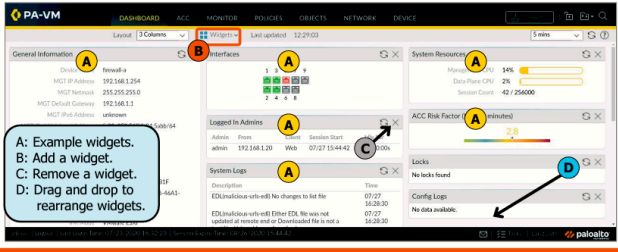
You can export threat and traffic information from the firewall and view it on other systems and platforms. For example, you can export logs off the firewall by using either SCP or FTP. You also can email reports to users or view reports as PDF files.

This section describes how to view threat and traffic information in the web interface **Dashboard**.

The Dashboard

For a Tech Doc about this topic, log into Live and search for "Dashboard Widgets"

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



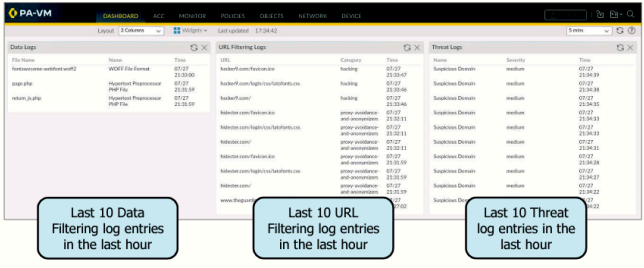
The web interface **Dashboard** consists of a customizable set of widgets. A widget is a tool that displays information in a pane on the **Dashboard**. PAN-OS® software includes more than a dozen built-in widgets, and you decide which ones to display on your **Dashboard**. The example shows nine widgets. Any changes that you make to the **Dashboard** affect only your login session.

Dashboard widgets display general firewall information, such as the software version, the operational status of each interface, high availability status, and resource use. The **Dashboard** widgets also display recent threat and traffic information.

Management of widgets on the **Dashboard** is easy. Use the **Widgets** drop-down menu to add widgets to the **Dashboard**. Click the **X** in a widget header bar to remove a widget from the **Dashboard**. Use your mouse pointer and drag and drop to arrange your widgets on the **Dashboard**. You can display your widgets on the **Dashboard** in two or three columns using the **Layout** drop-down menu.

Widgets for Viewing Threat Information

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



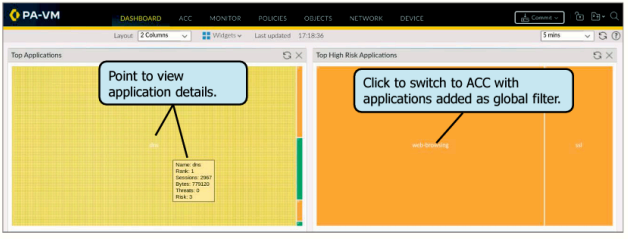
The **Dashboard** includes widgets that display the ten most recent threat events recorded in the logs in the last hour. The **Dashboard** is not the appropriate place to view older threat information. Use the firewall logs or reports to view less recent threat information.

To display the widgets shown here on the **Dashboard,** select **Widgets > Logs**. From the **Logs** drop-down menu, choose **Threat Logs**, **URL Filtering Logs,** or **Data Logs**.

The **Threat Logs** widget displays the threat ID, application, and date and time for the last ten entries in the Threat log for the last hour. The **URL Filtering Logs** widget displays the description, date, and time for the last ten entries in the URL Filtering log for the last hour. The **Data Logs** widget displays the description, date, and time for the last ten entries in the Data Filtering log for the last hour.

Widgets for Viewing Application Information

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

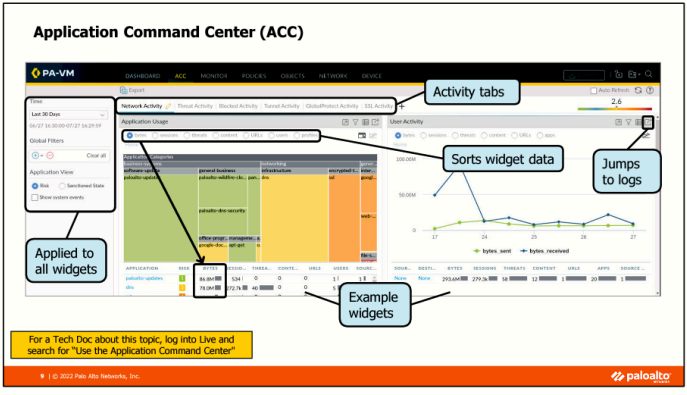


The **Top Applications** widget provides a concise view of the application traffic seen by the firewall. It displays the applications with the most sessions. The block size associated with each application indicates the relative number of sessions, and the color indicates the security risk associated with the application. The risk factor for applications is calculated by Palo Alto Networks on a scale from 1 to 5, where 1 is the lowest risk factor. Green indicates a risk factor of 1, blue is 2, yellow is 3, orange is 4, and red is 5.

The **Top High-Risk Applications** widget is similar but displays only the highest-risk applications with the most sessions. This information helps quickly indicate the highest risk applications seen most recently in your environment. Ensure that you have Security policy rules with attached Security Profiles to control and inspect this traffic.

When you click an application name in a widget, the web interface automatically switches to the Application Command Center view with the application name added as a global filter. The ACC and global filters are described later in this module.

This section describes how to view threat and traffic information in the web interface Application Command Center (or ACC).

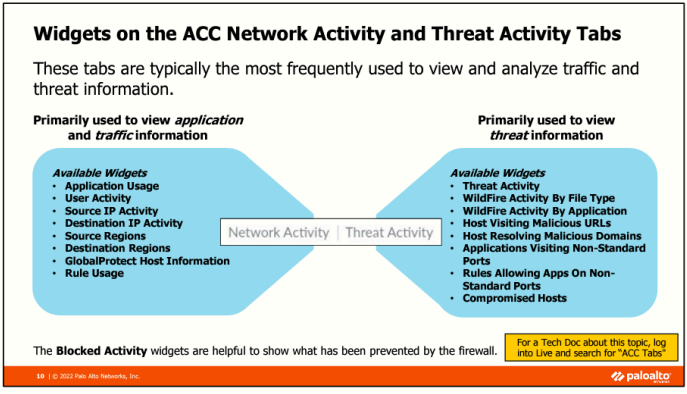


The **ACC** page is a collection of widgets that provide an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network. The **ACC** uses firewall log data to provide visibility into traffic patterns and threats. The **ACC** layout includes a tabbed view. Each tab has its widgets. You can also add a custom tab and include widgets that enable you to find the most critical information.

The **Time** range in the upper-left corner determines the time range displayed by all **ACC** widgets. Any **Global Filters** you add are applied across all **ACC** widgets. The **Application View** enables you to view applications by their risk or sanctioned status. If you select **Risk**, the colors green, blue, yellow, orange, and red are used to display application risk factors 1 to 5, where 1 is the lowest risk. If you select **Sanctioned State**, the colors green or blue indicate that you have tagged your applications as sanctioned or unsanctioned. A yellow color indicates a partially approved application. You could create a partially authorized application by inconsistently applying the sanctioned application tag across multiple virtual systems on a firewall.

You sort the data in each widget by selecting the **bytes**, **sessions**, **threats**, **content**, **URLs**, **users**, or **apps** radio button. Different widgets display different sets of sort filters. The display of the graphical and tabular data in the widget is updated and re-ordered based on the selected filter. In the example **Application Usage** widget, selection of **bytes** results in the applications being sorted top to bottom by those applications that have transferred the most bytes. You could sort the list by the number of sessions using the application, the number of threats seen by the application, the number of file transfers, or the number of URLs accessed by the application.

When you click the **Jump to Logs** icon, the **ACC** displays a list of logs. After selecting one of the logs from the list, the web interface switches to that log view. The **Jump to Logs** icon lets you view any log except for the User-ID, Alarm, and Authentication logs.



The **Network Activity** and **Threat Activity** tabs are typically the most frequently used ACC tabs.

Use the Network Activity tab widgets to display an overview of traffic and user activity on your network. This activity includes the top applications in use, the top users who generated traffic, and the most used Security policy rules. You also can view traffic activity by source or destination zone, region, or IP address or use GlobalProtect host information to view the most commonly used operating systems of the devices on the network.

Use the Threat Activity tab widgets to display an overview of the threats on the network, focusing on the top threats. Look for vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire® submissions by file type and application, and applications that use non-standard ports. The **Compromised Hosts** widget displays hosts potentially infected with malware attempting to phone home. It uses information provided by the automated correlation engine of the firewall to present an aggregated view of compromised hosts on your network. The automated correlation engine is described in more detail later in this module.

The **Blocked Activity** tab widgets focus on traffic prevented from coming into the network. These widgets enable you to view activity denied by application name, username, threat name, and blocked content. Blocked content is those files that were blocked by a File Blocking Profile. One widget also lists the top Security policy rules matched to block threats, content, and URLs.

Supplemental Notes

The correlation engine is available only on the PA-3x00, PA-5x00, PA-7000 Series firewalls, and Panorama. The **Compromised Hosts** widget does not appear on firewalls that do not include a correlation engine.

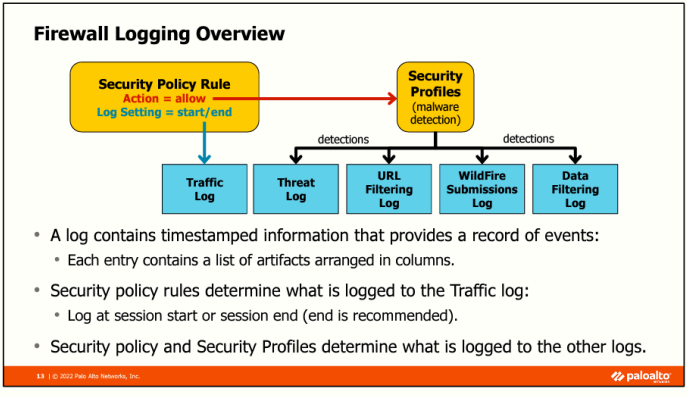
Example: Threat Activity Widget

For a Tech Doc about this topic, log into Live and search for "ACC Widgets"

The **Threat Activity** widget displays the threats seen on your network. The information is based on signature matches in Antivirus, Anti-Spyware, Vulnerability Protection Profiles, and viruses reported by WildFire.

The horizontal bar graph displays the number of vulnerabilities, spyware, and viruses detected using your Security Profiles during the selected time period. The bar graph also shows the number of viruses detected by WildFire submissions. The corresponding tabular data displays a top-10 list of the specific vulnerabilities, spyware, and viruses that the firewall detected. The event count sorts the list. The spyware is named **ZeroAccess.Gen Command and Control Traffic** have been seen the most in the selected time range.

This section describes how to view threat and traffic information in the web interface logs.



A log is an automatically generated, timestamped file that provides an audit trail for system events on the firewall or network traffic events that the firewall monitors. Log entries contain *artifacts*, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker. Log artifacts are arranged in columns in the logs. Each log type records information for a particular event type.

The **Log Setting** parameter in each Security policy rule determines whether the rule-matching traffic is logged to the Traffic log. If the **Log Setting** specifies to log at session start, then the log records the initial application discovered in the traffic. If the **Log Setting** specifies to log at session end, the log records the final application found in the traffic, assuming there were application shifts. Selection of logging at session start and end would result in logging an initial application and any final application, assuming there is an application shift. Logging at the session end is the recommended configuration because it results in smaller but still valuable logs.

Suppose the Security policy rule allows the matching traffic. In that case, the configuration of any Security Profiles determines what is logged to the Threat, URL Filtering, WildFire Submissions, and Data Filtering logs. Any malware detected by a Security Profile is logged only if configured with at least an “alert” action.

Example: Traffic Log

For a Tech Doc about this topic, log into Live and search for "Traffic Log Fields"

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

The Traffic log displays an entry for each firewall session and helps determine which your firewall is seeing applications. You can use the log information to provide intelligence when configuring your firewall Security policy.

The **Type** column indicates whether the entry is for the start or end of the session or whether the session was denied by policy. Options for this column are a *start*, *end*, and *deny*.

The **Action** column indicates whether the firewall allowed, denied, or dropped the session. A *drop* indicates the Security policy rule that blocked the traffic specified *any* application, and a *deny* indicates the rule identified a *specific* application. If the firewall drops traffic before identifying the application, such as when a rule drops all traffic for a particular service, the **Application** column displays *not-applicable*. If the application can be identified, the application name appears in the **Application** column. If not enough data was received to determine the application, *incomplete* appears in the **Application** column.

Click the **magnifying glass** icon beside an entry to view additional details about the session, such as whether an ICMP entry aggregates multiple sessions between the same source and destination. Aggregated sessions are indicated in the log by a value greater than 1 in the **Count** column. For example, if an application opens three consecutive sessions between the same IP addresses and port numbers, three is recorded in the **Count** column.

Example: Threat Log

For a Tech Doc about this topic, log into Live and search for "Threat Log Fields"

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.exe
	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
	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
	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
	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
	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
	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.

The Threat log displays entries when traffic matches one of the Security Profiles attached to a Security policy rule on the firewall. You must have at least an action of "alert" configured in the Security Profile.

Click the **magnifying glass** icon beside a threat entry to display details. For example, a **Count** value greater than 1 indicates that the log entry aggregates multiple threats of the same type between the same source and destination. If you configured the Security Profile to take packet captures, click the **down arrow** icon beside an entry to access the captured packets.

Critical-severity threats are serious threats, such as those that affect default installations of widely deployed software, resulting in root compromise of servers, or where the exploit code is widely available to attackers.

High-severity threats can become critical but have mitigating factors. For example, they might be difficult to exploit, not result in elevated privileges, or do not have a large victim pool.

Medium-severity threats are minor threats in which impact is minimized. Examples include DoS attacks that do not compromise the target, exploits that require an attacker to reside on the same LAN as the victim, threats that affect only non-standard configurations or obscure applications, or threats that provide limited access.

Low-severity threats are warning-level threats that have little impact on an organization's infrastructure. Such threats usually require local or physical system access, resulting in victim privacy issues and information leakage.

Informational-severity threats are suspicious events that do not pose an immediate threat but are reported to call attention to deeper problems that could exist.

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/istofonts...	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/istofonts.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.

The URL Filtering log displays traffic entries that match URL Filtering Profiles attached to Security policy rules. In the URL Filtering Profile, you must configure a URL category or website with at least an action of "alert" to generate URL Filtering log entries. For example, the firewall generates a log entry when a URL Filtering Profile *blocks* access to a specific website or URL category or when it *allows* access to a particular website or URL category.

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)

The firewall forwards samples to the WildFire cloud for analysis based on WildFire Analysis Profile settings. The firewall generates WildFire Submissions log entries for each sample it forwards, but only after WildFire completes its static and dynamic sample analysis and returns a verdict. WildFire Submissions log entries include the firewall "allow" or "block" action for the sample and the WildFire verdict for the sample.

Use the WildFire Submissions log to determine who sent the malware, who received the malware, and the filename or URL link used to deliver the malware.

Supplemental Notes

Samples with a *benign* verdict are safe and do not exhibit malicious behavior. Samples with a *grayware* verdict do not pose a direct security threat but can exhibit intrusive behavior. Samples with a *phishing* verdict should be blocked to prevent the possibility of credential theft. Samples with a *malicious* verdict pose a security threat. Malware can include viruses, worms, trojans, remote access tools, rootkits, and botnets. For samples that are identified as *malicious*, the WildFire cloud generates and distributes a signature to prevent future infection.

Example: Data Filtering Log

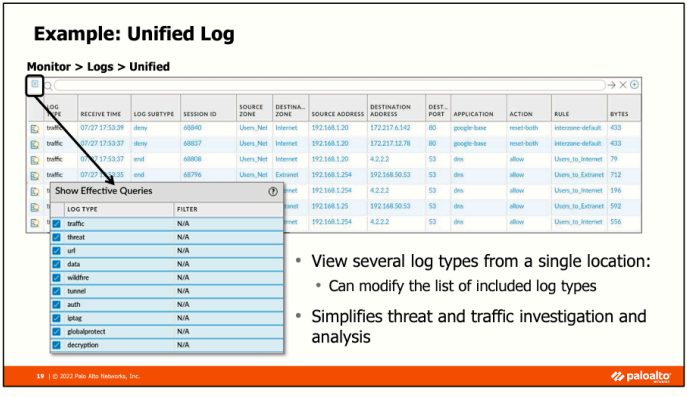
Monitor > Logs > Data Filtering

	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	044575911080bb0...	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

The Data Filtering log displays entries when a File Blocking rule or Data Filtering Profile rule matches a sensitive file or sensitive data transferred through the firewall. To generate log entries, you must configure the profile rules with at least the “alert” action. The File Blocking and Data Filtering Profiles help prevent sensitive information such as credit card numbers, U.S. Social Security numbers, or proprietary information from leaving the area that the firewall protects.

Use the log to answer questions such as where the file was sent, who sent the file, or which data was leaked. This information can be used for incidence response and further improve the firewall's security configuration.

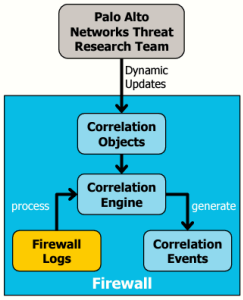


The Unified log displays log entries from the Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs. Display the Unified log to enable you to investigate and filter the latest entries from different log types in one place. You will not have to search through each log type separately.

Click the **Effective Queries** icon in the filter area to display or modify which log types display entries in the Unified log view. Notice that the **Log Type** column shows the name of the log that is the source of a specific Unified log entry. The URL Filtering log can have many entries in a busy environment. If you find that working with the volume of URL information recorded in the Unified log becomes too cumbersome, you can deselect **url**.

Correlation Engine, Objects, and Events

For a Tech Doc about this topic, log into Live and search for "Interpret Correlated 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

The automated correlation engine is a firewall-based or Panorama-based analytics tool that uses firewall logs to detect events on your network that require action to be taken. The engine correlates a series of threat events that, when combined, indicate a likely compromised host on your network. It enables you to assess the risk and prevent the exploitation of network resources. The automated correlation engine uses *correlation objects* to analyze the logs for patterns. After a match occurs, it generates a *correlation event*.

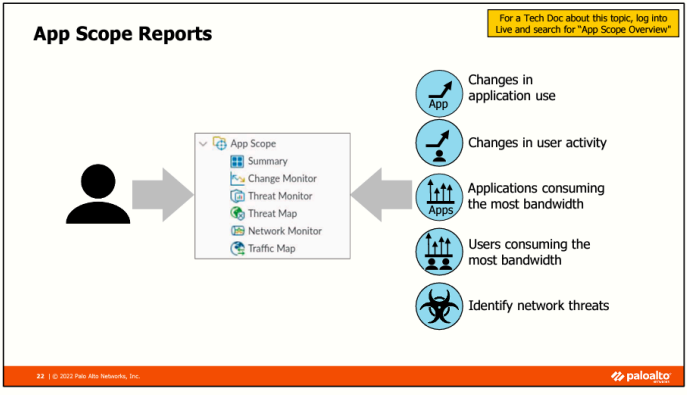
A *correlation object* connects isolated network events and looks for patterns that indicate a more significant event. A correlation object is a definition file that specifies three types of criteria: patterns to match against, the data sources to use, and the time period within which to look for pattern matches. Each pattern has a severity rating and a threshold for the number of times the pattern match must occur within a defined time limit to indicate malicious activity. When the match conditions are met, a correlated event is logged.

Correlation objects are defined and developed by the Palo Alto Networks threat research team and are delivered with dynamic updates to the firewall and Panorama. Before the firewall can obtain new correlation objects, it must have a *Threat Prevention* license.

A *correlation event* is logged when the patterns and thresholds defined in a correlation object match the traffic patterns on your network. A correlation event is your notification of a possibly infected host.

For example, when a host submits a file to the WildFire cloud and the verdict is *malicious*, the correlation object looks for other hosts or clients on the network that exhibit the same behavior seen in WildFire. If the malware sample had performed a DNS query and browsed to a malware domain, the correlation object will parse the firewall logs for a similar event. When the activity on a host matches the analysis in WildFire, a high-severity correlated event is logged.

This section describes how to view threat and traffic information in the web interface App Scope reports.



App Scope reports provide visibility and analysis tools to help you understand changes in application use and user activity, identify applications and users that consume the most network bandwidth, and identify network threats. You can use App Scope reports to learn any unusual or unexpected behavior quickly. Each App Scope report provides a dynamic, user-customizable window into the network.

App Scope Reports: What's Available?

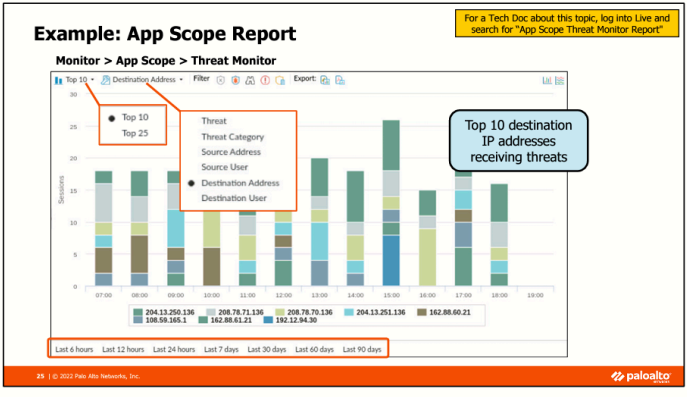
Report Name	Description
Summary Report	Set of six graphical reports displayed in a single browser pane
Top 5 Gainers	Applications showing largest increase in number of sessions (last 60 minutes)
Top 5 Losers	Applications showing largest decrease in number of sessions (last 60 minutes)
Top 5 Bandwidth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

The **Summary Report** is one of the App Scope reports. The **Summary Report** is a collection of six graphical reports. Each report is listed here, along with a short description. Take a moment to review the information.

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)

App Scope reports also include the five reports listed here and a short description. Take a moment to review the information.



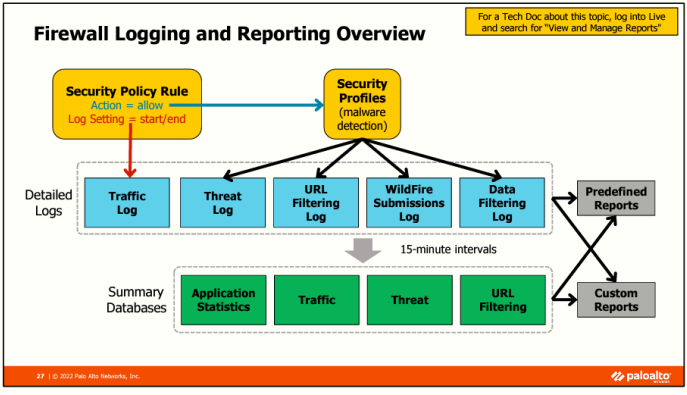
Here is an example of an App Scope report named the Threat Monitor. This example displays the top 10 destination IP addresses for those sessions that contained some detected threat signature. Point to a section of a bar on the chart to display a popup window with the destination IP address that the bar area represents. The total number of sessions containing threats to that destination IP address also is shown.

Notice that you can adjust the report to display the top 10 or 25 items. You also can change the report to show the top threats by name or the top threat categories by name. You can adjust the report to display the top IP addresses that have sent or received threats. You can also change the report to show the top users who have sent or received threats.

Notice the buttons at the bottom left of the example. These buttons can change the time period from the **Last 6 hours** up to the **Last 30 days**.

Click either a line or a bar on a chart to cause the web interface to switch to the **ACC** tab. The web interface automatically adds the clicked item as a **Global Filter** in the **ACC**. The **ACC** provides more detailed information about the item represented by the line or bar.

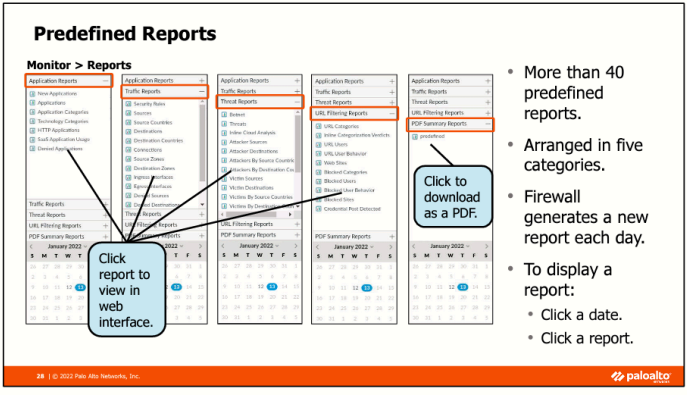
This section describes how to view threat and traffic information in the web interface predefined reports.



In a Security policy rule, if you configure the **Log Setting** value as **Log at Session Start** or **Log at Session End**, the session is logged to the Traffic log. Suppose you have attached one or more Security Profiles to a Security policy rule. In that case, the Security Profile configurations can log information to the detailed Threat, URL Filtering, WildFire Submissions, and Data Filtering logs.

Every 15 minutes, the firewall summarizes the information in the detailed logs and updates the summary databases. The firewall condenses the detailed log data by excluding some attributes from the summary databases, duplicate grouping sessions, and incrementing the repeat count in the **Count** column.

You can filter and present the detailed log data or the data of summary databases in the firewall predefined reports and in any custom reports that you have configured. The summary databases enable a faster response time when reports are generated.



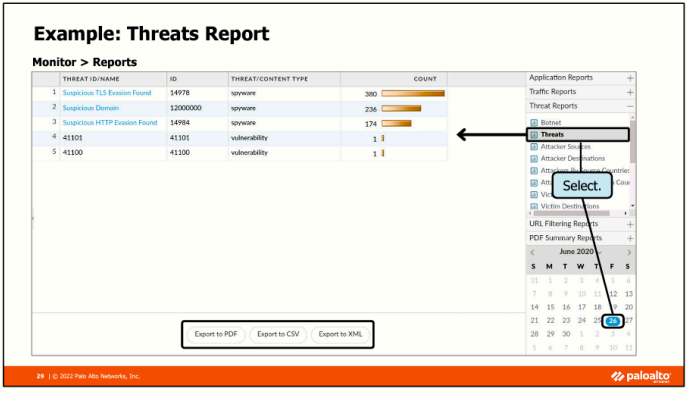
The firewall includes more than 40 predefined reports arranged in the web interface across five categories. Each category has been expanded to show the report names included in each category. The firewall runs each report every day. To display a report, click the desired date, expand a report category, and click a report name. The report information is shown in the web interface.

The **PDF Summary Reports** category includes a single **predefined** report by default, although you can create custom PDF summary reports. A PDF summary report is a set of up to 18 other reports collected into a single PDF file. The firewall summarizes each report to keep the PDF summary report brief. A PDF summary report is also unique because clicking a date and a report name does not display the report in the web interface. After clicking a report name, a PDF file is downloaded to the host running the web interface. You must navigate to the download directory of the host to open and view the report.

To create a custom PDF summary report, browse to **Monitor > PDF Reports > Manage PDF Summary** and click **Add**.

Supplemental Notes

The predefined reports are enabled by default. Each day a new report is generated. You might find that you do not use specific reports and might want to disable those reports to conserve firewall CPU, memory, and storage resources—the firewall reserves about 200MB of storage space to store reports. The amount of space reserved to store reports is not configurable. To disable any predefined report, browse **Device > Setup > Management** and open **Logging and Reporting Settings**. In the window that opens, click the **Pre-Defined Reports** tab and deselect the check box of any predefined report that you want to disable. The firewall will not generate these reports after you commit the configuration.



In the example Threats report for June 26, each entry in the report lists the name of a threat seen by the firewall on that day. In addition to the name, each entry displays the threat ID number, the type of threat, and a count of the number of times the threat was seen that day.

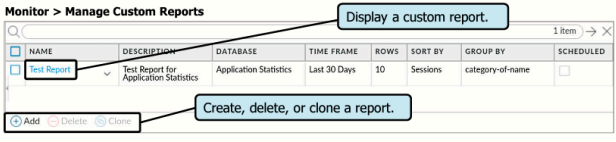
The firewall automatically displays the predefined reports in the web interface, but you can export them to PDF, CSV, or XML files. The export of a report helps present the content to key stakeholders or import it into another system for further analysis.

This section describes how to create custom reports to view threat and traffic information.

Custom Reports

For a Tech Doc about this topic, log into Live and search for "Generate Custom Reports"

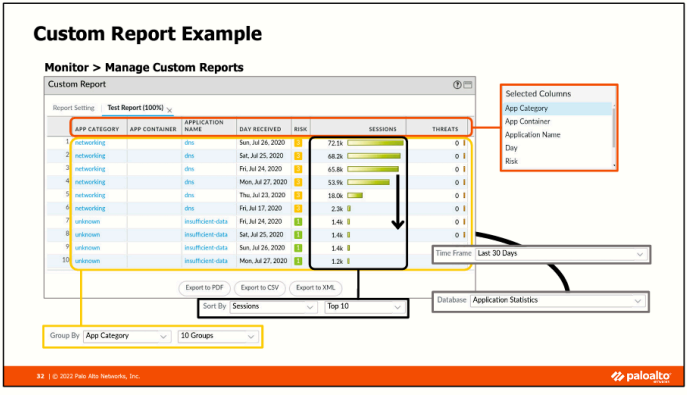
- Custom reports show only the information you want:
  - You choose the logs and log columns to view.
- Schedule reports or run-on demand.
- View a report:
  - In the web interface
  - By exporting a PDF, CSV, or XML file



Create custom reports that show exactly the information you want to see by including only those specific logs and log columns that provide the required information. Custom reports can be run on-demand or scheduled to run daily.

You create and manage custom reports by browsing **Monitor > Manage Custom Reports**.

To display a custom report, browse to **Monitor > Reports** and click to expand the **Custom Reports** category. (This category does not exist in the web interface until you have created at least one custom report.) The **Custom Reports** category lists any custom reports that you have created. To open and display a report, click a date and click a custom report name. The report opens in the web interface, but you can export it as a PDF, CSV, or XML file.



Here is a sample report based on the previous custom report configuration. You can generate a test report by clicking the **Run Now** link displayed on the **Report Setting** tab. You can display the test report by clicking the **Applications By Zone (100%)** tab. The report name is used as the tab name.

The firewall searched the **Traffic Summary** database for entries from the **Last 30 Calendar Days**. The search results yielded two security source zones that were used to group the results. The results grouped beneath the *inside* zone then were sorted by the number of **Sessions** in descending order. Likewise, the results grouped beneath the *dmz* zone were sorted by the number of **Sessions**.

Supplemental Notes

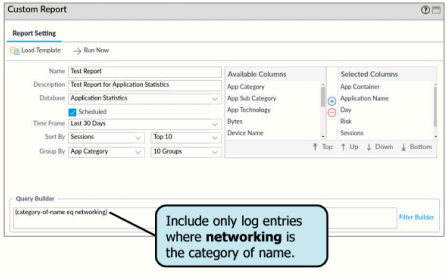
Ensure that the **Group By** value is large enough to accommodate the number of items you want to see in the report. For example, if you had nine source zones, you would need to select at least **Top 10** to have all the source zones appear in the report. **Top 25** and **Top 50** also are available for selection.

Ensure that the **Sort By** value is large enough to accommodate the number of items you want to see in the report. For example, if you think you might have as many as 50 applications to report, you would need to select at least **Top 50**. Options from **Top 5** to **Top 1000** are available for selection.

Custom Report with a Query Builder Filter

For a Tech Doc about this topic, log into Live and search for "Custom Reports"

Monitor > Manage Custom Reports > Add



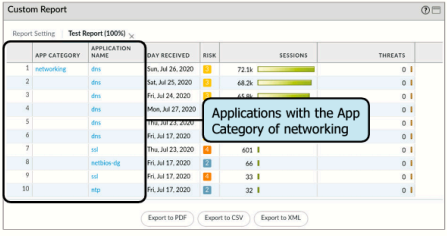
- **Query Builder** applies filters to source log.
- Only log entries matching the filter are included in the report.
- Filters match only if a specific *value* is in a column.
- This example reports only applications where the category of name equals networking.

The **Query Builder** enables you to apply additional filters to the source log before generating a report. Click the **Filter Builder** link to open a new window and configure the filter to use in your report. The resulting filter, or filters, appear in the **Query Builder** section, as shown here.

In the example, the only entries from the last 30 days of the **Application Statistics** database that would be included in the report are those that have the category of name networking.

Query Builder Report Example

Monitor > Manage Custom Reports



- 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.

Here is an example of the last report that included an optional **Query Builder** filter string. The report displays a sorted list of the top 10 applications seen by the firewall in the *networking* App Category. You can use this information to decide how to configure your perimeter Security policy rules.

You can change the application category in the filter string to discover which firewall is seeing applications in other application categories. For example, if you had a *general-business category*, you could modify the filter string to (category-of-name eq *general-business*). You could report which applications are seen in every application category except the *networking* category by changing the filter string to (category-of-name neq *networking*). This filter string's neq or not-equal operator would configure the report to display application information for all application categories except the *networking* category.

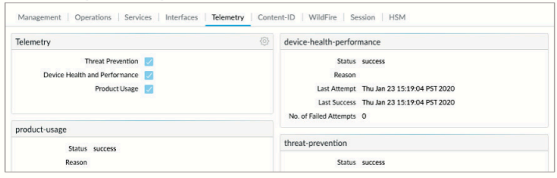
This section describes how to forward Threat and Traffic log information to external services.

Device Telemetry

For a Tech Doc about this topic, log into Live and search for "Device Telemetry Overview"

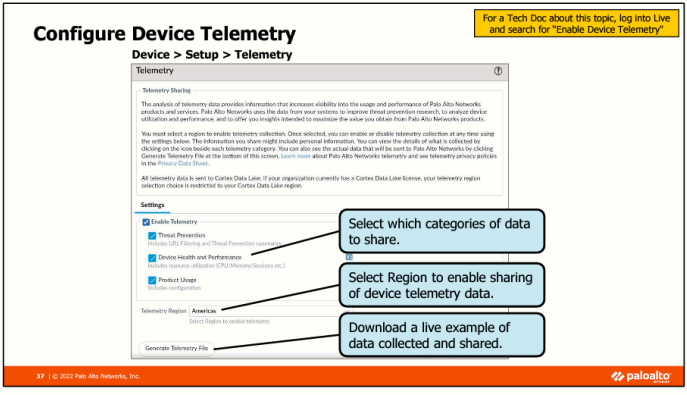
- Shared data with Palo Alto Networks.
- Data is used to improve visibility into device health, performance, capacity planning, and configuration.
- Requires a Cortex Data Lake license.

Device > Setup > Telemetry



With the release of PAN-OS 10.0, device telemetry has been extended to collect more data from your firewall. The collected data is used for the same purposes as it was in previous PAN-OS releases and includes sharing threat intelligence data, providing enhanced intrusion prevention, evaluation of threat signatures, improved malware detection within PAN-DB URL filtering, DNS-based command-and-control (C2) signatures, and WildFire. The collected data will help with applications designed to enhance device health, performance, capacity planning, and configuration visibility.

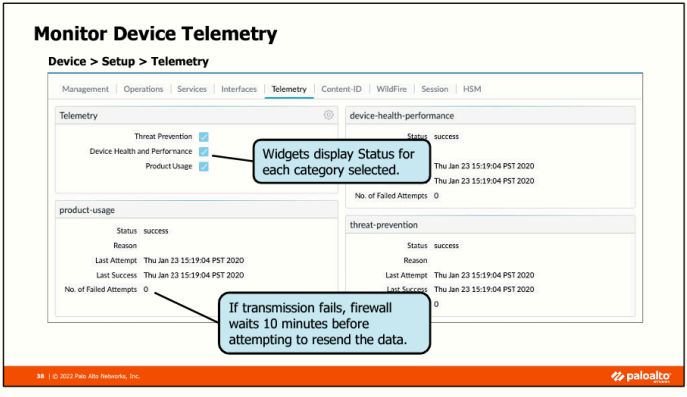
By default, all telemetry data is collected and stored locally on your firewall for a limited period of time. This data can not be shared with Palo Alto Networks unless your organization has a Cortex Data Lake license.



Suppose your organization does have a Cortex Data Lake license. In that case, you select the destination region of your telemetry data and determine what data is collected and shared by enabling or disabling categories of data. The destination region is limited to the region that your Cortex Data Lake is configured to use. There are three categories of data collection: Threat Prevention, Device Health and Performance, and Product Usage.

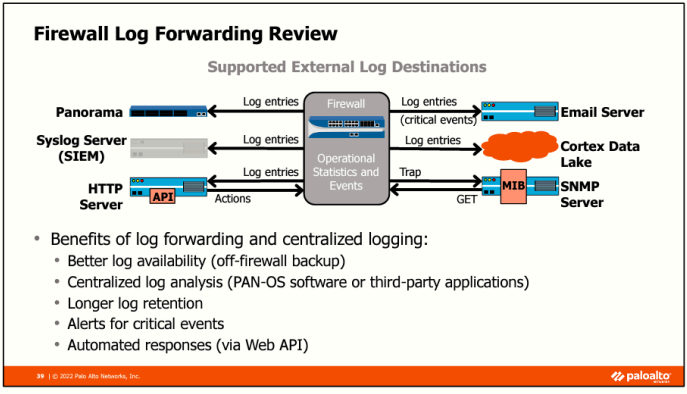
You can obtain a live sample of the data that your firewall is collecting for telemetry purposes by selecting the **Generate Telemetry File** button. The data collection will take a few minutes, depending on the speed of your firewall. When the process completes, click **Download Device Telemetry Data**. The telemetry bundle is a compressed file, and it is placed in your default browser download directory.

Once configured, the firewall collects and sends telemetry data at fixed intervals. The collection is defined on a category-by-category basis and can be set to send collected data every 20 minutes, every 4 hours, or once per week.



Telemetry widgets display the sharing status for each telemetry category. Each widget displays the **Status**, **Last Attempt** to connect to Cortex Data Lake, the **Last Successful** connection, the **Number of Failed Attempts**, and the **Reason** for a failed attempt.

Telemetry is collected into data bundles. Each bundle is an aggregation of all the data collected up to the data transmission point. When a bundle has been successfully sent to Palo Alto Networks, it is deleted from the device, and status information is updated in each widget. If an error occurs while sending a bundle to Palo Alto Networks, the firewall waits 10 minutes and then tries to send the bundle again.

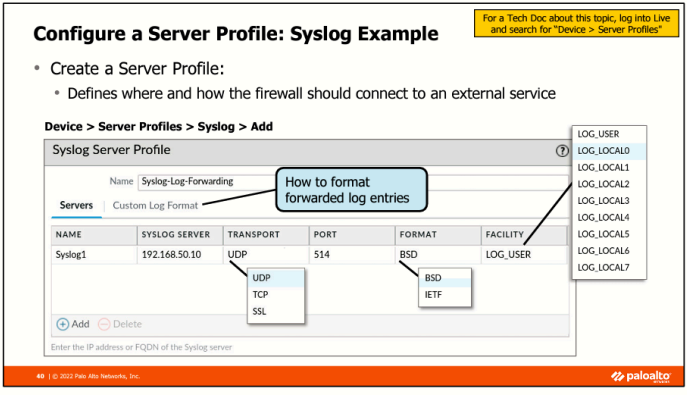


The firewall records operational statistics and events in its log files. You can configure the firewall to forward all log entries to external services. The benefits of log forwarding and centralized logging include better log availability because the firewall copies its logs on external storage. Another advantage of forwarding logs to a central location is that centralized analysis by Panorama or a third-party tool is enabled. Forwarding logs to an external service can also increase your log retention time. Log forwarding also allows you to send alerts to users in response to critical events or automate responses to firewall activities.

Forwarding firewall logs to your Panorama enables centralized collection and analysis of logs. Forwarding firewall logs to a Syslog server enables off-firewall storage and backup and centralized log analysis. You can forward log entries to an email server for critical firewall events such as the failure of a data plane interface or a critical threat. Users assigned to respond to the event can be notified by email message. Typically, you should forward only critical events to email. You also can forward log entries to an HTTP server. If the HTTP server has an API that can parse the log entries, you can configure the HTTP server to take action based on a firewall event. For example, the HTTP server could submit a service ticket with a technical support organization.

The firewall can also forward log entries to cloud-based Cortex Data Lake. Cortex Data Lake enables you to aggregate, view, and analyze log data from many firewalls simultaneously.

The firewall can work with an SNMP server that supports GET and TRAP operations. An SNMP server can issue GET requests to the firewall that return operational statistics information. PAN-OS software does not support SNMP SET requests to configure a firewall. As events occur on the firewall, it can send SNMP traps to the SNMP server that enable the SNMP server to record the event and notify users. Before your SNMP server can work with the firewall, you must load generic enterprise and PAN-OS MIBs on the SNMP server. Palo Alto Networks MIB files can be downloaded from docs.paloaltonetworks.com/resources/snmp-mib-files. Generic enterprise MIB files can be downloaded from https://tools.ietf.org. The required MIBs are listed in *PAN-OS* https://*Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin.html.



Before you can forward log entries to an external service, you must configure the firewall with the server's connection information. Use a Server Profile to configure a firewall with the necessary information to connect to the external service. The example here is of a Syslog Server Profile. You should configure the Syslog server settings of the firewall to match the type and configuration of your Syslog server.

The example configures the firewall to connect to an external Syslog server. The IP address of the *BSD-based* Syslog server is *192.168.50.10* and is reachable at *UDP* port *514*. The Syslog facility used to record log information is *LOG_USER*. Other available facilities are shown in the screenshot.

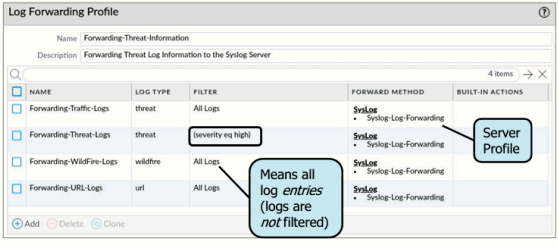
You can configure the firewall to use UDP, TCP, or SSL to connect to an external Syslog server. The firewall can format the log entries according to the BSD or the IETF standards. The **Custom Log Format** tab lets you configure custom Syslog formats that enable the firewall to work with many different Syslog vendor solutions.

Configure Logs to Forward: Example

For a Tech Doc about this topic, log into Live and search for "Objects > Log Forwarding"

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

Objects > Log Forwarding > Add

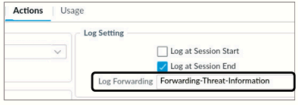


Browse to **Objects > Log Forwarding** and click **Add** to configure a Log Forwarding Profile. A Log Forwarding Profile configures which logs or log entries to forward to external services. In this example, the Log Forwarding Profile configures the firewall to forward all log entries from the Traffic, Threat, WildFire Submissions, URL Filtering, and Data Filtering logs to an external Syslog server.

Click **Add** in this window to configure which log or log entries to forward to which external service. A Log Forwarding Profile does not have to forward all logs to the same service. In the example, the final entry forwards logs to an email service rather than to a Syslog service. Also, a filter was added to the Threat log that causes only log entries with a severity level of *high* or *critical* to be forwarded to an email server. The filter (*severity geq high*) is interpreted to mean any Threat log entry with a severity level greater than or equal to high.

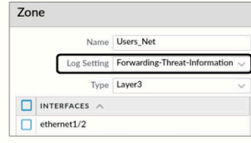
Apply Log Forwarding

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

After configuring a Log Forwarding Profile, you must apply it to either a Security policy rule or a security zone.

To add a Log Forwarding Profile to a Security policy rule, browse **Policies > Security** and open a rule. Click the rule's **Actions** tab and select a Log Forwarding Profile for the **Log Forwarding** setting. The firewall forwards any logs or log entries for traffic matching the Security policy rule and the Log Forwarding Profile settings.

To add a Log Forwarding Profile to a security zone, browse **Network > Zones** and open a zone. Select a Log Forwarding Profile for the **Log Setting**. Any threats detected by a Zone Protection Profile are forwarded according to the Log Forwarding Profile configuration.`

Supplemental Notes

If you name a Log Forwarding Profile *default*, that profile will be selected automatically for the **Log Forwarding** setting when a new Security policy rule is created. A profile named *default* also will be selected automatically as the **Log Setting** when a new security zone is created. You can override the default profile by selecting another profile in either case.

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

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"Threat and Traffic Information"

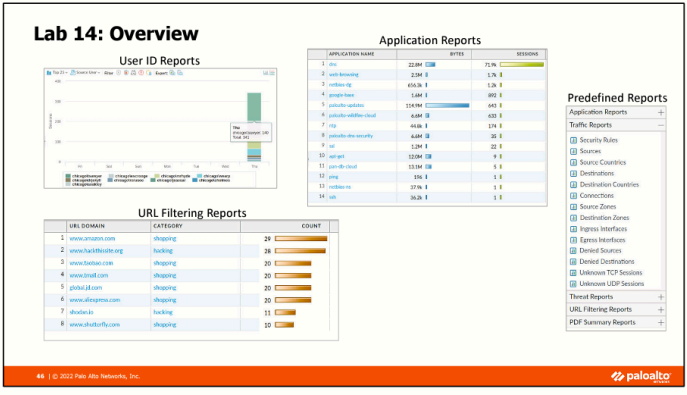
Review Questions

1. Which two actions affect all of the widgets in the Application Command Center? (Choose two.)
   a. setting a local filter
   b. setting a global filter
   c. setting a global search
   d. selecting a time range
2. Which two firewall features to display information using widgets? (Choose two.)
   a. ACC
   b. Dashboard
   c. Traffic log
   d. botnet report
3. True or false? You can customize the list of logs that are aggregated into the Unified log.
   a. true
   b. false
4. Which three statements about the automated correlation engine are correct? (Choose three.)
   a. It detects possible infected hosts.
   b. It is available only in Panorama.
   c. It uses correlation objects as input.
   d. It outputs correlation events.
   e. It requires Cortex Data Lake.
5. True or false? SNMP GET requests a firewall return operational statistics, and SNMP SET requests update the firewall configuration.
   a. true
   b. false
6. Which three statements about the predefined reports are correct? (Choose three.)
   a. There are more than 40 predefined reports.
   b. They are generated daily by default.
   c. They are grouped into five categories.

Review Questions

1. Which two actions affect all of the widgets in the Application Command Center? (Choose two.)
   a. setting a local filter
   b. setting a global filter
   c. setting a global search
   d. selecting a time range
2. Which two firewall features to display information using widgets? (Choose two.)
   a. ACC
   b. Dashboard
   c. Traffic log
   d. botnet report
3. True or false? You can customize the list of logs that are aggregated into the Unified log.
   a. true
   b. false
4. Which three statements about the automated correlation engine are correct? (Choose three.)
   a. It detects possible infected hosts.
   b. It is available only in Panorama.
   c. It uses correlation objects as input.
   d. It outputs correlation events.
   e. It requires Cortex Data Lake.
5. True or false? SNMP GET requests a firewall return operational statistics, and SNMP SET requests update the firewall configuration.
   a. true
   b. false
6. Which three statements about the predefined reports are correct? (Choose three.)
   a. There are more than 40 predefined reports.
   b. They are generated daily by default.
   c. They are grouped into five categories.

d. They are customizable.
e. They are emailed daily to users.



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

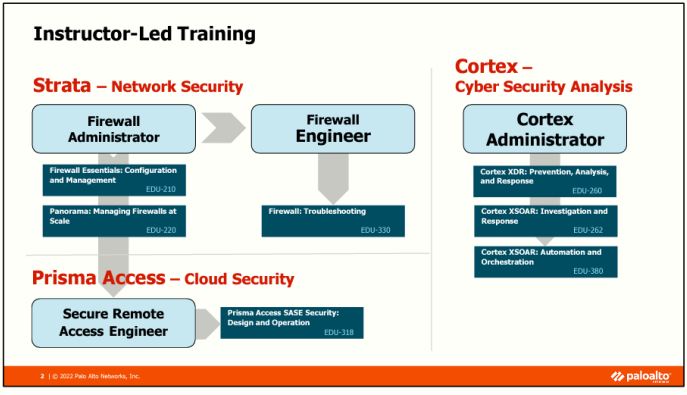
Lab 14: Locating Valuable Information Using Logs and Reports

- 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

Answers to Review Questions

1. b, d
2. a, b
3. a (true)
4. a, c, d
5. b (false)
6. a, b, c

Now that you have finished your course, what do you do next? This module offers suggestions for improving your network security, endpoint security, and cloud security knowledge and skills.



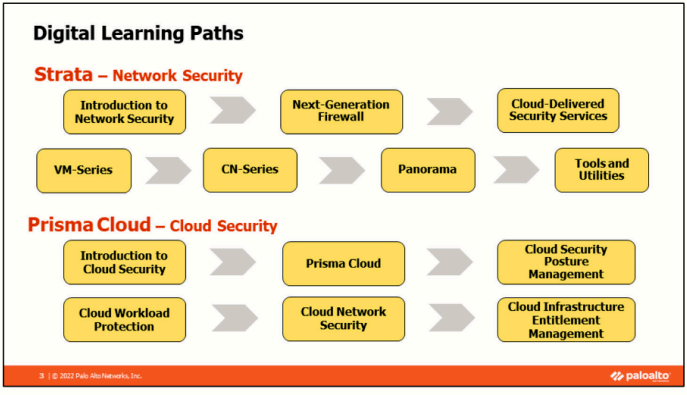
The image illustrates sample learning paths designed to support different job roles. All courses shown here are instructor-led courses.

For example, if you need to learn how to deploy and manage firewalls, you can take the EDU-210 course. If you intend to manage multiple firewalls remotely from Panorama, then you can take the EDU-220 course.

If you need to learn to tune your firewall policies or troubleshoot firewall issues, you can take EDU-330, after having completed the Firewall Administrator track.

If you need to learn how to deploy Prisma Access to securely connect and manage your remote users and remote sites, you can take EDU-318, after having completed the Firewall Administrator track.

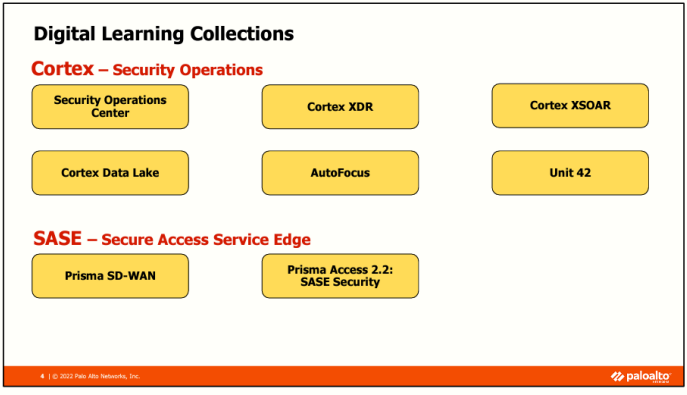
Take a moment to review the sample job roles and the courses recommended to prepare you for one of these job roles.



The slide shows the digital learning paths for Strata and Prisma Cloud products. Unlike instructor-led courses, these digital learning paths comprise multiple standalone activities that can be consumed at your own pace.

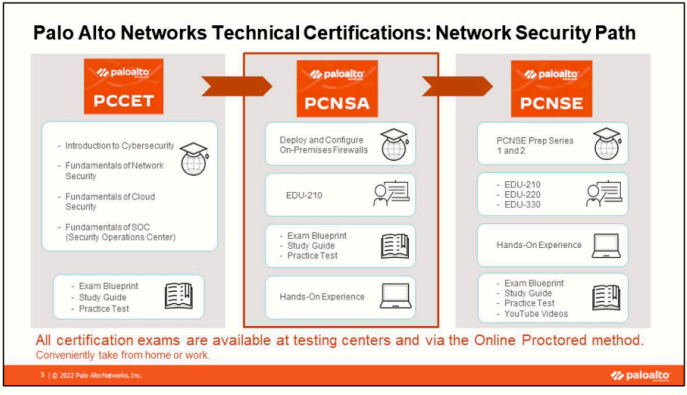
For example, if you need to learn how to deploy and manage firewalls, you can start with the Next-Generation Firewalls path. This path will navigate you through multiple lessons relevant to Network Security. After you have completed that path, you may select another to continue learning about firewalls, or select a path focused on another product.

For more information about each digital-learning course, log in to Beacon (beacon.paloaltonetworks.com) and search for the course name.



The slide shows the digital-learning collections for Cortex and SASE products.

For more information about each digital-learning course, log in to beacon.paloaltonetworks.com (external students) or flexlearn.paloaltonetworks.com (internal students) and search for the course name.



Palo Alto Networks certifications provide assurance that your knowledge of cybersecurity, network security, and how to deploy and operate the Palo Alto Networks product portfolio meets an established industry standard.

The **Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)** certification verifies that a person possesses knowledge of the cutting-edge cyberthreats of today and the technologies available to mitigate those threats. The PCCET is an introductory certification that validates your up-to-date knowledge about cybersecurity, network security, cloud security, and security operations center (SOC) security principles.

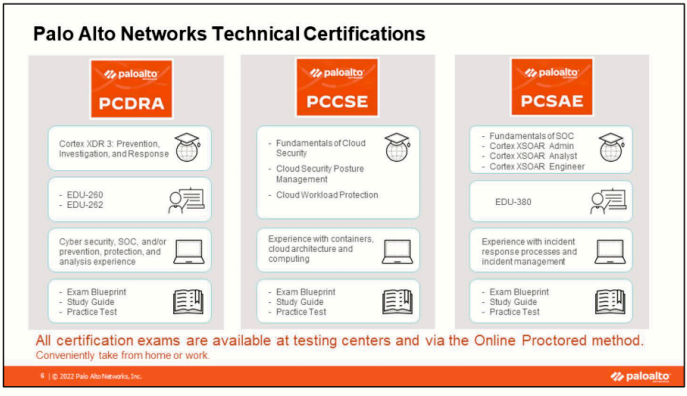
The **Palo Alto Networks Certified Network Security Administrator (PCNSA)** certification verifies that a person can operate Palo Alto Networks Next-Generation Firewalls to protect networks from cyberthreats. The PCNSA is a fundamental certification that validates your ability to configure the central features of the Palo Alto Networks Next-Generation Firewall and to effectively operate the firewalls to enable network traffic based on who (User-ID), what (App-ID), and when (policy), all while ensuring security (Content-ID).

The **Palo Alto Networks Certified Network Security Engineer (PCNSE)** certification verifies that a person can design, deploy, configure, maintain, and troubleshoot the majority of Palo Alto Networks product portfolio implementations. The PCNSE is an expert-level certification that validates your knowledge of the product portfolio, thus ensuring that you can make use of its full functionality to benefit your company and showcase your expertise.

Online Proctored (OP) exams are a new option from Palo Alto Networks. Now you can take certification exams in your own home or office while being monitored by a remote proctor. This option provides more convenience for you by removing the requirement to travel to an authorized testing center.

The process of scheduling an Online Proctored exam is easy and convenient: sign in or create an account at https://home.pearsonvue.com/paloaltonetworks and register. After you register, select the exam you want to schedule and look for the option to select **OP**.

To learn more about Palo Alto Networks certifications, visit www.paloaltonetworks.com/certification.

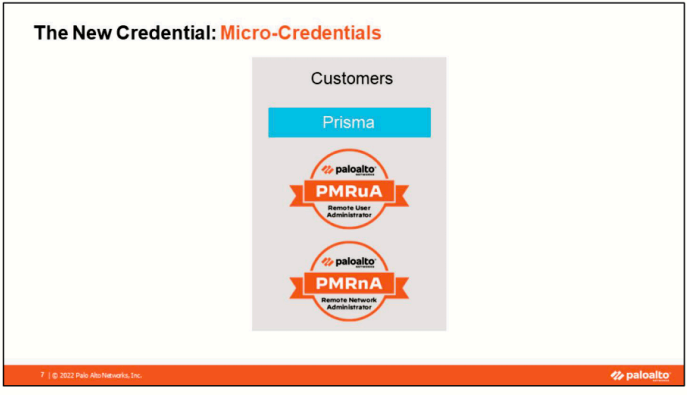


The **Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA)** certification validates that engineers possess the in-depth skills and knowledge to manage & respond to incidents, have exposure to different OS platforms, and have demonstrated the highest standard of deployment methodology and operational best practices associated with Palo Alto Networks Cortex® XDR™.

The **Prisma Certified Cloud Security Engineer (PCCSE)** certification validates the knowledge, skills, and abilities required to onboard, deploy, and administer all aspects of Prisma Cloud. Individuals with the PCCSE certification will have demonstrated in-depth knowledge of Palo Alto Networks Prisma Cloud technology and resources.

The **Palo Alto Networks Certified Security Automation Engineer (PCSAE)** certification validates the knowledge and skills required to develop, analyze, and administer the Palo Alto Networks Cortex XSOAR security orchestration, automation, and response platform with native threat intelligence management.

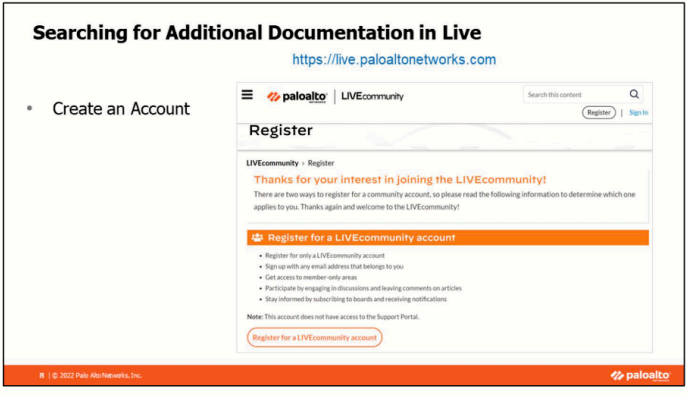
To learn more about Palo Alto Networks certifications, visit: www.paloaltonetworks.com/certification



The **Palo Alto Networks Micro-Credential Remote user Administrator** (**PMRuA)** micro-credential validates the knowledge, skills, and abilities required for a network engineer responsible for deploying Prisma SASE. PMRuA-credentialed individuals have demonstrated the comprehensive knowledge and skills to implement SASE for Secure Mobile Users.

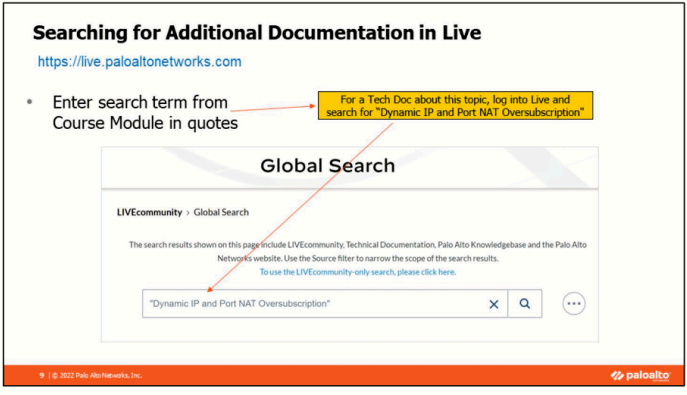
The **Palo Alto Networks Micro-Credential Remote network Administrator** (**PMRnA**) micro-credential validates the comprehensive knowledge, skills, and abilities required for a network engineer deploying Prisma SASE and implementing SD-WAN for remote networks.

To learn more about Palo Alto Networks certifications, visit: www.paloaltonetworks.com/certification



Throughout this course, you will find numerous references to external documentation and resources that you can use to delve deeper into topics, features and functions of the product. These references are available in the Palo Alto Networks LIVEcommunity, but you must have an account to access them.

Creating an account is free.

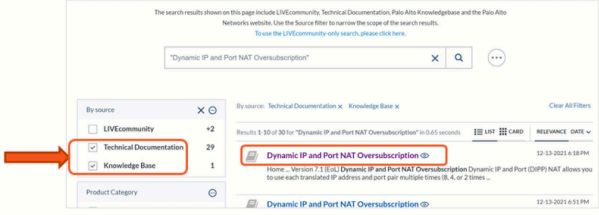


Once you have created your LIVEcommunity account, use the Global Search function to locate additional information. Be sure to put the search terms in quotation marks in order to locate the appropriate resource more quickly.

Searching for Additional Documentation in Live

https://live.paloaltonetworks.com

- Check **Technical Documentation** and **Knowledge Base**
- Select appropriate entry from search results

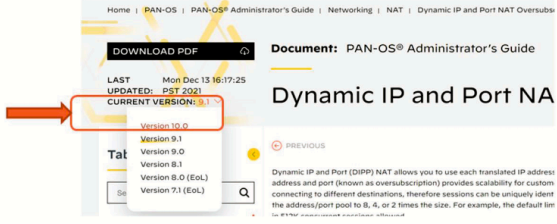


The references listed in this course will typically be located within the first few entries returned in the search results.

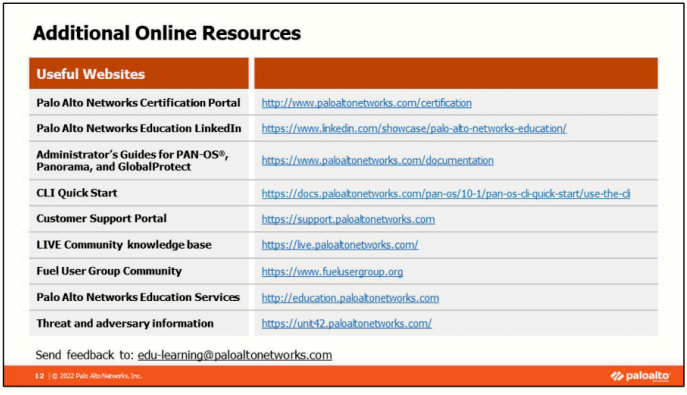
Searching for Additional Documentation in Live

https://live.paloaltonetworks.com

- Select appropriate PAN-OS Version



When you locate an article, be sure to select the appropriate version of PAN-OS to see information specific to your firewall or Panorama instance.



The Customer Support Portal helps you to get assistance managing Palo Alto Networks firewalls. The website has links that enable you to:

- Download software and updates for your firewalls
- Open and manage support cases
- Access product documentation and white papers
- Share custom content such as custom App-IDs, custom threats, CLI scripts, and other tools

The LIVE Community lets you connect with peers to ask questions, exchange ideas, and share experiences and knowledge. The member community is built by Palo Alto Networks users asking and answering questions.

The Palo Alto Networks Education Services website is the primary source of information regarding training about Palo Alto Networks firewalls. You can access course catalog and scheduling information for any of the courses offered by Palo Alto Networks Education Services. You also can find information about all certification programs.