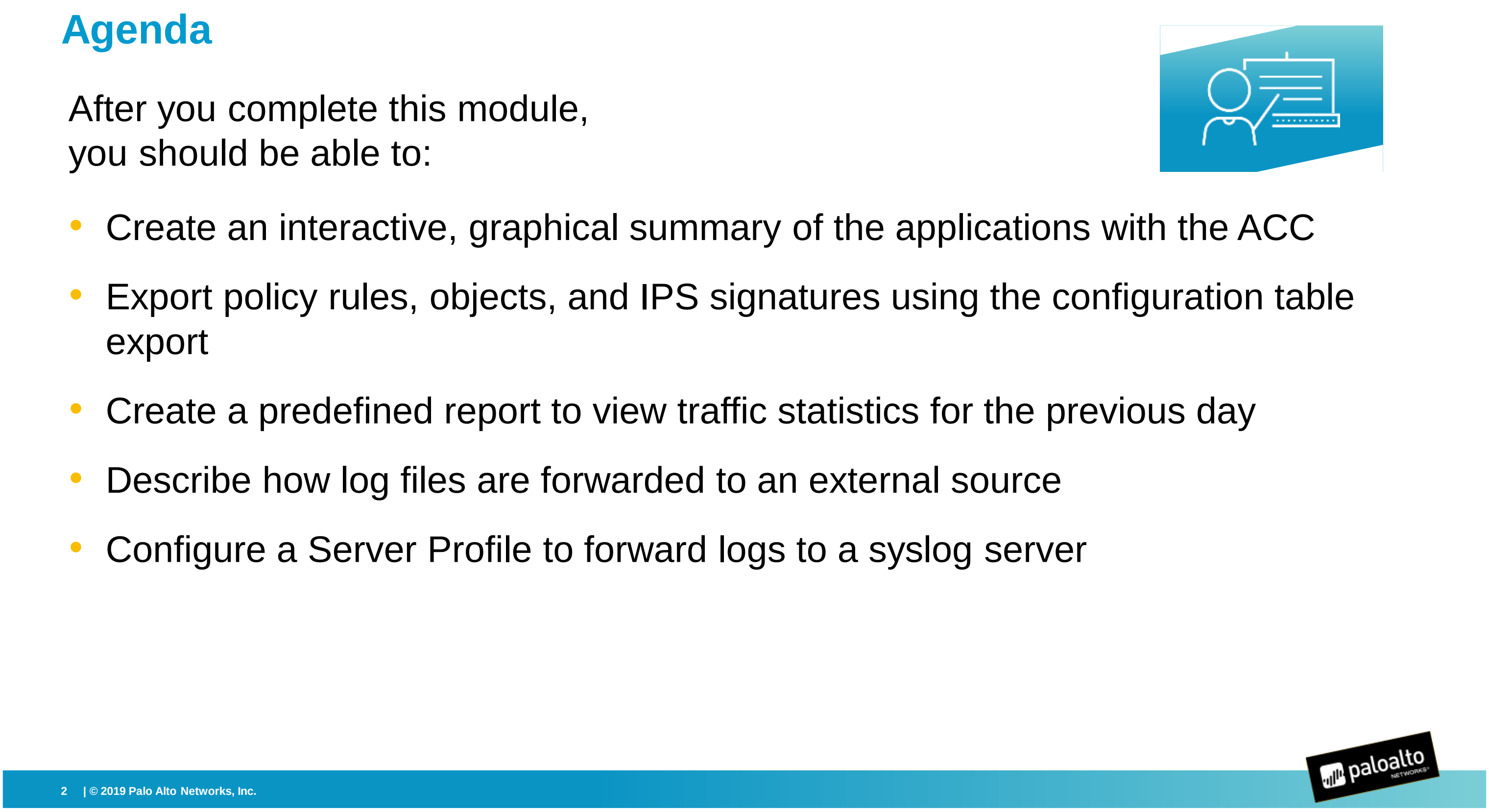
MONITORING AND REPORTING

EDU-210 Version A
PAN-OS® 9.0

SEE AND SHARE

- Dashboard, ACC, and monitor
- Log forwarding
- Syslog
- Configuring SNMP



Agenda

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

- Create an interactive, graphical summary of the applications with the ACC
- Export policy rules, objects, and IPS signatures using the configuration table export
- Create a predefined report to view traffic statistics for the previous day
- Describe how log files are forwarded to an external source
- Configure a Server Profile to forward logs to a syslog server

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

- Create an interactive, graphical summary of the applications with the ACC
- Export policy rules, objects, and IPS signatures using the configuration table export
- Create a predefined report to view traffic statistics for the previous day
- Describe how log files are forwarded to an external source
- Configure a Server Profile to forward logs to a syslog server

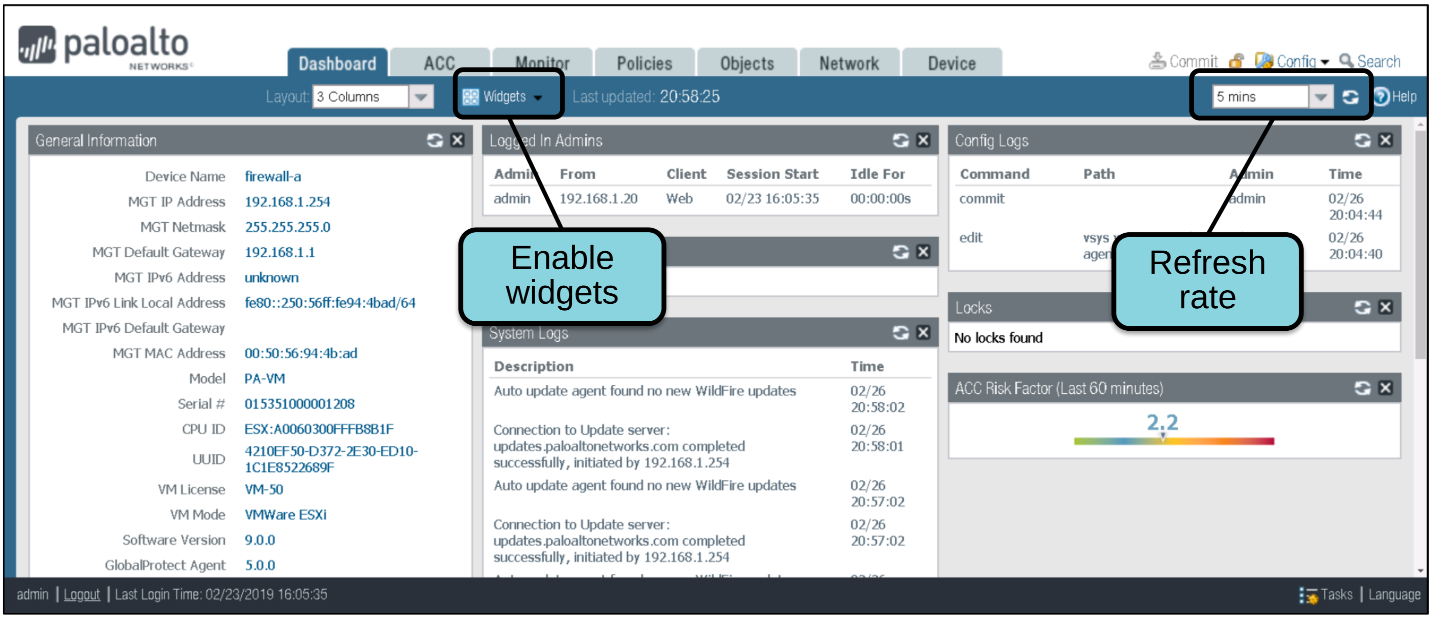
Dashboard, ACC, and Monitor

Log Forwarding

Syslog

Configuring SNMP

Palo Alto Networks Firewall Dashboard



Layout: 3 Columns

Last updated: 20:58:25

5 mins

Enable widgets

Refresh rate

General Information

Device Name	firewall-a
MGT IP Address	192.168.1.254
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168.1.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::250:56ff:fe94:4bad/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:50:56:94:4b:ad
Model	PA-VM
Serial #	015351000001208
CPU ID	ESX:A0060300FFFB8B1F
UUID	4210EF50-D372-2E30-ED10-1C1E8522689F
VM License	VM-50
VM Mode	VMWare ESXi
Software Version	9.0.0
GlobalProtect Agent	5.0.0

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	192.168.1.20	Web	02/23 16:05:35	00:00:00s

System Logs

Description	Time
Auto update agent found no new WildFire updates	02/26 20:58:02
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	02/26 20:58:01
Auto update agent found no new WildFire updates	02/26 20:57:02
Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	02/26 20:57:02

Config Logs

Command	Path	Admin	Time
commit		admin	02/26 20:04:44
edit	vsys agen		02/26 20:04:40

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

2.2

admin | Logout | Last Login Time: 02/23/2019 16:05:35

The **Dashboard** tab widgets show general device information, such as:

- Software version
- Operational status of each interface
- Resource use
- Up to 10 of the most recent entries in the Threat log
- Configuration
- System logs

All of the available widgets are displayed by default, but each administrator can remove and add individual widgets, as needed.

Click the **refresh** icon to update the **Dashboard**, or an individual widget.

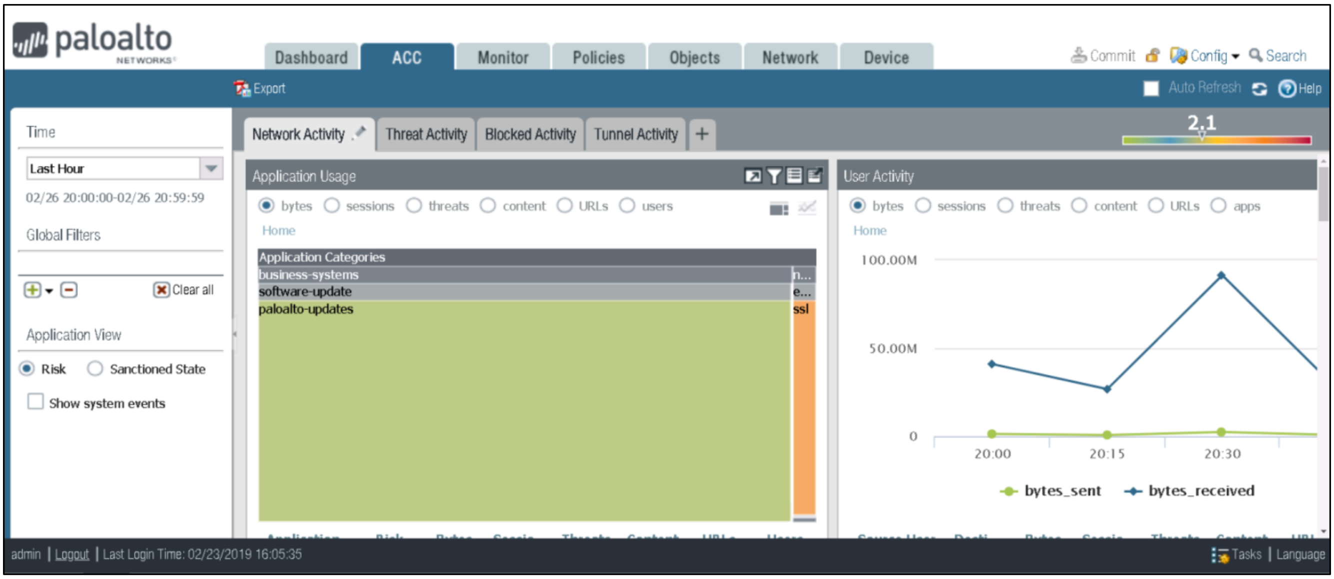
To change the automatic refresh interval, select an interval from the drop-down list (**1 min**, **2 mins**, **5 mins**, or **Manual**).

To add a widget to the **Dashboard**, click the **Widget** drop-down list in the title bar, select a category, and select the widget name.

To delete a widget, click the small **x** in the title bar of the widget.

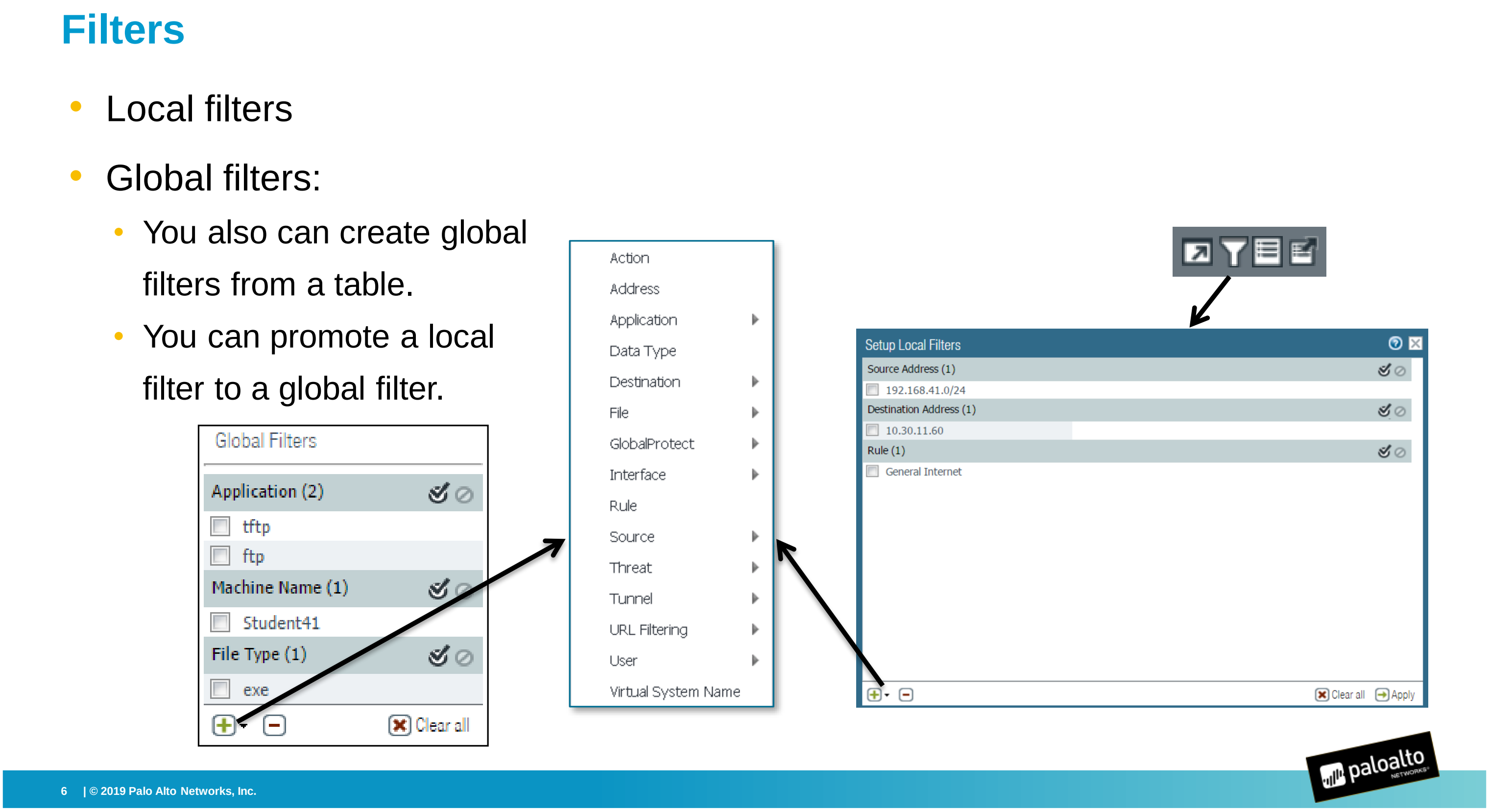
Application Command Center (ACC)

- ACC uses the firewall logs to provide an interactive, graphical summary of the applications, users, URLs, threats, and content traversing the firewall.



The ACC is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing your network. The ACC uses the firewall logs to provide visibility into traffic patterns and information about threats that can be acted on. The ACC layout includes a tabbed view of **Network Activity**, **Threat Activity**, **Blocked Activity**, and **Tunnel Activity**. Each tab includes pertinent widgets for better visualization of traffic patterns on your network. The graphical representation allows you to interact with the data and to visualize the relationships between events on the network so that you can uncover anomalies or find ways to enhance your network security rules. For a personalized view of your network, you also can add a custom tab and include widgets that allow you to look deeper into the information that is most important to you:

- Tabs: The ACC includes four predefined tabs that provide visibility into network traffic, threat activity, blocked activity, and tunnel activity. Each tab includes a default set of widgets that best represent the events or trends associated with the tab. The widgets enable you to survey the data using filters such as bytes received or bytes sent, number of sessions, type of content, and URL categories.
- Time: The charts or graphs in each widget provide a real-time and historic view. You can choose a custom range or use the predefined time periods that range from the last 15 minutes up to the last 30 days or last 30 calendar days.
- Global Filters: The global filters allow you to set the filter across all tabs. The charts and graphs apply the selected filters before rendering the data.



Filters

- Local filters
- Global filters:
  - You also can create global filters from a table.
  - You can promote a local filter to a global filter.

6 | © 2019 Palo Alto Networks, Inc.

Local Filters
Apply local filters to a specific widget. A local filter allows you to interact with the graph and to customize the display so that you can see the details and access the information you want to monitor on a specific widget. A local filter is persistent across reboots.

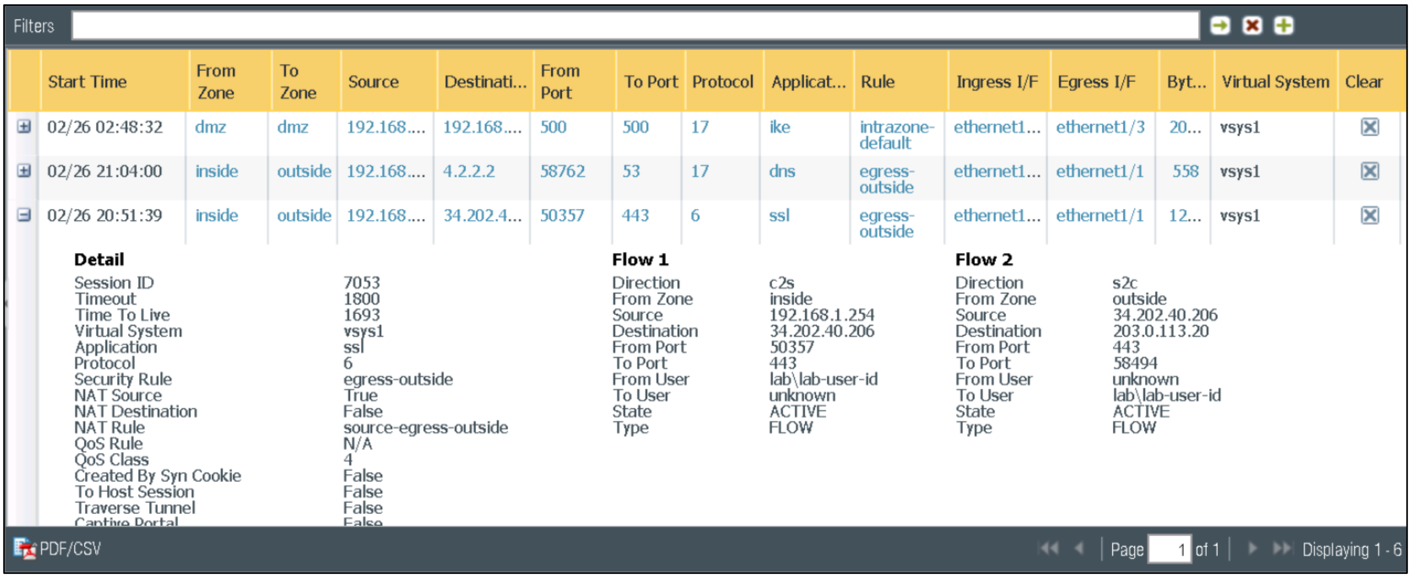
Global Filters
Apply global filters across all the tabs in the ACC. A global filter allows you to limit the display to the details you care about now and to exclude the unrelated information from the current display. For example, to display all events relating to a specific user and application, you can apply the user’s IP address or username and the application as a global filter and display only information pertaining to the user and the application through all the tabs and widgets on the ACC. Global filters are not persistent.

You can apply global filters in three ways:

- Set a global filter from a table: Select an attribute from a table in any widget and apply the attribute as a global filter
- Promote a local filter to a global filter: Allows you to take a local filter, which can be an attribute in a graph or table in a widget, and to apply the attribute globally. When you elevate a local filter to a global filter, the display is updated across all the tabs on the ACC.
- Define a global filter: Define a filter using the **Global Filters** pane on the ACC

Session Browser

Monitor > Session Browser



	Start Time	From Zone	To Zone	Source	Destinati...	From Port	To Port	Protocol	Applicat...	Rule	Ingress I/F	Egress I/F	Byt...	Virtual System	Clear
⊞	02/26 02:48:32	dmz	dmz	192.168....	192.168....	500	500	17	ike	intrazone-default	ethernet1...	ethernet1/3	20...	vsys1	☒
⊞	02/26 21:04:00	inside	outside	192.168....	4.2.2.2	58762	53	17	dns	egress-outside	ethernet1...	ethernet1/1	558	vsys1	☒
⊟	02/26 20:51:39	inside	outside	192.168....	34.202.4...	50357	443	6	ssl	egress-outside	ethernet1...	ethernet1/1	12...	vsys1	☒

Detail	
Session ID	7053
Timeout	1800
Time To Live	1693
Virtual System	vsys1
Application	ssl
Protocol	6
Security Rule	egress-outside
NAT Source	True
NAT Destination	False
NAT Rule	source-egress-outside
QoS Rule	N/A
QoS Class	4
Created By Syn Cookie	False
To Host Session	False
Traverse Tunnel	False
Captive Portal	False

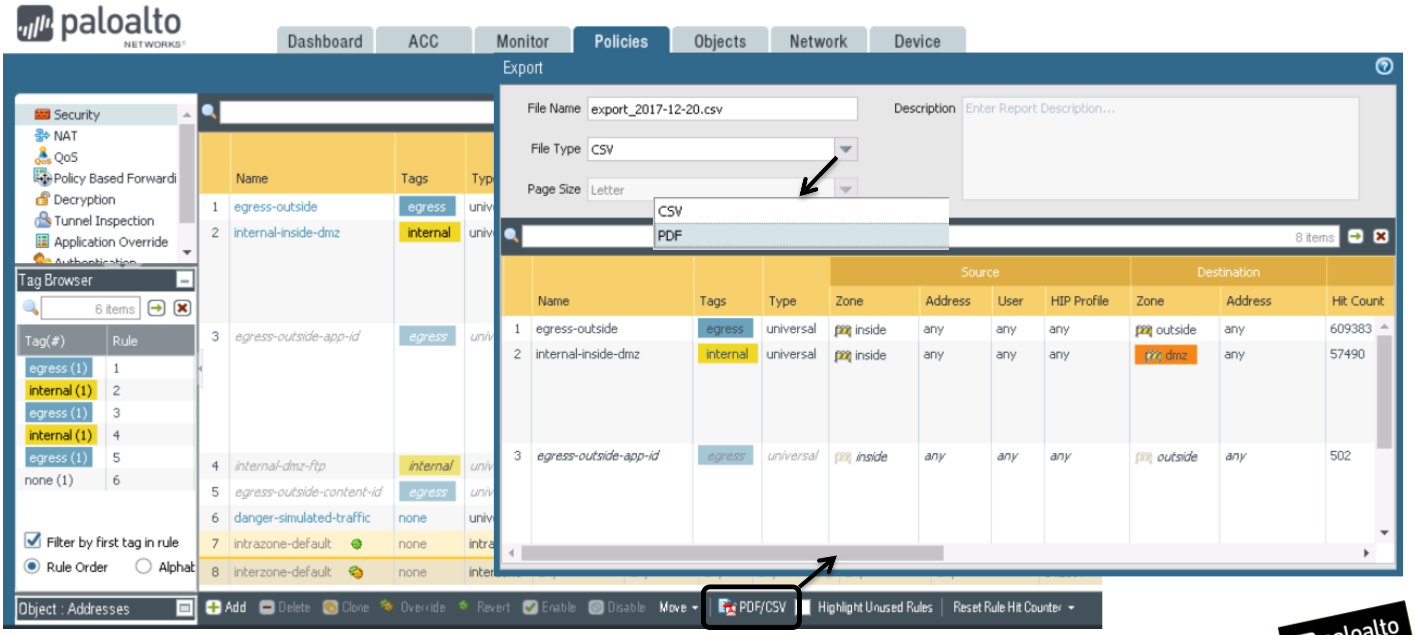
Flow 1	
Direction	c2s
From Zone	inside
Source	192.168.1.254
Destination	34.202.40.206
From Port	50357
To Port	443
From User	lab\lab-user-id
To User	unknown
State	ACTIVE
Type	FLOW

Flow 2	
Direction	s2c
From Zone	outside
Source	34.202.40.206
Destination	203.0.113.20
From Port	443
To Port	58494
From User	unknown
To User	lab\lab-user-id
State	ACTIVE
Type	FLOW

Select **Monitor** > **Session Browser** to browse and filter sessions that are current on the firewall.

Configuration Table Export

Policies > Security > PDF/CSV



Export

File Name: export_2017-12-20.csv

File Type: CSV

Page Size: Letter

CSV
PDF

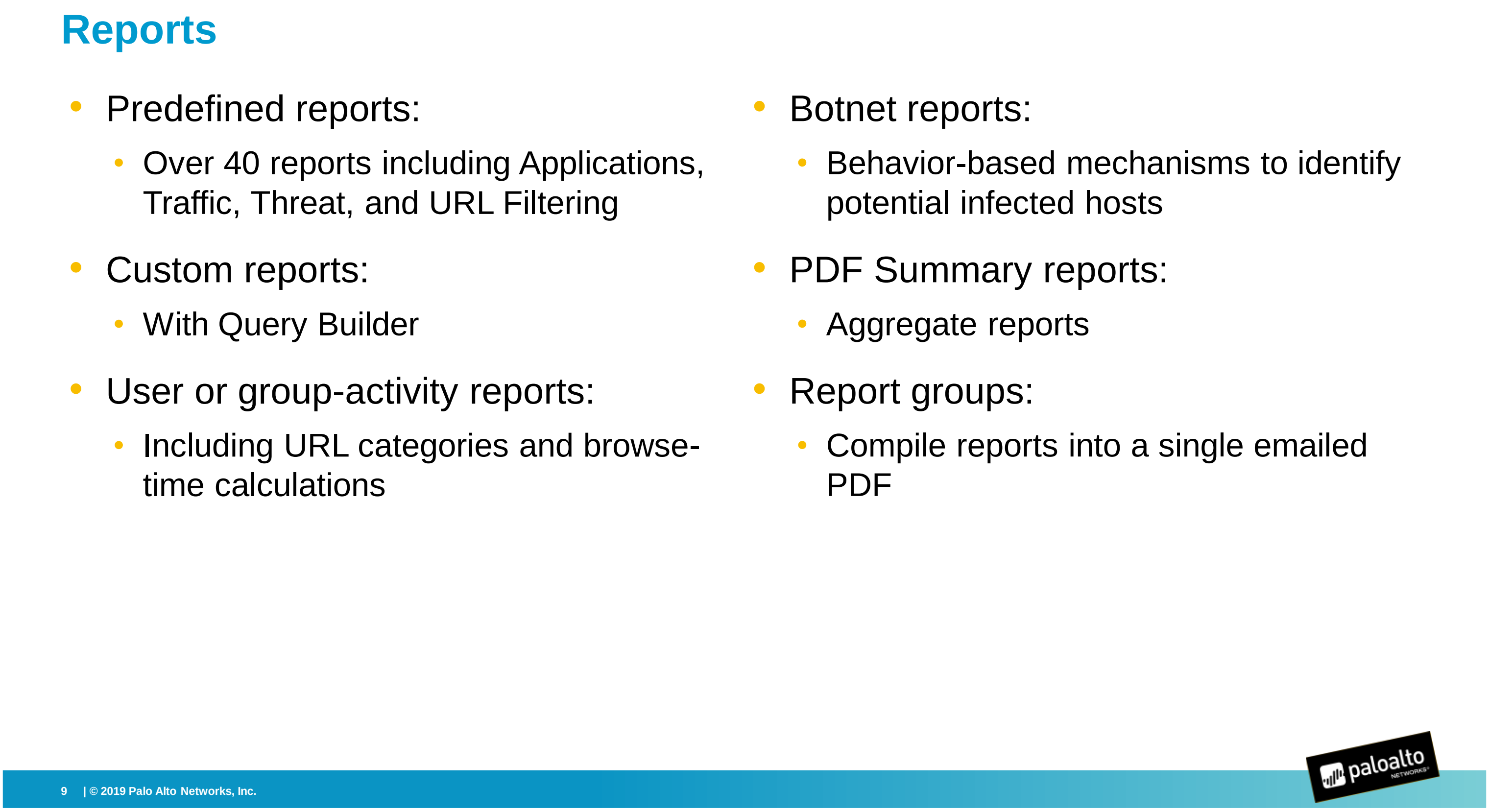
Description: Enter Report Description…

8 items

				Source				Destination		
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count
1	egress-outside	egress	universal	inside	any	any	any	outside	any	609383
2	internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any	57490
3	*egress-outside-app-id*	*egress*	*universal*	*inside*	*any*	*any*	*any*	*outside*	*any*	502

Starting with PAN-OS® 8.1, you can export policy rules, objects, and IPS signatures from Panorama and firewalls to demonstrate regulatory compliance to external auditors, to conduct periodic reviews of the firewall configuration, and to generate reports about firewall policies. You no longer need to give your auditors direct access to your firewalls, to take screenshots, or to use the XML API to generate configuration reports.

From the web interface, you can export configuration data for **Policies**, **Objects**, **Network**, **Device**, and Panorama configurations, and the **Exceptions** in the **Antivirus**, **Anti-Spyware**, and **Vulnerability Protection**. Configuration table export works like a print function, and generated files cannot be imported back into the firewall. The data that you view on the web interface is exported into either a PDF or CSV file format. You can apply filters that match your report criteria and search within PDF reports to quickly find specific data. After you export the configuration table data, a system log is generated to record the event.



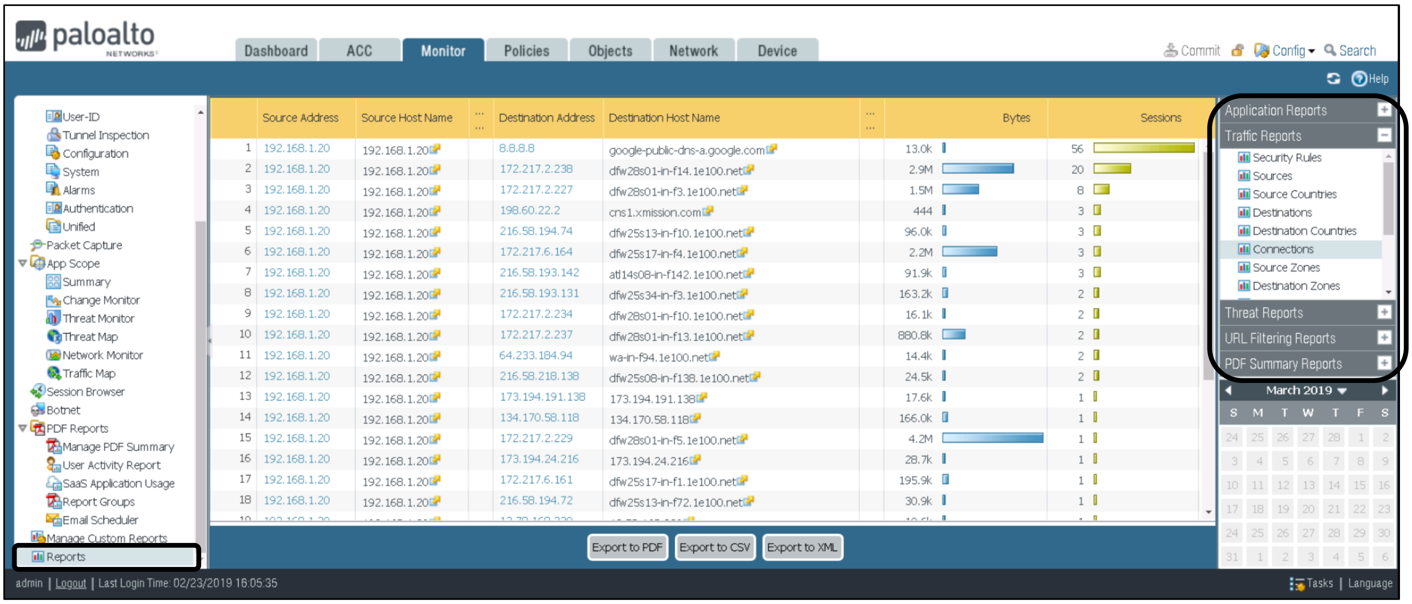
Reports

- Predefined reports:
  - Over 40 reports including Applications, Traffic, Threat, and URL Filtering
- Custom reports:
  - With Query Builder
- User or group-activity reports:
  - Including URL categories and browse-time calculations
- Botnet reports:
  - Behavior-based mechanisms to identify potential infected hosts
- PDF Summary reports:
  - Aggregate reports
- Report groups:
  - Compile reports into a single emailed PDF

The web interface enables you to display network and firewall activity using a variety of built-in and custom reports. These reports can be helpful as you research current threats to your organization.

Predefined Reports

Monitor > Reports



	Source Address	Source Host Name	Destination Address	Destination Host Name	Bytes	Sessions
1	192.168.1.20	192.168.1.20	8.8.8.8	google-public-dns-a.google.com	13.0k	56
2	192.168.1.20	192.168.1.20	172.217.2.238	dfw28s01-in-f14.1e100.net	2.9M	20
3	192.168.1.20	192.168.1.20	172.217.2.227	dfw28s01-in-f3.1e100.net	1.5M	8
4	192.168.1.20	192.168.1.20	198.60.22.2	cns1.xmission.com	444	3
5	192.168.1.20	192.168.1.20	216.58.194.74	dfw25s13-in-f10.1e100.net	96.0k	3
6	192.168.1.20	192.168.1.20	172.217.6.164	dfw25s17-in-f4.1e100.net	2.2M	3
7	192.168.1.20	192.168.1.20	216.58.193.142	atl14s08-in-f142.1e100.net	91.9k	3
8	192.168.1.20	192.168.1.20	216.58.193.131	dfw25s34-in-f3.1e100.net	163.2k	2
9	192.168.1.20	192.168.1.20	172.217.2.234	dfw28s01-in-f10.1e100.net	16.1k	2
10	192.168.1.20	192.168.1.20	172.217.2.237	dfw28s01-in-f13.1e100.net	880.8k	2
11	192.168.1.20	192.168.1.20	64.233.184.94	wa-in-f94.1e100.net	14.4k	2
12	192.168.1.20	192.168.1.20	216.58.218.138	dfw25s08-in-f138.1e100.net	24.5k	2
13	192.168.1.20	192.168.1.20	173.194.191.138	173.194.191.138	17.6k	1
14	192.168.1.20	192.168.1.20	134.170.58.118	134.170.58.118	166.0k	1
15	192.168.1.20	192.168.1.20	172.217.2.229	dfw28s01-in-f5.1e100.net	4.2M	1
16	192.168.1.20	192.168.1.20	173.194.24.216	173.194.24.216	28.7k	1
17	192.168.1.20	192.168.1.20	172.217.6.161	dfw25s17-in-f1.1e100.net	195.9k	1
18	192.168.1.20	192.168.1.20	216.58.194.72	dfw25s13-in-f72.1e100.net	30.9k	1

The firewall provides various “top 50” reports of the traffic statistics for the previous day or for a selected day in the previous week.

To display the reports, click the report names on the left side of the page under the **Monitor** tab. By default, all reports are displayed for the previous calendar day.

To display reports for any of the previous days, select a report generation date from the **Select** drop-down list at the bottom of the page.

The reports are listed in sections.

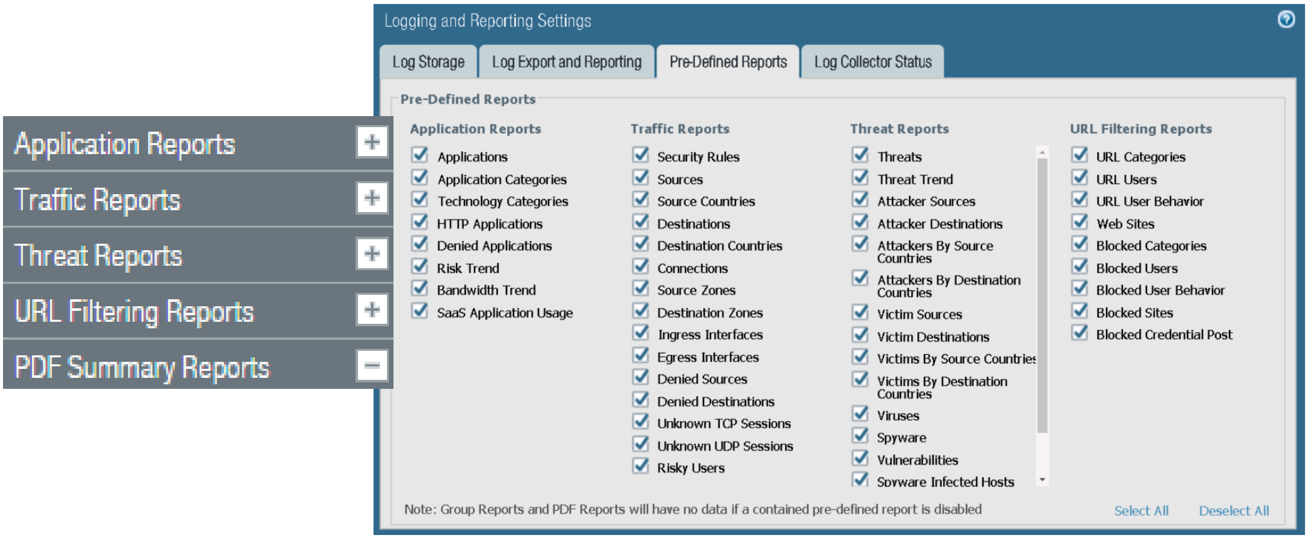
Information can be displayed in each report for the selected time period.

Reports can be saved to the local system in either PDF or CSV format.

Logging and Reporting Settings

- About 40 predefined reports are generated every day.

Device > Setup > Management > Logging and Reporting Settings



Logging and Reporting Settings

Log Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

Pre-Defined Reports

Application Reports

☑ Applications
☑ Application Categories
☑ Technology Categories
☑ HTTP Applications
☑ Denied Applications
☑ Risk Trend
☑ Bandwidth Trend
☑ SaaS Application Usage

Traffic Reports

☑ Security Rules
☑ Sources
☑ Source Countries
☑ Destinations
☑ Destination Countries
☑ Connections
☑ Source Zones
☑ Destination Zones
☑ Ingress Interfaces
☑ Egress Interfaces
☑ Denied Sources
☑ Denied Destinations
☑ Unknown TCP Sessions
☑ Unknown UDP Sessions
☑ Risky Users

Threat Reports

☑ Threats
☑ Threat Trend
☑ Attacker Sources
☑ Attacker Destinations
☑ Attackers By Source Countries
☑ Attackers By Destination Countries
☑ Victim Sources
☑ Victim Destinations
☑ Victims By Source Countries
☑ Victims By Destination Countries
☑ Viruses
☑ Spyware
☑ Vulnerabilities
☑ Spyware Infected Hosts

URL Filtering Reports

☑ URL Categories
☑ URL Users
☑ URL User Behavior
☑ Web Sites
☑ Blocked Categories
☑ Blocked Users
☑ Blocked User Behavior
☑ Blocked Sites
☑ Blocked Credential Post

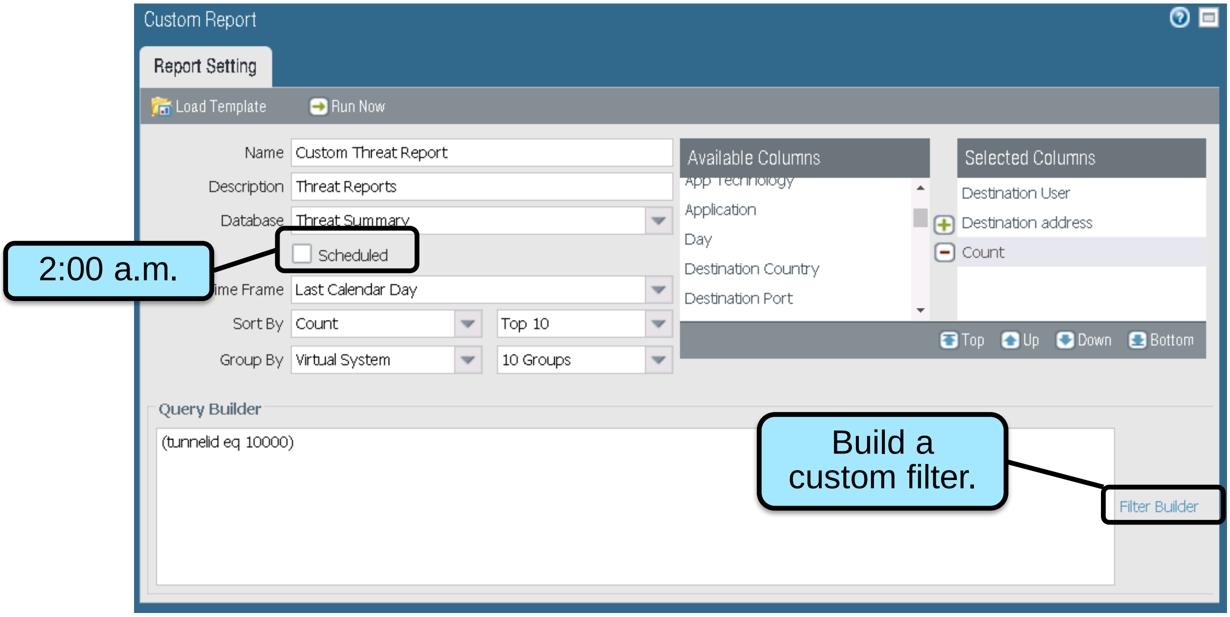
Note: Group Reports and PDF Reports will have no data if a contained pre-defined report is disabled

Select All Deselect All

The specific number of predefined reports generated is variable, and changes independently of firmware.

Custom Reports

Monitor > Manage Custom Report



Custom Report

Report Setting

Name: Custom Threat Report

Description: Threat Reports

Database: Threat Summary

☐ Scheduled

ime Frame: Last Calendar Day

Sort By: Count | Top 10

Group By: Virtual System | 10 Groups

Available Columns: App Technology, Application, Day, Destination Country, Destination Port

Selected Columns: Destination User, Destination address, Count

Query Builder

(tunnelid eq 10000)

2:00 a.m.

Build a custom filter.

To base a report on a predefined template, click **Load Template** and choose the template. You then can edit the template and save it as a custom report.

One possible column is SaaS, which allows you to see information about the use of hosted applications such as Lotus Notes, NetSuite, Salesforce, SharePoint, and Workday.

Select the **Scheduled** check box to run the report each day at 2 a.m. The report is available for viewing in the **Reports** column on the side.

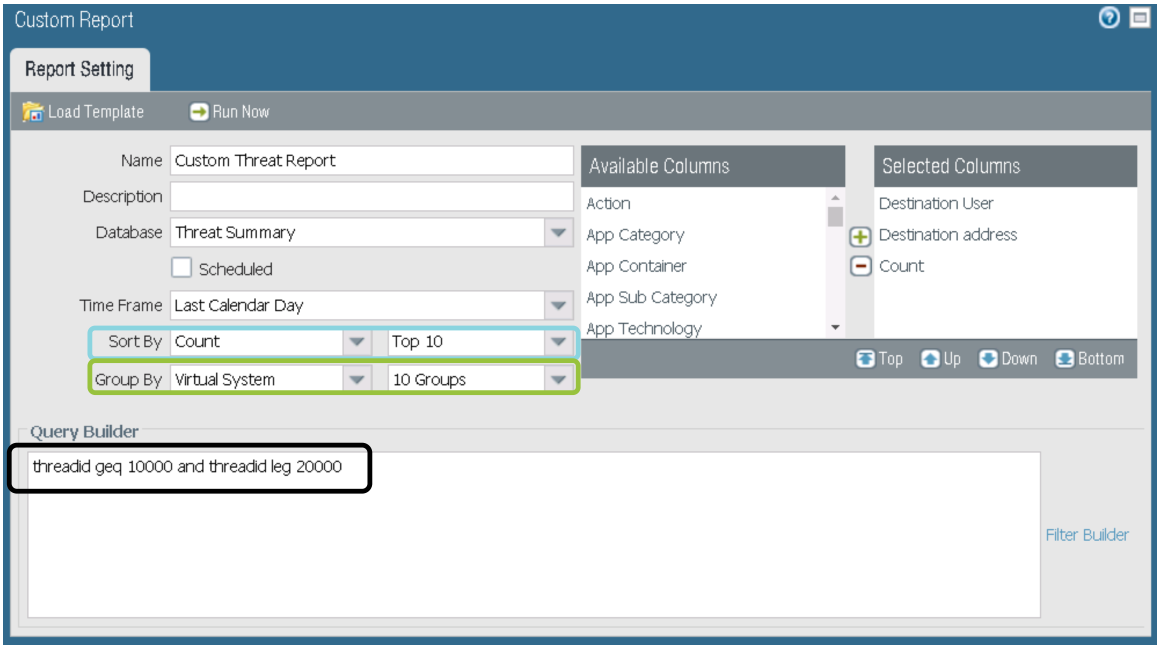
Click **Run Now** for the report to become available immediately.

The **Query Builder** allows you to define specific queries to further refine the selected attributes.

The **Query Builder** also enables customization of the report through use of the “and” and “or” connectors and match criteria consisting of an attribute, operator, and value. You then can include or exclude data that matches the query.

Queries enable the generation of a more focused collation of information in a report.

Sort and Group



Custom Report

Report Setting

Load Template | Run Now

Name: Custom Threat Report

Description:

Database: Threat Summary

□ Scheduled

Time Frame: Last Calendar Day

Sort By: Count | Top 10

Group By: Virtual System | 10 Groups

Available Columns	Selected Columns
Action	Destination User
App Category	Destination address
App Container	Count
App Sub Category	
App Technology	

Top | Up | Down | Bottom

Query Builder

```
threadid geq 10000 and threadid leq 20000
```

Filter Builder

Match

Sort

Group

Database Field

- Summary databases:
  - For traffic, threat, application, URL, and tunnel statistics
  - Condensed
- Detailed logs:
  - Provide much more information but can consume substantial storage and processing resources

Attributes

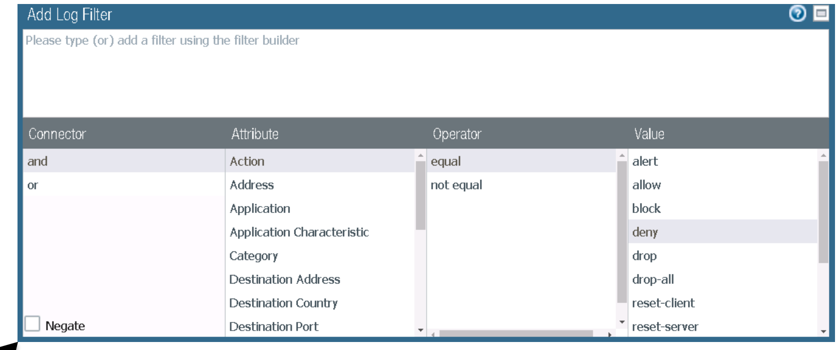
- Match criteria

Sort By and Group By Fields

- **Sort By** option specifies the attribute that is used to order attributes in a report.
- **Group By** option allows you to select an attribute and use it as an anchor for grouping data.

User or Group Activity Reports

- User or Group Activity reports summarize the web activity of individual users or user groups.
- User-ID technology must be enabled.

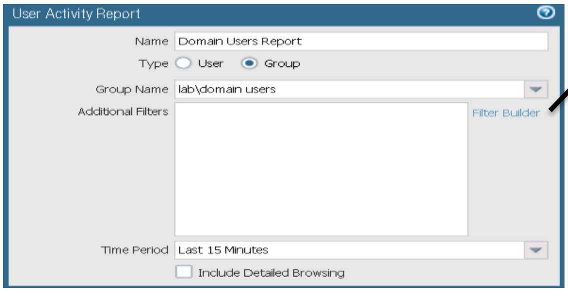


Add Log Filter

Please type (or) add a filter using the filter builder

Connector	Attribute	Operator	Value
and	Action	equal	alert
or	Address	not equal	allow
	Application		block
	Application Characteristic		deny
	Category		drop
	Destination Address		drop-all
	Destination Country		reset-client
□ Negate	Destination Port		reset-server

Monitor > PDF Reports > User Activity Report



User Activity Report

Name: Domain Users Report

Type: ○ User ● Group

Group Name: lab\domain users

Additional Filters:

Time Period: Last 15 Minutes

□ Include Detailed Browsing

A completed report can be downloaded in PDF form. Note that the User/Group Activity reports are not saved locally on the firewall.

1. Select **Monitor** > **PDF Reports** > **User Activity Report**.

2. Click **Add** and then enter a **Name** for the report.

3. Create the report:
   - For a User Activity report: Select **User** and enter the **Username** or IP address (**IPv4** or **IPv6**) of the user who will be the subject of the report.
   - For a Group Activity report: Select **Group** and select the **Group Name** from which to retrieve user group information in the report.
   - For a Custom User or Group Activity report: Select **Filter Builder** and select the appropriate **Connector**, **Attribute**, **Operator**, and **Value** for your report.

4. Select the time period for the report from the drop-down list:
   - **Note:** The number of logs that are analyzed in a User Activity report is determined by the number of rows defined on the **Max Rows in User Activity Report** on the **Logging and Reporting Settings** section in **Device** > **Setup** > **Management**.

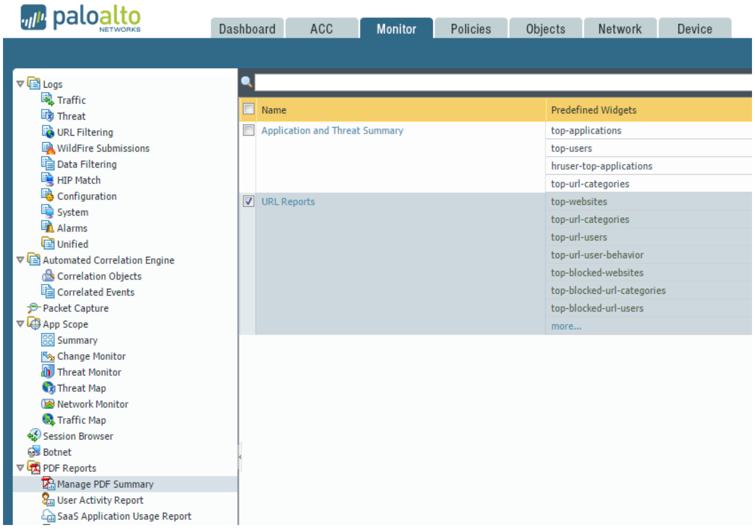
5. Select **Include Detailed Browsing** to include detailed URL logs in the report:
   - The detailed browsing information can include a large volume of logs (thousands of logs) for the selected user or user group and can make the report very large.

6. To run the report on demand, click **Run Now**.

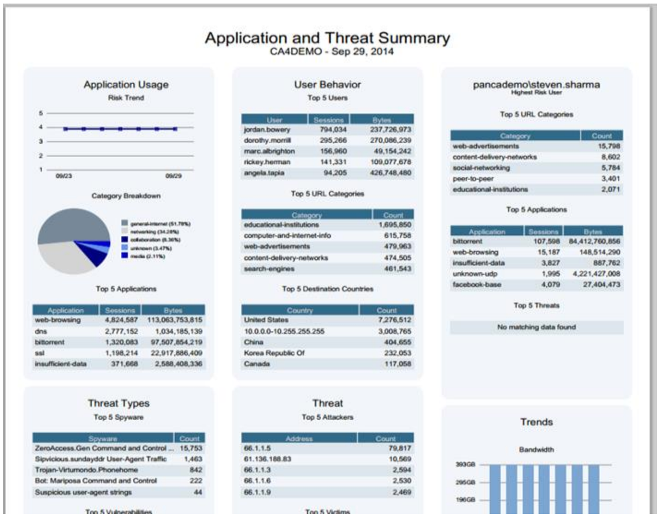
7. To save the report, click **OK**:
   - User/Group Activity reports cannot be saved on the firewall.

PDF Summary Reports

Monitor > PDF Reports > Manage PDF Summary



	Name	Predefined Widgets
□	Application and Threat Summary	top-applications top-users hruser-top-applications top-url-categories
☑	URL Reports	top-websites top-url-categories top-url-users top-url-user-behavior top-blocked-websites top-blocked-url-categories top-blocked-url-users more...



Application and Threat Summary
CA4DEMO - Sep 29, 2014

Application Usage

Risk Trend

Category Breakdown

Top 5 Applications

Application	Sessions	Bytes
web-browsing	4,824,587	113,063,753,815
dns	2,777,152	1,034,185,139
bittorrent	1,320,083	97,507,854,219
ssl	1,198,214	22,917,886,409
insufficient-data	371,668	2,588,408,336

User Behavior

Top 5 Users

User	Sessions	Bytes
jordan.bowery	794,034	237,726,973
dorothy.morrill	295,266	270,086,239
marc.albrighton	156,960	49,154,242
rickey.herman	141,331	109,077,678
angela.tapia	94,205	426,748,480

Top 5 URL Categories

Category	Count
educational-institutions	1,695,850
computer-and-internet-info	615,758
web-advertisements	479,963
content-delivery-networks	474,505
search-engines	461,543

Top 5 Destination Countries

Country	Count
United States	7,276,512
10.0.0.0-10.255.255.255	3,008,765
China	404,655
Korea Republic Of	232,053
Canada	117,058

pancademo\steven.sharma
Highest Risk User

Top 5 URL Categories

Category	Count
web-advertisements	15,798
content-delivery-networks	8,602
social-networking	5,784
peer-to-peer	3,401
educational-institutions	2,071

Top 5 Applications

Application	Sessions	Bytes
bittorrent	107,598	84,412,760,856
web-browsing	15,187	148,514,290
insufficient-data	3,827	887,762
unknown-udp	1,995	4,221,427,008
facebook-base	4,079	27,404,473

Top 5 Threats

No matching data found

Threat Types

Top 5 Spyware

Spyware	Count
ZeroAccess.Gen Command and Control ...	15,753
Sipvicious.sundayddr User-Agent Traffic	1,463
Trojan-Virtumondo.Phonehome	842
Bot: Mariposa Command and Control	222
Suspicious user-agent strings	44

Top 5 Vulnerabilities

Threat

Top 5 Attackers

Address	Count
66.1.1.5	79,817
61.136.188.83	10,569
66.1.1.3	2,594
66.1.1.6	2,530
66.1.1.9	2,469

Top 5 Victims

Trends

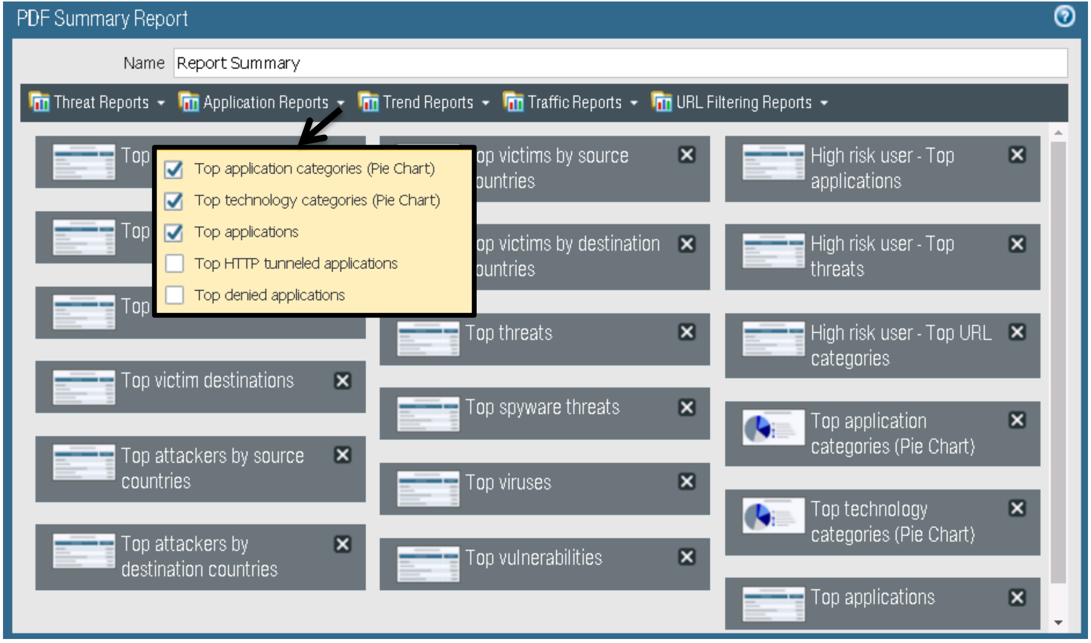
Bandwidth

PDF summary reports contain:

- Information compiled from existing reports based on data for the top 5 in each category
- Trend charts that are not available in other reports

Generate PDF Summary Reports

Monitor > PDF Reports > Manage PDF Summary



PDF Summary Report

Name: Report Summary

☑ Top application categories (Pie Chart)
☑ Top technology categories (Pie Chart)
☑ Top applications
□ Top HTTP tunneled applications
□ Top denied applications

Threat Reports
Application Reports
Trend Reports
Traffic Reports
URL Filtering Reports
Top
Top
Top
Top victim destinations
Top attackers by source countries
Top attackers by destination countries
op victims by source ountries
op victims by destination ountries
Top threats
Top spyware threats
Top viruses
Top vulnerabilities
High risk user - Top applications
High risk user - Top threats
High risk user - Top URL categories
Top application categories (Pie Chart)
Top technology categories (Pie Chart)
Top applications

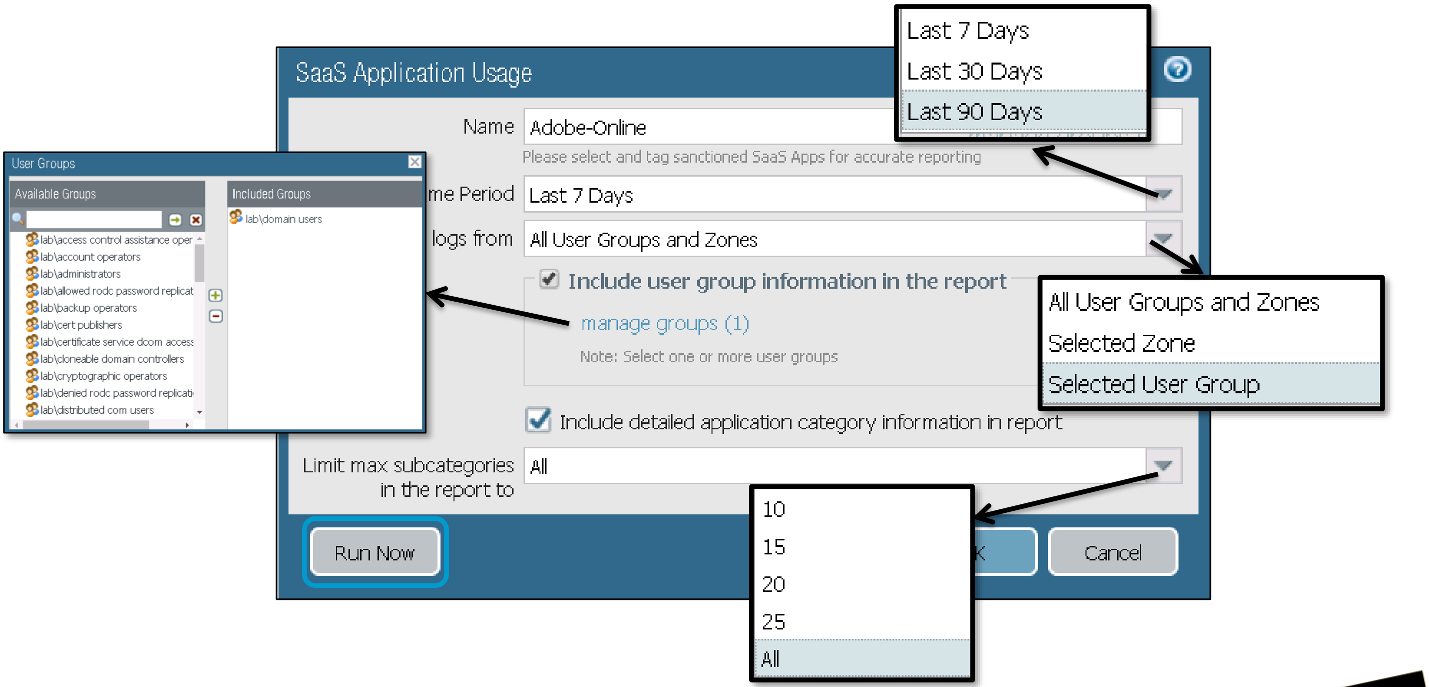
Use the drop-down list for each report group and select one or more of the elements to design the PDF Summary report.

A maximum of 18 report elements may be included:

1. To display the report, go to **Monitor > PDF Reports**.
2. Select **Manage PDF Summary Reports**.
3. Select a **date**.

The report downloads as a PDF.

SaaS Application Usage Report



SaaS Application Usage

Name: Adobe-Online

Please select and tag sanctioned SaaS Apps for accurate reporting

me Period Last 7 Days

logs from All User Groups and Zones

☑ Include user group information in the report

manage groups (1)

Note: Select one or more user groups

☑ Include detailed application category information in report

Limit max subcategories in the report to: All

User Groups

Available Groups	Included Groups
lab\access control assistance oper	lab\domain users
lab\account operators	
lab\administrators	
lab\allowed rodc password replicat	
lab\backup operators	
lab\cert publishers	
lab\certificate service dcom access	
lab\cloneable domain controllers	
lab\cryptographic operators	
lab\denied rodc password replicati	
lab\distributed com users	

You must use the predefined **Sanctioned** tag (with the blue-colored background) to indicate that you sanctioned an application, otherwise the firewall will fail to recognize the tag and the report will be inaccurate.

By default, the report includes detailed information about the top SaaS and non-SaaS application subcategories, which can make the report large by page count and file size. Clear the **Include detailed application category information in report** check box if you want to reduce the file size and restrict the page count to eight pages.

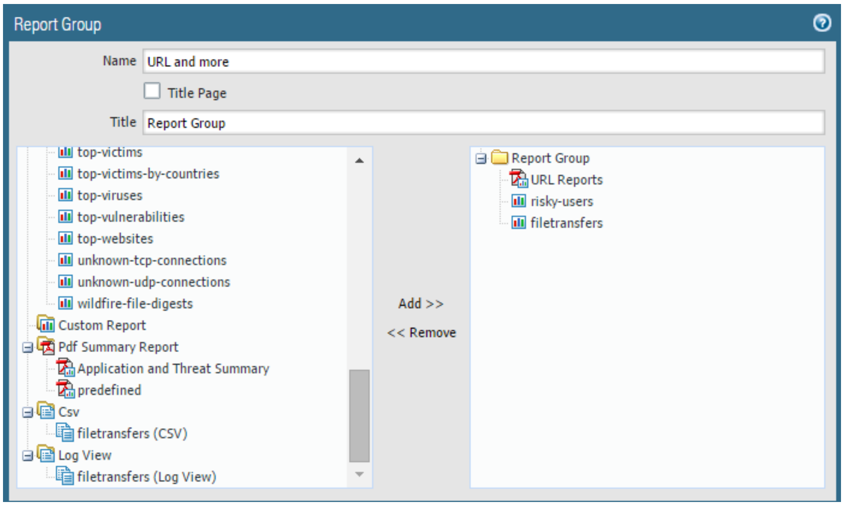
You can schedule the report for email delivery as a PDF file attachment on all models except for the PA-200, PA-500, and PA-2000 Series firewalls. For these models of firewalls, an embedded link is included within the email that will allow you to display the report in a web browser.

Use your insights from this report to consolidate the list of business-critical and approved SaaS applications and to enforce policies for controlling unsanctioned applications that pose an unnecessary risk for malware propagation and data leaks. Information shown for each application in a subcategory includes the top users who transferred data, the top blocked or alerted file types, and the top threats for each application. This section of the report also tallies the total number of WildFire® submissions and verdicts for samples submitted by the firewall per application.

Report Groups

- Report groups create a set of reports that the firewall compiles into a single report.

Monitor > PDF Reports > Report Groups



Report Group

Name URL and more

☐ Title Page

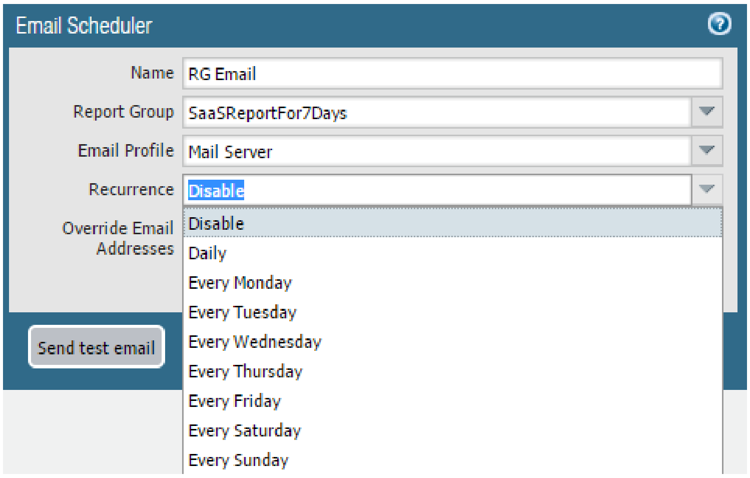
Title Report Group

Report groups enable you to create sets of reports that the firewall can compile and send as a single aggregate PDF report with an optional title page and all the constituent reports included.

Emailing Reports

- A report group must be emailed, rather than downloaded.
- Create a Server Profile for your email server:
  - Device > Server Profiles > Email
  - Specify recipients
- Scheduled reports are sent at 2:00 a.m.

Monitor > PDF Reports > Email Scheduler


Email Scheduler

Name: RG Email
Report Group: SaaSReportFor7Days
Email Profile: Mail Server
Recurrence: Disable
Override Email Addresses

The **Override Email Addresses** field allows a report to be sent exclusively to the recipients specified.

When recipients are added to the override recipient email(s), the report is not sent to the recipients configured in the email Server Profile.

Use this option for those occasions when the report is for the attention of someone other than the administrators or recipients defined in the email Server Profile.

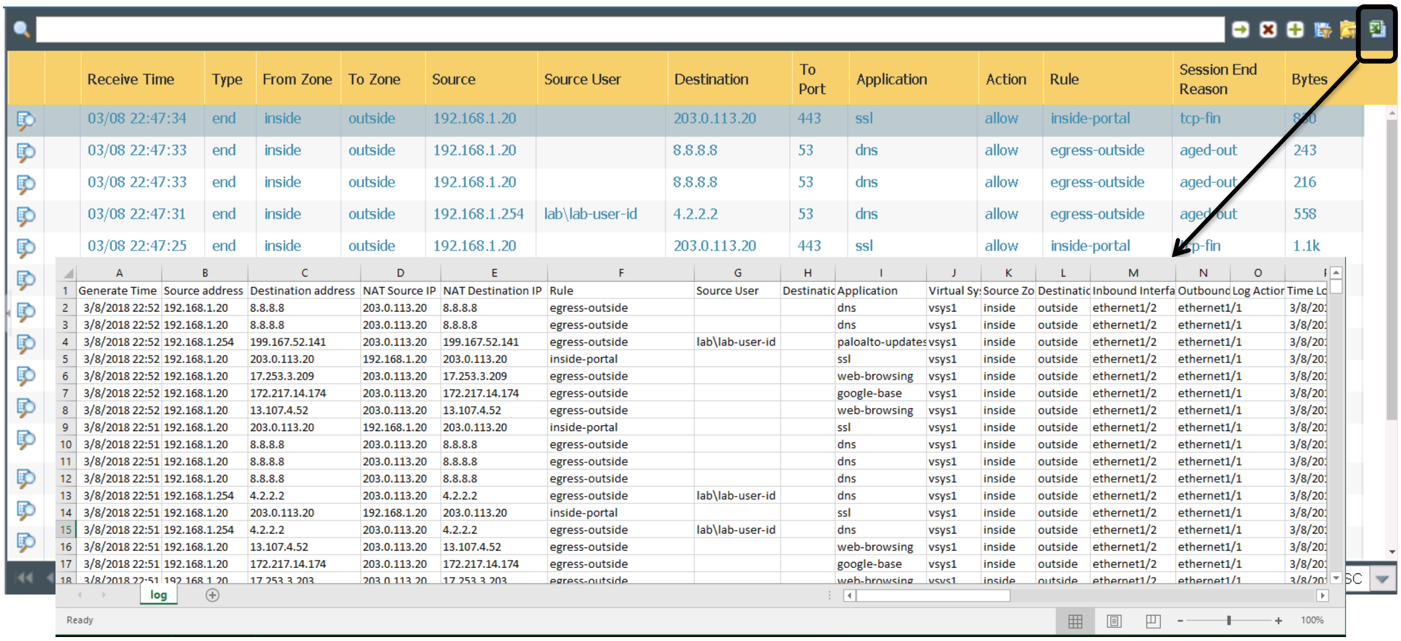
Dashboard, ACC, and monitor

Log forwarding

Syslog

Configuring SNMP

Exporting Current Log Listing to CSV



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
03/08 22:47:34	end	inside	outside	192.168.1.20		203.0.113.20	443	ssl	allow	inside-portal	tcp-fin	830
03/08 22:47:33	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	egress-outside	aged-out	243
03/08 22:47:33	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	egress-outside	aged-out	216
03/08 22:47:31	end	inside	outside	192.168.1.254	lab\lab-user-id	4.2.2.2	53	dns	allow	egress-outside	aged-out	558
03/08 22:47:25	end	inside	outside	192.168.1.20		203.0.113.20	443	ssl	allow	inside-portal	tcp-fin	1.1k

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Generate Time	Source address	Destination address	NAT Source IP	NAT Destination IP	Rule	Source User	Destinatic	Application	Virtual Sy:	Source Zo	Destinatic	Inbound Interfa	Outbound	Log Actior	Time Lo
2	3/8/2018 22:52	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside			dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
3	3/8/2018 22:52	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside			dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
4	3/8/2018 22:52	192.168.1.254	199.167.52.141	203.0.113.20	199.167.52.141	egress-outside	lab\lab-user-id		paloalto-updates	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
5	3/8/2018 22:52	192.168.1.20	203.0.113.20	192.168.1.20	203.0.113.20	inside-portal			ssl	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
6	3/8/2018 22:52	192.168.1.20	17.253.3.209	203.0.113.20	17.253.3.209	egress-outside			web-browsing	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
7	3/8/2018 22:52	192.168.1.20	172.217.14.174	203.0.113.20	172.217.14.174	egress-outside			google-base	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
8	3/8/2018 22:52	192.168.1.20	13.107.4.52	203.0.113.20	13.107.4.52	egress-outside			web-browsing	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
9	3/8/2018 22:51	192.168.1.20	203.0.113.20	192.168.1.20	203.0.113.20	inside-portal			ssl	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
10	3/8/2018 22:51	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside			dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
11	3/8/2018 22:51	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside			dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
12	3/8/2018 22:51	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside			dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
13	3/8/2018 22:51	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside	lab\lab-user-id		dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
14	3/8/2018 22:51	192.168.1.20	203.0.113.20	192.168.1.20	203.0.113.20	inside-portal			ssl	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
15	3/8/2018 22:51	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside	lab\lab-user-id		dns	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
16	3/8/2018 22:51	192.168.1.20	13.107.4.52	203.0.113.20	13.107.4.52	egress-outside			web-browsing	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
17	3/8/2018 22:51	192.168.1.20	172.217.14.174	203.0.113.20	172.217.14.174	egress-outside			google-base	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20
18	3/8/2018 22:51	192.168.1.20	17.253.3.203	203.0.113.20	17.253.3.203	egress-outside			web-browsing	vsys1	inside	outside	ethernet1/2	ethernet1/1		3/8/20

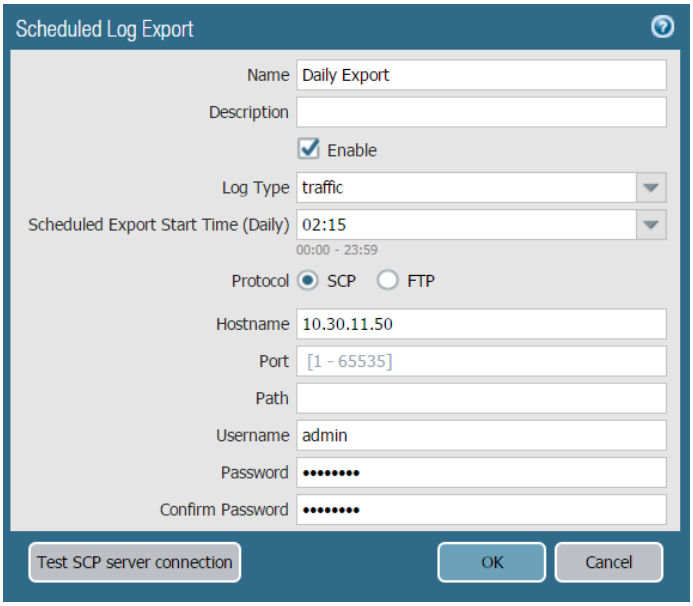
To export the current log listing in CSV format, select the **Export to CSV** icon. By default, export of the log listing to CSV format generates a CSV report with up to 65,535 rows of logs.

To change the limit of the number of rows displayed in CSV reports, use the **Max Rows in CSV Export** field on the **Log Export and Reporting** subtab. (Select **Device** > **Setup** > **Management** > **Logging and Reporting Settings**.)

Scheduled Log Export

- Schedule daily export of any of the logs to an FTP or Secure Copy (SCP) server in CSV format
- Traffic, Threat, URL, Data Filtering, HIP Match, and WildFire logs can be exported.

Device > Scheduled Log Export

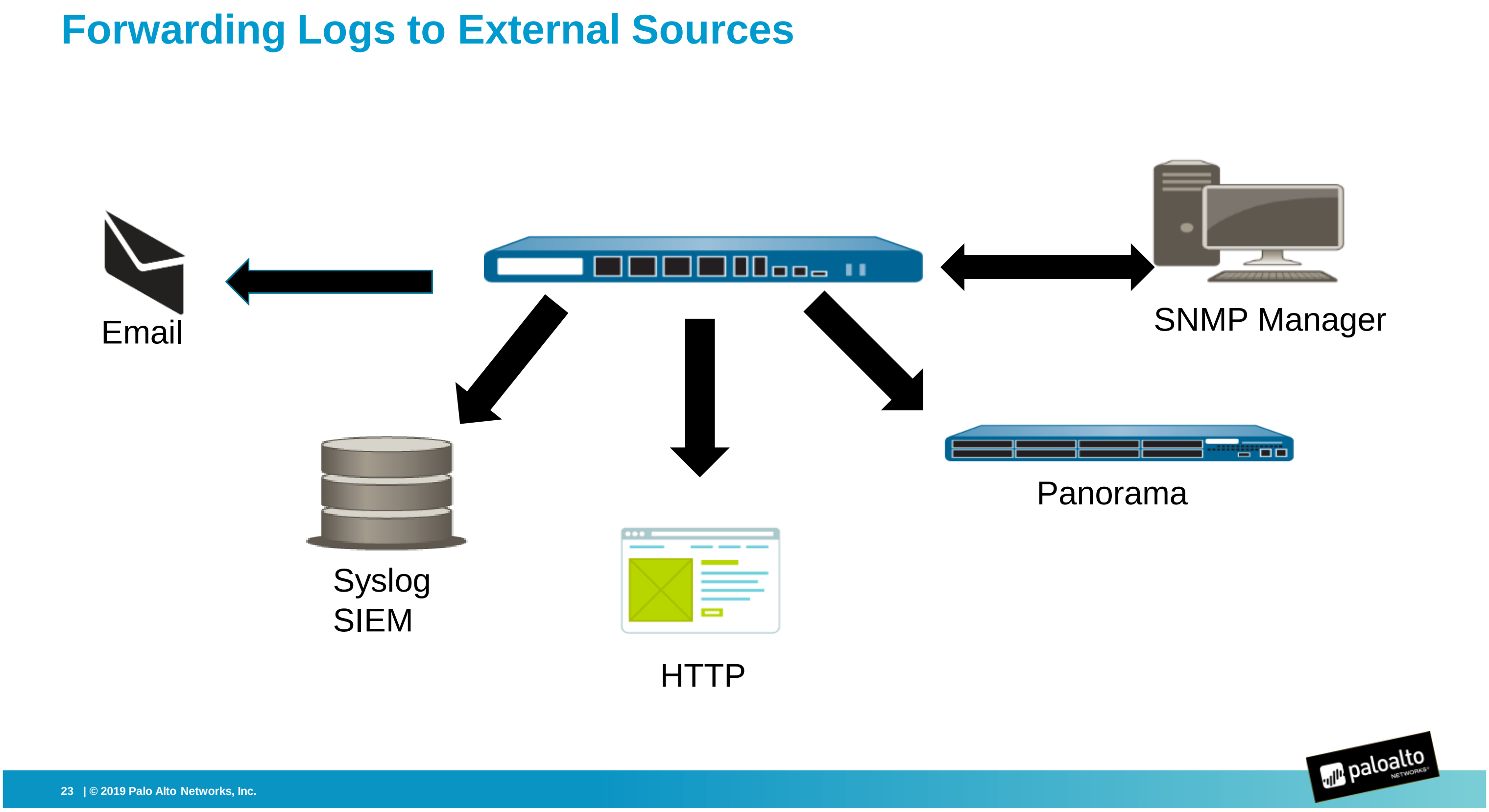


Scheduled Log Export

Name	Daily Export
Description	
	☑ Enable
Log Type	traffic
Scheduled Export Start Time (Daily)	02:15 00:00 - 23:59
Protocol	● SCP ○ FTP
Hostname	10.30.11.50
Port	[1 - 65535]
Path	
Username	admin
Password	••••••••
Confirm Password	••••••••

After the first export, the system exports only logs collected since the last export.

The log file will include only logs of the last calendar day.



Forwarding Logs to External Sources

23 | © 2019 Palo Alto Networks, Inc.

The firewall provides logs that record configuration changes, system events, security threats, and traffic flows. Logs can be forwarded to a Panorama management appliance, which then can generate SNMP traps or syslog messages, and send email notifications.

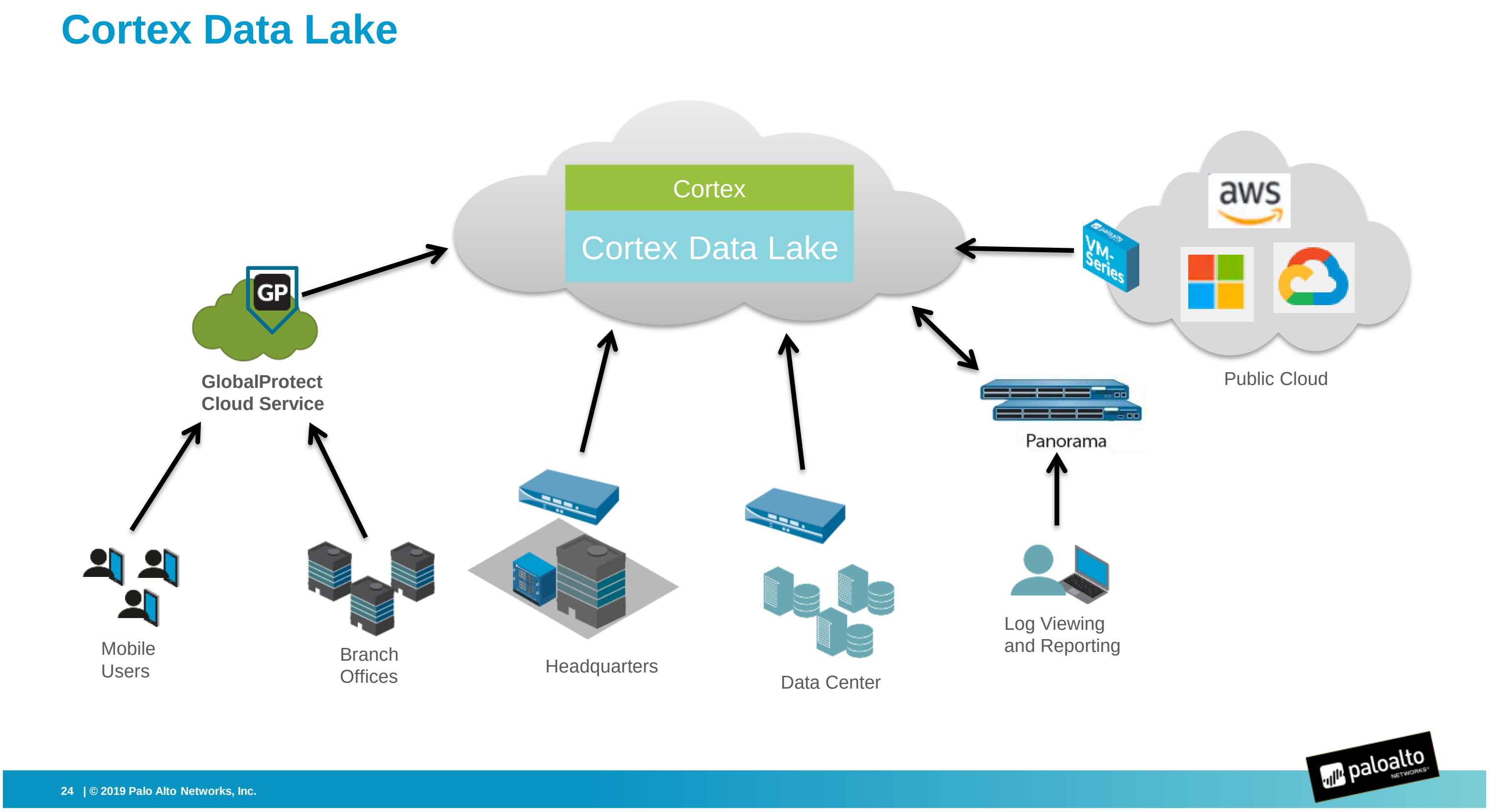
The firewall also can forward logs using HTTP/HTTPS. This capability allows the firewall to integrate with external systems that provide an HTTP-based API and to trigger automated actions when a specific event occurs on the firewall.

Logs most commonly are sent to Panorama or to an external syslog server for long-term storage and analysis.

Panorama provides the ability to manage a distributed network of Palo Alto Networks firewalls from a centralized location where you can:

- View of all your firewall traffic
- Manage all aspects of device configuration
- Push global policies
- Generate reports about traffic patterns or security incidents

Panorama is available as either a dedicated management appliance known as the M-100 or M-500, or as a virtual machine. When the M-100 appliance is used as a Log Collector, its maximum storage capacity is 8 terabytes. The M-500 appliance supports 24 terabytes.



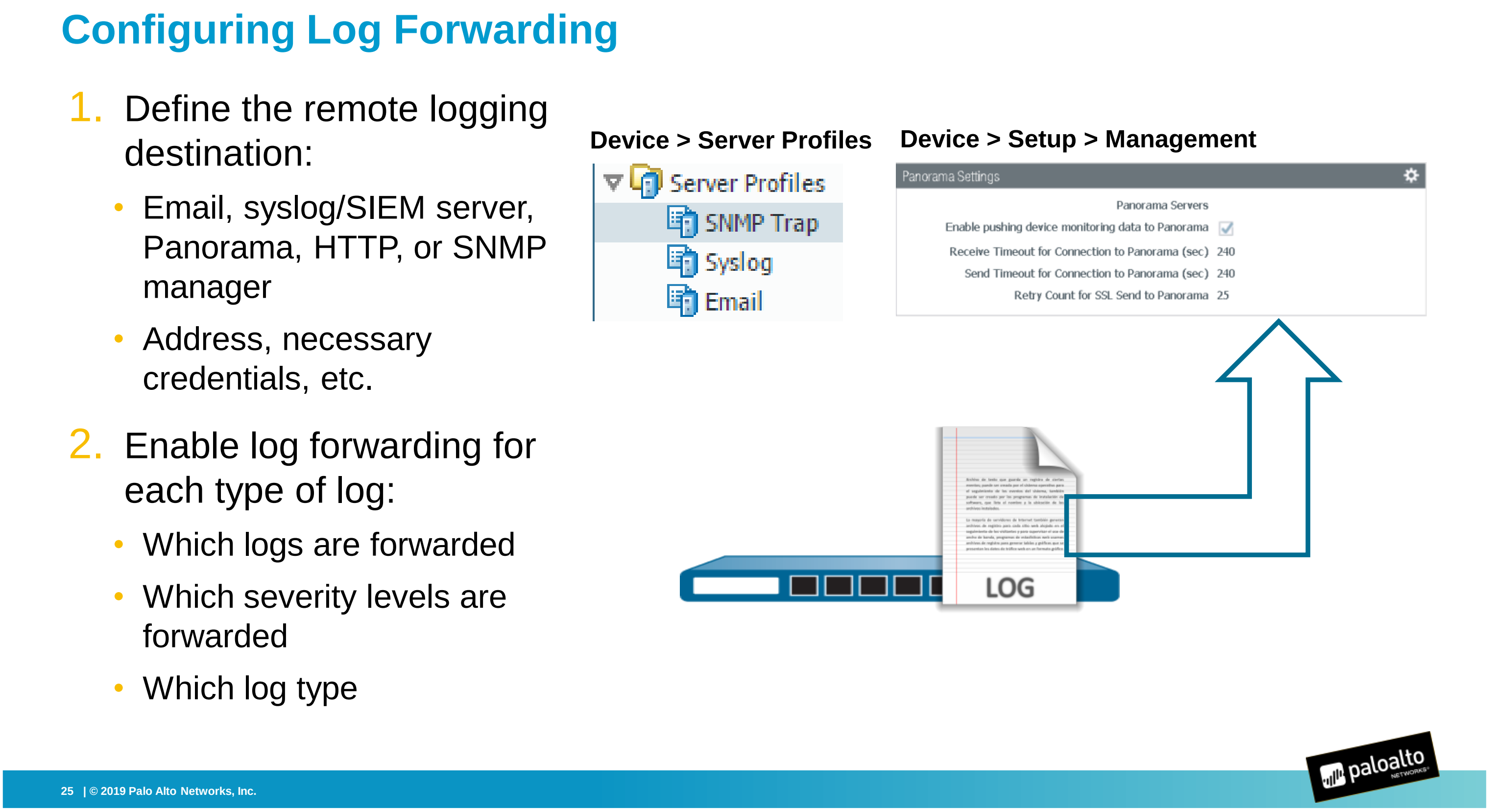
Cortex Data Lake

24 | © 2019 Palo Alto Networks, Inc.

Cortex Data Lake, formerly known as the Logging Service, provides cloud-based, centralized log storage and aggregation for your on-premises, virtual, private cloud, and public cloud firewalls, and for GlobalProtect cloud service. Panorama provides the interface for the logs stored in Cortex Data Lake. From Panorama, you can see an aggregated view of all logs and you can generate reports and perform log analysis and forensics on the logged data.

Cortex Data Lake provides data isolation to isolate your data from other customers, thereby avoiding cross-contamination of your logged data. Data redundancy is maintained through storage of multiple copies of your log database to ensure access to your logs when needed. Current Cortex Data Lake facilities are in two geographical regions: North America and Europe. Locations will be added over time. You can configure the location to forward your log data for storage.

Cortex Data Lake provides a solution for log collection that is the central repository of all logs generated from all services and firewalls. Cortex Data Lake unlocks the power of artificial intelligence for cybersecurity with services built to collect and store all your data combined with artifacts from a growing global community. The Cortex Data Lake service ingest logs and provides log forwarding to third parties. It offers flexible options to expand storage and log ingestion rates on demand without requiring you to purchase new hardware or to manually provision a new virtual machine.



Configuring Log Forwarding

1. Define the remote logging destination:
   - Email, syslog/SIEM server, Panorama, HTTP, or SNMP manager
   - Address, necessary credentials, etc.
2. Enable log forwarding for each type of log:
   - Which logs are forwarded
   - Which severity levels are forwarded
   - Which log type

Device > Server Profiles

- Server Profiles
  - SNMP Trap
  - Syslog
  - Email

Device > Setup > Management

Panorama Settings

Panorama Servers

Enable pushing device monitoring data to Panorama	☑
Receive Timeout for Connection to Panorama (sec)	240
Send Timeout for Connection to Panorama (sec)	240
Retry Count for SSL Send to Panorama	25

Depending on the type and severity of the data in the log files, you may want to be alerted to critical events that require attention, or have policies that require the archival of the data for longer than it can be stored on the firewall. In these cases, you want to forward the log data to an external service for archive, notification, and/or analysis.

To forward log data to an external service, complete these tasks:

1. Configure the firewall to access the remote services that will be receiving the logs
2. Configure each log type for forwarding

Define the Server Profiles for SNMP trap repositories, syslog servers, and email servers on **Device** > **Server Profiles**.

Define the address of the Panorama management appliance on **Device** > **Setup** > **Management**.

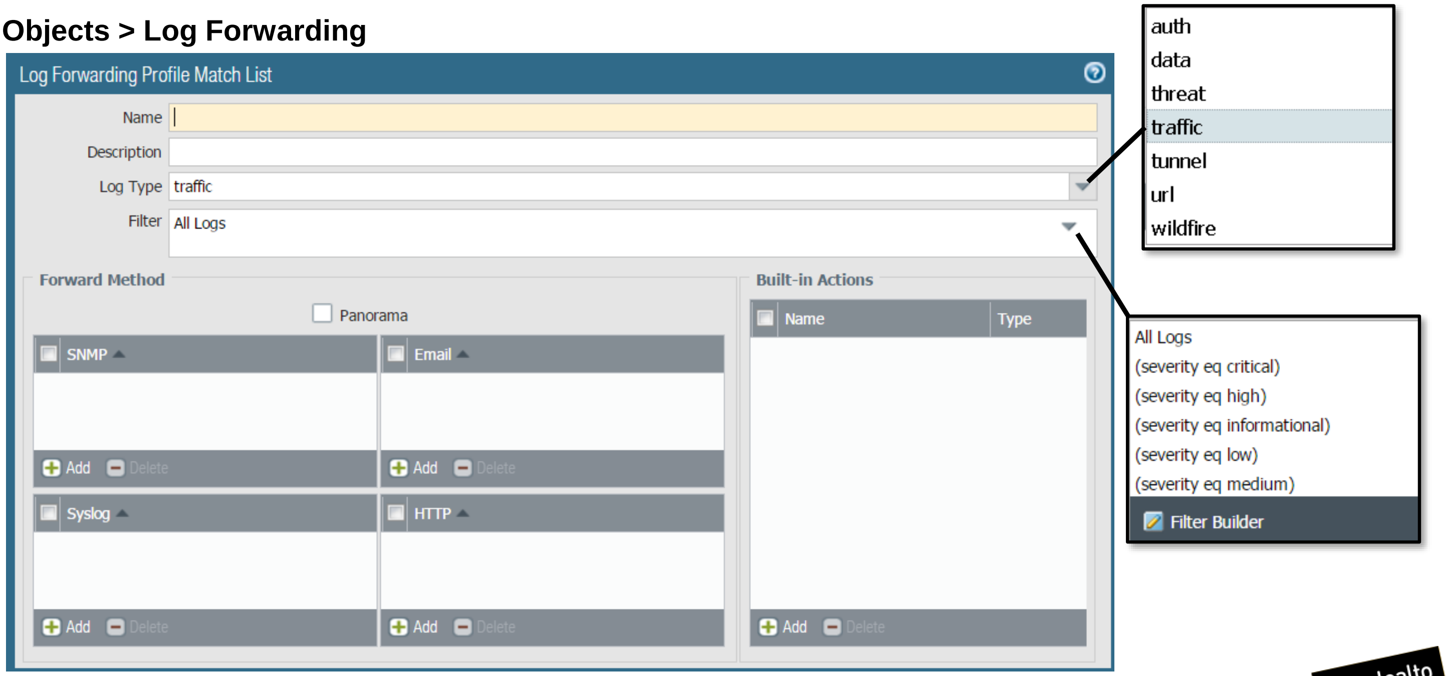
For System, Configuration, User-ID, and HIP Match logs, go to **Device** > **Log Settings** and select (or create additional) Server Profiles.

System messages about the firewall itself are visible in the system logs:

- Often system issues arise because of changes made to the device configuration.
- Specific information about configuration events is logged in a separate configuration log for ease of troubleshooting.
- The system and configuration logs are good candidates for alerts over email or SNMP.
- Email and SNMP traps make the most sense for critical and high-severity events that may require immediate attention or notification.
- Events captured by these logs include failed login attempts and configuration commits.

Selective Log Forwarding: Filtering

Objects > Log Forwarding



Log Forwarding Profile Match List

Name:

Description:

Log Type: traffic

Filter: All Logs

Log Forwarding objects are defined in **Objects** > **Log Forwarding**:

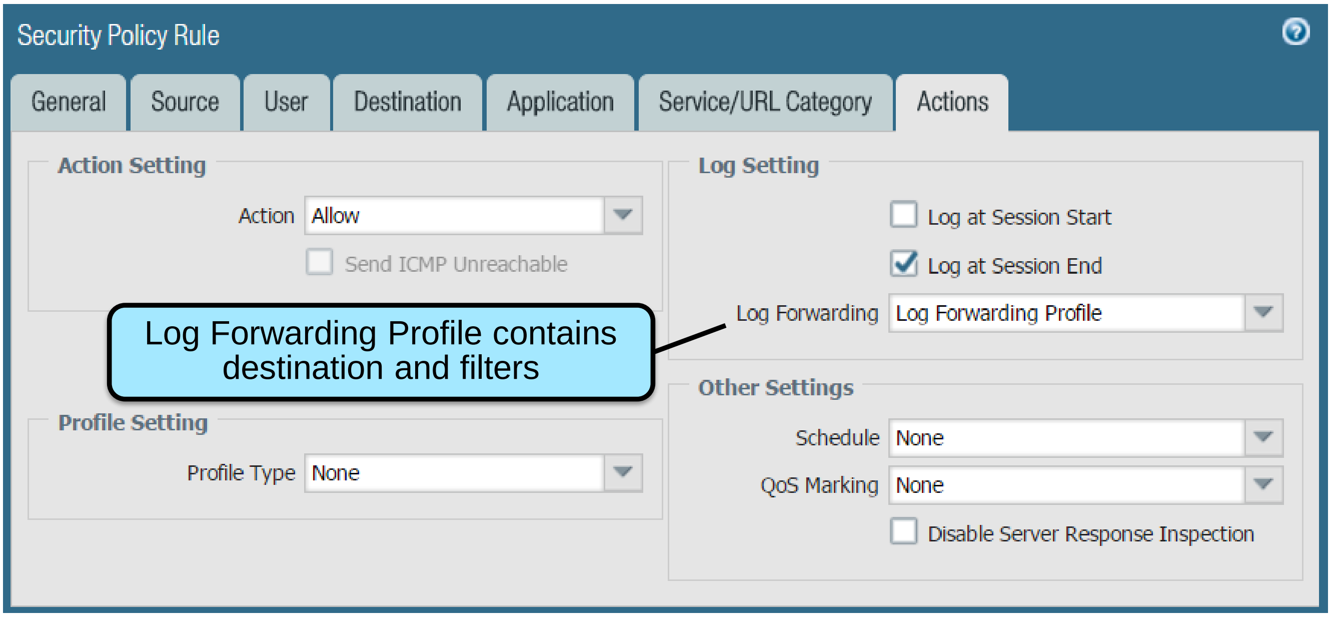
- The Log Forwarding object defines which Server Profile to use for each external service that will receive log information. The Log Forwarding profile defines the destination for each log type. The Log Forwarding profile is then used as part of your configuration in your policy rules and network zones.
- These objects are defined separately for Traffic, Threat, WildFire, URL, Data, GTP, Tunnel, and Authentication logs.

You can filter the logs that are to be forwarded in two primary ways:

- By **Severity**: Categories are predefined on a per-log entry basis.
- By **Query Filter**: The same logic is used as that used to filter log entries in the **Monitor** tab.

Applying Log Forwarding in a Security Policy Rule

Policies > Security



Security Policy Rule

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: Log Forwarding Profile

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Log Forwarding Profile contains destination and filters

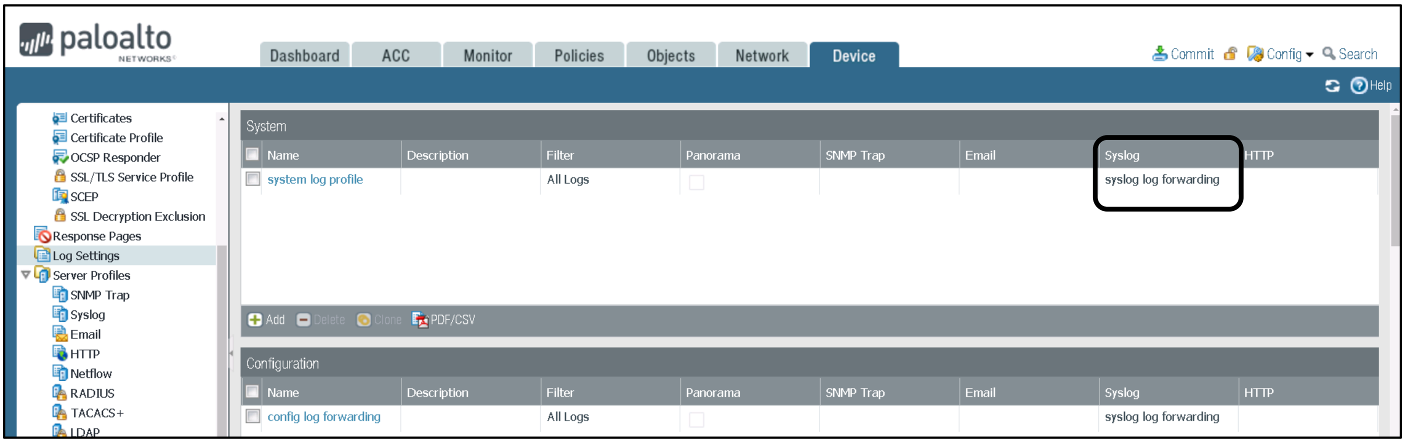
Each Security policy can specify a Log Forwarding Profile that determines whether Traffic log entries are logged remotely with the Panorama management appliance and/or sent as SNMP traps, syslog messages, or email notifications.

Different Log Forwarding Profiles can be applied to different Security policy rules.

By default, only local logging is performed.

Log Forwarding Example: Syslog

Device > Log Settings



System

□	Name	Description	Filter	Panorama	SNMP Trap	Email	Syslog	HTTP
□	system log profile		All Logs	□			syslog log forwarding	

Configuration

□	Name	Description	Filter	Panorama	SNMP Trap	Email	Syslog	HTTP
□	config log forwarding		All Logs	□			syslog log forwarding	

- Specific profiles are then applied to a Security policy rule.

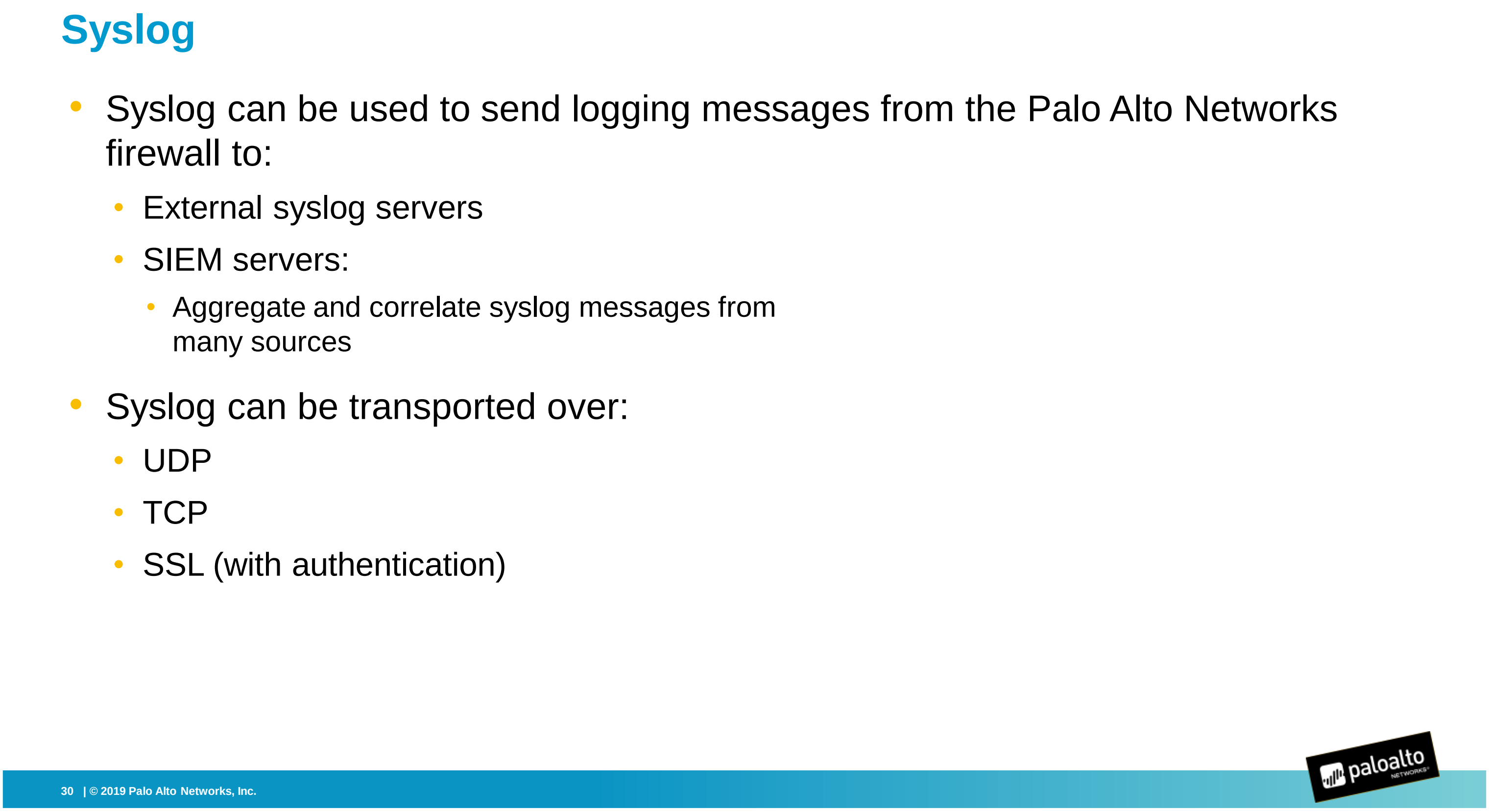
Log Forwarding Profiles are consolidated on the **Device** > **Log Settings** page. This page provides a single view of all the Log Forwarding Profiles. These profiles are visible only to, and can be applied only to, the appropriate type of policy rule.

Dashboard, ACC, and monitor

Log forwarding

Syslog

Configuring SNMP



Syslog

- Syslog can be used to send logging messages from the Palo Alto Networks firewall to:
  - External syslog servers
  - SIEM servers:
    - Aggregate and correlate syslog messages from many sources
- Syslog can be transported over:
  - UDP
  - TCP
  - SSL (with authentication)

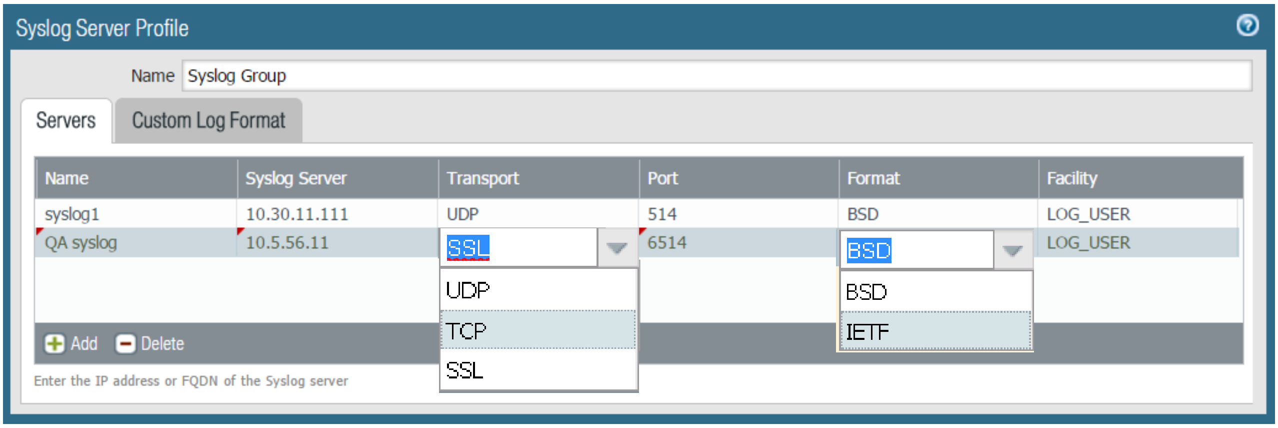
Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices such as routers, firewalls, and printers from different vendors into a central repository for archive, analysis, and reporting.

Syslog log forwarding can be used to forward logs to a SIEM, or System Information and Event Manager. Many SIEM vendors and models are compatible with PAN-OS software. To determine if your SIEM is compatible, see the list of Palo Alto Networks technology partners to learn if your SIEM vendor is among them. The list of technology partners is at https://www.paloaltonetworks.com/partners/alliance.

Creating a Syslog Server Profile

- UDP and TCP default port 514
- SSL default port 6514

Device > Server Profiles > Syslog



Syslog Server Profile

Name: Syslog Group

Name	Syslog Server	Transport	Port	Format	Facility
syslog1	10.30.11.111	UDP	514	BSD	LOG_USER
QA syslog	10.5.56.11	SSL	6514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

To generate syslog messages for System, Configuration, Traffic, Threat, or HIP Match logs, specify one or more syslog servers with a Server Profile. After you define the Syslog Profiles, the profiles can then be used for System and Configuration log entries:

- **Syslog Server**: Enter the IP address of the syslog server.
- **Transport**: Select whether to transport the syslog messages over UDP, TCP, or SSL.
- **Port**: Enter the port number of the syslog server. (The standard port for UDP and TCP is 514; the standard port for SSL is 6514.)
- **Format**: Specify the syslog format to use: **BSD** (the default) or **IETF**.
- **Facility**: Choose a level from the drop-down list.

For additional information, see the document *PAN-OS Syslog Integration* at https://live.paloaltonetworks.com/t5/Documentation-Articles/PAN-OS-Syslog-Integration/ta-p/55323.

Compared to traditional syslog over UDP, syslog over TCP and SSL is a more secure method of transferring valuable syslog messages.

Before PAN-OS 6.0, syslog messages were sent over UDP transport only. This method of transfer is not as reliable or secure as with TCP and SSL.

Certain customer deployments have syslog messages relayed to centralized servers that may be sent over unreliable or unsecure links.

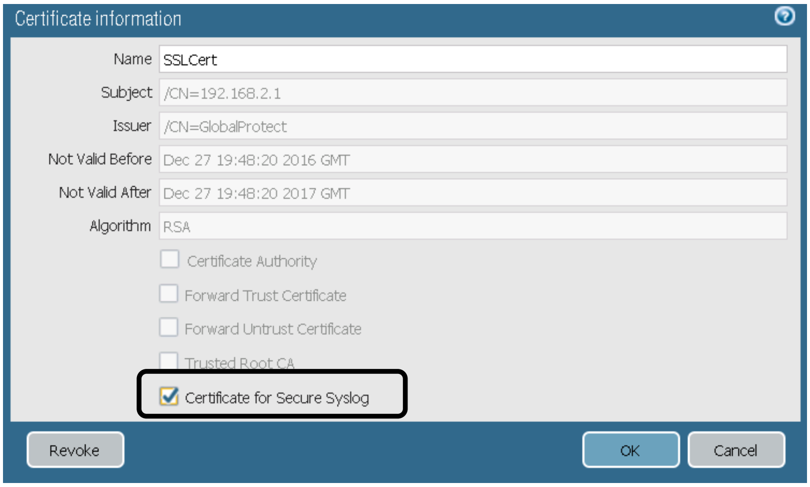
Transport syslogs over TCP and SSL provide for more reliable and secure transport.

TCP has more overhead and expense in overall performance than UDP, but the impact probably will not be detrimental to the overall performance of the network and environment. TCP has less overhead and cost than does SSL.

Using SSL for Syslog

- Local certificate required for syslog server client authentication
- Private key must be available
- Cannot be stored on a hardware security module (HSM)

Device > Certificate Management > Certificates



Certificate information

Name: SSLCert

Subject: /CN=192.168.2.1

Issuer: /CN=GlobalProtect

Not Valid Before: Dec 27 19:48:20 2016 GMT

Not Valid After: Dec 27 19:48:20 2017 GMT

Algorithm: RSA

□ Certificate Authority

□ Forward Trust Certificate

□ Forward Untrust Certificate

□ Trusted Root CA

☑ Certificate for Secure Syslog

If the syslog server uses client authentication, a local certificate is required.

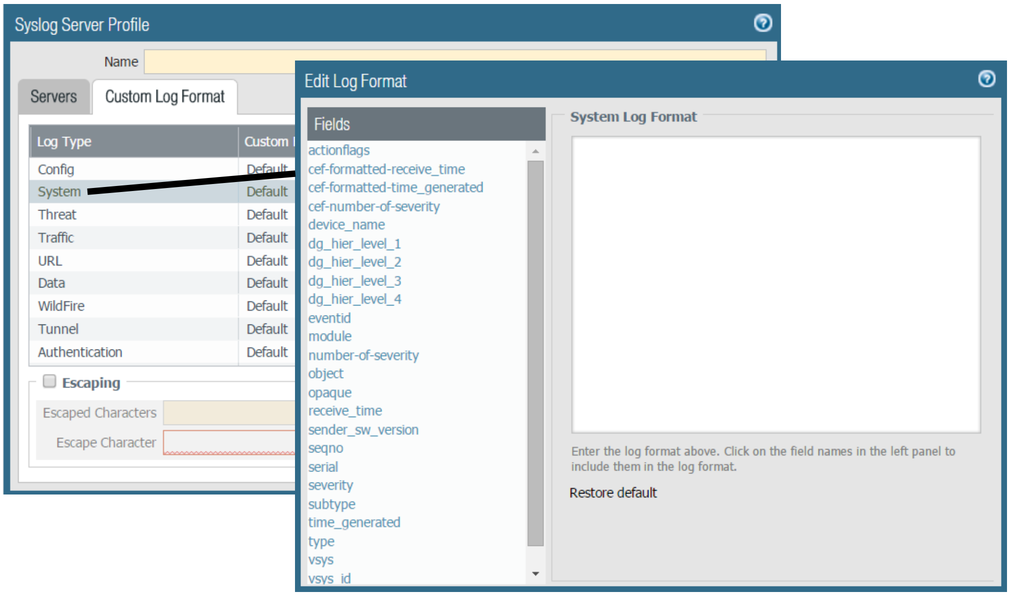
The private key must be available and cannot be stored on an HSM.

To get a certificate:

- Import a certificate into the Palo Alto Networks firewall:
  - Purchase a certificate created by a trusted certificate authority, or CA
  - Generate a certificate signing request to give the CA on the Palo Alto Networks firewall
  - Create a certificate by using Active Directory or some other facility with your own CA certificate
- Create a self-signed certificate on the Palo Alto Networks firewall:
  - Create a CA root certificate on the Palo Alto Networks firewall
  - Create a certificate signed by that CA root certificate

Syslog Custom Log Format

Device > Server Profiles > Syslog



Syslog Server Profile

Name

Servers | Custom Log Format

Log Type	Custom
Config	Default
System	Default
Threat	Default
Traffic	Default
URL	Default
Data	Default
WildFire	Default
Tunnel	Default
Authentication	Default

□ Escaping

Escaped Characters

Escape Character

Edit Log Format

Fields

actionflags
cef-formatted-receive_time
cef-formatted-time_generated
cef-number-of-severity
device_name
dg_hier_level_1
dg_hier_level_2
dg_hier_level_3
dg_hier_level_4
eventid
module
number-of-severity
object
opaque
receive_time
sender_sw_version
seqno
serial
severity
subtype
time_generated
type
vsys
vsys_id

System Log Format

Enter the log format above. Click on the field names in the left panel to include them in the log format.

Restore default

- Customize the format of the syslog messages to work with specific syslog or SIEM servers

Dashboard, ACC, and monitor

Log forwarding

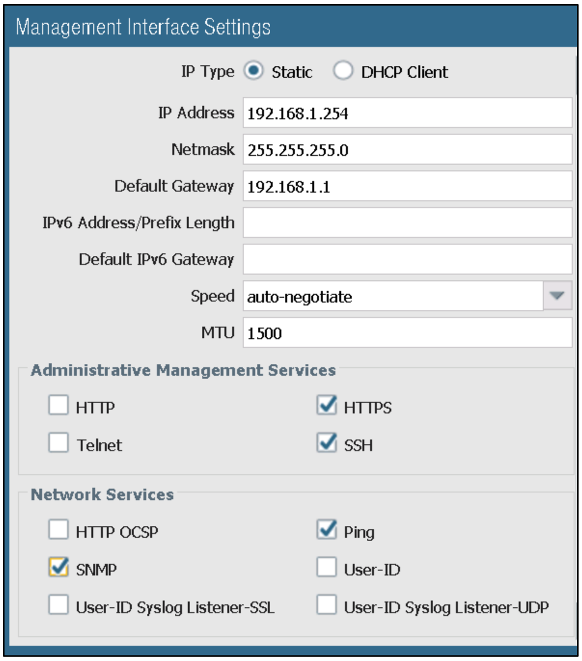
Syslog

Configuring SNMP

SNMP Monitoring Overview

- Enable inbound SNMP on the MGT interface
- Load PAN-OS MIBs into the SNMP Manager

Device > Setup > Interfaces > Management



Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address	192.168.1.254
Netmask	255.255.255.0
Default Gateway	192.168.1.1
IPv6 Address/Prefix Length	
Default IPv6 Gateway	
Speed	auto-negotiate
MTU	1500

Administrative Management Services

□ HTTP	☑ HTTPS
□ Telnet	☑ SSH

Network Services

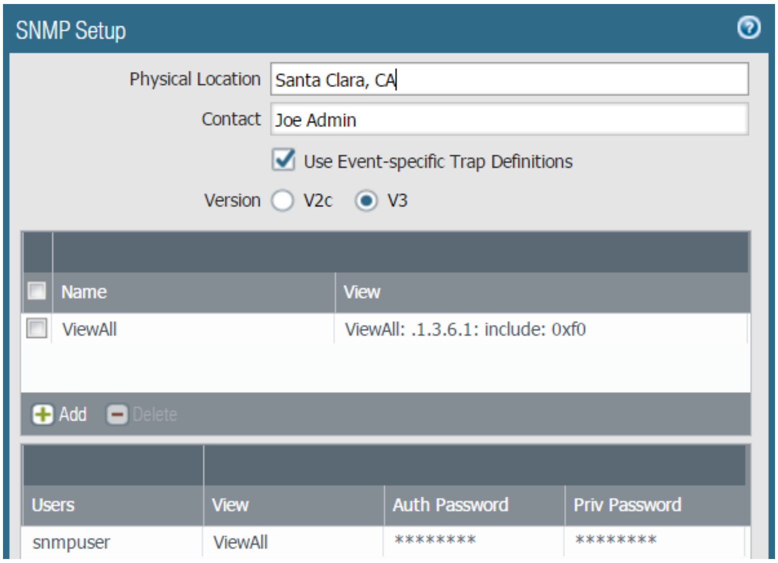
□ HTTP OCSP	☑ Ping
☑ SNMP	□ User-ID
□ User-ID Syslog Listener-SSL	□ User-ID Syslog Listener-UDP

If the SNMP Manager is on a non-MGT interface, allow SNMP on the Interface Management Profile for that interface. Also create a service route for SNMP to use that interface.

Configuring SNMP Settings

- View:
  - Enter an OID and a mask to determine which parts of the MIB can be seen
- Users:
  - Select View for user
  - Username, Auth Password, and Priv Password should match in SNMP Manager

Device > Setup > Operations > Miscellaneous > SNMP Setup



SNMP Setup

Physical Location: Santa Clara, CA

Contact: Joe Admin

☑ Use Event-specific Trap Definitions

Version ○ V2c ● V3

□	Name	View
□	ViewAll	ViewAll: .1.3.6.1: include: 0xf0

Users	View	Auth Password	Priv Password
snmpuser	ViewAll	********	********

For the **View** option, enter an OID and a mask to determine which parts of the MIB can be seen:

- OID .1.3.6.1 mask 0xf0 to see everything
- To see more information, use OID .1 mask 0x80.

For the **Users** view, select **View for User**:

- **Username**, **Auth Password**, and **Priv Password** should match in the SNMP manager:
  - Auth uses SHA

The **SNMP Community String** should match the **Community String** in the SNMP Manager.

Enterprise-specific MIBs can be downloaded from https://www.paloaltonetworks.com/documentation/misc/snmp-mibs.html.

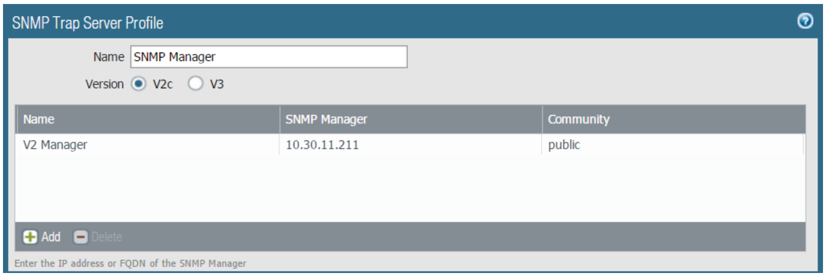
Note that for PAN-OS 7.0 and later, logical interfaces such as tunnels, aggregate groups, and vsys-specific subinterfaces also can be monitored using SNMP.

Also in PAN-OS 7.0 and later, global counters have been added to the PAN-COMMON-MIB.my MIB to track DoS-related events, IP fragmentation, TCP state, and packet drops.

Creating an SNMP Traps Server Profile

- SNMPv2:
  - Trap Repository Address
  - Community String
- SNMPv3:
  - Username
  - EngineID
  - Passwords

Device > Server Profiles > SNMP Trap



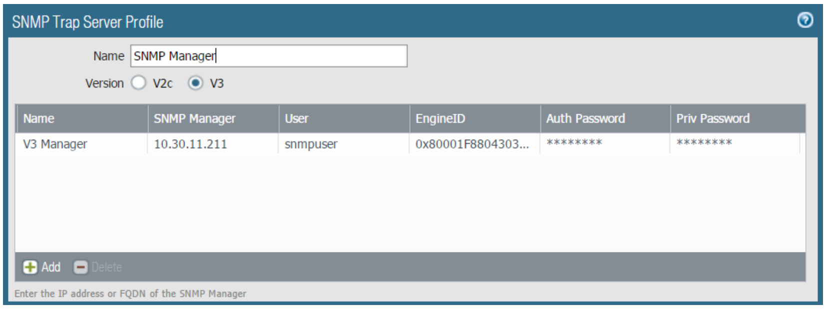
SNMP Trap Server Profile

Name: SNMP Manager

Version ● V2c ○ V3

Name	SNMP Manager	Community
V2 Manager	10.30.11.211	public

Enter the IP address or FQDN of the SNMP Manager



SNMP Trap Server Profile

Name: SNMP Manager

Version ○ V2c ● V3

Name	SNMP Manager	User	EngineID	Auth Password	Priv Password
V3 Manager	10.30.11.211	snmpuser	0x80001F8804303...	********	********

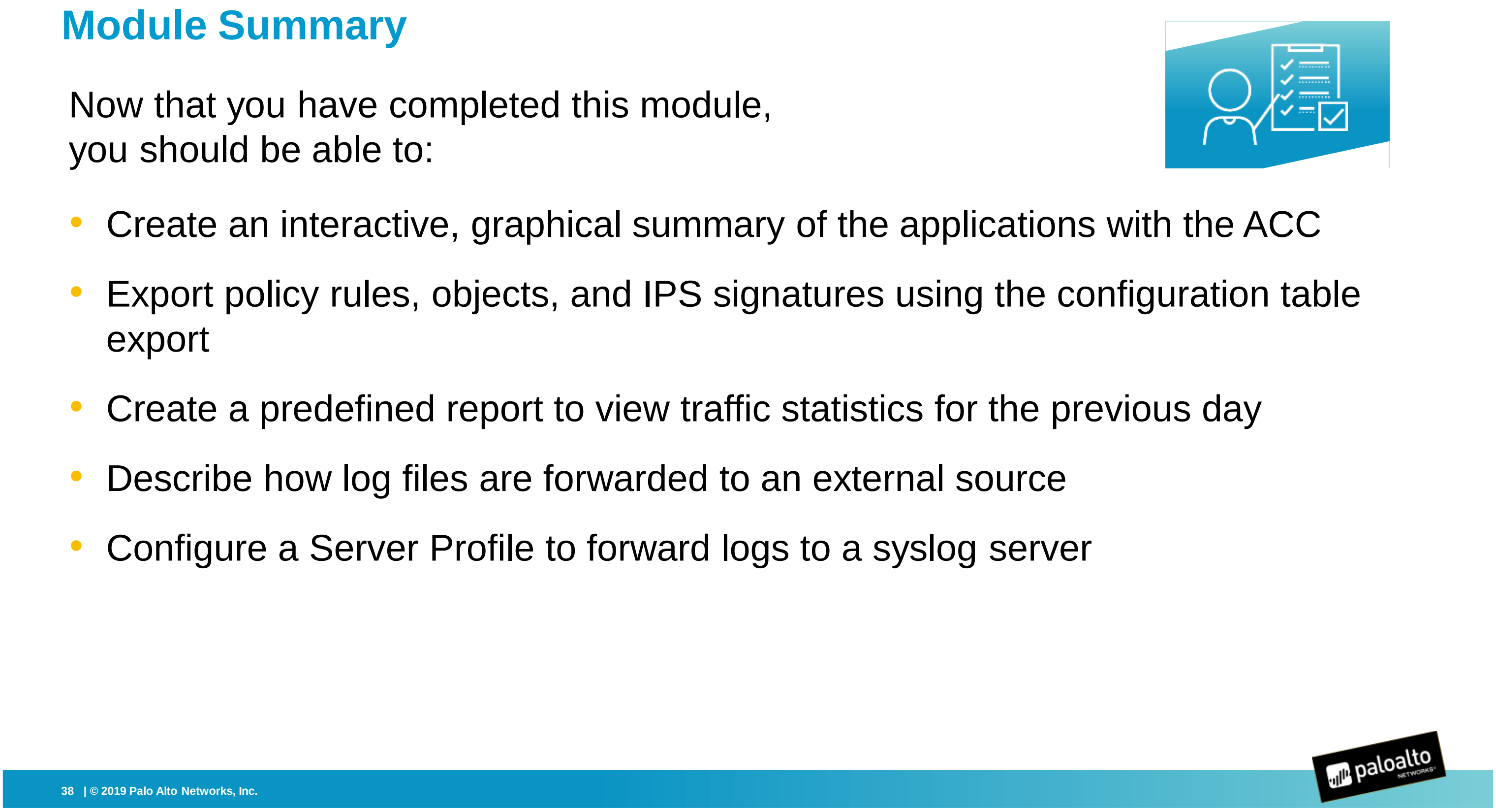
Enter the IP address or FQDN of the SNMP Manager

SNMPv2

- Trap Repository Address
- Community String

SNMPv3

- Username
- EngineID:
  - From SNMP GET OID 1.3.6.1.6.3.10.2.1.1.0
- Passwords:
  - Auth uses SHA
  - Privilege uses AES



Module Summary

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

- Create an interactive, graphical summary of the applications with the ACC
- Export policy rules, objects, and IPS signatures using the configuration table export
- Create a predefined report to view traffic statistics for the previous day
- Describe how log files are forwarded to an external source
- Configure a Server Profile to forward logs to a syslog server

38 | © 2019 Palo Alto Networks, Inc.

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

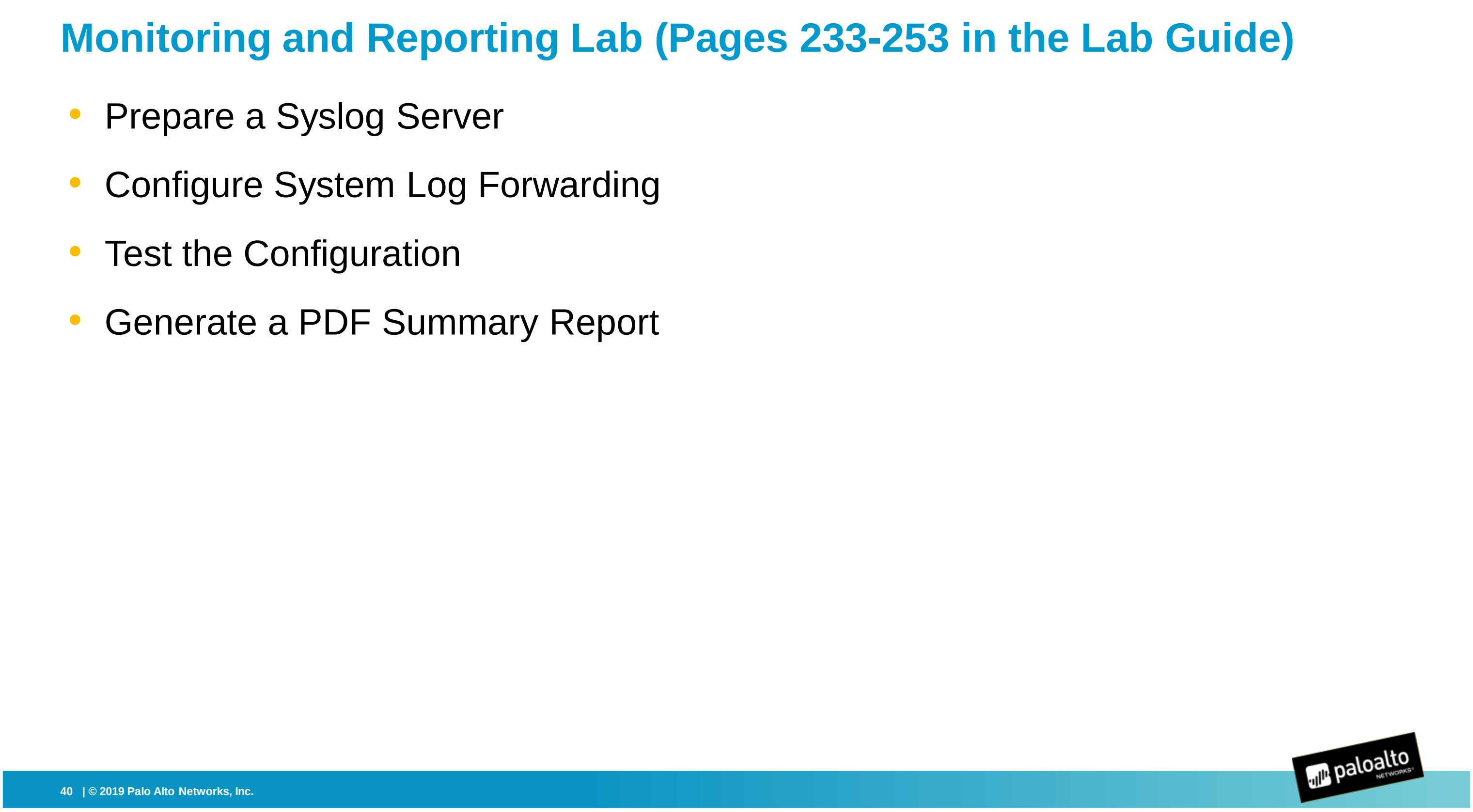
- Create an interactive, graphical summary of the applications with the ACC
- Export policy rules, objects, and IPS signatures using the configuration table export
- Create a predefined report to view traffic statistics for the previous day
- Describe how log files are forwarded to an external source
- Configure a Server Profile to forward logs to a syslog server

Questions?

39 | © 2019 Palo Alto Networks, Inc.

Review Questions

1. Logs can be forwarded to which four of the following Remote Logging Destinations? (Choose four.)
   a. Email
   b. Syslog
   c. Common access log
   d. Panorama
   e. SNMP
2. A log can be exported to which format?
   a. CSV
   b. PDF
   c. PPT
   d. XLS
3. True or false? A Report Group must be sent as a scheduled email. It cannot be downloaded directly.
   a. true
   b. false
4. A SaaS application that you formally approve for use on your network is which type of application?
   a. sanctioned
   b. production
   c. unsanctioned
   d. service



Monitoring and Reporting Lab (Pages 233-253 in the Lab Guide)

- Prepare a Syslog Server
- Configure System Log Forwarding
- Test the Configuration
- Generate a PDF Summary Report

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b, d, e
2. a
3. a (true)
4. a

This page intentionally left blank