PALO ALTO NETWORKS EDU-210

Lab 12: Monitoring and Reporting

Document Version: 2017-09-29

Contents

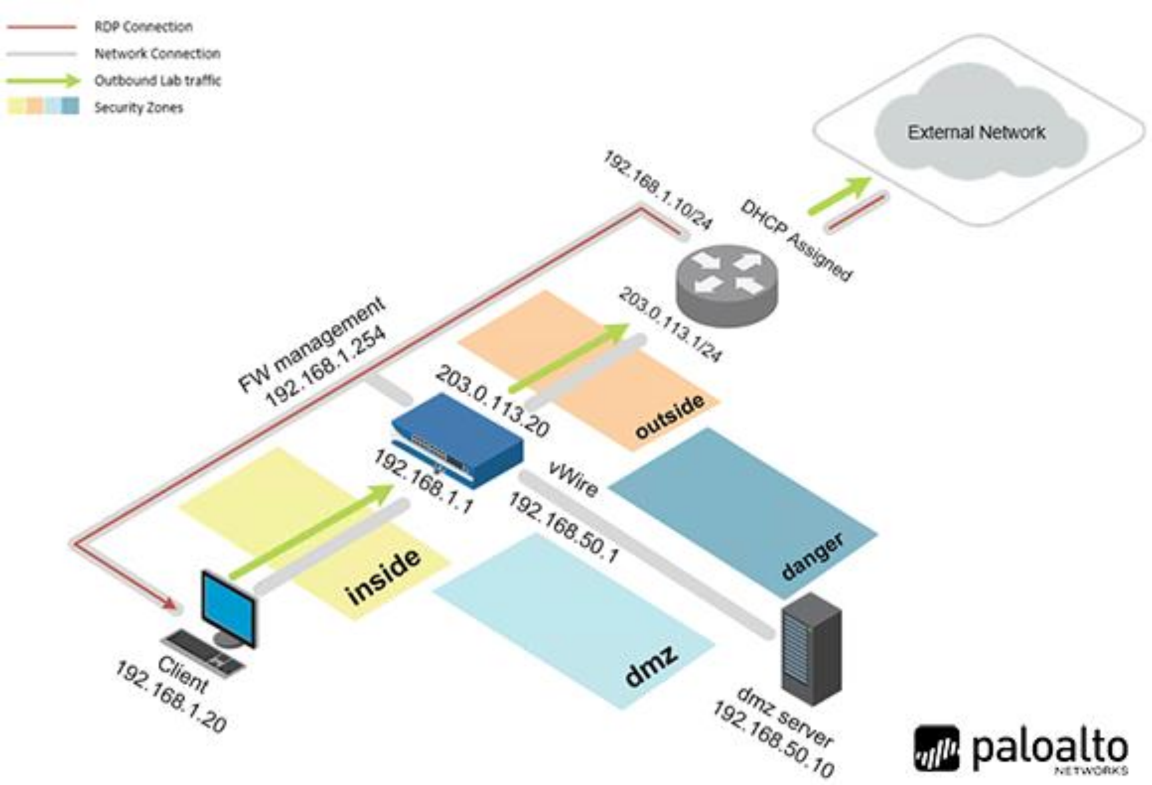
Introduction

Now that the firewalls are up and running we need to begin analyzing the data from these firewalls. The data will be coming from the different logs on the system. To effectively utilize this information we need to become familiar with the different logs and how to search that information.

Objectives

- Explore the Session Browser, App-Scope, and Application Command Center (ACC).
- Investigate traffic via the ACC and logs.
- Generate a User Activity report.
- Create a Custom report.
- Create a Report Group.
- Configure an email schedule.

Lab Topology



Lab Settings

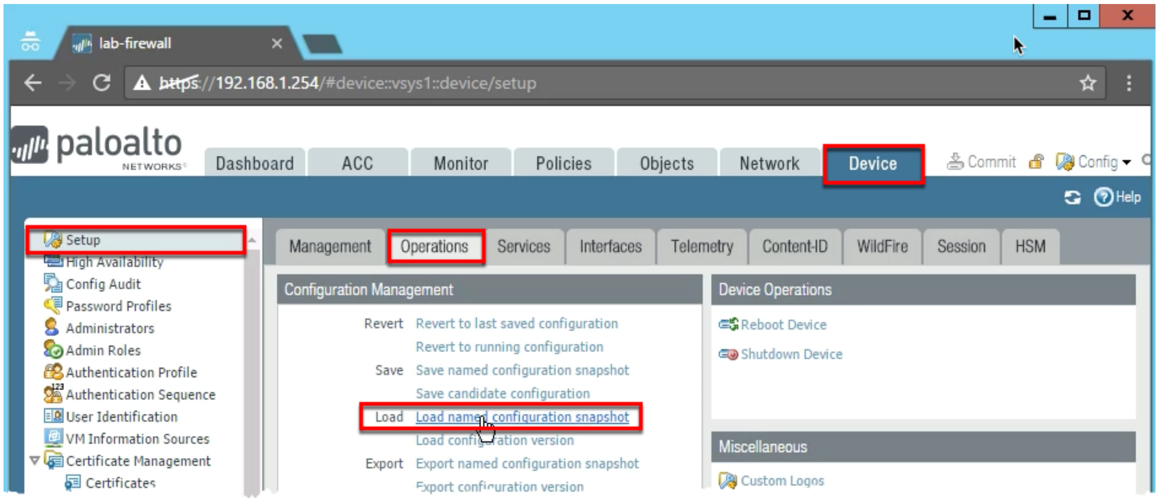
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

12 Lab: Interface Configuration

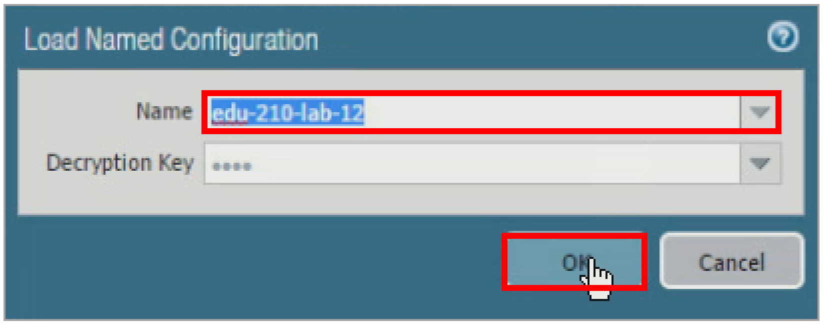
12.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



https://192.168.1.254/#device::vsys1::device/setup

3. Select **edu-210-lab-12** and click **OK**.



Load Named Configuration

Name: edu-210-lab-12

Decryption Key: ••••

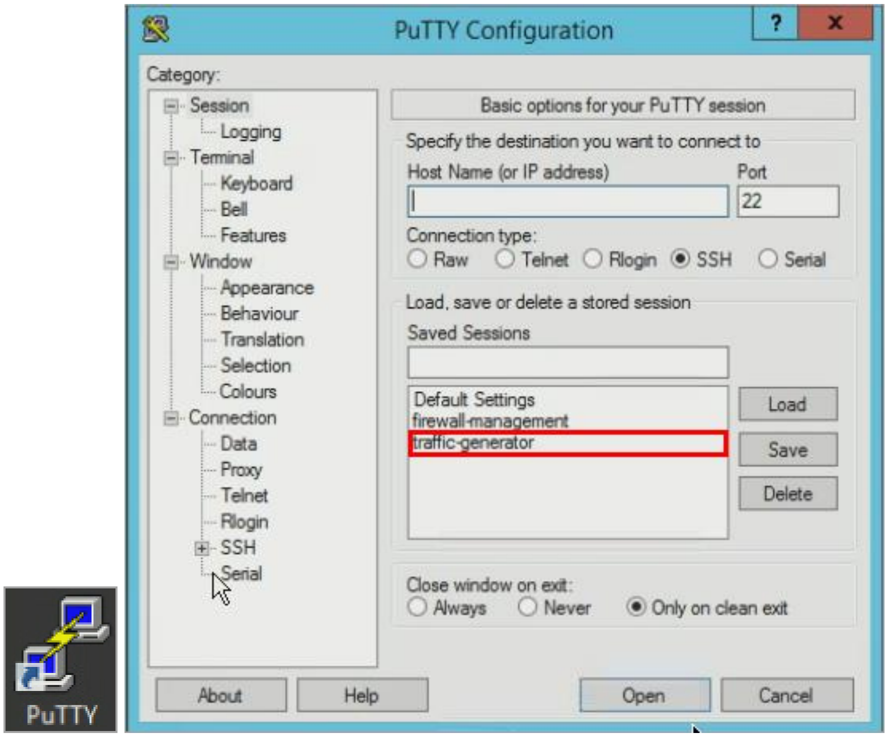
4. Click **Close**.
5. **Commit** all changes.

12.1 Generate Traffic

Pre-populate the firewall with log entries and usernames that you can observe and investigate in this lab.

The metrics displayed in the lab screenshots and the metrics displayed on your lab firewall might be different.

1. On the Windows desktop, open **PuTTY** then double-click **traffic-generator**.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

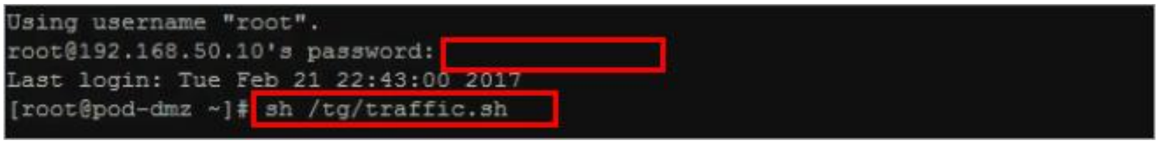
Default Settings
firewall-management
traffic-generator

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Enter the following information when prompted.

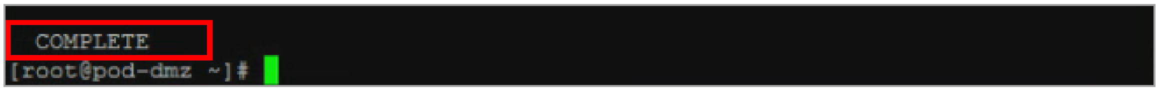
Parameter	Value
Password	`Pal0Alt0`

3. While in the PuTTY window, type the command sh /tg/traffic.sh.



```
Using username "root".
root@192.168.50.10's password:
Last login: Tue Feb 21 22:43:00 2017
[root@pod-dmz ~]# sh /tg/traffic.sh
```

After you execute the command, it can take up to 10 minutes to complete. Wait until it is finished before proceeding.



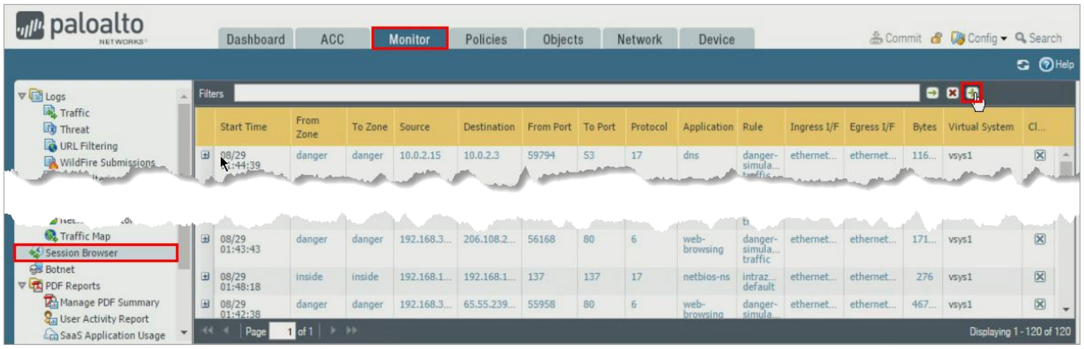
```
  COMPLETE
[root@pod-dmz ~]#
```

12.2 Explore the Session Browser

The Session Browser enables you to browse and filter current running sessions on the firewall.

1. Select **Monitor > Session Browser** then click the **Plus** icon at the top-right of the window to open the **Filters** pane.

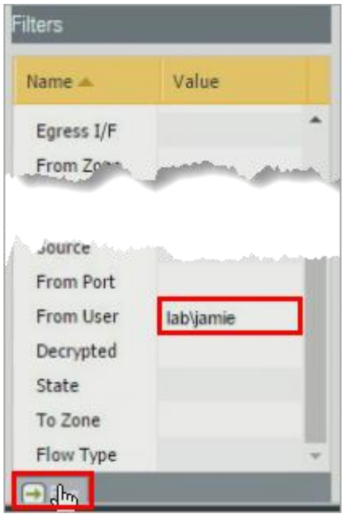
If you don't see the plus icon then the **Filters** pane may have presented itself automatically.



Start Time	From Zone	To Zone	Source	Destination	From Port	To Port	Protocol	Application	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System	Cl...
08/29 01:44:39	danger	danger	10.0.2.15	10.0.2.3	59794	53	17	dns	danger-simula...	ethernet...	ethernet...	116...	vsys1	☒
08/29 01:43:43	danger	danger	192.168.3...	206.108.2...	56168	80	6	web-browsing	danger-simula... traffic	ethernet...	ethernet...	171...	vsys1	☒
08/29 01:48:18	inside	inside	192.168.1...	192.168.1...	137	137	17	netbios-ns	intraz... default	ethernet...	ethernet...	276	vsys1	☒
08/29 01:42:38	danger	danger	192.168.3...	65.55.239...	55958	80	6	web-browsing	danger-simula...	ethernet...	ethernet...	467...	vsys1	☒

You might be able to see simulated sessions from the generated traffic. Notice that there is no Source User column.

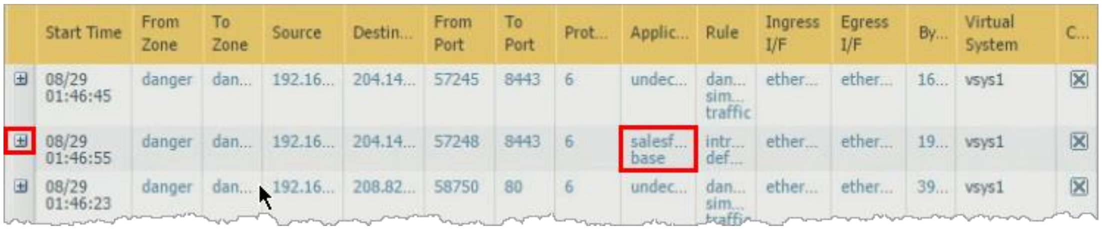
2. Type `lab\jamie` in the **From User** field then click **Run**.



Name	Value
Egress I/F	
From Zone	
Source	
From Port	
From User	lab\jamie
Decrypted	
State	
To Zone	
Flow Type	

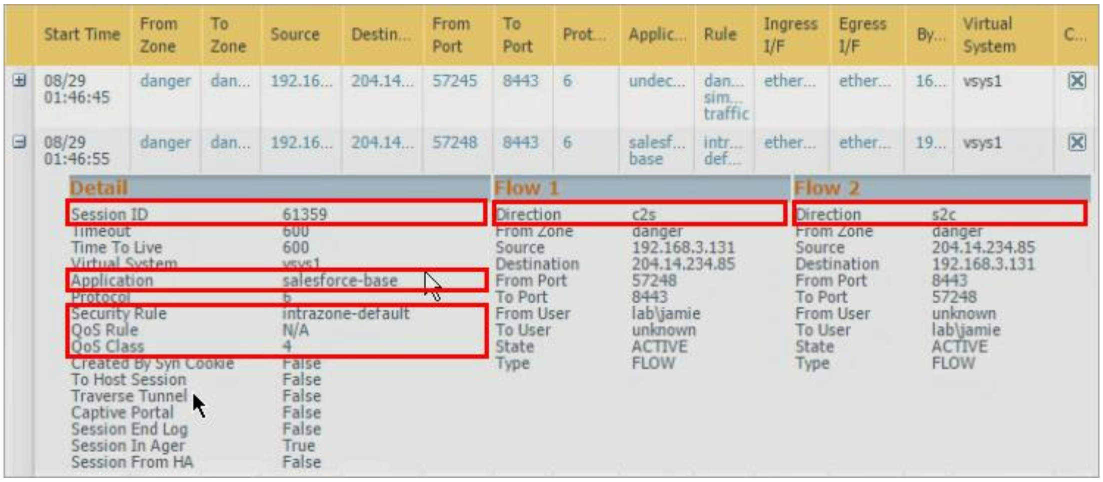
3. Notice that, even though there is not a Source User column, there is an ability to search for the **From User**. You can also search for **To User**.

4. Locate a **salesforce-base** entry and click the **Plus** icon on the left to expand the display.



	Start Time	From Zone	To Zone	Source	Destin...	From Port	To Port	Prot...	Applic...	Rule	Ingress I/F	Egress I/F	By...	Virtual System	C...
⊞	08/29 01:46:45	danger	dan...	192.16...	204.14...	57245	8443	6	undec...	dan... sim... traffic	ether...	ether...	16...	vsys1	☒
⊞	08/29 01:46:55	danger	dan...	192.16...	204.14...	57248	8443	6	salesf... base	intr... def...	ether...	ether...	19...	vsys1	☒
⊞	08/29 01:46:23	danger	dan...	192.16...	208.82...	58750	80	6	undec...	dan... sim... traffic	ether...	ether...	39...	vsys1	☒

5. Notice the three sections labeled **Detail**, **Flow 1**, and **Flow 2.**



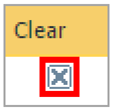
	Start Time	From Zone	To Zone	Source	Destin...	From Port	To Port	Prot...	Applic...	Rule	Ingress I/F	Egress I/F	By...	Virtual System	C...
⊞	08/29 01:46:45	danger	dan...	192.16...	204.14...	57245	8443	6	undec...	dan... sim... traffic	ether...	ether...	16...	vsys1	☒
⊟	08/29 01:46:55	danger	dan...	192.16...	204.14...	57248	8443	6	salesf... base	intr... def...	ether...	ether...	19...	vsys1	☒

Detail		Flow 1		Flow 2	
Session ID	61359	Direction	c2s	Direction	s2c
Timeout	600	From Zone	danger	From Zone	danger
Time To Live	600	Source	192.168.3.131	Source	204.14.234.85
Virtual System	vsys1	Destination	204.14.234.85	Destination	192.168.3.131
Application	salesforce-base	From Port	57248	From Port	8443
Protocol	6	To Port	8443	To Port	57248
Security Rule	intrazone-default	From User	lab\jamie	From User	unknown
QoS Rule	N/A	To User	unknown	To User	lab\jamie
QoS Class	4	State	ACTIVE	State	ACTIVE
Created By Syn Cookie	False	Type	FLOW	Type	FLOW
To Host Session	False				
Traverse Tunnel	False				
Captive Portal	False				
Session End Log	False				
Session In Ager	True				
Session From HA	False				

In the Detail section, you can see various items of information. Important items that can help when troubleshooting are **Session ID**, **Application**, **Security Rule**, **QoS Rule**, and **Class**.

Notice under **Flow 1** the direction **c2s** (Client to Server) and under **Flow 2** the direction **s2c** (Server to Client). These flows provide information about both the request and response traffic.

6. You can end an active session by clicking the **X** icon at the far right of a session row.



12.3 Explore App-Scope

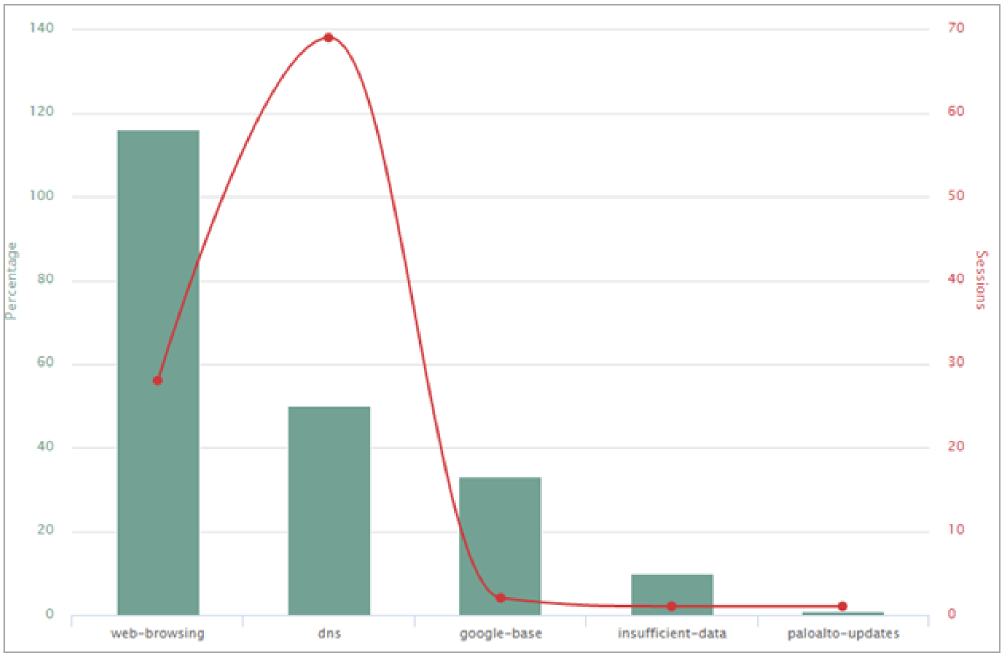
With the App-Scope reports, you can quickly see if any behavior is unusual or unexpected, which helps identify problematic behavior. Each report provides a dynamic, user-customizable window into the network. Long-term trends are difficult to represent in a lab environment. However, knowing where to look is key to finding potential issues.

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

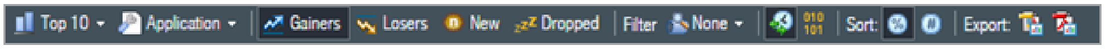
   The Summary report displays charts for the top five gainers, losers, and bandwidth-consuming applications, application categories, users, and sources.

2. Select **Monitor > App Scope > Change Monitor**.

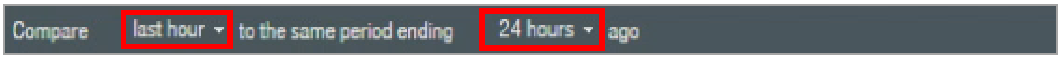
   The Change Monitor report displays changes over a specified time period. For example, the following figure displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and are sorted by percentage.



3. The type of information displayed can be controlled at the top. The displayed Graph can be exported as a PDF or PNG.



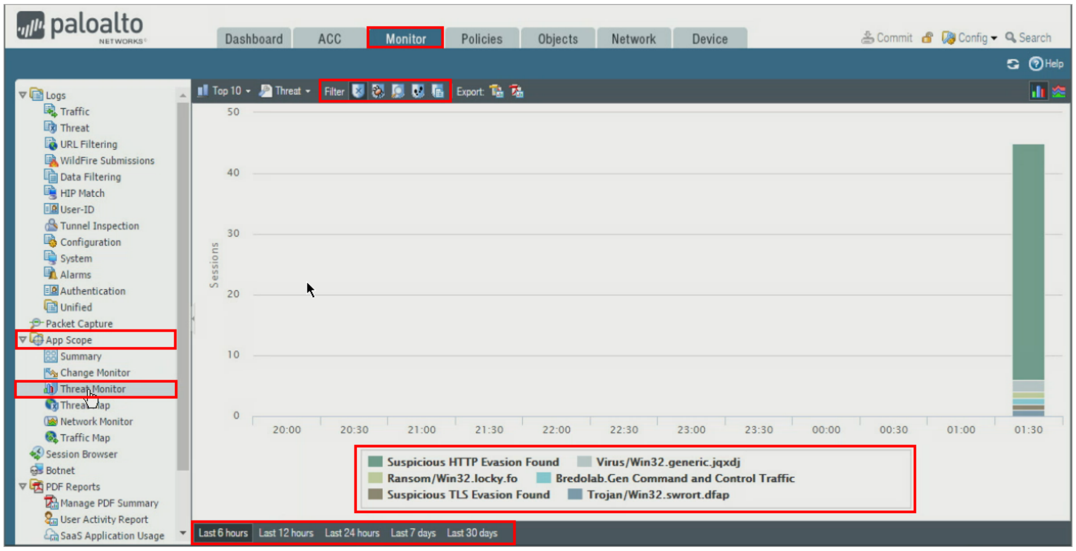
4. The **time period** also can be changed at the bottom.



Compare last hour to the same period ending 24 hours ago

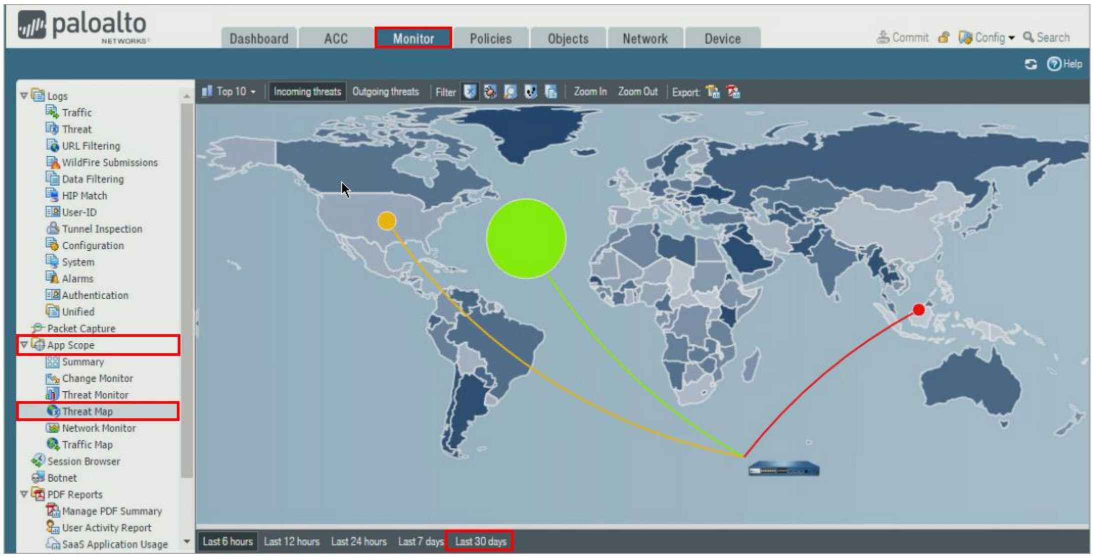
5. Select **Monitor > App Scope > Threat Monitor**.

   The Threat Monitor report displays a count of the top threats over the selected time period. By default, the figure shows the top 10 threat types for the past six hours.



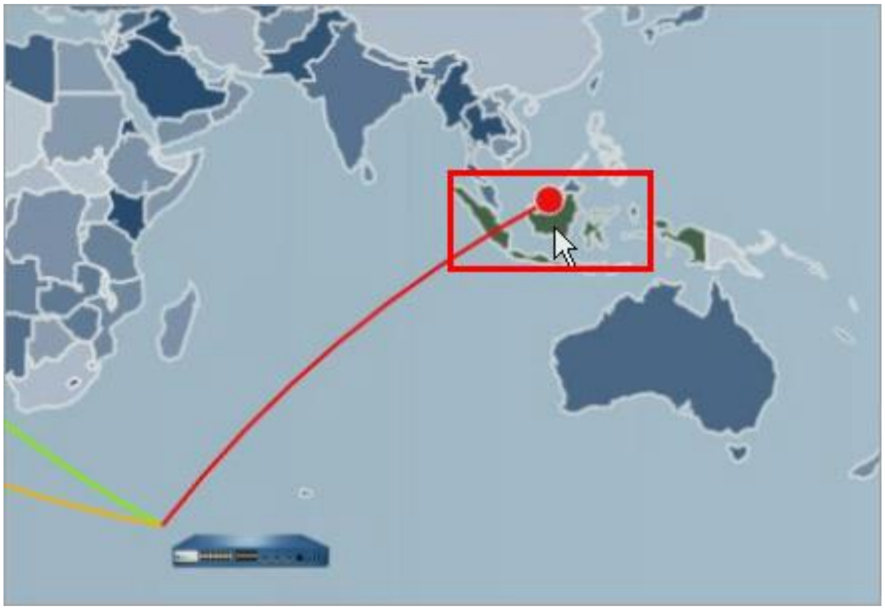
   The type of threat also can be filtered at the top and the time period can be changed to the Last 6 hours, 12 hours, 24 hours, 7 days, or 30 days.

6. Select **Monitor > App Scope > Threat Map** then click **Last 30 Days**.

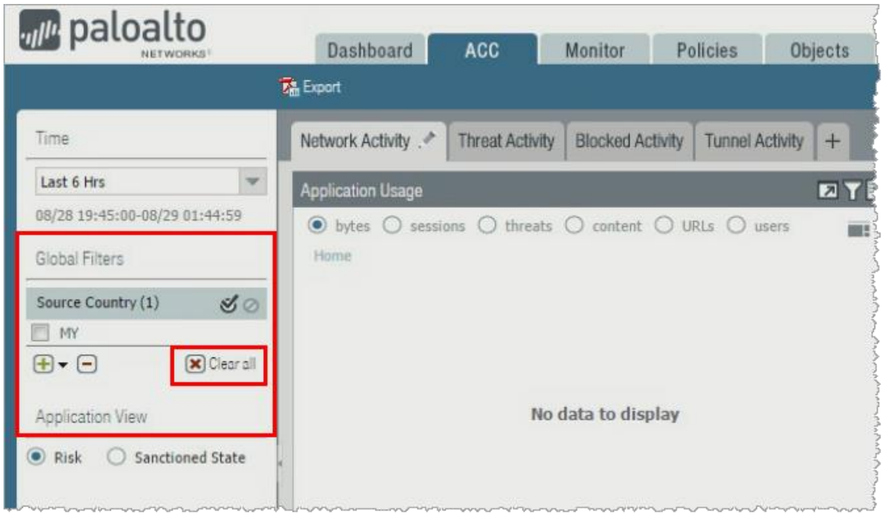


   The Threat Map report shows a geographical view of threats, including severity.

7. Click **Malaysia**.



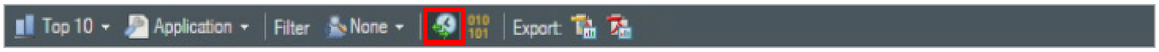
The ACC opens with a global filter referencing Malaysia (MY):

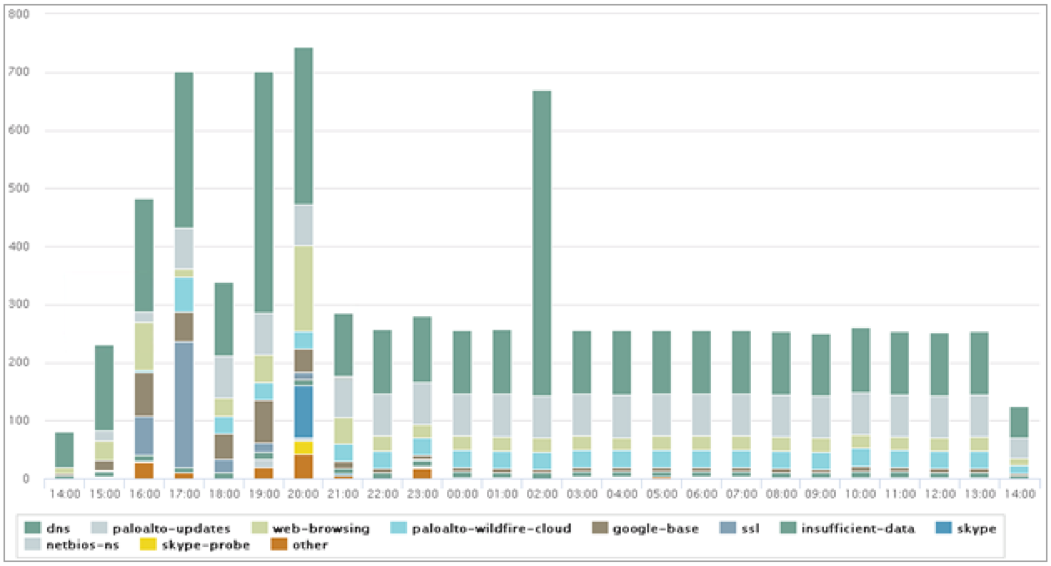


8. Click **Clear all** to clear the Global Filter.
9. Select **Monitor > App Scope > Network Monitor**.

   The Network Monitor report displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded, as indicated in the legend below the chart. For example, the following diagram shows application bandwidth for the past six hours based on session information.

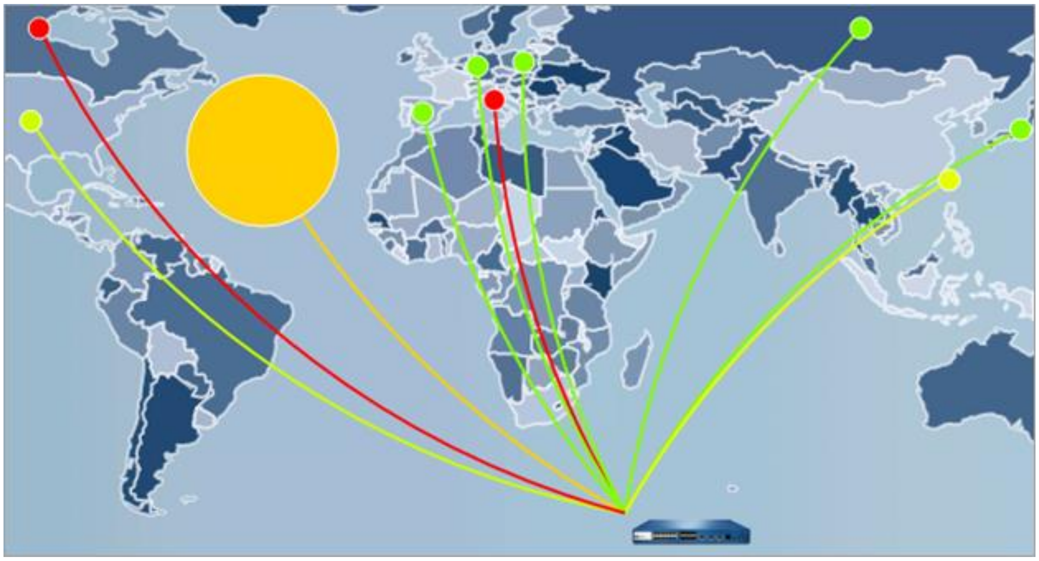
10. Click the **Session Count** icon to display the information by Session Count and not Bytes.





As is standard in all App-Scope graph items, you can click an application color, which switches your view in the WebUI to the ACC tab.

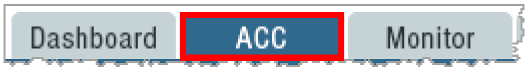
11. Select **Monitor > App Scope > Traffic Map**. The Traffic Map report shows a geographical view of traffic flows according to sessions or flows.



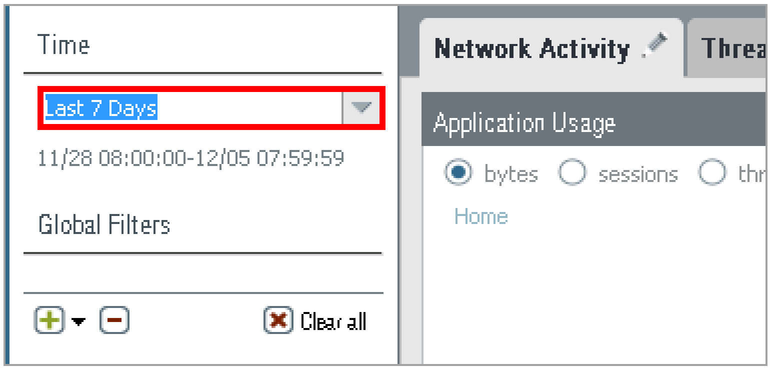
12.4 Explore the ACC

The ACC is an analytical tool that provides actionable intelligence about the activity within your network. The ACC uses the firewall logs to graphically depict traffic trends on your network.

1. Click the **ACC** tab.



2. Click the **Time** drop-down list and select **Last 7 Days**.



Time

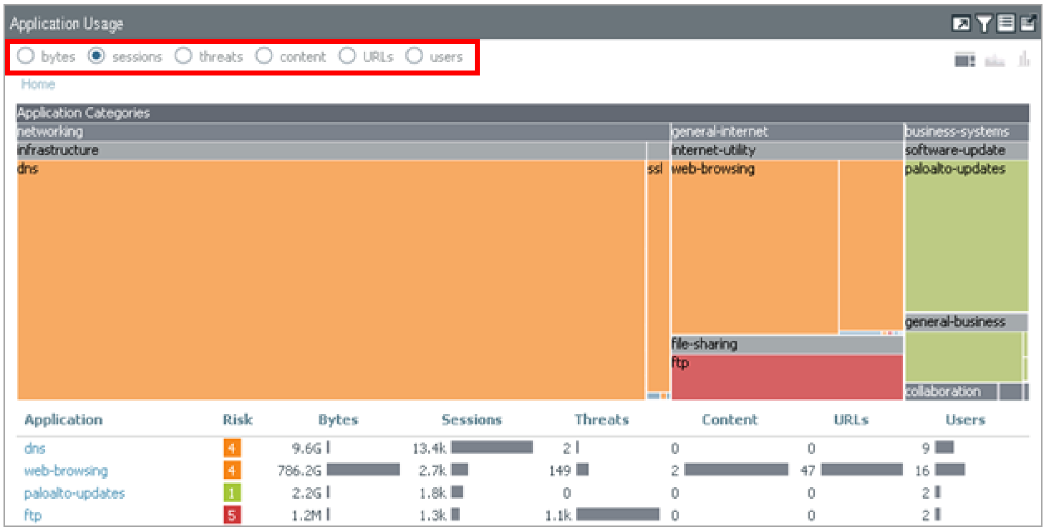
Last 7 Days

11/28 08:00:00-12/05 07:59:59

Global Filters

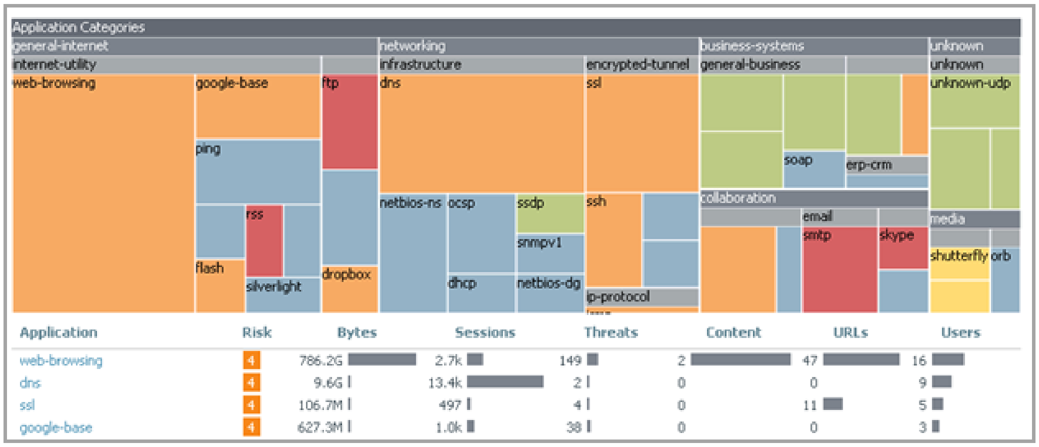
3. Explore the information available on the **Network Activity** tab. This tab displays an overview of traffic and user activity on your network. It focuses on the top applications being used; the top users who generate traffic with detailed information about the bytes, content, threats, or URLs accessed by the user; and the most used security rules against which traffic matches occur.

Notice that in every pane you can display data by bytes, sessions, threats, content, URLs, and users.



Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
dns	4	9.6G	13.4k	2	0	0	9
web-browsing	4	786.2G	2.7k	149	2	47	16
paloalto-updates	1	2.2G	1.8k	0	0	0	2
ftp	5	1.2M	1.3k	1.1k	0	0	2

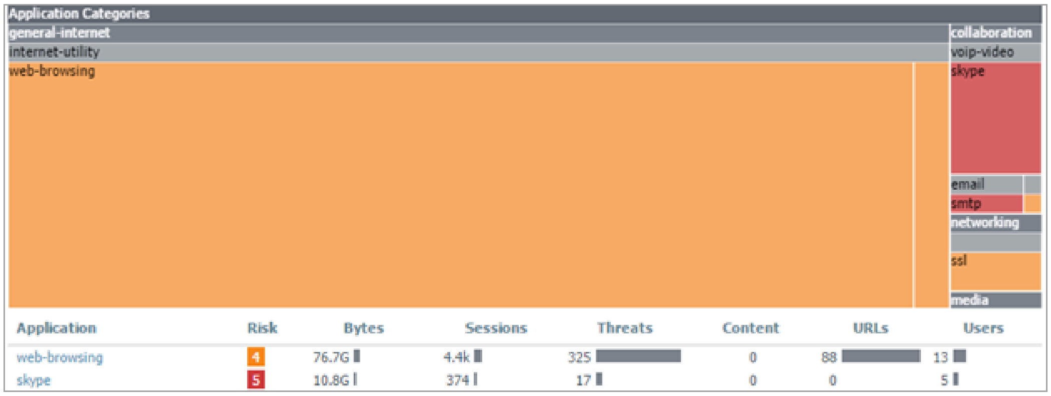
4. Select the **users** option. Notice how the application use seems more consistent across all colors versus bytes.



Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
web-browsing	4	786.2G	2.7k	149	2	47	16
dns	4	9.6G	13.4k	2	0	0	9
ssl	4	106.7M	497	4	0	11	5
google-base	4	627.3M	1.0k	38	0	0	3

This information indicates that one application does not supersede any other application in overall use by users.

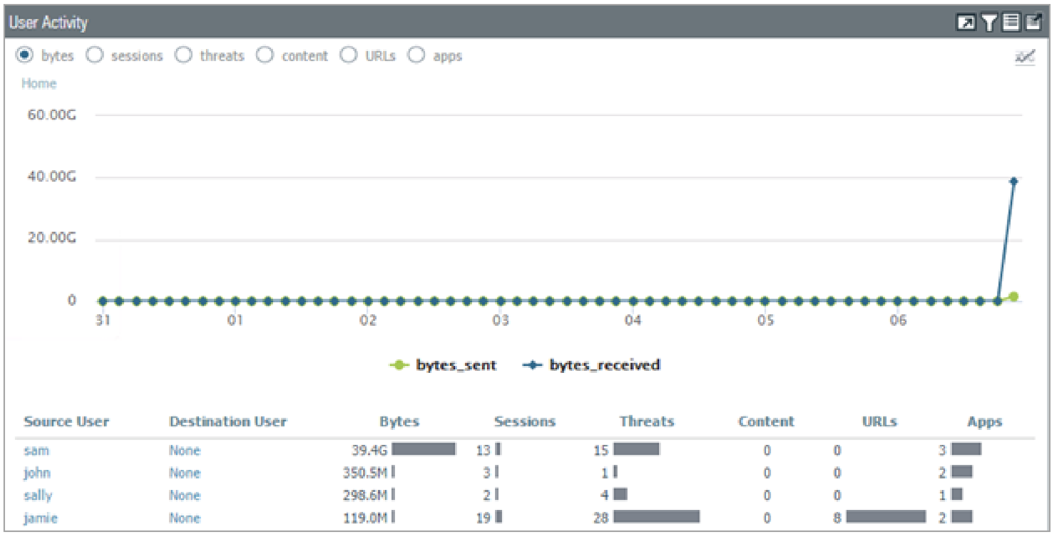
5. Select **threats** in the **Application Usage** pane.



Application	Risk	Bytes	Sessions	Threats	Content	URLs	Users
web-browsing	4	76.7G	4.4k	325	0	88	13
skype	5	10.8G	374	17	0	0	5

Given the displayed information you can see that web-browsing is the primary source of threats in this environment.

6. Focus your attention on the **User Activity** pane. Which user consumed the most bandwidth in the past seven days?



User Activity

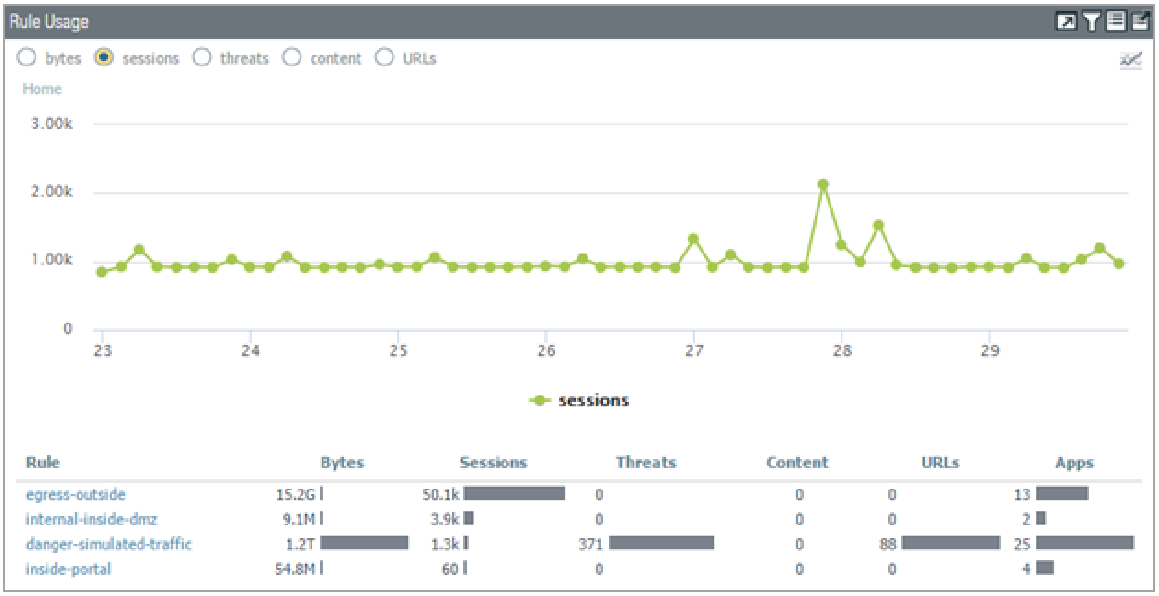
● bytes ○ sessions ○ threats ○ content ○ URLs ○ apps

Home

Source User	Destination User	Bytes	Sessions	Threats	Content	URLs	Apps
sam	None	39.4G	13	15	0	0	3
john	None	350.5M	3	1	0	0	2
sally	None	298.6M	2	4	0	0	1
jamie	None	119.0M	19	28	0	8	2

From the graph in the example, you can see that Jamie has consumed the most bandwidth. Your user might be different.

7. Focus your attention on the bottom-right **Rule Usage** pane.
8. Select **sessions**. Which Security policy rule has been used the most?



Rule Usage

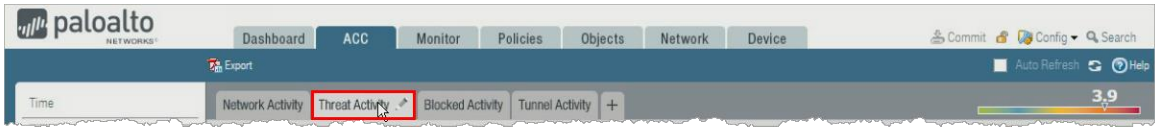
○ bytes ● sessions ○ threats ○ content ○ URLs

Home

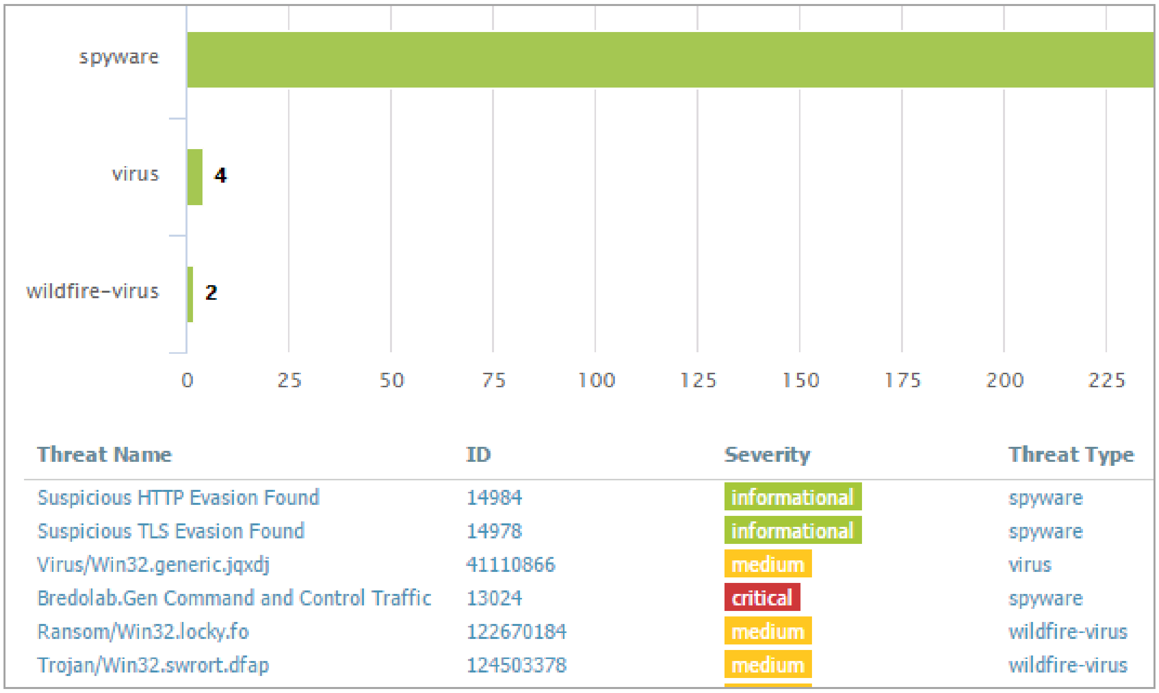
Rule	Bytes	Sessions	Threats	Content	URLs	Apps
egress-outside	15.2G	50.1k	0	0	0	13
internal-inside-dmz	9.1M	3.9k	0	0	0	2
danger-simulated-traffic	1.2T	1.3k	371	0	88	25
inside-portal	54.8M	60	0	0	0	4

From the displayed information, you can see that the most active rule based on session count is egress-outside.

9. Click the **Threat Activity** tab:



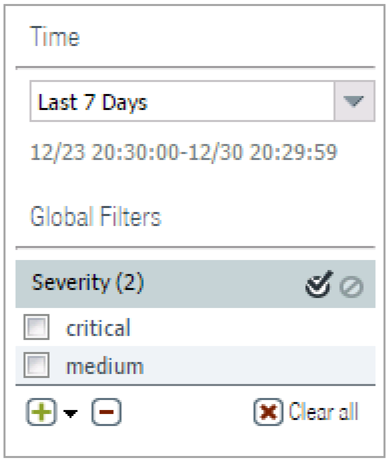
This tab displays an overview of the threats on the network. It focuses on the top threats: vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top WildFire submissions by file type and application, and applications that use non-standard ports.



Threat Name	ID	Severity	Threat Type
Suspicious HTTP Evasion Found	14984	informational	spyware
Suspicious TLS Evasion Found	14978	informational	spyware
Virus/Win32.generic.jqxdj	41110866	medium	virus
Bredolab.Gen Command and Control Traffic	13024	critical	spyware
Ransom/Win32.locky.fo	122670184	medium	wildfire-virus
Trojan/Win32.swrort.dfap	124503378	medium	wildfire-virus

Notice that there are informational entries that might not be useful.

10. Create a global filter for only medium and critical severities.



Time

Last 7 Days

12/23 20:30:00-12/30 20:29:59

Global Filters

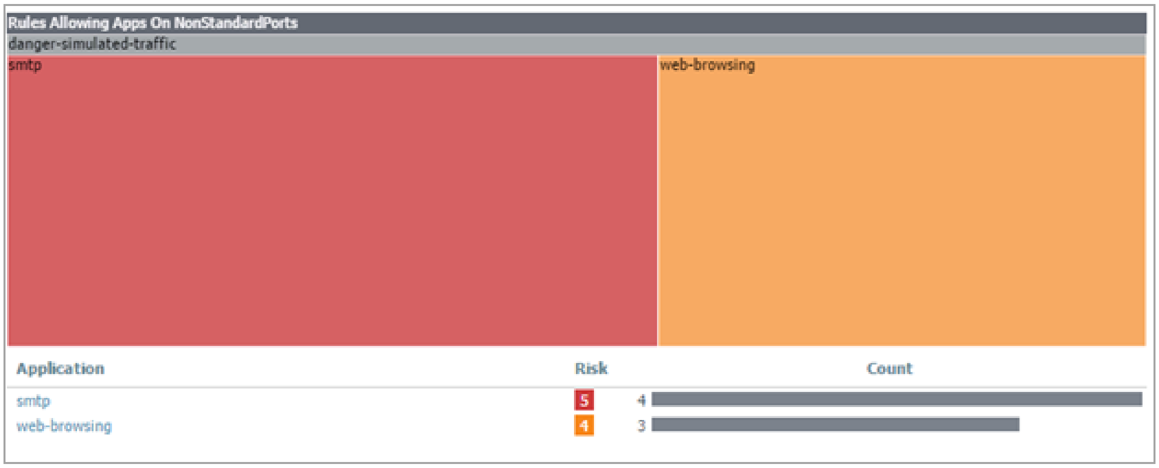
Severity (2)

□ critical

□ medium

Notice that the graph updates to display only critical and medium severities.

11. Scroll down to the bottom-right and notice the **Rules Allowing Apps On Non Standard Ports** pane.



Rules Allowing Apps On NonStandardPorts

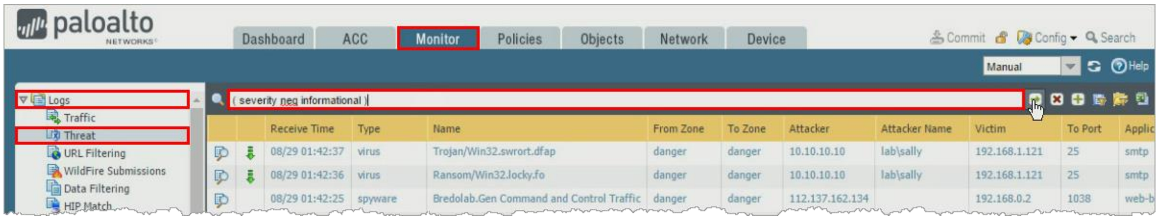
danger-simulated-traffic

Application	Risk	Count
smtp	5	4
web-browsing	4	3

This pane is good for identifying rules that need to enforce the application-default service setting.

12.5 Investigate Traffic

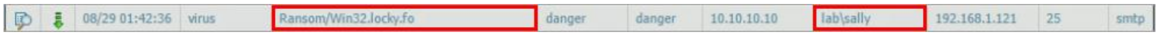
1. In the WebUI select **Monitor > Logs > Threat** then type the filter `(severity neq informational)` into the log filter text box and press **Enter**.



(severity neq informational)

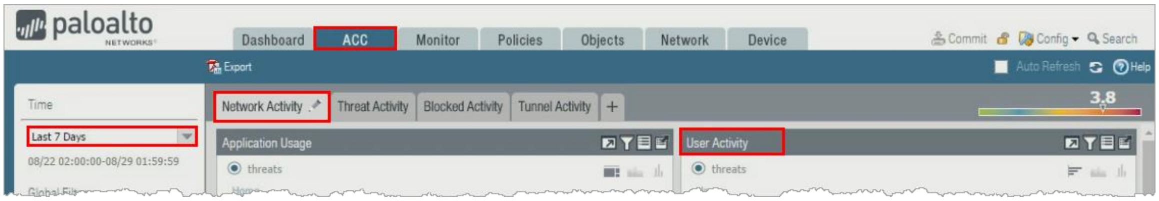
Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Applic
08/29 01:42:37	virus	Trojan/Win32.swrort.dfap	danger	danger	10.10.10.10	lab\sally	192.168.1.121	25	smtp
08/29 01:42:36	virus	Ransom/Win32.locky.fo	danger	danger	10.10.10.10	lab\sally	192.168.1.121	25	smtp
08/29 01:42:25	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	112.137.162.134		192.168.0.2	1038	web-b

2. Locate the first entry referencing **locky** and notice that the user sally is associated with it



08/29 01:42:36	virus	Ransom/Win32.locky.fo	danger	danger	10.10.10.10	lab\sally	192.168.1.121	25	smtp

3. Click the **ACC** tab, ensure that the **Time** drop-down list is **Last 7 Days**, the **Network Activity** tab is selected then move to the **User Activity** pane.

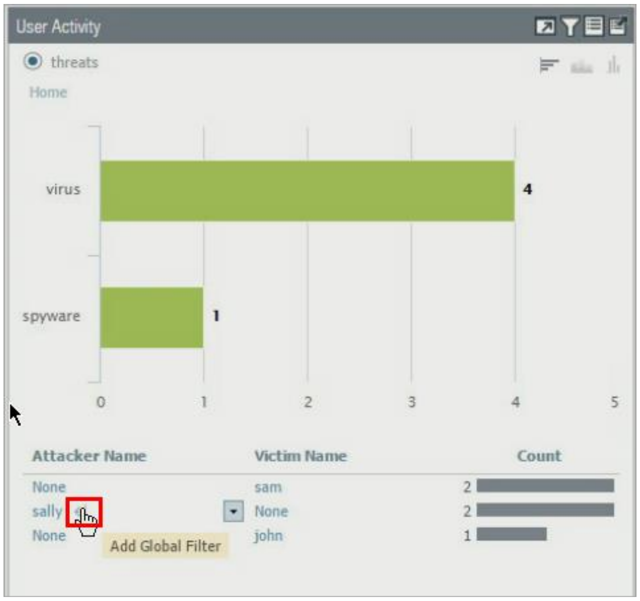


Time

Last 7 Days

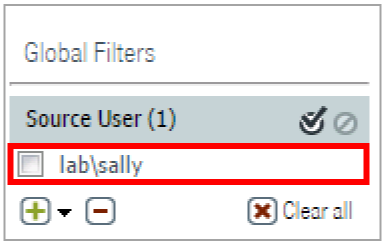
08/22 02:00:00-08/29 01:59:59

4. Use the left-arrow to promote **sally** to a Global Filter.



Attacker Name	Victim Name	Count
None	sam	2
sally	None	2
None	john	1

5. Ensure that sally was promoted to a **Global Filter.**



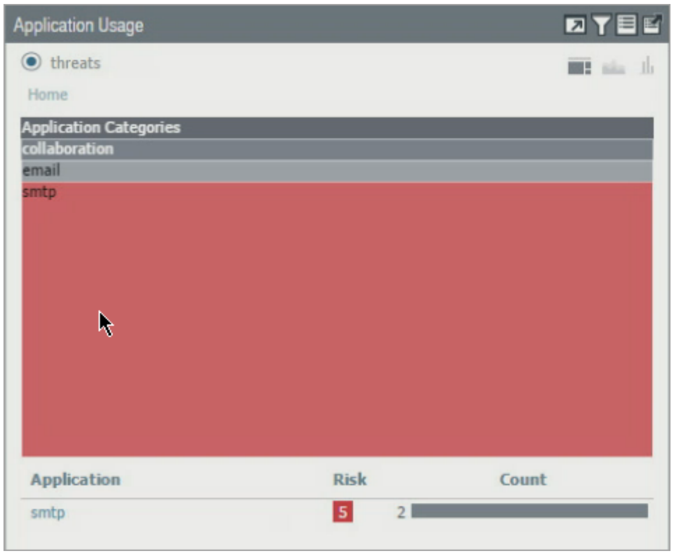
Global Filters

Source User (1)

□ lab\sally

Clear all

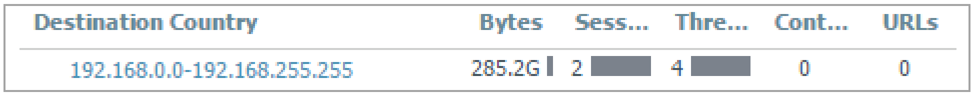
Notice that all window panes have updated to show only information based on sally.



Application	Risk	Count
smtp	5	2

From the displayed information, you can see that sally is associated only with smtp traffic, which could indicate a possible infection and lateral movement.

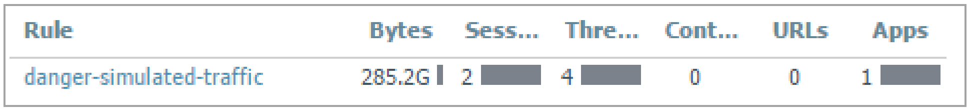
6. Scroll down and locate the **Destination Regions** pane.



Destination Country	Bytes	Sess...	Thre...	Cont...	URLs
192.168.0.0-192.168.255.255	285.2G	2	4	0	0

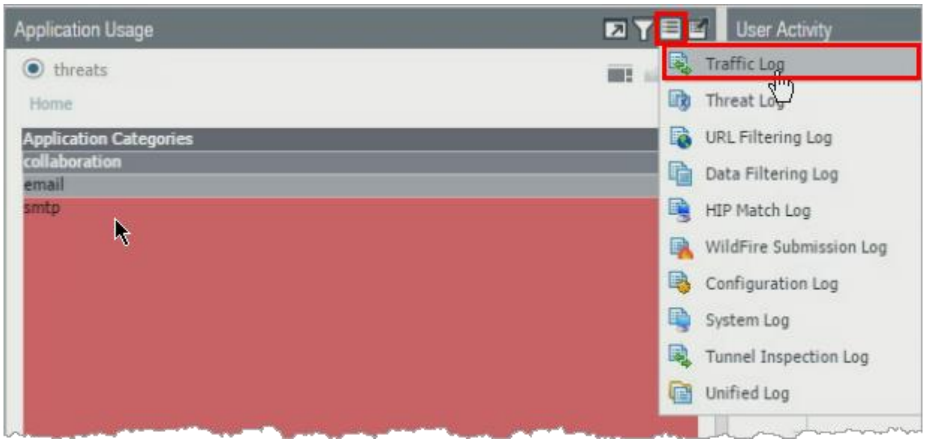
Notice that this is an internal network, which could indicate that sally is using corporate e-mail and not an external source or that there might be a rogue SMTP relay.

7. Scroll down to the **Rule Usage** pane. Notice that only one rule allowed this traffic. If this were a production environment, inspection should be done to ensure that this rule is operating effectively. For example, should the rule allow SMTP? If not, is this a rogue SMTP relay?



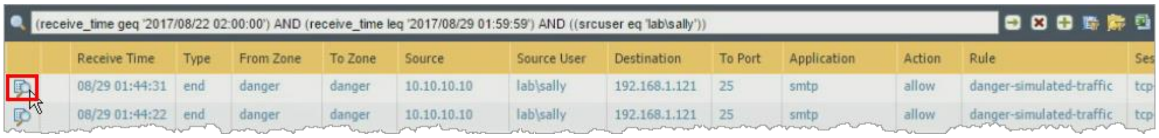
Rule	Bytes	Sess...	Thre...	Cont...	URLs	Apps
danger-simulated-traffic	285.2G	2	4	0	0	1

8. Scroll to the top-left **Application Usage** pane.
9. Click the **Jump to Logs** icon and select **Traffic Log**:



Notice that the WebUI switched views to the Traffic log with a predefined filter.

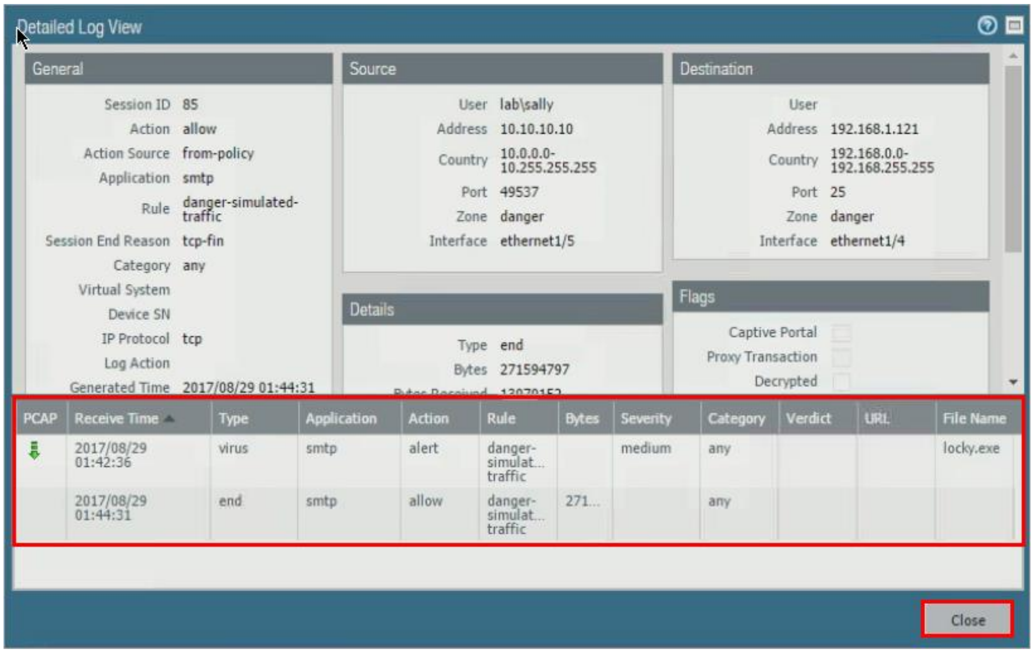
10. Select the **Detailed Log View** icon.



```
(receive_time geq '2017/08/22 02:00:00') AND (receive_time leq '2017/08/29 01:59:59') AND ((srcuser eq 'lab\sally'))
```

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Ses
	08/29 01:44:31	end	danger	danger	10.10.10.10	lab\sally	192.168.1.121	25	smtp	allow	danger-simulated-traffic	tcp
	08/29 01:44:22	end	danger	danger	10.10.10.10	lab\sally	192.168.1.121	25	smtp	allow	danger-simulated-traffic	tcp

11. At the bottom of the **Detailed Log View** window that popped up, you can see the associated threat entries. Click **Close** when finished observing.



General

Session ID 85
Action allow
Action Source from-policy
Application smtp
Rule danger-simulated-traffic
Session End Reason tcp-fin
Category any
Virtual System
Device SN
IP Protocol tcp
Log Action
Generated Time 2017/08/29 01:44:31

Source

User lab\sally
Address 10.10.10.10
Country 10.0.0.0-10.255.255.255
Port 49537
Zone danger
Interface ethernet1/5

Destination

User
Address 192.168.1.121
Country 192.168.0.0-192.168.255.255
Port 25
Zone danger
Interface ethernet1/4

Details

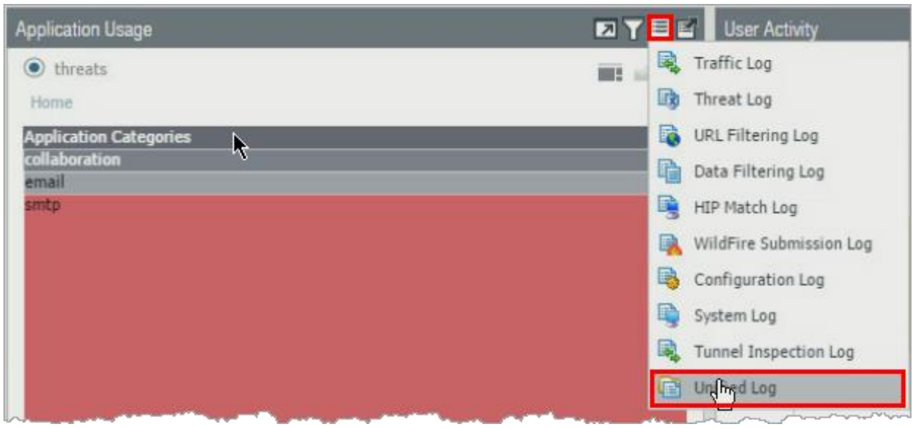
Type end
Bytes 271594797
Bytes Received 13070152

Flags

Captive Portal □
Proxy Transaction □
Decrypted □

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
⇩	2017/08/29 01:42:36	virus	smtp	alert	danger-simulat... traffic		medium	any			locky.exe
	2017/08/29 01:44:31	end	smtp	allow	danger-simulat... traffic	271...		any			

12. Click the **ACC** tab then ensure the **Network Activity** tab is selected.
13. Under **Application Usage** click the **Jump to Logs** icon and select the **Unified Log**.

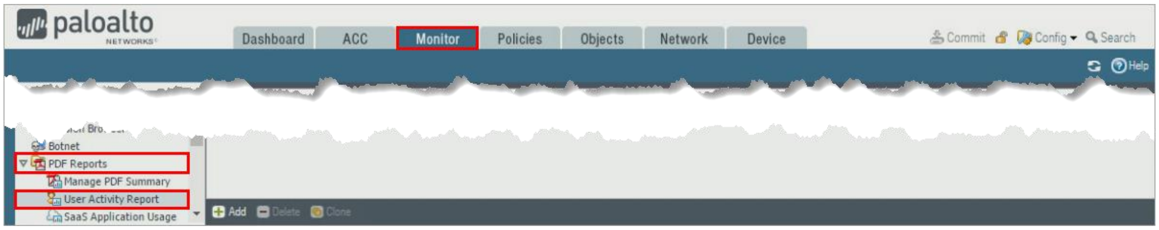


Notice that you now see both Traffic and Threat logs in one unified display, which can help with correlation.

12.6 User Activity Report

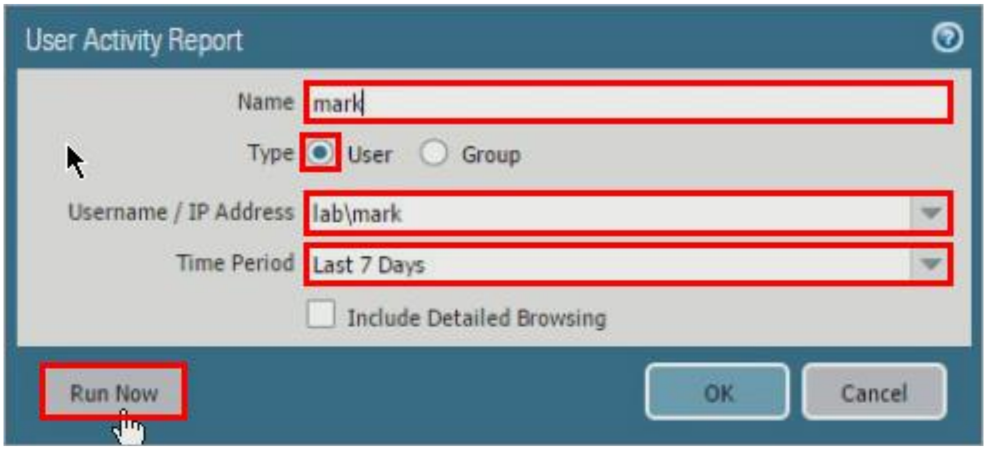
The firewall can generate reports that summarize the activity of individual users or user groups.

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



2. Click **Add** to define a new user activity report:

Parameter	Value
Name	`mark`
Type	`User`
Username / IP Address	`lab\mark`
Time Period	`Last 7 days`



User Activity Report

Name: mark

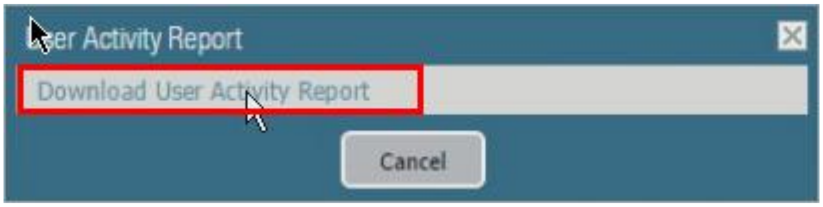
Type: ● User ○ Group

Username / IP Address: lab\mark

Time Period: Last 7 Days

□ Include Detailed Browsing

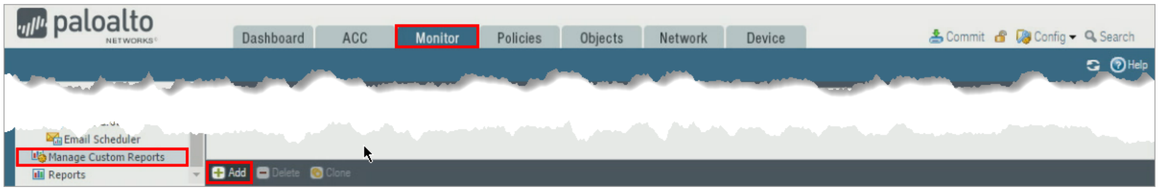
3. Click **Run Now**.
4. **Download** and **open** the report when it finishes.



5. Browse through the report to get familiar with the presented information. You can also include detailed browsing history that will include an approximate time a user spends on a website (not available when specifying a group).

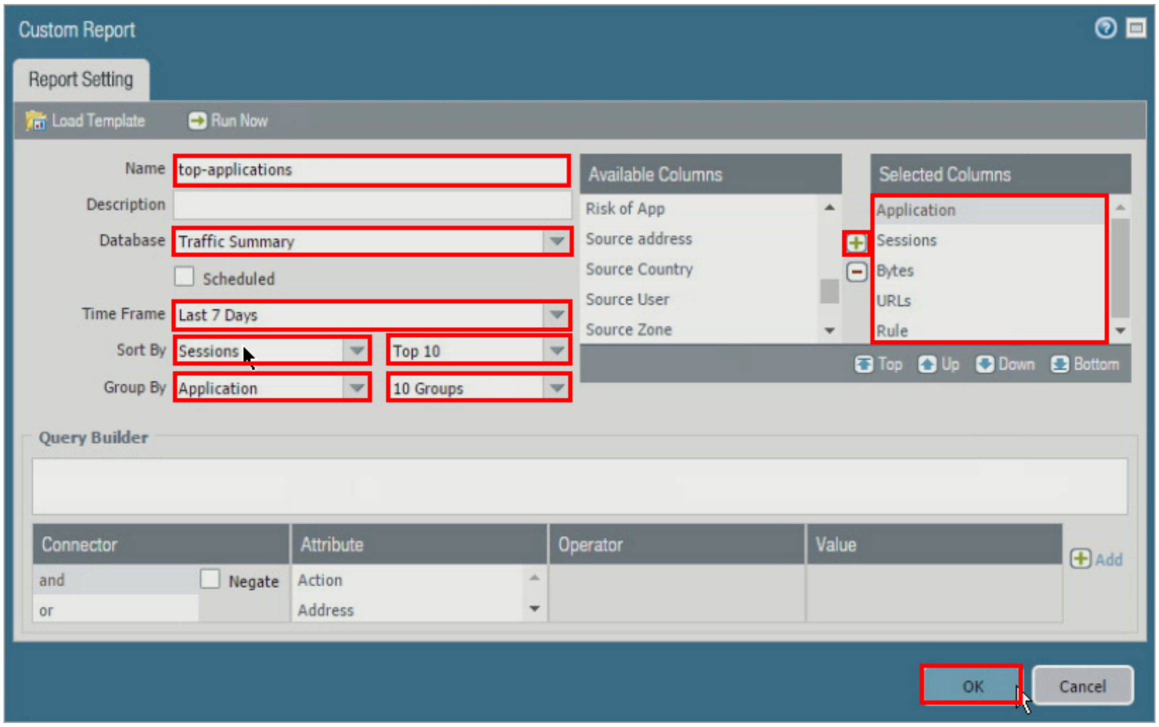
12.7 Create a Custom Report

1. Select **Monitor > Manage Custom Reports** then click **Add**.



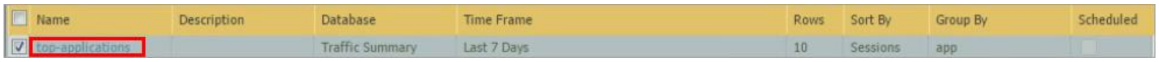
2. In the **Custom Report** window fill out the following then click **OK**.

Parameter	Value
Name	`top-applications`
Database	**`Traffic Summary`**
Time Frame	**`Last 7 Days`**
Sort By	**`Sessions and Top 10`**
Group By	**`Application and 10 Groups`**
Selected Columns	**`Application`** **`Sessions`** **`Bytes`** **`URLs`** **`Rule`**



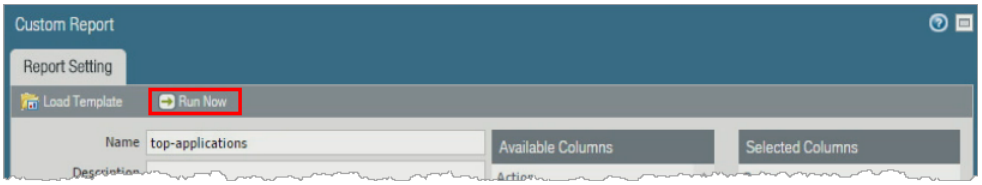
Name: top-applications
Description:
Database: Traffic Summary
□ Scheduled
Time Frame: Last 7 Days
Sort By: Sessions, Top 10
Group By: Application, 10 Groups
Selected Columns: Application, Sessions, Bytes, URLs, Rule

3. Click the **top-applications** report to reopen the Custom Report window.



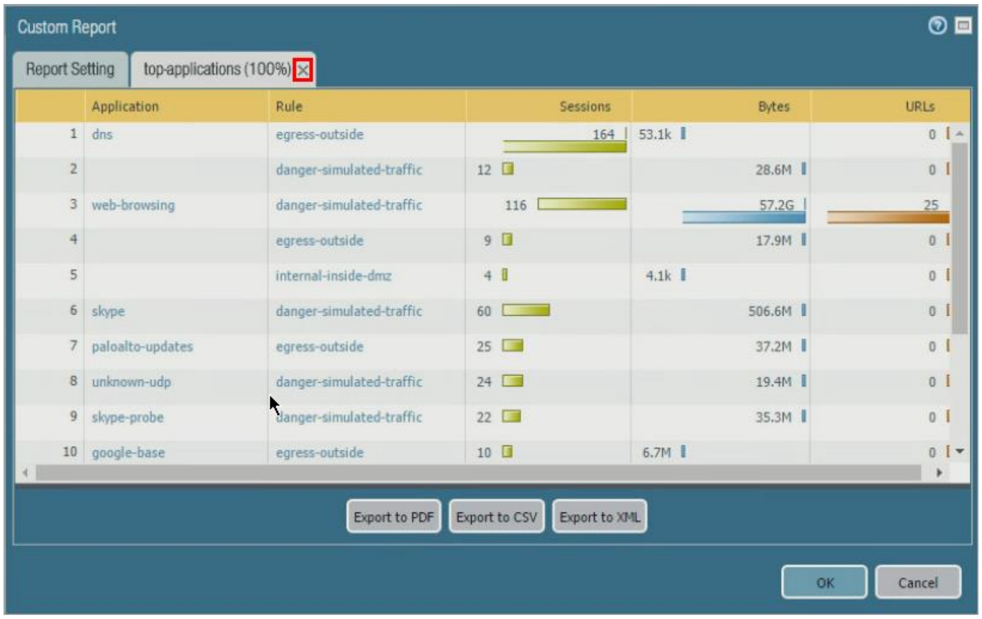
□ Name	Description	Database	Time Frame	Rows	Sort By	Group By	Scheduled
☑ top-applications		Traffic Summary	Last 7 Days	10	Sessions	app	□

4. Click **Run Now** to generate the report. The report will appear in a new tab in the browser window.



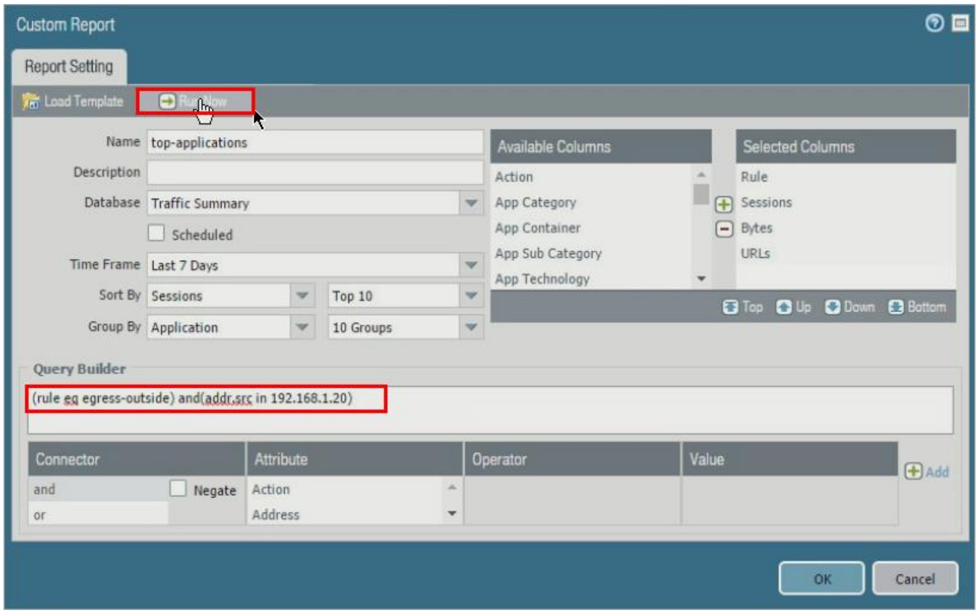
Name: top-applications

5. Close the **top-applications** tab containing the report.



	Application	Rule	Sessions	Bytes	URLs
1	dns	egress-outside	164	53.1k	0
2		danger-simulated-traffic	12	28.6M	0
3	web-browsing	danger-simulated-traffic	116	57.2G	25
4		egress-outside	9	17.9M	0
5		internal-inside-dmz	4	4.1k	0
6	skype	danger-simulated-traffic	60	506.6M	0
7	paloalto-updates	egress-outside	25	37.2M	0
8	unknown-udp	danger-simulated-traffic	24	19.4M	0
9	skype-probe	danger-simulated-traffic	22	35.3M	0
10	google-base	egress-outside	10	6.7M	0

6. On the **Report Setting** tab, create the following query using the Query Builder: `(rule eq egress-outside) and (addr.src in 192.168.1.20)` then click **Run Now** to run the report again, this time with the query.



Name: top-applications

Description:

Database: Traffic Summary

□ Scheduled

Time Frame: Last 7 Days

Sort By: Sessions, Top 10

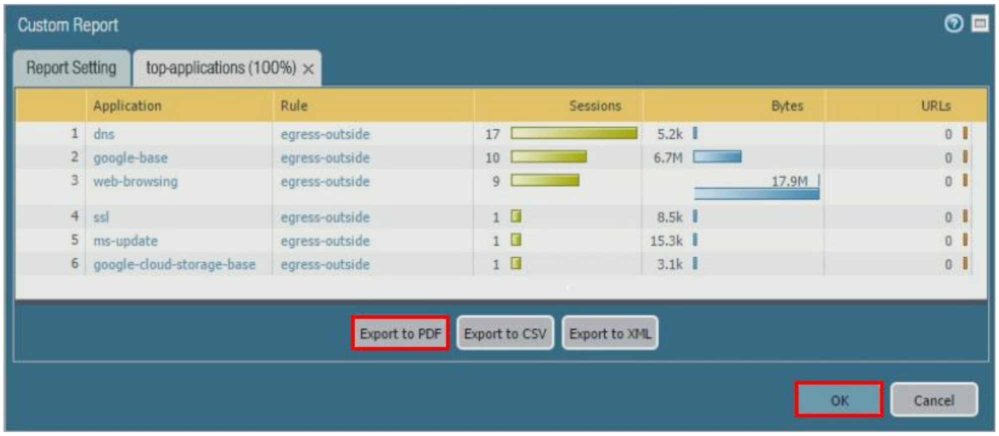
Group By: Application, 10 Groups

Selected Columns: Rule, Sessions, Bytes, URLs

Query Builder: (rule eq egress-outside) and(addr.src in 192.168.1.20)

Connector: and / or, □ Negate

7. Click **Export to PDF** to save the report as a PDF. (You might need to disable your browser's popup blocker.)

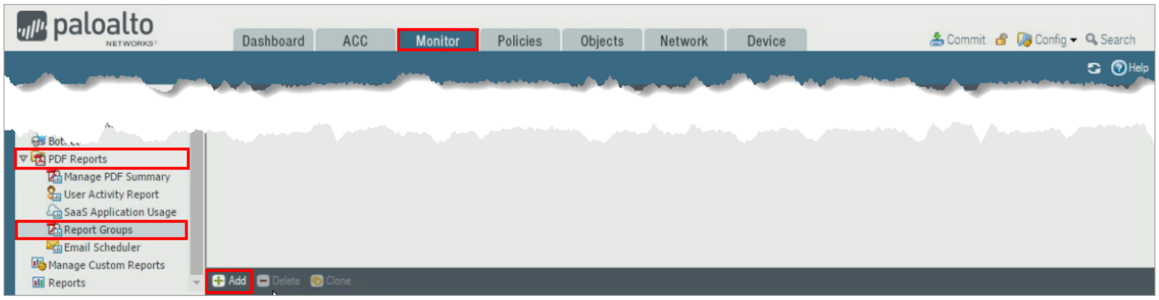


	Application	Rule	Sessions	Bytes	URLs
1	dns	egress-outside	17	5.2k	0
2	google-base	egress-outside	10	6.7M	0
3	web-browsing	egress-outside	9	17.9M	0
4	ssl	egress-outside	1	8.5k	0
5	ms-update	egress-outside	1	15.3k	0
6	google-cloud-storage-base	egress-outside	1	3.1k	0

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

12.8 Create a Report Group

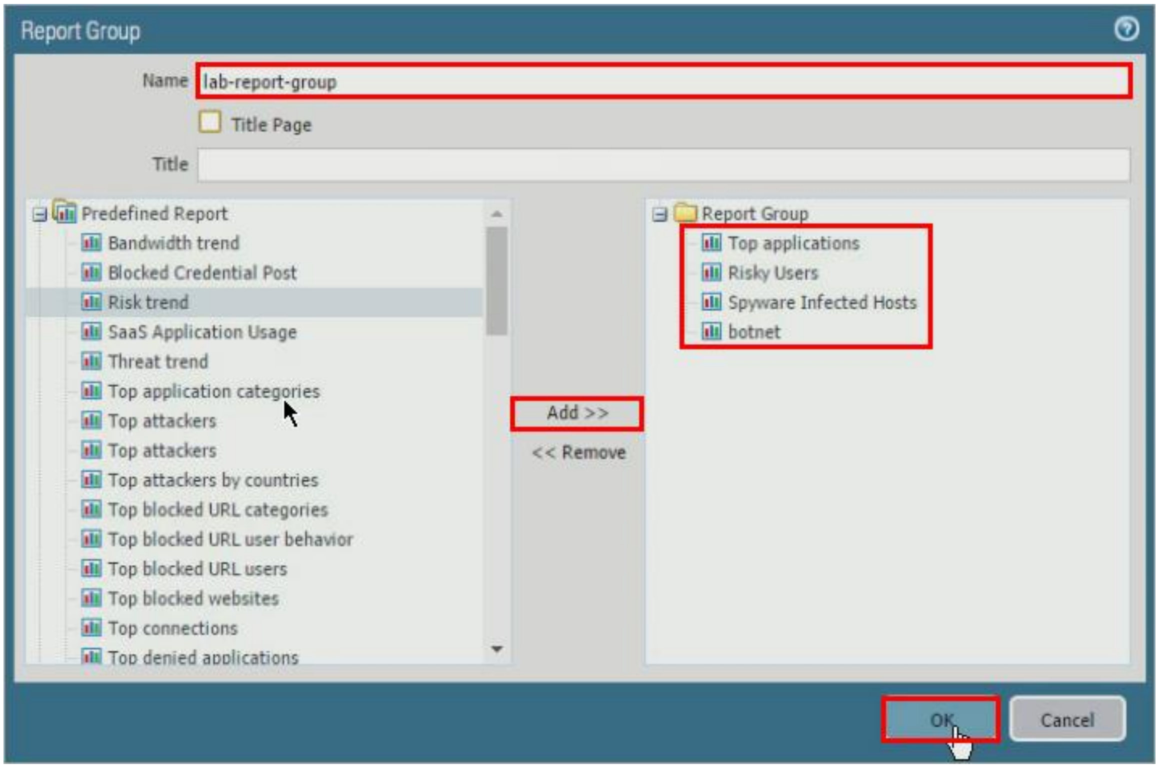
1. In the WebUI select **Monitor > PDF Reports > Report Groups** then click **Add** to define a new Report Group.



2. In the **Report Group** window fill out the following then click **OK**.

Parameter	Value
Name	`lab-report-group`

Reports	`Top applications`
	`Risky Users`
	`Spyware Infected Hosts`
	`botnet`



Report Group

Name: lab-report-group

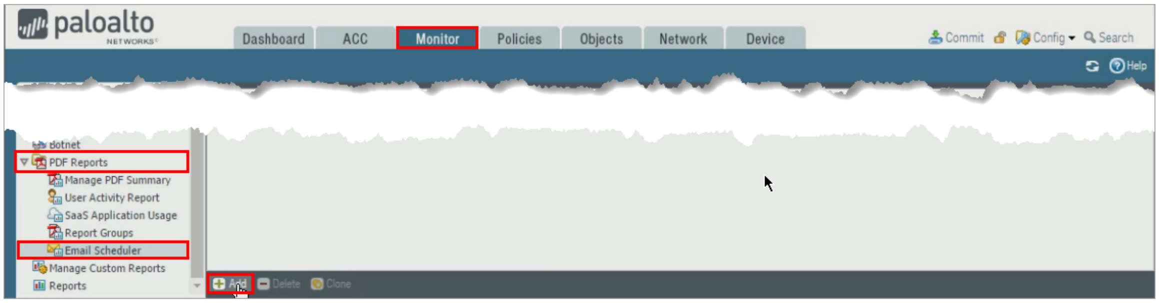
☐ Title Page

Title:

Report Group:
- Top applications
- Risky Users
- Spyware Infected Hosts
- botnet

12.9 Schedule Report Group Email

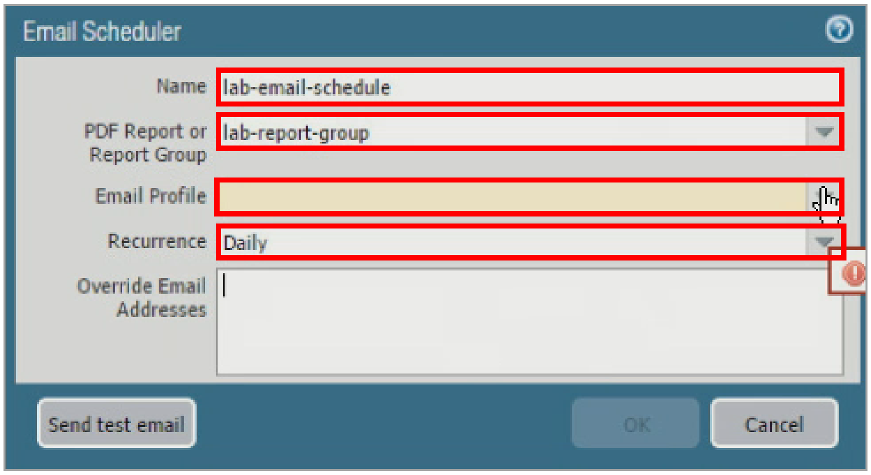
1. In the WebUI select **Monitor > PDF Reports > Email Scheduler** then click **Add.**



2. In the Email Scheduler window fill out the following.

Selecting **new** in the Email Profile dropbox will pop open the **Email Server Profile** window covered in the next step.

Parameter	Value
Name	`lab-email-schedule`
Report Group	**`lab-report-group`**
Recurrence	**`Daily`**
Email Profile	`New` **`Email Profile`**



Email Scheduler

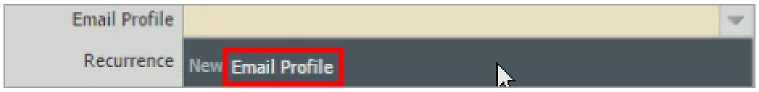
Name: lab-email-schedule

PDF Report or Report Group: lab-report-group

Email Profile:

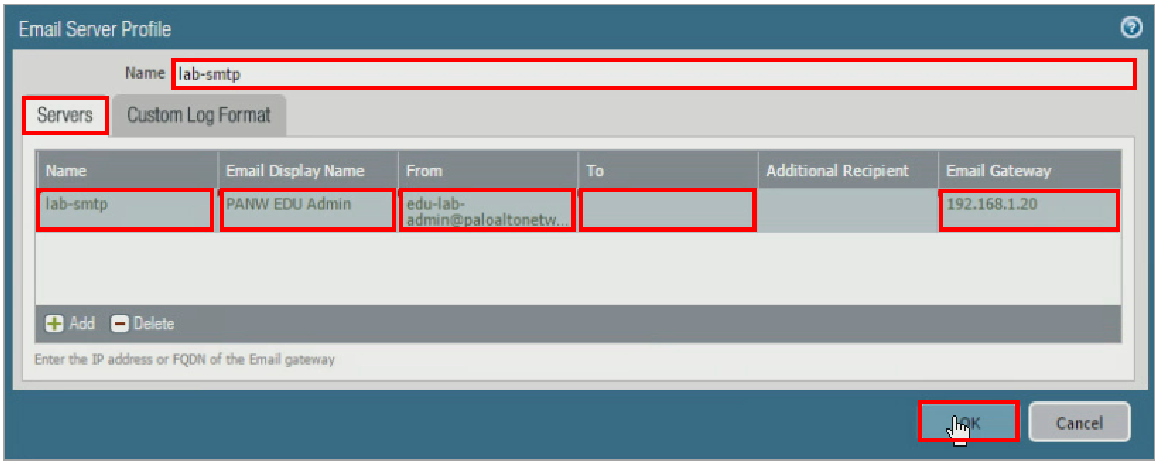
Recurrence: Daily

Override Email Addresses:



3. In the **Email Server Profile** window configure the following.

Parameter	Value
Name	`lab-smtp`
Email Display Name	`PANW EDU Admin`
From	`edu-lab-admin@paloaltonetworks.com`
To	`<your_email@address>`
Email Gateway	`192.168.1.20`



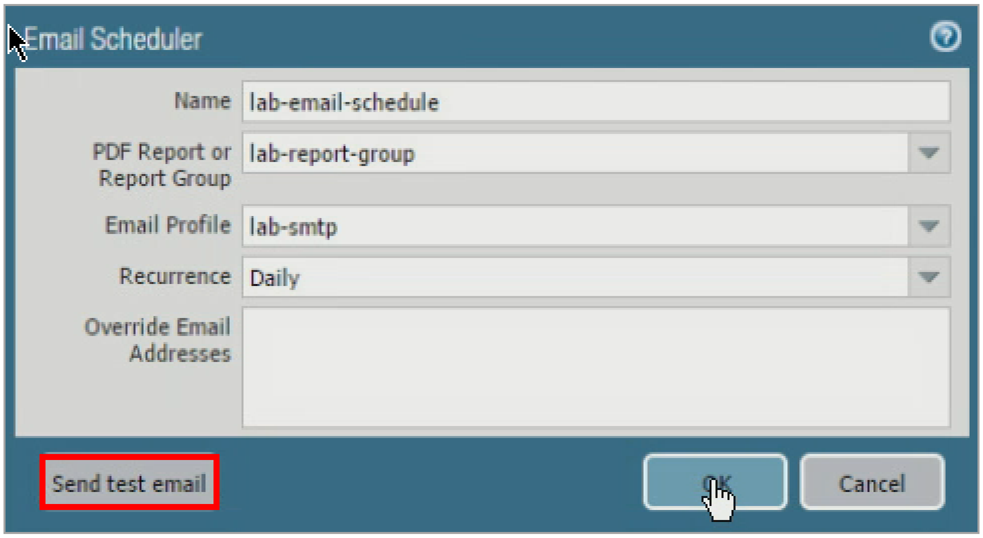
Email Server Profile

Name: lab-smtp

Name	Email Display Name	From	To	Additional Recipient	Email Gateway
lab-smtp	PANW EDU Admin	edu-lab-admin@paloaltonetw...			192.168.1.20

Enter the IP address or FQDN of the Email gateway

4. Click **OK** to close the Email Server Profile window.
5. Click **Send test email**. A test email will be sent to the address you provided. Wait for and confirm its arrival.



Email Scheduler

Name: lab-email-schedule

PDF Report or Report Group: lab-report-group

Email Profile: lab-smtp

Recurrence: Daily

Override Email Addresses:

You may need to check your SPAM folder.

6. Click **OK** to close the Email Scheduler window.

Stop. This is the end of the Monitoring and Reporting lab.