



## **PALO ALTO NETWORKS EDU-210**



### **Lab 12: Monitoring and Reporting**

**Document Version: 2020-06-26**

Copyright © 2020 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Contents.....	2
Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
12 Monitoring and Reporting .....	6
12.0 Load Lab Configuration.....	6
12.1 Generate Traffic.....	9
12.2 Explore the Session Browser .....	10
12.3 Explore the App Scope Reports .....	13
12.4 Explore the ACC .....	19
12.5 Investigate the Traffic.....	24
12.6 Generate a User Activity Report.....	29
12.7 Create a Custom Report .....	31
12.8 Create a Report Group .....	35
12.9 Schedule a Report Group Email.....	37

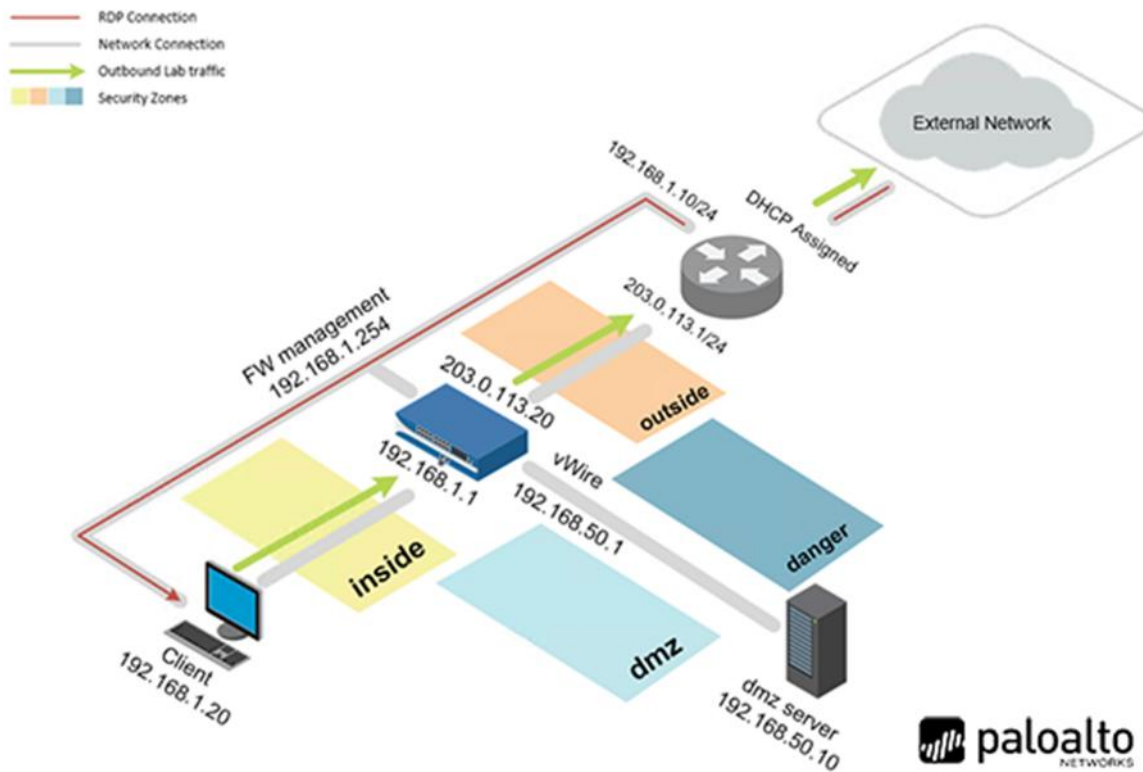
## Introduction

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 logs on the system. To effectively utilize this information, we need to become familiar with the variety of logs available 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	192.168.1.20	lab-user	Train1ng\$
Firewall	192.168.1.254	admin	Train1ng\$

## 12 Monitoring and Reporting

### 12.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as **lab-user** using the password **Train1ng\$**.



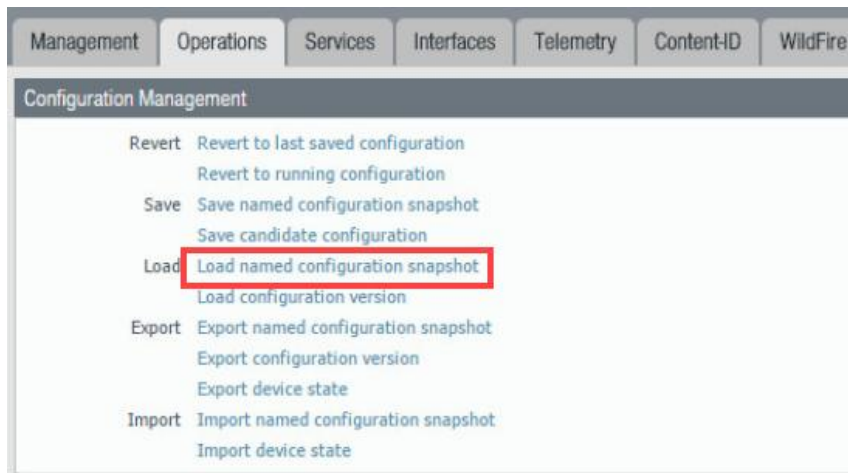
3. Launch the **Chromium Web Browser** and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	Train1ng\$

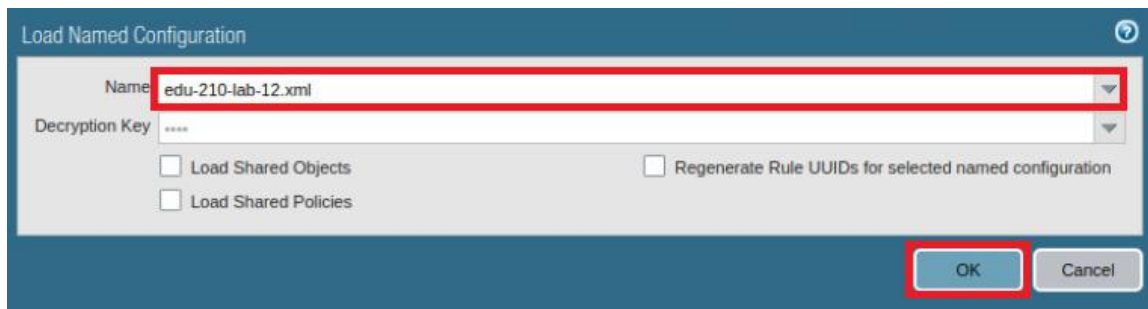
6. In the web interface, select **Device > Setup > Operations**.



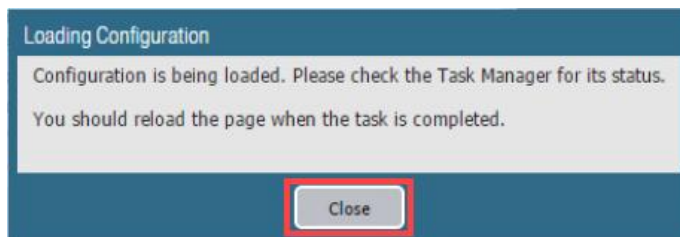
7. Click **Load named configuration snapshot**:



8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-12.xml**. Click **OK**.



9. Click **Close**.

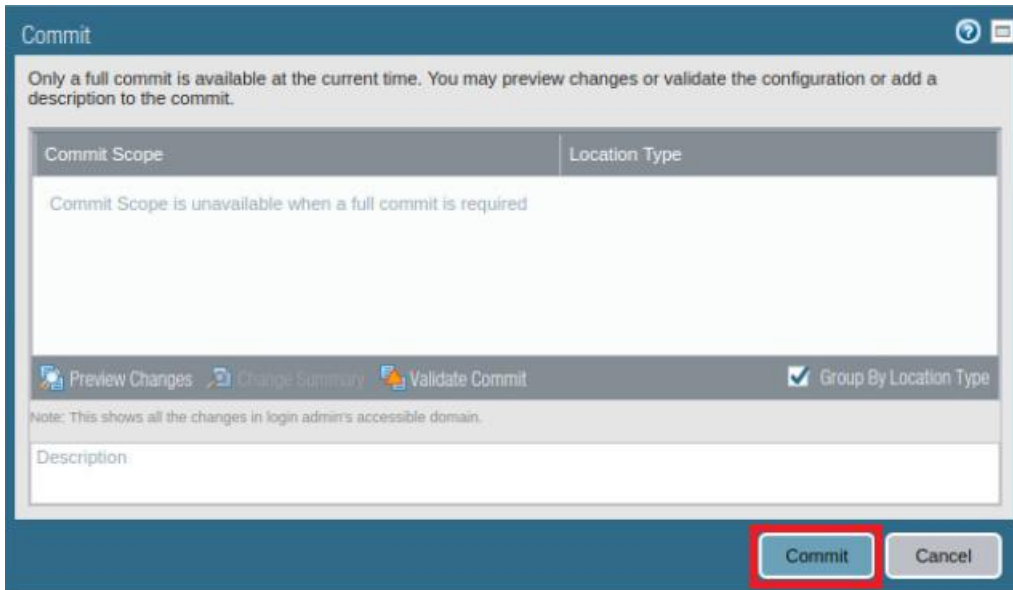


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

10. Click the **Commit** link at the top-right of the web interface.

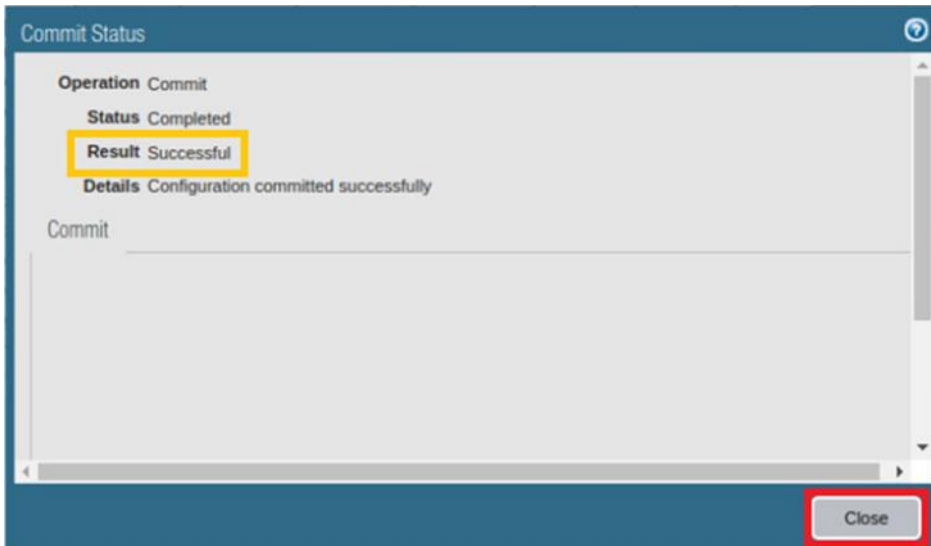


11. Click **Commit** and wait until the commit process is complete.



The 'Commit' dialog box has a title bar with a question mark icon and a close icon. The main text reads: 'Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.' Below this is a table with two columns: 'Commit Scope' and 'Location Type'. The 'Commit Scope' cell contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table is a row of buttons: 'Preview Changes', 'Change Summary', 'Validate Commit', and a checked checkbox labeled 'Group By Location Type'. Below the buttons is a text area labeled 'Description' with the note: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

12. Once completed successfully, click **Close** to continue.



The 'Commit Status' dialog box has a title bar with a question mark icon and a close icon. The main content area shows the following information: 'Operation Commit', 'Status Completed', 'Result Successful' (highlighted with a yellow box), and 'Details Configuration committed successfully'. Below this is a text area labeled 'Commit'. At the bottom right is a button labeled 'Close' (highlighted with a red box).



## 12.1 Generate Traffic

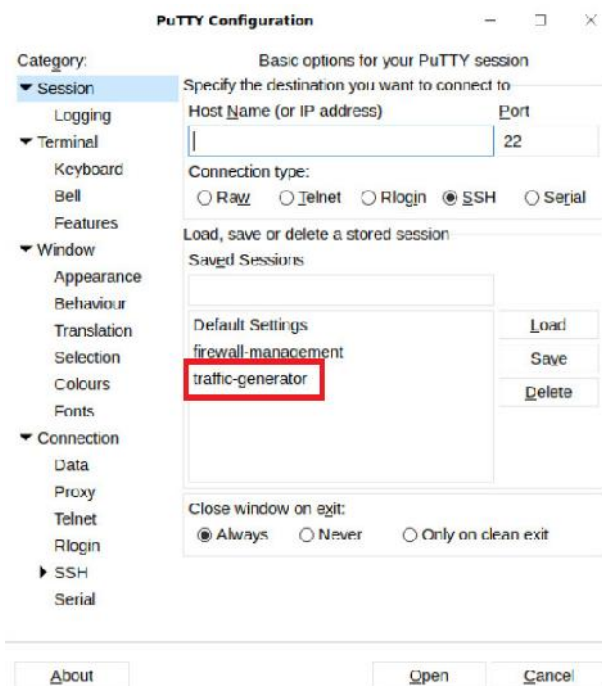
In this task, you will pre-populate the firewall with log entries and usernames that you can observe and investigate in this lab.



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



1. On the Client desktop, double-click the **PuTTY** icon.
2. In the *PuTTY Configuration* window, double-click **traffic-generator**.



3. Log in as **root** with **pa10A1t0** as the password.

```
login as: root
root@192.168.50.10's password:
Last login: Thu Feb 27 04:13:48 2020
[root@pod-dmz ~]#
```

- While in the *PuTTY* window, type the following CLI command and observe the output.

```
[root@pod-dmz ~]# sh /tg/traffic.sh
```

```
[root@pod-dmz ~]# sh /tg/traffic.sh

THIS COULD TAKE UP TO 15 MINUTES

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
   0      0     0         0             0      0      0      0
   0      0     0         0             0      0      0      0
0    0    0    0    0    0    0    0 --:--:-- 0:02:07 --:--:-- 0curl: (7) Failed connect to 192.168.50.1:443; Connection timed out

GENERATING TRAFFIC
```



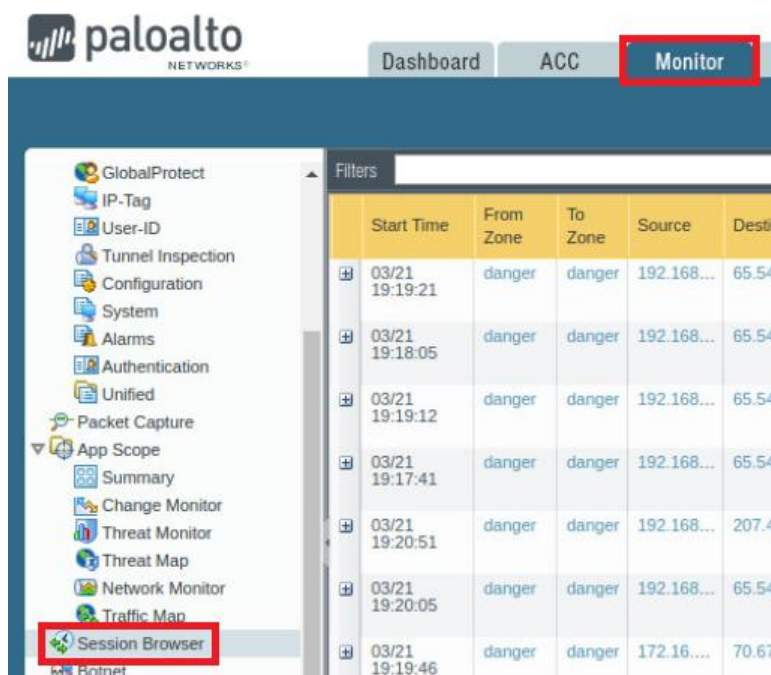
After you execute the command, wait until the script finishes before proceeding to the next step.


- Once the script completes, type **exit** to close the *PuTTY* window.

## 12.2 Explore the Session Browser

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

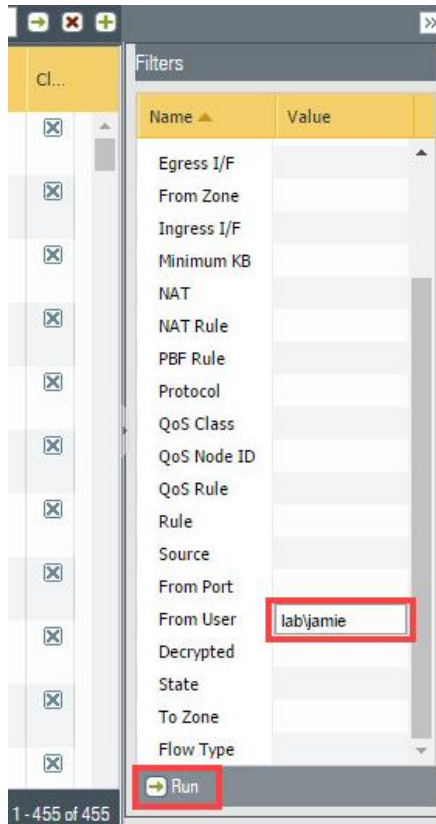
- Change focus to the firewall's web interface and navigate to **Monitor > Session Browser**.




2. Clear any existing filters and then click the **plus**  icon at the top-right of the window to open the *Filters* pane if not opened already.
3. Type **lab\jamie** in the *From User* field and then click **Run**.




Notice, you may need to zoom out for the **Run** button to be visible. Press **Ctrl** and **-** (the minus symbol) on the keyboard at the same time to zoom out. Once you press **Run** you can press **Ctrl** and **+** (the plus symbol) to zoom back in.



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 the *To User*. If a search for the user *lab\jamie* does not produce results, the session most likely has not completed and you will need to rerun the traffic generator.

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

	Start Time	From Zone	To Zone	Source	Destinat...	From Port	To Port	Proto...	Applica...	Rule	Ingress I/F
	20:12:59								browsing	simu... traffic	
	03/28 20:10:51	danger	danger	192.168...	72.14.2...	52214	443	6	google-base	dang... simu... traffic	ethern...

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

Star: Time	From Zone	To Zone	Source	Destinat...	From Port	To Port	Proto...	Applica...	Rule	Ingress I/F	Egress I/F	Bytes	Virtual System	C...
20:12:59								browsing	simu... traffic					
03/28 20:10:51	danger	danger	192.168...	72.14.2...	52214	443	6	google-base	dang... simu... traffic	ethern...	ethern...	12...	vsys1	<input checked="" type="checkbox"/>
<div> <div> <b>Detail</b> <div> <div>Session ID10316</div> <div>Time To Live15</div> <div>Virtual Systemvsys1</div> <div>Applicationgoogle-base</div> <div>Security Ruledanger-simulated-traffic</div> <div>URL Categorysearch-engines, low-risk</div> <div>QoS RuleN/A</div> <div>QoS Class4</div> <div>Created by sym cookieFalse</div> <div>To Host SessionFalse</div> <div>Traverse TunnelFalse</div> <div>Captive PortalFalse</div> <div>Session End LogTrue</div> <div>Session In AgeTrue</div> <div>Session From HAFalse</div> </div> </div> <div> <b>Flow 1</b> <div> <div>Directionc2s</div> <div>From Zonedanger</div> <div>Source192.168.3.131</div> <div>Destination72.14.213.102</div> <div>From Port52214</div> <div>To Port443</div> <div>From Userlab/iamie</div> <div>To Userunknown</div> <div>StateACTIVE</div> <div>TypeFLOW</div> </div> </div> <div> <b>Flow 2</b> <div> <div>Directions2c</div> <div>From Zonedanger</div> <div>Source72.14.213.102</div> <div>Destination192.168.3.131</div> <div>From Port443</div> <div>To Port52214</div> <div>From Userunknown</div> <div>To Userlab/iamie</div> <div>StateACTIVE</div> <div>TypeFLOW</div> </div> </div> </div>														




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 *QoS 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.

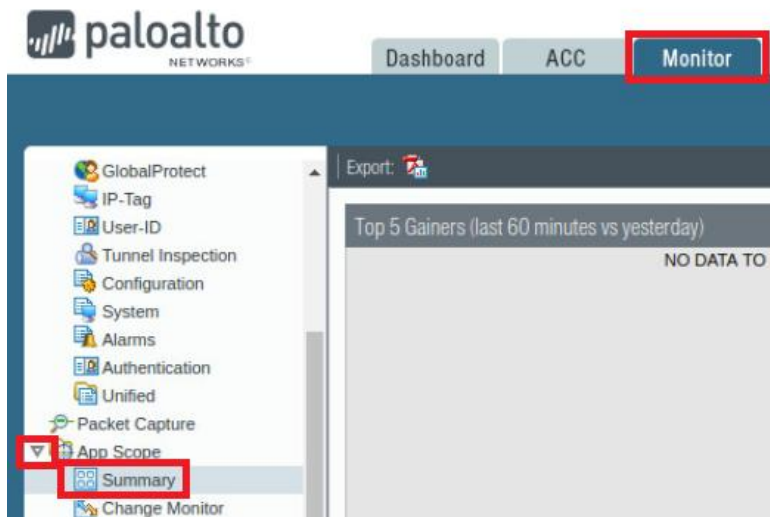


6. You can end an active session by clicking the **X**  icon at the far-right of a session row.
7. Leave the firewall web interface open to continue with the next task.

### 12.3 Explore the App Scope Reports

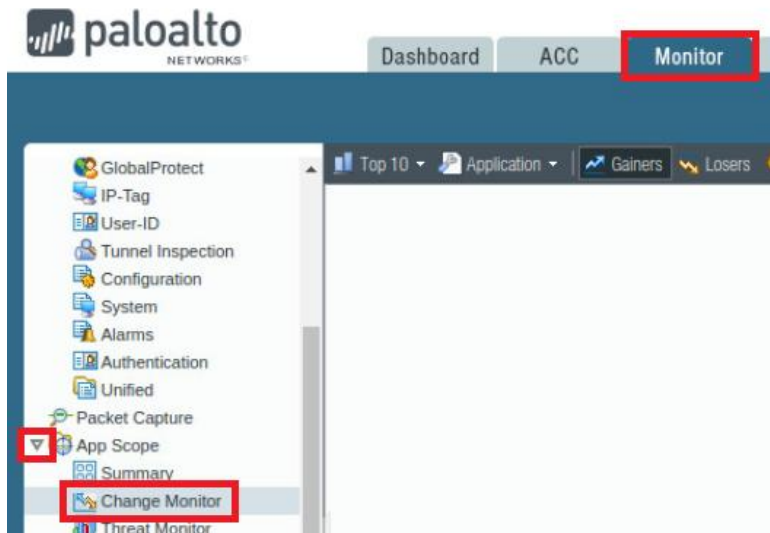
App Scope reports help you to quickly see if any application behavior is unusual or unexpected, which helps you to identify problematic behavior. Each report provides a dynamic, user-customizable window into the network. Long-term trends are difficult to represent in a lab environment. However, knowledge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

1. In the web interface, navigate to **Monitor > App Scope > Summary**.

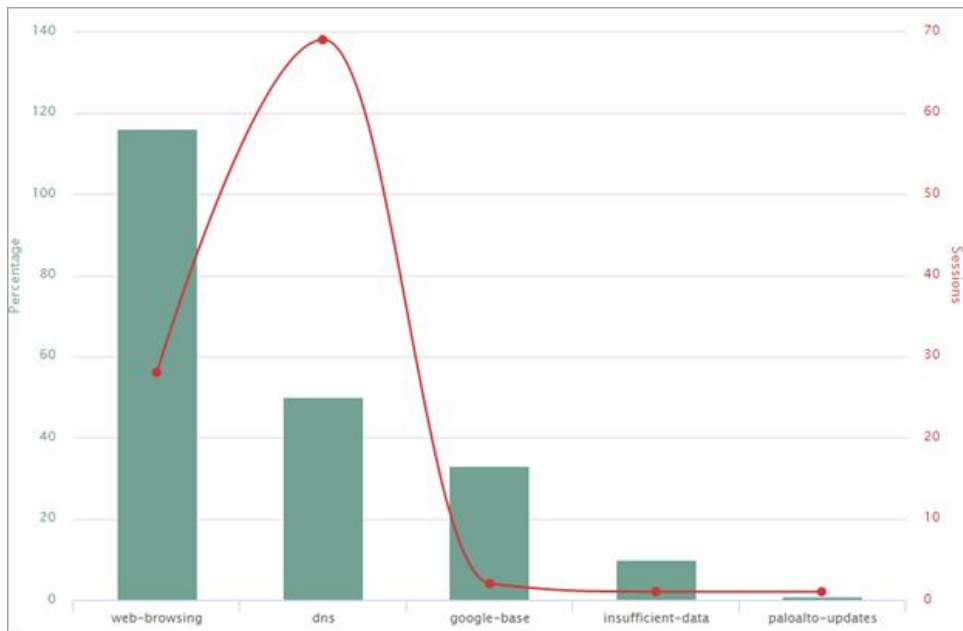


The *Summary* report displays charts for the top five gainers, losers, bandwidth-consuming source, App categories, and threats.

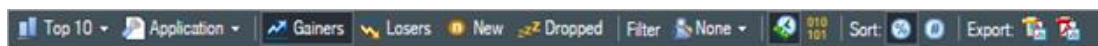
2. In the web interface, navigate to **Monitor > App Scope > Change Monitor**.



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.



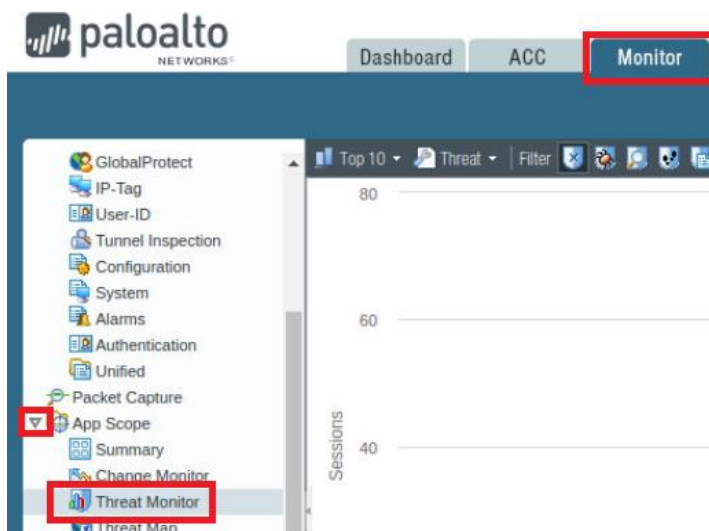
The type of information displayed can be controlled at the top. The displayed graph can be exported as a PDF or PNG.



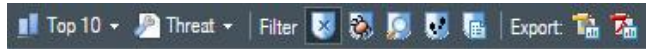
The time period also can be changed at the bottom.



3. In the web interface, navigate to **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.



The time period can be changed to the Last 6 hours, 12 hours, 24 hours, 7 days, or 30 days.



4. In the web interface, navigate to **Monitor > App Scope > Threat Map**.



5. Click **Last 30 Days** at the bottom of the screen.



6. At the top of the screen, click **Outgoing Threats**.





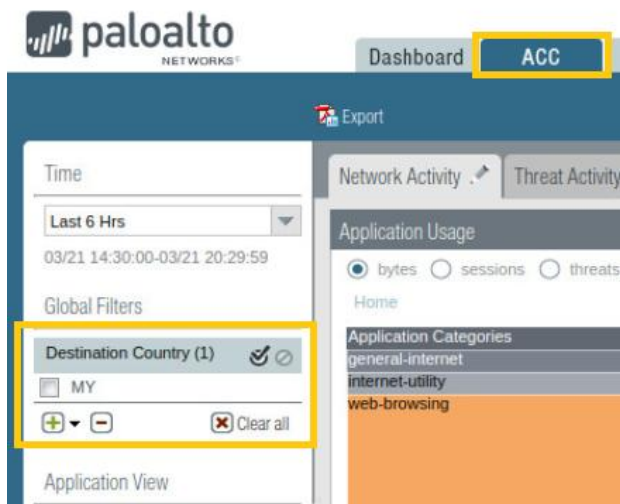
7. You now should see the geographical locations with threats and their average risk level.



8. Click a geographical location that has a dot showing the threats from the firewall, for example, Malaysia.



9. Notice the ACC opens with a global filter in the left pane referencing *Malaysia (MY)* or the geographical location you clicked.

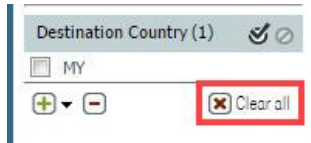




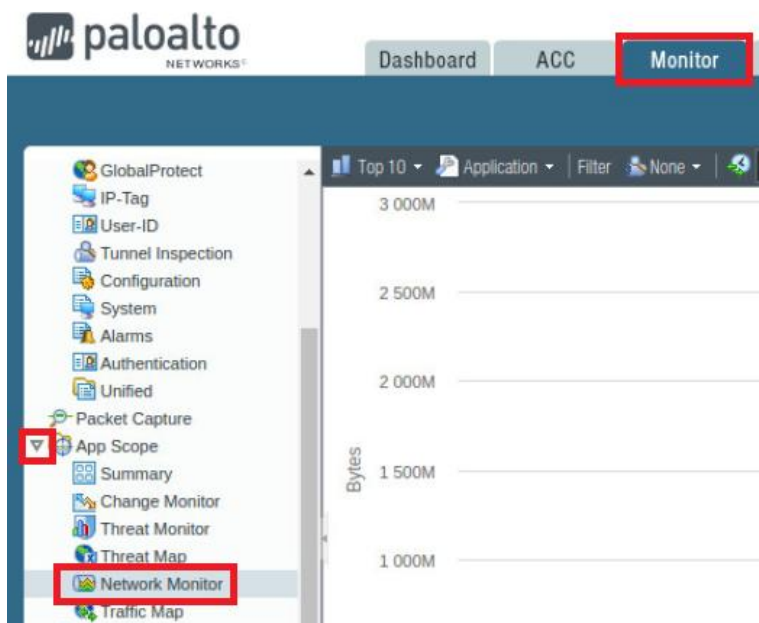


If the ACC does not open the first time you click on the geographical location, click on it once more and it should redirect you to the ACC panel.


10. Click the **Clear all** button to clear the *Global Filters*.



11. In the web interface, navigate to **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.

12. 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 to switch your view in the web interface to the *ACC* tab.

13. In the web interface, navigate to **Monitor > App Scope > Traffic Map**.



14. Change the view to show the **Last 7 days** by clicking the option at the bottom of the screen.



- The *Traffic Map* report shows a geographical view of traffic flows according to sessions or flows. Click **Outgoing Traffic** at the top of the screen.



- Leave the firewall web interface open to continue with the next task.

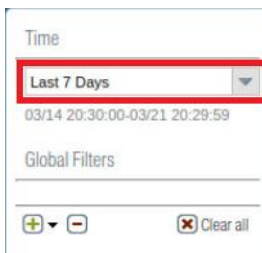
## 12.4 Explore the ACC

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

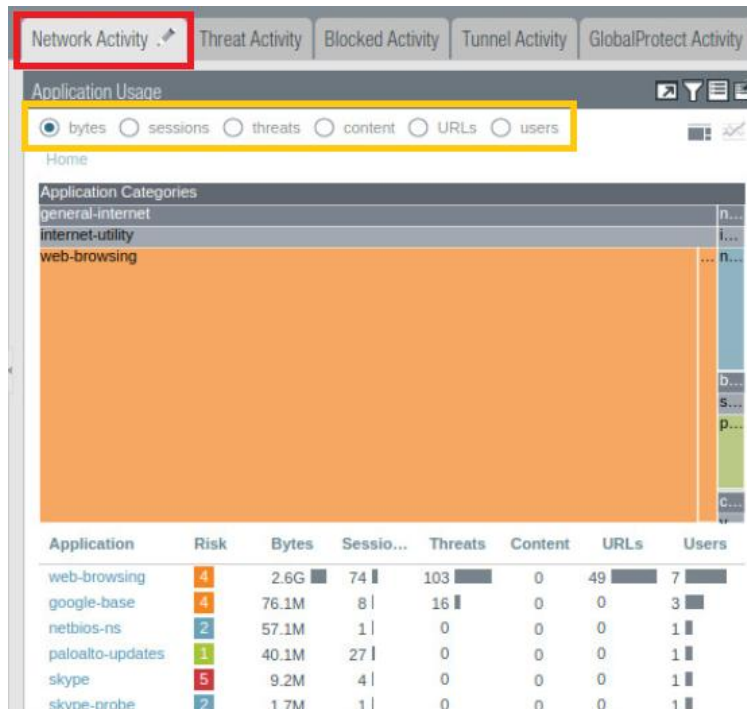
- In the web interface, click the **ACC** tab.



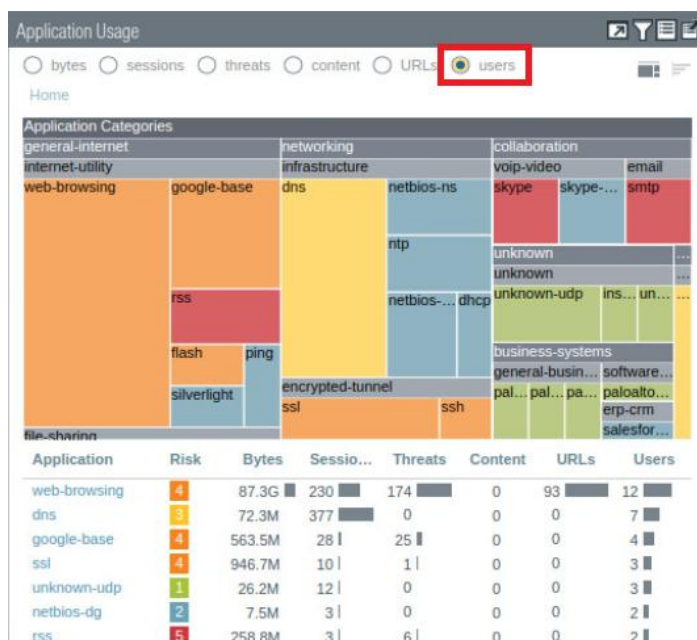
- In the left pane, click the **Time** dropdown list and select **Last 7 Days**.



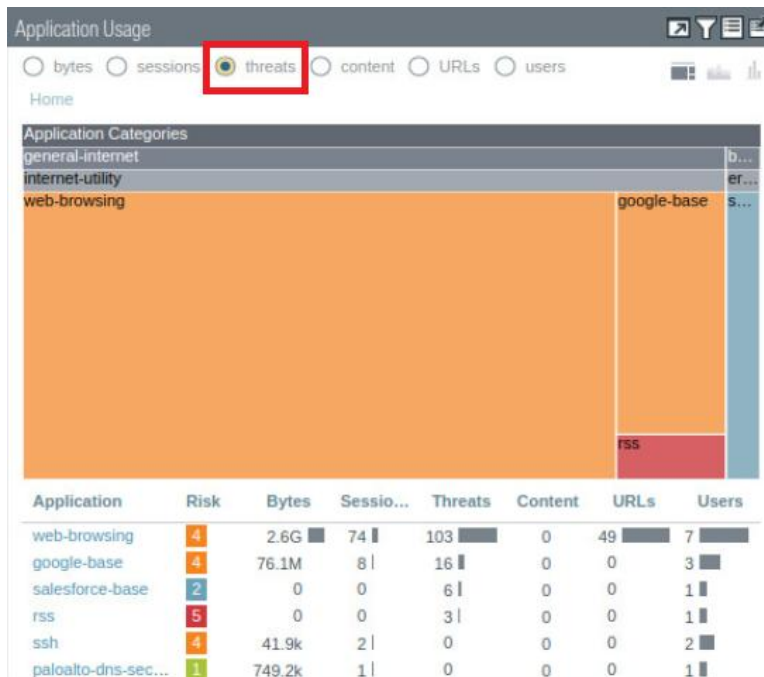
- Explore the information available on the **Network Activity** tab. This tab displays an overview of traffic and user activity on your network. It focuses on the top applications being used, the top users who generate traffic with detailed information about the bytes, content, threats, or URLs accessed by the user and the most used security rules against which traffic matches occur. Notice that in every pane, you can display data in bytes, sessions, threats, content, URLs, and users.



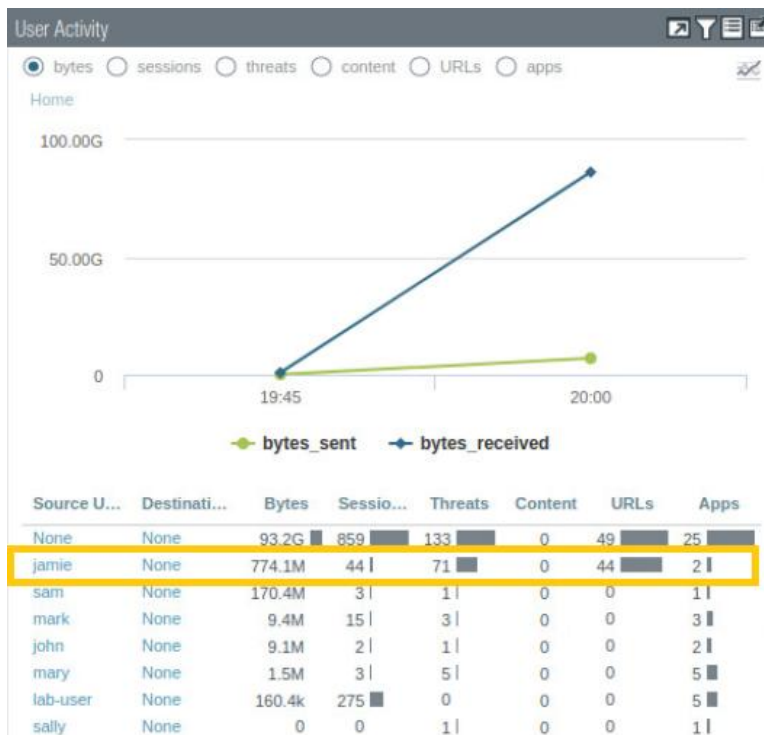
- Select the **users** option in the *Application Usage* widget. Notice how the application use seems more consistent across all colors versus bytes. This information indicates that one application does not supersede any other application in overall use by users.



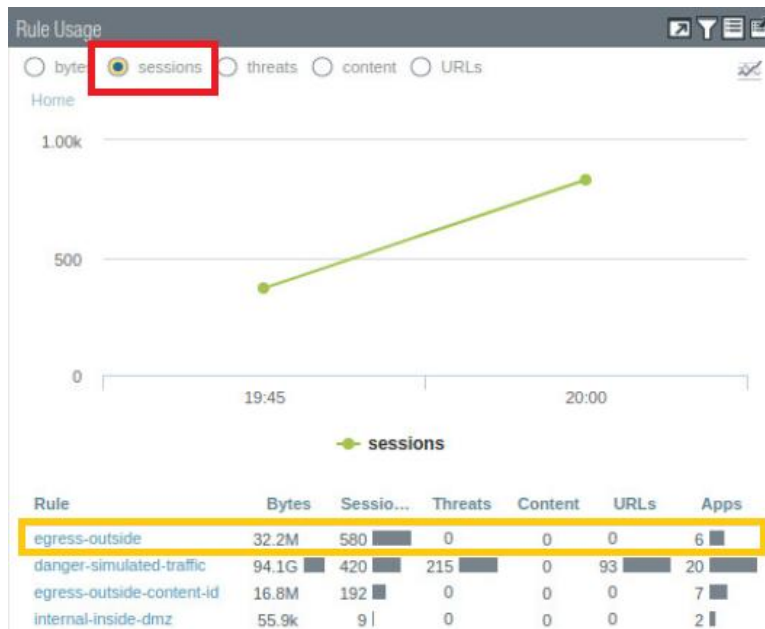
5. Select **threats** in the *Application Usage* widget.



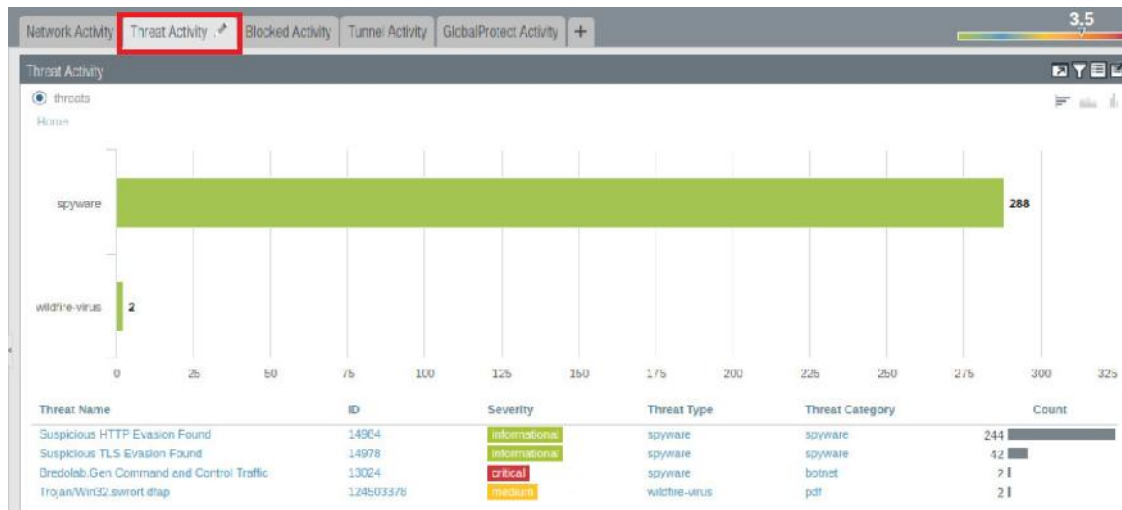
6. Focus your attention on the **User Activity** widget. The graph in the example shows that *Jamie* has consumed the most bandwidth.




7. Scroll down and focus your attention on the bottom-right **Policy Optimizer (Rule Usage)** widget and select the **sessions** radio button. The displayed information in the example shows that the most active rule, based on session count is *egress-outside*.



8. Click the **Threat Activity** tab.

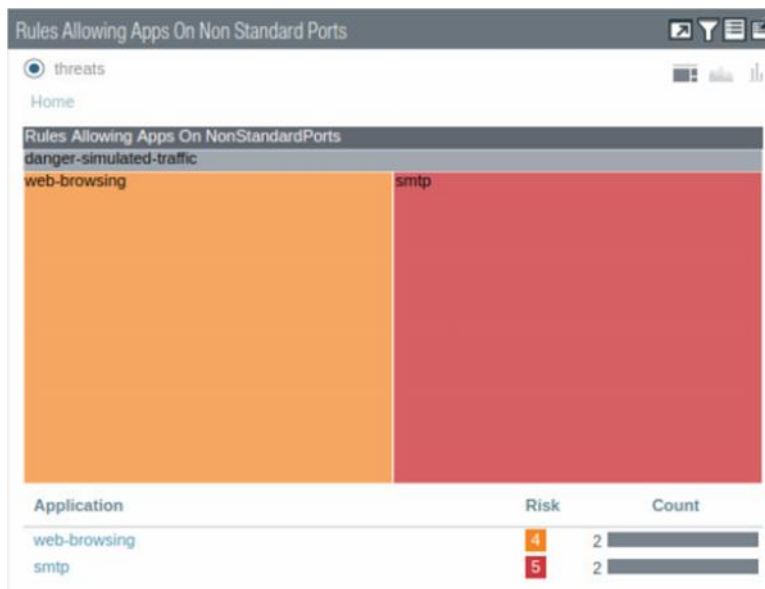


The *Threat* tab displays an overview of the threats on the network. It focuses on the top threats: vulnerabilities, spyware, viruses, hosts visiting malicious domains or URLs, top *WildFire* submissions by file type and application, and applications that use non-standard ports.

9. Locate the **Global Filters** on the left side of the ACC and click the **plus** icon  and go to **Threat > Severity**. Add **critical** and **medium** to the *Global Filters*. Notice that the graph updates to display only critical and medium severities.



10. Scroll down to the bottom-right and notice the **Rules Allowing Apps On Non Standard Ports** widget. This pane is helpful for identifying rules that need to enforce the application-default service setting.



11. Leave the firewall web interface open to continue with the next task.




## 12.5 Investigate the Traffic



1. In the web interface, navigate to **Monitor > Logs > Threat**.



2. Clear any existing filters and type **(severity neq informational)** into the log filter text box, followed by pressing the **Enter** key.



3. Locate the first entry referencing the source user *john* and see which threat type and filename is associated with user *john*. Click on the **detailed log view**  icon for this entry.

	Receive Time	Type	Name	From Zone	To Zone	Source address	Source User
	03/28 20:10:32	wildfire-virus	Trojan/Win32.sworrt.dfap	danger	danger	10.10.10.10	lab\sally
	03/28 20:10:21	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2	lab\john

4. Notice at the bottom of the *Detailed Log View* should be the associated threat entries. View the information to see which thread type and filename is associated with the user *john* and then click **Close**.

**Detailed Log View**

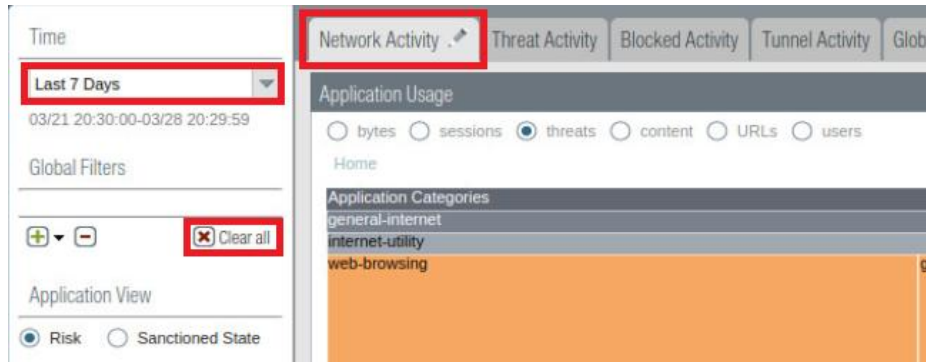
General		Source		Destination	
Session ID	54584	Source User	lab\john	Destination User	
Action	alert	Source	192.168.0.2	Destination	112.137.162.134
Application	web-browsing	Country	192.168.0.0-192.168.255.255	Country	Malaysia
Rule	danger-simulated-traffic	Port	1038	Port	80
Rule UUID	69349207-dcf6-40fd-bcf5-2d8ad54d9069	Zone	danger	Zone	danger
Device SN		Interface	ethernet1/4	Interface	ethernet1/5
IP Protocol	tcp				
Log Action					
Generated Time	2020/03/28 20:10:21				
Receive Time	2020/03/28 20:10:21				
Tunnel Type	N/A				
		<b>Details</b> Threat Type: spyware Threat Name: Bredolab.Gen Command and Control Traffic			

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2020/03/28 20:29:13	end	web-browsing	allow	danger-simula... traffic	69349...	99...		high-risk				
	2020/03/28 20:10:21	spyware	web-browsing	alert	danger-simula... traffic	69349...		critical	high-risk				contro...

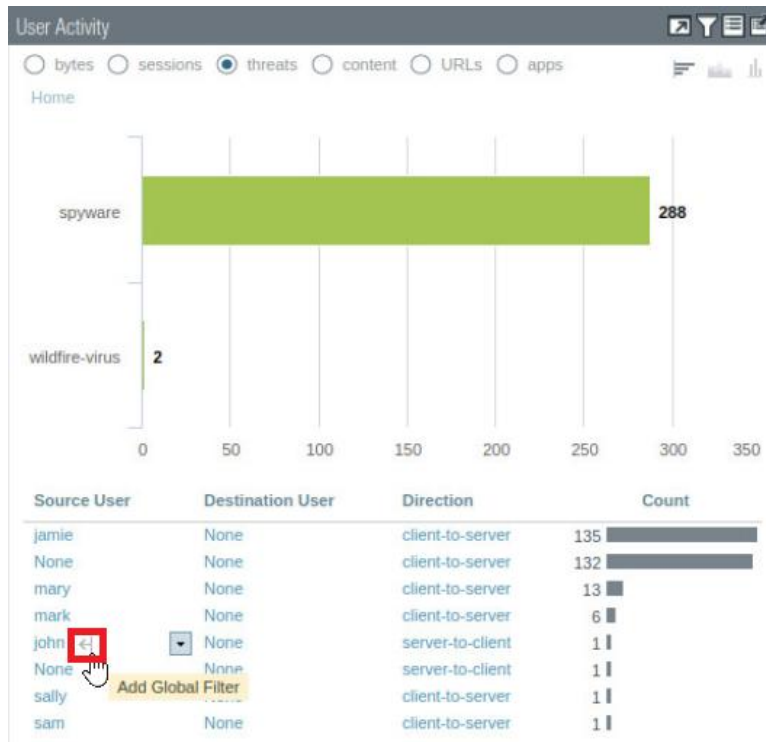
**Close**



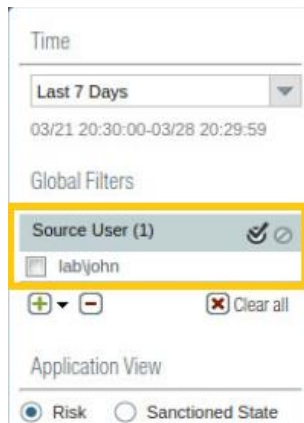
- Click on the **ACC** tab.
- Select the **Network Activity** tab and remove any existing global filters. Ensure that the **Time** dropdown list is **Last 7 Days**.



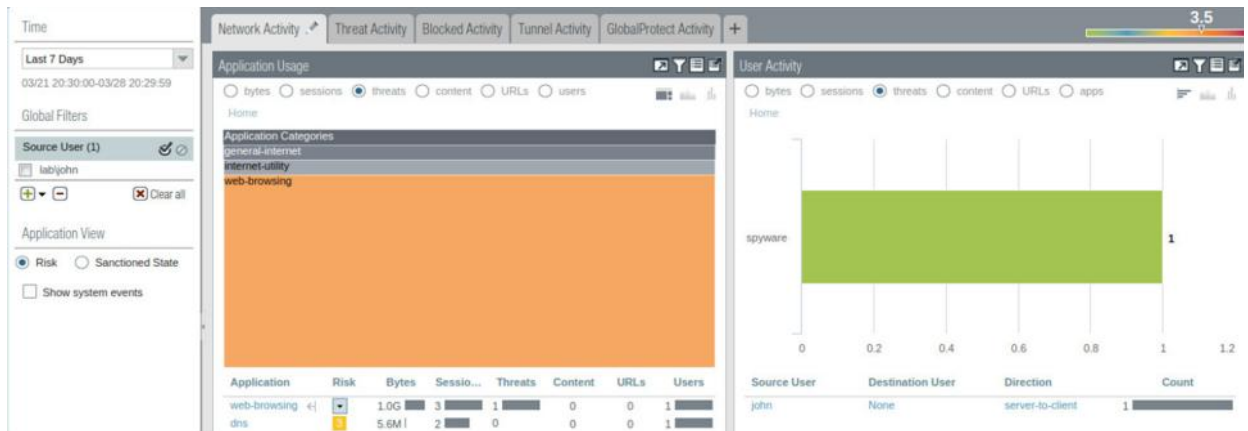
- Focus on the **User Activity** pane and hover your mouse over **john**, then proceed to click the **left-arrow** to promote *john* to the *Global Filter*.



8. In the left pane, ensure that *john* was promoted to a *Global Filter*.



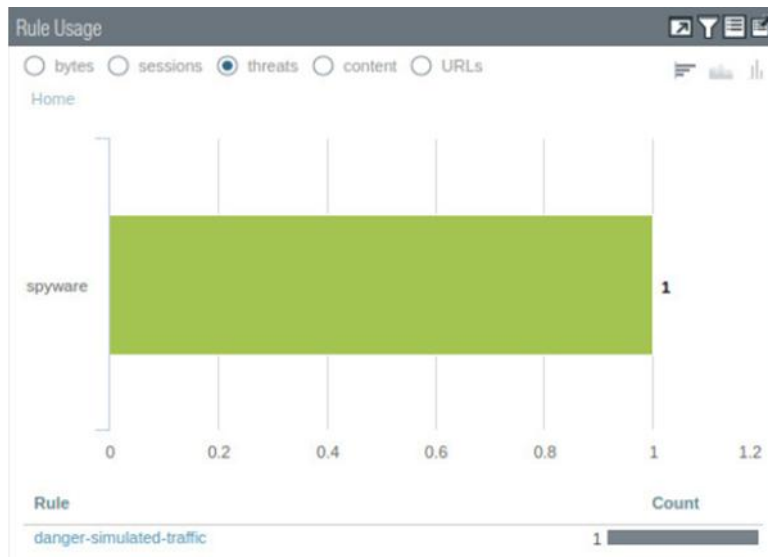
9. Notice that all window panes have been updated to only show information based on *john*. Also, notice that *john* is shown to be associated with *web-browsing* traffic.



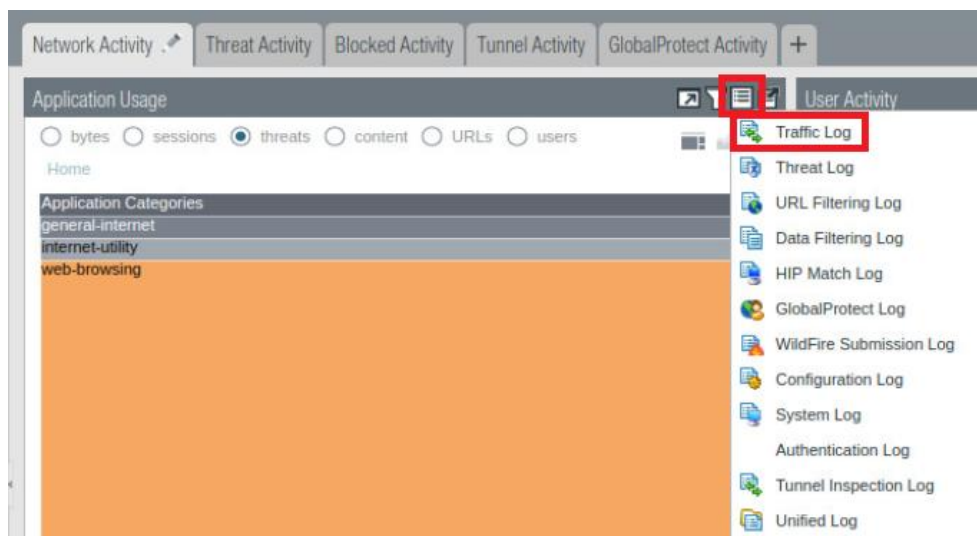
10. Scroll down and locate the **Destination Regions** pane. Notice that this is associated with the country *Malaysia*.



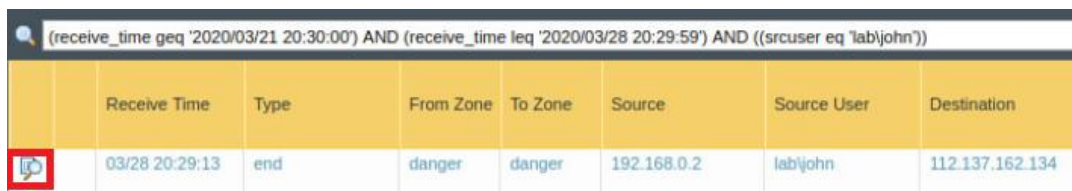
11. Scroll down further to the **Policy Optimizer (Rule Usage)** pane. Notice that only one rule allowed this traffic. If we were in a production environment, inspection should be done to ensure that this rule is operating effectively.




12. Scroll to the upper-left **Application Usage** pane. Click the **Jump to Logs** icon and select **Traffic Log**.



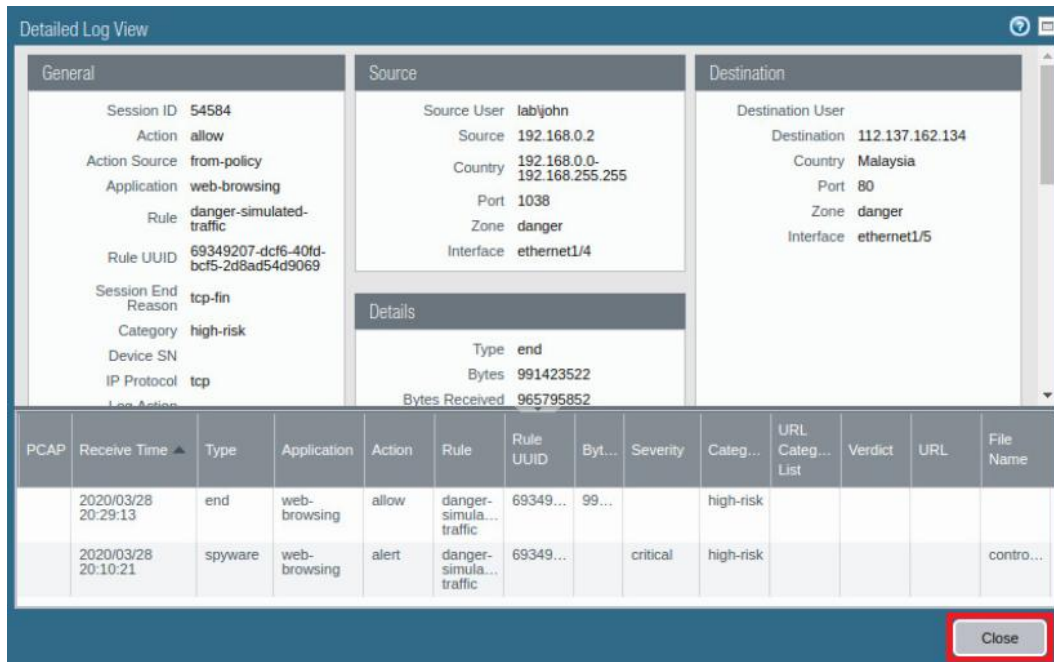
13. Notice that the web interface switched views to the Traffic log with a predefined filter. Select the **Detailed Log view** icon for the entry.



The Traffic Log view displays a table of log entries. A search filter is applied: `(receive_time geq '2020/03/21 20:30:00') AND (receive_time leq '2020/03/28 20:29:59') AND ((srcuser eq 'labjohn'))`. The table has columns for Receive Time, Type, From Zone, To Zone, Source, Source User, and Destination. A red box highlights the 'Detailed Log view' icon for the first entry.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	03/28 20:29:13	end	danger	danger	192.168.0.2	labjohn	112.137.162.134

14. In the *Detailed Log View* window, notice at the bottom the associated threat entries. Click **Close**.



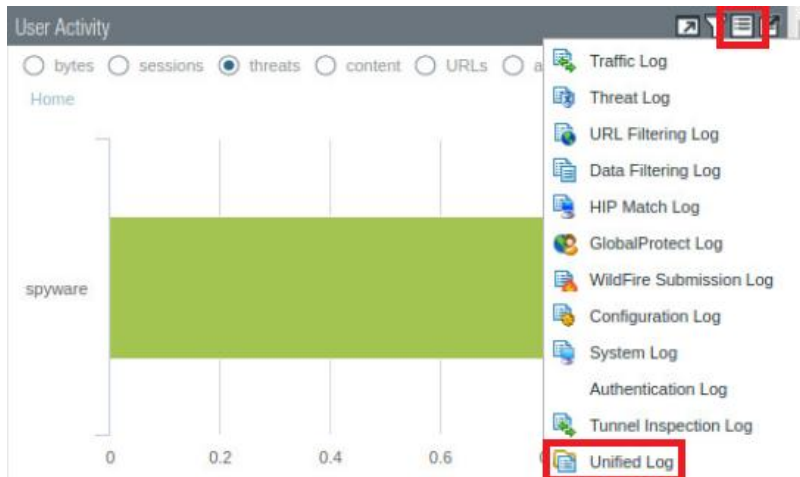
The **Detailed Log View** window displays session information and threat entries. The **General** tab shows session details, the **Source** tab shows source information, and the **Destination** tab shows destination information. The **Details** tab shows session end reason and category. The bottom table lists threat entries.

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ...	Verdict	URL	File Name
	2020/03/28 20:29:13	end	web-browsing	allow	danger-simula...	69349...	99...		high-risk				
	2020/03/28 20:10:21	spyware	web-browsing	alert	danger-simula...	69349...		critical	high-risk				contro...

A **Close** button is located at the bottom right of the window.

15. Click on the **ACC** tab.


16. On the **User Activity** pane, click the **Jump to Logs** icon and select the **Unified Log**.





The **User Activity** pane shows a bar chart with a green bar labeled "spyware". A dropdown menu is open, showing a list of logs. The **Unified Log** option is highlighted.

- Traffic Log
- Threat Log
- URL Filtering Log
- Data Filtering Log
- HIP Match Log
- GlobalProtect Log
- WildFire Submission Log
- Configuration Log
- System Log
- Authentication Log
- Tunnel Inspection Log
- Unified Log**

17. Notice that the Traffic and Threat logs now are in one unified display, which can help correlation activities.



The **Unified Log** display shows a search bar with the query: `(receive_time geq '2020/03/21 20:45:00') AND (receive_time leq '2020/03/28 20:44:59') AND ((srcuser eq 'labjohn'))`. The table below shows the results.

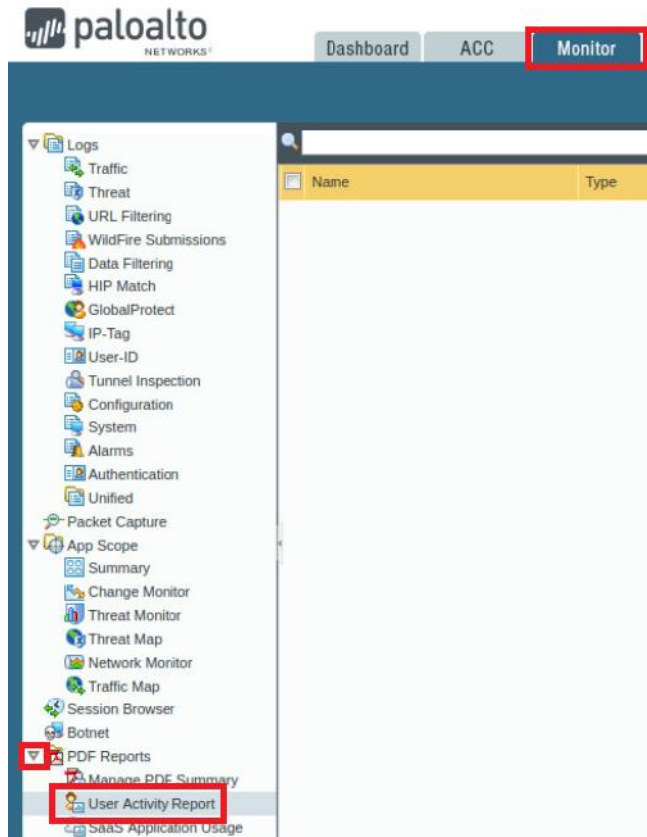
	Log Type	Receive Time	Log Subtype	Session ID	Source Zone	Destinati... Zone	Source address	Source User	Destination address
	traffic	03/28 20:29:13	end	54584	danger	danger	192.168.0.2	labjohn	112.137.162.134
	traffic	03/28 20:27:49	end	10347	danger	danger	192.168.0.2	labjohn	112.137.162.134

18. Leave the firewall web interface open to continue with the next task.

## 12.6 Generate a User Activity Report

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

1. In the web interface, navigate to **Monitor > PDF Reports > User Activity Report**.

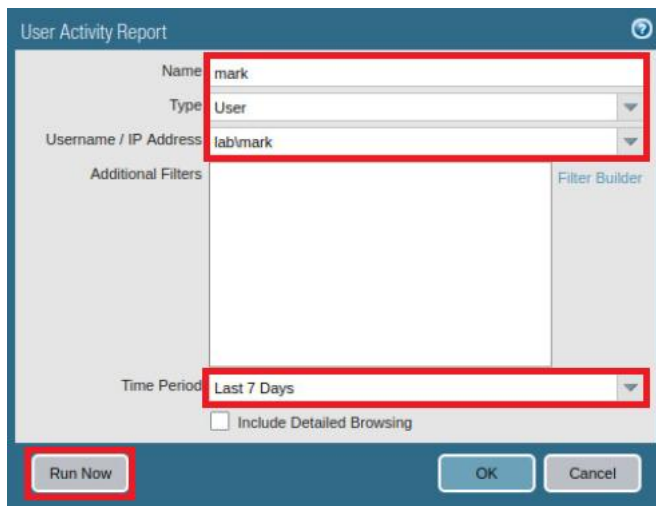


2. Click **Add** to define a new user activity report.



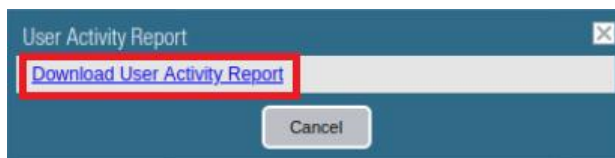
3. In the *User Activity Report* window, enter the following. Once finished, click **Run Now**.

Parameter	Value
Name	Type mark
Type	Verify that the <b>User</b> radio button is selected
Username / IP Address	Type <b>tab\mark</b>
Time Period	Select <b>Last 7 days</b> from the dropdown list

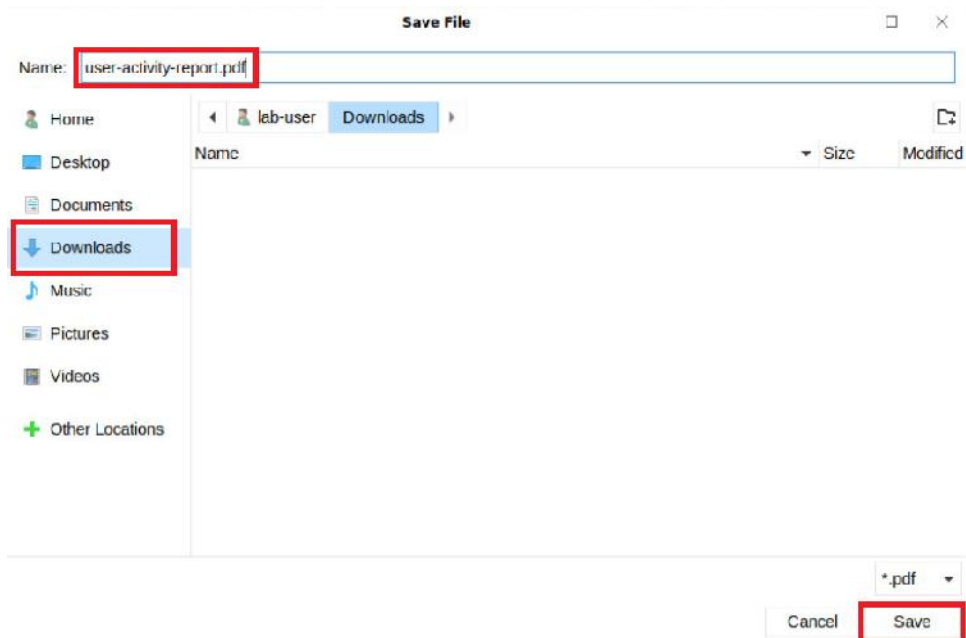


The 'User Activity Report' dialog box is shown. It has a blue header bar with a question mark icon. The main area is divided into two columns. The left column contains fields for 'Name' (text input with 'mark'), 'Type' (dropdown menu with 'User'), and 'Username / IP Address' (text input with 'lab/mark'). Below these is a large empty box labeled 'Additional Filters'. The right column is labeled 'Filter Builder'. At the bottom, there is a 'Time Period' dropdown menu set to 'Last 7 Days', an unchecked checkbox for 'Include Detailed Browsing', and three buttons: 'Run Now', 'OK', and 'Cancel'. Red boxes highlight the 'Name', 'Type', 'Username / IP Address' fields, the 'Time Period' dropdown, and the 'Run Now' button.

- Click the **Download User Activity Report** link and open the report when it finishes downloading to the local system.



- In the *Save File* window, save the report to the **Downloads** directory and click **Save**.



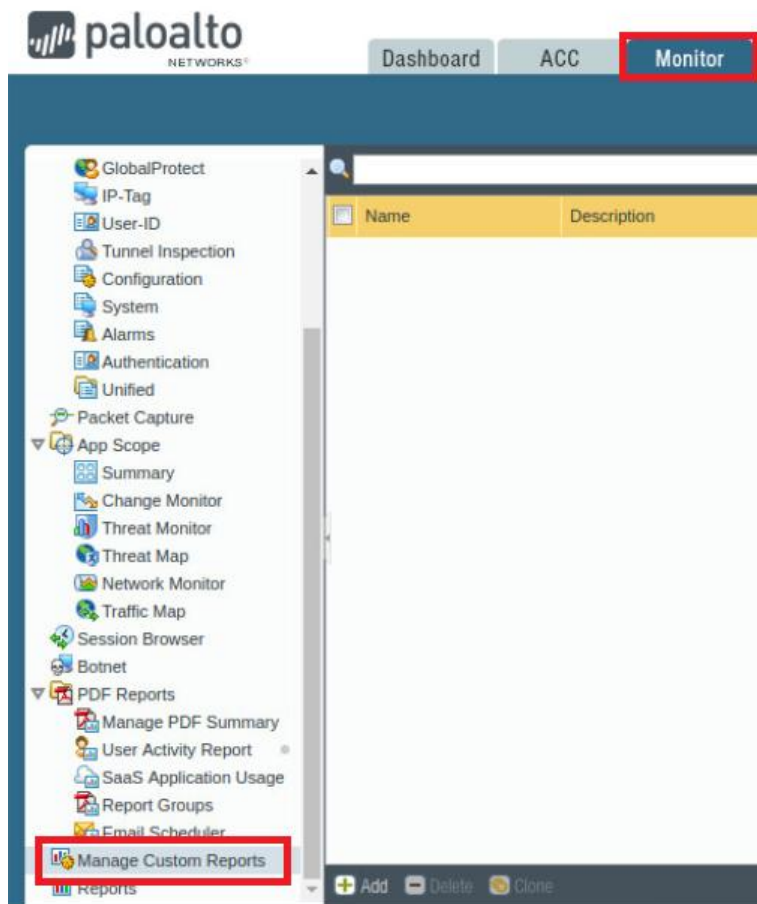
- In the bottom-left corner of the *Chrome* browser window, click the report to open the report.



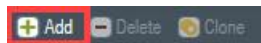
7. Browse through the report to get familiar with the presented information. You can also include a detailed browsing history that will include an approximate time a user spends on a website (this information is not available when a group is specified instead of an individual user). Close the report browser tab when finished.
8. Back on the firewall's web interface, click **Cancel** to close the *User Activity Report* window.
9. Click **OK** to close the *User Activity Report* configuration window.

## 12.7 Create a Custom Report

1. In the web interface, navigate to **Monitor > Manage Custom Reports**.



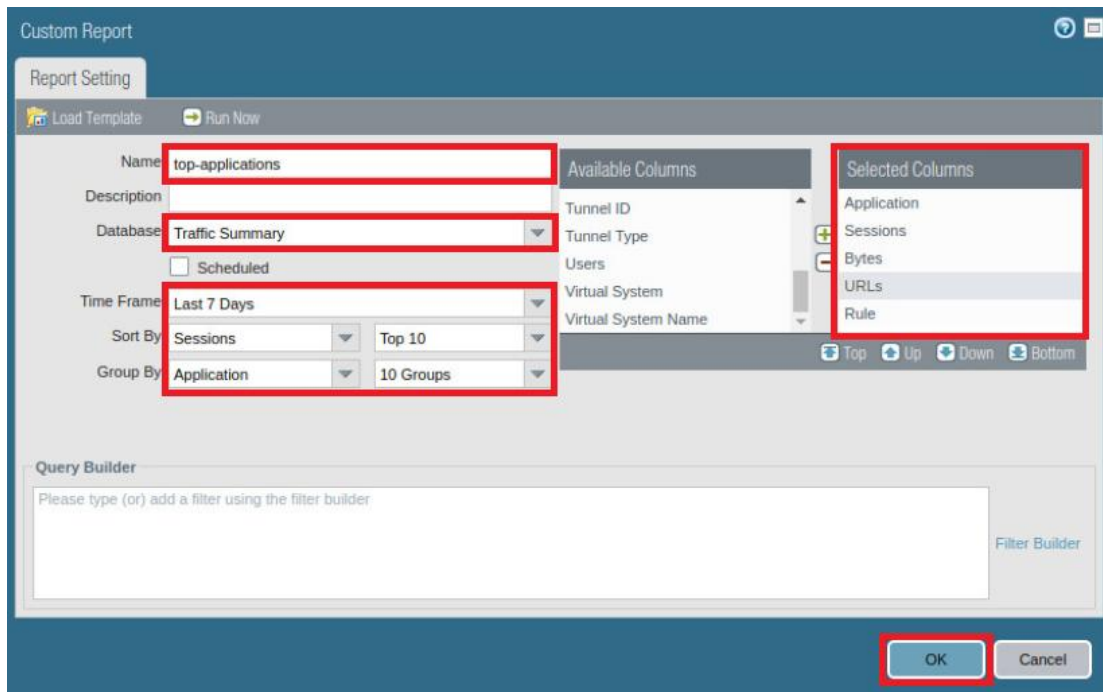
2. Click **Add** to define a new *Custom Report*.





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

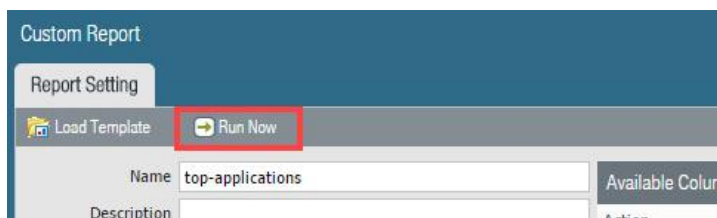
Parameter	Value
Name	Type <b>top-applications</b>
Database	Select <b>Summary Databases &gt; Traffic</b> from the dropdown list
Time Frame	Select <b>Last 7 Days</b> from the dropdown list
Sort By	Select <b>Sessions</b> and <b>Top 10</b> from the dropdown list
Group By	Select <b>Application</b> and <b>10 Groups</b> from the dropdown list
Selected Columns	Move <b>Application, Sessions, Bytes, URLs, and Rule</b> to the <i>Selected Columns</i> pane



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

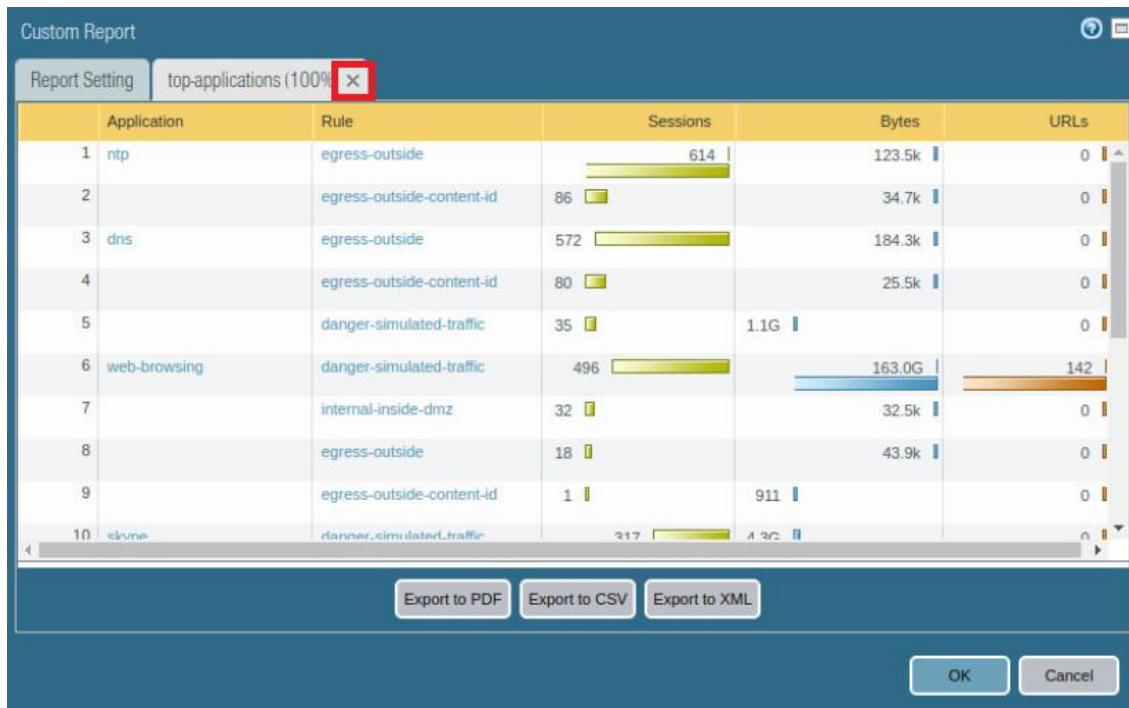
<input type="checkbox"/>	Name	Description	Database	Time Frame
<input checked="" type="checkbox"/>	<b>top-applications</b>		Traffic Summary	Last 7 Days

5. Click **Run Now** to generate the report. The report will appear in a new tab in the *Custom Report* window.

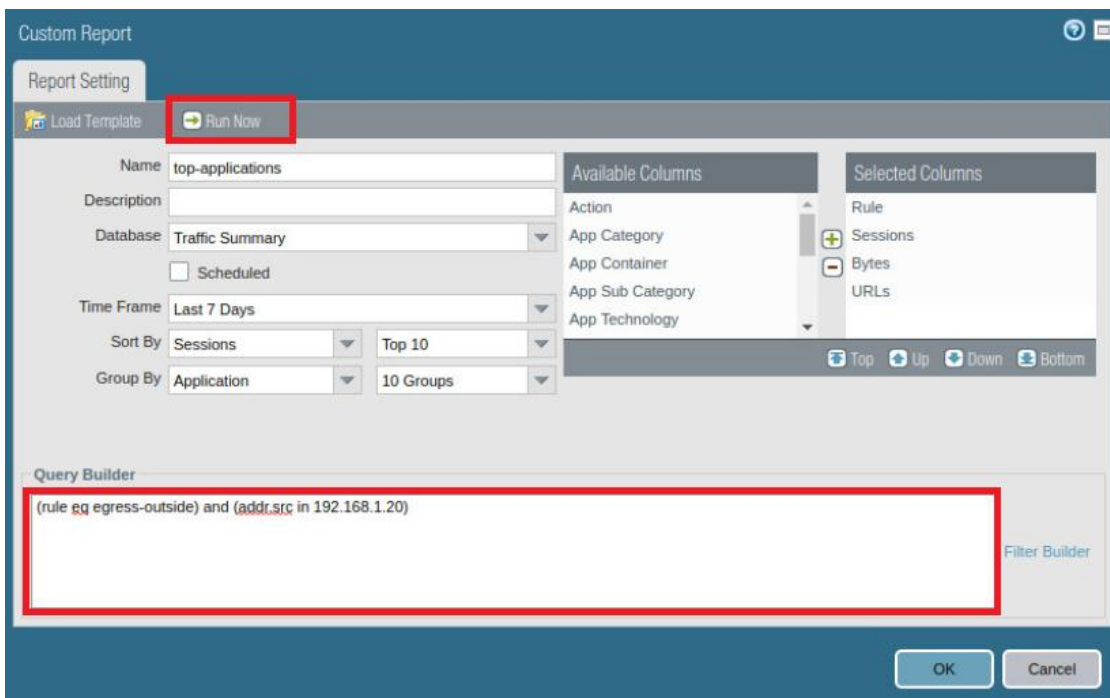




6. Close the **top-applications** tab containing the report.



7. 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**) and then click **Run Now** to run the report again, this time with the query.



Custom Report

Report Setting

Load Template Run Now

Name: top-applications

Description:

Database: Traffic Summary

☐ Scheduled

Time Frame: Last 7 Days

Sort By: Sessions Top 10

Group By: Application 10 Groups

Available Columns:

- Action
- App Category
- App Container
- App Sub Category
- App Technology

Selected Columns:

- Rule
- Sessions
- Bytes
- URLs

Query Builder

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

Filter Builder

OK Cancel

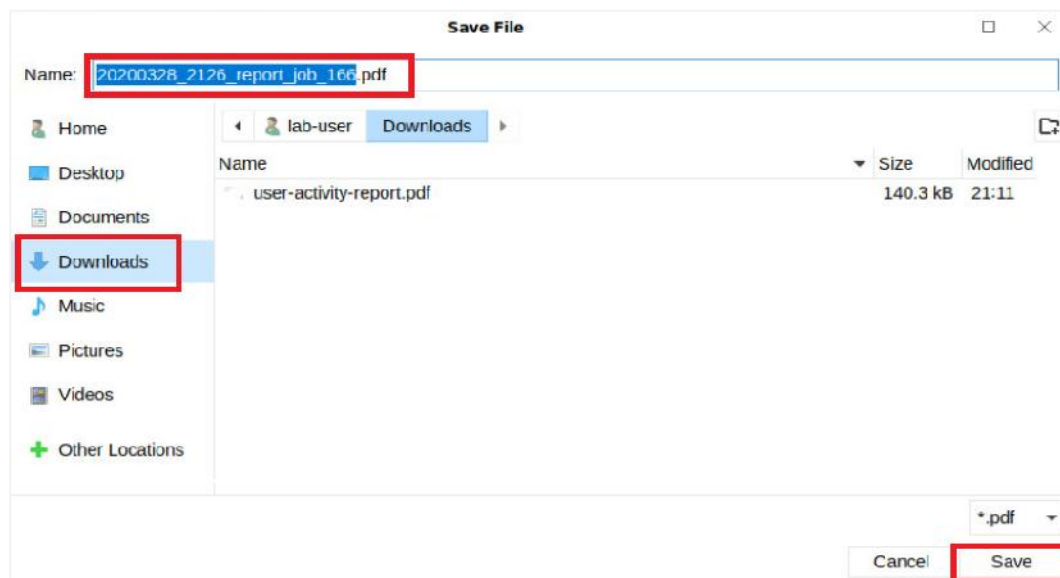
8. Click **Export to PDF** to save the report as a PDF.



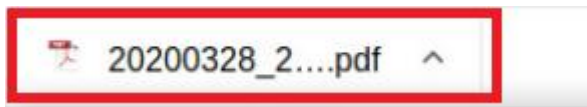
9. If you receive a warning that a pop-up was blocked, click on the **notification icon** and select the **Always allow pop-ups** radio button, then click **Done**.



10. Click on the **Export to PDF** button once more.
11. In the *Save File* window, save the report to the **Downloads** directory and click **Save**.



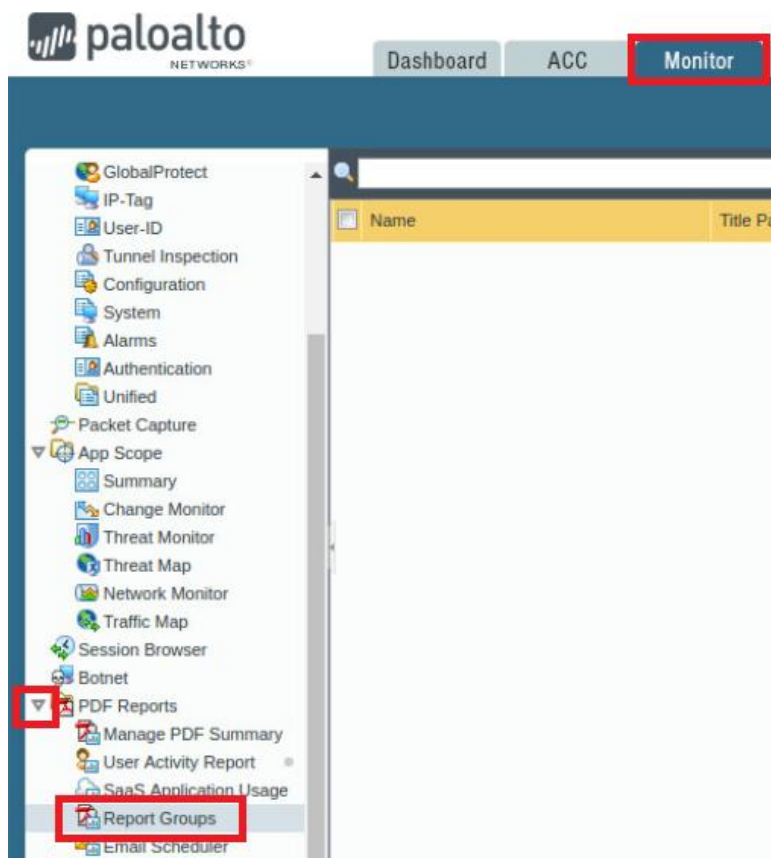
12. In the bottom-left corner of the *Chrome* browser window, click the report to open the report.



13. Review the report and browser tab when finished.
14. Back on the firewall's web interface, click **OK** to close the *Custom Report* window.
15. Leave the firewall web interface open to continue with the next task.

## 12.8 Create a Report Group

1. In the web interface, navigate to **Monitor > PDF Reports > Report Groups**.

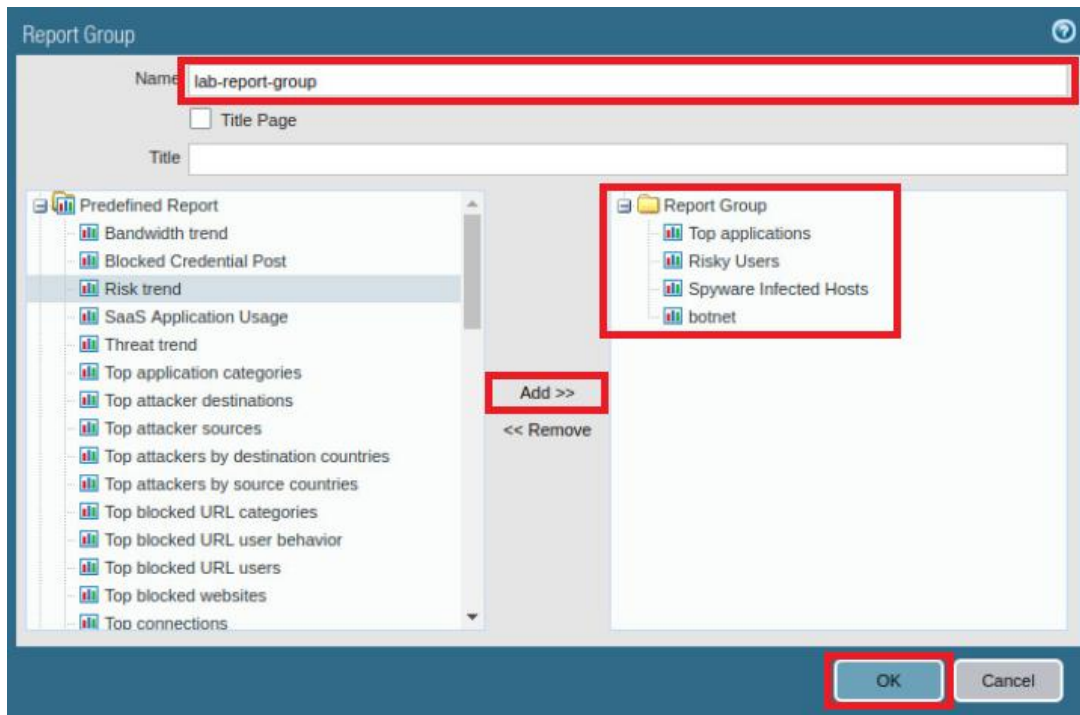


2. Click **Add** to define a new report group.



3. In the *Report Group* window, fill out the following and then click **OK**.

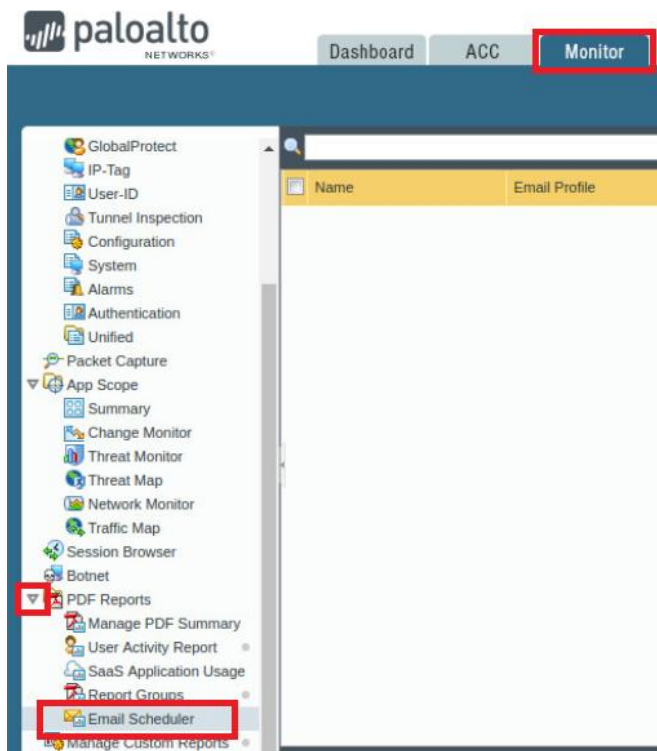
Parameter	Value
Name	Type lab-report-group
Reports	Add the following: <b>Top Applications</b> <b>Risky Users</b> <b>Spyware Infected Hosts</b> <b>botnet</b>



4. Leave the firewall web interface open to continue with the next task.

## 12.9 Schedule a Report Group Email

1. In the web interface, navigate to **Monitor > PDF Reports > Email Scheduler**.

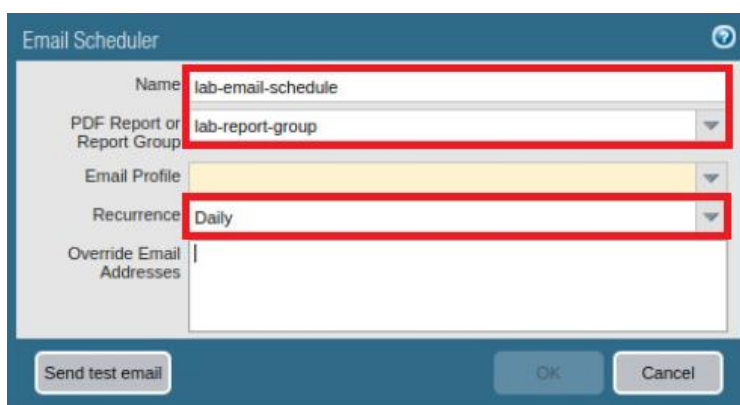


2. Click **Add** to define a new email schedule.

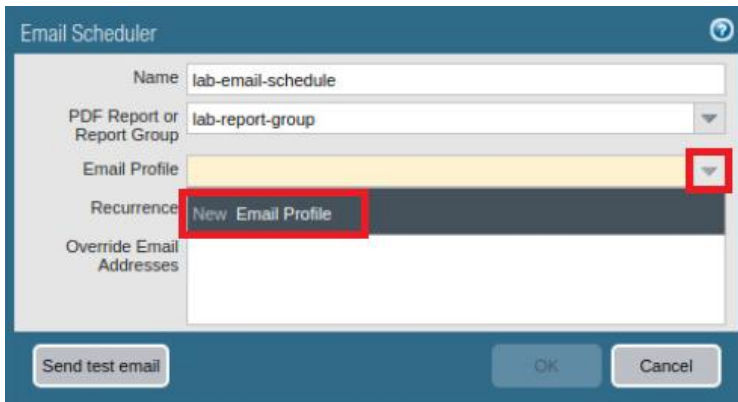


3. In the *Email Scheduler* window, fill out the following.

Parameter	Value
Name	Type <b>lab-email-schedule</b>
Report Group	Select <b>lab-report-group</b> from the dropdown list
Recurrence	Select <b>Daily</b> from the dropdown list



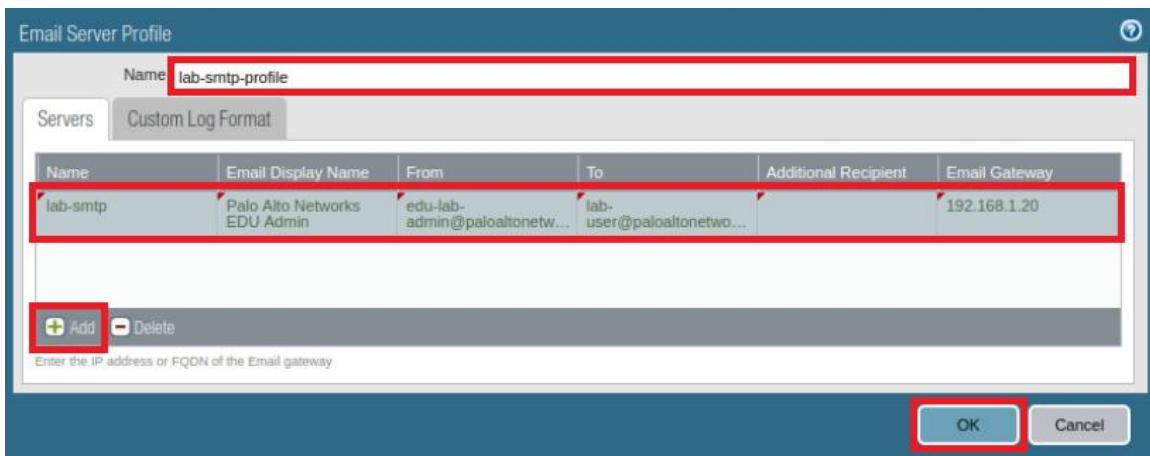
- In the *Email Scheduler* window, select **New Email Profile** from the *Email Profile* dropdown list.



The screenshot shows the 'Email Scheduler' window. The 'Name' field contains 'lab-email-schedule'. The 'PDF Report or Report Group' dropdown is set to 'lab-report-group'. The 'Email Profile' dropdown is open, and 'New Email Profile' is highlighted. The 'Recurrence' field is empty. The 'Override Email Addresses' field is empty. At the bottom, there are buttons for 'Send test email', 'OK', and 'Cancel'.

- Notice the *Email Server Profile* window appears. Type **lab-smtp-profile** into the *Name* text field. Click **Add** and configure the following.

Parameter	Value
Name	Type lab-smtp
Email Display Name	Type Palo Alto Networks EDU Admin
From	Type edu-lab-admin@paloaltonetworks.com
To	Type lab-user@paloaltonetworks.com
Email Gateway	Type 192.168.1.20



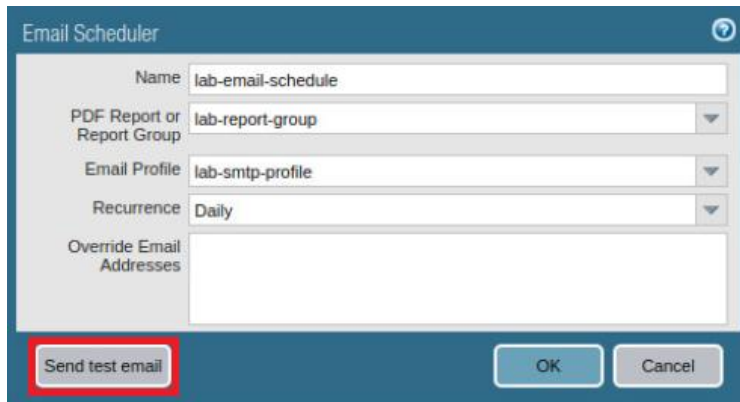
The screenshot shows the 'Email Server Profile' window. The 'Name' field contains 'lab-smtp-profile'. The 'Servers' tab is selected. Below the tab, there is a table with the following data:

Name	Email Display Name	From	To	Additional Recipient	Email Gateway
lab-smtp	Palo Alto Networks EDU Admin	edu-lab-admin@paloaltonetw...	lab-user@paloaltonetwo...		192.168.1.20

At the bottom left, there are 'Add' and 'Delete' buttons. Below the table, there is a text input field with the placeholder 'Enter the IP address or FQDN of the Email gateway'. At the bottom right, there are 'OK' and 'Cancel' buttons.

- Click **OK** to close the *Email Server Profile* window.

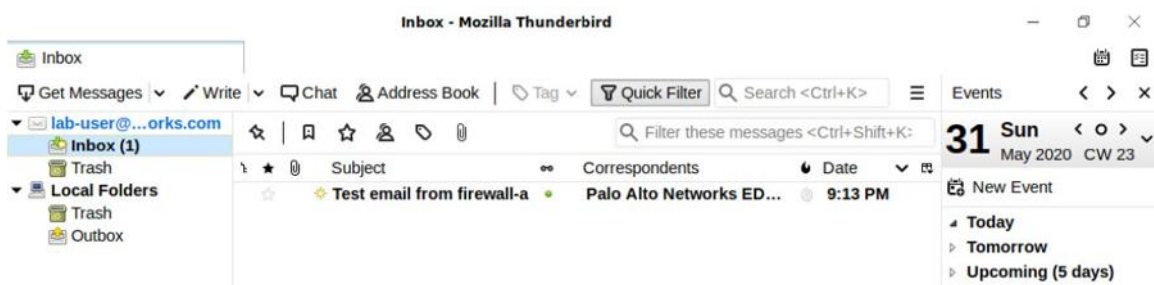
- Back on the *Email Scheduler* window, click **Send test email**. A test email will be sent to the address you provided. Wait for and confirm its arrival.



The **Email Scheduler** dialog box is shown. It has a blue title bar with a question mark icon. The fields are: Name (lab-email-schedule), PDF Report or Report Group (lab-report-group), Email Profile (lab-smtp-profile), Recurrence (Daily), and Override Email Addresses (empty). At the bottom, there are three buttons: **Send test email** (highlighted with a red rectangle), **OK**, and **Cancel**.

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

- On the Client desktop, double-click the **Thunderbird Mail** icon.
- Review the **Test email from firewall-a** email.



- The lab is now complete; you may end the reservation.