PALO ALTO NETWORKS EDU-210

Lab 12: Monitoring and Reporting

Document Version: 2020-01-22

Contents

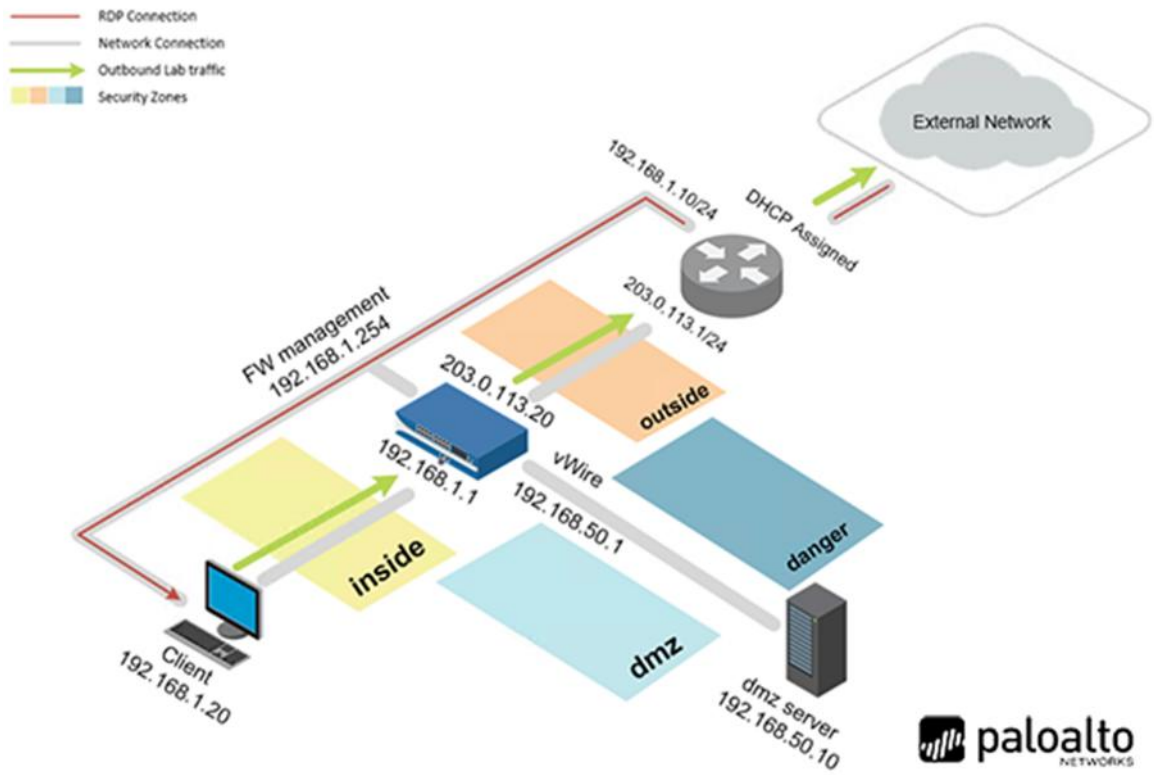
Introduction

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 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`	`Pal0Alt0`
Firewall	192.168.1.254	`admin`	`admin`

1 Monitoring and Reporting

1.0 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.

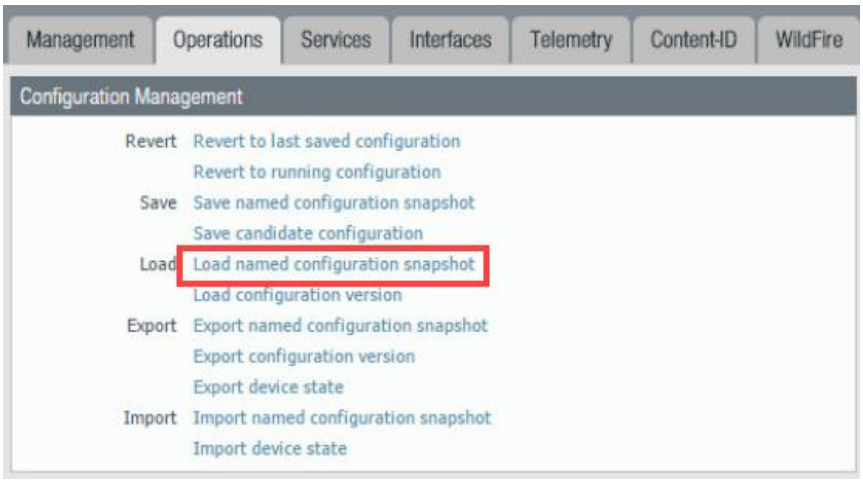
2. Click within the splash screen to bring up the login screen. Log in as **`lab-user`** using the password **`Pal0Alt0`**.

3. Launch the **Chrome** 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:

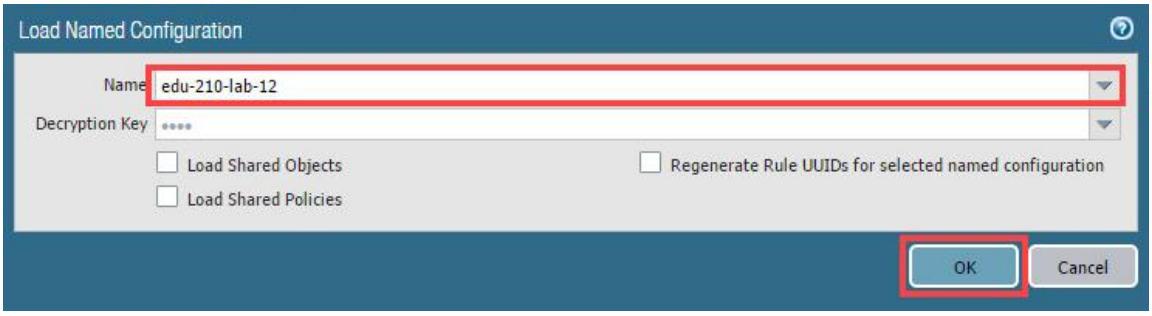
Parameter	Value
Name	**`admin`**
Password	**`admin`**

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

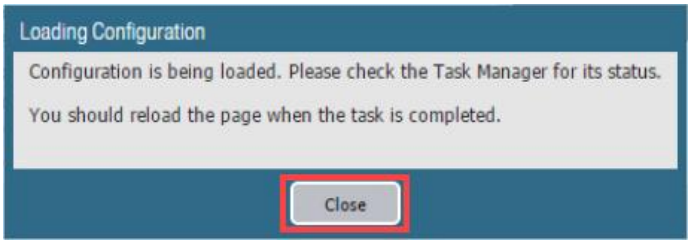
7. Click **Load named configuration snapshot**:



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

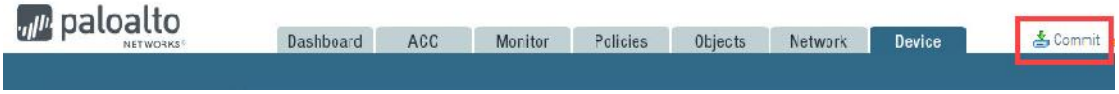


9. Click **Close**.

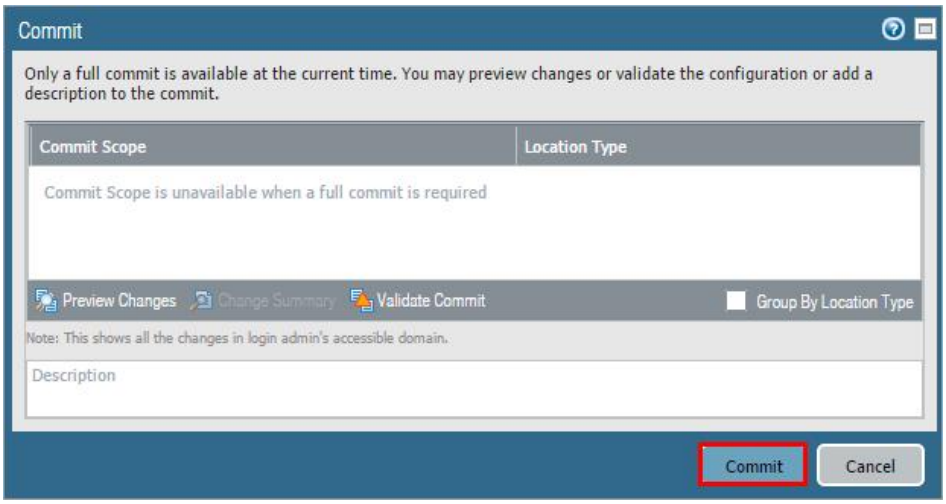


The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

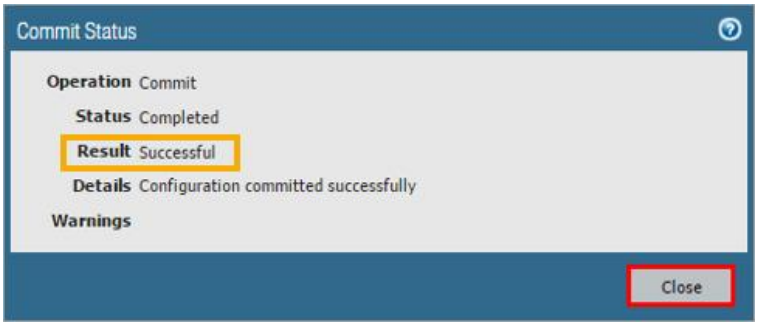
10. Click the **Commit** link at the top-right of the web interface.



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



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



1.1 Generate Traffic

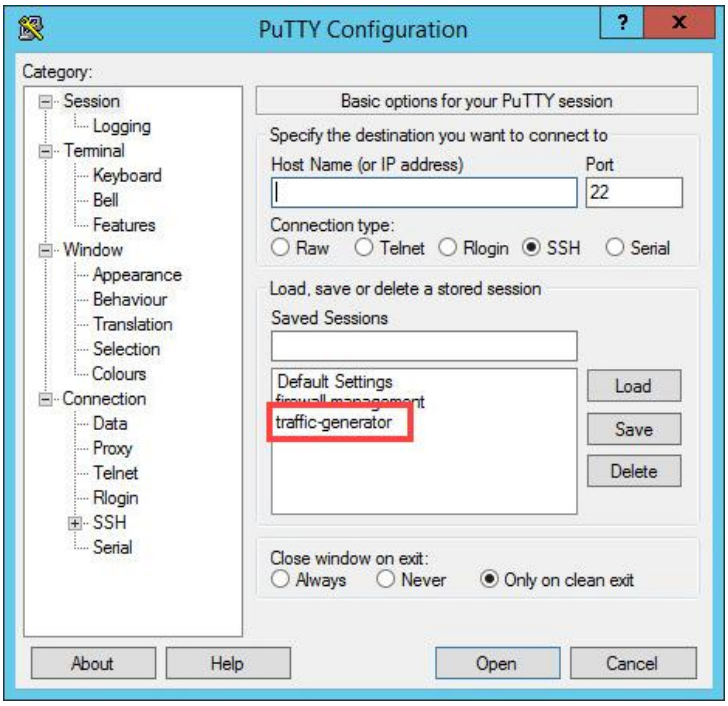
In this task, you will pre-populate the firewall with log entries and usernames that you can observe and investigate in this lab.

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

1. On the Windows desktop, double-click the **PuTTY** 

icon.

2. In the *PuTTY Configuration* window, double-click **traffic-generator**.



3. Log in as **`root`** with **`Pal0Alt0`** as the password.

```
Using username "root".
root@192.168.50.10's password:
Last login: Tue Aug  6 20:57:35 2019
[root@pod-dmz ~]#
```

4. While in the *PuTTY* window, enter the command: **`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  Cur
rent
                                 Dload  Upload   Total   Spent    Left  Speed
100  1041  100   161  100   880     21    117  0:00:07  0:00:07 --:--:--   208


  GENERATING TRAFFIC
```

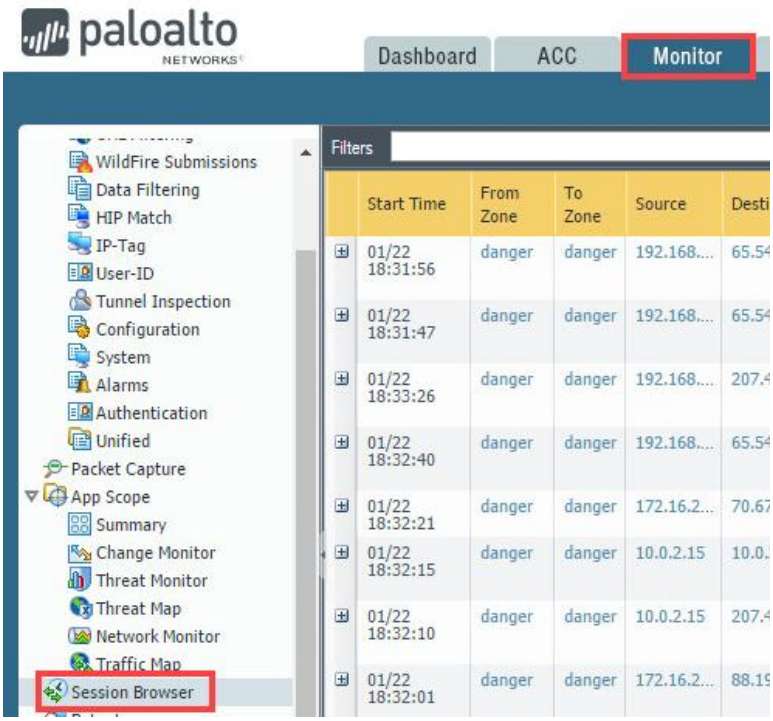
After you execute the command, wait until the script finishes before proceeding to the next step.

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

1.2 Explore the Session Browser

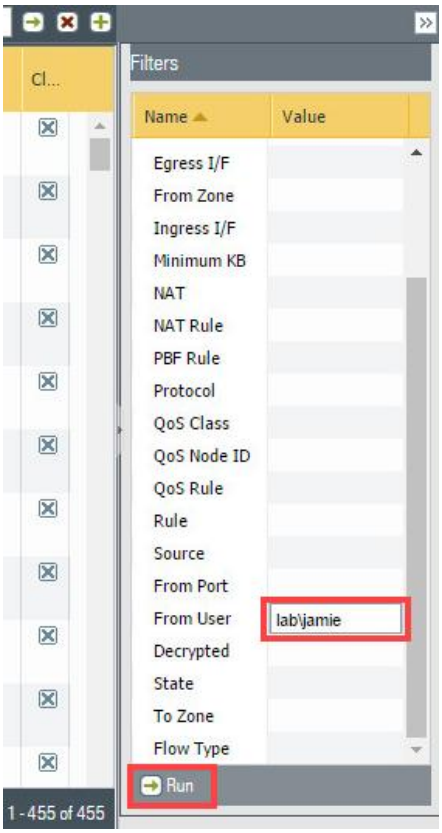
The *Session Browser* enables you to browse and filter current running sessions on the firewall.

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



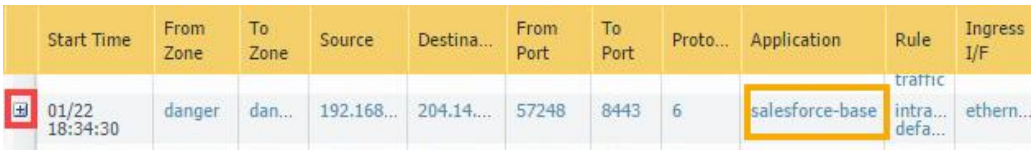
2. Clear any existing filters and then click the **plus** icon at the top-right of the window to open the *Filters* pane if not opened already.

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

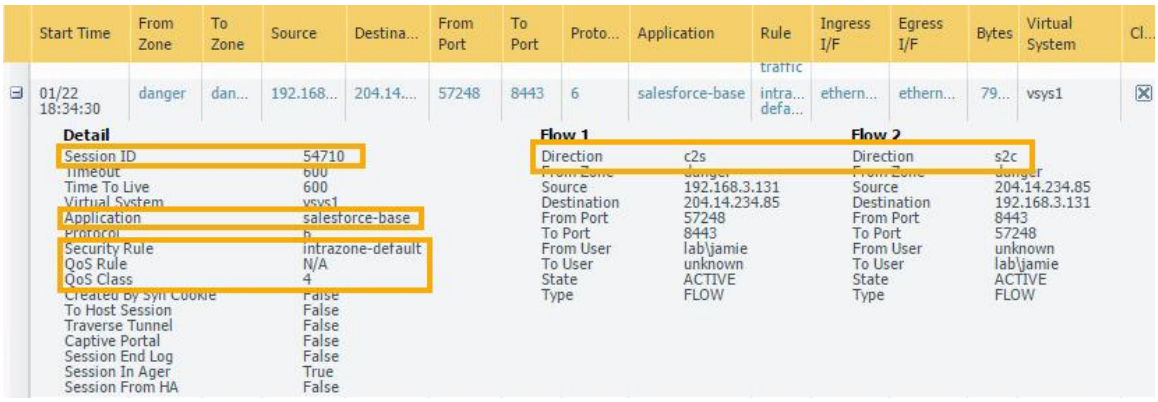


Notice that, even though there is not a *Source User* column, there is an ability to search for the *From User*. You can also search for the *To User.* If a search for the user *lab\jamie* does not produce results, the session most likely has not completed and you will need to rerun the traffic generator.

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



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



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.

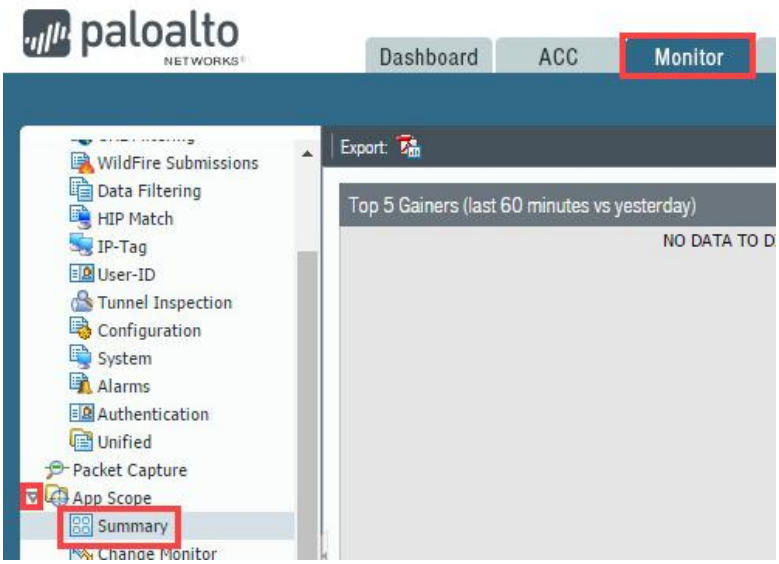
6. You can end an active session by clicking the **X** 

icon at the far-right of a session row.
7. Leave the firewall web interface open to continue with the next task.

1.3 Explore the App Scope Reports

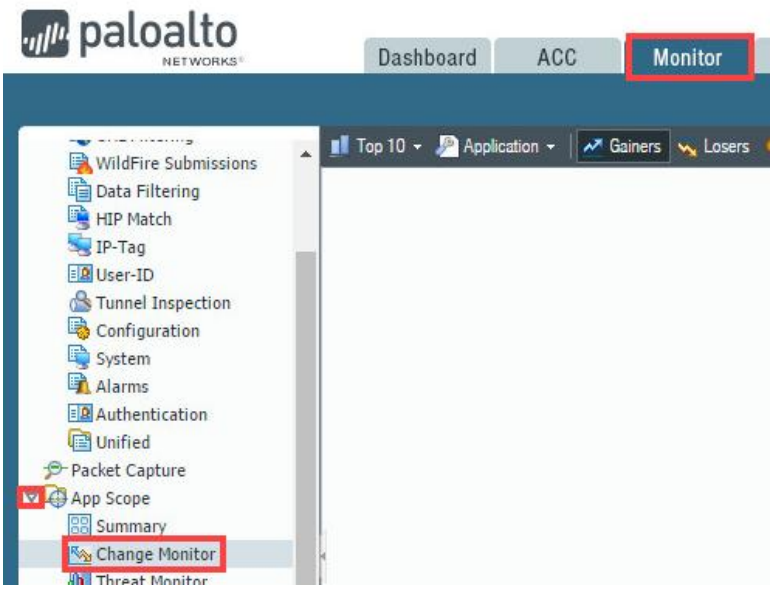
App Scope reports help you to quickly see if any application behavior is unusual or unexpected, which helps you to identify problematic behavior. Each report provides a dynamic, user-customizable window into the network. Long-term trends are difficult to represent in a lab environment. However, knowledge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

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

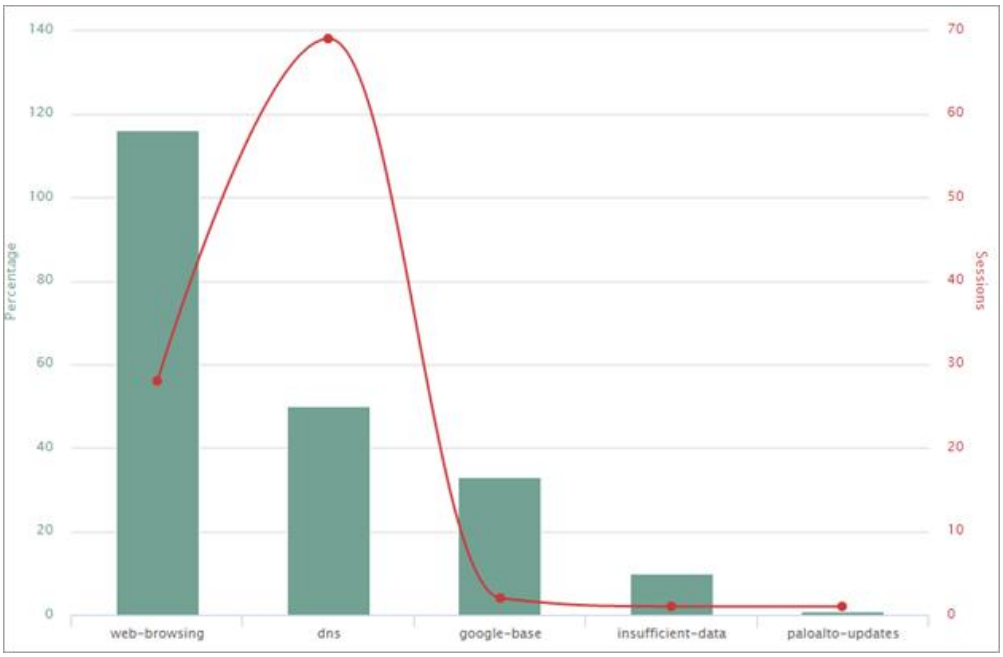


The *Summary* report displays charts for the top five gainers, losers, bandwidth-consuming source, App categories, and threats.

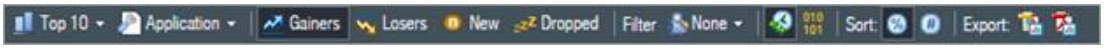
2. In the web interface, navigate to **Monitor > App Scope > Change Monitor**.



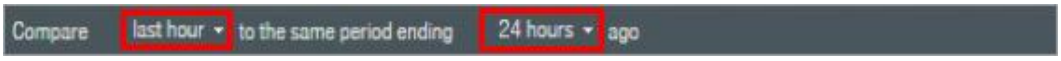
The *Change Monitor* report displays changes over a specified time period. For example, the following figure displays the top applications that gained in use over the last hour as compared with the last 24-hour period. The top applications are determined by session count and are sorted by percentage.



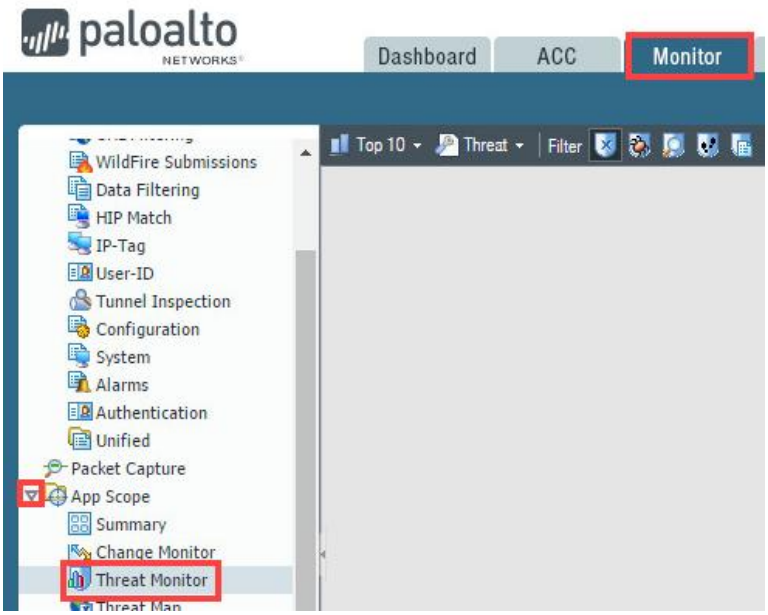
The type of information displayed can be controlled at the top. The displayed Graph can be exported as a PDF or PNG.



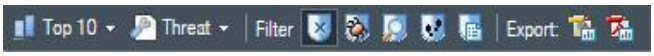
The time period also can be changed at the bottom.



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

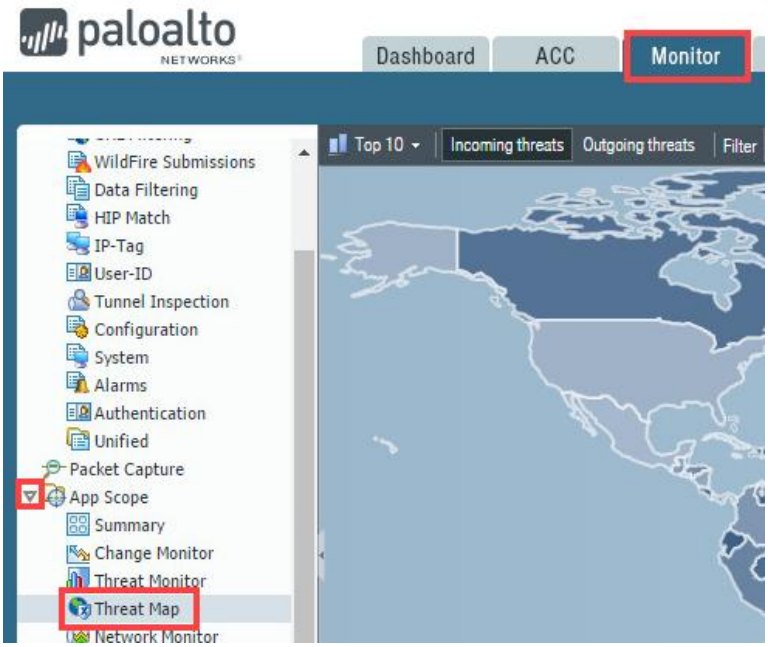


The *Threat Monitor* report displays a count of the top threats over the selected time period. By default, the figure shows the top 10 threat types for the past six hours. The type of threat also can be filtered at the top.



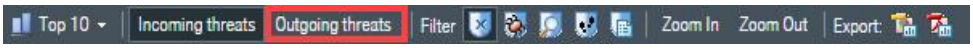
The time period can be changed to the Last 6 hours, 12 hours, 24 hours, 7 days, or 30 days.

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



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

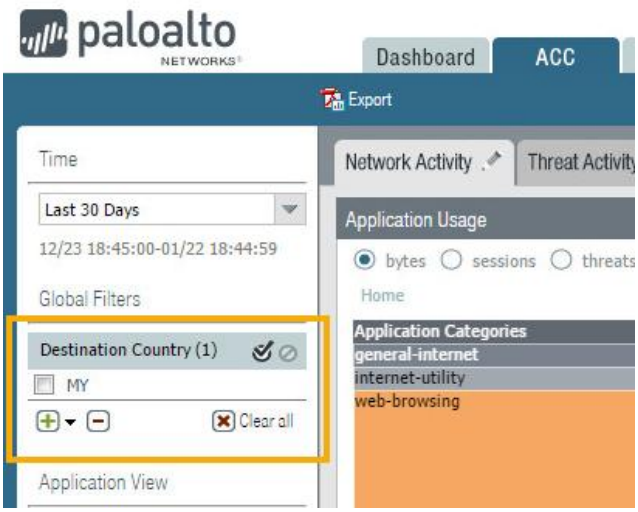
6. At the top of the screen, click **Outgoing Threats**.



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

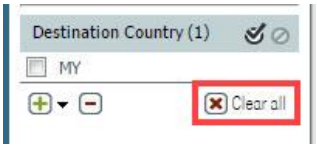
8. Click a geographical location that has a dot showing the threats from the firewall, for example, Malaysia.

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

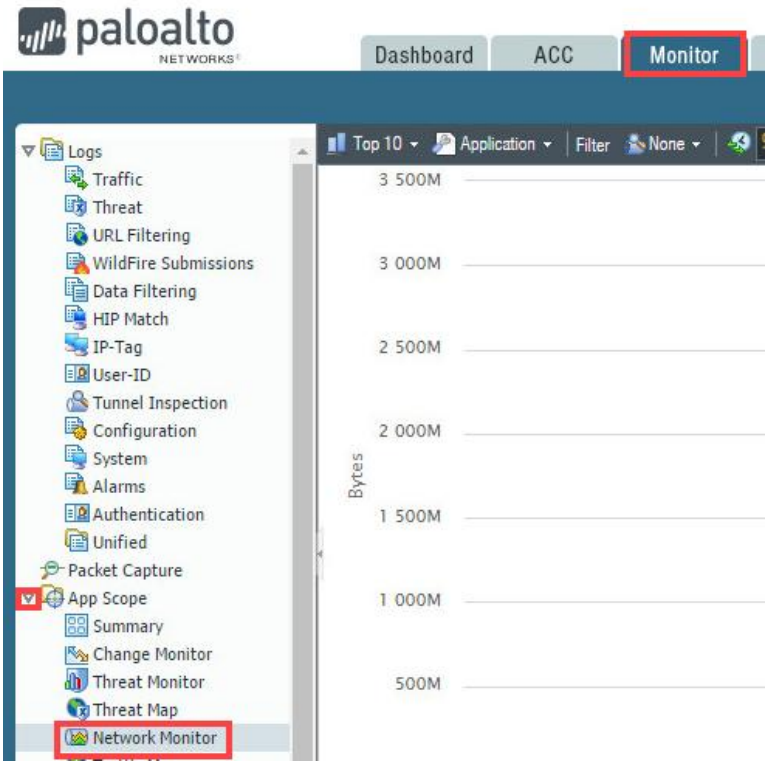


If the *ACC* does not open the first time you click on the geographical location, click on it once more and it should redirect you to the *ACC* panel.

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



11. In the web interface, navigate to **Monitor > App Scope > Network Monitor**.



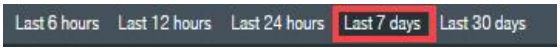
The *Network Monitor* report displays the bandwidth dedicated to different network functions over the specified period of time. Each network function is color-coded, as indicated in the legend below the chart. For example, the following diagram shows application bandwidth for the past six hours based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



15. 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.

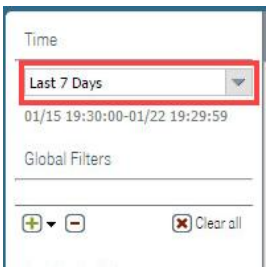
16. Leave the firewall web interface open to continue with the next task.

1.4 Explore the ACC

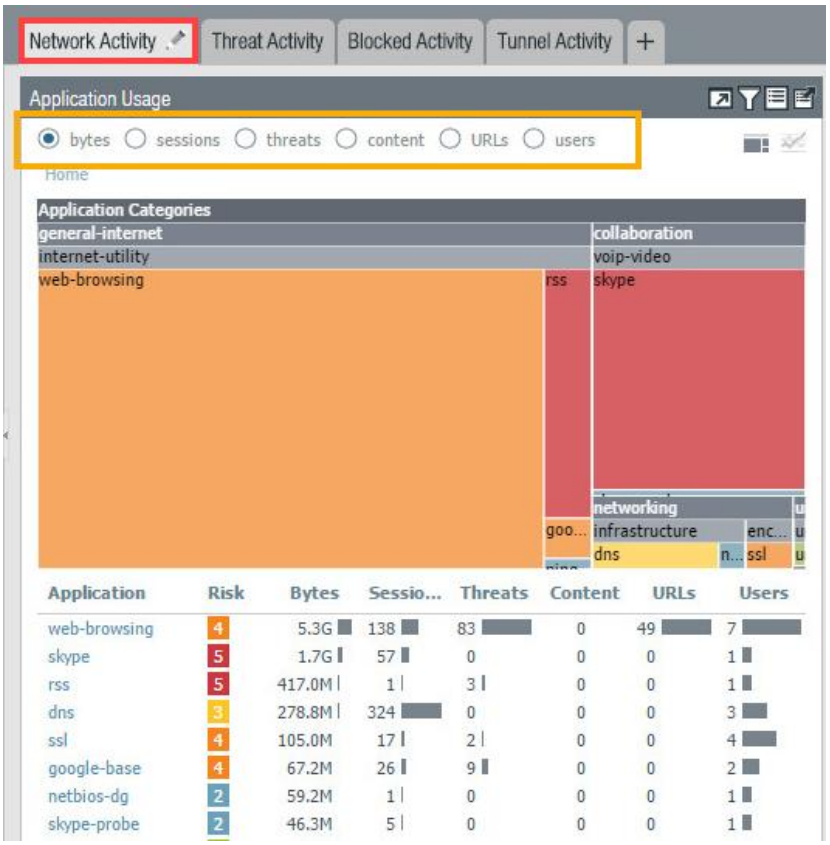
The *ACC* is an analytical tool that provides useful intelligence about the activity within your network. The *ACC* uses the firewall logs to graphically depict traffic trends on your network.

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

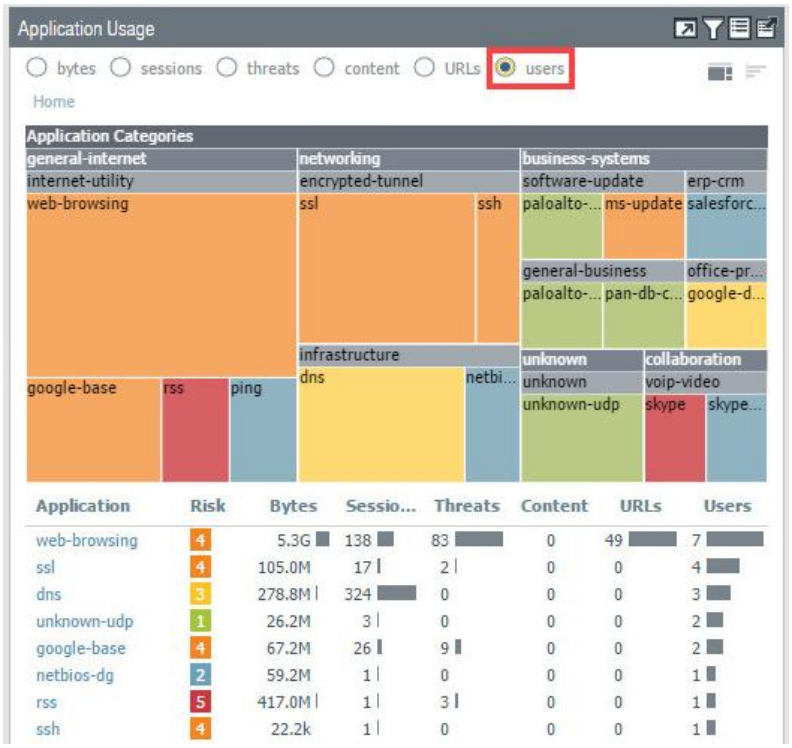
2. In the left pane, click the **Time** drop-down list and select **Last 7 Days**.



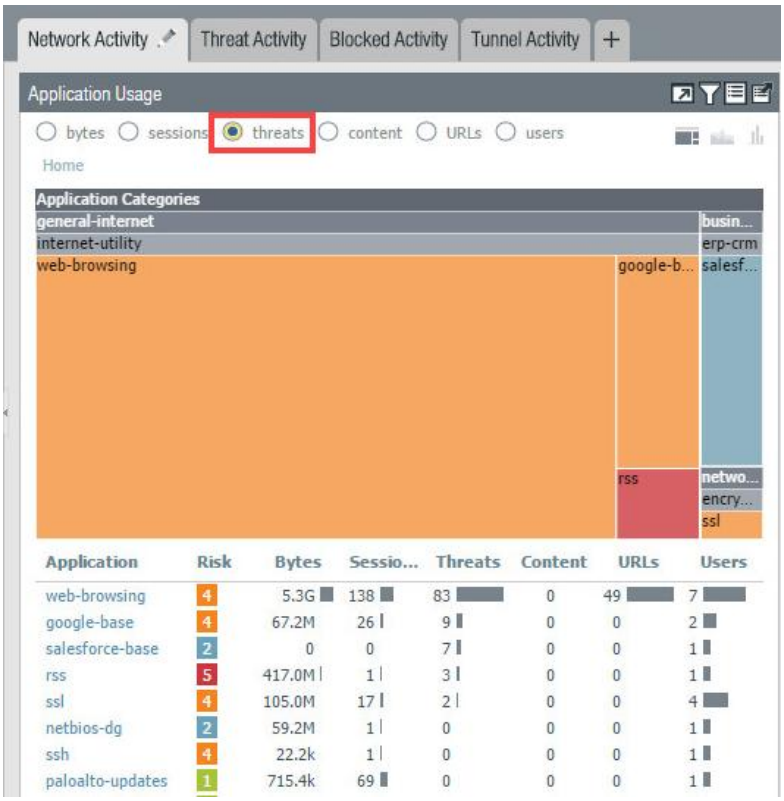
3. Explore the information available on the **Network Activity** tab. This tab displays an overview of traffic and user activity on your network. It focuses on the top applications being used; the top users who generate traffic with detailed information about the bytes, content, threats, or URLs accessed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



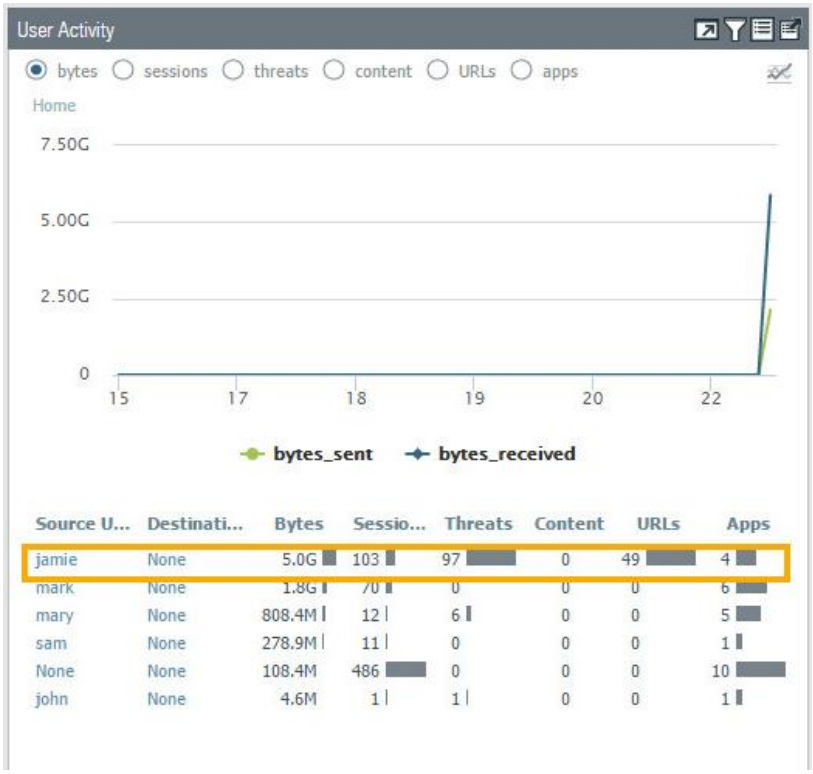
4. Select the **users** option in the *Application Usage* widget. Notice how the application use seems more consistent across all colors versus bytes. This information indicates that one application does not supersede any other application in overall use by users.



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

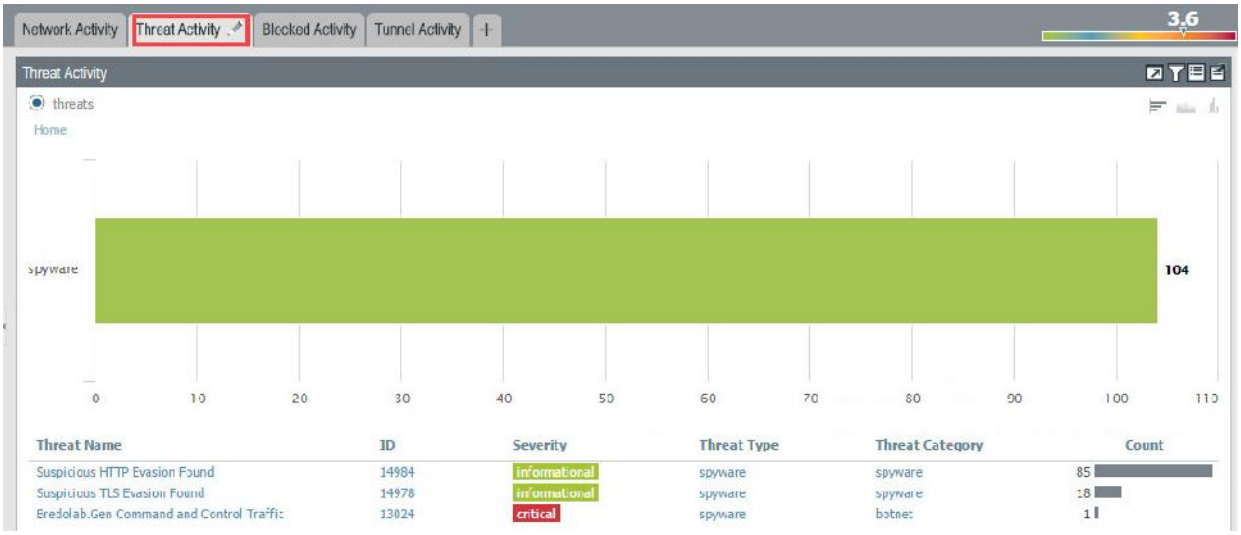


6. Focus your attention on the **User Activity** widget. The graph in the example shows that *Jamie* has consumed the most bandwidth.



7. Scroll down and focus your attention on the bottom-right **Policy Optimizer** (*Rule Usage* pane) 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.

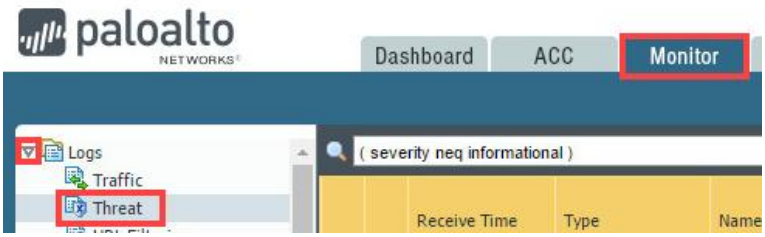
9. Locate the **Global Filters** on the left side of the *ACC* and click the **plus** icon and go to **Threat > Severity**. Add **critical** and **medium** to the *Global Filters*. Notice that the graph updates to display only critical and medium severities.

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.

1.5 Investigate the Traffic

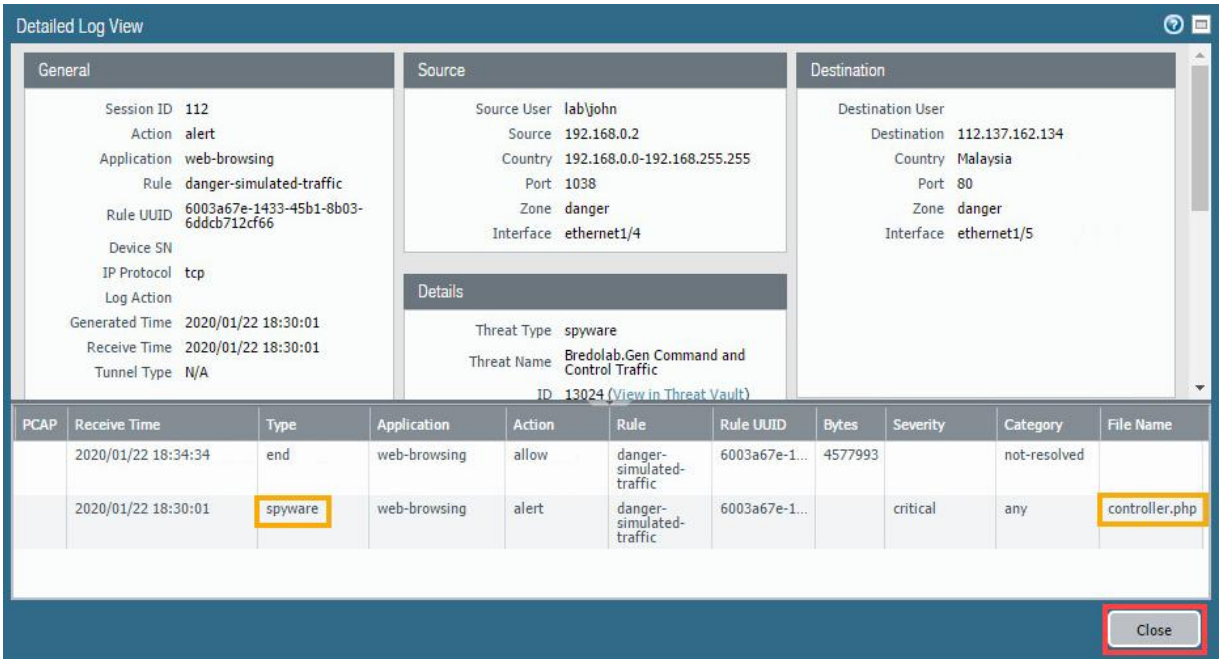
12. In the web interface, navigate to **Monitor > Logs > Threat**.



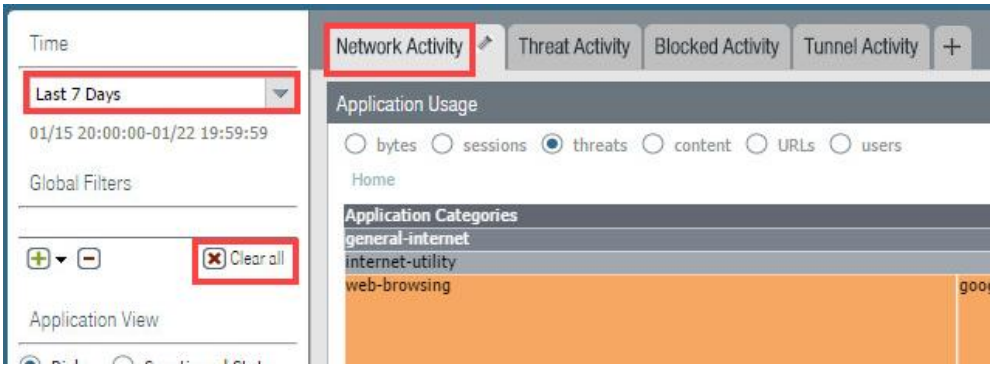
13. Clear any existing filters and type **`(severity neq informational)`** into the log filter text box, followed by pressing the **Enter** key.

14. 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.

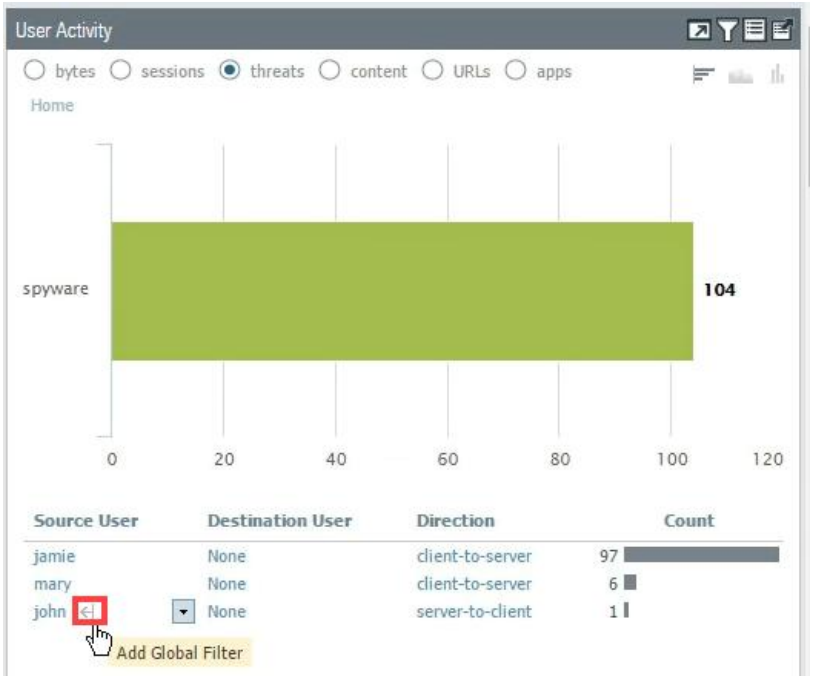
15. Notice at the bottom of the *Detailed Log* view should be the associated threat entries. View the information to see which thread type and filename is associated with the user john and then click **Close**.



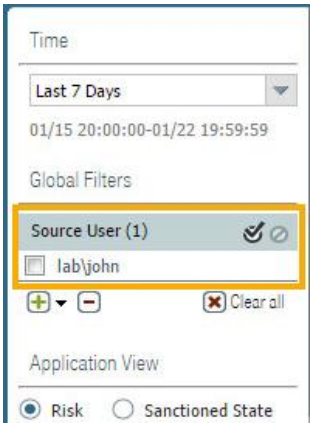
16. Click on the **ACC** tab.
17. Select the **Network Activity** tab and remove any existing global filters. Ensure that the **Time** drop-down list is **Last 7 Days**.



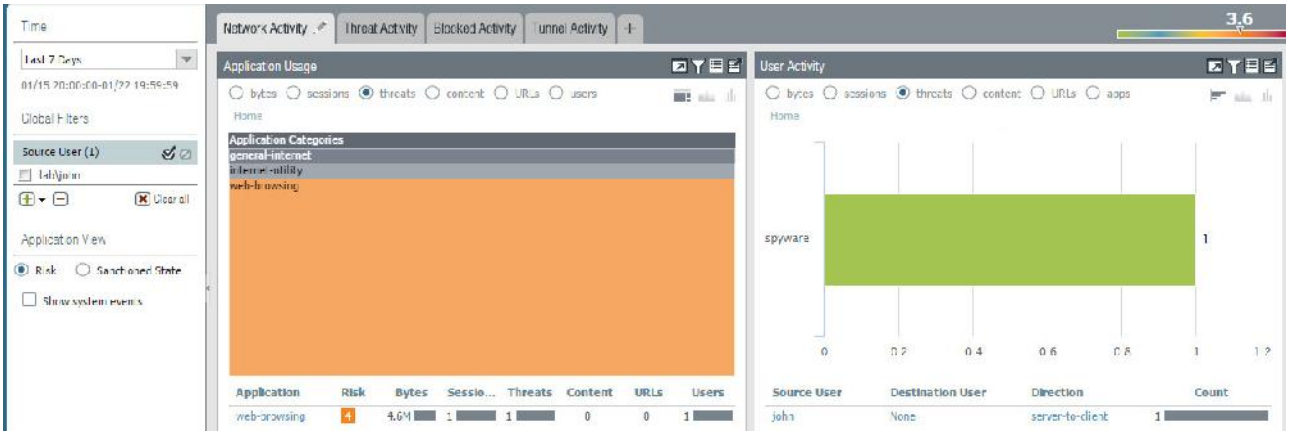
18. Focus on the **User Activity** pane and hover your mouse over **john**, then proceed to click the left-arrow to promote *john* to the *Global Filter*.



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

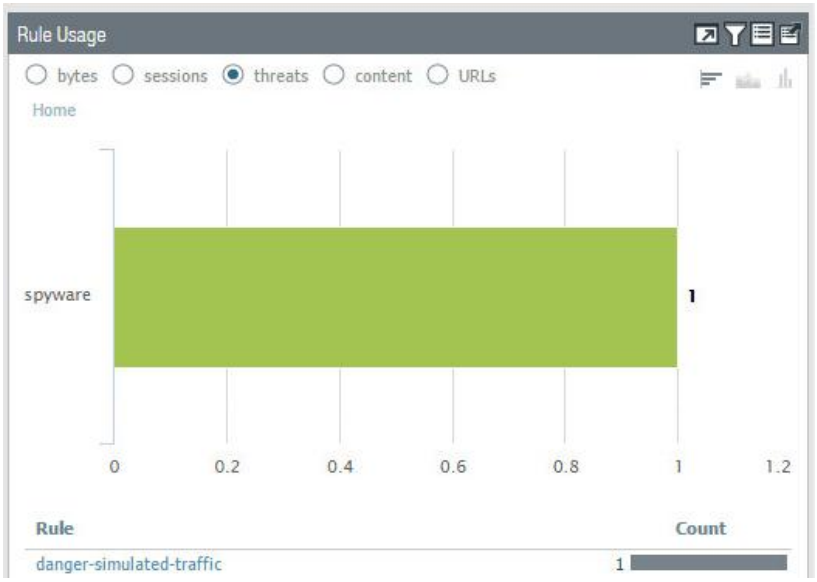


20. Notice that all window panes have been updated to only show information based on *john*. Also notice that *john* is shown to be associated with *web-browsing* traffic.

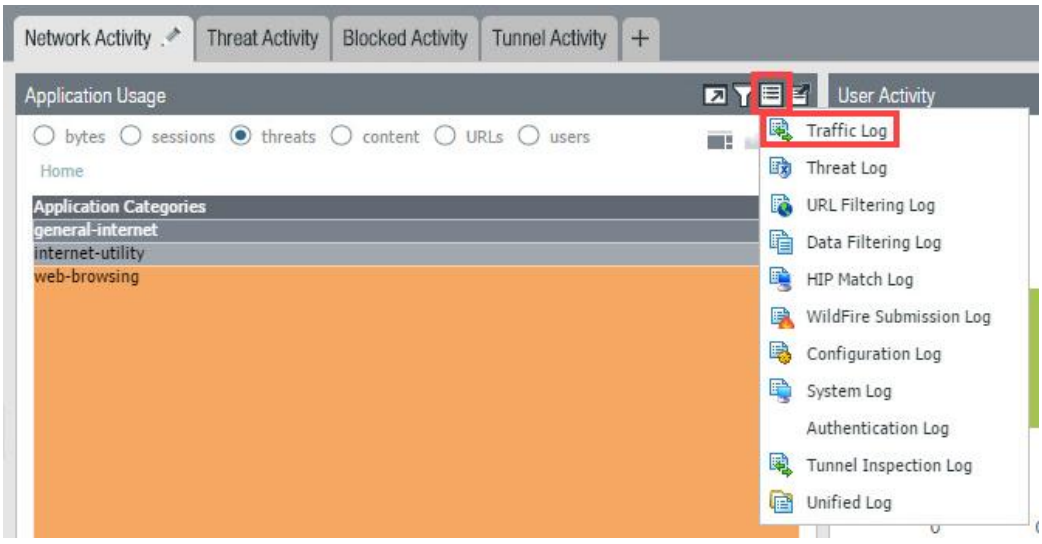


21. Scroll down and locate the **Destination Regions** pane. Notice that this is associated with the country *Malaysia*.

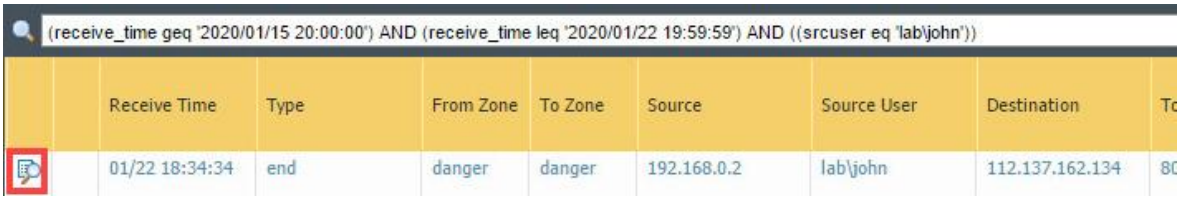
22. Scroll down further to the **Policy Optimizer** (*Rule Usage*) pane. Notice that only one rule allowed this traffic. If we were in a production environment, inspection should be done to ensure that this rule is operating effectively.



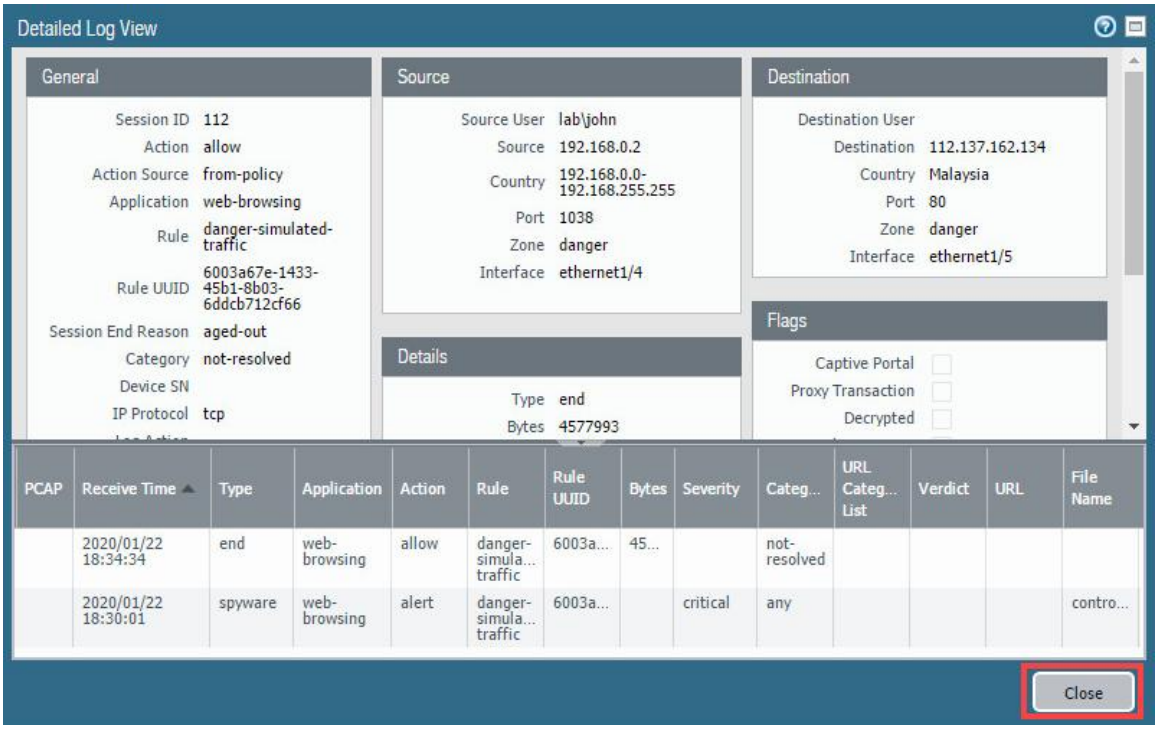
23. Scroll to the upper-left **Application Usage** pane. Click the **Jump to Logs** icon and select **Traffic Log**.



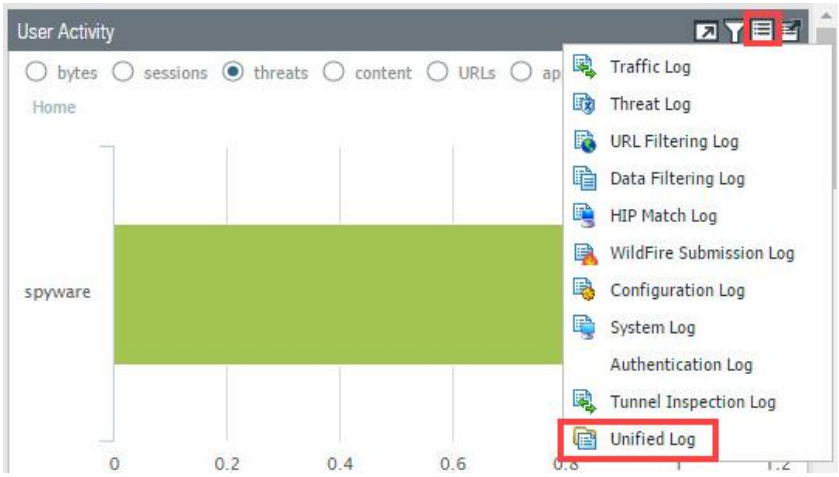
24. Notice that the web interface switched views to the Traffic log with a predefined filter. Select the **Detailed Log view** icon for the entry.



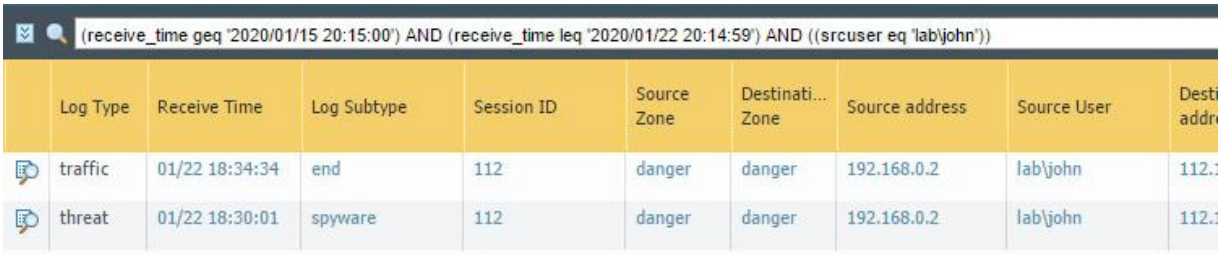
25. In the *Detailed Log View* window, notice at the bottom the associated threat entries. Click **Close**.



26. Click on the **ACC** tab.
27. On the **User Activity** pane, click the **Jump to Logs** icon and select the **Unified Log**.



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

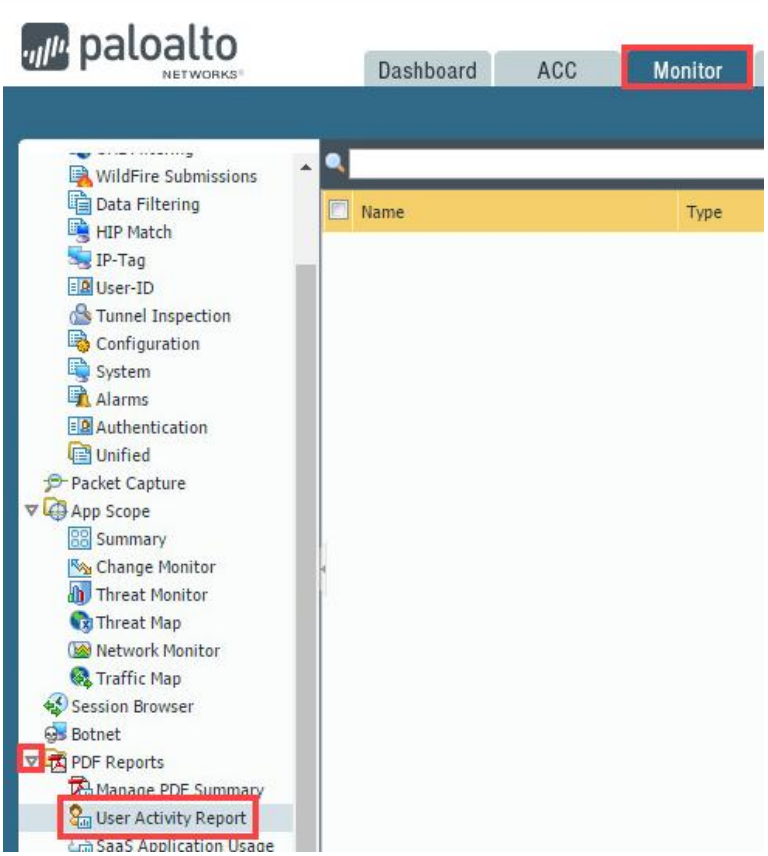


29. Leave the firewall web interface open to continue with the next task.

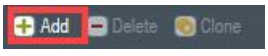
1.6 Generate a User Activity Report

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**.

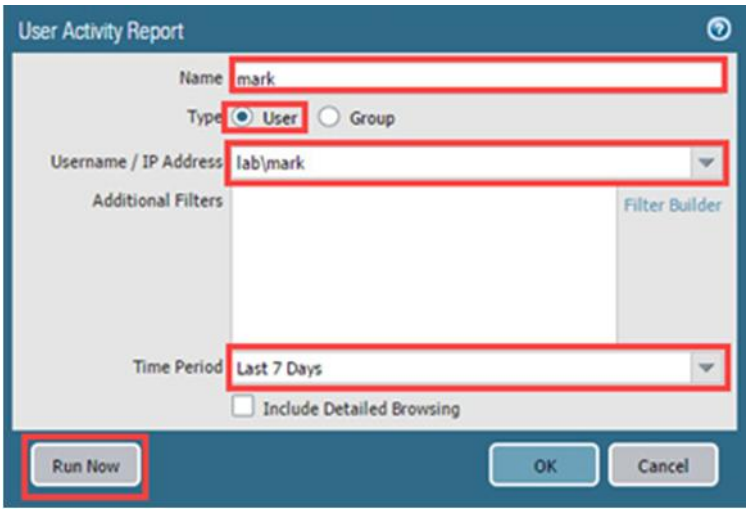


2. Click **Add** to define a new user activity report.

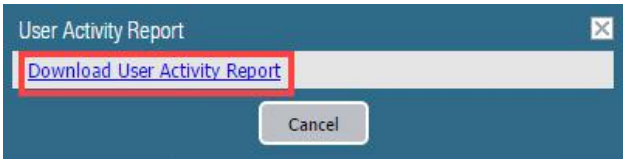


3. In the *User Activity Report* window, enter the following. Once finished, click **Run Now**.

Parameter	Value
Name	Type **`mark`**
Type	Verify that the **User** radio button is selected
Username / IP Address	Type **`lab\mark`**
Time Period	Select **Last 7 days** from the drop-down list



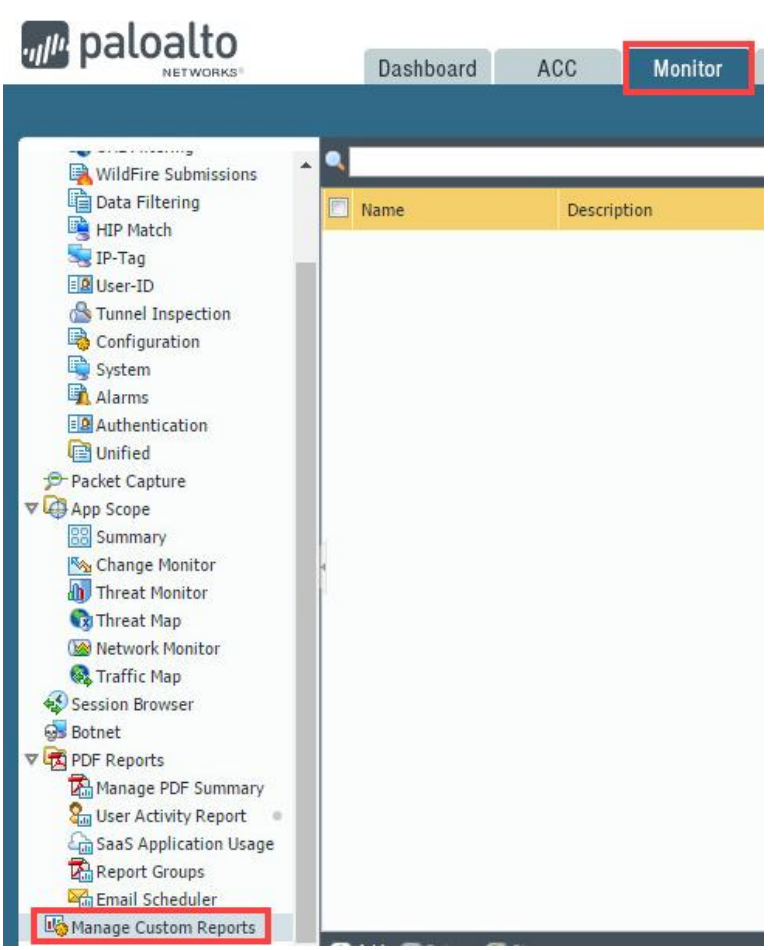
4. Click the **Download User Activity Report** link and open the report when it finishes downloading to the local system.



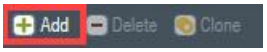
5. Browse through the report to get familiar with the presented information. You can also include a detailed browsing history that will include an approximate time a user spends on a website (this information is not available when a group is specified instead of an individual user). Close the report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

1.7 Create a Custom Report

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

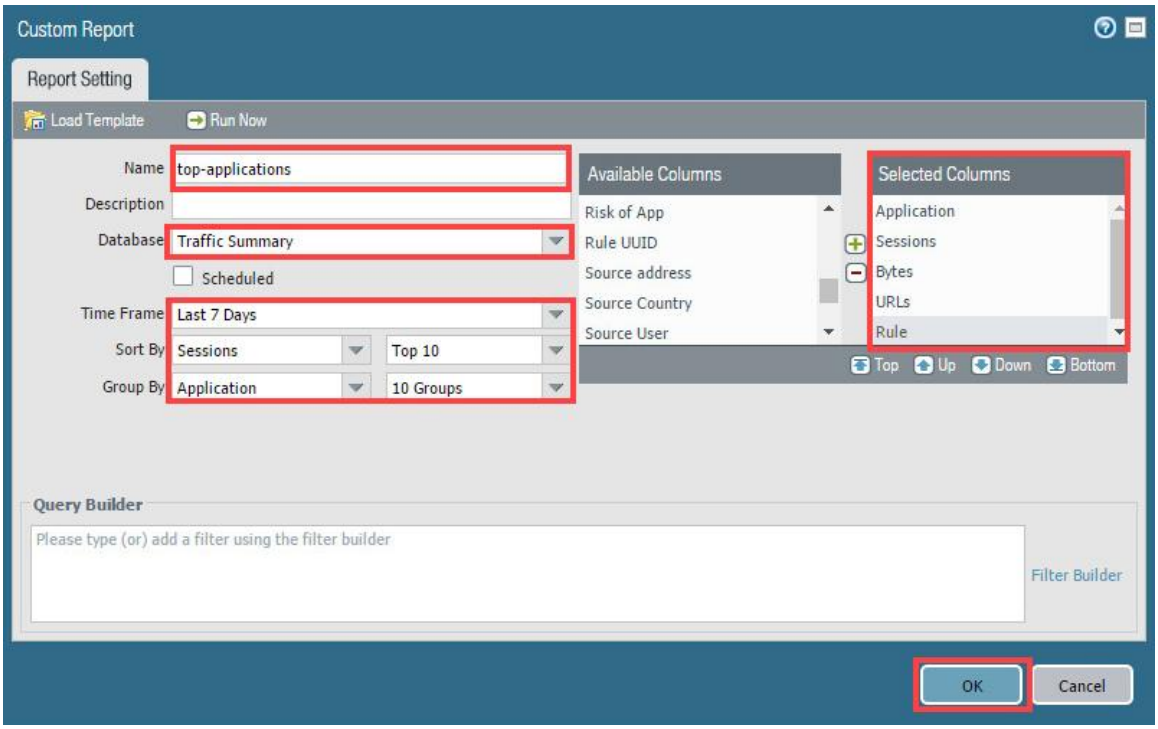


2. Click **Add** to define a new *Custom Report*.

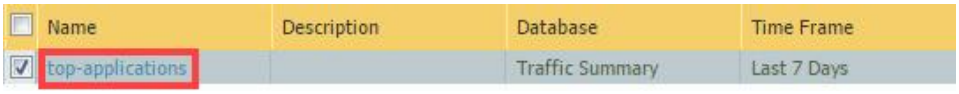


3. In the *Custom Report* window, fill out the following then click **OK**.

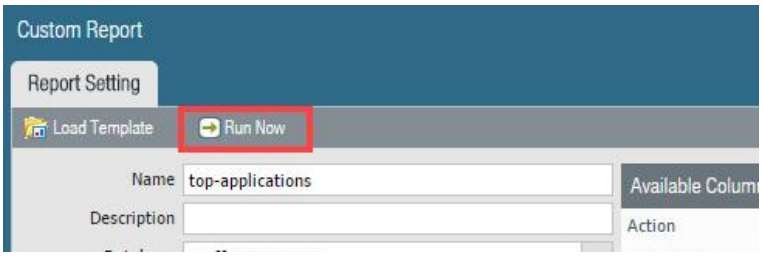
Parameter	Value
Name	Type **`top-applications`**
Database	Select **Summary Databases > Traffic** from the drop-down list
Time Frame	Select **Last 7 Days** from the drop-down list
Sort By	Select **Sessions** and **Top 10** from the drop-down list
Group By	Select **Application** and **10 Groups** from the drop-down list
Selected Columns	Move **Application**, **Sessions**, **Bytes**, **URLs**, and **Rule** to the *Selected Columns* pane



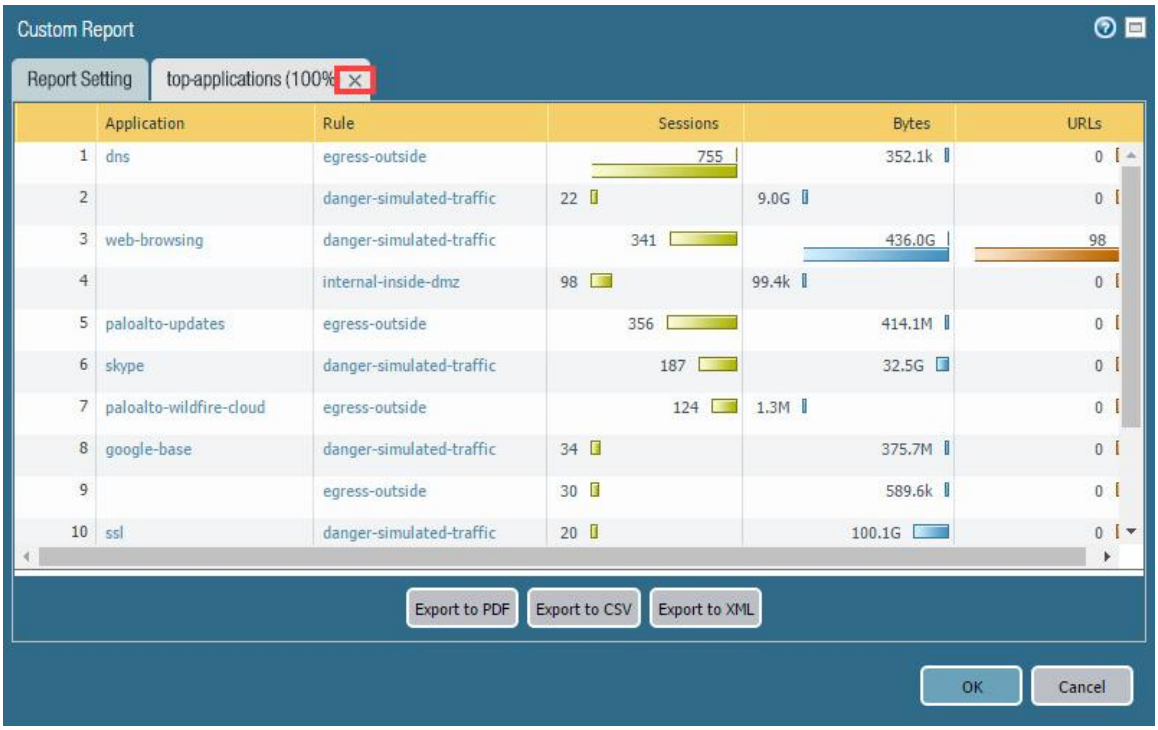
4. Click the **top-applications** report to reopen the *Custom Report* window.



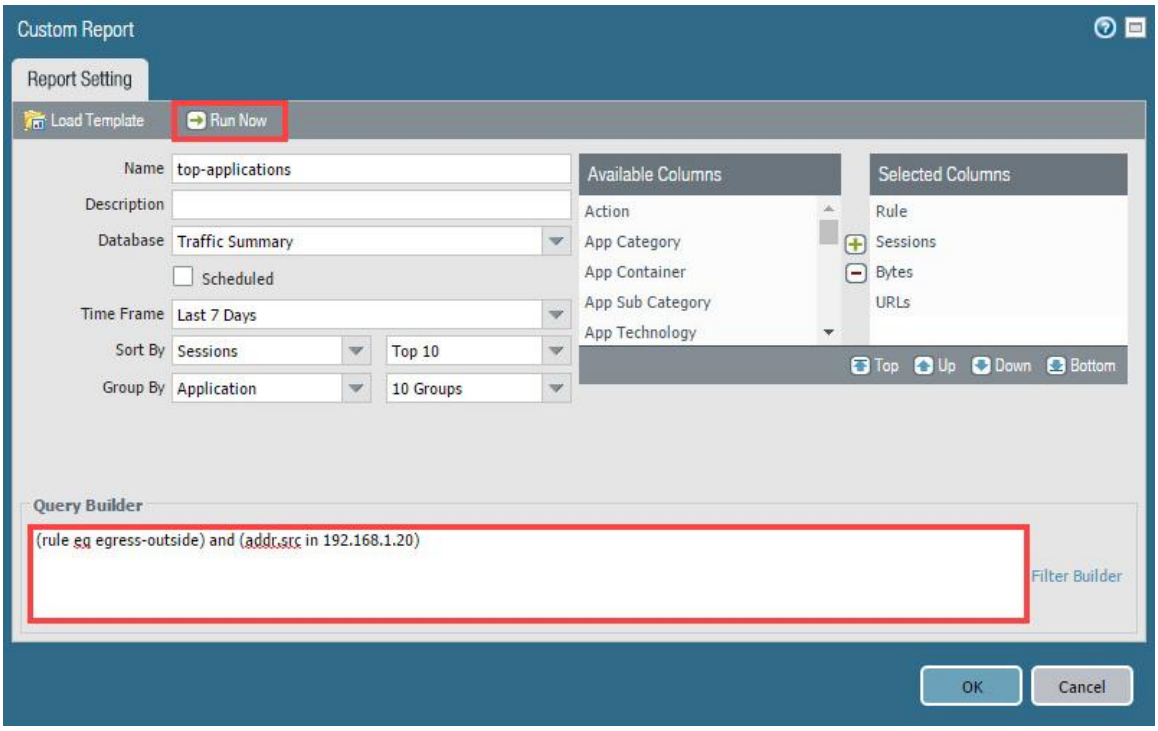
5. Click **Run Now** to generate the report. The report will appear in a new tab in the *Custom Report* window.



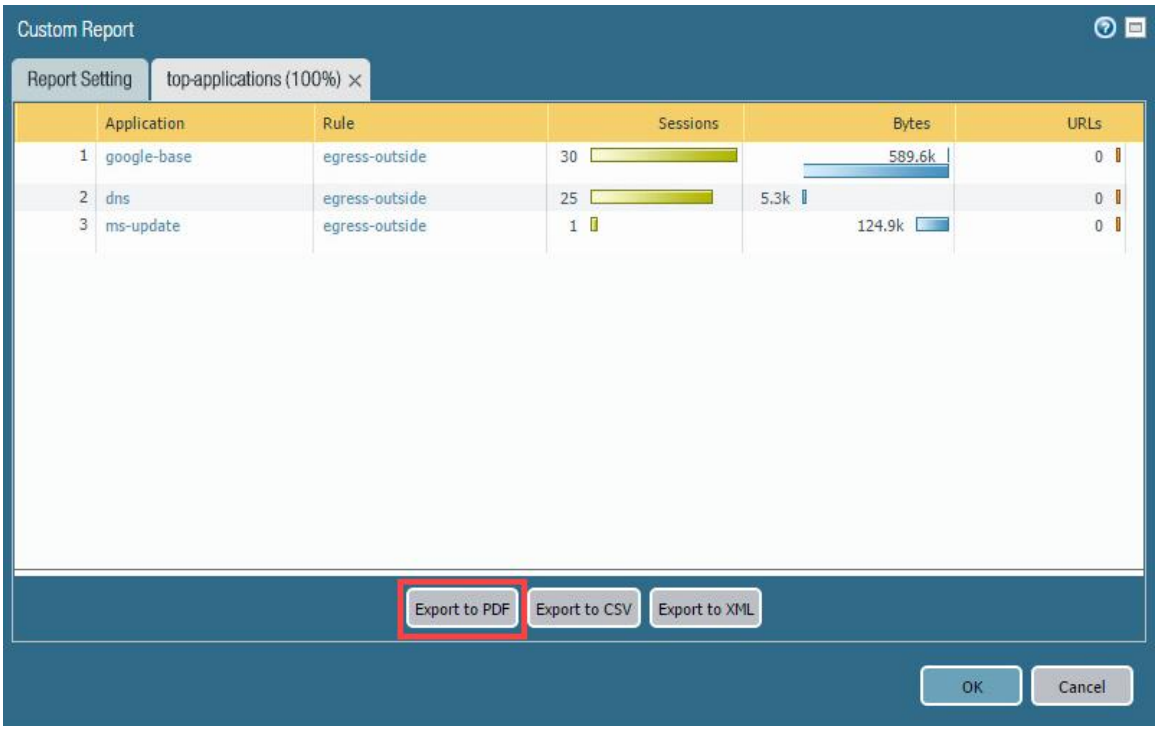
6. Close the **top-applications** tab containing the report.



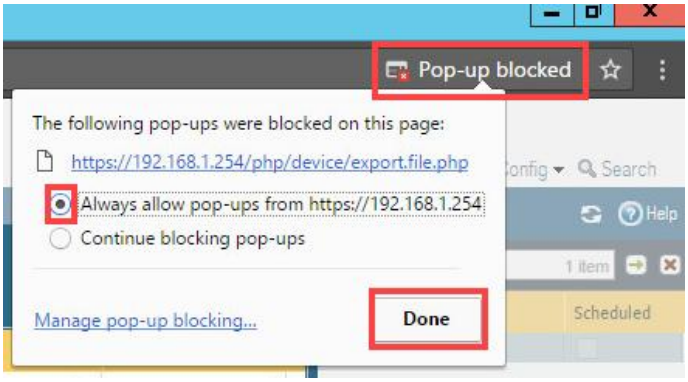
7. On the **Report Setting** tab, create the following query using the *Query Builder*: **`(rule eq egress-outside) and (addr.src in 192.168.1.20)`** and then click **Run Now** to run the report again, this time with the query.



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



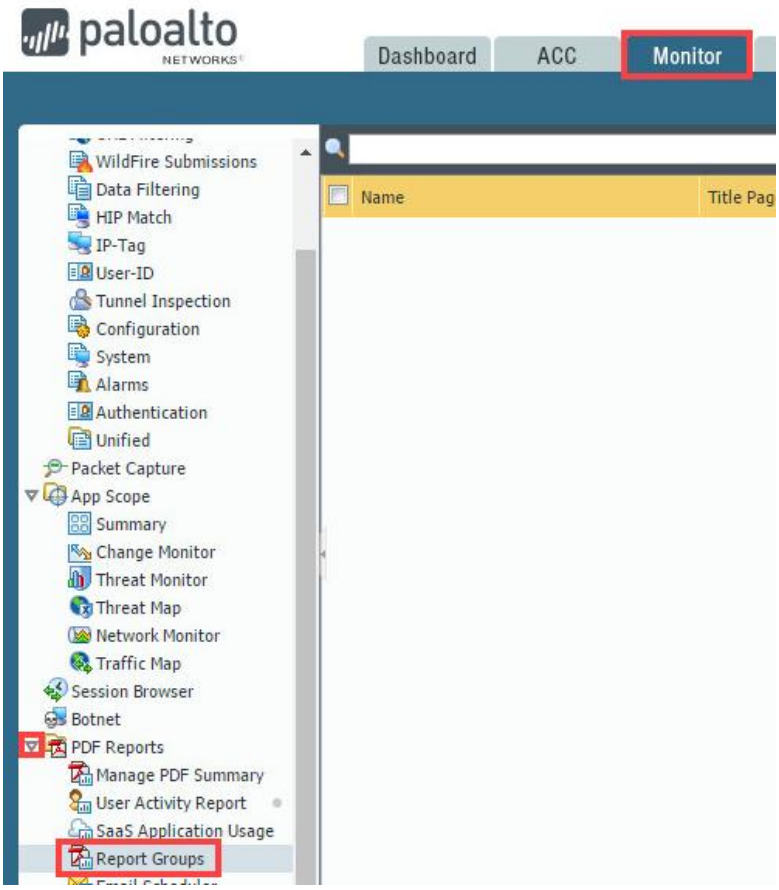
9. If you receive a warning that a pop-up was blocked, click on the **notification icon** and select the **Always allow pop-ups** radio button, then click **Done**.



10. Click on the **Export to PDF** button once more and notice the report is now downloaded. Open it.
11. Review the report and close it when finished.
12. Back on the firewall's web interface, click **OK** to close the *Custom Report* window.
13. Leave the firewall web interface open to continue with the next task.

1.8 Create a Report Group

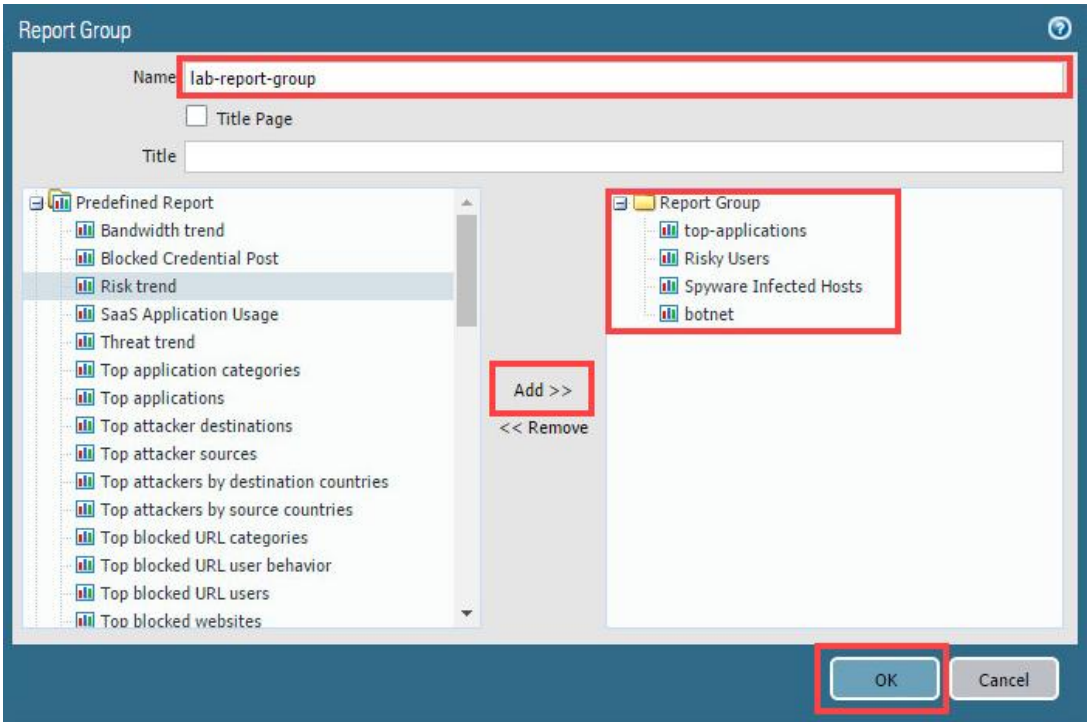
1. In the web interface, navigate to **Monitor > PDF Reports > Report Groups**.



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

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

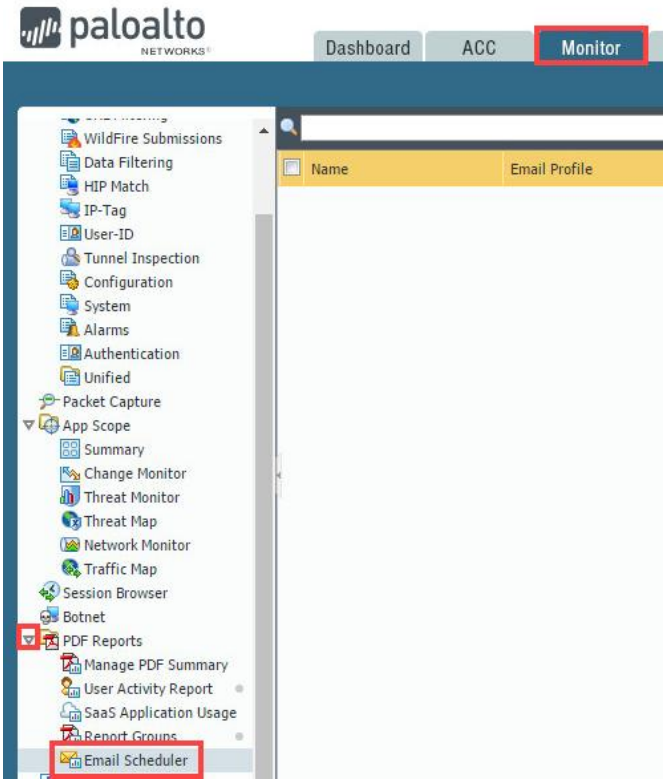
Parameter	Value
Name	Type **`lab-report-group`**
Reports	Add the following: **top-applications** **Ricky Users** **Spyware Infected Hosts** **botnet**



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

1.9 Schedule a Report Group Email

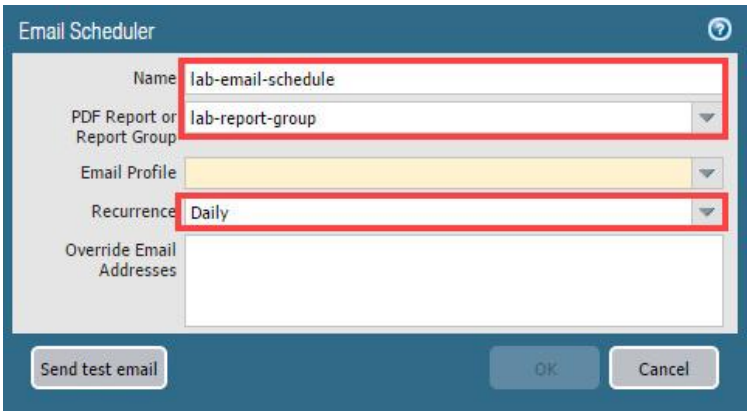
1. In the web interface, navigate to **Monitor > PDF Reports > Email Scheduler**.



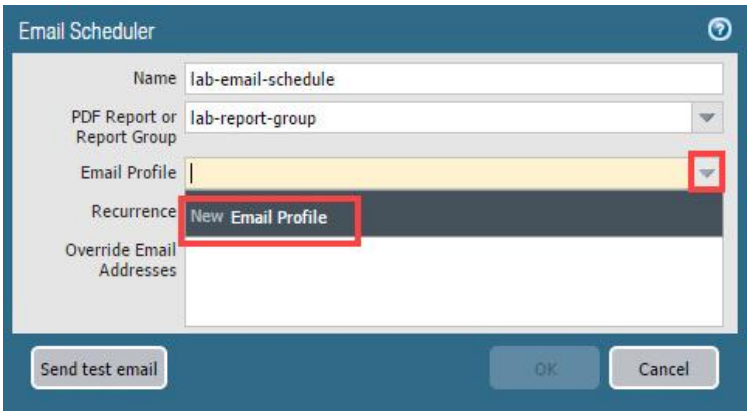
2. Click **Add** to define a new email schedule.

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

Parameter	Value
Name	Type **`lab-email-schedule`**
Report Group	Select **lab-report-group** from the drop-down list
Recurrence	Select **Daily** from the drop-down list

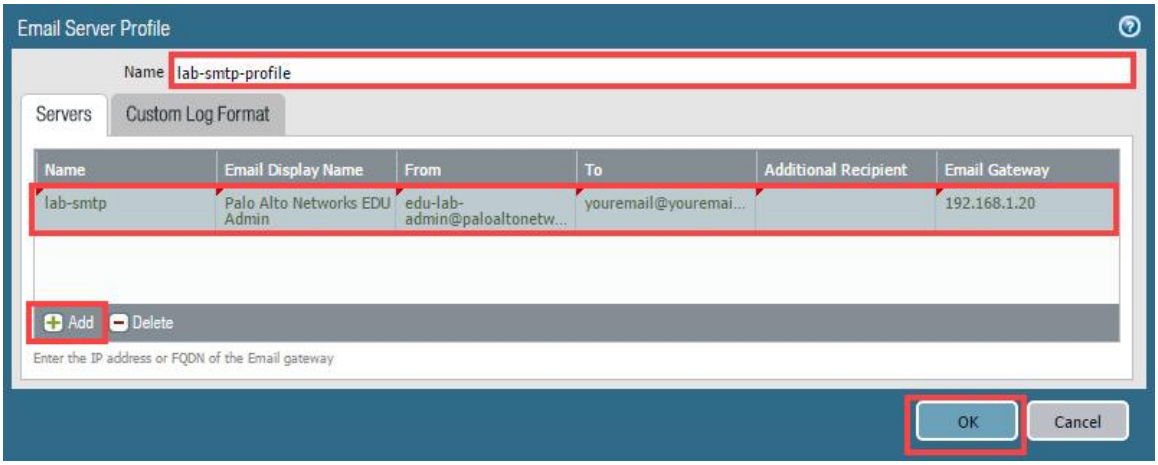


4. In the *Email Scheduler* window, select **New Email Profile** from the *Email Profile* drop-down list.

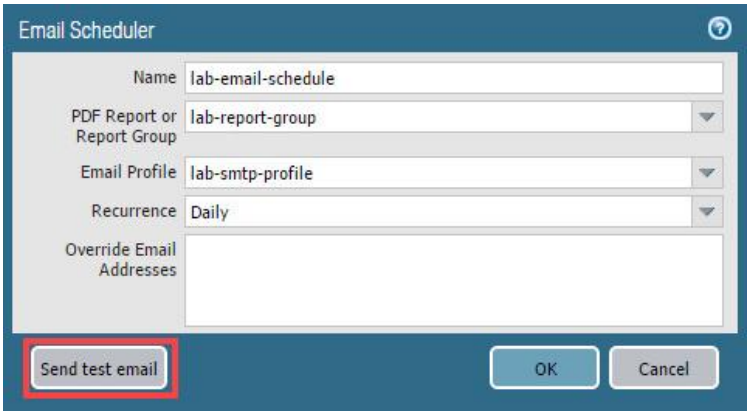


5. Notice the *Email Server Profile* window appears. Type **`lab-smtp-profile`** into the *Name* text field. Click **Add** and configure the following.

Parameter	Value
Name	Type **`lab-smtp`**
Email Display Name	Type **`Palo Alto Networks EDU Admin`**
From	Type **`edu-lab-admin@paloaltonetworks.com`**
To	Type **`<your-email-address>`**
Email Gateway	Type **`192.168.1.20`**



6. Click **OK** to close the *Email Server Profile* window.
7. 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.



You may need to check your SPAM folder.

8. Click **OK** to close the *Email Scheduler* window.
9. The lab is now complete; you may end the reservation.

