



NETWORK SECURITY FUNDAMENTALS V2

Lab 8: Backing up Firewall Logs

Document Version: **2022-12-23**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark 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

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Backing up Firewall Logs	6
1.0 Load Lab Configuration	6
1.1 Back Up Firewall Logs	11

Introduction

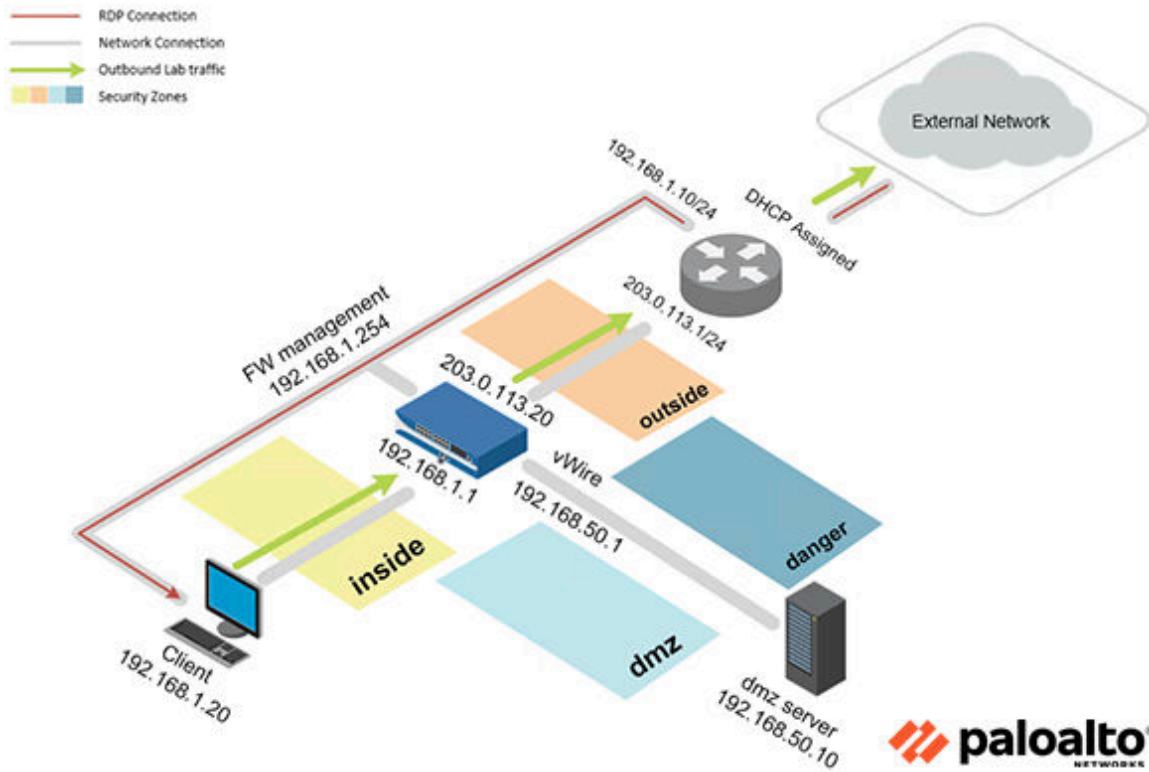
In this lab, you will back up your Firewall logs using both FTP and SCP protocols.

Objective

In this lab, you will perform the following tasks:

- Back up Firewall Logs

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.

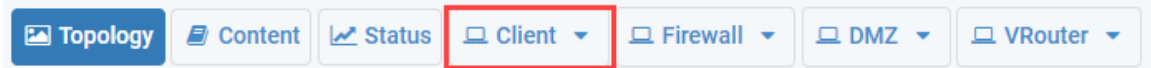
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Backing up Firewall Logs

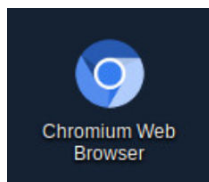
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

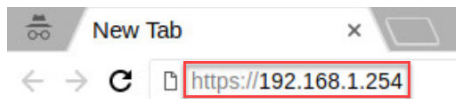
1. Click on the **Client** tab to access the Client PC.



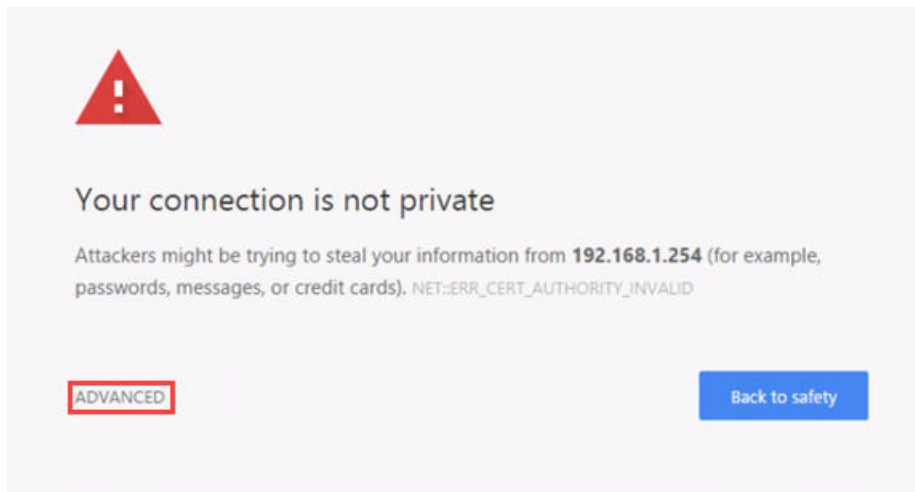
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium** icon located on the Desktop.



4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

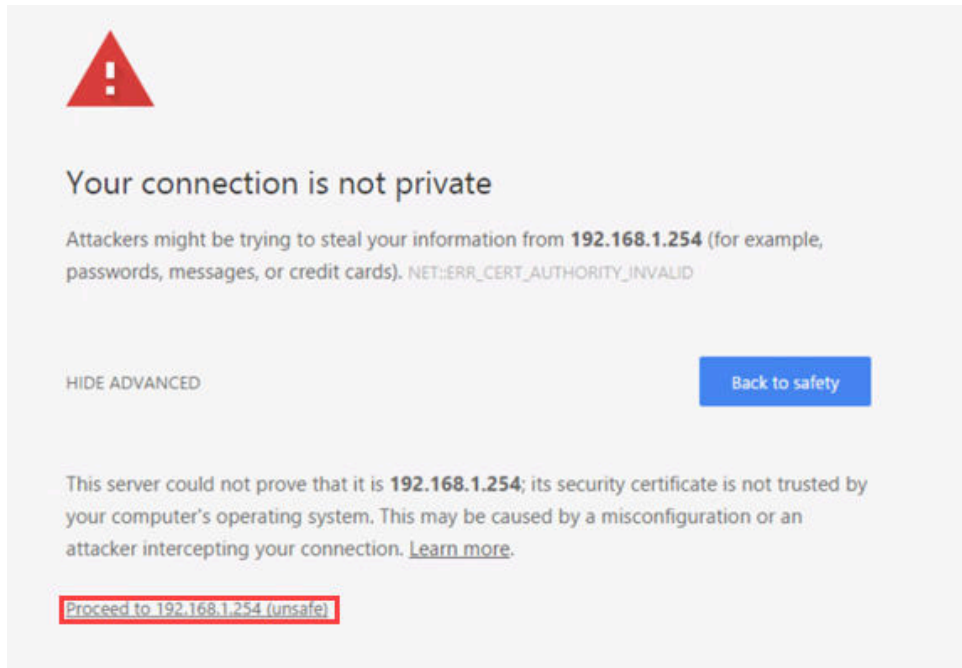


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

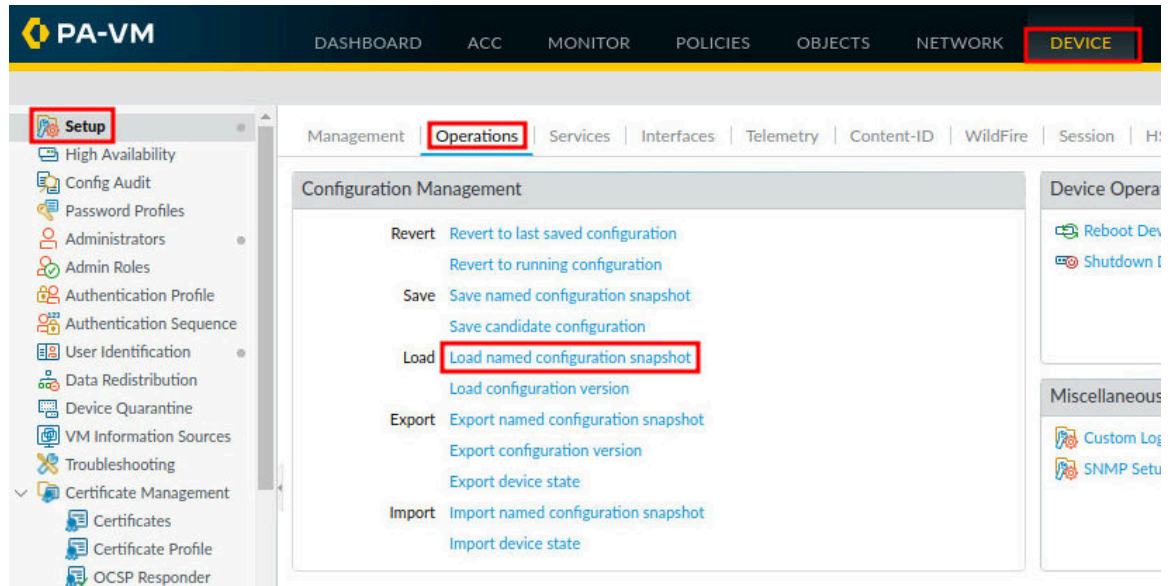
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



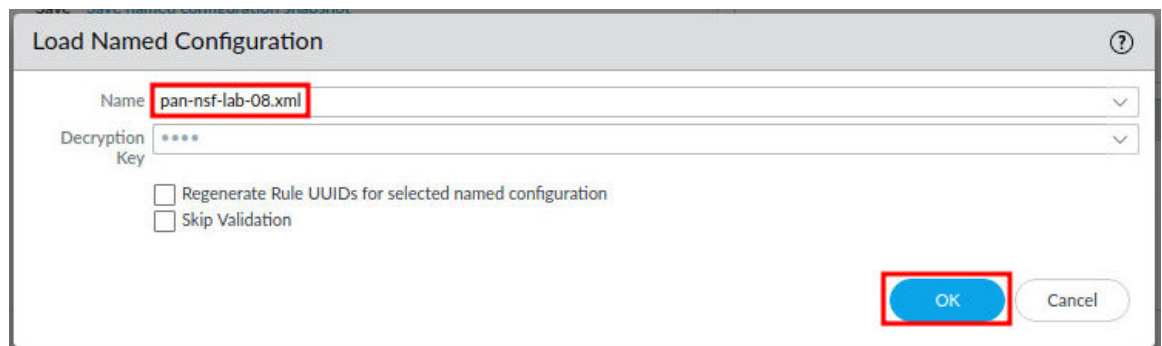
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



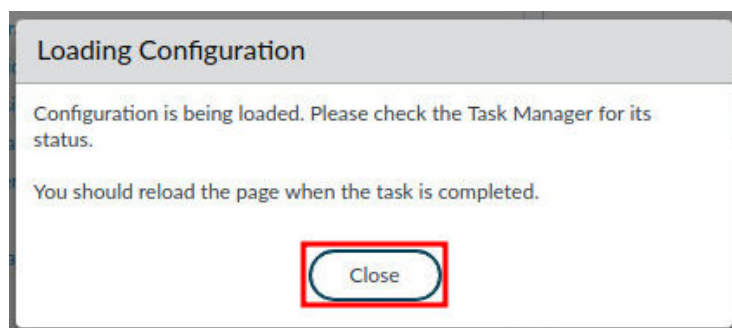
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



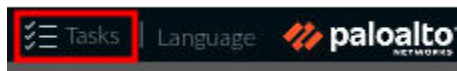
9. In the *Load Named Configuration* window, select **pan-nsf-lab-08.xml** from the *Name* dropdown box and click **OK**.



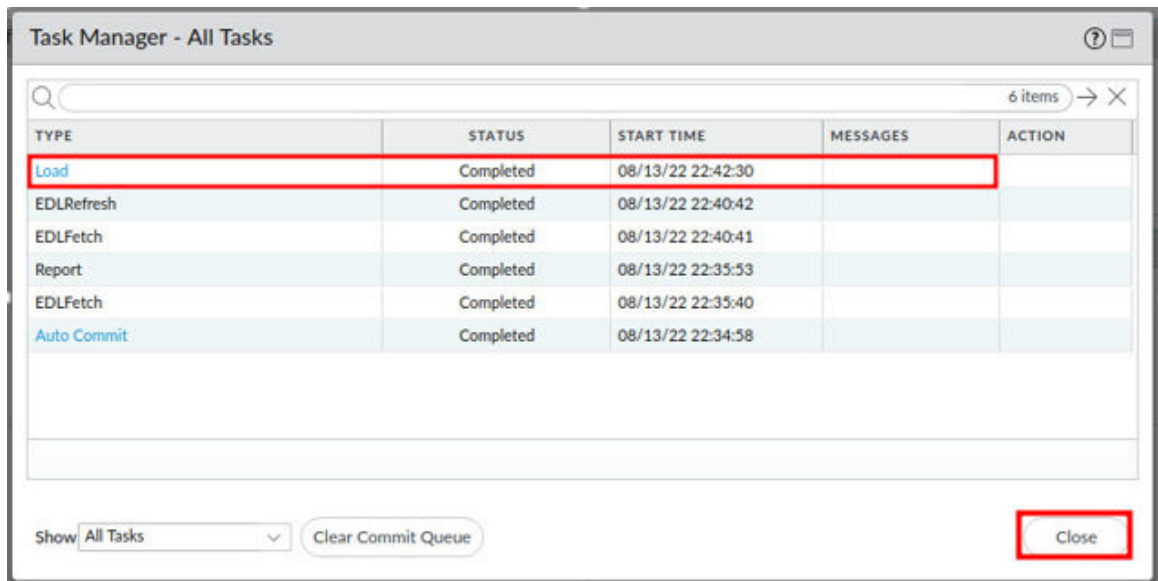
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



11. Click the **Tasks** icon located at the bottom-right of the web interface.



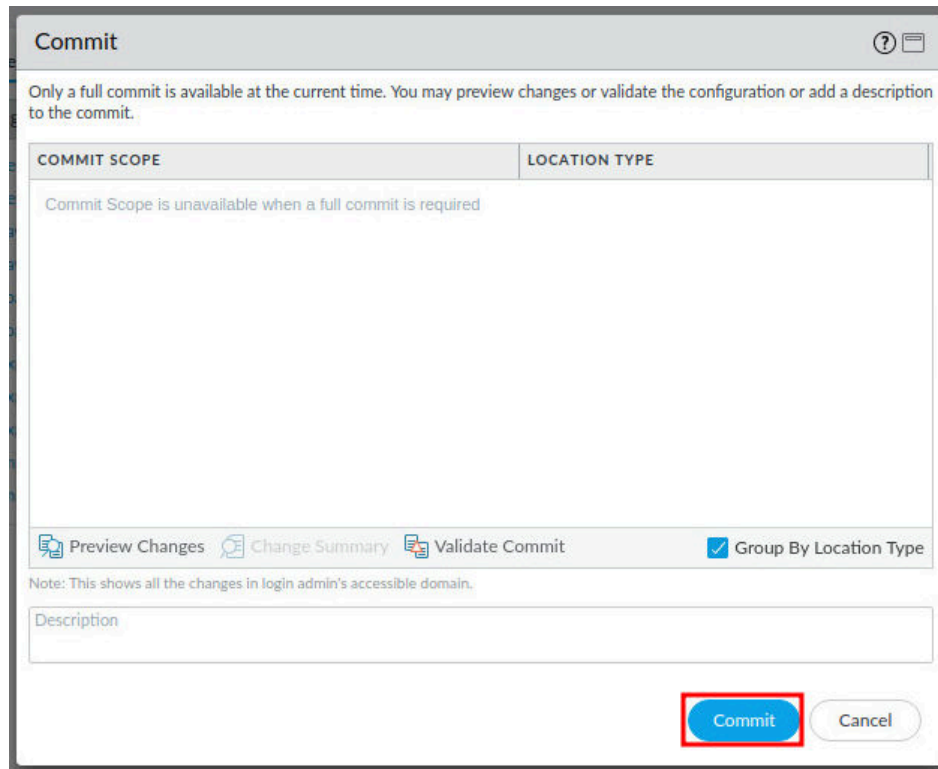
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



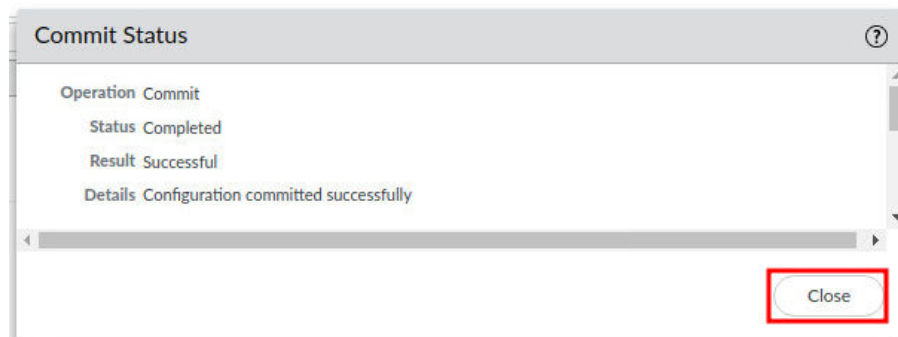
13. Click the **Commit** link located at the top-right of the web interface.



14. In the *Commit* window, click **Commit** to proceed with committing the changes.



15. When the commit operation successfully completes, click **Close** to continue.

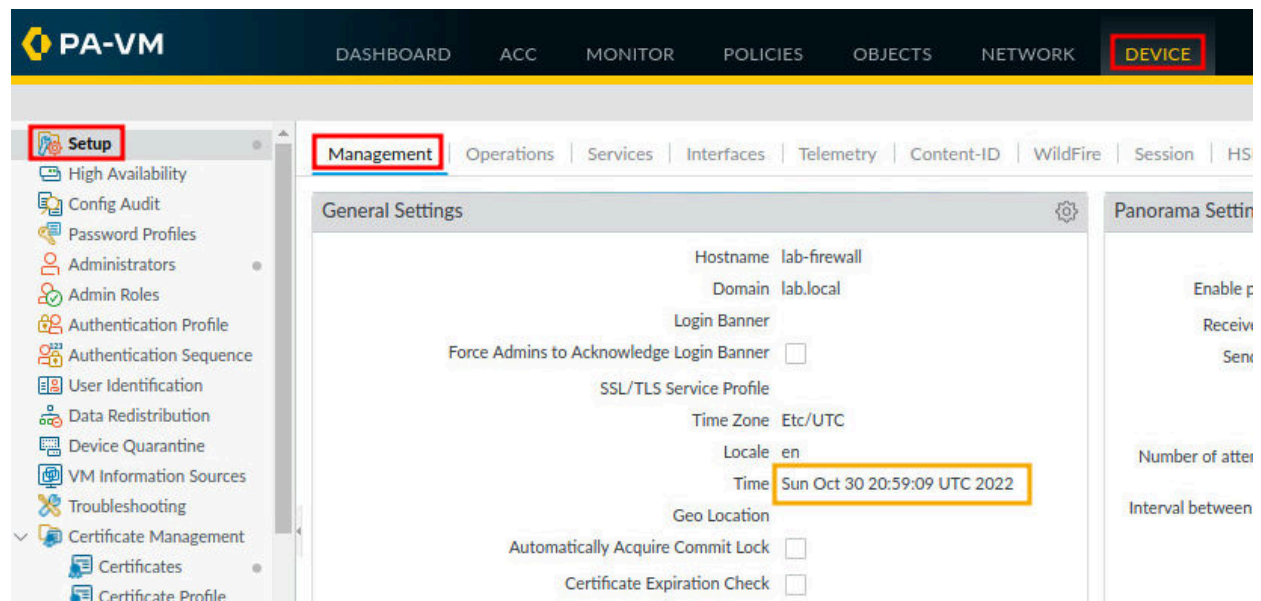


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

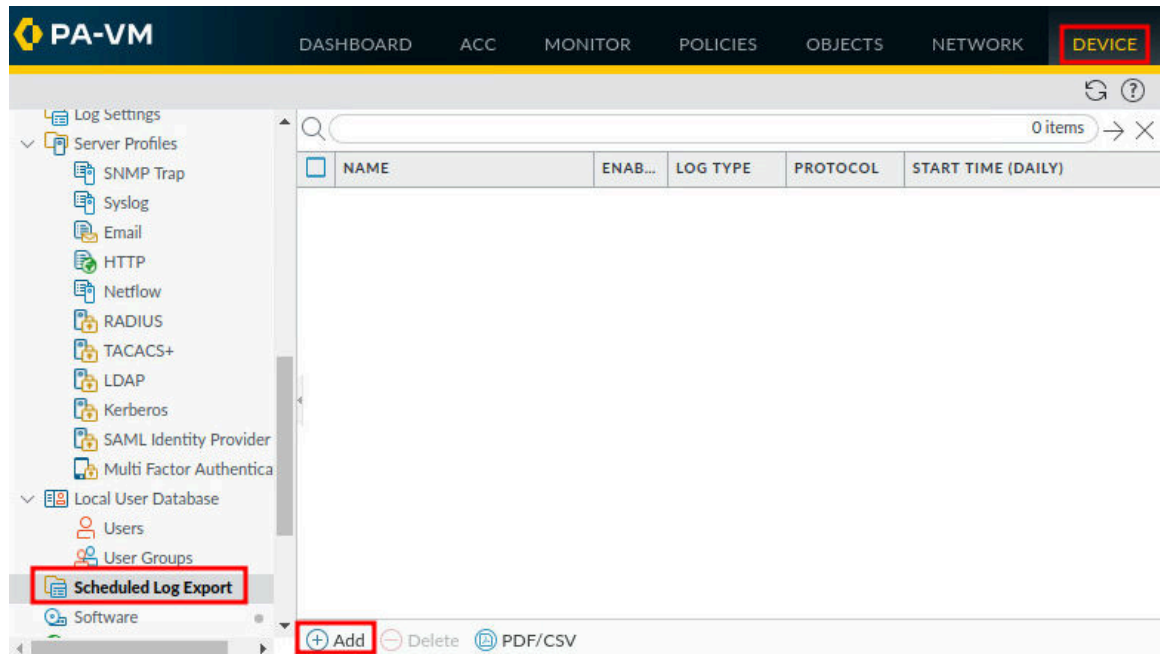
1.1 Back Up Firewall Logs

In this section, you will export Firewall logs to another location. Exporting firewall logs to an FTP Server is beneficial for keeping logs in the event that the logs are overwritten, or an unforeseen event happens to the Firewall, and the logs cannot be retrieved.

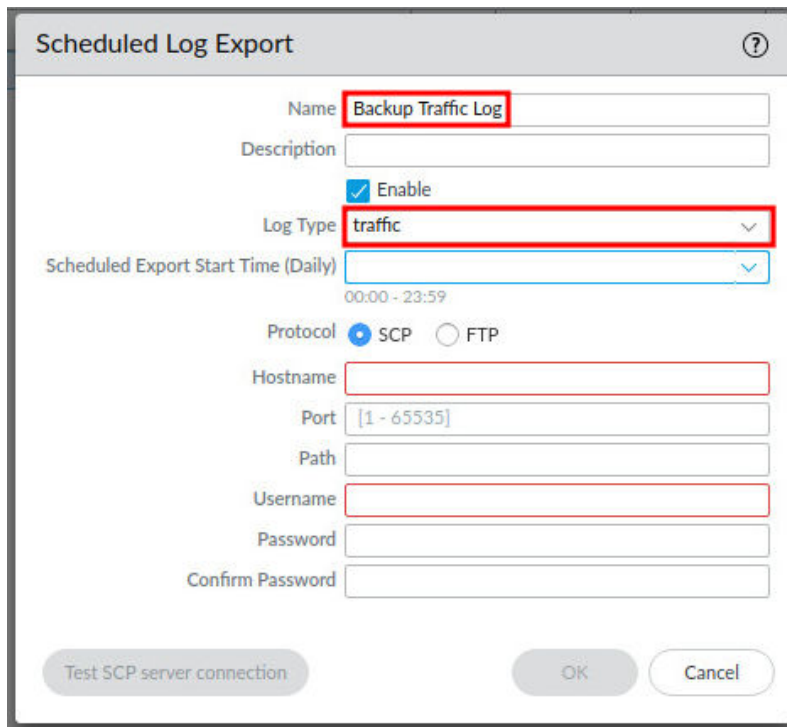
1. Make note of the time on the Firewall. Click on the **Device** tab, next click on the **Setup**. Next, click on the **Management** tab and view the current time on the firewall. (In this example, the time was 1:28 AM). If you convert this time to military time, it will be 0128 hours. Add 10 minutes to the current time to make it 0138 hours for the next step. This will allow enough time to properly configure the scheduled log export.



2. Navigate to **Device > Scheduled Log Export > Add**. You may need to scroll down on the left side panel.

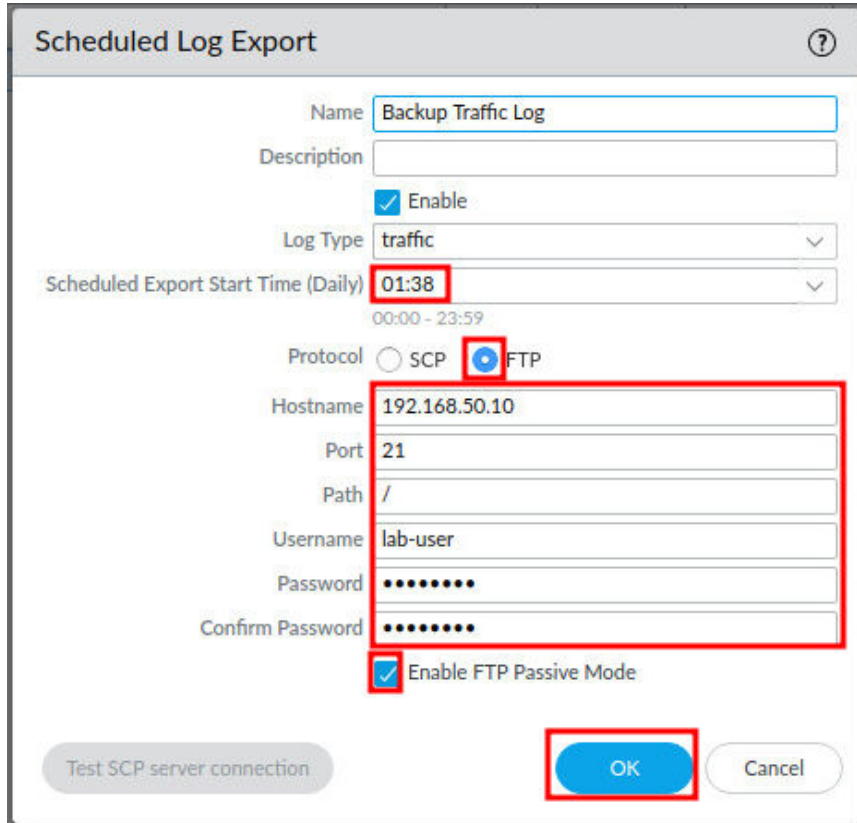


3. In the *Scheduled Log Export* window, type **Backup Traffic Log** in the *Name* field. Next, make sure the *Log Type* is set to **traffic**.



The screenshot shows the 'Scheduled Log Export' configuration window. The 'Name' field is filled with 'Backup Traffic Log' (highlighted with a red box). The 'Log Type' dropdown menu is set to 'traffic' (highlighted with a red box). Other fields include 'Description', 'Enable' (checked), 'Scheduled Export Start Time (Daily)' (00:00 - 23:59), 'Protocol' (SCP selected), 'Hostname', 'Port' (1 - 65535), 'Path', 'Username', 'Password', and 'Confirm Password'. At the bottom, there are buttons for 'Test SCP server connection', 'OK', and 'Cancel'.

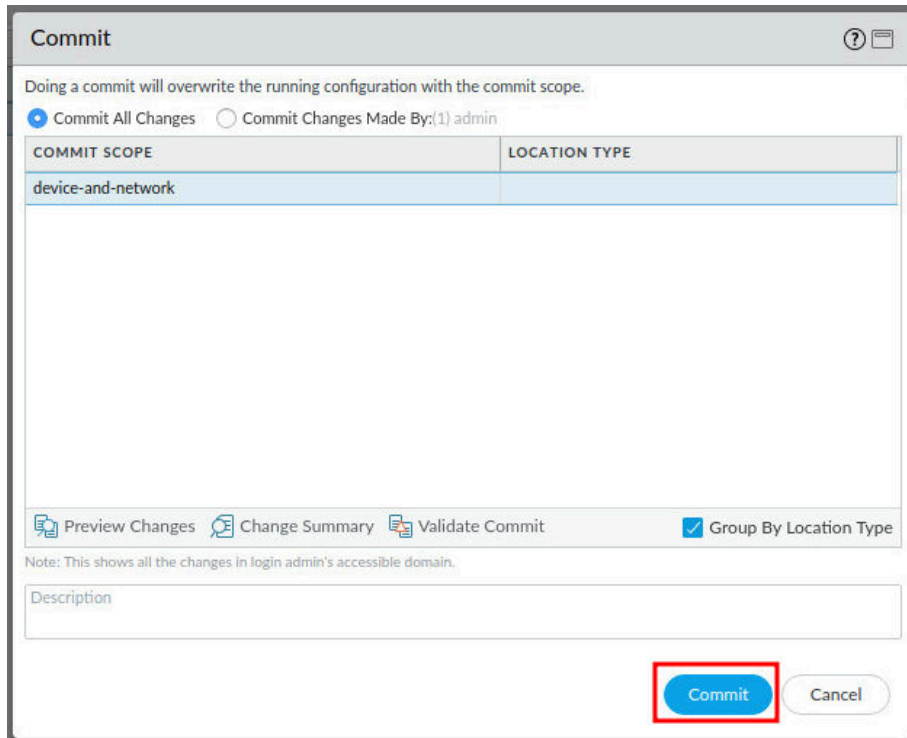
4. In the *Scheduled Log Export* window, add 5 minutes to the current time and type that in the *Scheduled Export Start Time (Daily)* field. The time format is in 24-hour time. (In this example, we want the job to run at 06:45 AM). Next, click the radio button for **FTP**. Then, in the *Hostname* field, type 192.168.50.10. Next, in the *Port* field, type 21. Then, in the *Path* field, type /. Next, in the *Username* field, type lab-user. Then, in the *Password* and *Confirm Password* fields, type paloalto. Finally, click the checkbox for **Enable FTP Passive Mode** and click **OK**.



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



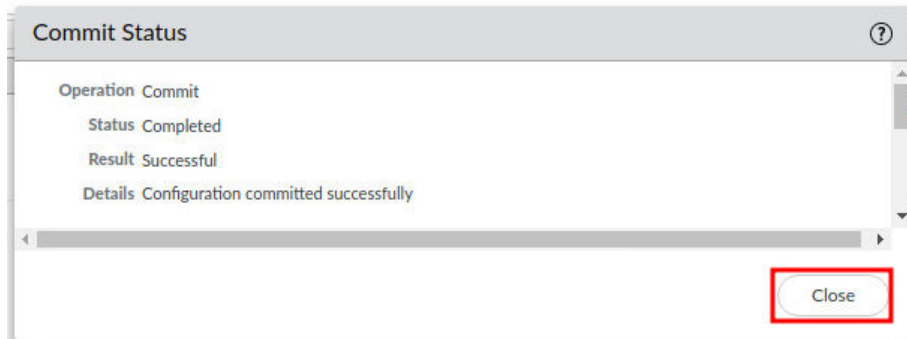
6. In the *Commit* window, click **Commit** to proceed with committing the changes.



The screenshot shows the 'Commit' window in a network management interface. At the top, a message states: 'Doing a commit will overwrite the running configuration with the commit scope.' Below this, there are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. A table with two columns, 'COMMIT SCOPE' and 'LOCATION TYPE', is shown. The first row has 'device-and-network' under 'COMMIT SCOPE' and is empty under 'LOCATION TYPE'. Below the table, there are three icons with labels: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these is a checked checkbox labeled 'Group By Location Type'. A note below reads: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right, there are two buttons: 'Commit' (highlighted with a red rectangle) and 'Cancel'.

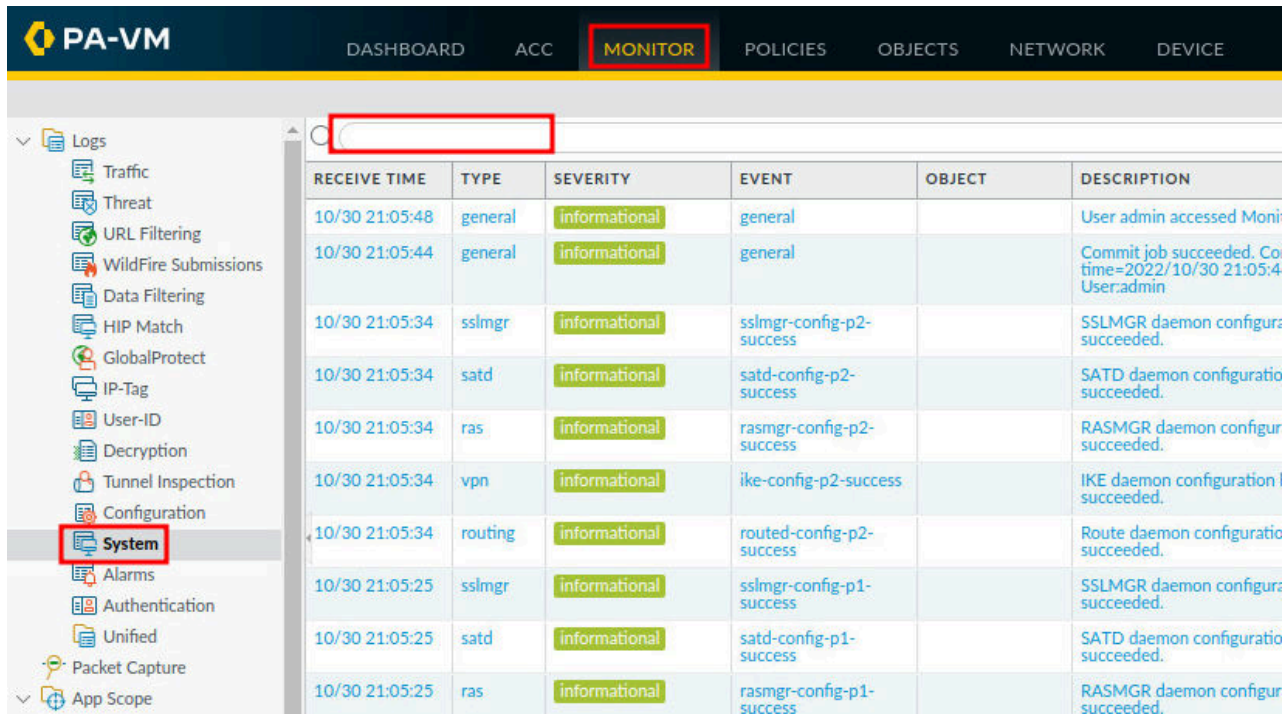
COMMIT SCOPE	LOCATION TYPE
device-and-network	

7. When the commit operation successfully completes, click **Close** to continue.



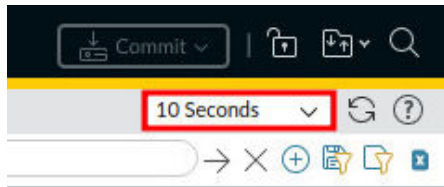
The screenshot shows the 'Commit Status' window. It displays the following information: 'Operation: Commit', 'Status: Completed', 'Result: Successful', and 'Details: Configuration committed successfully'. At the bottom right, there is a 'Close' button, which is highlighted with a red rectangle.

8. Navigate to **Monitor > Logs > System**. If there is text present in the *Filter* text box, delete it before moving to the next step.



RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
10/30 21:05:48	general	informational	general		User admin accessed Moni
10/30 21:05:44	general	informational	general		Commit job succeeded. Co time=2022/10/30 21:05:4 User:admin
10/30 21:05:34	sslmgr	informational	sslmgr-config-p2- success		SSLMGR daemon configura succeeded.
10/30 21:05:34	satd	informational	satd-config-p2- success		SATD daemon configuratio succeeded.
10/30 21:05:34	ras	informational	rasmgr-config-p2- success		RASMGR daemon configur succeeded.
10/30 21:05:34	vpn	informational	ike-config-p2-success		IKE daemon configuration succeeded.
10/30 21:05:34	routing	informational	routed-config-p2- success		Route daemon configuratio succeeded.
10/30 21:05:25	sslmgr	informational	sslmgr-config-p1- success		SSLMGR daemon configura succeeded.
10/30 21:05:25	satd	informational	satd-config-p1- success		SATD daemon configuratio succeeded.
10/30 21:05:25	ras	informational	rasmgr-config-p1- success		RASMGR daemon configur succeeded.

9. Change the *Refresh* dropbox to **10 Seconds** at the top-right.



10. After the time you set for the job to run, you will see a log entry that shows a completed log export of the traffic log to the FTP server. You will need to allow several minutes for the *System* logs to reflect the successful log export.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
10/30 21:07:02	general	informational	general		Succeed marking traffic log as exported
10/30 21:07:01	general	informational	general		Succeed exporting traffic log via ftp (last- calendar-day)
10/30 21:05:48	general	informational	general		User admin accessed Monitor tab
10/30 21:05:44	general	informational	general		Commit job succeeded. Completion time=2022/10/30 21:05:44. Jobid=157. User:admin

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