PAN9 CYBERSECURITY GATEWAY

Lab 11: Backing up Firewall Logs

Document Version: 2020-01-24

Contents

Introduction

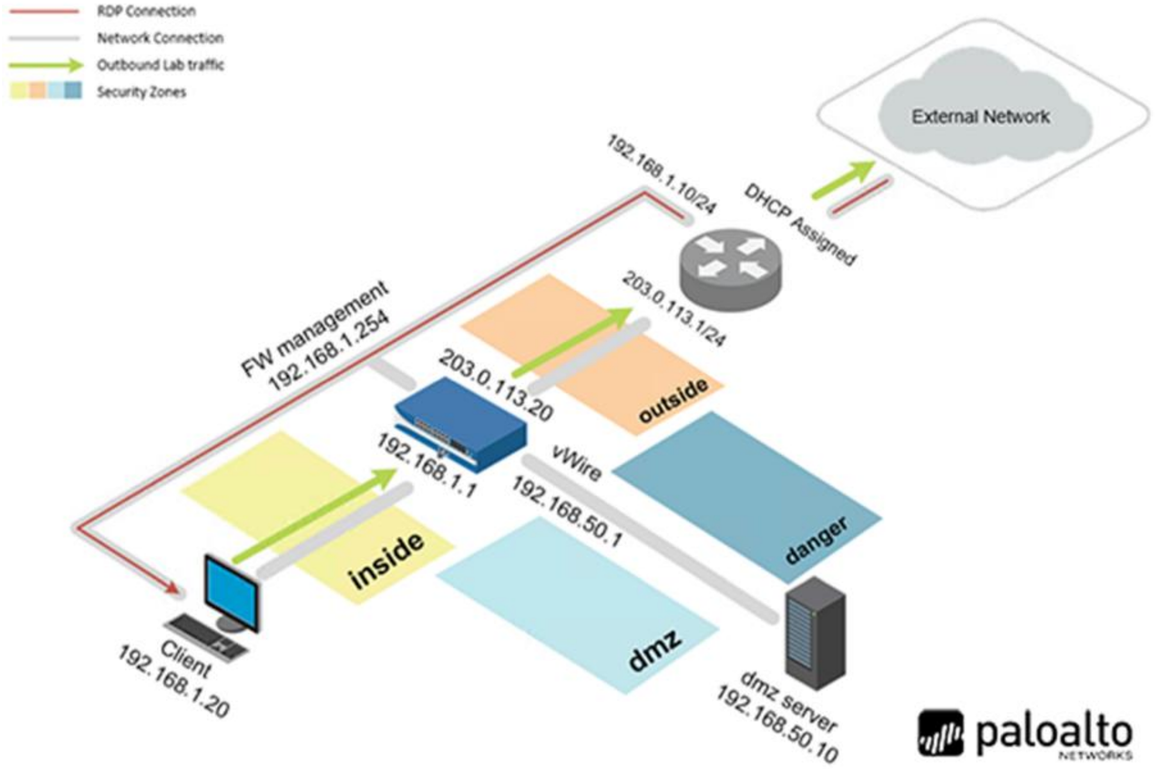
In this lab, you will back up your Firewall logs using both FTP and SCP protocols.

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.

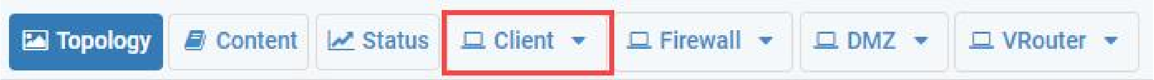
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

11 Lab: Backing up Firewall Logs

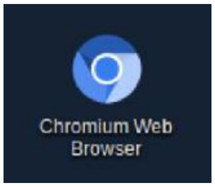
11.0 Load Lab Configuration

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

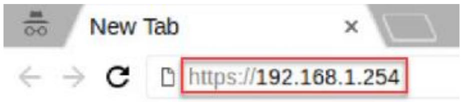
1. Click on the **Client** tab to access the Client PC.



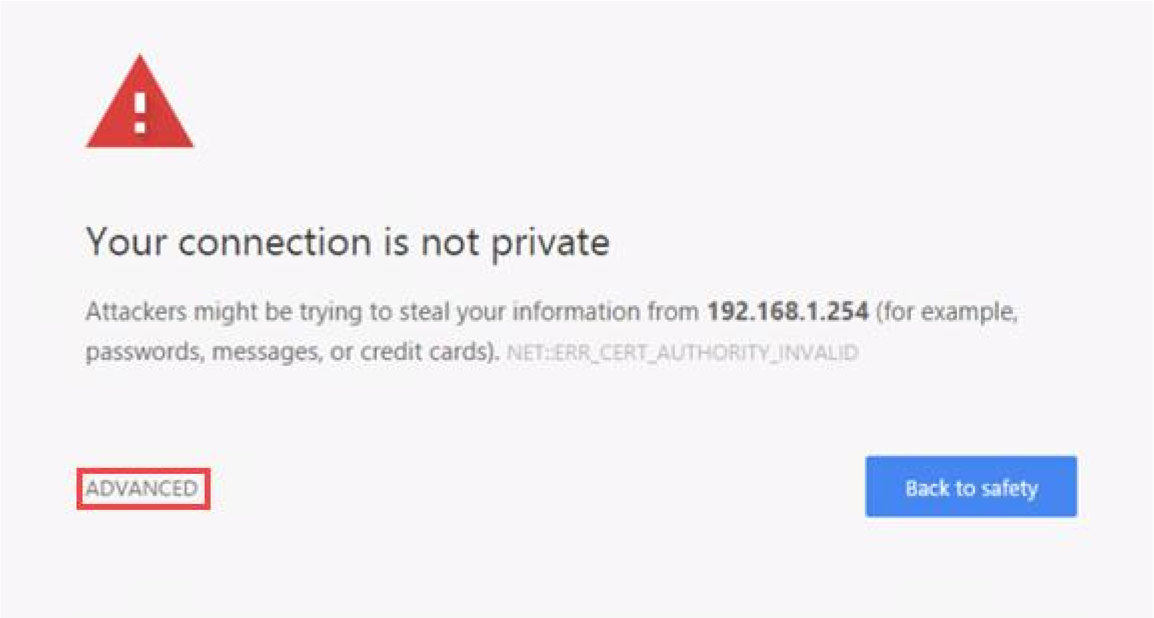
2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium** icon located on the Desktop.



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.

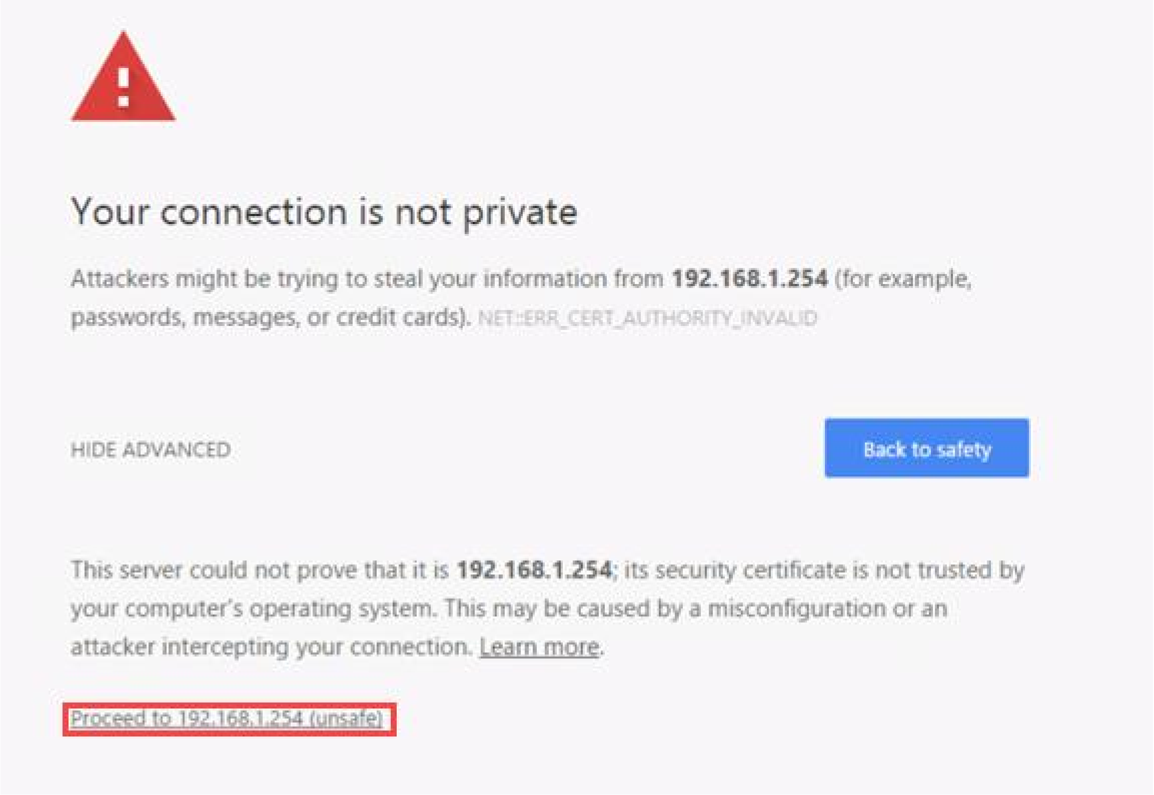


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.

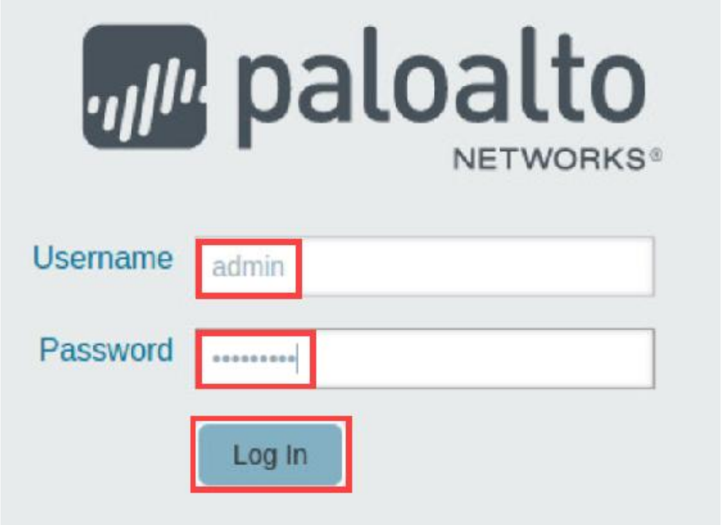


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

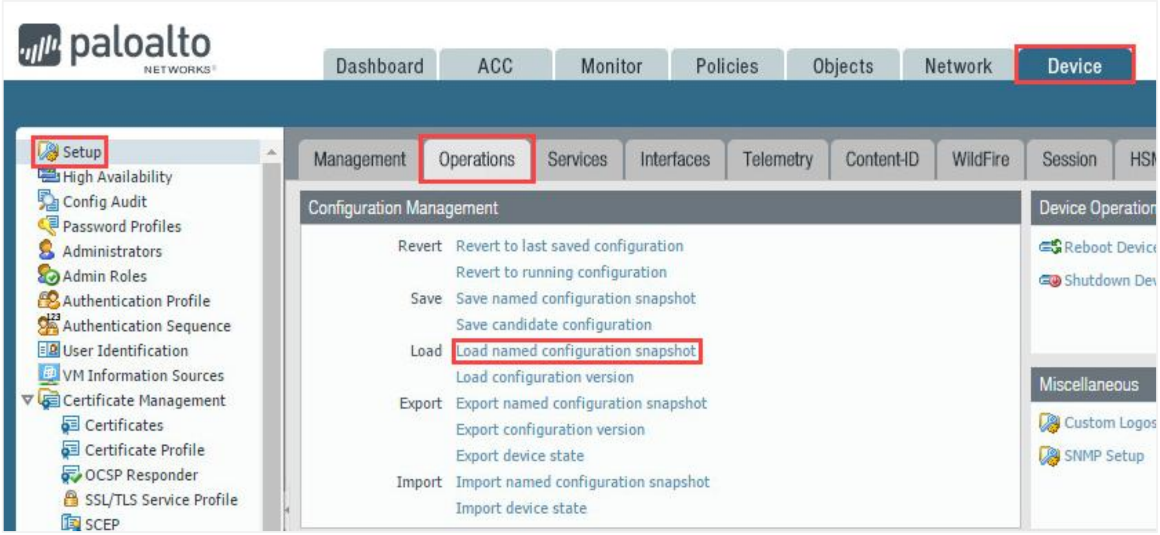
7. Log in to the Firewall web interface as username **admin**, password **Train1ng$.**



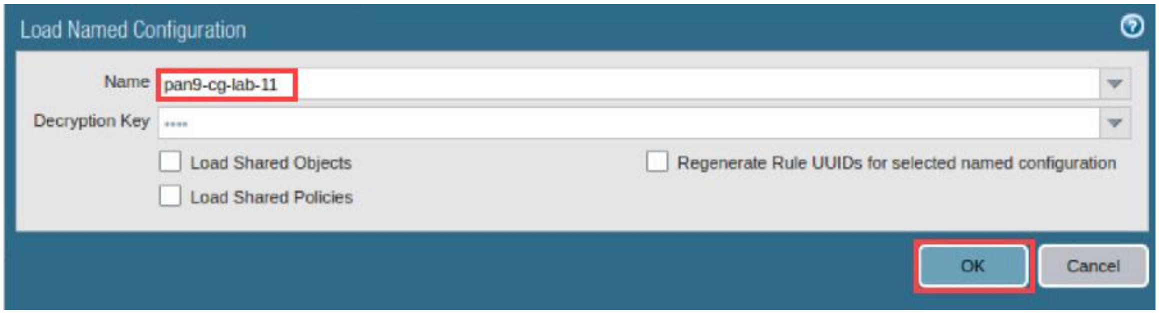
Username admin

Password ••••••••••

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 **pan9-cg-lab-11** from the *Name* dropdown box and click **OK**.



Load Named Configuration

Name pan9-cg-lab-11

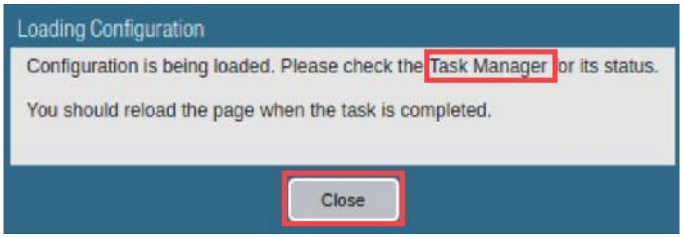
Decryption Key ••••

□ Load Shared Objects

□ Regenerate Rule UUIDs for selected named configuration

□ Load Shared Policies

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.

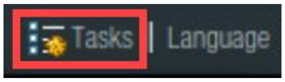


Loading Configuration

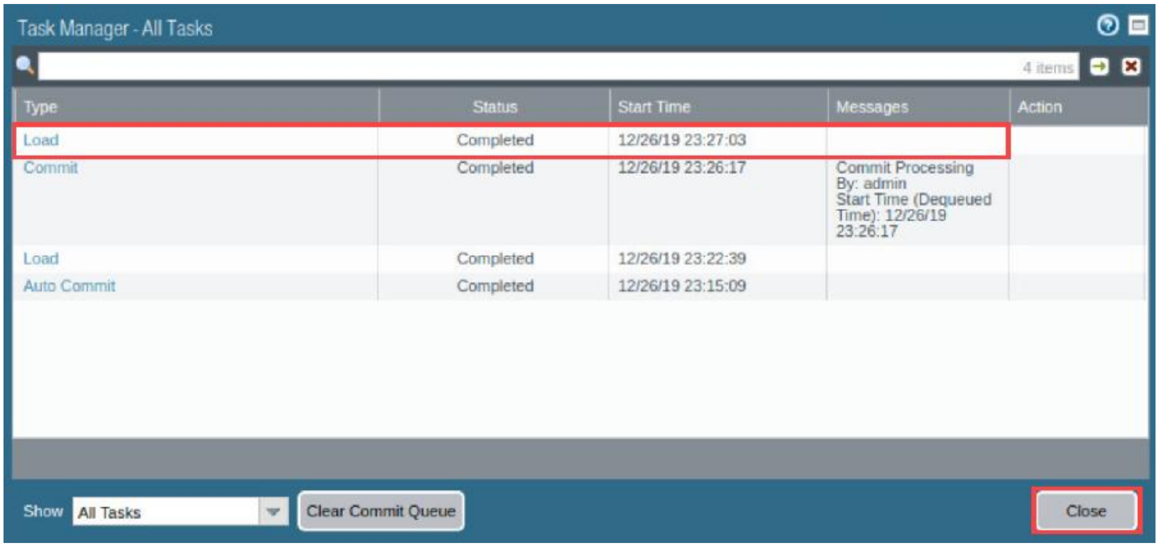
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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**.

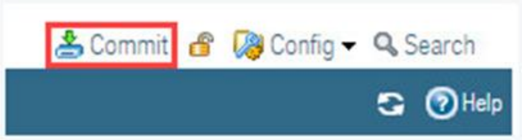


Task Manager - All Tasks

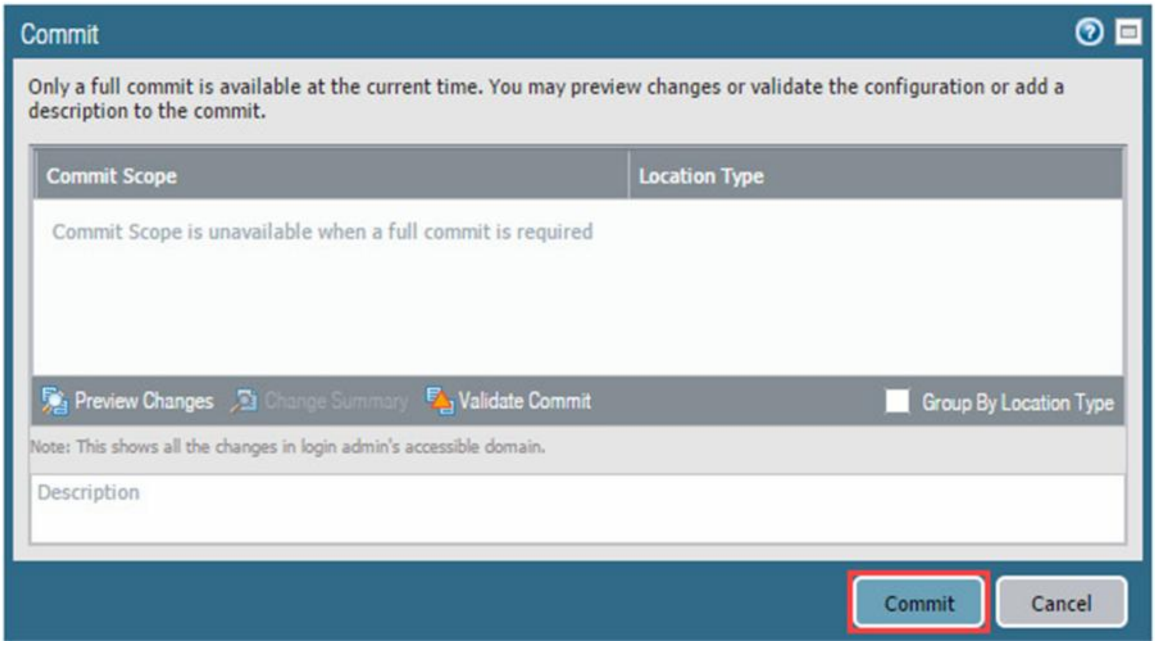
4 items

Type	Status	Start Time	Messages	Action
Load	Completed	12/26/19 23:27:03		
Commit	Completed	12/26/19 23:26:17	Commit Processing By: admin Start Time (Dequeued Time): 12/26/19 23:26:17	
Load	Completed	12/26/19 23:22:39		
Auto Commit	Completed	12/26/19 23:15:09		

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.



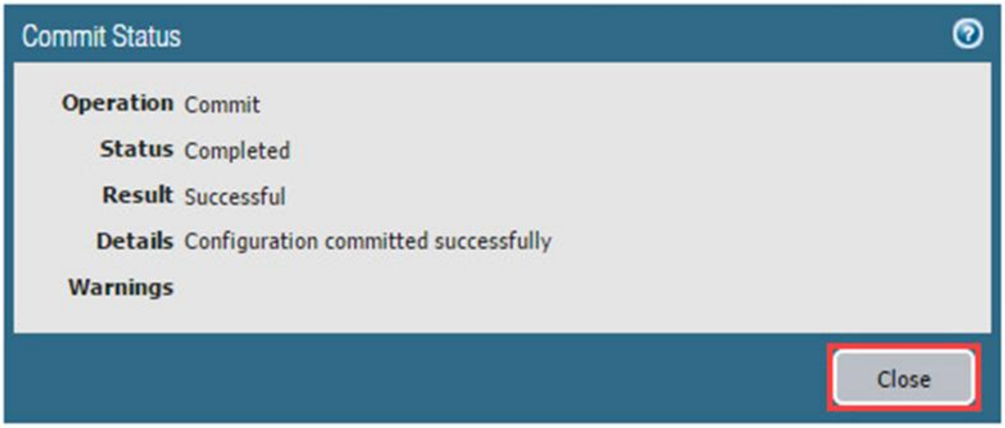
Commit

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.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

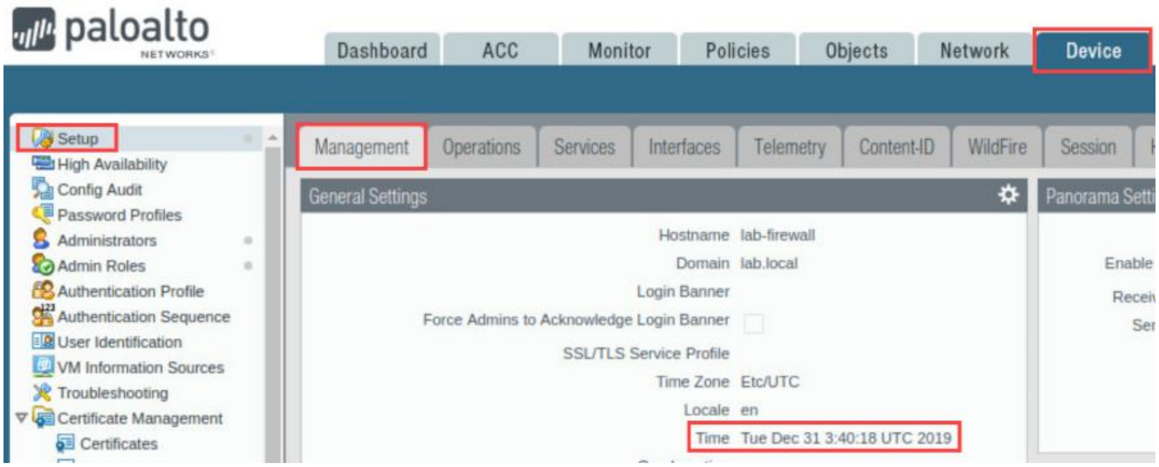
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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.

11.1 Back Up Firewall Logs

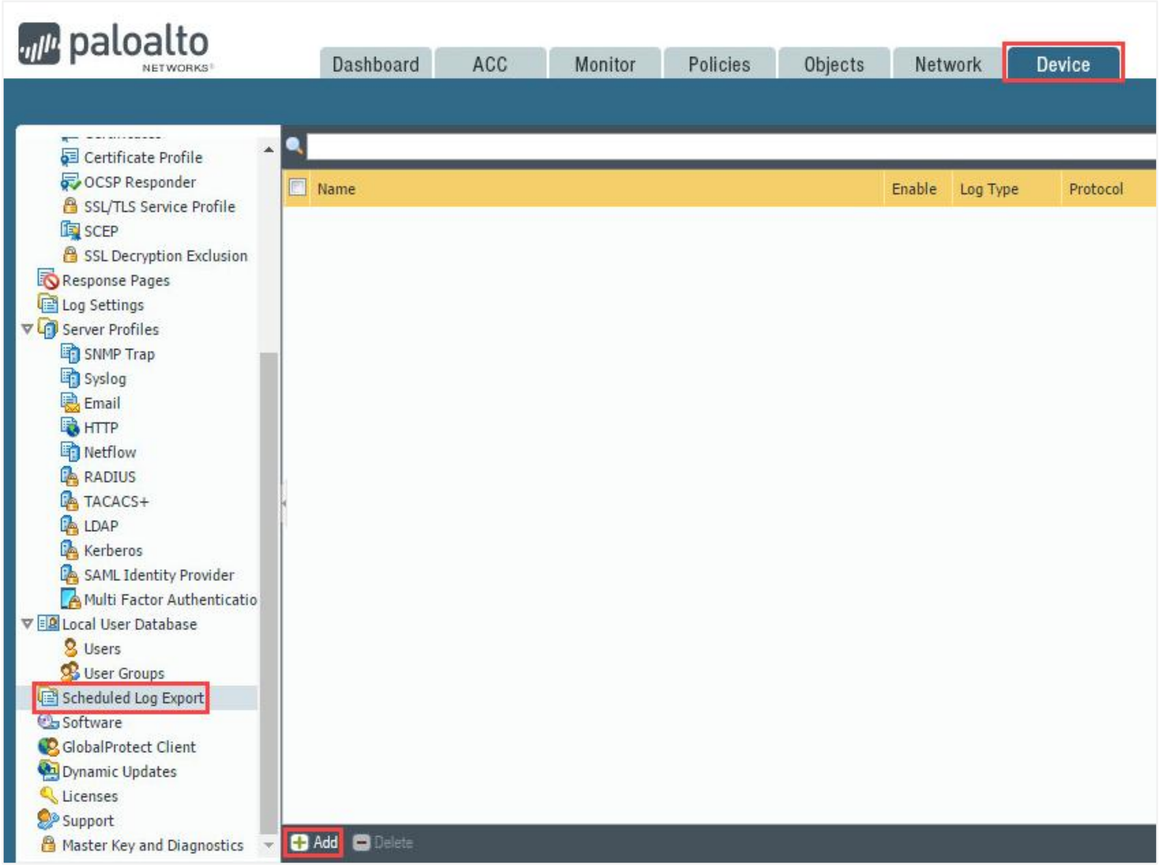
In this section, you will export Firewall logs to another location. Exporting firewall logs to an FTP Server is beneficial for keeping logs in the event that the logs are overwritten, or an unforeseen event happens to the Firewall, and the logs cannot be retrieved**.**

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 3:40 AM). If you convert this time to military time, it will be 0340 hours. Add 5 to 10 minutes to the current time to make it 0346 hours for the next step. This will allow enough time to properly configure the scheduled log export.

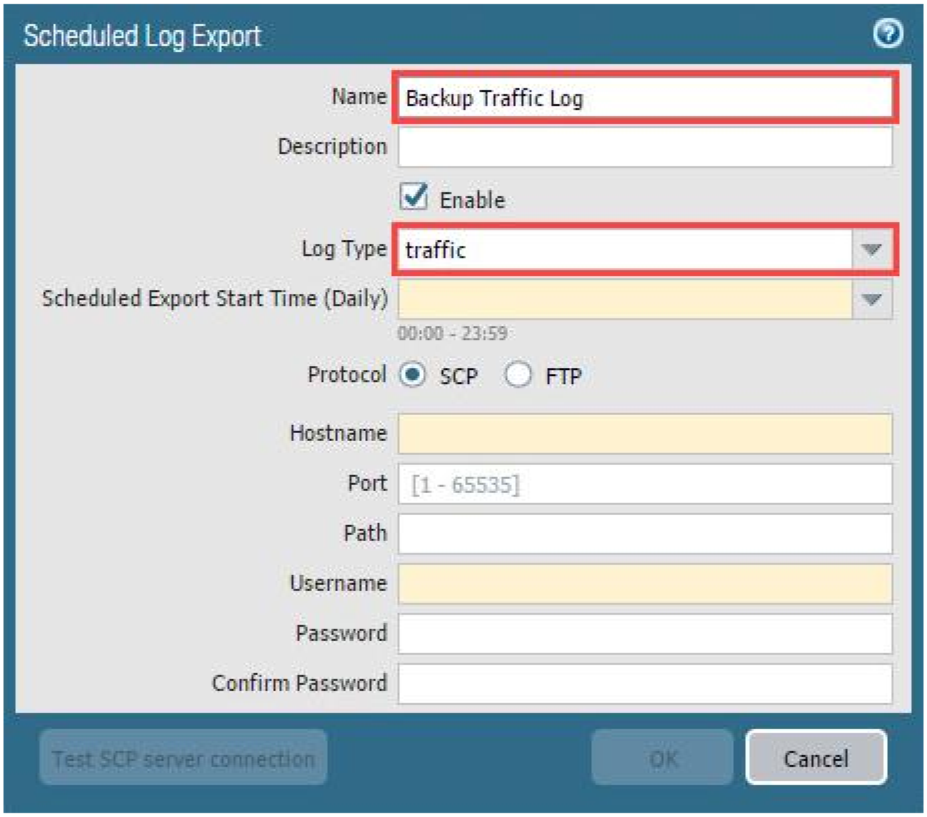


Hostname lab-firewall
Domain lab.local
Login Banner
Force Admins to Acknowledge Login Banner ☐
SSL/TLS Service Profile
Time Zone Etc/UTC
Locale en
Time Tue Dec 31 3:40:18 UTC 2019

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



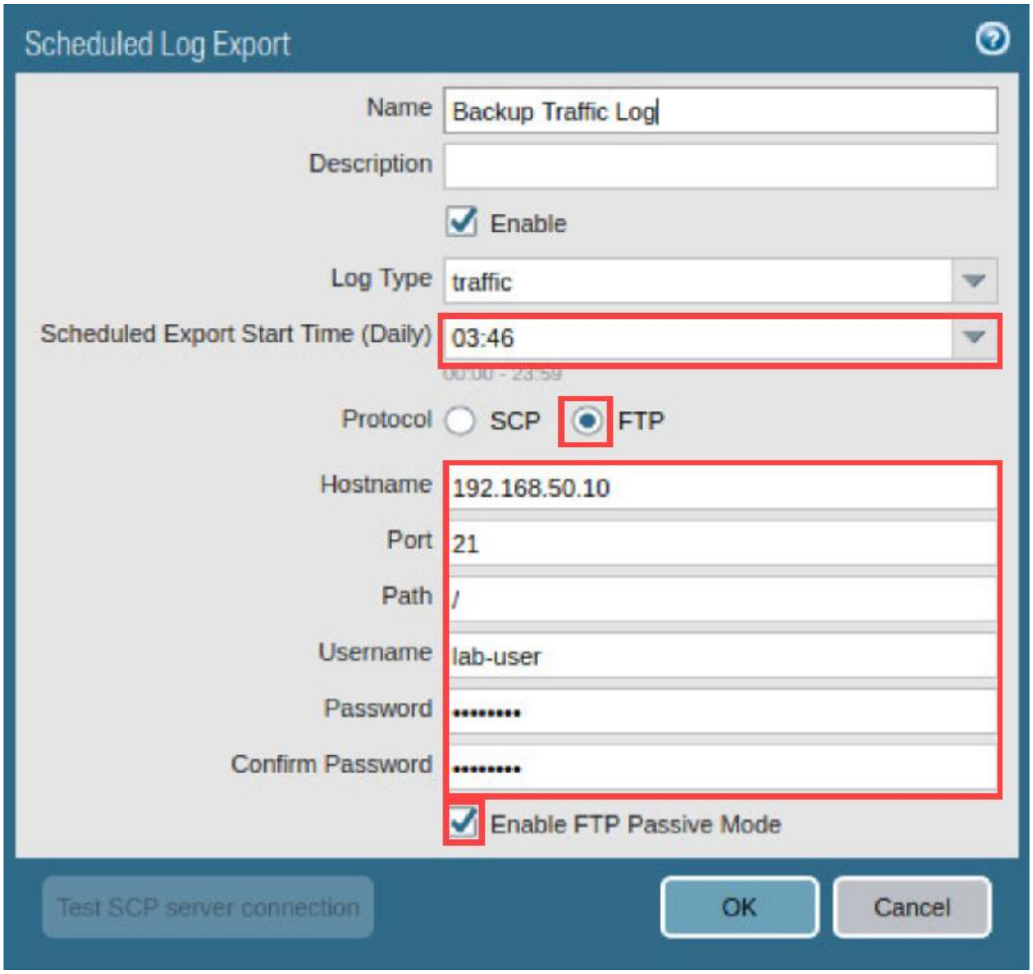
3. In the *Scheduled Log Export* window, type `Backup Traffic Log` in the *Name* field. Next, make sure the *Log Type* is set to **traffic**.



Scheduled Log Export

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

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 3:36 AM, so 03:46 is used). 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.**



Scheduled Log Export

Name: Backup Traffic Log

Description:

☑ Enable

Log Type: traffic

Scheduled Export Start Time (Daily): 03:46

00:00 - 23:59

Protocol ○ SCP ● FTP

Hostname: 192.168.50.10

Port: 21

Path: /

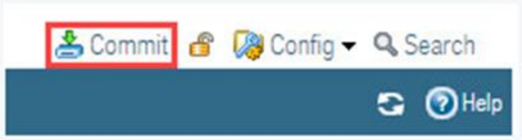
Username: lab-user

Password: ••••••••

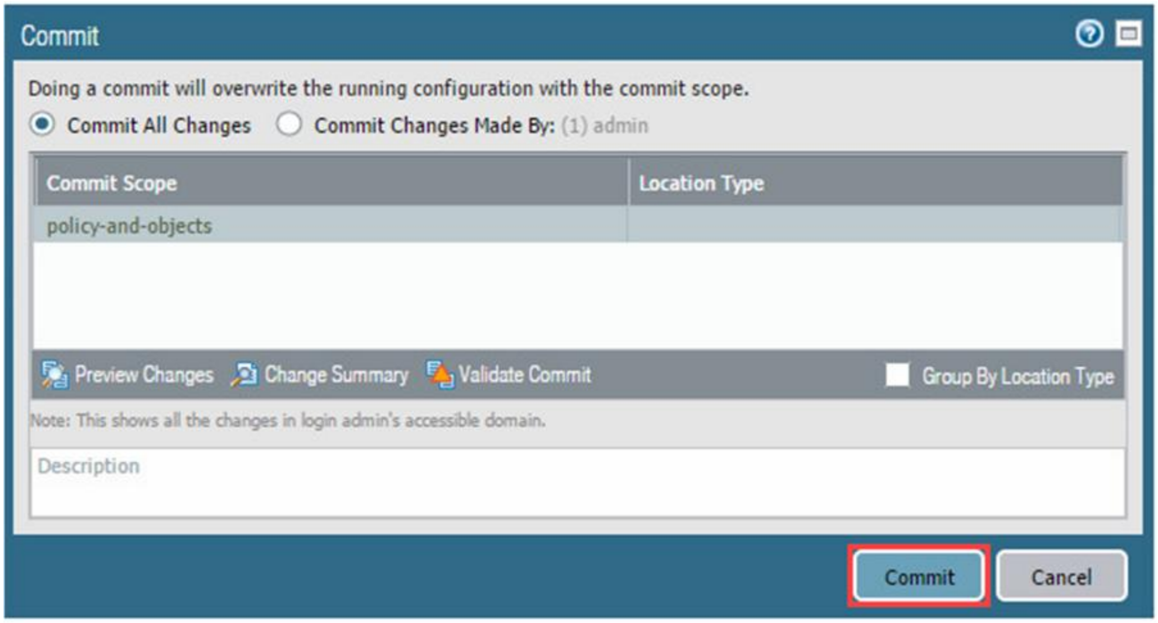
Confirm Password: ••••••••

☑ Enable FTP Passive Mode

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.



Commit

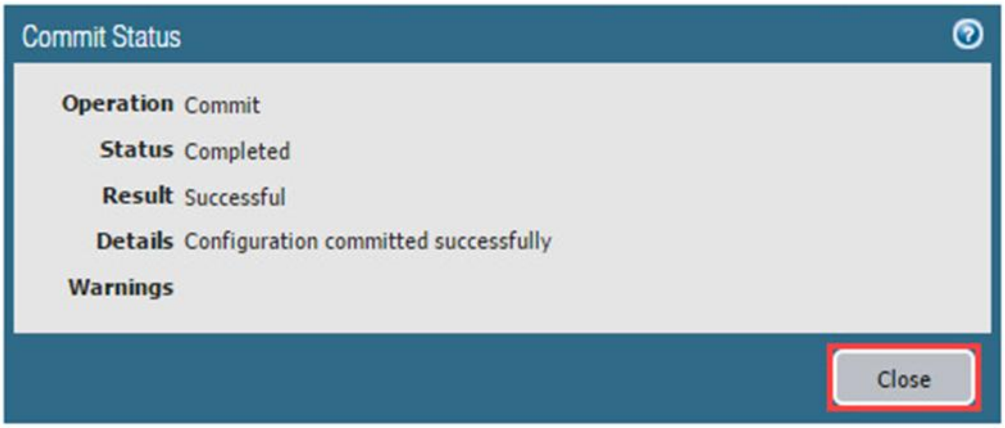
Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
policy-and-objects	

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

Operation Commit

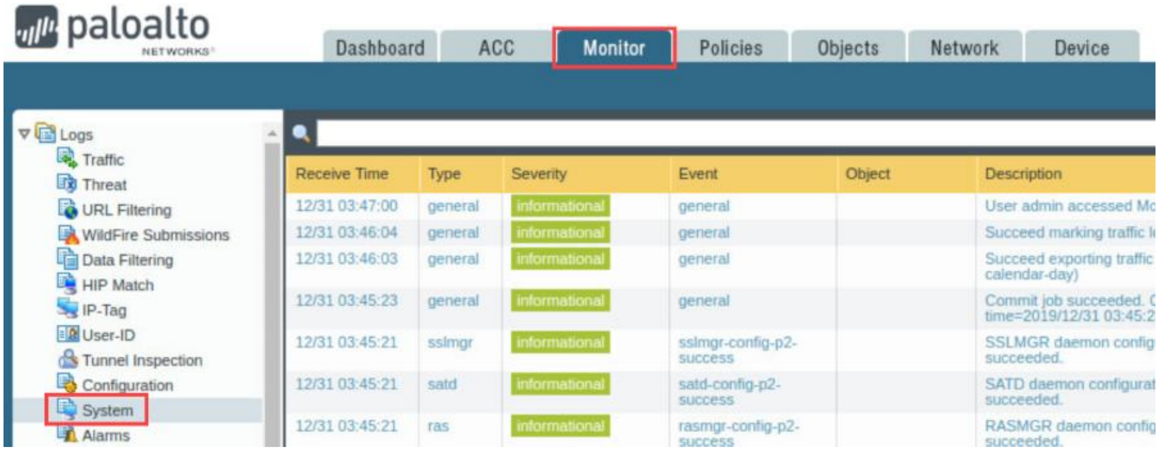
Status Completed

Result Successful

Details Configuration committed successfully

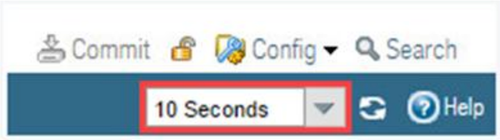
Warnings

8. Navigate to **Monitor > Logs > System**.

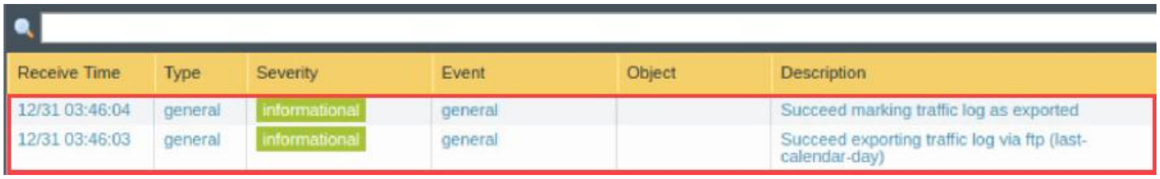


Receive Time	Type	Severity	Event	Object	Description
12/31 03:47:00	general	informational	general		User admin accessed Mc
12/31 03:46:04	general	informational	general		Succeed marking traffic l
12/31 03:46:03	general	informational	general		Succeed exporting traffic calendar-day)
12/31 03:45:23	general	informational	general		Commit job succeeded. C time=2019/12/31 03:45:2
12/31 03:45:21	sslmgr	informational	sslmgr-config-p2-success		SSLMGR daemon config succeeded.
12/31 03:45:21	satd	informational	satd-config-p2-success		SATD daemon configurat succeeded.
12/31 03:45:21	ras	informational	rasmgr-config-p2-success		RASMGR daemon config 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 2 - 3 minutes for the *System* logs to reflect the successful log export.



Receive Time	Type	Severity	Event	Object	Description
12/31 03:46:04	general	informational	general		Succeed marking traffic log as exported
12/31 03:46:03	general	informational	general		Succeed exporting traffic log via ftp (last-calendar-day)

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