SECURITY OPERATIONS FUNDAMENTALS V2

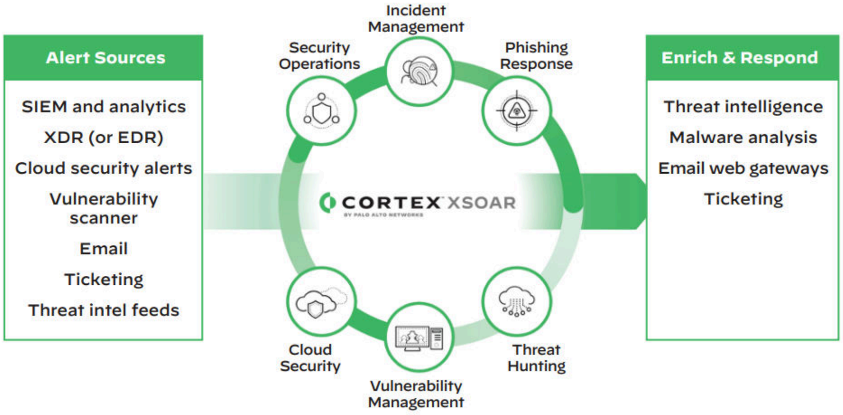
Lab 1: Network Traffic Analysis

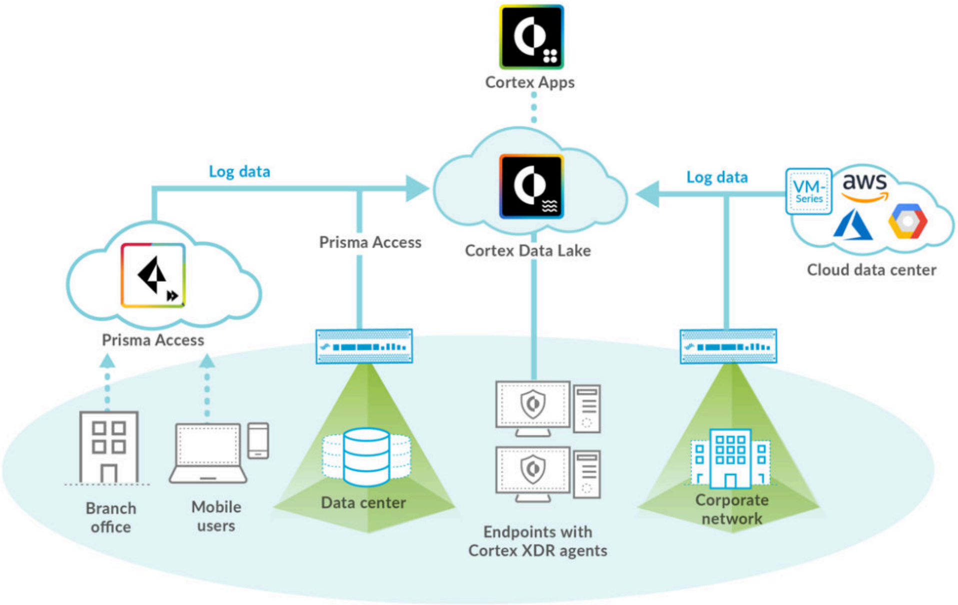
Document Version: 2022-12-23

Contents

Introduction

In this lab, you will analyze data from the Palo Alto Networks Firewall. The data will be coming from the logs on the Palo Alto Networks Firewall. To effectively utilize the information, you will become familiar with a variety of logs and how to search the logs.



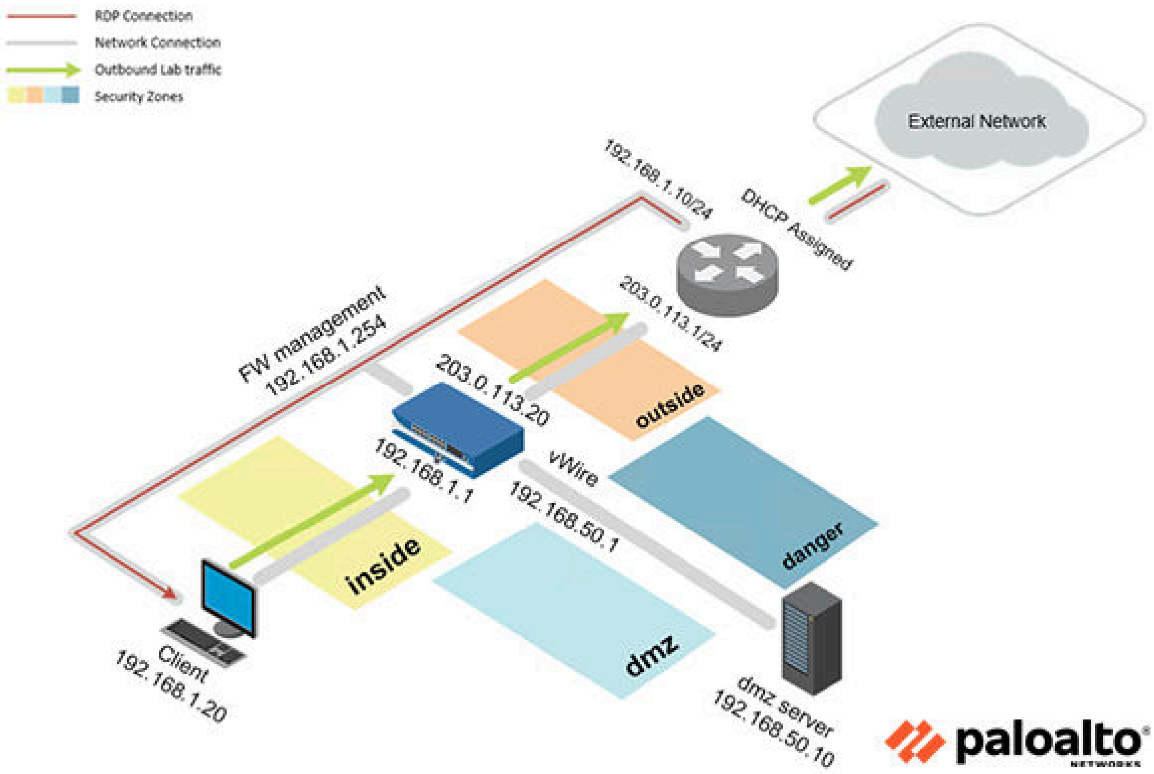


Objective

In this lab, you will perform the following tasks:

- Configure log forwarding on the firewall appliance
- Generate traffic
- Test log forwarding
- Export the firewall appliance’s traffic log as a csv file
- Perform data analysis on the exported traffic csv file

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.

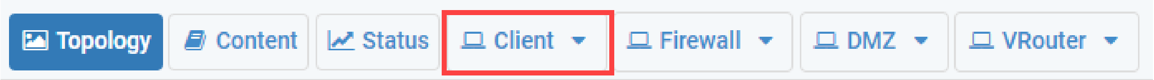
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Network Traffic Analysis

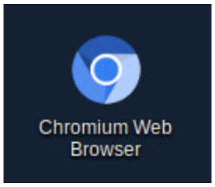
1.0 Load Lab Configuration

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

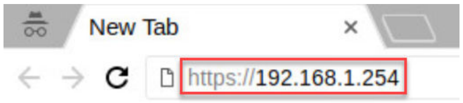
1. Click on the **Client** tab to access the client PC.



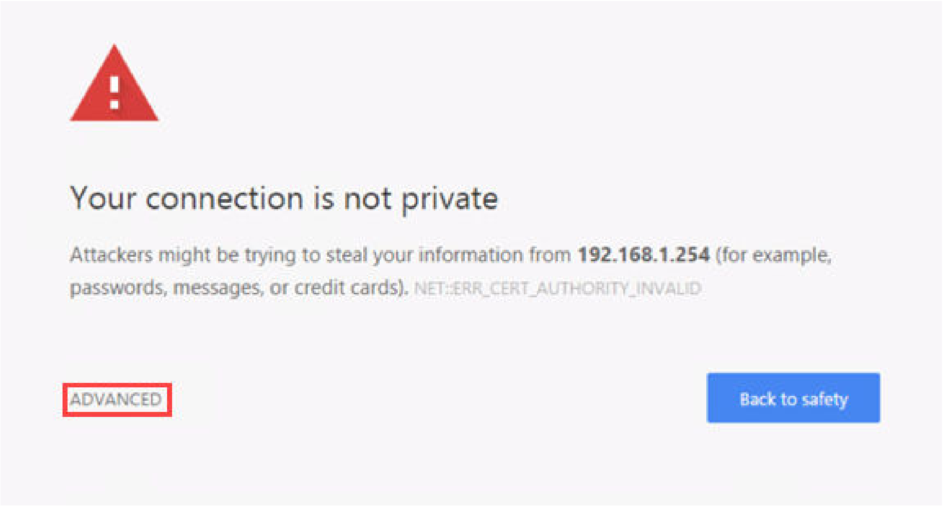
2. Log in to the client PC with the username `lab-user` and password `Pal0Alt0!`.
3. Double-click the **Chromium** icon located on the desktop.



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.

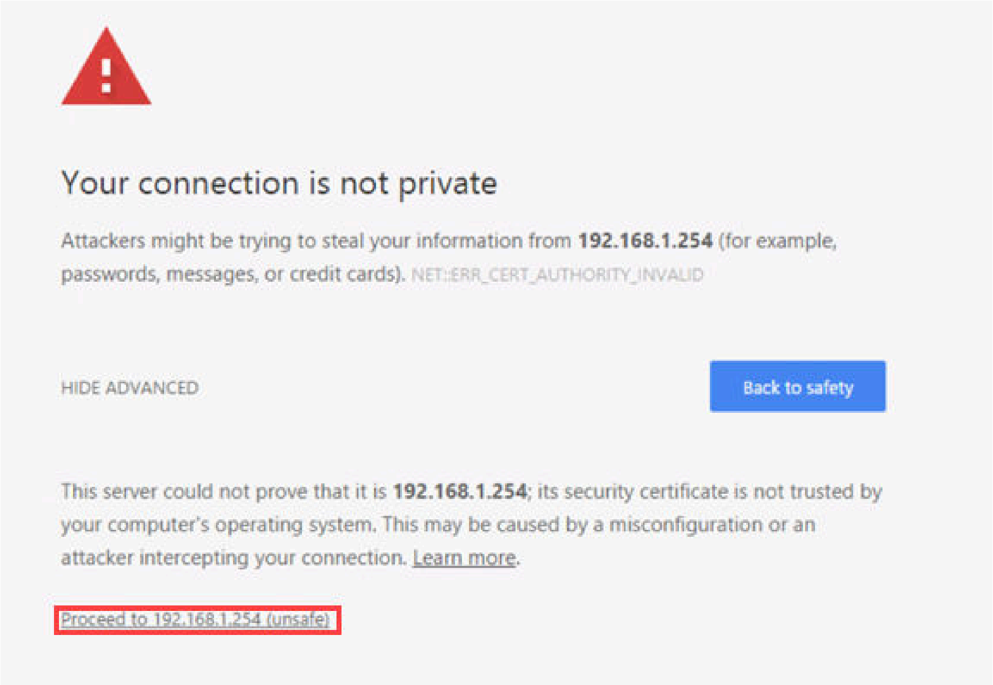


Your connection is not private

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 encounter the *“Unable to connect”* or *“502 Bad Gateway”* message while attempting to connect to the IP specified 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)**.

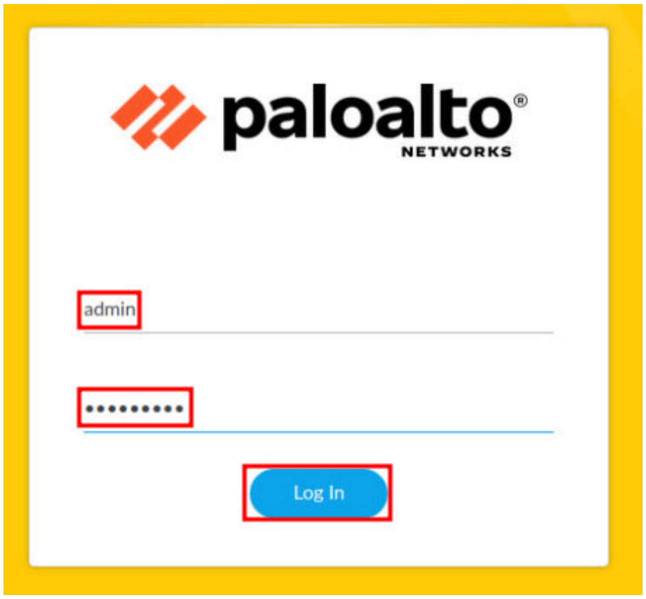


Your connection is not private

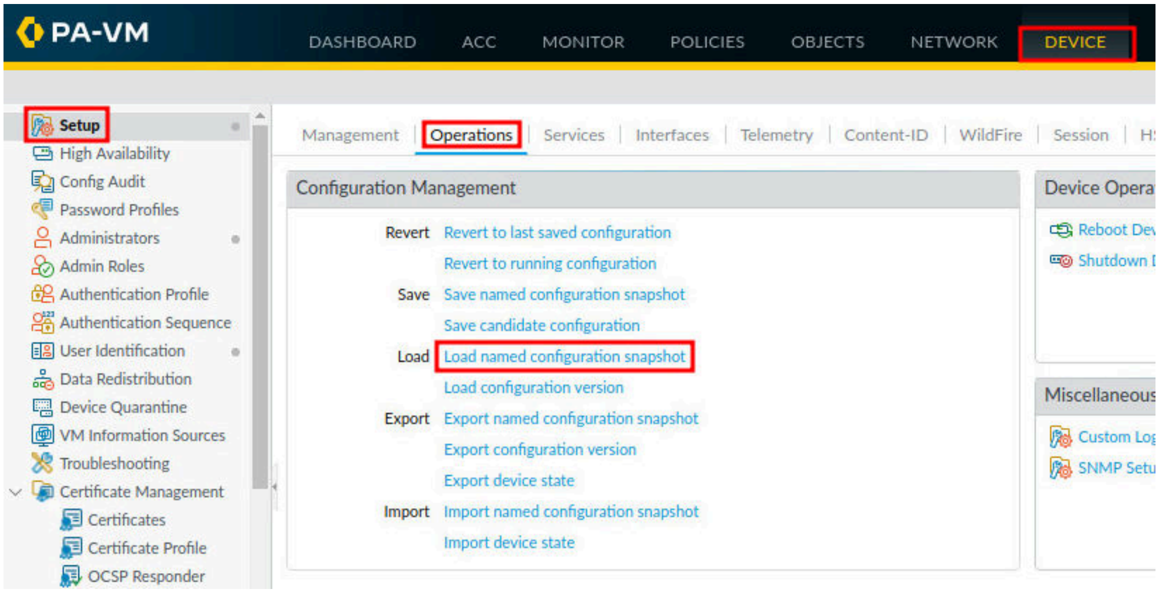
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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.

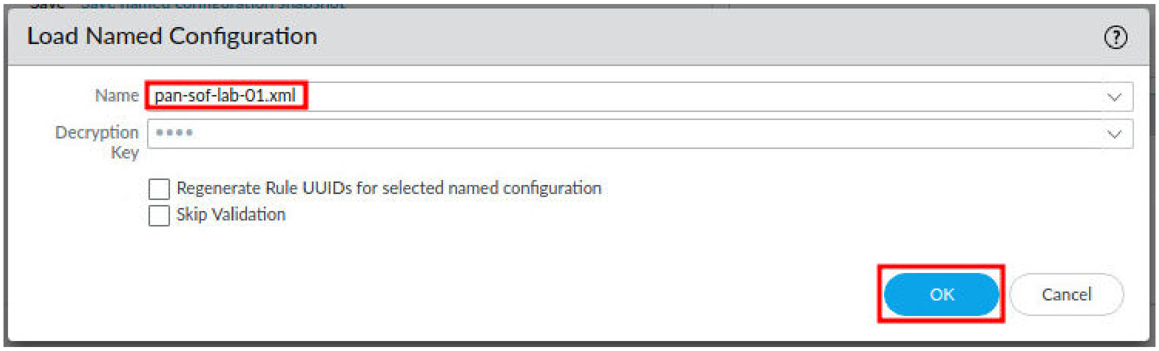
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



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-sof-lab-01.xml** from the *Name* dropdown box and click **OK**.



Load Named Configuration

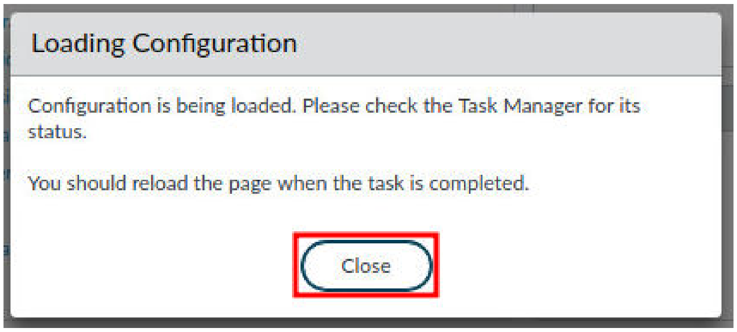
Name: pan-sof-lab-01.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

10. In the *Loading Configuration* window, a message will say *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.

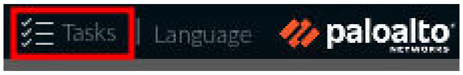


Loading Configuration

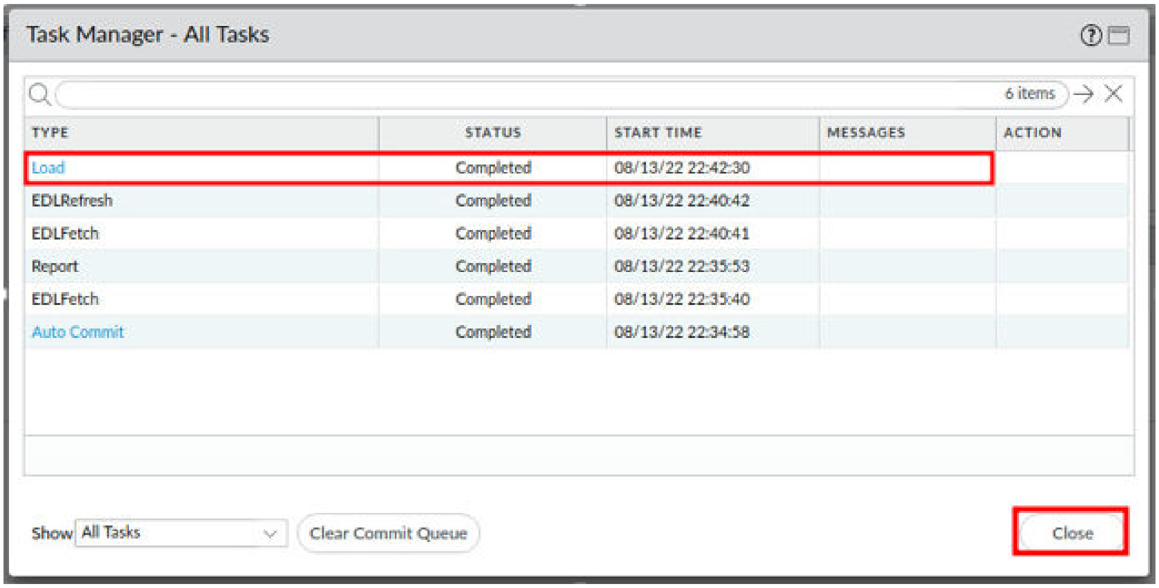
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



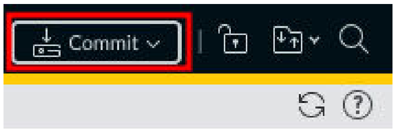
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



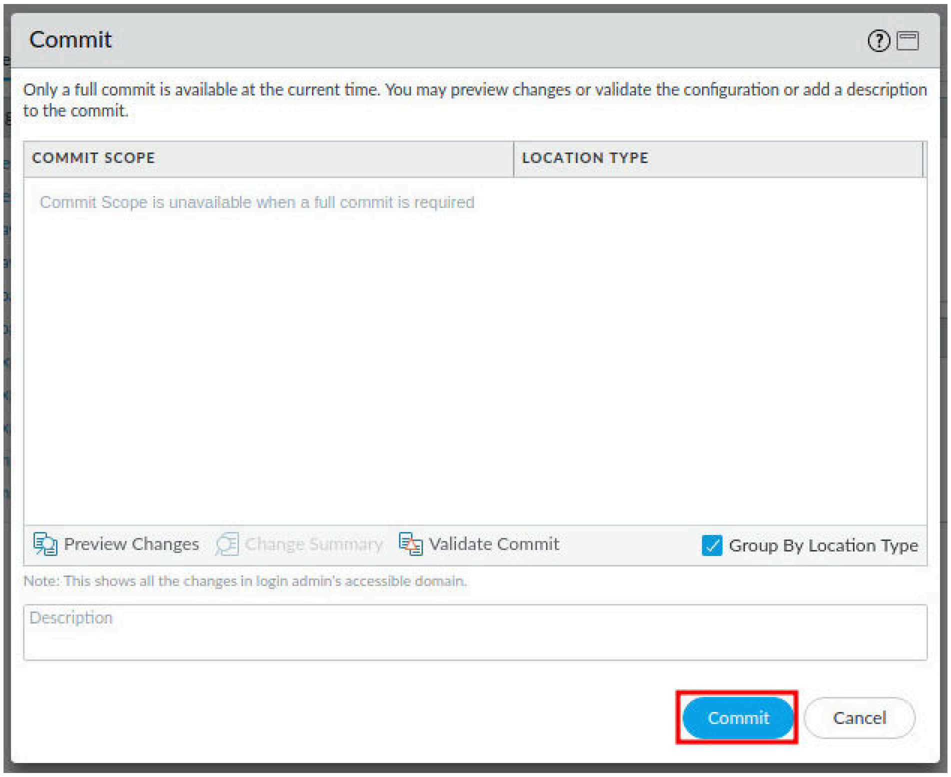
TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

Show All Tasks

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.



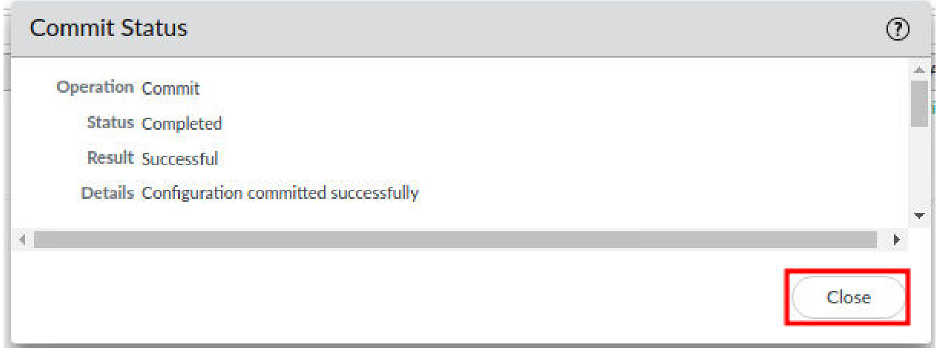
Commit

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

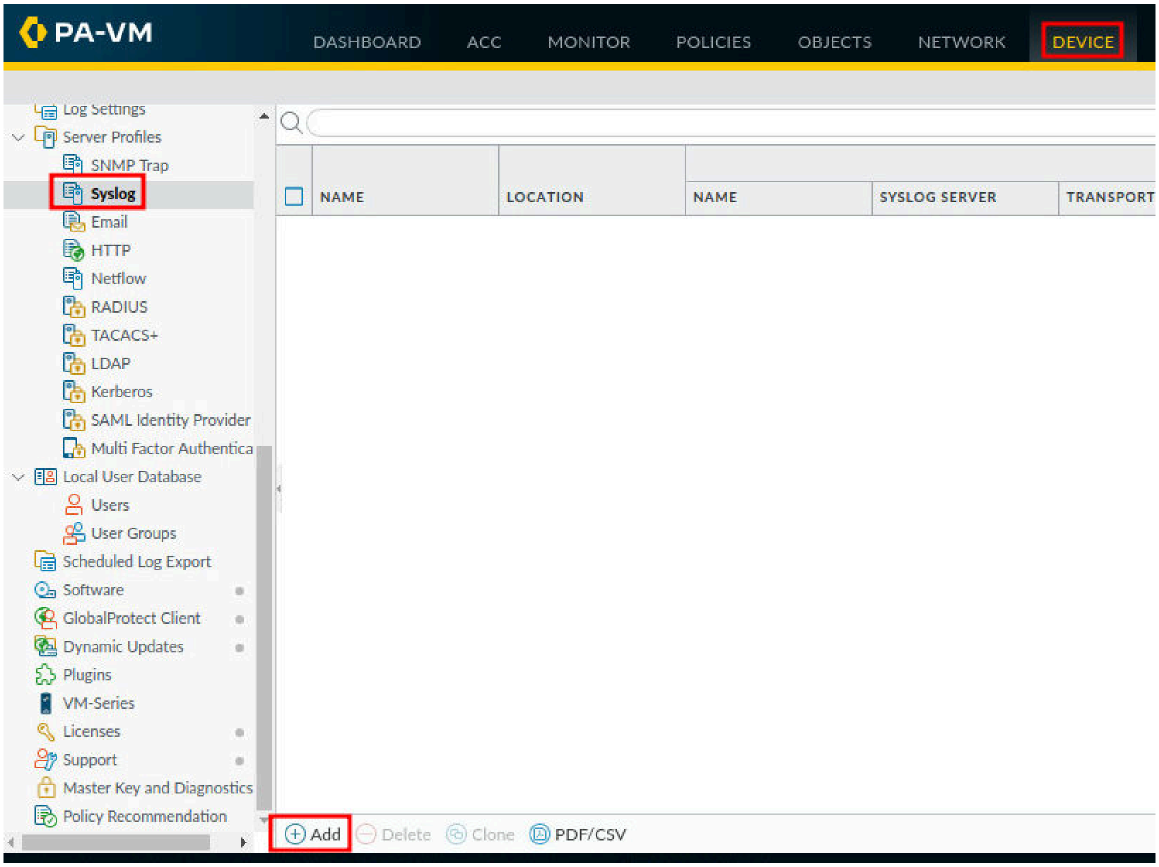
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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.

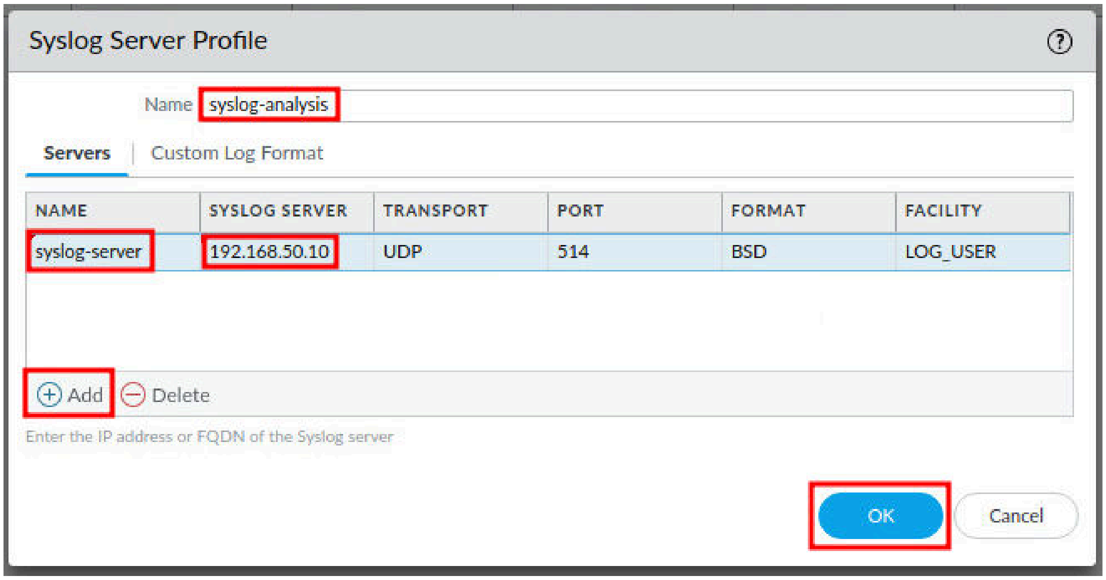
1.1 Export Firewall Log Data for Analysis

In this section, you are going to forward your Firewall's threat log to your DMZ server running syslog. Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices - such as routers, firewalls, printers - from different vendors into a central repository for archiving, analysis, and reporting. Palo Alto Networks Firewalls can forward every type of log they generate to an external Syslog server. You can use TCP or SSL for reliable and secure log forwarding, or UDP for non-secure forwarding.

1. Navigate to **Device > Server Profiles > Syslog > Add**.



2. In the *Syslog Server Profile* window, type `syslog-analysis` in the *Name* field. Click **Add**. Type `syslog-server` in the *Name* column, and `192.168.50.10` for the *Syslog Server* (the IP address of the DMZ server). Click **OK**.



Syslog Server Profile

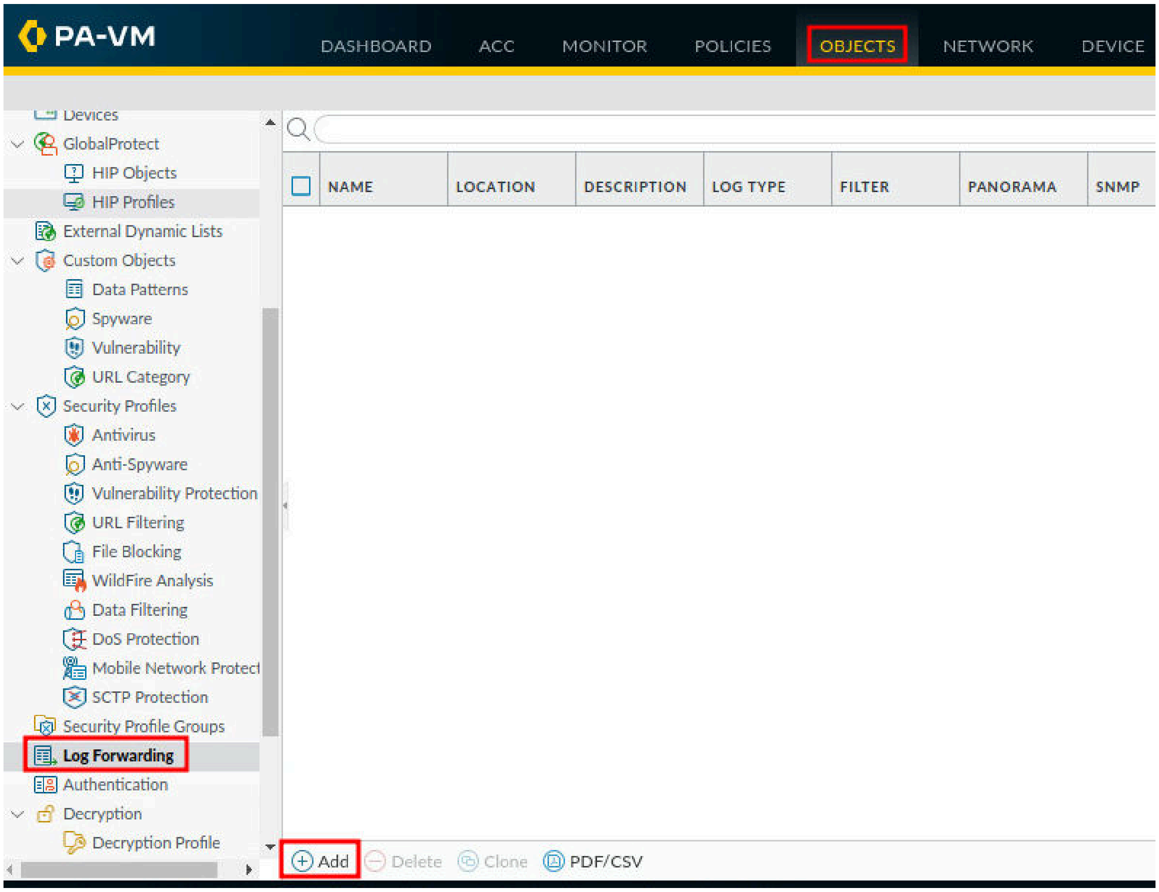
Name: syslog-analysis

Servers | Custom Log Format

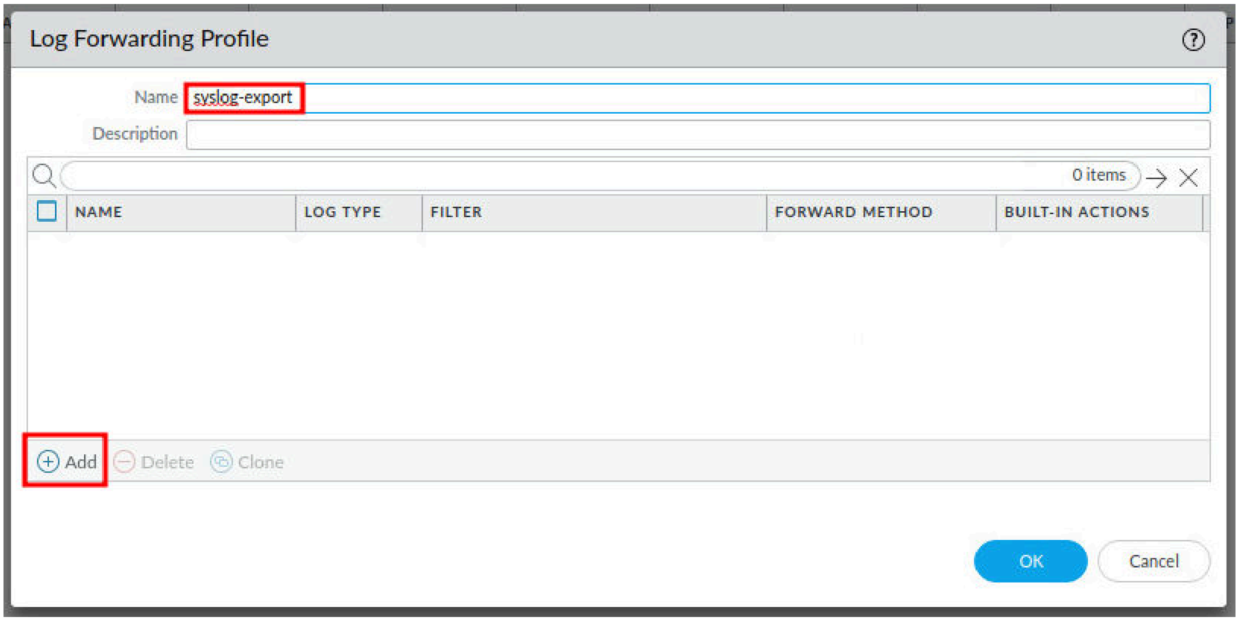
NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
syslog-server	192.168.50.10	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

3. Navigate to **Objects > Log Forwarding > Add**.



4. In the *Log Forwarding Profile* window, type `syslog-export` for the *Name*. Click **Add**.



Log Forwarding Profile

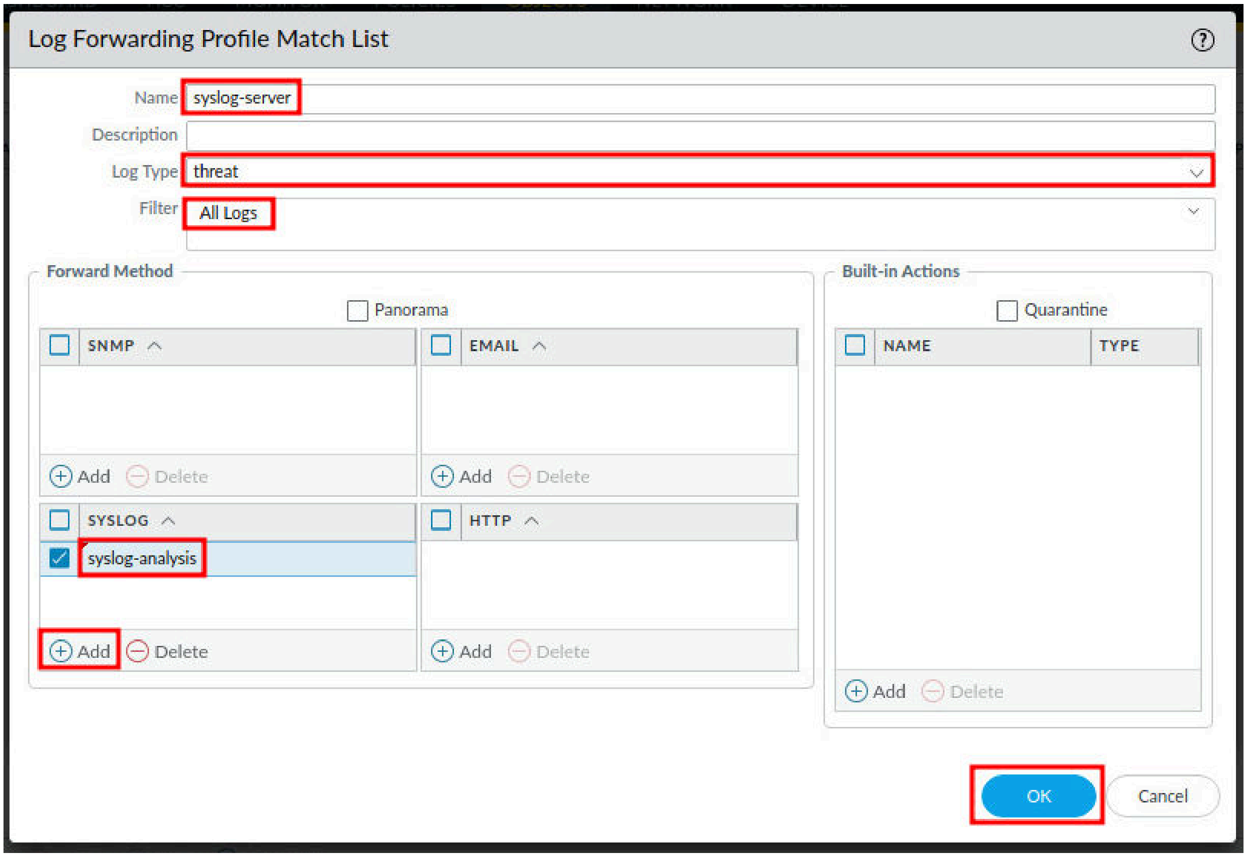
Name: syslog-export

Description:

0 items

□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS

5. In the *Log Forwarding Profile Match List* window, type `syslog-server` in the *Name* field. Next, select **threat** in the *Log Type* field and verify **All Logs** is selected in the *Filter* field. Under the *Syslog* section, click **Add**. Finally, select **syslog-analysis** (the profile you created in a previous step) and click **OK**.



Log Forwarding Profile Match List

Name: syslog-server

Description:

Log Type: threat

Filter: All Logs

Forward Method

□ Panorama

□	SNMP

□	EMAIL

□	SYSLOG
☑	syslog-analysis

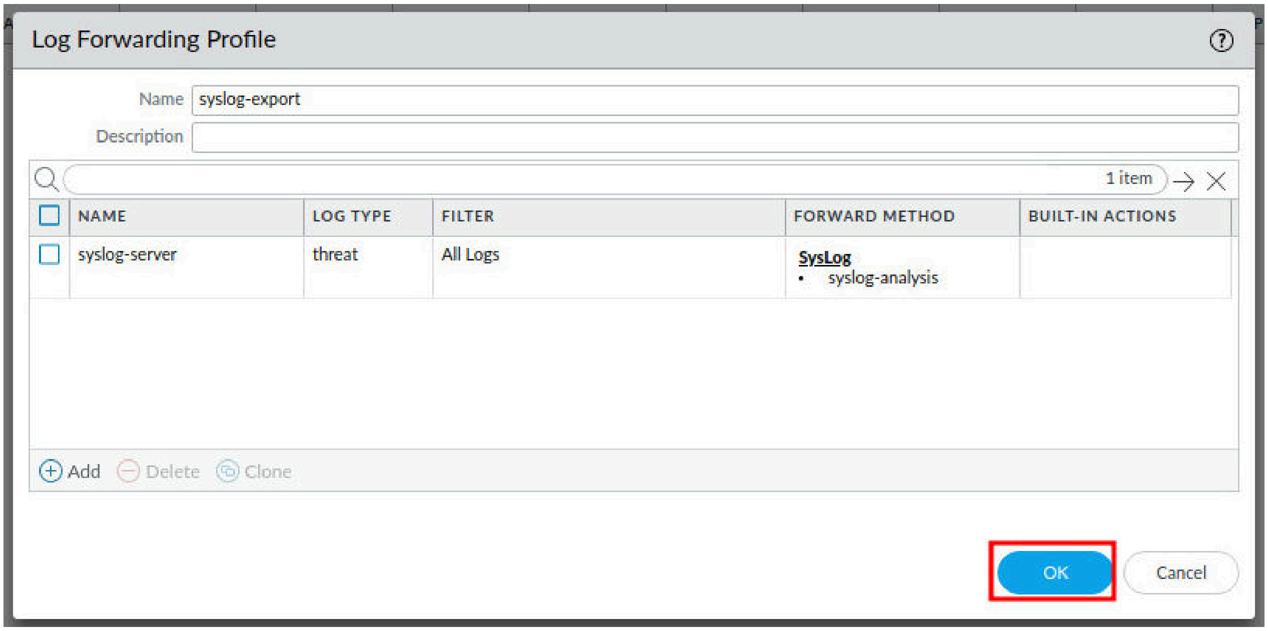
□	HTTP

Built-in Actions

□ Quarantine

□	NAME	TYPE

6. On the *Log Forwarding Profile* window, click **OK**.



Log Forwarding Profile

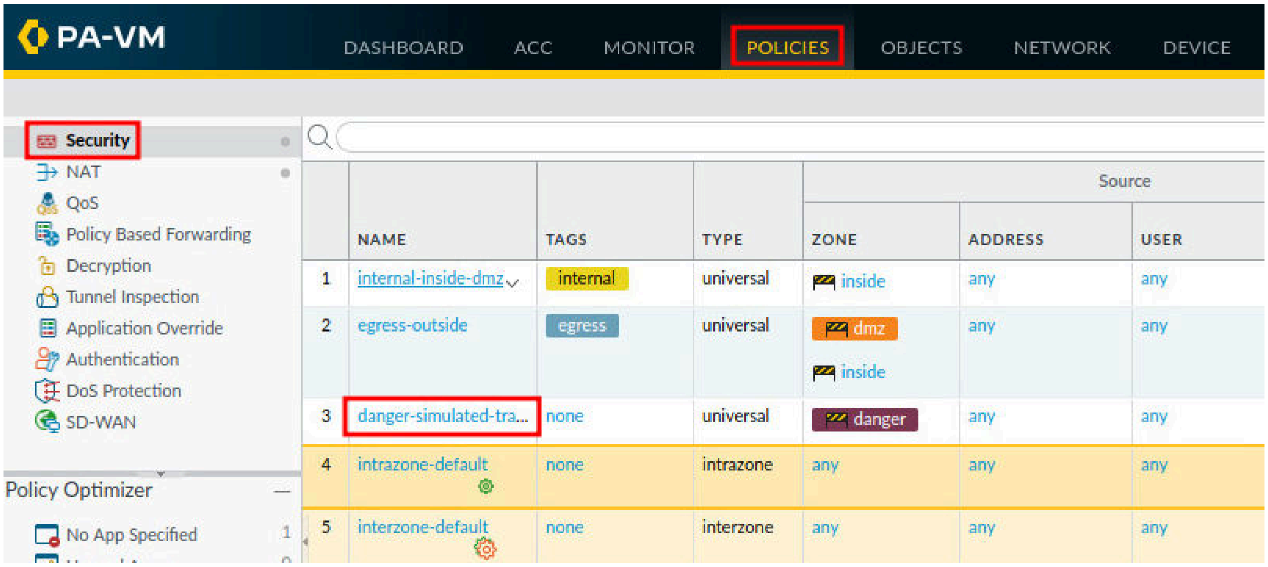
Name: syslog-export

Description:

1 item

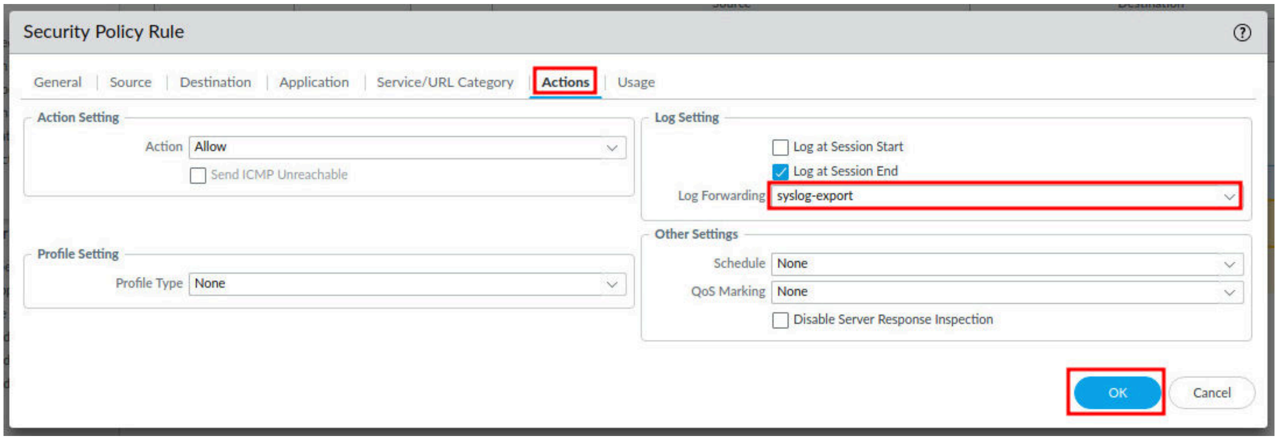
□	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
□	syslog-server	threat	All Logs	SysLog • syslog-analysis	

7. Navigate to **Policies > Security > danger-simulated-traffic**.



				Source		
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	internal-inside-dmz	internal	universal	inside	any	any
2	egress-outside	egress	universal	dmz inside	any	any
3	danger-simulated-tra...	none	universal	danger	any	any
4	intrazone-default	none	intrazone	any	any	any
5	interzone-default	none	interzone	any	any	any

8. In the *Security Policy Rule* window, click on the **Actions** tab. Select **syslog-export** in the *Log Forwarding* dropdown. Click **OK**.



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: syslog-export

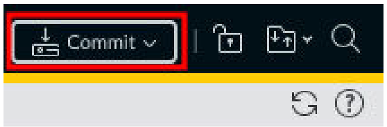
Other Settings

Schedule: None

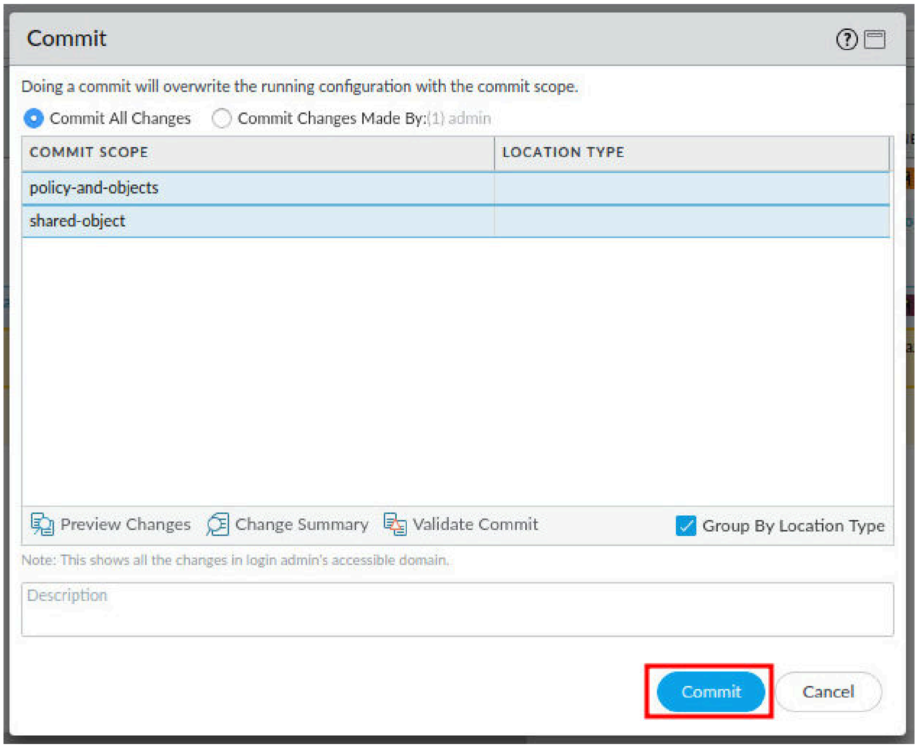
QoS Marking: None

□ Disable Server Response Inspection

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



10. In the *Commit* window, click **Commit**.



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

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

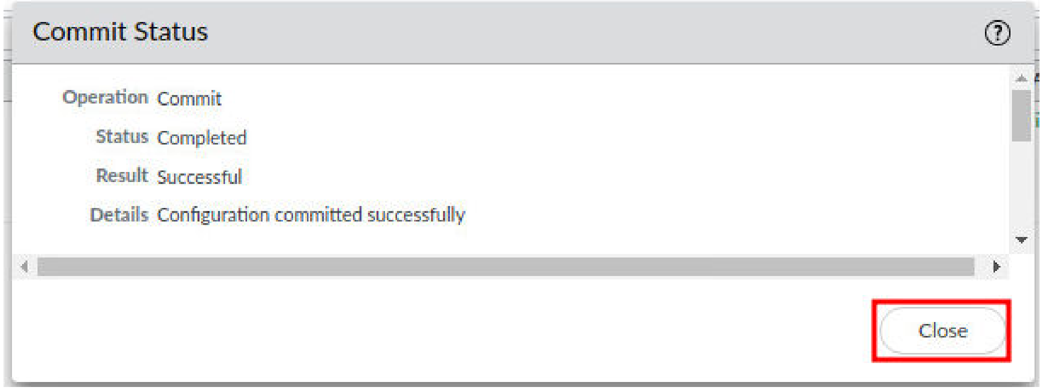
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
shared-object	

☑ Group By Location Type

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

Description

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



Commit Status

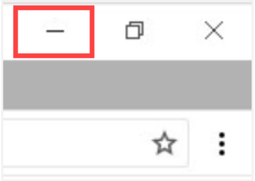
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

1.2 Generate Traffic for Firewall Analysis

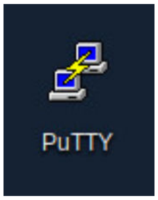
In this section, you will pre-populate the Firewall with log entries and usernames that you can observe and investigate.

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

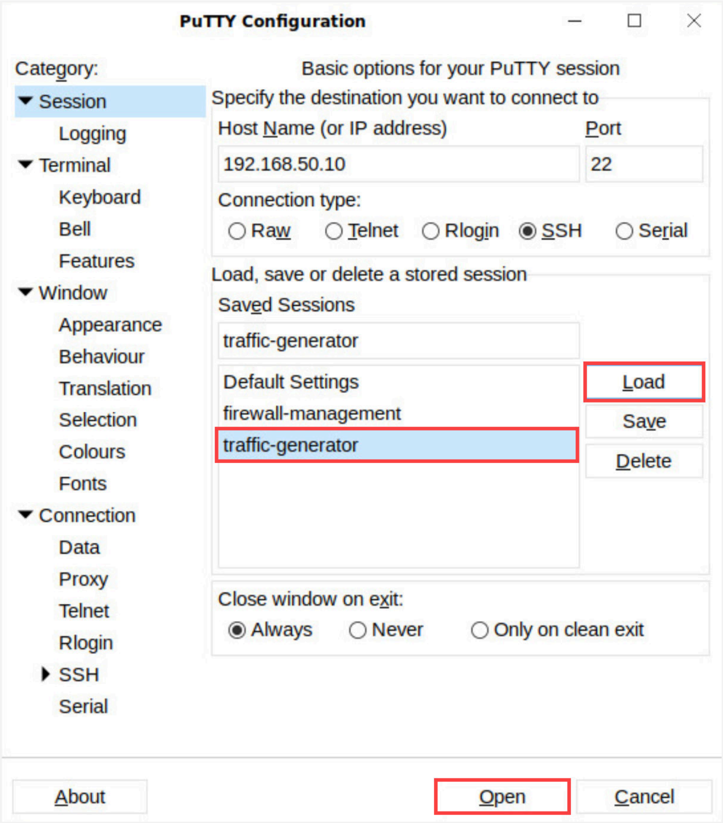
1. Minimize *Chromium* in the upper-right corner.



2. Double-click the **PuTTY** application on the client desktop.



3. From the *PuTTY Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.



Host Name (or IP address): 192.168.50.10

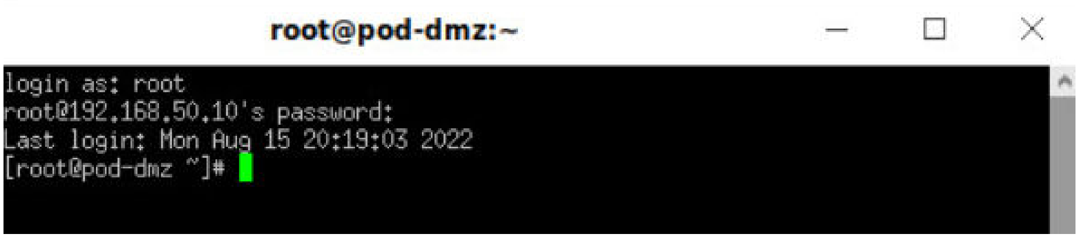
Port: 22

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

Saved Sessions: traffic-generator

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

4. At the *login as:* prompt, type `root`. Type `Pal0Alt0!` for the password, and press **Enter**.

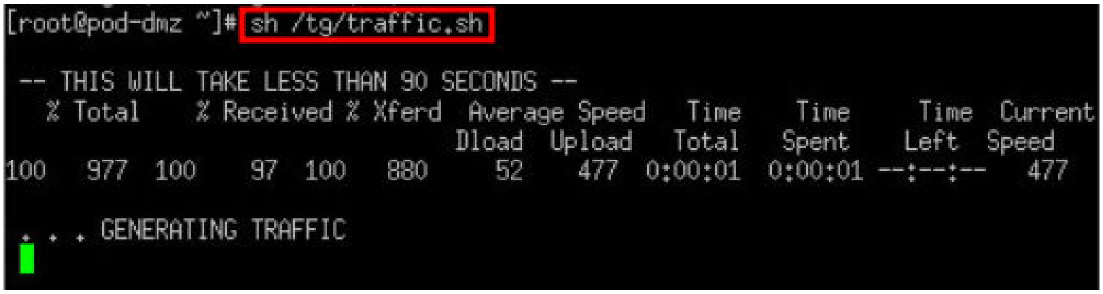


```
login as: root
root@192.168.50.10's password:
Last login: Mon Aug 15 20:19:03 2022
[root@pod-dmz ~]#
```

Notice the cursor will not move while you type the password.

5. Capture traffic packets to the Palo Alto Networks Firewall by typing the command below then pressing **Enter**.

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

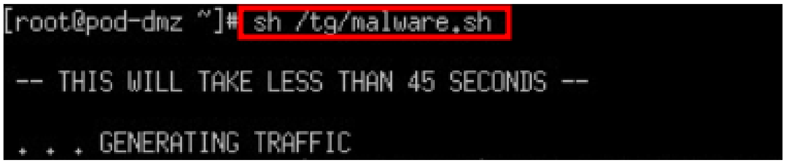


```
[root@pod-dmz ~]# sh /tg/traffic.sh

 -- THIS WILL TAKE LESS THAN 90 SECONDS --
   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   977  100    97  100   880     52    477  0:00:01  0:00:01 --:--:--   477

 . . . GENERATING TRAFFIC
```

After you execute the `.sh` command, wait until the scripts finish before proceeding to the next step.

6. Push malware packet captures to the Palo Alto Networks Firewall by typing the command below then pressing **Enter**.

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



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

 -- THIS WILL TAKE LESS THAN 45 SECONDS --

 . . . GENERATING TRAFFIC
```

After you execute the `.sh` command, wait until the scripts finish before proceeding to the next step.

Please Note

The firewall appliance will analyze this traffic and categorize it as threats and store the traffic in its threat log. The firewall's log forwarding profile will also forward this log traffic to your DMZ server's syslog server for permanent storage and for further analysis to possibly include machine learning (ML) analysis.

7. Once the scripts finish executing, type `exit` then press **Enter** to end the PuTTY ssh session to **192.168.50.10** (DMZ server)**.**

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

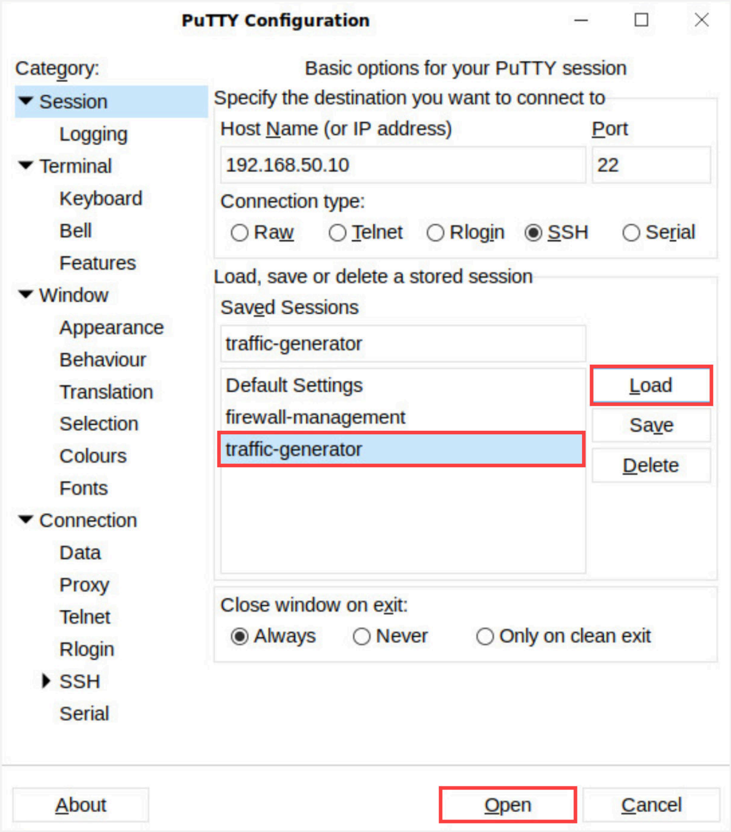
1.3 Log Analysis

In this section, you will view the log data on the DMZ server.

> **Please Note**
>
> Organizations using Cortex XDR and XSOAR would export their logs from endpoints, network appliances, firewall appliances and cloud service providers to the Cortex Data lake for further data analysis incorporating machine learning (ML). ML programs can discover obscure incidences of compromise and report these incidences to the Security Operations Center's Cortex XSOAR service for event triage and mitigation.

1. Double-click the **PuTTY** application on the client desktop.

2. From the *PuTTY Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.50.10

Port: 22

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

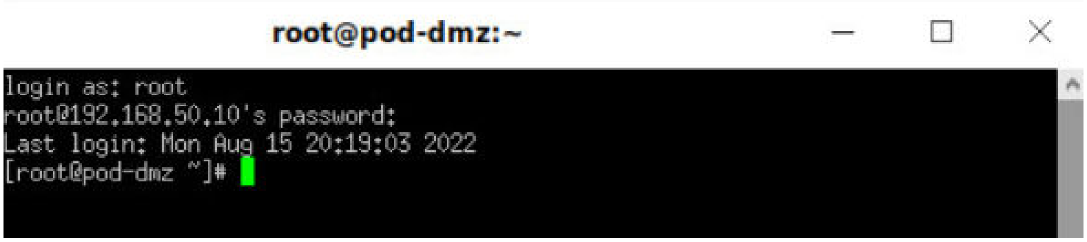
Load, save or delete a stored session

Saved Sessions: traffic-generator

Default Settings
firewall-management
traffic-generator

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

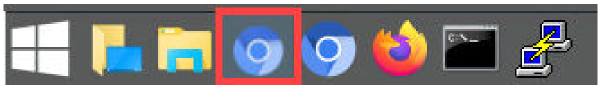
3. At the *login as:* prompt, type `root`. Type `Pal0Alt0!` for the password, and press **Enter**.



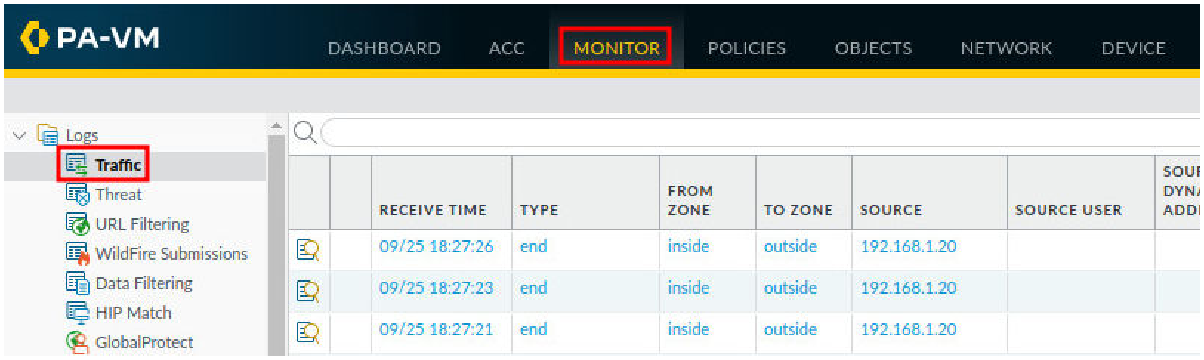
```
login as: root
root@192.168.50.10's password:
Last login: Mon Aug 15 20:19:03 2022
[root@pod-dmz ~]#
```

Notice the cursor will not move while you type the password.

4. Navigate back to the *Palo Alto Networks Firewall Web-UI* by clicking on the minimized **Chromium** icon in the lower-left of the student desktop.

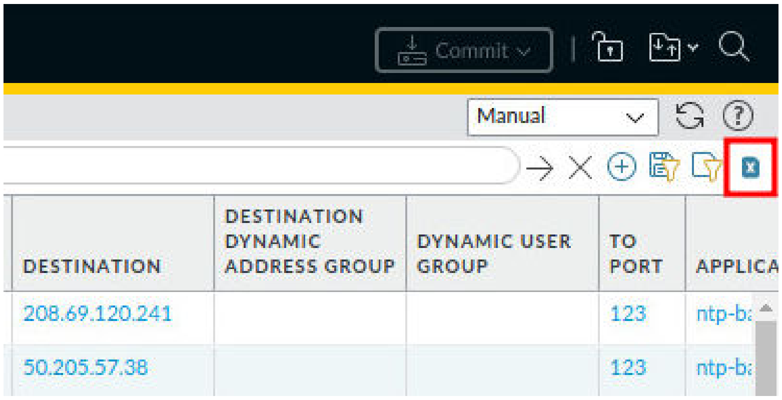


5. Navigate to **Monitor > Logs > Traffic**.



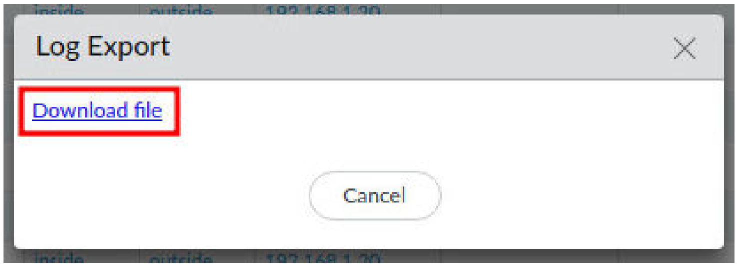
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOUR DYN ADDI
	09/25 18:27:26	end	inside	outside	192.168.1.20		
	09/25 18:27:23	end	inside	outside	192.168.1.20		
	09/25 18:27:21	end	inside	outside	192.168.1.20		

6. Click the **spreadsheet** icon to export the Firewall's traffic log as a *csv file*.

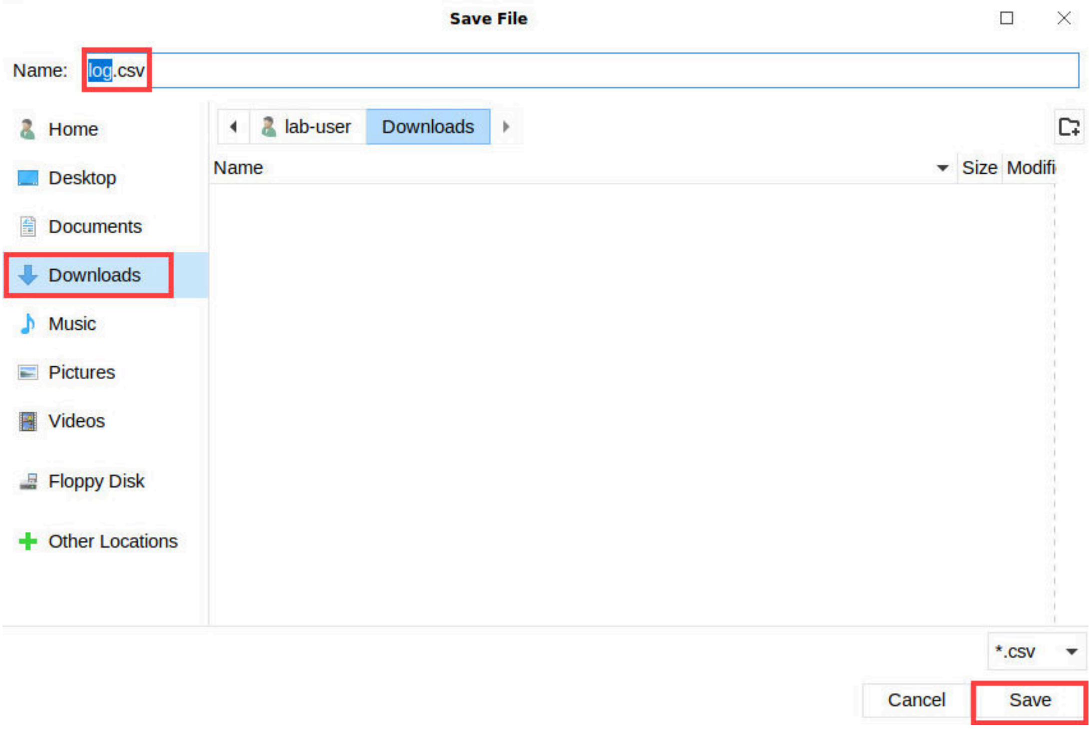


DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICA
208.69.120.241			123	ntp-b:
50.205.57.38			123	ntp-b:

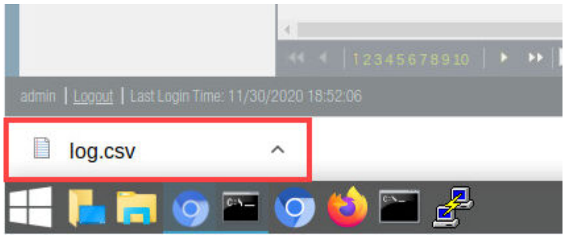
7. In the *Log Export* window, click **Download file**.



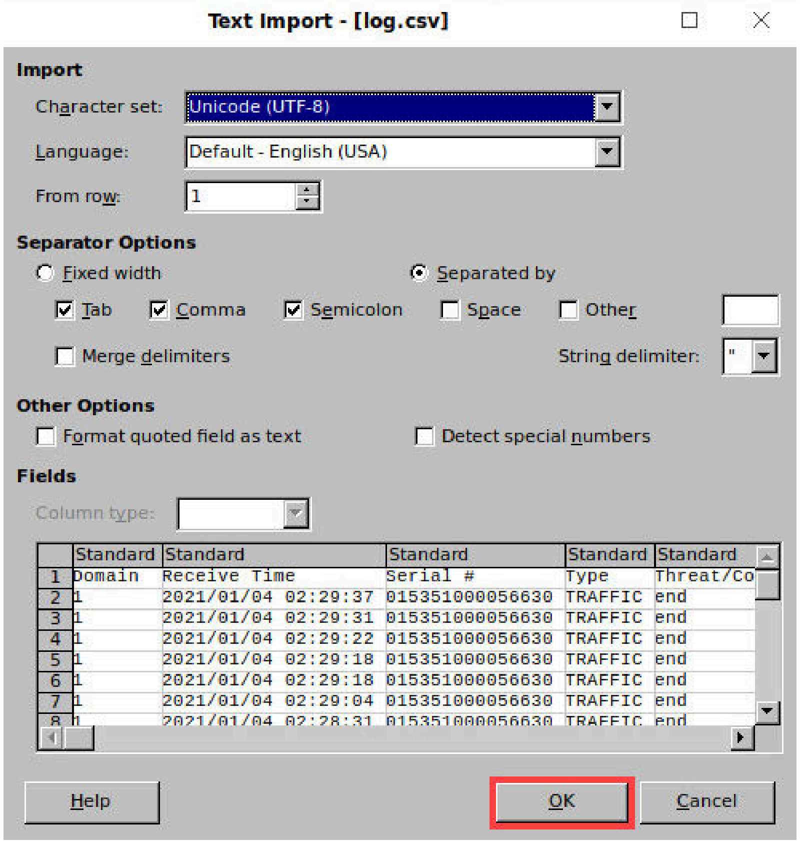
8. In the *Save File* window, verify that the name **log.csv** is showing, select **Downloads** and click **Save**.



9. From the client, click the **log.csv** file that you downloaded in *steps* **5** and **6**.



10. In the *Text Import – [log.csv]* window, click **OK**.



Text Import - [log.csv]

Import

Character set: Unicode (UTF-8)

Language: Default - English (USA)

From row: 1

Separator Options

○ Fixed width ● Separated by

☑ Tab ☑ Comma ☑ Semicolon □ Space □ Other

□ Merge delimiters String delimiter: "

Other Options

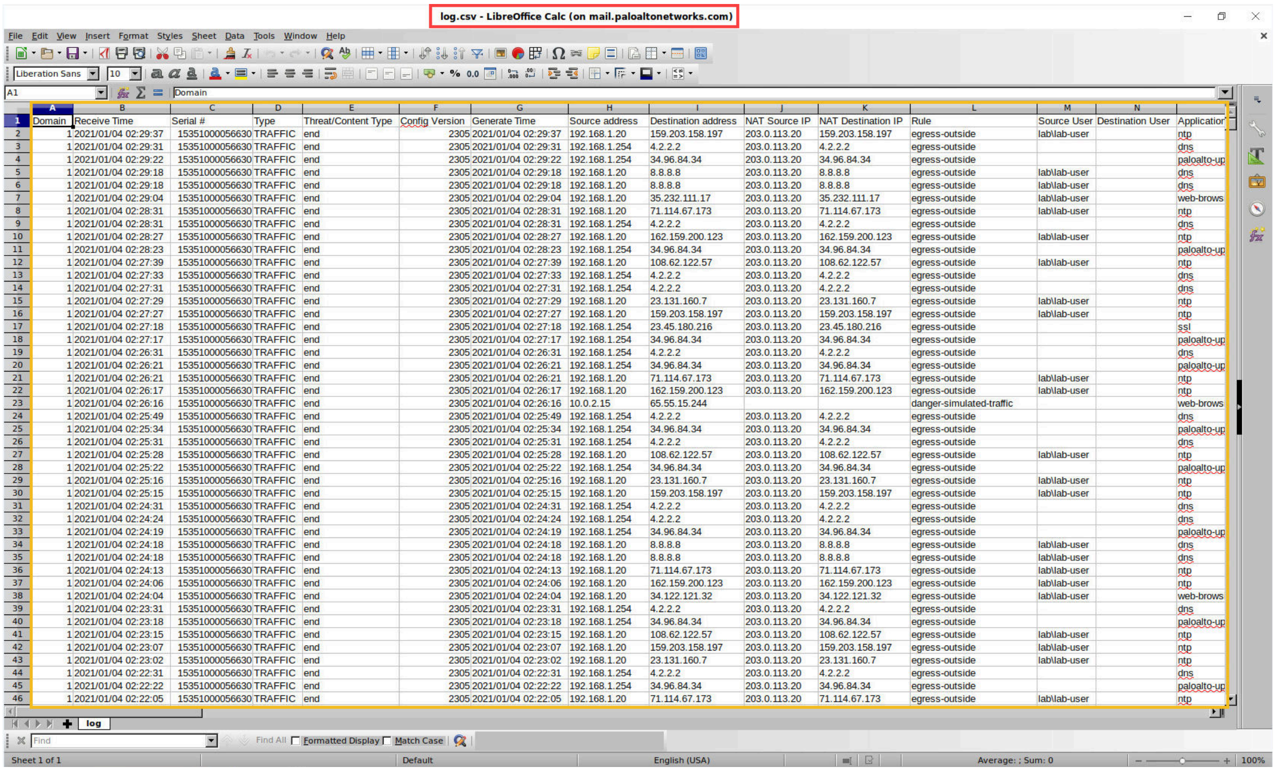
□ Format quoted field as text □ Detect special numbers

Fields

Column type:

	Standard	Standard	Standard	Standard	Standard
1	Domain	Receive Time	Serial #	Type	Threat/Co
2	1	2021/01/04 02:29:37	015351000056630	TRAFFIC	end
3	1	2021/01/04 02:29:31	015351000056630	TRAFFIC	end
4	1	2021/01/04 02:29:22	015351000056630	TRAFFIC	end
5	1	2021/01/04 02:29:18	015351000056630	TRAFFIC	end
6	1	2021/01/04 02:29:18	015351000056630	TRAFFIC	end
7	1	2021/01/04 02:29:04	015351000056630	TRAFFIC	end
8	1	2021/01/04 02:28:31	015351000056630	TRAFFIC	end

11. Observe the Firewall's logged traffic using LibreOffice.



log.csv - LibreOffice Calc (on mail.paloaltonetworks.com)

File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10
A1

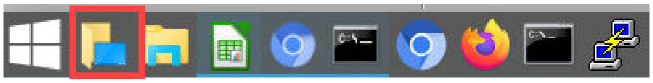
Domain

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	Domain	Receive Time	Serial #	Type	Threat/Content Type	Config Version	Generate Time	Source address	Destination address	NAT Source IP	NAT Destination IP	Rule	Source User	Destination User	Applicatio
2	1	2021/01/04 02:29:37	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:37	192.168.1.20	159.203.158.197	203.0.113.20	159.203.158.197	egress-outside	lab\lab-user		ntp
3	1	2021/01/04 02:29:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
4	1	2021/01/04 02:29:22	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:22	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
5	1	2021/01/04 02:29:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:18	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside	lab\lab-user		dns
6	1	2021/01/04 02:29:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:18	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside	lab\lab-user		dns
7	1	2021/01/04 02:29:04	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:04	192.168.1.20	35.232.111.17	203.0.113.20	35.232.111.17	egress-outside	lab\lab-user		web-brows
8	1	2021/01/04 02:28:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:31	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab\lab-user		ntp
9	1	2021/01/04 02:28:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
10	1	2021/01/04 02:28:27	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:27	192.168.1.20	162.159.200.123	203.0.113.20	162.159.200.123	egress-outside	lab\lab-user		ntp
11	1	2021/01/04 02:28:23	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:23	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
12	1	2021/01/04 02:27:39	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:39	192.168.1.20	108.62.122.57	203.0.113.20	108.62.122.57	egress-outside	lab\lab-user		ntp
13	1	2021/01/04 02:27:33	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:33	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
14	1	2021/01/04 02:27:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
15	1	2021/01/04 02:27:29	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:29	192.168.1.20	23.131.160.7	203.0.113.20	23.131.160.7	egress-outside	lab\lab-user		ntp
16	1	2021/01/04 02:27:27	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:27	192.168.1.20	159.203.158.197	203.0.113.20	159.203.158.197	egress-outside	lab\lab-user		ntp
17	1	2021/01/04 02:27:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:18	192.168.1.254	23.45.180.216	203.0.113.20	23.45.180.216	egress-outside			ssl
18	1	2021/01/04 02:27:17	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:17	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
19	1	2021/01/04 02:26:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
20	1	2021/01/04 02:26:21	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:21	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
21	1	2021/01/04 02:26:21	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:21	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab\lab-user		ntp
22	1	2021/01/04 02:26:17	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:17	192.168.1.20	162.159.200.123	203.0.113.20	162.159.200.123	egress-outside	lab\lab-user		ntp
23	1	2021/01/04 02:26:16	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:16	10.0.2.15	65.55.15.244			danger-simulated-traffic			web-brows
24	1	2021/01/04 02:25:49	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:49	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
25	1	2021/01/04 02:25:34	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:34	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
26	1	2021/01/04 02:25:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
27	1	2021/01/04 02:25:28	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:28	192.168.1.20	108.62.122.57	203.0.113.20	108.62.122.57	egress-outside	lab\lab-user		ntp
28	1	2021/01/04 02:25:22	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:22	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
29	1	2021/01/04 02:25:16	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:16	192.168.1.20	23.131.160.7	203.0.113.20	23.131.160.7	egress-outside	lab\lab-user		ntp
30	1	2021/01/04 02:25:15	15351000056630	TRAFFIC	end	2305	2021/01/04 02:25:15	192.168.1.20	159.203.158.197	203.0.113.20	159.203.158.197	egress-outside	lab\lab-user		ntp
31	1	2021/01/04 02:24:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
32	1	2021/01/04 02:24:24	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:24	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
33	1	2021/01/04 02:24:19	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:19	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
34	1	2021/01/04 02:24:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:18	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside	lab\lab-user		dns
35	1	2021/01/04 02:24:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:18	192.168.1.20	8.8.8.8	203.0.113.20	8.8.8.8	egress-outside	lab\lab-user		dns
36	1	2021/01/04 02:24:13	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:13	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab\lab-user		ntp
37	1	2021/01/04 02:24:06	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:06	192.168.1.20	162.159.200.123	203.0.113.20	162.159.200.123	egress-outside	lab\lab-user		ntp
38	1	2021/01/04 02:24:04	15351000056630	TRAFFIC	end	2305	2021/01/04 02:24:04	192.168.1.20	34.122.121.32	203.0.113.20	34.122.121.32	egress-outside	lab\lab-user		web-brows
39	1	2021/01/04 02:23:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:23:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
40	1	2021/01/04 02:23:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:23:18	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
41	1	2021/01/04 02:23:15	15351000056630	TRAFFIC	end	2305	2021/01/04 02:23:15	192.168.1.20	108.62.122.57	203.0.113.20	108.62.122.57	egress-outside	lab\lab-user		ntp
42	1	2021/01/04 02:23:07	15351000056630	TRAFFIC	end	2305	2021/01/04 02:23:07	192.168.1.20	159.203.158.197	203.0.113.20	159.203.158.197	egress-outside	lab\lab-user		ntp
43	1	2021/01/04 02:23:02	15351000056630	TRAFFIC	end	2305	2021/01/04 02:23:02	192.168.1.20	23.131.160.7	203.0.113.20	23.131.160.7	egress-outside	lab\lab-user		ntp
44	1	2021/01/04 02:22:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:22:31	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside			dns
45	1	2021/01/04 02:22:22	15351000056630	TRAFFIC	end	2305	2021/01/04 02:22:22	192.168.1.254	34.96.84.34	203.0.113.20	34.96.84.34	egress-outside			paloalto-up
46	1	2021/01/04 02:22:05	15351000056630	TRAFFIC	end	2305	2021/01/04 02:22:05	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab\lab-user		ntp

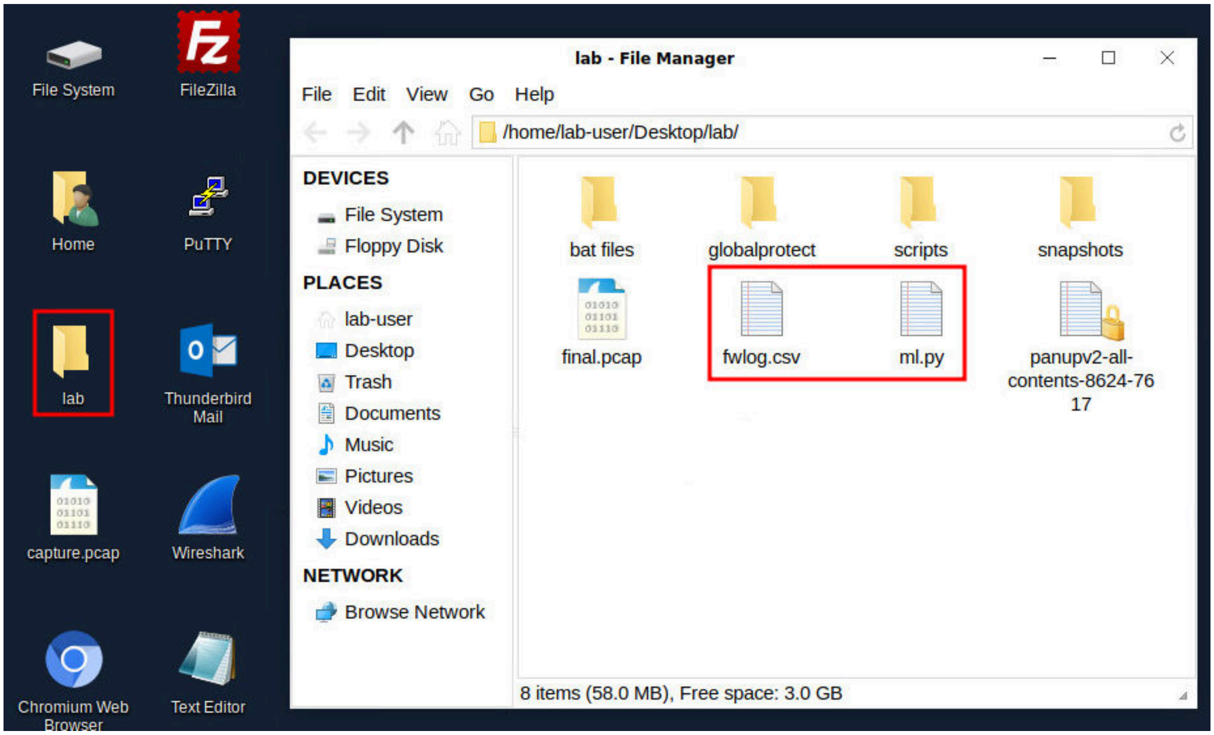
Please Note

If you were using Cortex XSOAR in your organization's Security Operations Center, traffic data from 100s of firewall appliances, network appliances and endpoints would be forwarded to the Cortex Data Lake. The Cortex Data Lake would then analyze this vast quantity of data and use machine learning (ML) to detect anomalies indicating incidents of compromise.

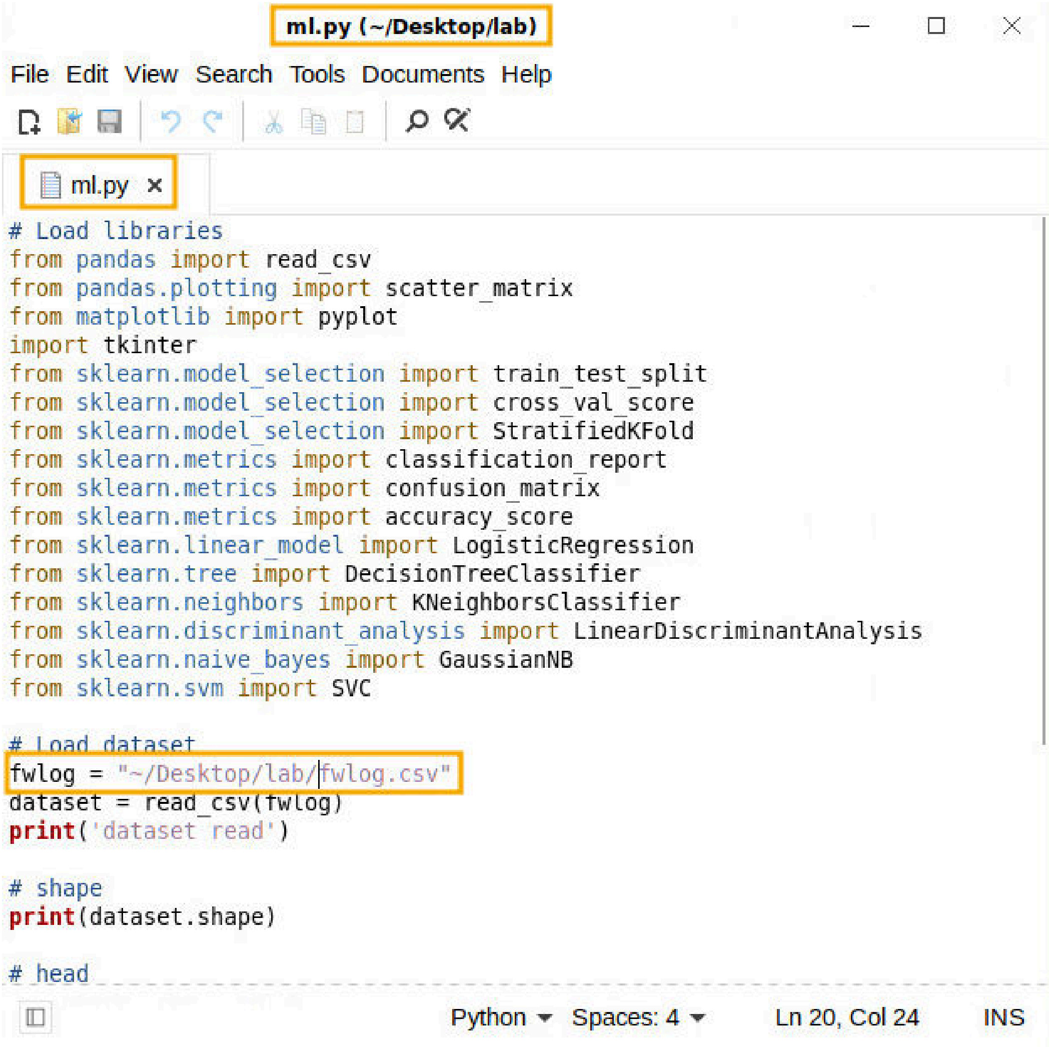
12. On the lower-left of the client desktop, click the **Minimize all open windows and show the desktop** icon.



13. Double-click the **lab** folder. In the *lab – File Manager* window, there is a Python program named **ml.py** that will use the python script module to analyze the data in the **fwlog.csv** file. The **fwlog.csv** file is a modified version of the **log.csv** file you downloaded from the Palo Alto Networks Firewall. The **fwlog.csv** file contains only **5** column fields from the **log.csv** file.



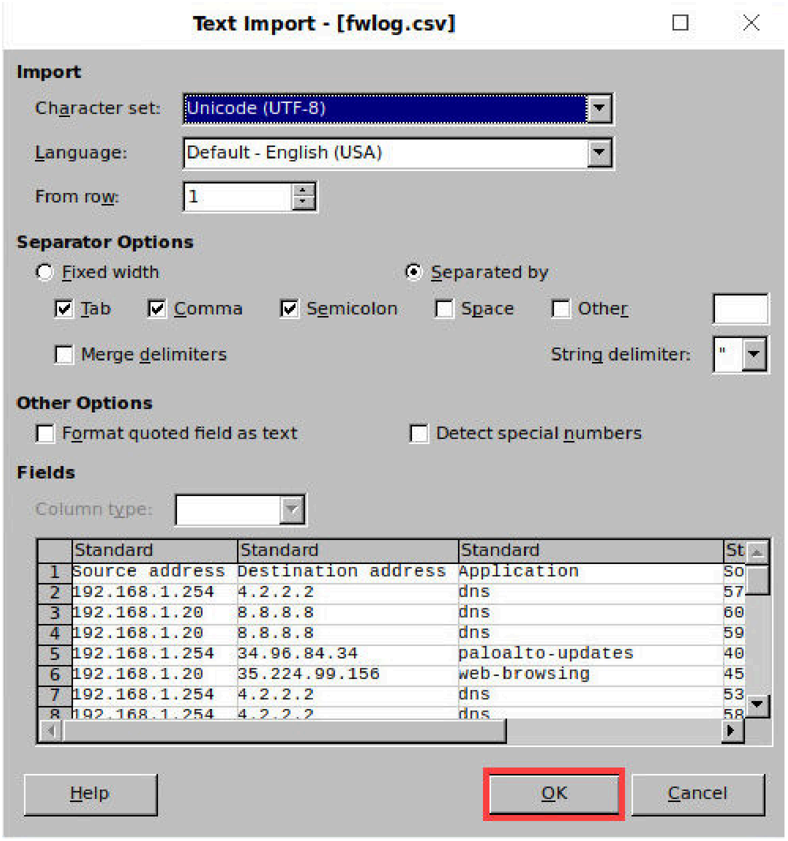
14. Double-click the **ml.py** file and explore the contents. Notice the **fwlog.csv** file that will be analyzed from the **ml.py** script.


ml.py (~/Desktop/lab)
File Edit View Search Tools Documents Help
ml.py ×
Python Spaces: 4 Ln 20, Col 24 INS

```
# Load libraries
from pandas import read_csv
from pandas.plotting import scatter_matrix
from matplotlib import pyplot
import tkinter
from sklearn.model_selection import train_test_split
from sklearn.model_selection import cross_val_score
from sklearn.model_selection import StratifiedKFold
from sklearn.metrics import classification_report
from sklearn.metrics import confusion_matrix
from sklearn.metrics import accuracy_score
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.neighbors import KNeighborsClassifier
from sklearn.discriminant_analysis import LinearDiscriminantAnalysis
from sklearn.naive_bayes import GaussianNB
from sklearn.svm import SVC

# Load dataset
fwlog = "~/Desktop/lab/fwlog.csv"
dataset = read_csv(fwlog)
print('dataset read')

# shape
print(dataset.shape)

# head
```

15. Close the **ml.py** file by clicking on the **X** icon.

16. Double click the **fwlog.csv** file. When the *Text Import –[fwlog.csv]* window appears, click **OK**.



Text Import - [fwlog.csv]

Import

Character set: Unicode (UTF-8)

Language: Default - English (USA)

From row: 1

Separator Options

○ Fixed width ● Separated by

☑ Tab ☑ Comma ☑ Semicolon ☐ Space ☐ Other

☐ Merge delimiters String delimiter: "

Other Options

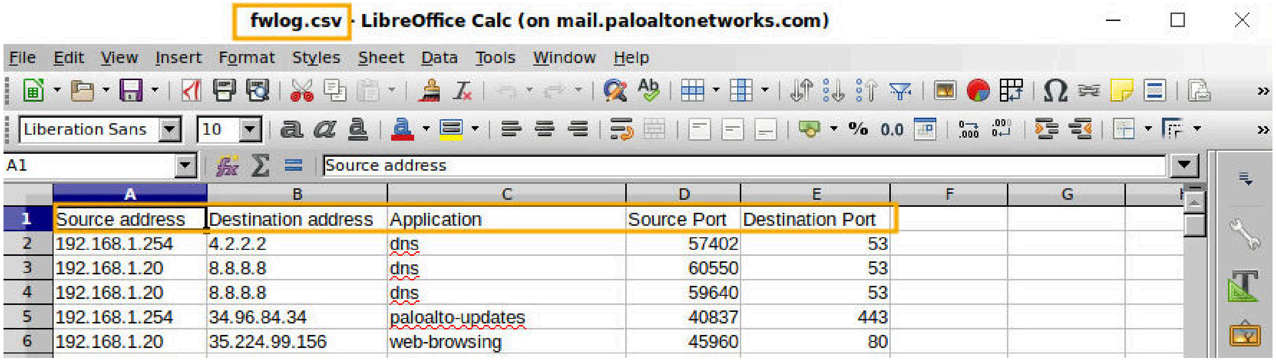
☐ Format quoted field as text ☐ Detect special numbers

Fields

Column type:

```
   Standard       Standard             Standard          St
1  Source address Destination address  Application       So
2  192.168.1.254  4.2.2.2              dns               57
3  192.168.1.20   8.8.8.8              dns               60
4  192.168.1.20   8.8.8.8              dns               59
5  192.168.1.254  34.96.84.34          paloalto-updates  40
6  192.168.1.20   35.224.99.156        web-browsing      45
7  192.168.1.254  4.2.2.2              dns               53
8  192.168.1.254  4.2.2.2              dns               58
```

17. Explore the contents of the **fwlog.csv** file. Notice the 5 columns of **Source address**, **Destination address**, **Application**, **Source Port** and **Destination Port**.



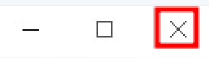
fwlog.csv - LibreOffice Calc (on mail.paloaltonetworks.com)

File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10
A1

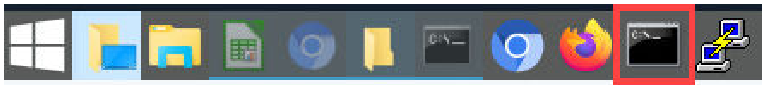
Source address

	A	B	C	D	E	F	G
1	Source address	Destination address	Application	Source Port	Destination Port		
2	192.168.1.254	4.2.2.2	dns	57402	53		
3	192.168.1.20	8.8.8.8	dns	60550	53		
4	192.168.1.20	8.8.8.8	dns	59640	53		
5	192.168.1.254	34.96.84.34	paloalto-updates	40837	443		
6	192.168.1.20	35.224.99.156	web-browsing	45960	80		

18. Close the **fwlog.csv** file by clicking on the **X** icon.

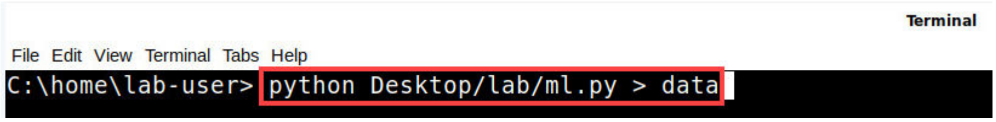


19. On the client desktop, open a *terminal* window by clicking on the **Xfce Terminal** icon.



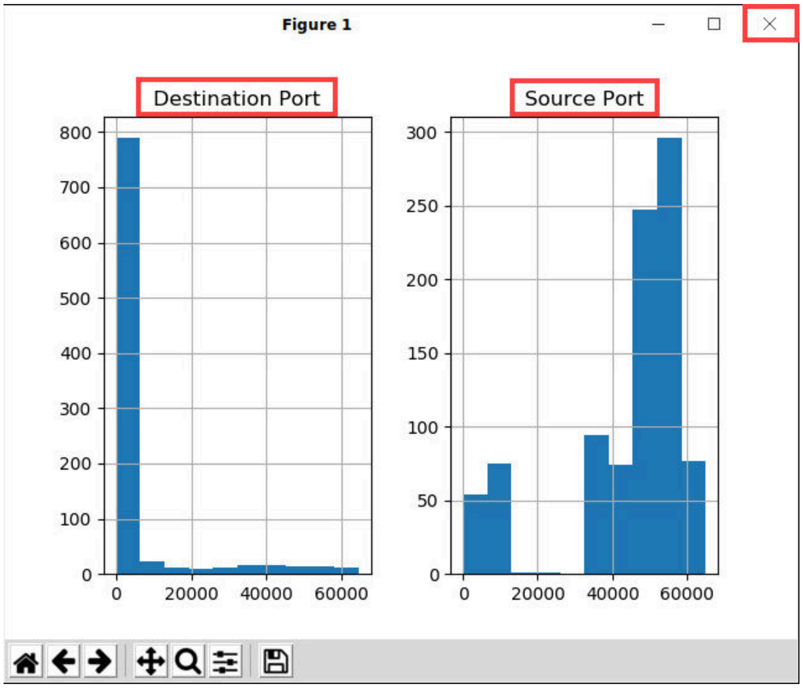
20. Execute the **ml.py** python file by typing the command below.

```
C:\home\lab-user> python Desktop/lab/ml.py > data
```



```
C:\home\lab-user> python Desktop/lab/ml.py > data
```

21. View the data from the histogram in the *Figure 1* window. This will display a *histogram* that will show information about the **Source** and **Destination** ports, and other information about the log entries in a file named **data**. After viewing the information from the histogram, close it by clicking on the **X** icon to complete the command execution.

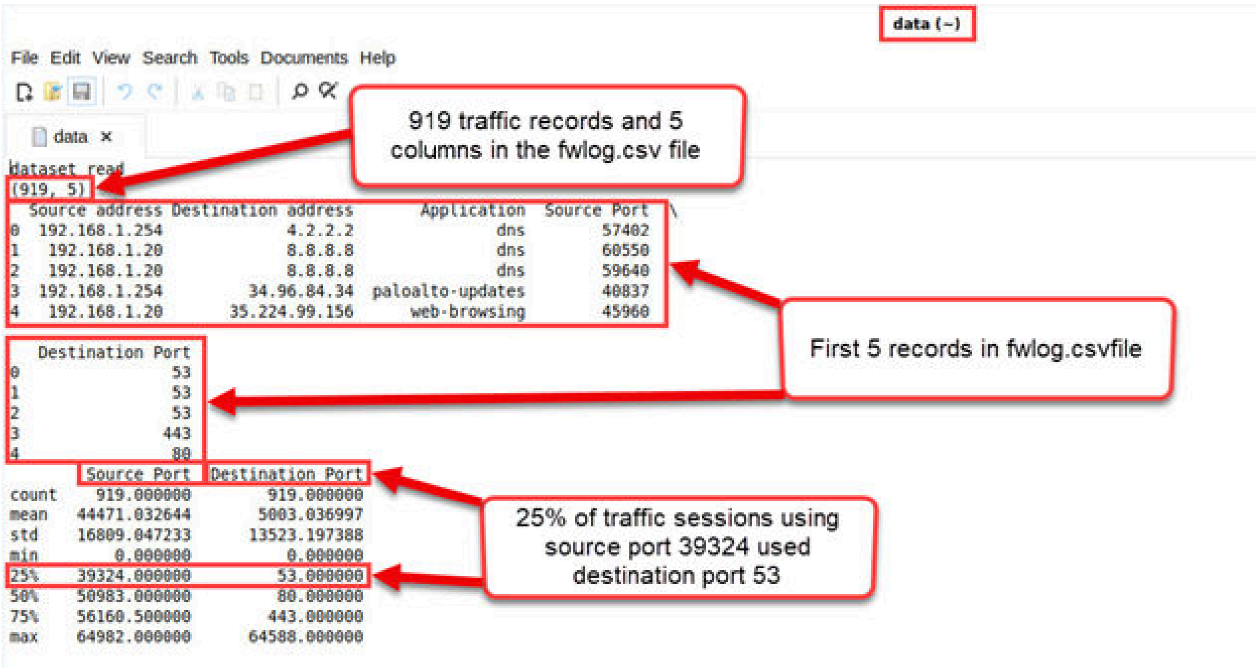


22. In the *terminal* window, open the **data** file created by typing the command below.

```
C:\home\lab-user> xed data
```

```
C:\home\lab-user> xed data
```

23. Explore the information in the **data** file about the *Palo Alto Networks Firewall* traffic.



```
Dataset read
(919, 5)
  Source address Destination address        Application  Source Port  \
0  192.168.1.254             4.2.2.2                dns        57402
1   192.168.1.20             8.8.8.8                dns        60550
2   192.168.1.20             8.8.8.8                dns        59640
3  192.168.1.254         34.96.84.34   paloalto-updates        40837
4   192.168.1.20       35.224.99.156       web-browsing        45960

   Destination Port
0                53
1                53
2                53
3               443
4                80
        Source Port  Destination Port
count    919.000000        919.000000
mean   44471.032644       5003.036997
std    16809.047233      13523.197388
min        0.000000          0.000000
25%    39324.000000         53.000000
50%    50983.000000         80.000000
75%    56160.500000        443.000000
max    64982.000000      64588.000000
```

919 traffic records and 5 columns in the fwlog.csv file

First 5 records in fwlog.csvfile

25% of traffic sessions using source port 39324 used destination port 53

24. The lab is now complete; you may end your reservation.