



# SECURITY OPERATIONS FUNDAMENTALS

## Lab 1: Network Traffic Analysis

Document Version: **2021-01-29**

Copyright © 2021 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB+ is a registered trademark of Network Development Group, Inc.

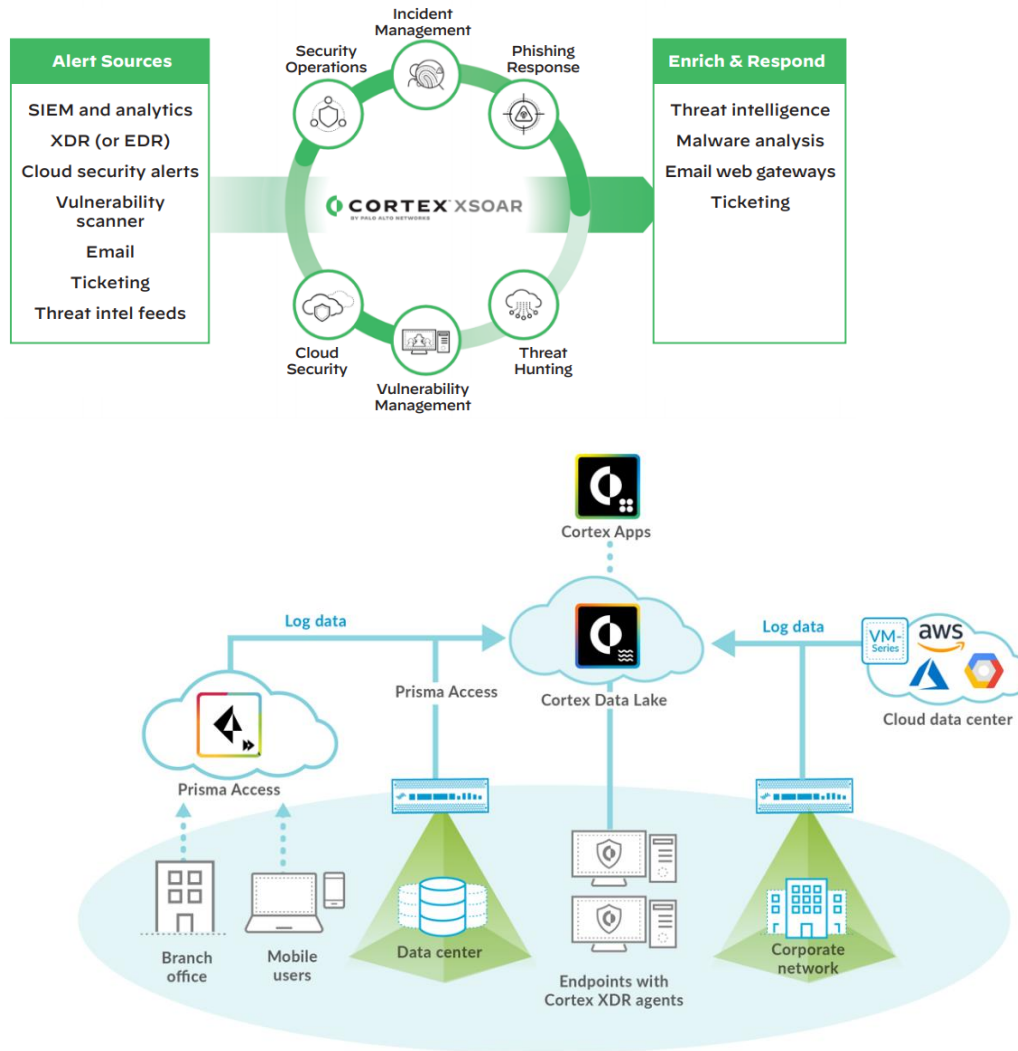
Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Introduction .....	3
Objective .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Network Traffic Analysis .....	6
1.0 Load Lab Configuration .....	6
1.1 Export Firewall Log Data for Analysis .....	11
1.2 Generate Traffic for Firewall Analysis .....	17
1.3 Log Analysis .....	19

## 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.

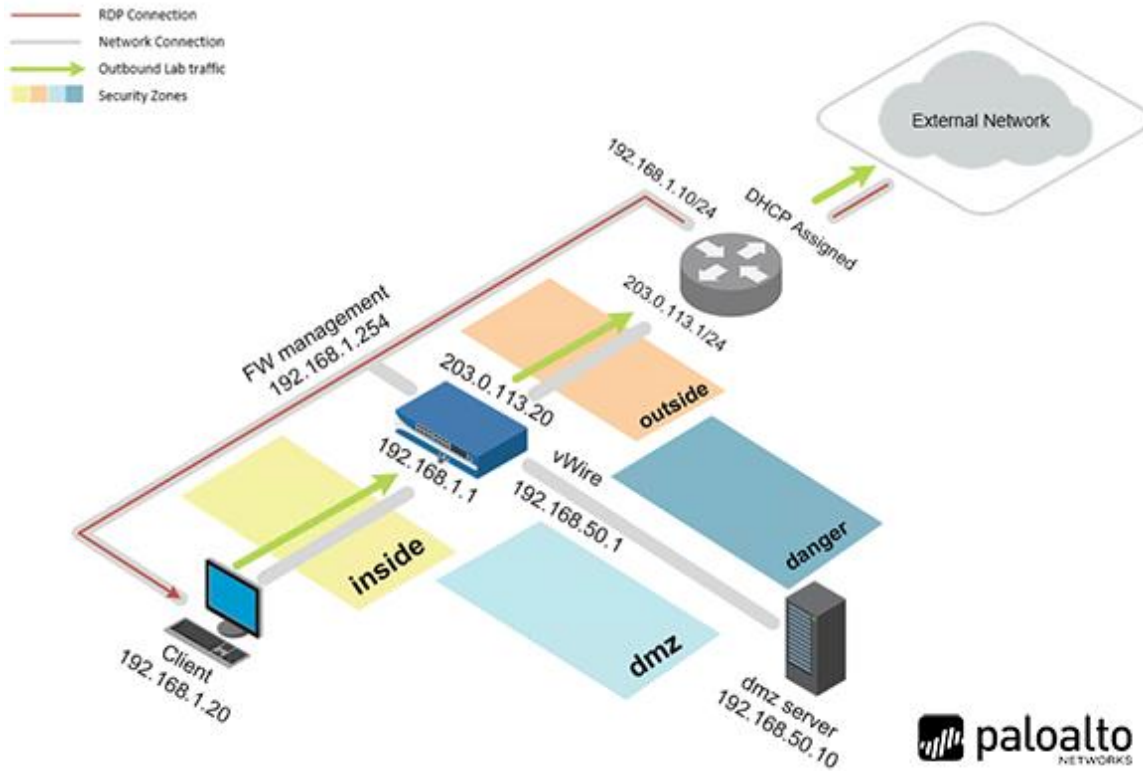


## Objective

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.

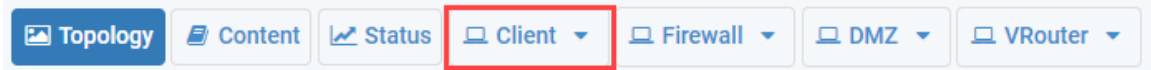
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

## 1 Network Traffic Analysis

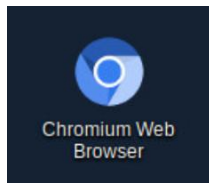
### 1.0 Load Lab Configuration

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

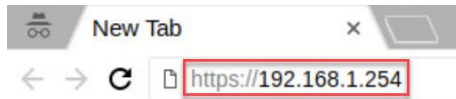
1. Click on the **Client** tab to access the client PC.



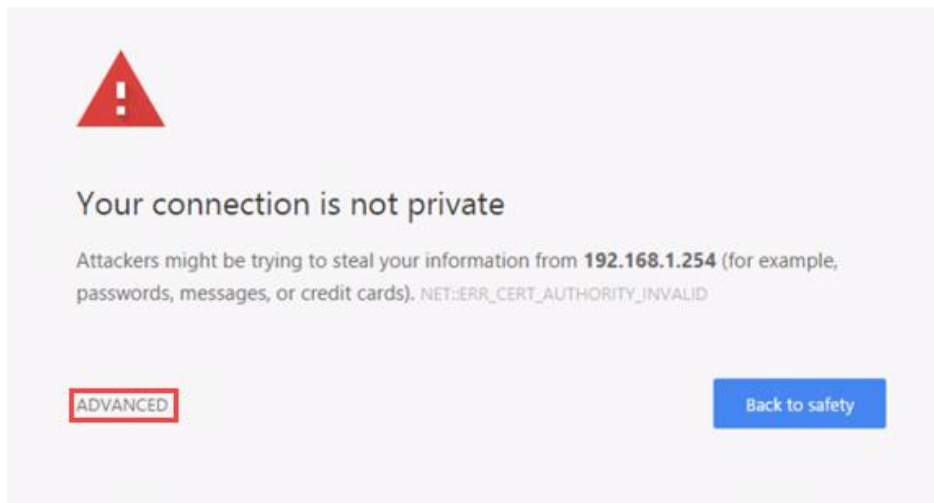
2. Log in to the client PC with the username **lab-user** and password **Train1ng\$**.
3. Double-click the **Chromium** icon located on the desktop.



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

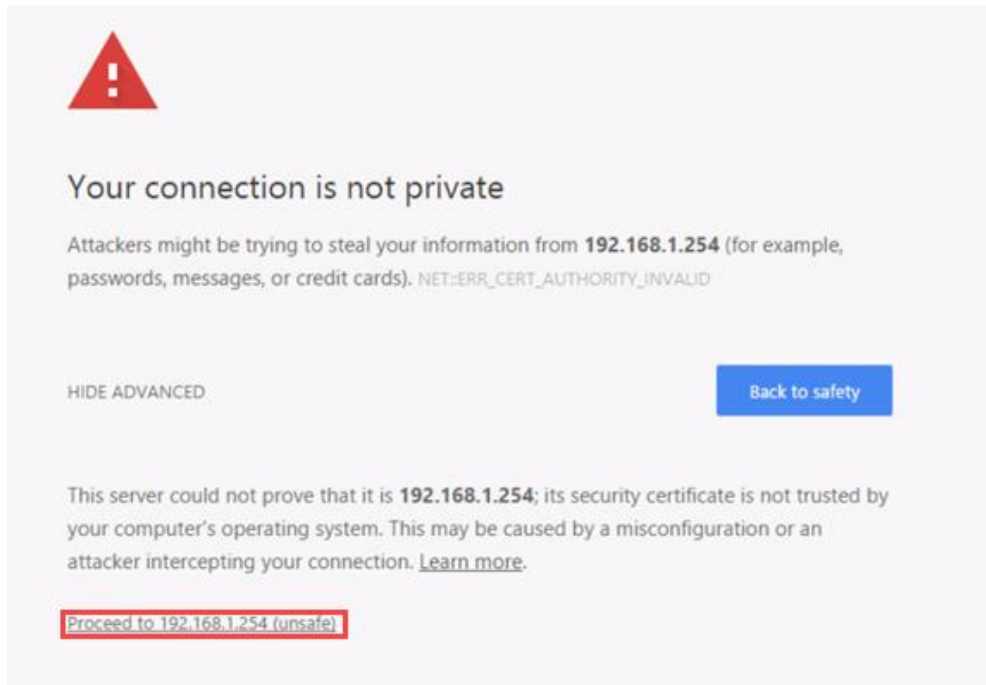


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

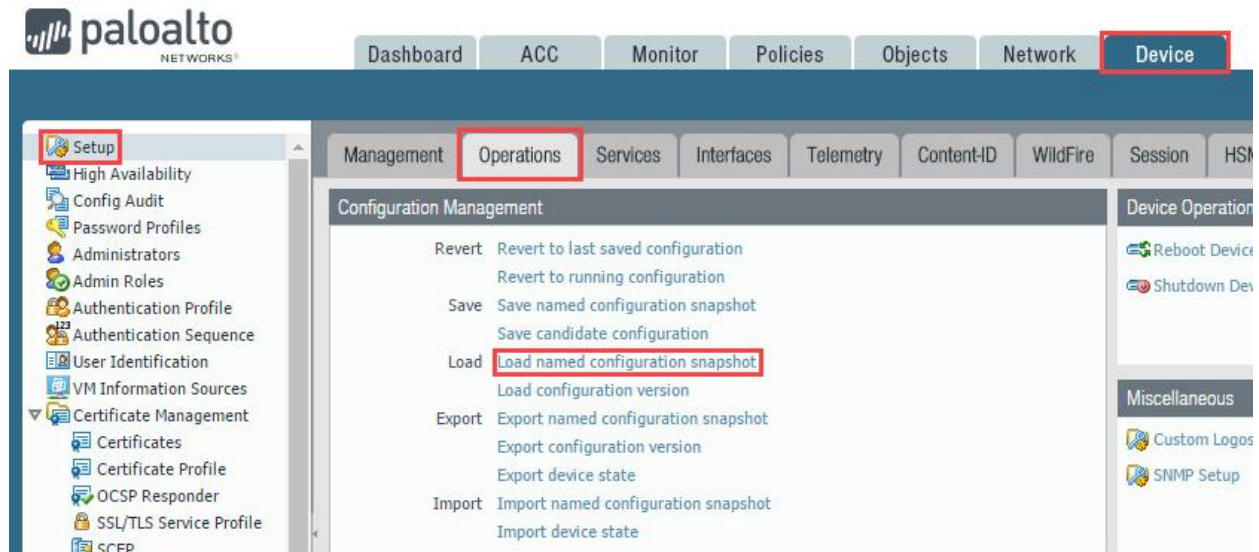
- Click on **Proceed to 192.168.1.254 (unsafe)**.



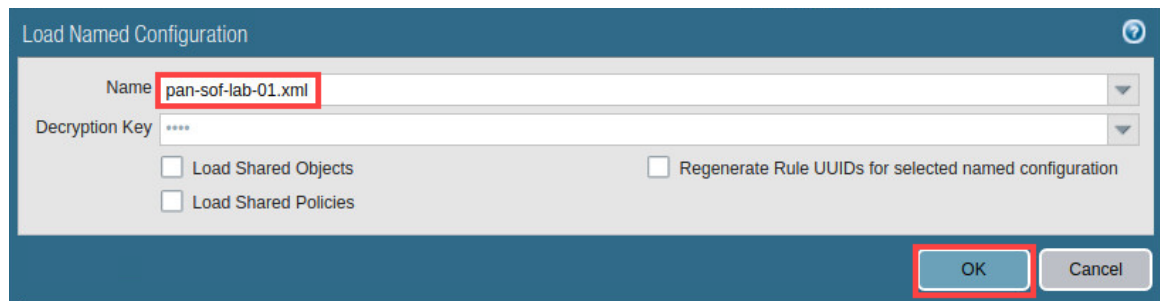
- Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



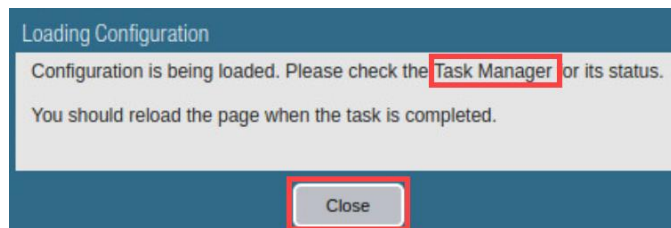
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



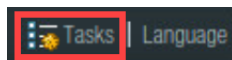
- In the *Load Named Configuration* window, select **pan-sof-lab-01.xml** from the *Name* dropdown box and click **OK**.



- 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.

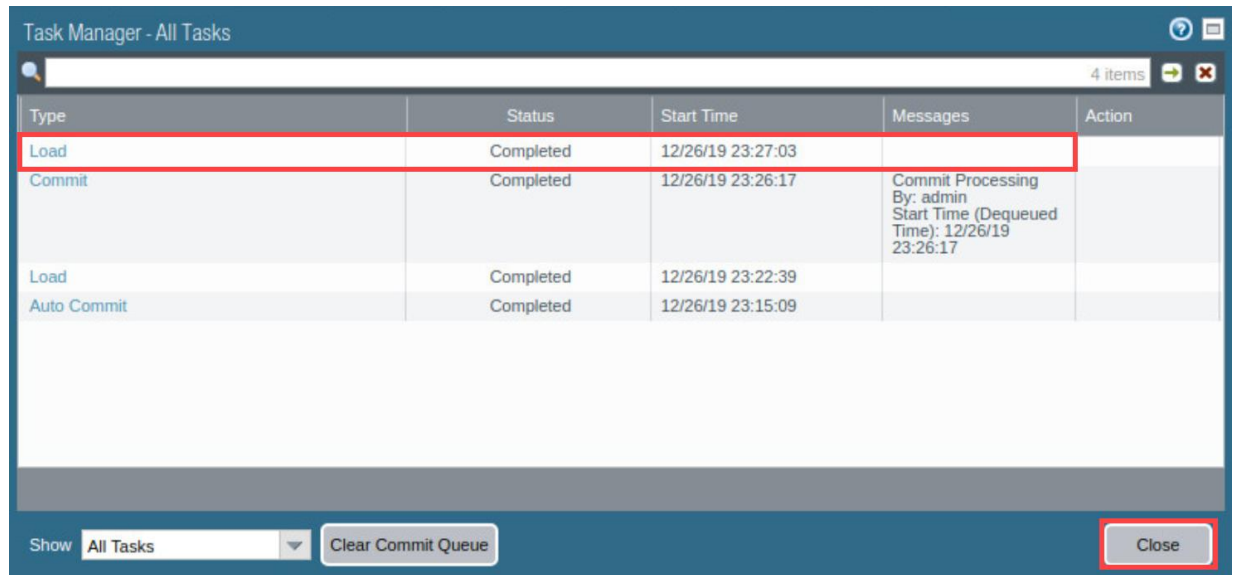


- Click the **Tasks** icon located at the bottom-right of the web interface.





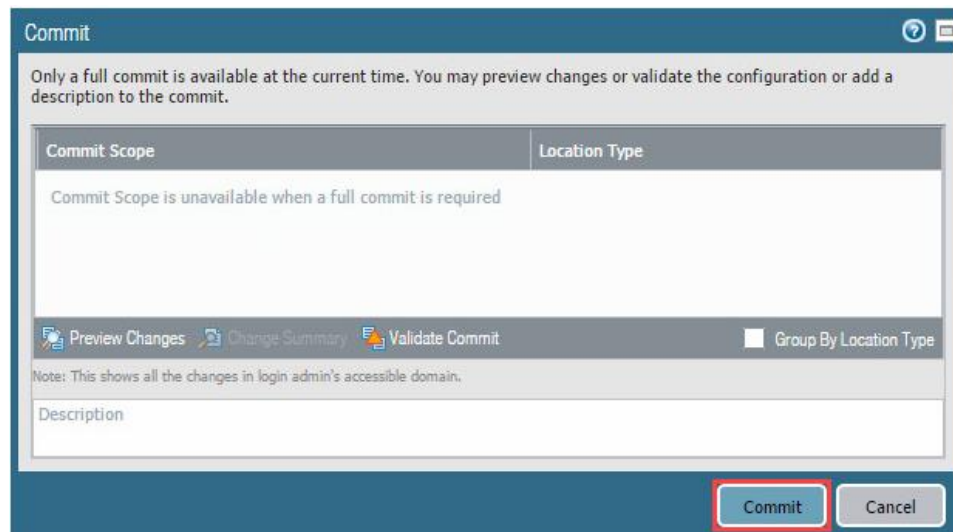
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



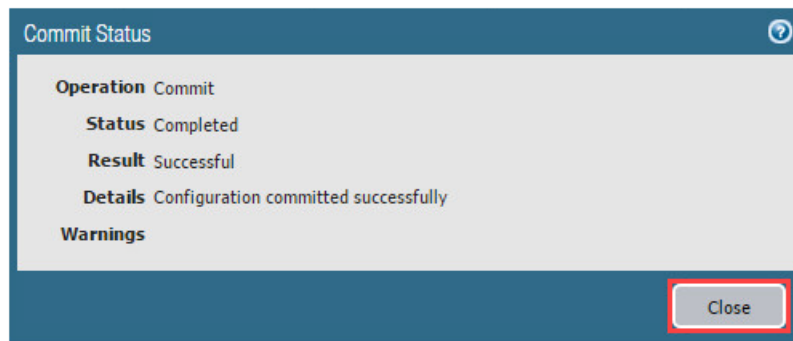
13. Click the **Commit** link located at the top-right of the web interface.



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



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

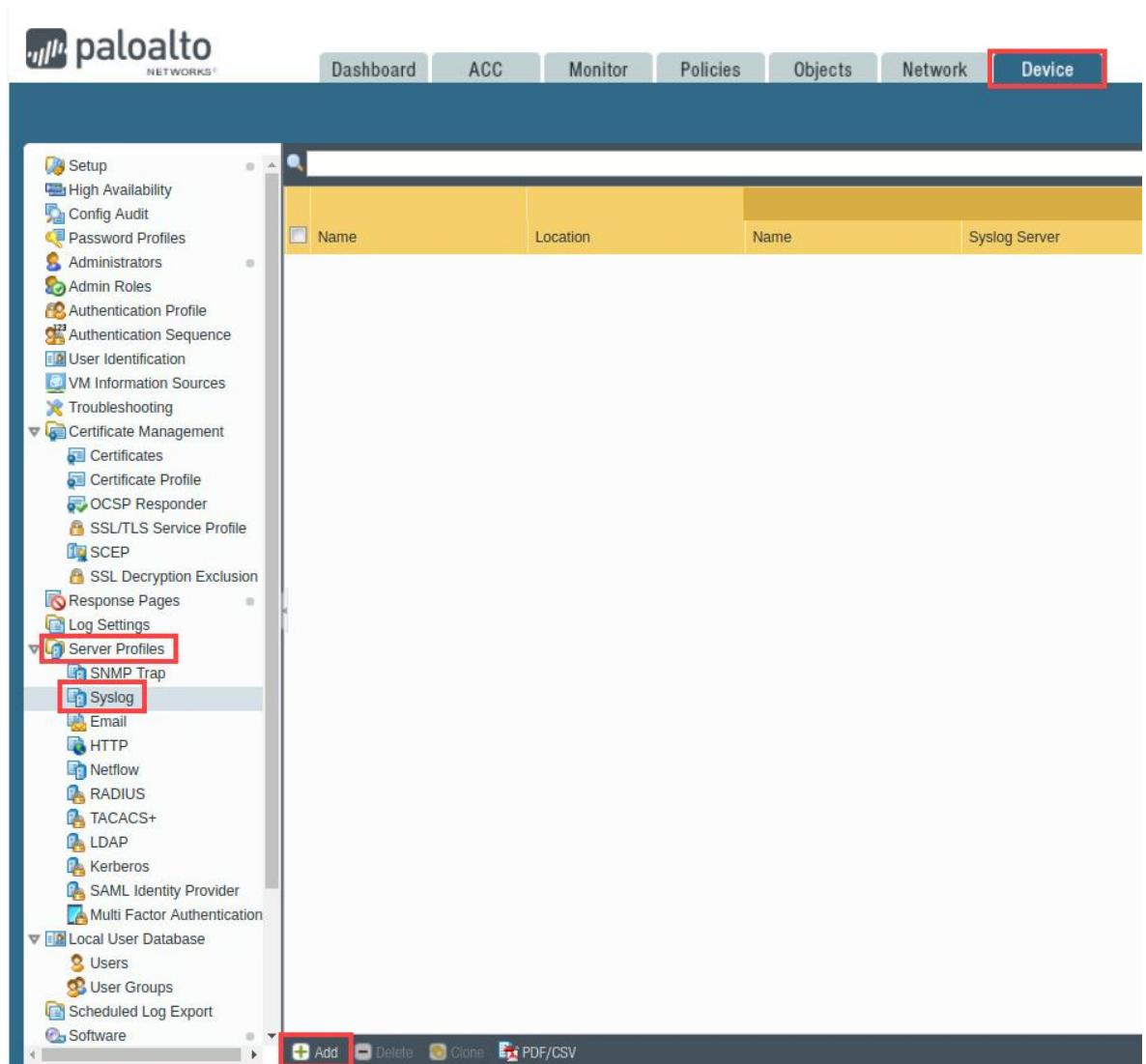


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

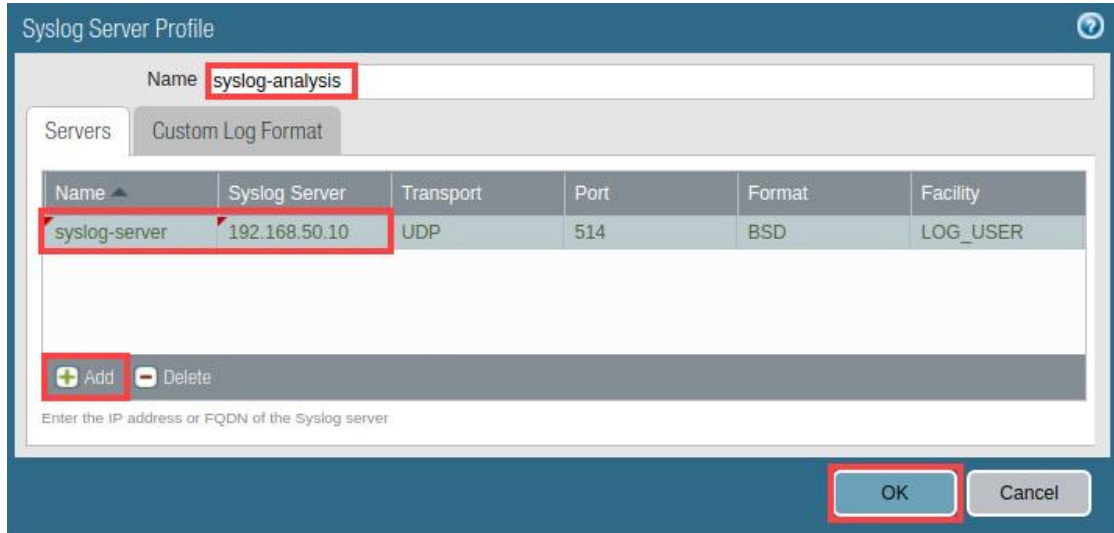
## 1.1 Export Firewall Log Data for Analysis

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**.

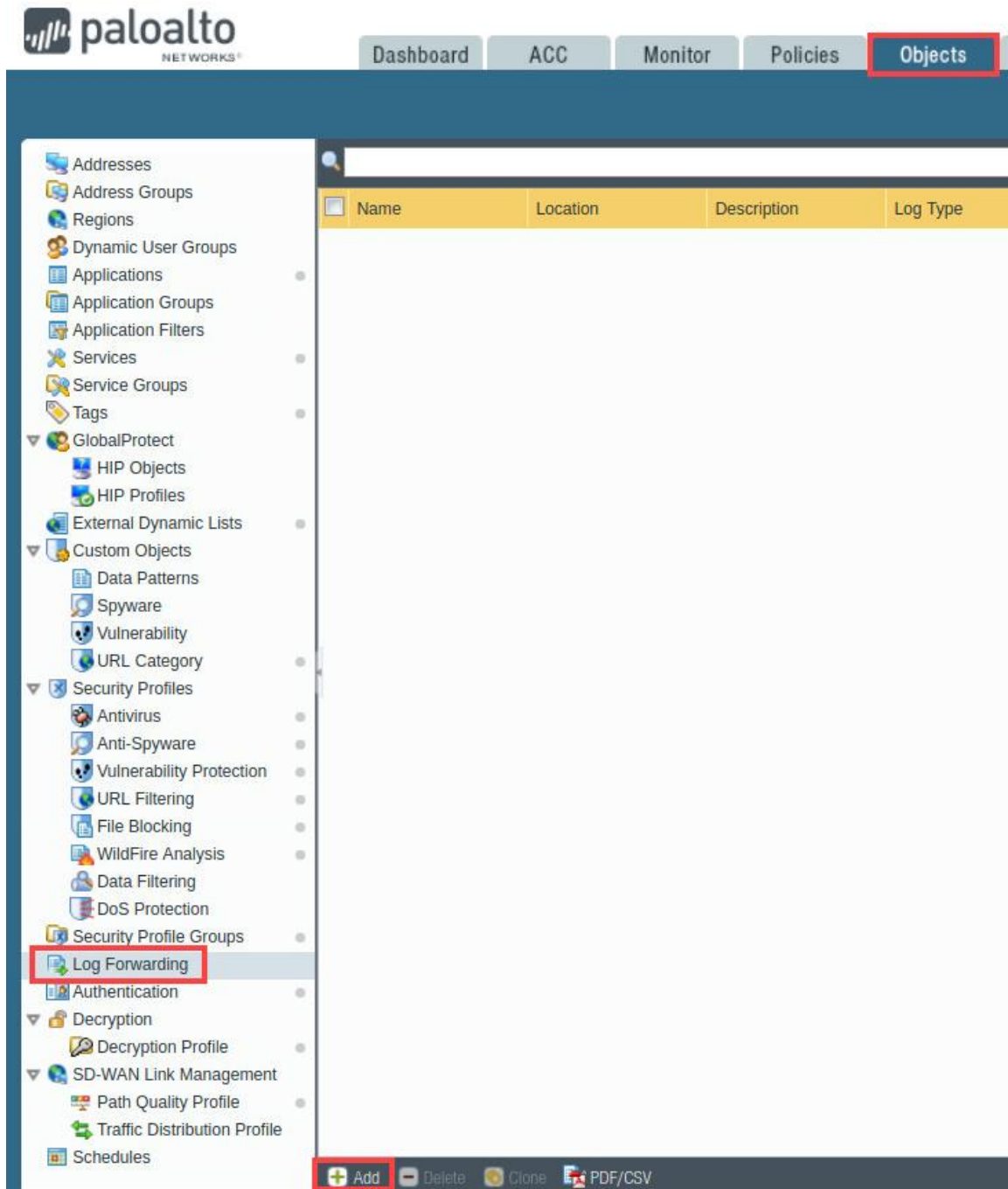


The image shows the 'Syslog Server Profile' configuration window. The 'Name' field at the top is set to 'syslog-analysis'. Below this, there are two tabs: 'Servers' and 'Custom Log Format'. The 'Servers' tab is active, displaying a table with the following data:

Name	Syslog Server	Transport	Port	Format	Facility
syslog-server	192.168.50.10	UDP	514	BSD	LOG_USER

Below the table, there is an 'Add' button (with a plus icon) and a 'Delete' button (with a minus icon). The 'Add' button is highlighted with a red box. Below these buttons, there is a text input field with the placeholder text 'Enter the IP address or FQDN of the Syslog server'. At the bottom right of the window, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red box.

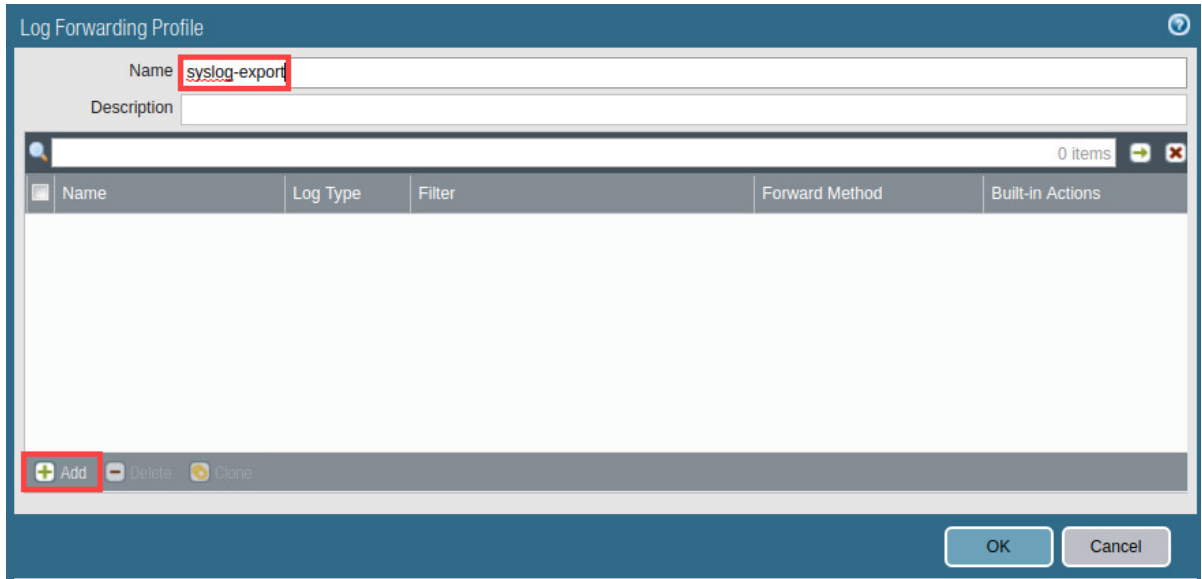
3. Navigate to **Objects > Log Forwarding > Add**.



The screenshot shows the Palo Alto Networks GUI. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, and Objects. The Objects tab is selected. On the left sidebar, the Log Forwarding option is highlighted. The main content area displays a table with columns: Name, Location, Description, and Log Type. At the bottom of the screen, there is a toolbar with buttons for Add, Delete, Clone, and PDF/CSV. The Add button is highlighted with a red box.

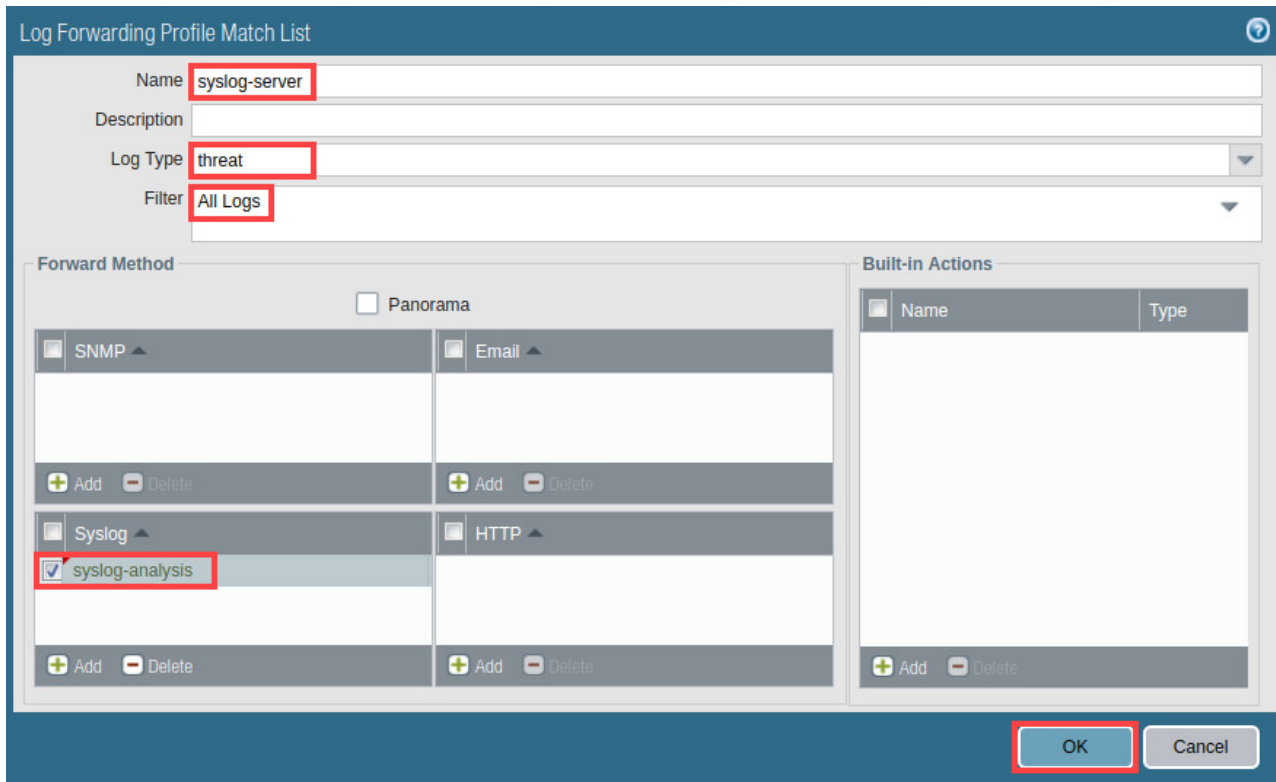
Name	Location	Description	Log Type
------	----------	-------------	----------

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



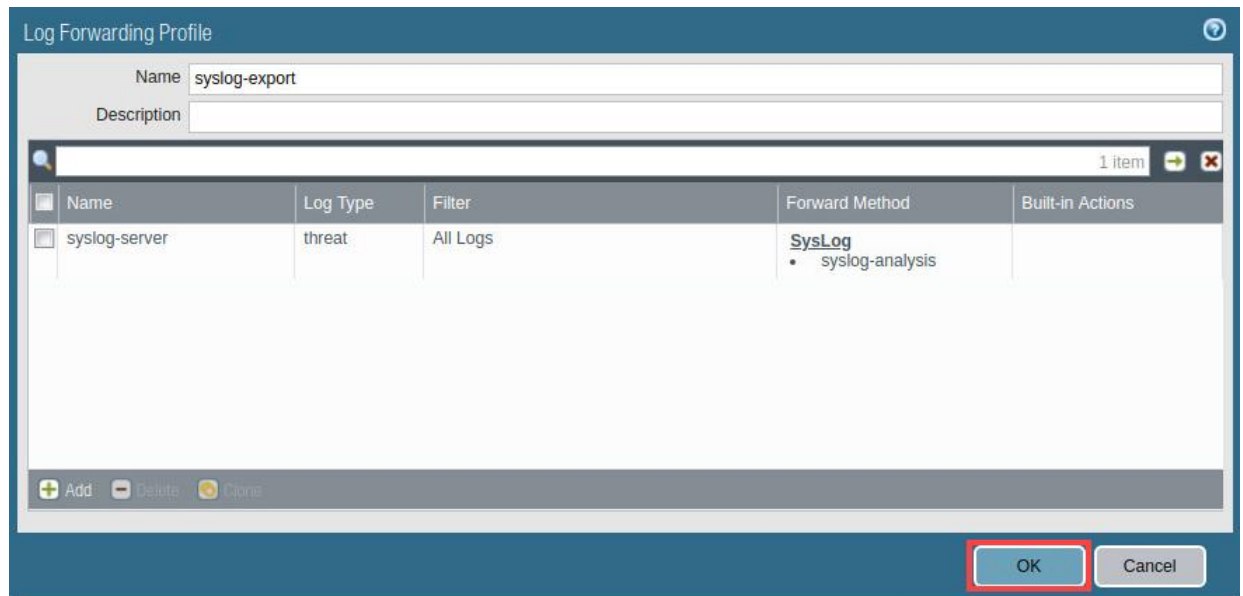
The screenshot shows the 'Log Forwarding Profile' window. The 'Name' field is populated with 'syslog-export' and is highlighted with a red box. Below the 'Name' field is an empty 'Description' field. A table with columns 'Name', 'Log Type', 'Filter', 'Forward Method', and 'Built-in Actions' is shown, currently containing 0 items. At the bottom left, the '+ Add' button is highlighted with a red box. At the bottom right are 'OK' and 'Cancel' buttons.

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**.

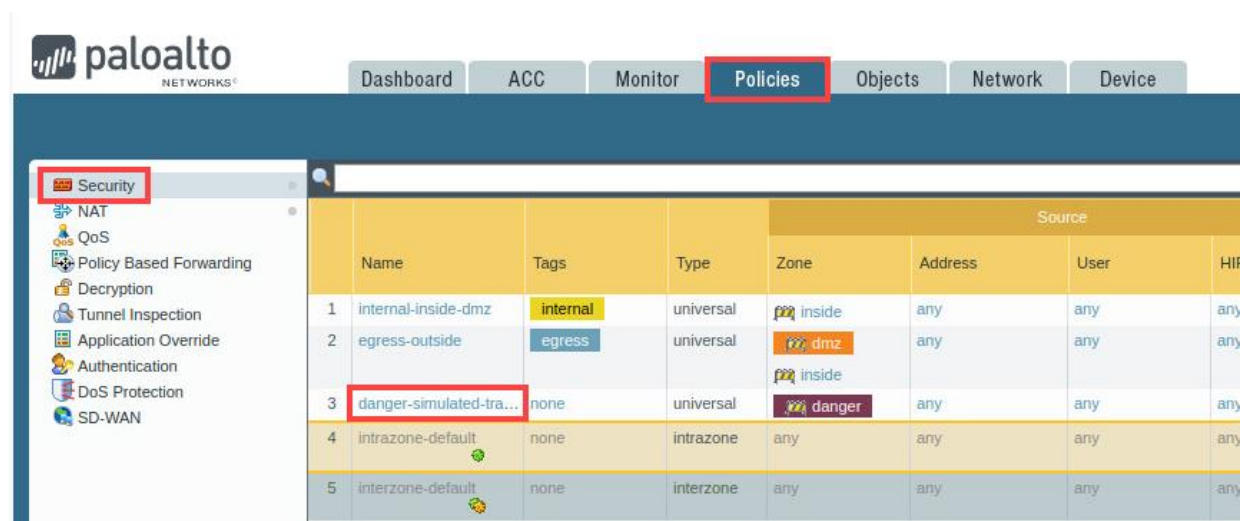


The screenshot shows the 'Log Forwarding Profile Match List' window. The 'Name' field is populated with 'syslog-server' and is highlighted with a red box. The 'Log Type' dropdown is set to 'threat' and is highlighted with a red box. The 'Filter' dropdown is set to 'All Logs' and is highlighted with a red box. Under the 'Forward Method' section, the 'Syslog' subsection is expanded, and the 'syslog-analysis' entry is checked and highlighted with a red box. The 'Built-in Actions' section is empty. At the bottom right, the 'OK' button is highlighted with a red box.

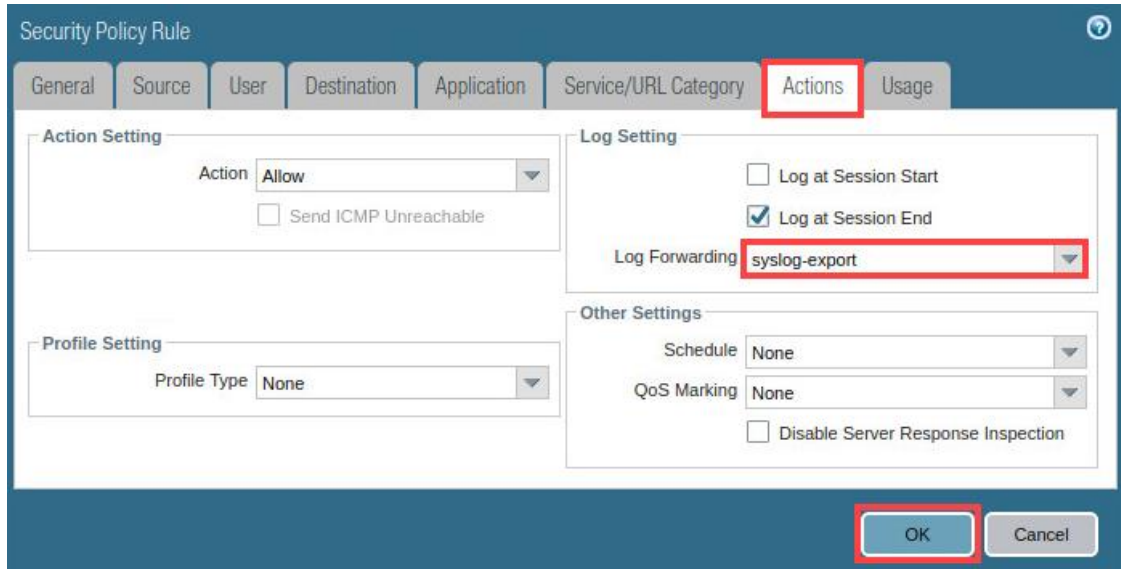
6. On the *Log Forwarding Profile* window, click **OK**.



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



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

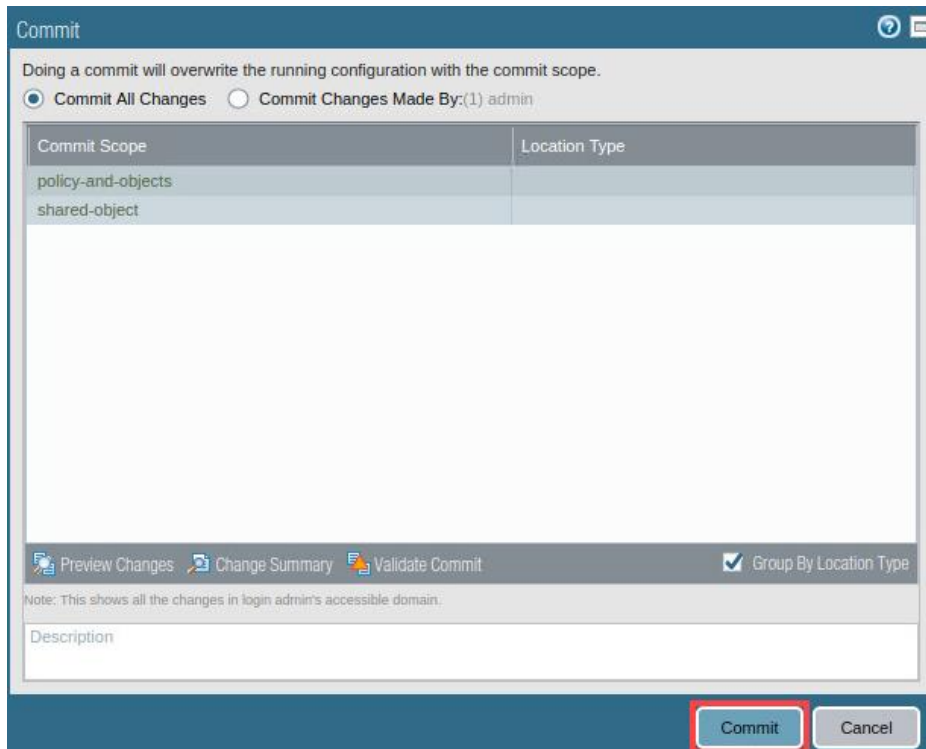


The **Security Policy Rule** window is shown with the **Actions** tab selected. The **Action Setting** section has **Action** set to **Allow** and **Send ICMP Unreachable** unchecked. The **Log Setting** section has **Log at Session Start** unchecked, **Log at Session End** checked, and **Log Forwarding** set to **syslog-export**. The **Profile Setting** section has **Profile Type** set to **None**. The **Other Settings** section has **Schedule** and **QoS Marking** both set to **None**, and **Disable Server Response Inspection** unchecked. The **OK** button is highlighted.

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



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



The **Commit** window is shown. It displays a message: "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 lists the commit scope and location type:

Commit Scope	Location Type
policy-and-objects	
shared-object	

At the bottom, there are links for **Preview Changes**, **Change Summary**, and **Validate Commit**, along with a checked **Group By Location Type** checkbox. A note states: "Note: This shows all the changes in login admin's accessible domain." The **Commit** button is highlighted.



## 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.



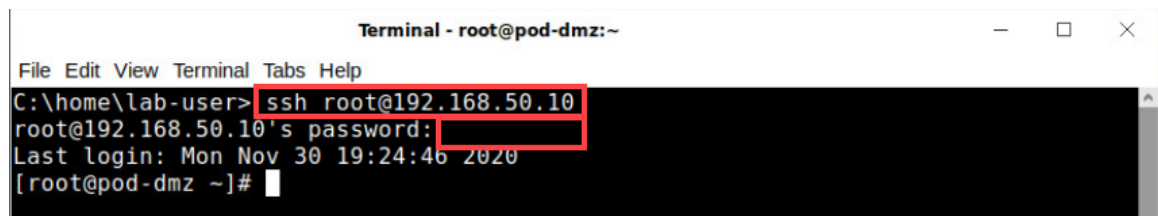
The metrics displayed in the lab screenshots and the metrics displayed on your lab Firewall might be different.

1. On the student desktop, open an *Xfce Terminal* window by clicking on the **Terminal** icon.



2. SSH to the *DMZ* by typing the command below. Use **pa10A1t0** for the password. If prompted, enter **yes** to continue connecting. Press **Enter**.

```
C:\home\lab-user> ssh root@192.168.50.10
```



3. Capture traffic packets to the Palo Alto Networks Firewall by typing the command below.

```
[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
   100    987   100    107   100    880     45    370   0:00:02   0:00:02   --:--:--   370

. . . GENERATING TRAFFIC
```



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

4. Push malware packet captures to the Palo Alto Networks Firewall by typing the command below.

```
[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.

5. Once the scripts finish executing, type `exit` to end the `ssh` session to **192.168.50.10** (DMZ server).

```
[root@pod-dmz ~]# exit
logout
Connection to 192.168.50.10 closed.
C:\home\lab-user>
```

6. Close the *terminal* window by clicking on **X** icon located at the top-right. Continue to the next task.

Terminal - root@pod-dmz:~



### 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. On the student desktop, open an *Xfce Terminal* window by clicking on the **Terminal** icon.



2. SSH to the *DMZ* by typing the command below. Use **Pa10A1t0** for the password. If prompted, enter **yes** to continue connecting. Press **Enter**.

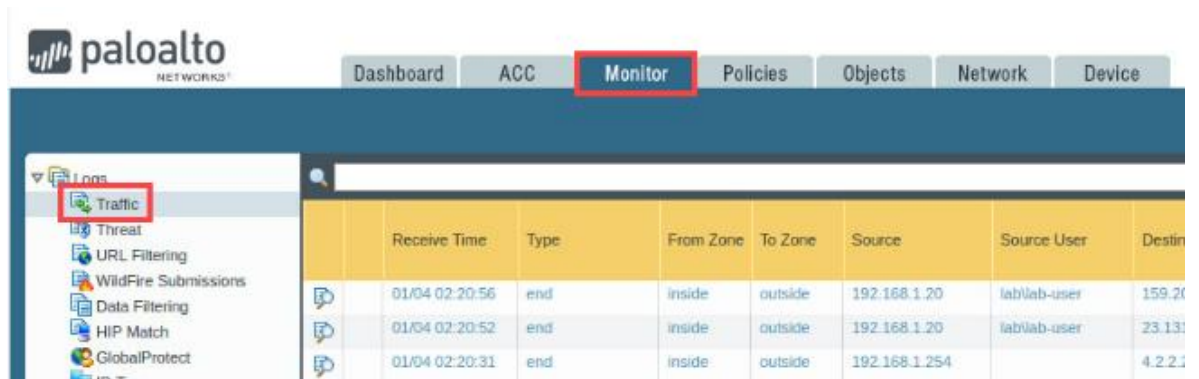
```
C:\home\lab-user> ssh root@192.168.50.10
```



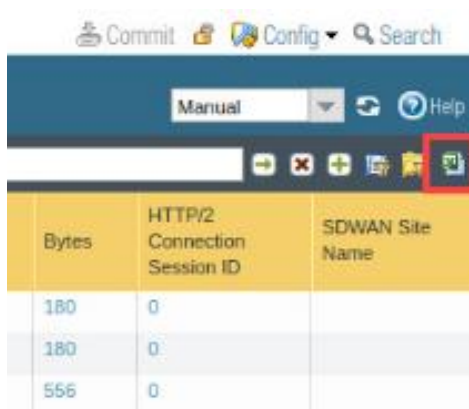
3. Navigate back to the *Palo Alto Networks Firewall Web-UI* by clicking on the minimized **Chromium** icon in the lower-left of the student desktop.



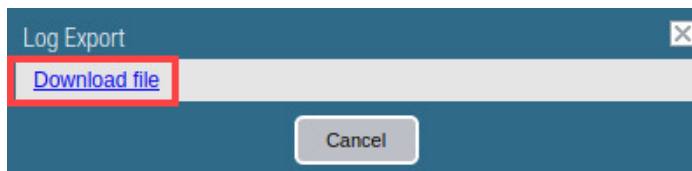
4. Navigate to **Monitor > Logs > Traffic**.



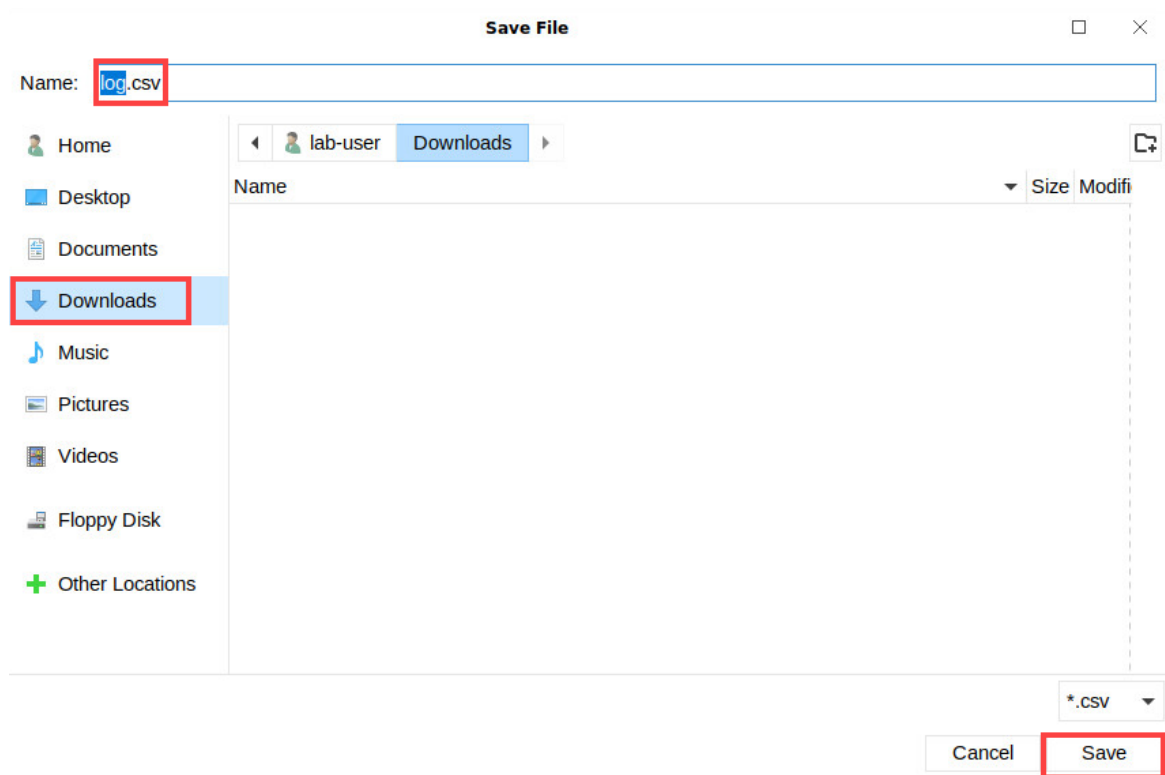
5. Click the **spreadsheet** icon to export the Firewall's traffic log as a *csv file*.



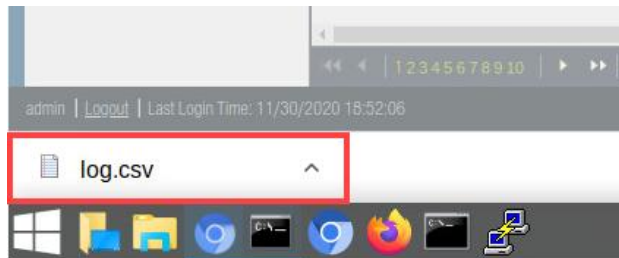
6. In the *Log Export* window, click **Download file**.



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



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



9. 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
	Domain	Receive Time	Serial #	Type	Threat/Co
1					
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

**Help** **OK** **Cancel**

## 10. Observe the Firewall's logged traffic using LibreOffice.

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	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
1	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	rsp
2	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
3	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	paltoalto-up	dns
4	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
5	1	2021/01/04 02:29:18	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:18	192.168.1.20	35.232.111.17	203.0.113.20	35.232.111.17	egress-outside	lab/lab-user	web-brows
6	1	2021/01/04 02:29:04	15351000056630	TRAFFIC	end	2305	2021/01/04 02:29:04	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab/lab-user	rsp
7	1	2021/01/04 02:28:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:31	192.168.1.20	162.159.200.123	203.0.113.20	162.159.200.123	egress-outside	lab/lab-user	rsp
8	1	2021/01/04 02:28:27	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:27	192.168.1.20	108.62.122.57	203.0.113.20	108.62.122.57	egress-outside	lab/lab-user	rsp
9	1	2021/01/04 02:28:23	15351000056630	TRAFFIC	end	2305	2021/01/04 02:28:23	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside		dns
10	1	2021/01/04 02:27:39	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:39	192.168.1.20	23.131.160.7	203.0.113.20	23.131.160.7	egress-outside	lab/lab-user	rsp
11	1	2021/01/04 02:27:33	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:33	192.168.1.254	159.203.158.197	203.0.113.20	159.203.158.197	egress-outside	lab/lab-user	rsp
12	1	2021/01/04 02:27:31	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:31	192.168.1.254	23.45.180.216	203.0.113.20	23.45.180.216	egress-outside		dns
13	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	paltoalto-up	dns
14	1	2021/01/04 02:27:17	15351000056630	TRAFFIC	end	2305	2021/01/04 02:27:17	192.168.1.254	4.2.2.2	203.0.113.20	4.2.2.2	egress-outside		dns
15	1	2021/01/04 02:26:31	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
16	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	paltoalto-up	dns
17	1	2021/01/04 02:26:17	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:17	192.168.1.20	71.114.67.173	203.0.113.20	71.114.67.173	egress-outside	lab/lab-user	rsp
18	1	2021/01/04 02:26:16	15351000056630	TRAFFIC	end	2305	2021/01/04 02:26:16	192.168.1.20	162.159.200.123	203.0.113.20	162.159.200.123	egress-outside	lab/lab-user	web-brows
19	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	203.0.113.20	65.55.15.244	egress-outside		dns
20	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
21	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	paltoalto-up	dns
22	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
23	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	rsp
24	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	paltoalto-up	dns
25	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	rsp
26	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	rsp
27	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
28	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
29	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	paltoalto-up	dns
30	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
31	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
32	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	web-brows
33	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	rsp
34	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
35	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
36	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	paltoalto-up	dns
37	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	rsp
38	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	rsp
39	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	rsp
40	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
41	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	paltoalto-up	dns
42	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	rsp

Sheet 1 of 1



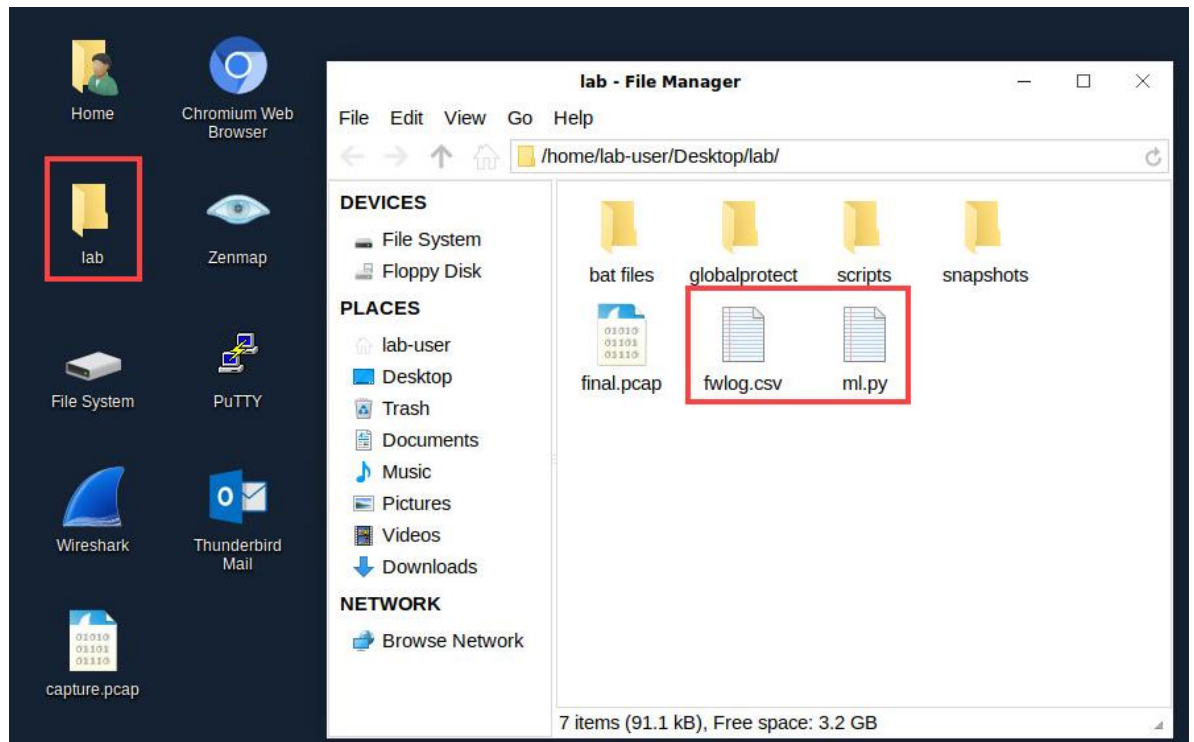
**Please Note**

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.

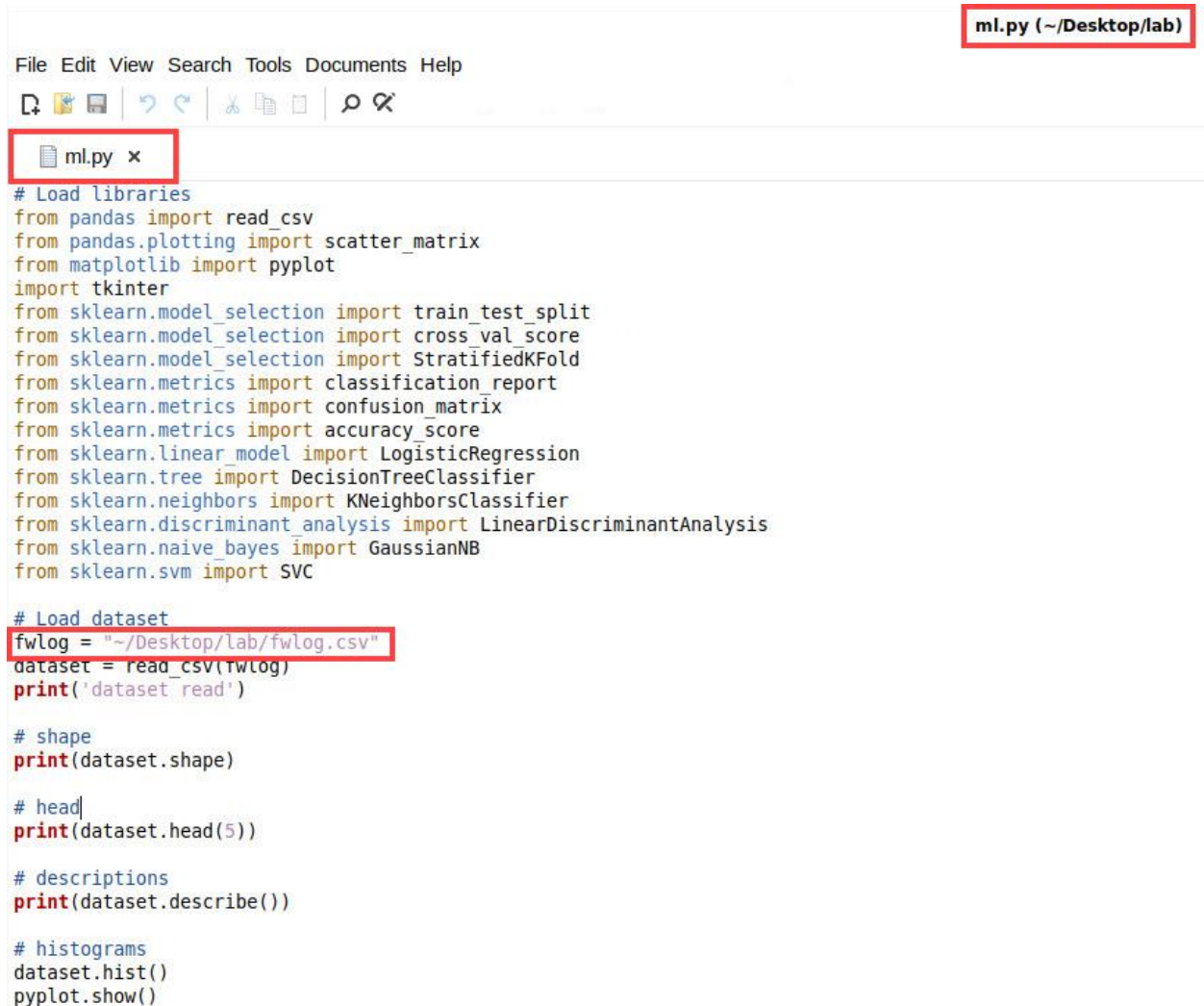
11. On the lower-left of the client desktop, click the **Minimize all open windows and show the desktop** icon.



12. 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.



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



```
File Edit View Search Tools Documents Help
ml.py x
# 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')

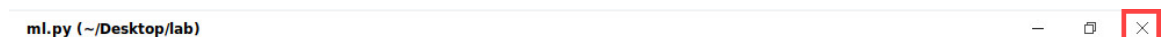
# shape
print(dataset.shape)

# head
print(dataset.head(5))

# descriptions
print(dataset.describe())

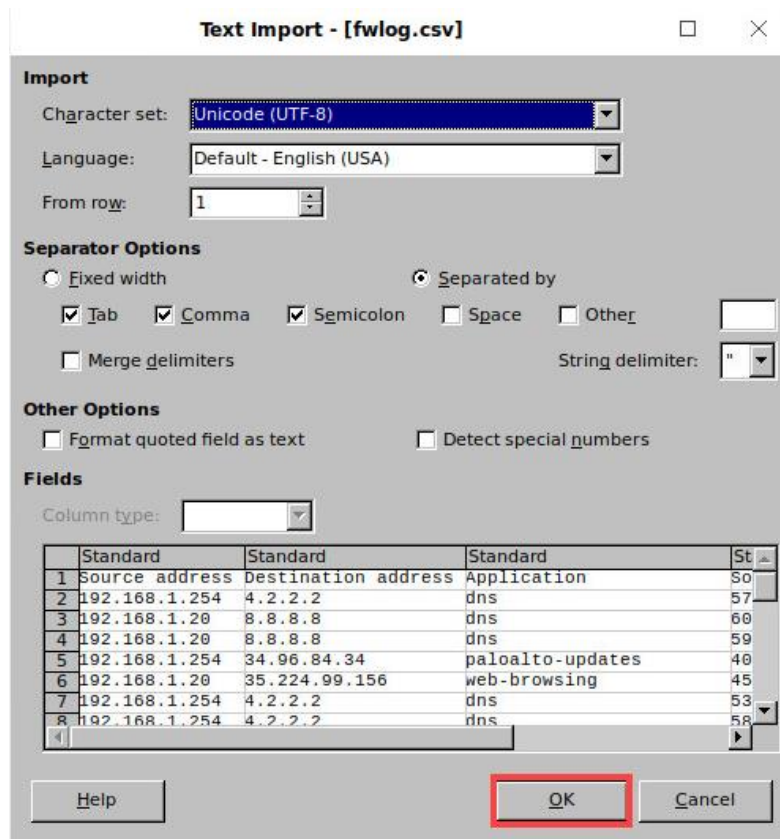
# histograms
dataset.hist()
pyplot.show()
```

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





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



16. 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)

	A	B	C	D	E	F	G	H	I
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				
7	192.168.1.254	4.2.2.2	dns	53510	53				
8	192.168.1.254	4.2.2.2	dns	50722	53				

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

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

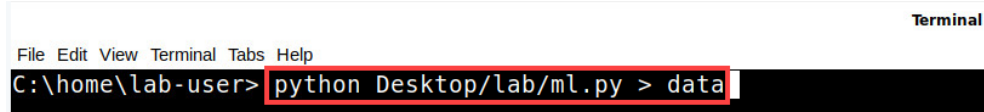


18. On the client desktop, open a *terminal* window by clicking on the **Xfce Terminal** icon.

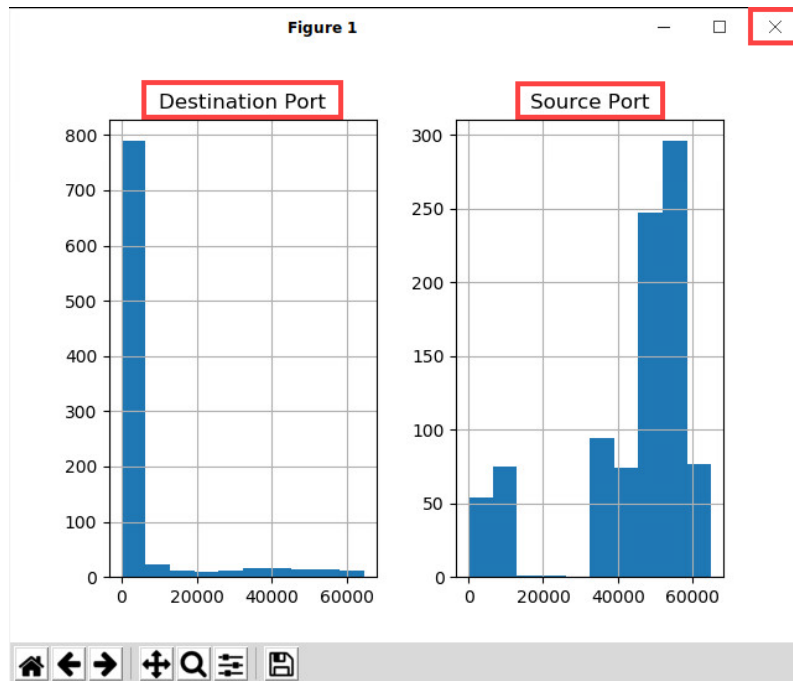


19. Execute the **ml.py** python file by typing the command below.

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



20. 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.

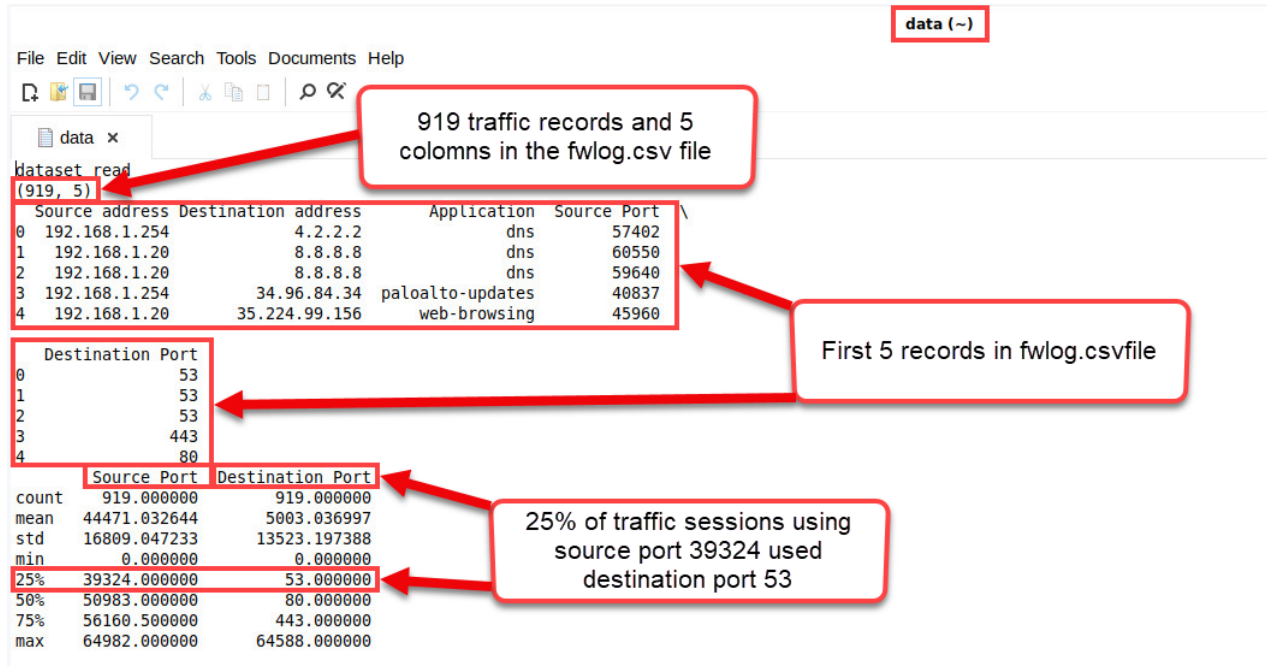


21. In the *terminal* window, open the **data** file created by typing the command below.

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

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

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



The screenshot shows a Jupyter Notebook interface with a file named 'data (~)' open. The notebook displays the first 5 records of a CSV file named 'fwlog.csv'. The data is presented in two tables. The first table shows the first 5 records, and the second table shows a summary of the data.

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

**First 5 records in fwlog.csvfile**

	Source address	Destination address	Application	Source Port	Destination Port
0	192.168.1.254	4.2.2.2	dns	57402	53
1	192.168.1.20	8.8.8.8	dns	60550	53
2	192.168.1.20	8.8.8.8	dns	59640	53
3	192.168.1.254	34.96.84.34	paloalto-updates	40837	443
4	192.168.1.20	35.224.99.156	web-browsing	45960	80

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

	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

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