SECURITY OPERATIONS FUNDAMENTALS

Lab 1: Network Traffic Analysis

Document Version: 2021-01-29

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

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

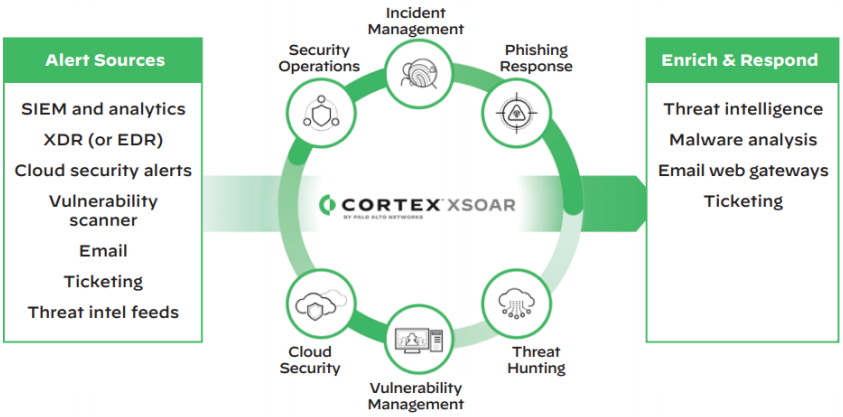
Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

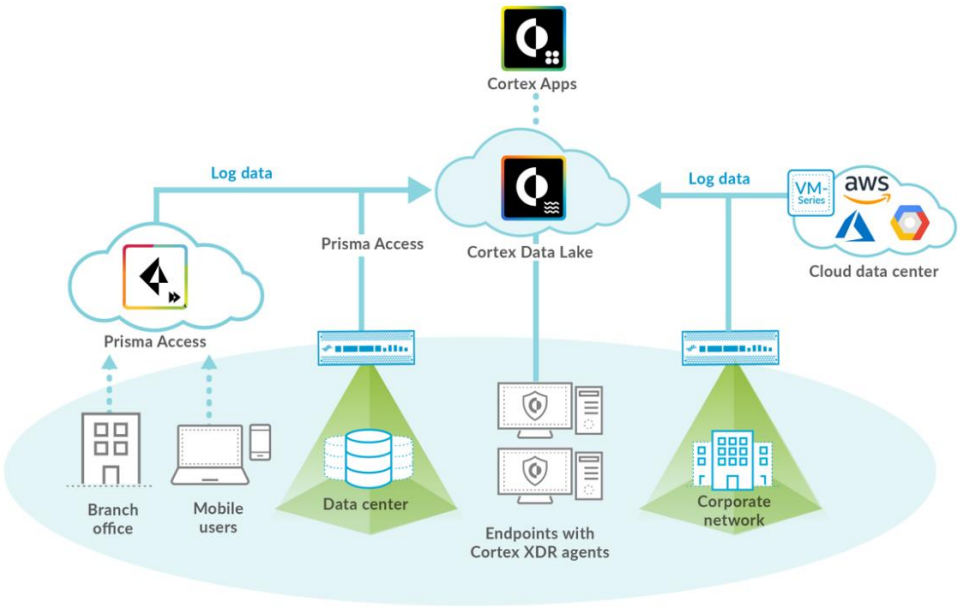
Contents

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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.





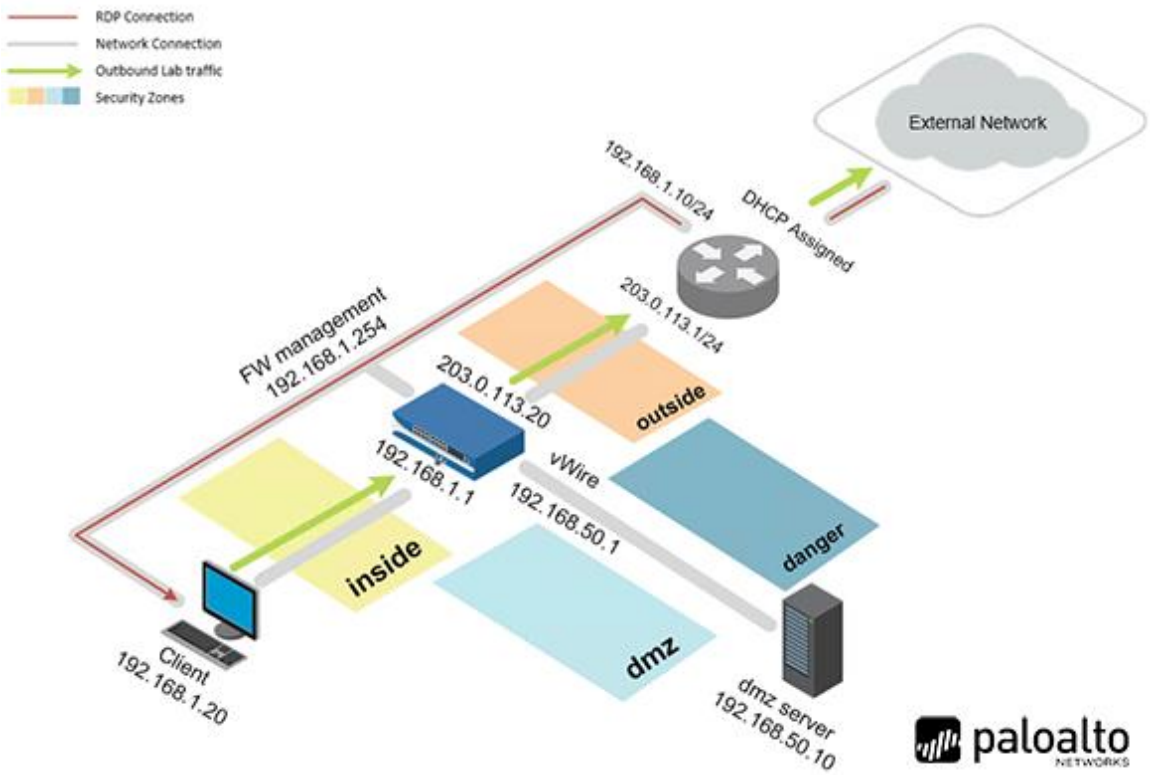
Objective

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

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

Lab Topology



 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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$

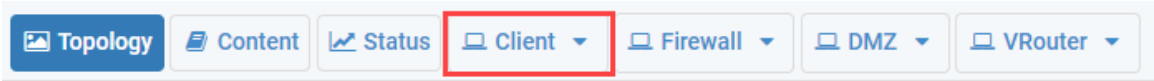
Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1 Network Traffic Analysis

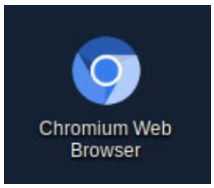
1.0 Load Lab Configuration

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

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

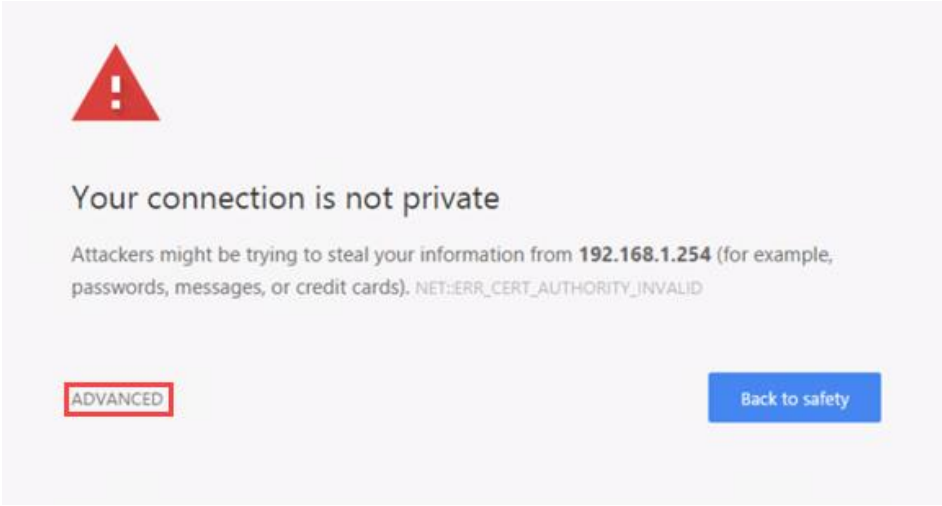


2. Log in to the client PC with the username **`lab-user`** and password **`Train1ng$`**.
3. Double-click the **Chromium** icon located on the desktop.



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

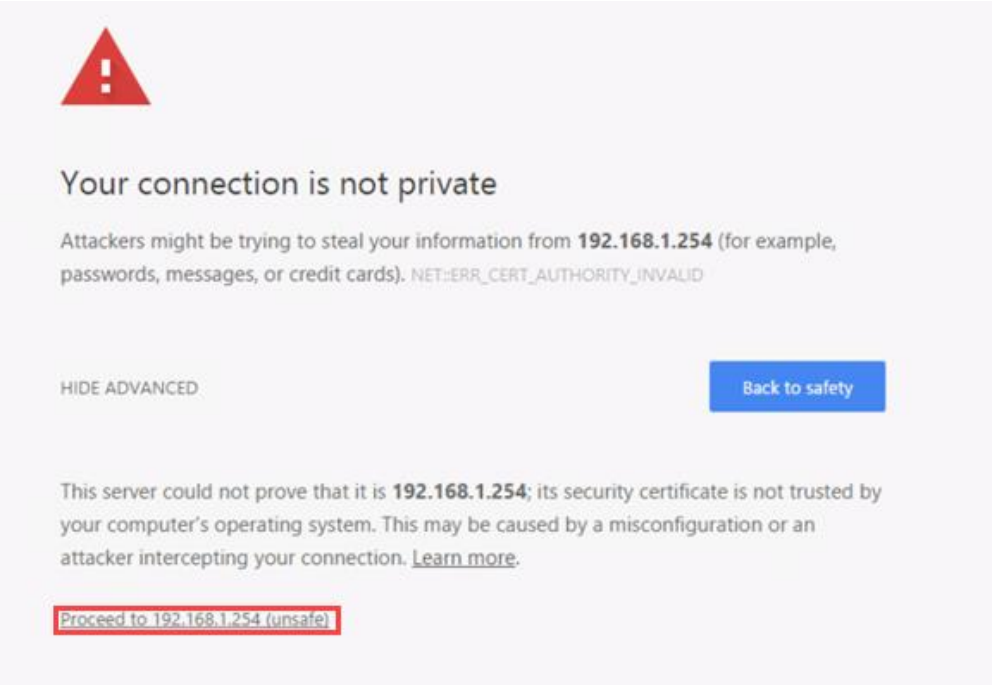
5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



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.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

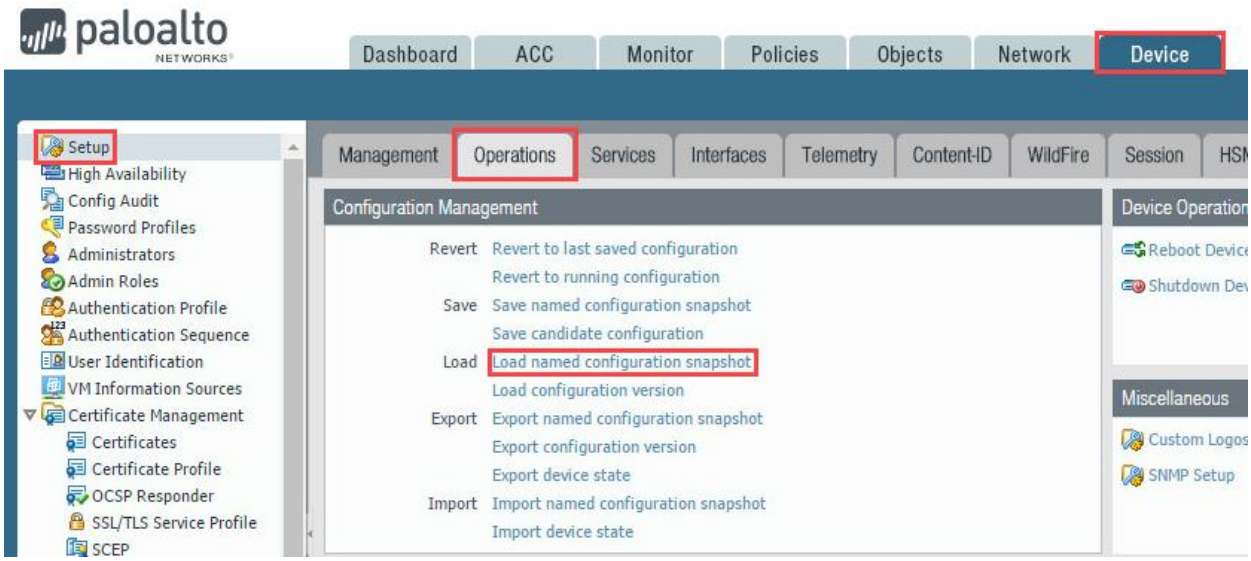
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



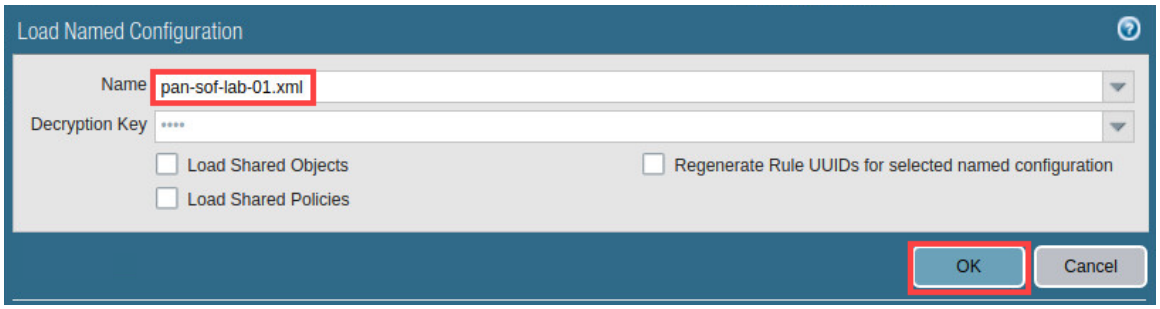
7. Log in to the Firewall web interface as username **`admin`**, password **`Train1ng$`**.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

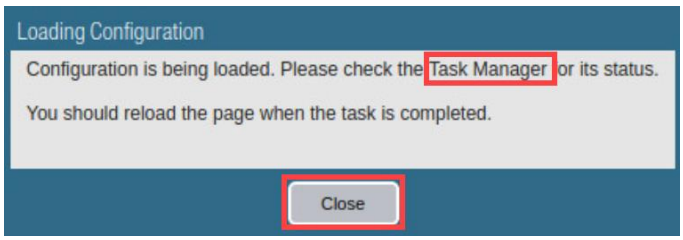
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



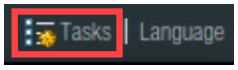
9. In the *Load Named Configuration* window, select **pan-sof-lab-01.xml** from the *Name* dropdown box and click **OK**.



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.

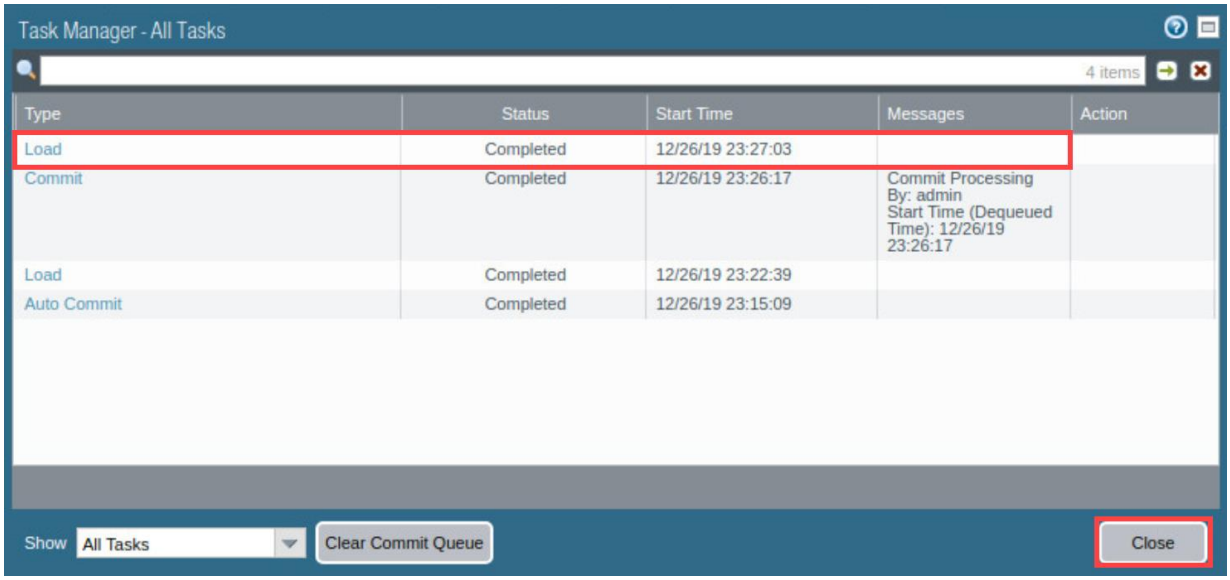


11. Click the **Tasks** icon located at the bottom-right of the web interface.



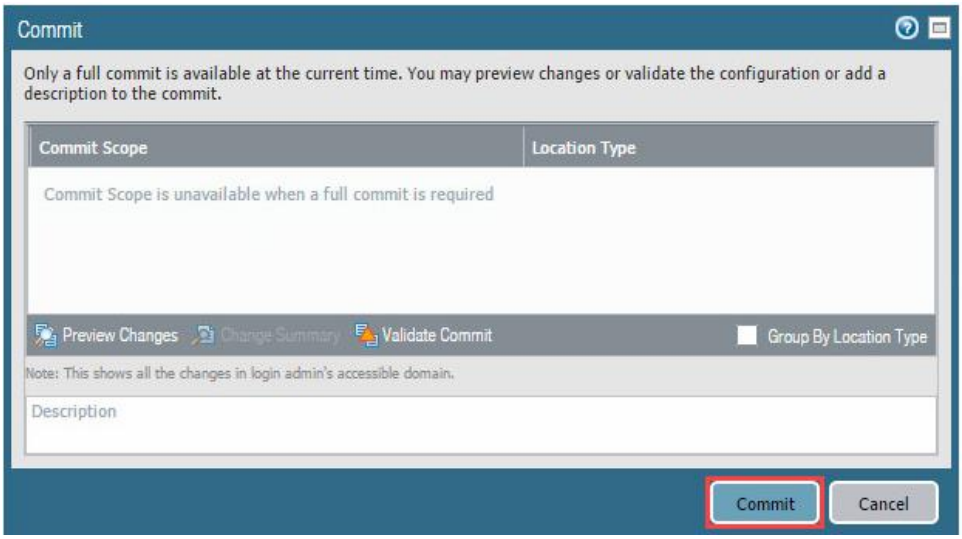
 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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



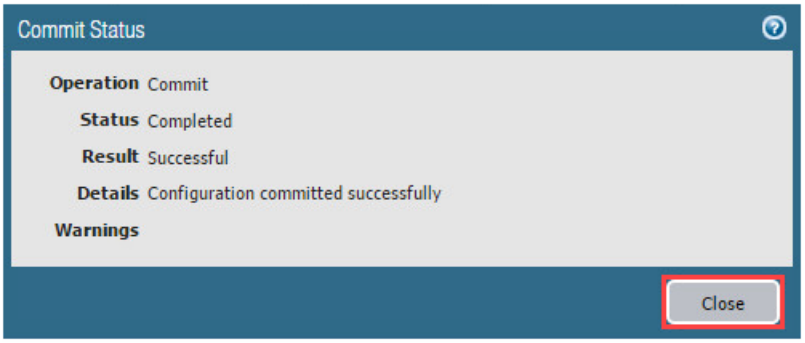
13. Click the **Commit** link located at the top-right of the web interface.

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



 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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



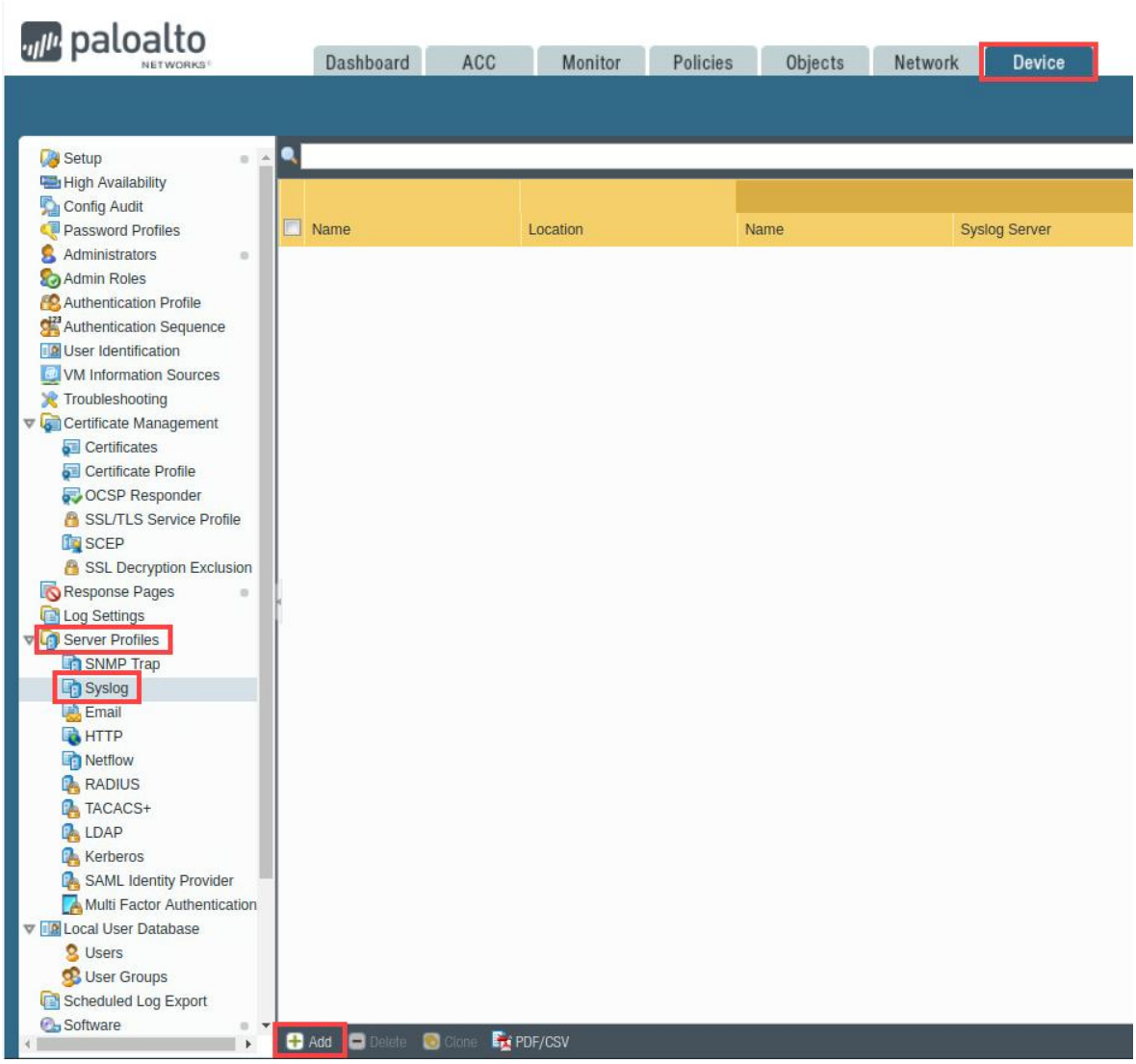
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

1.1 Export Firewall Log Data for Analysis

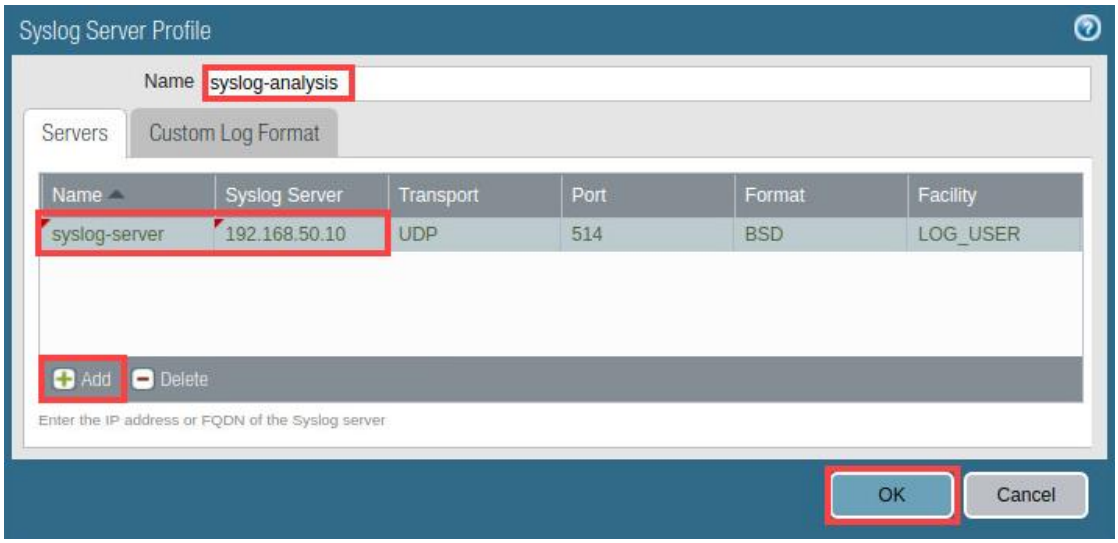
In this section, you are going to forward your Firewall's threat log to your DMZ server running syslog. Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices - such as routers, firewalls, printers - from different vendors into a central repository 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**.



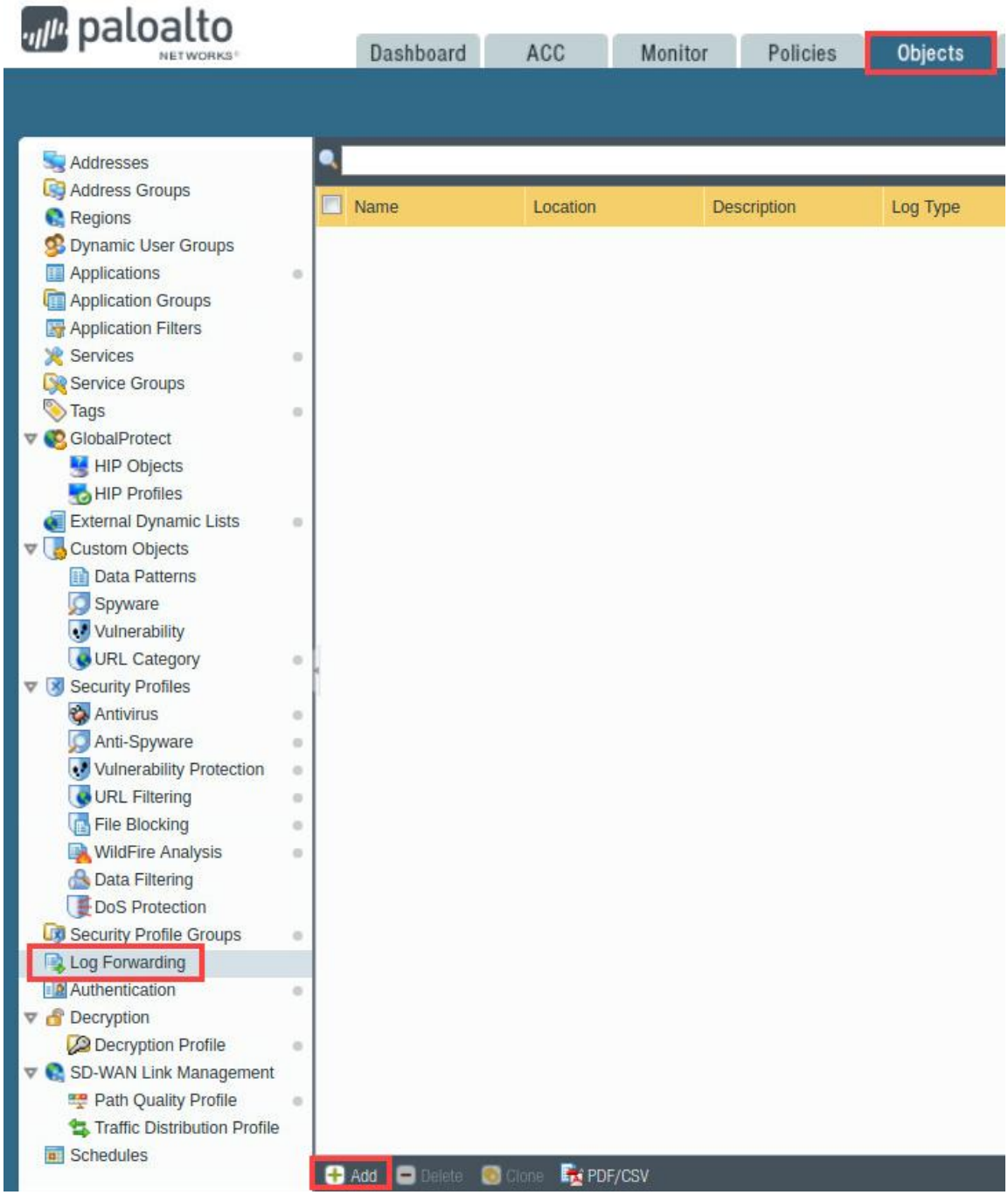
 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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**.



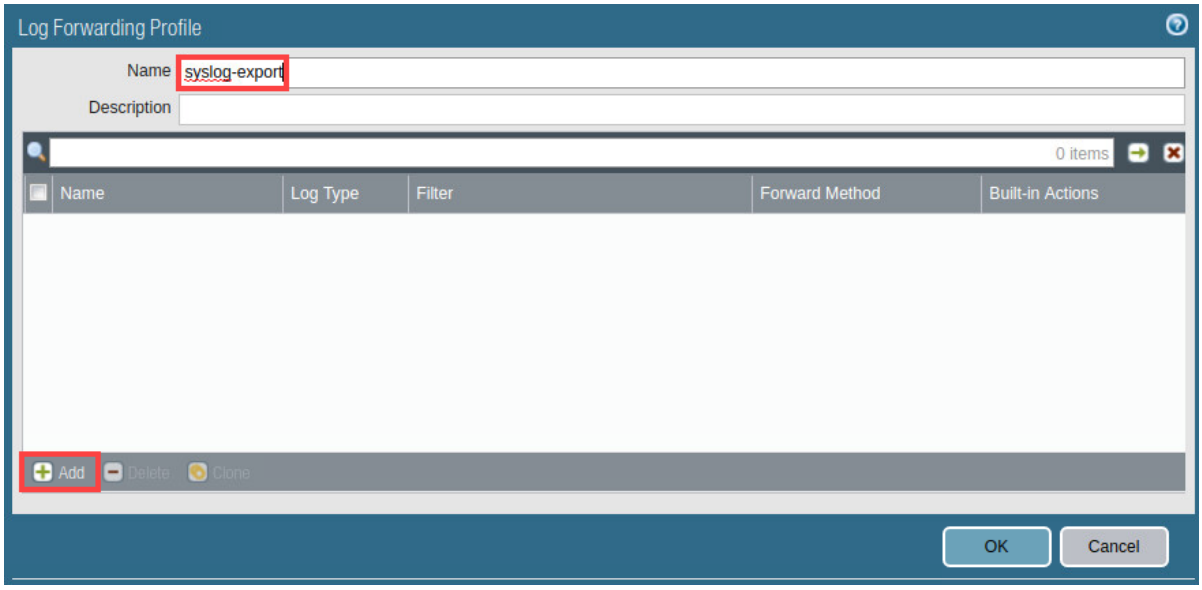
 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

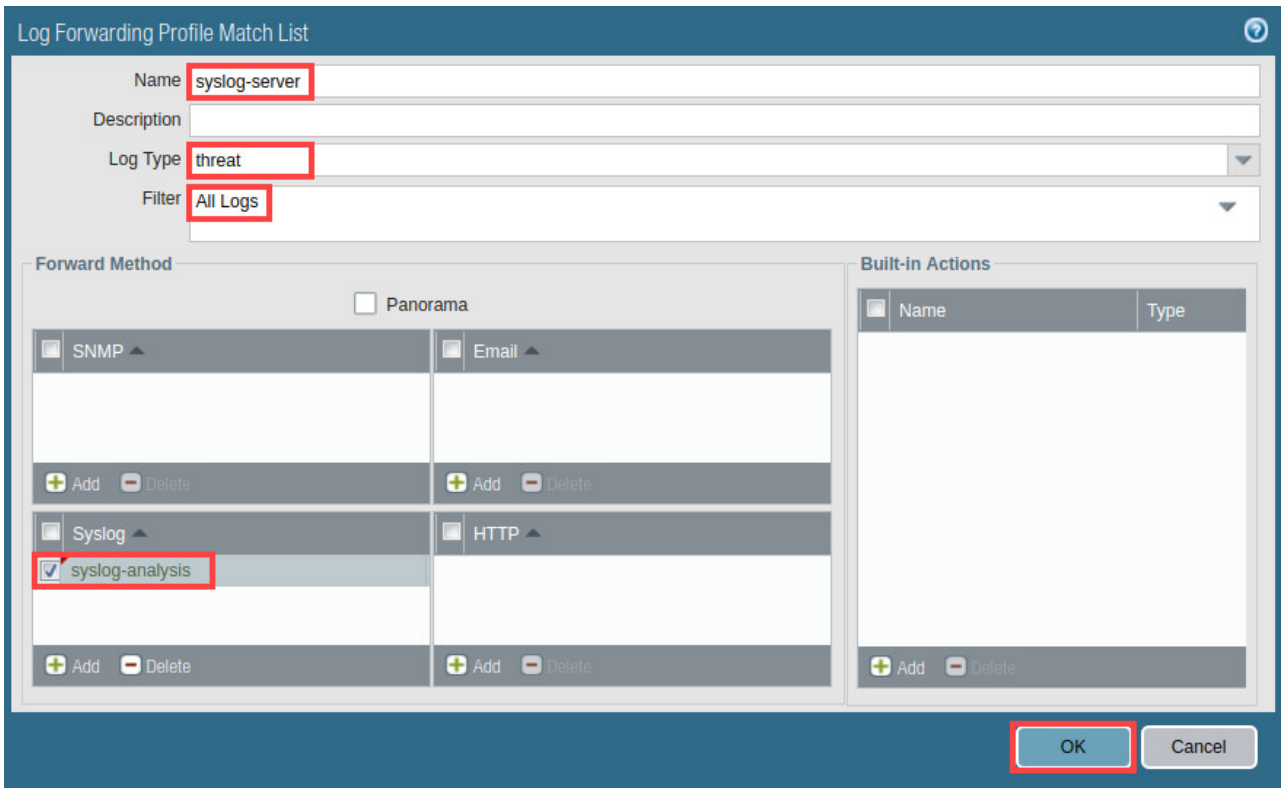


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

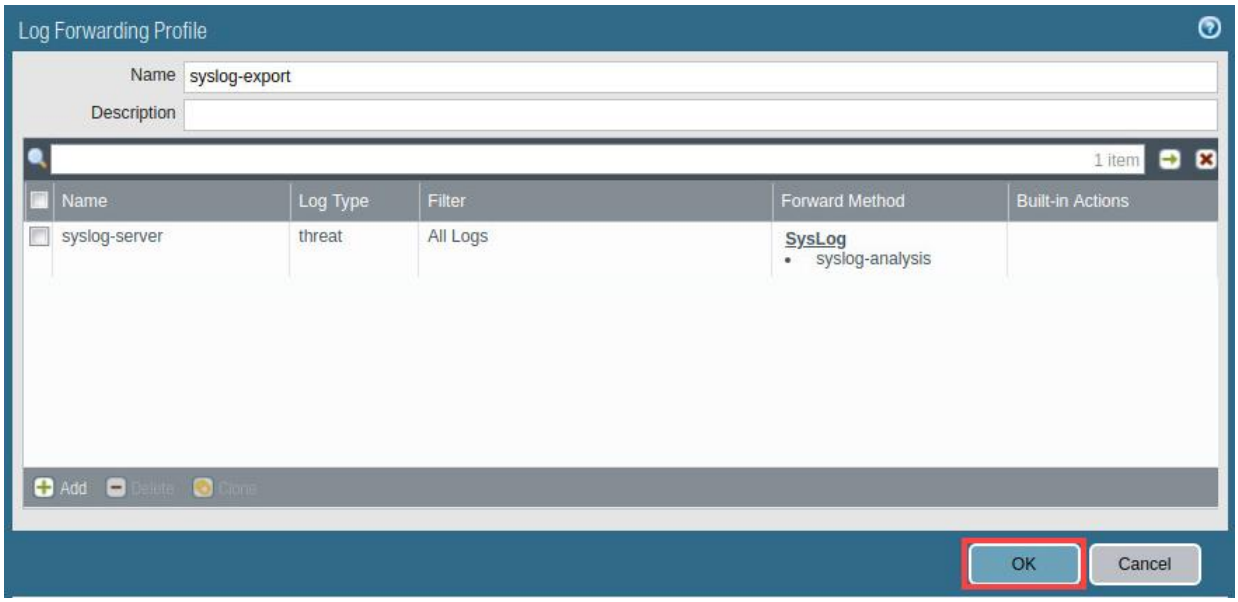


5. In the *Log Forwarding Profile Match List* window, type `syslog-server` in the *Name* field. Next, select **threat** in the *Log Type* field and verify **All Logs** is selected in the *Filter* field. Under the *Syslog* section, click **Add**. Finally, select **syslog-analysis** (the profile you created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

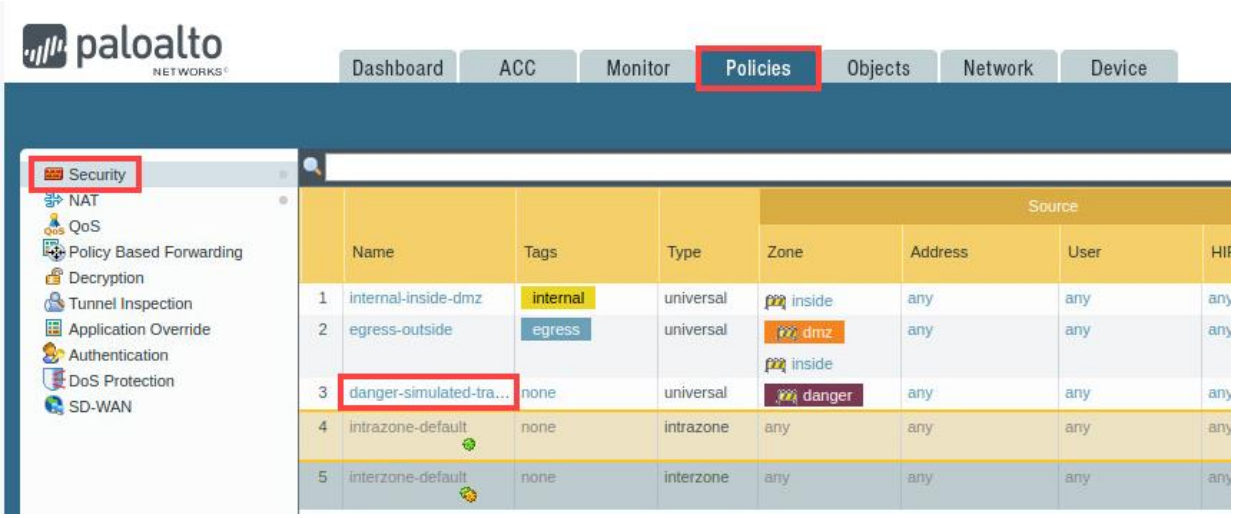


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

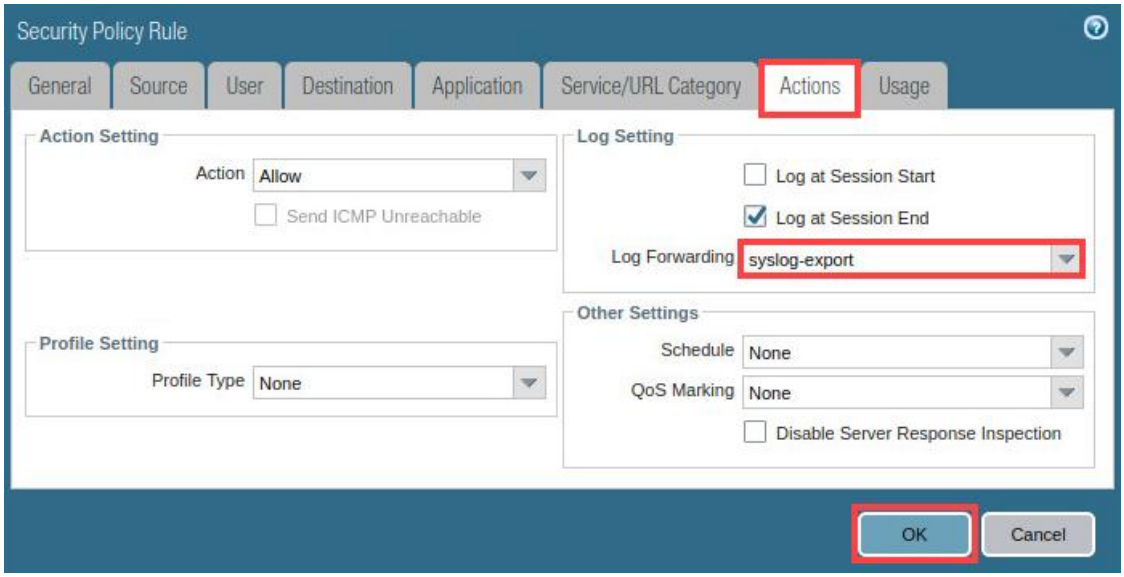


7. Navigate to **Policies > Security > danger-simulated-traffic**.



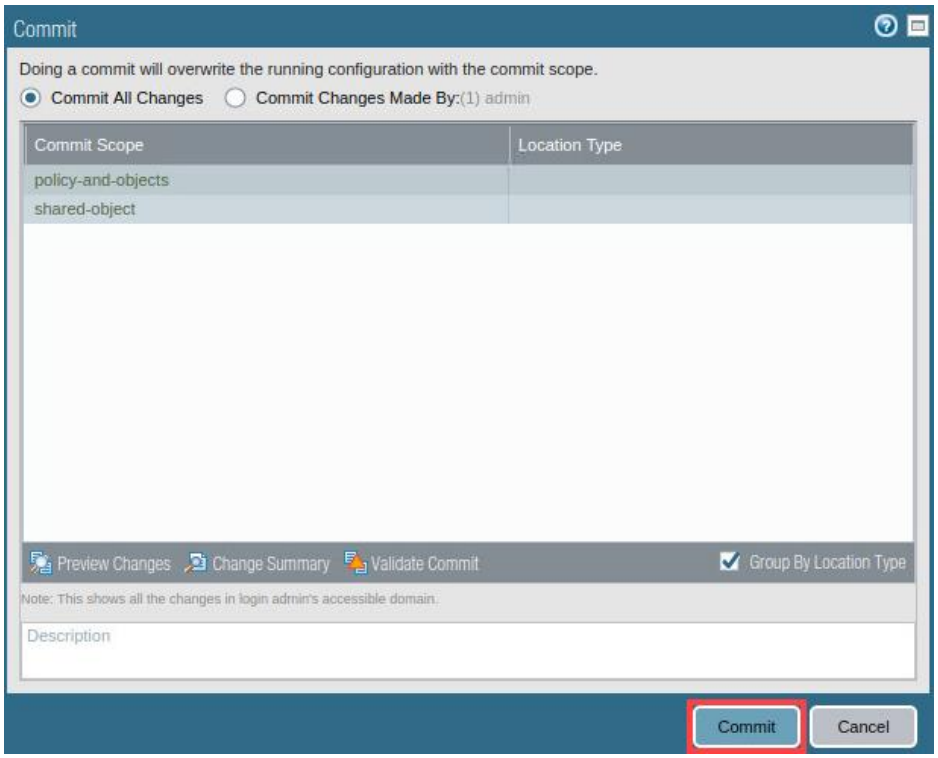
 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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



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

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



 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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.

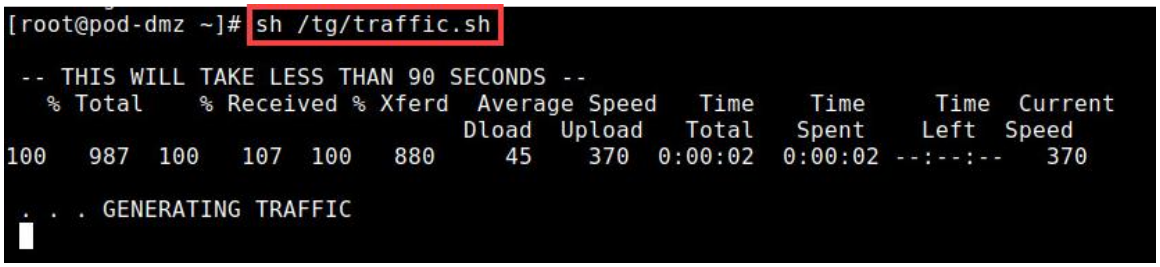
1. On the student desktop, open an *Xfce Terminal* window by clicking on the **Terminal** icon.

2. SSH to the *DMZ* by typing the command below. Use `PaloAlto` 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
```



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

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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.

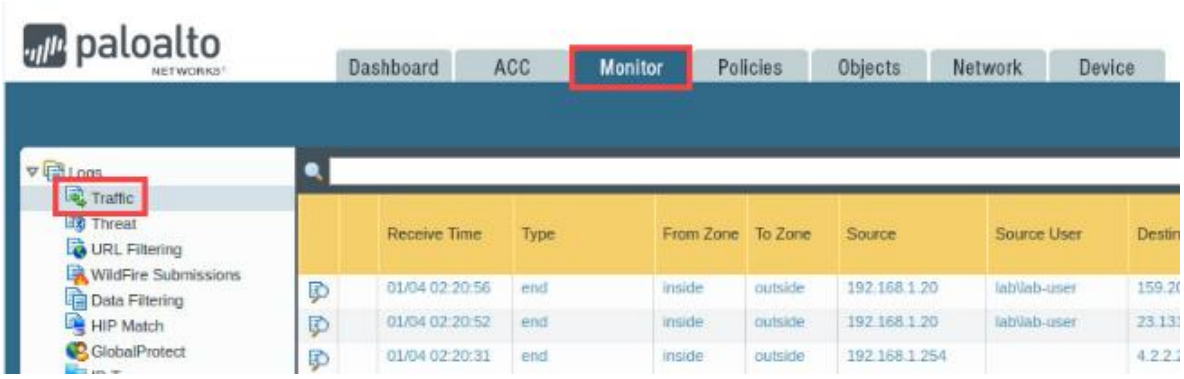
2. SSH to the *DMZ* by typing the command below. Use `PaloAlto` for the password. If prompted, enter `yes` to continue connecting. Press **Enter**.

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

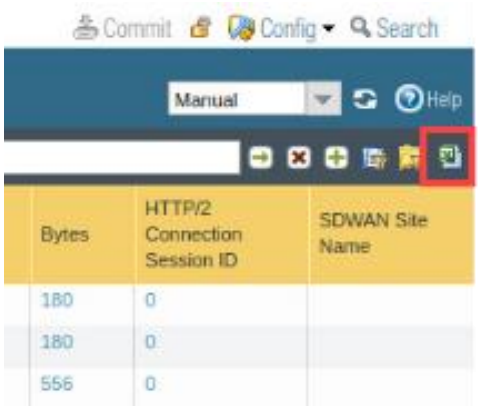
3. Navigate back to the *Palo Alto Networks Firewall Web-UI* by clicking on the minimized **Chromium** icon in the lower-left of the student desktop.

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

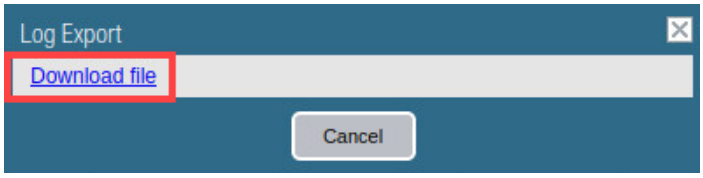
4. Navigate to **Monitor > Logs > Traffic**.



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

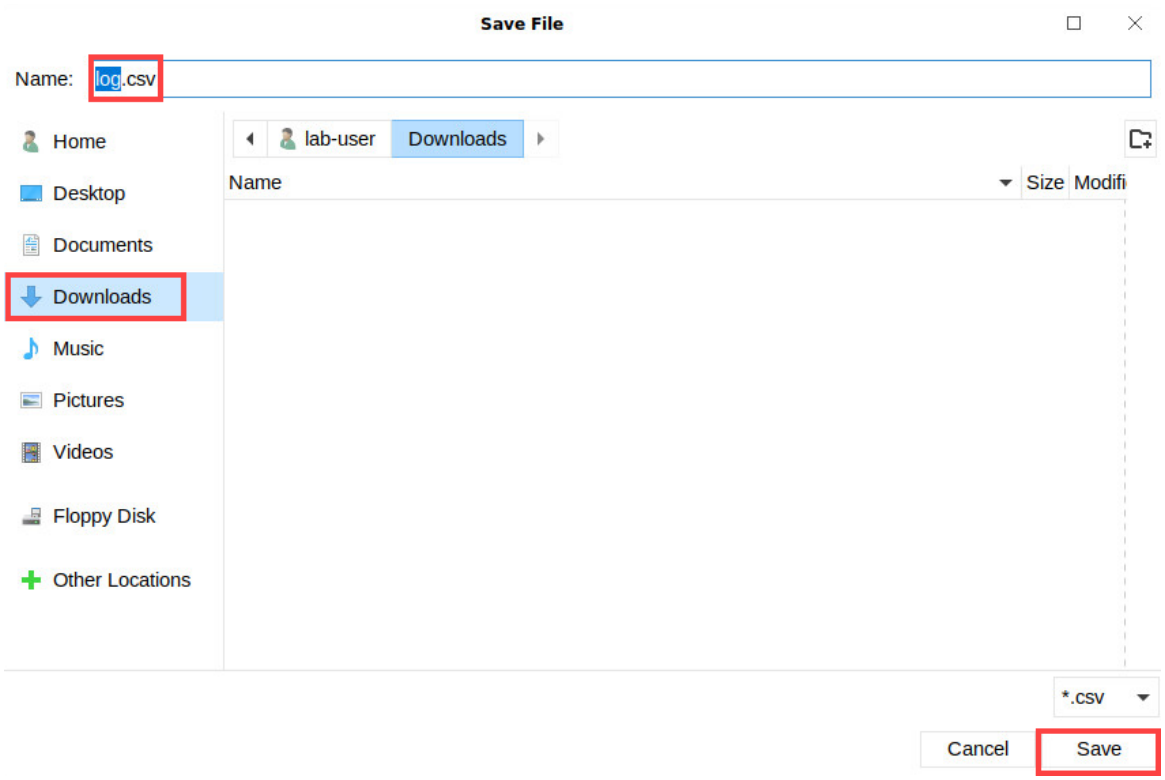


6. In the *Log Export* window, click **Download file**.

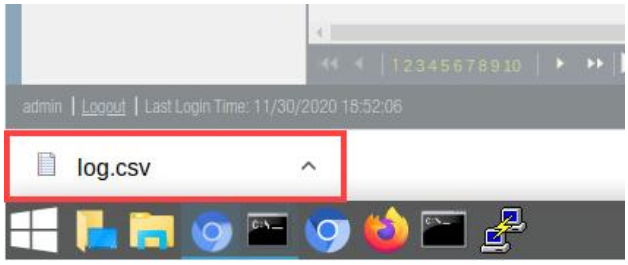


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

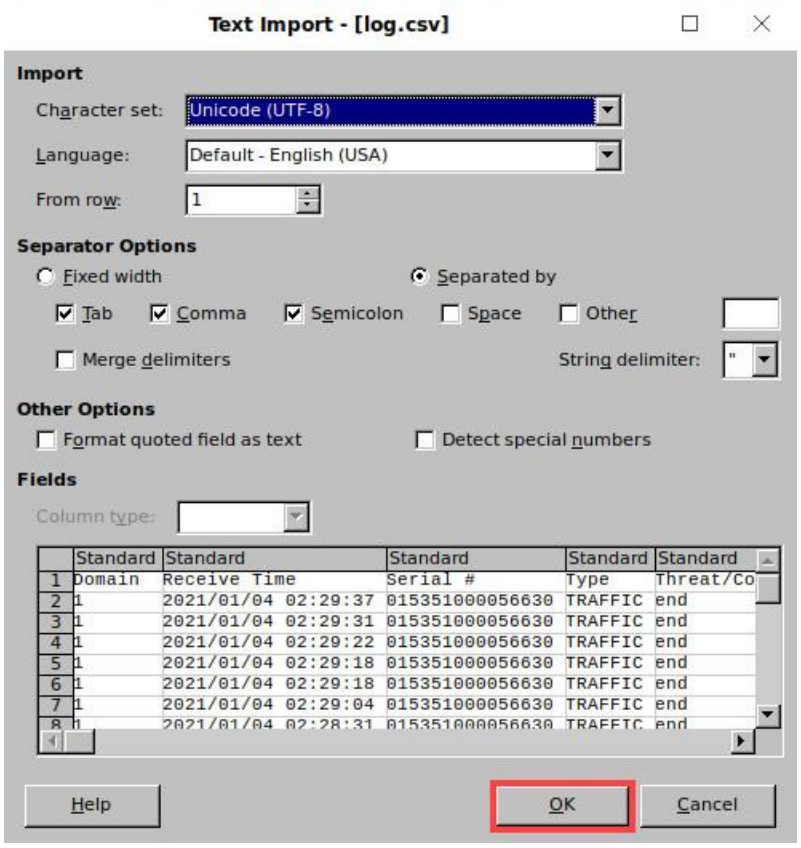


8. From the client, click the **log.csv** file that you downloaded in *steps* **5** and **6**.

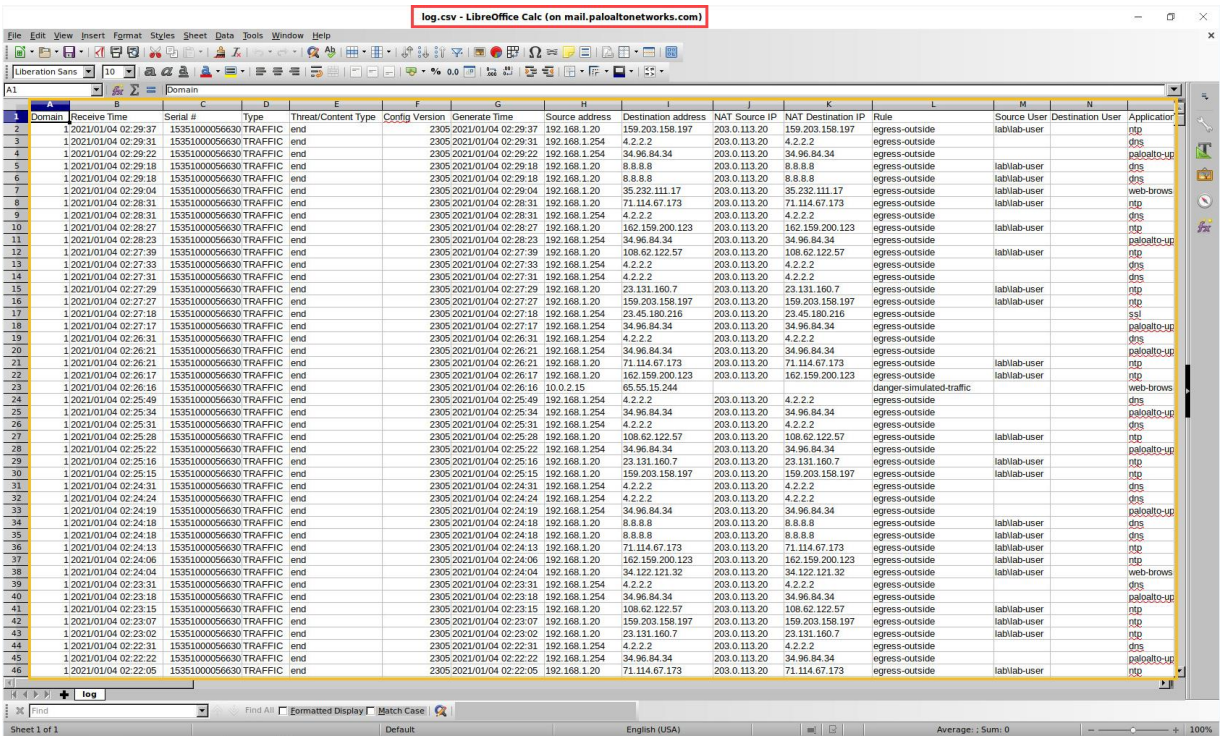


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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



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

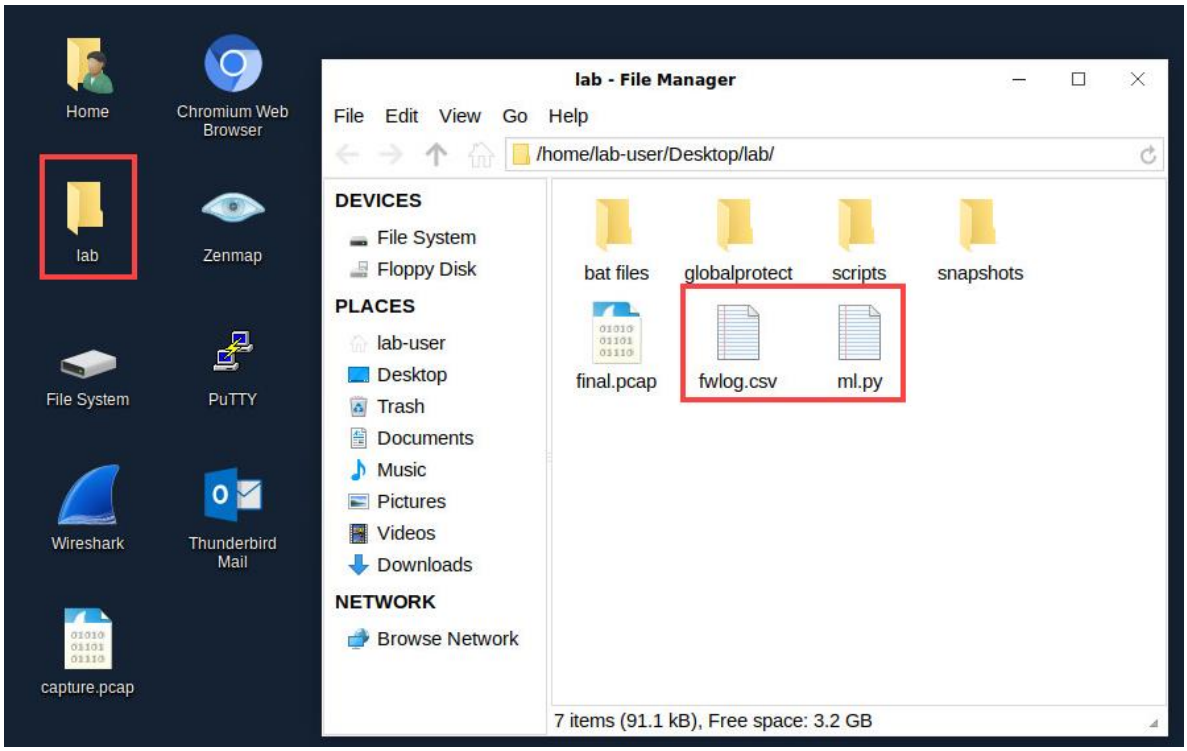


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

> **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.

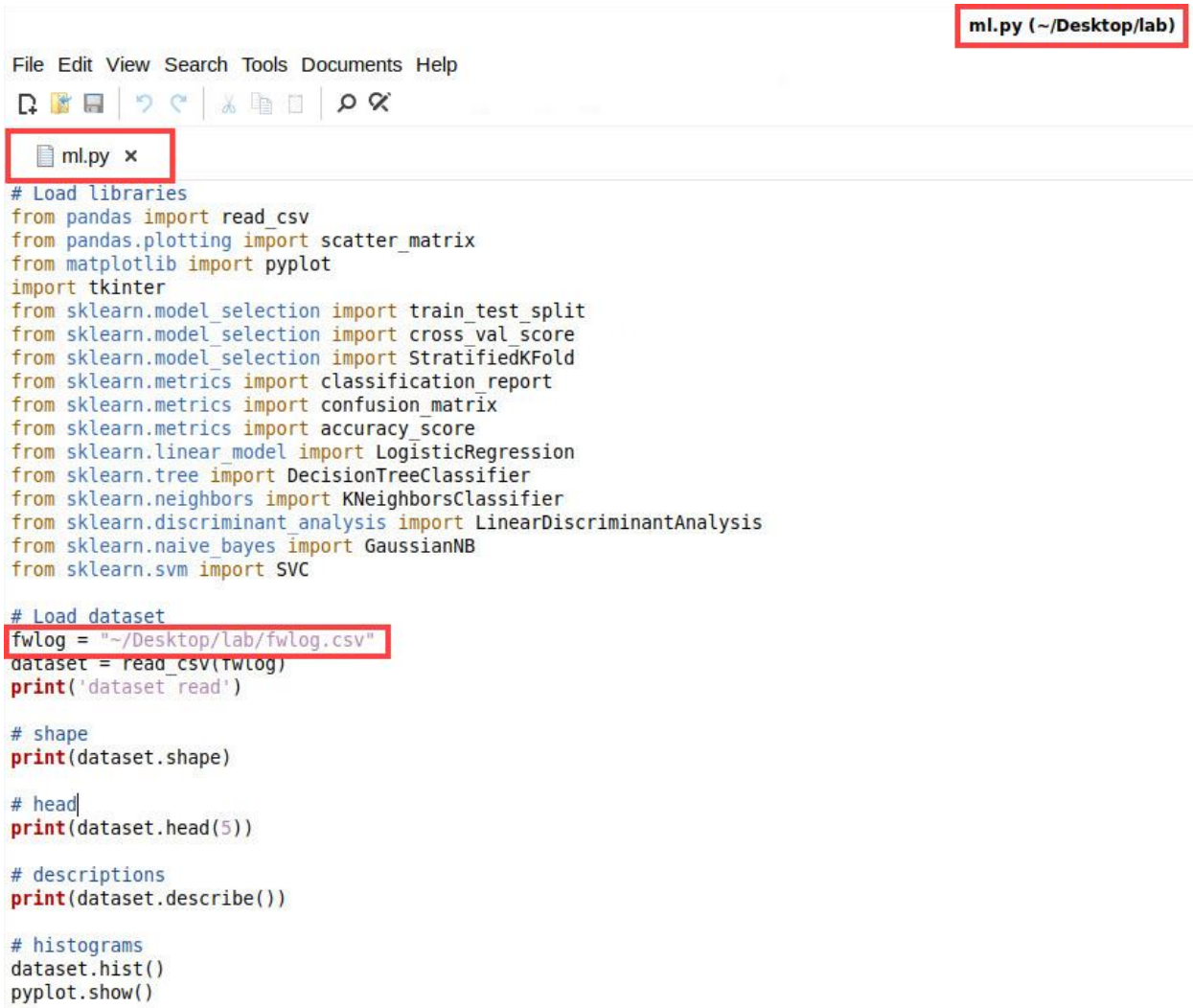
11. On the lower-left of the client desktop, click the **Minimize all open windows and show the desktop** icon.

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.

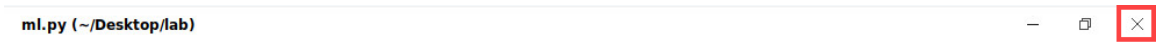


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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.

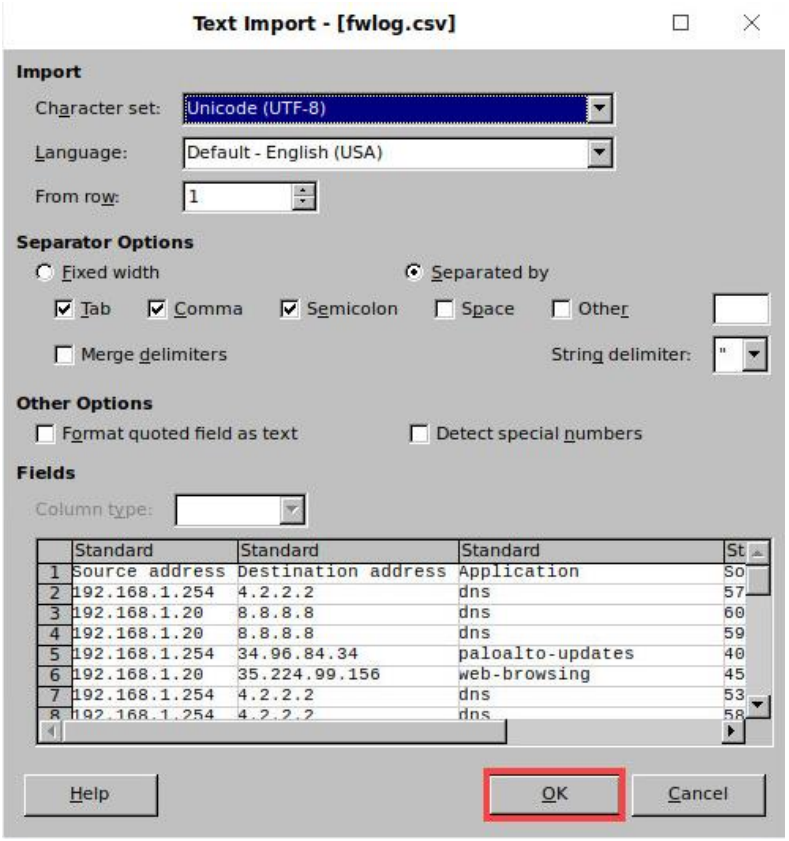


14. Close the **ml.py** file by clicking on the **X** icon.

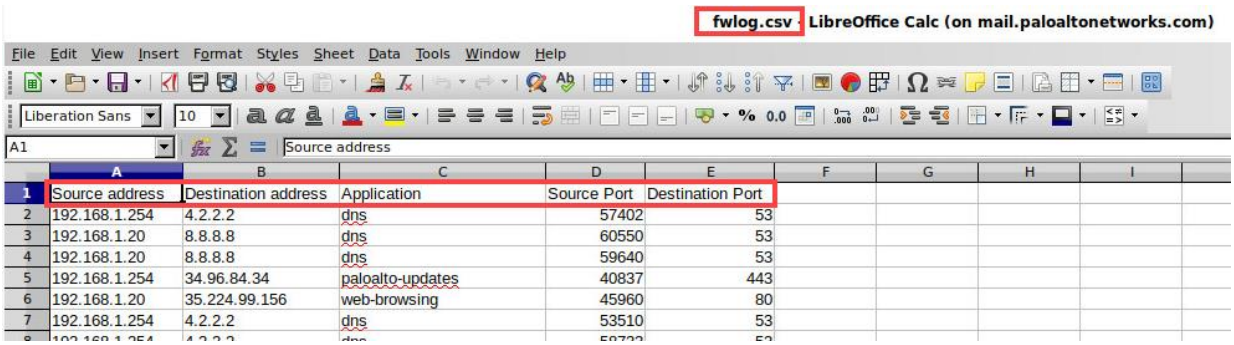


 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

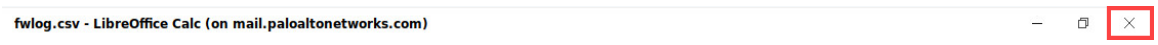
15. Double click the **fwlog.csv** file. When the *Text Import –[fwlog.csv]* window appears, click **OK**.



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

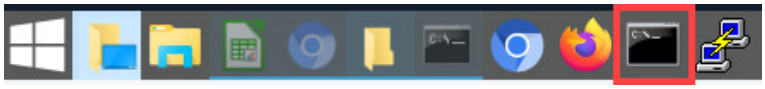


17. Close the **fwlog.csv** file by clicking on the **X** icon.



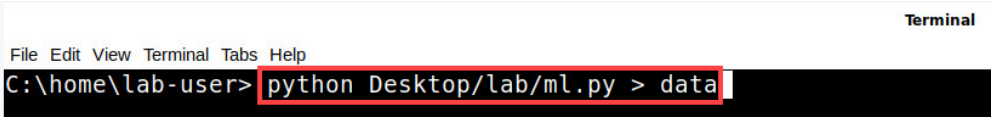
 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

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

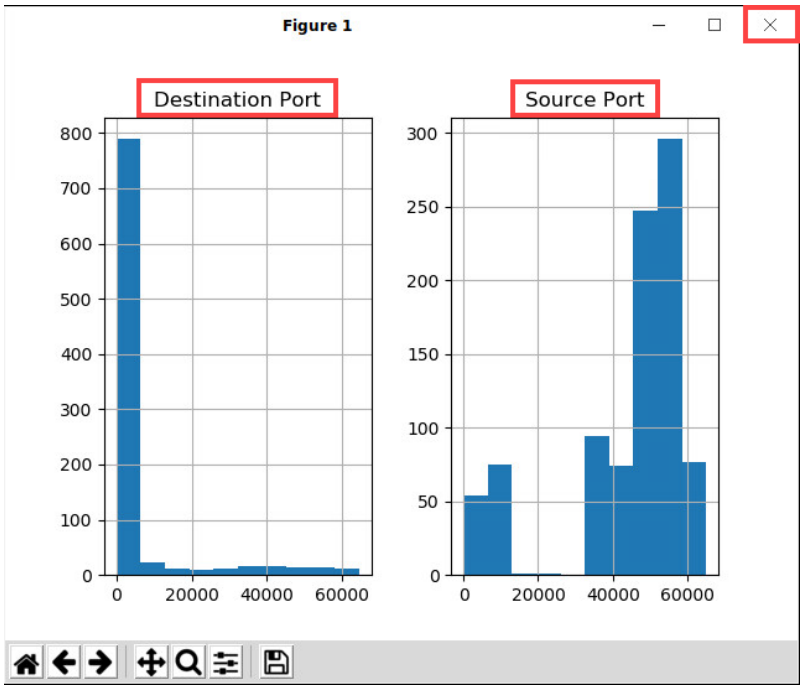


19. Execute the **ml.py** python file by typing the command below.

```
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.

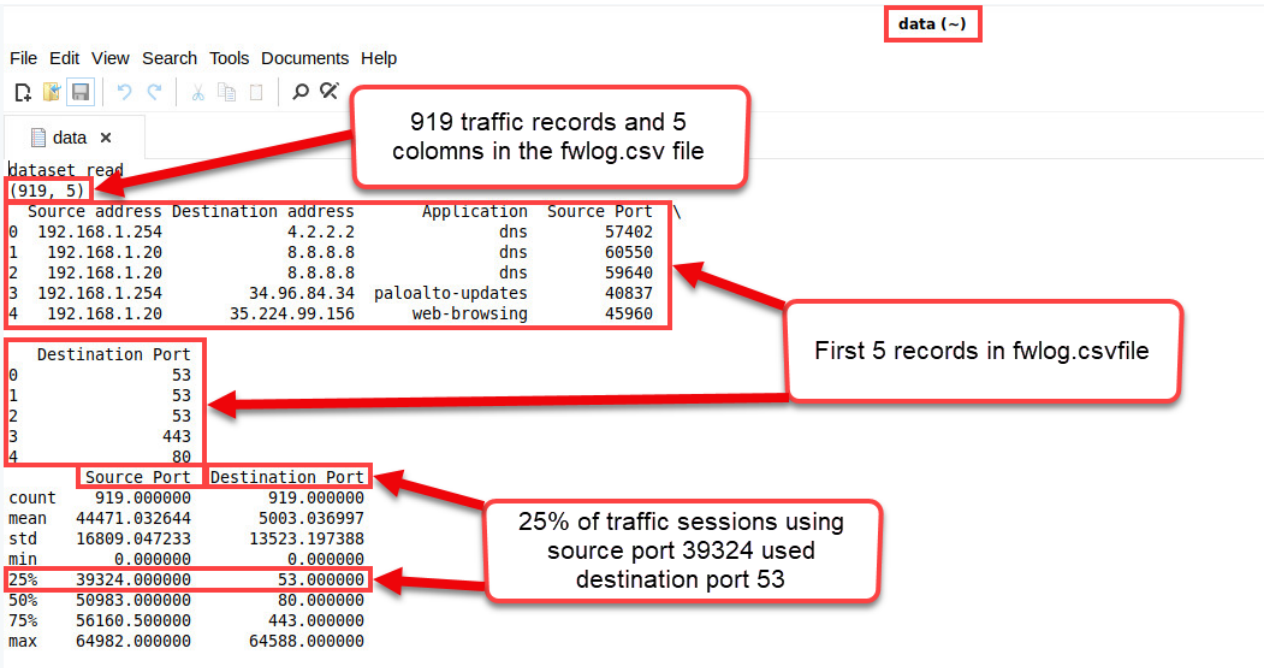


21. In the *terminal* window, open the **data** file created by typing the command below.

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

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com

22. 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
```

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

 Copyright © 2021 Network Development Group, Inc. www.netdevgroup.com