



SECURITY OPERATIONS FUNDAMENTALS

Lab 3: Analyzing Firewall Logs

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

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
3 Analyzing Firewall Logs	6
3.0 Load Lab Configuration	6
3.1 Generate Traffic to the Firewall	10
3.2 Review Traffic in the Firewall Logs	14

Introduction

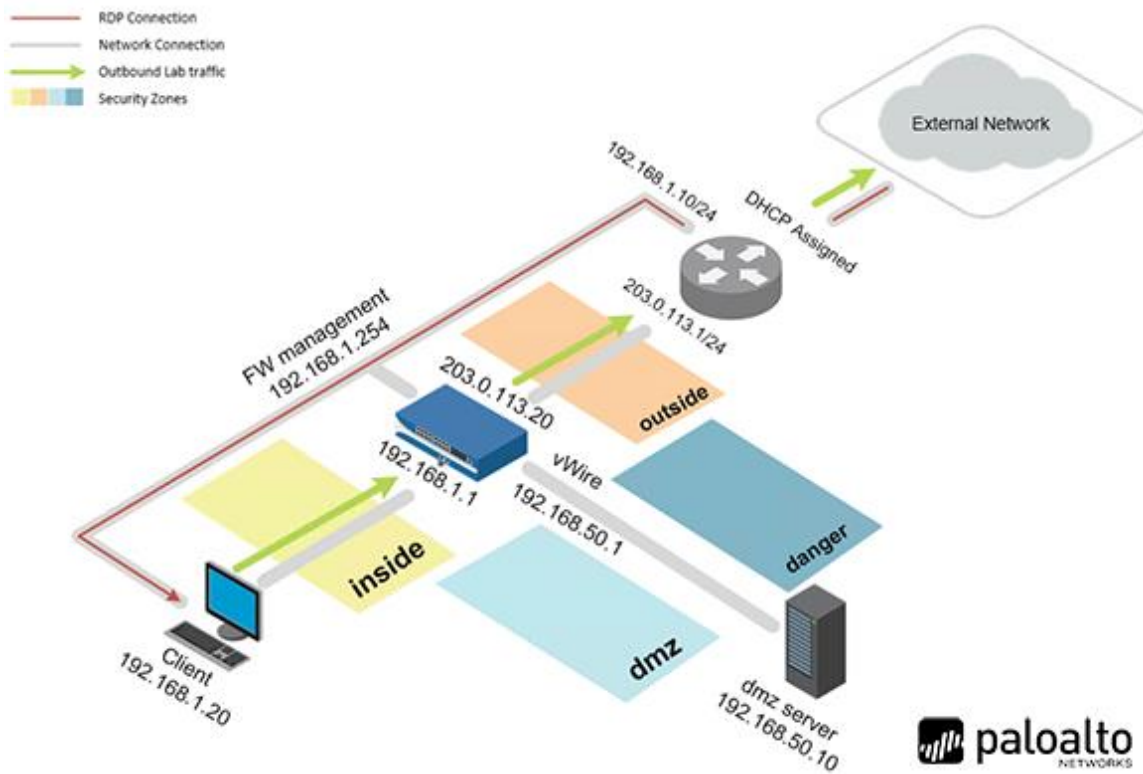
In this lab, you will generate traffic and use the Firewall logs to analyze the traffic.

Objective

In this lab, you will perform the following tasks:

- Generate Traffic to the Firewall
- Review Traffic in the Firewall Logs

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

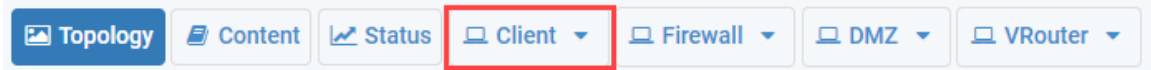
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

3 Analyzing Firewall Logs

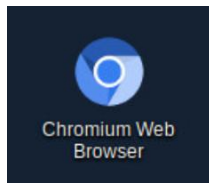
3.0 Load Lab Configuration

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

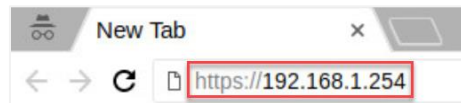
1. Click on the **Client** tab to access the client PC.



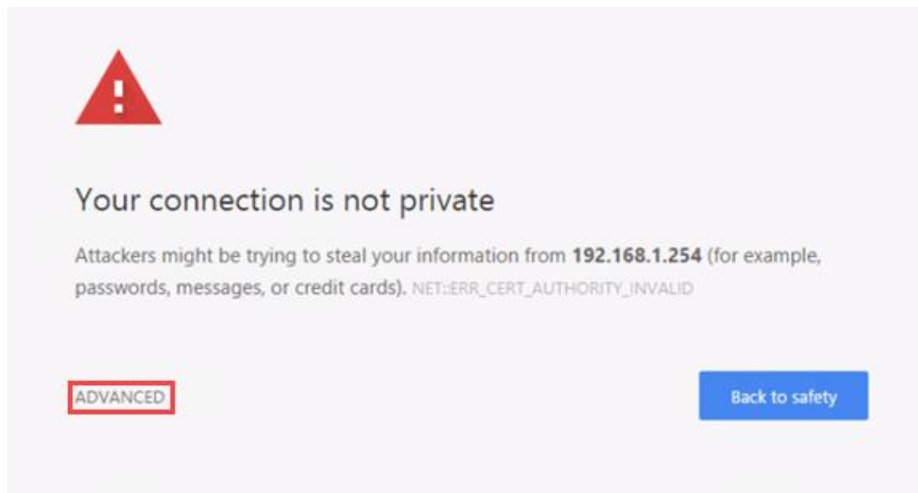
2. Log in to the client PC with the username **lab-user** and password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

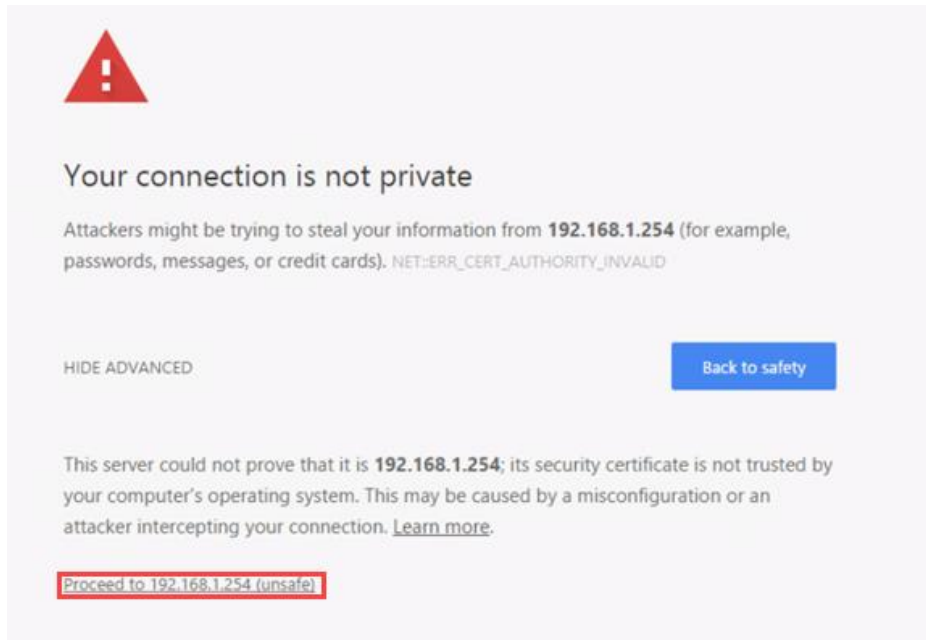


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

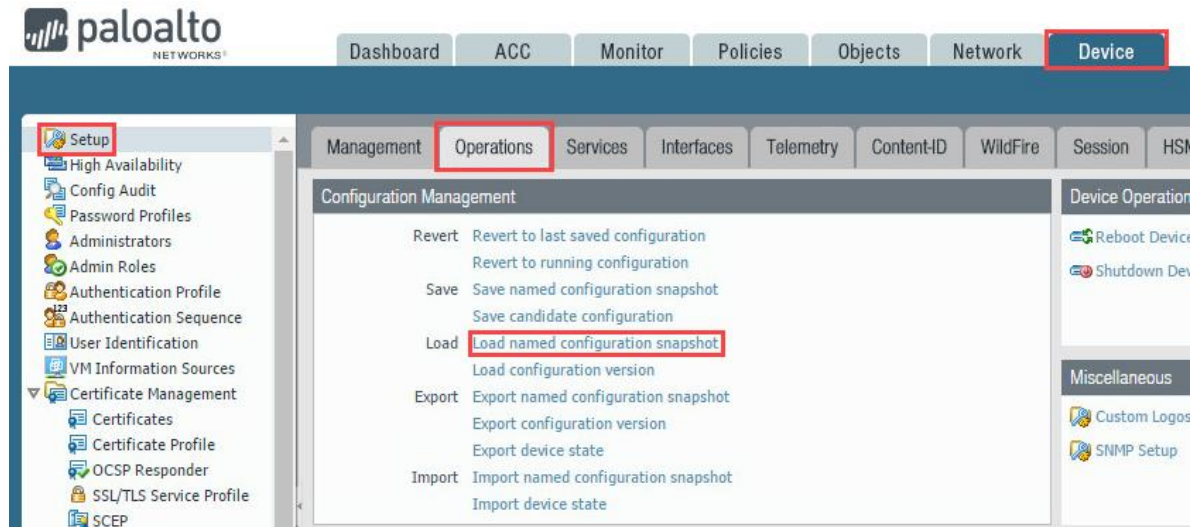
- Click on **Proceed to 192.168.1.254 (unsafe)**.



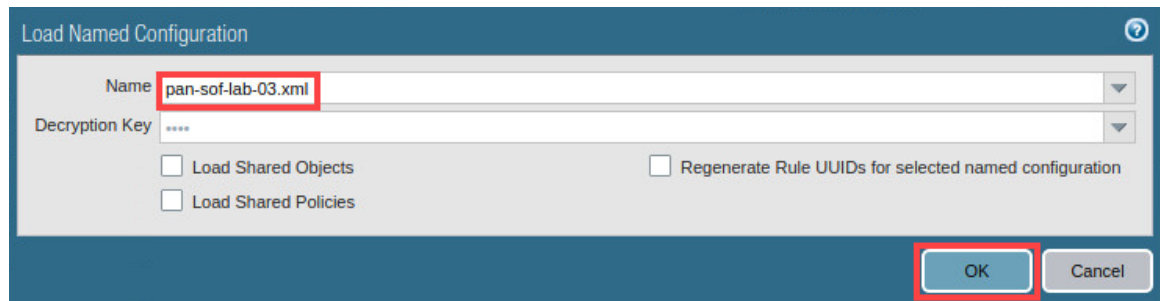
- Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



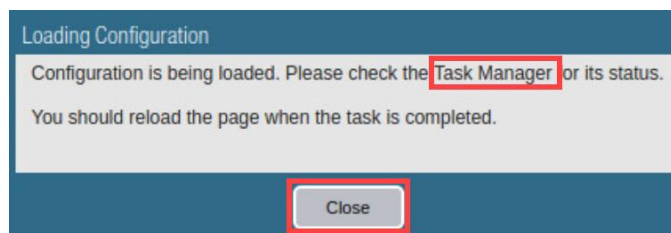
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



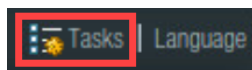
9. In the *Load Named Configuration* window, select **pan-sof-lab-03.xml** from the *Name* drop-down box and click **OK**.



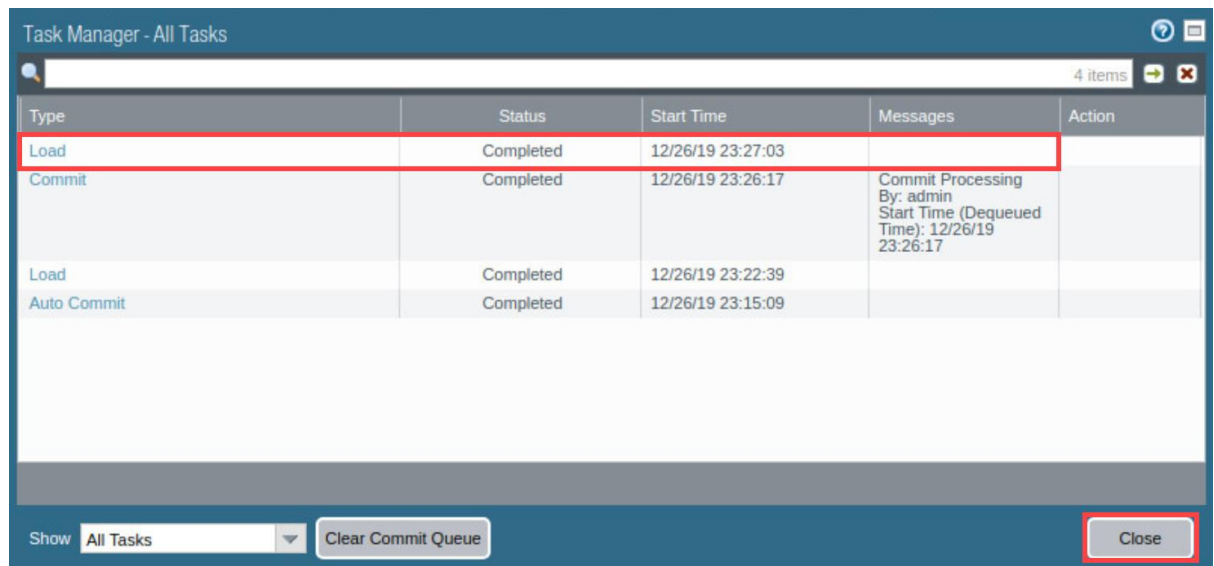
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



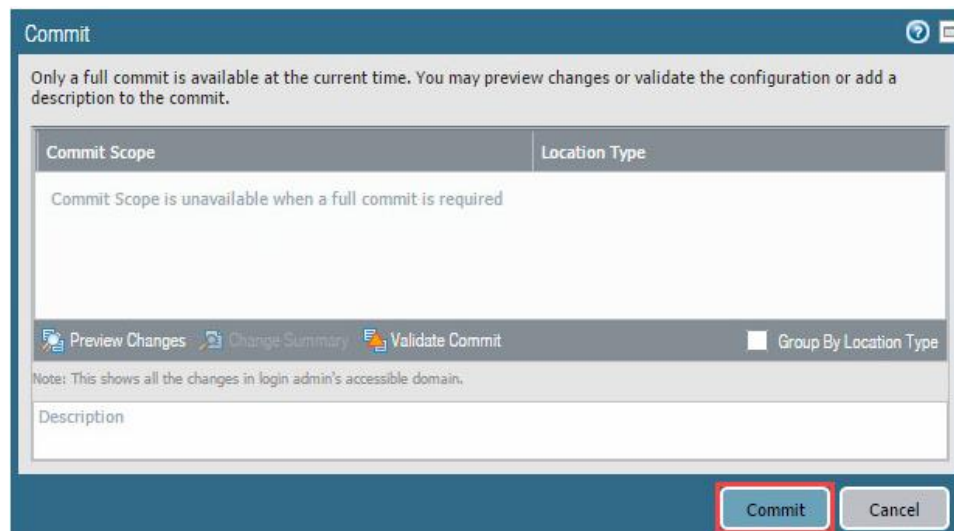
12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.



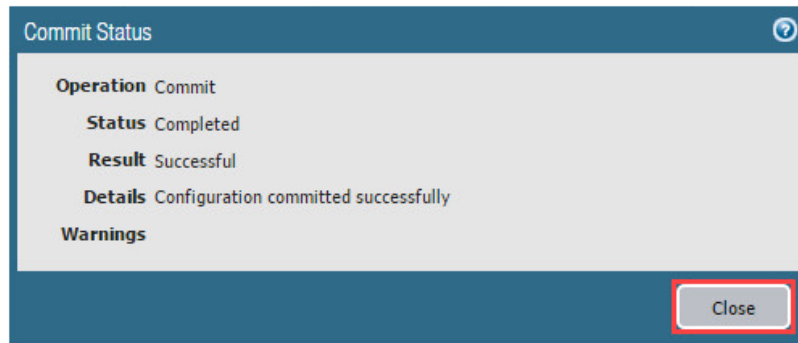
13. Click the **Commit** link located at the top-right of the web interface.



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



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

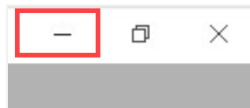


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

3.1 Generate Traffic to the Firewall

In this section, you will generate traffic to the Firewall using a script that is replaying previously-captured traffic.

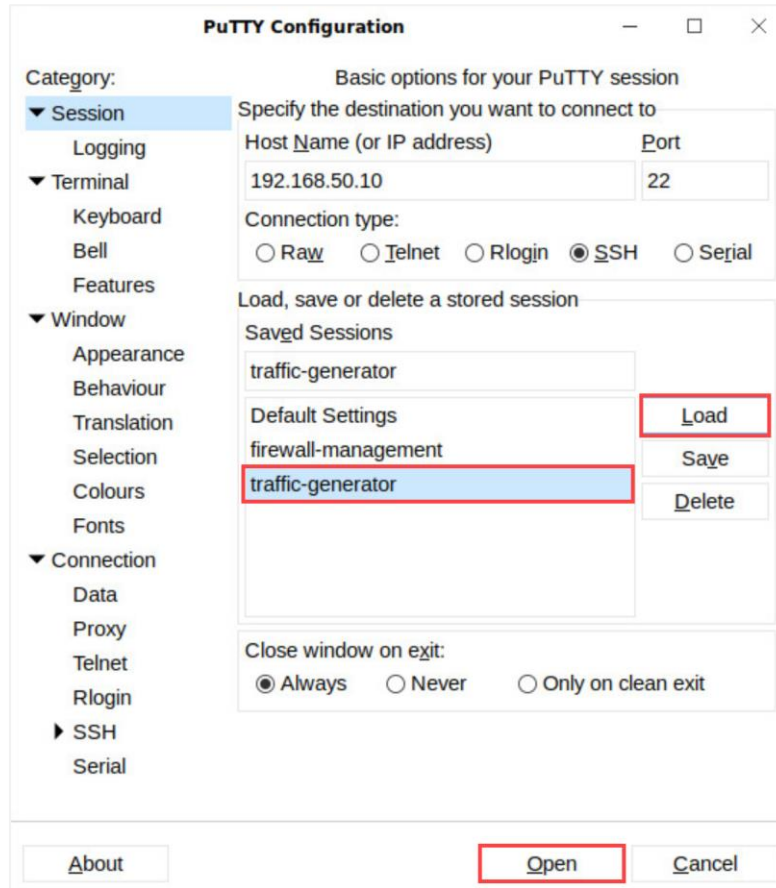
1. Minimize *Chromium* in the upper-right corner.



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



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

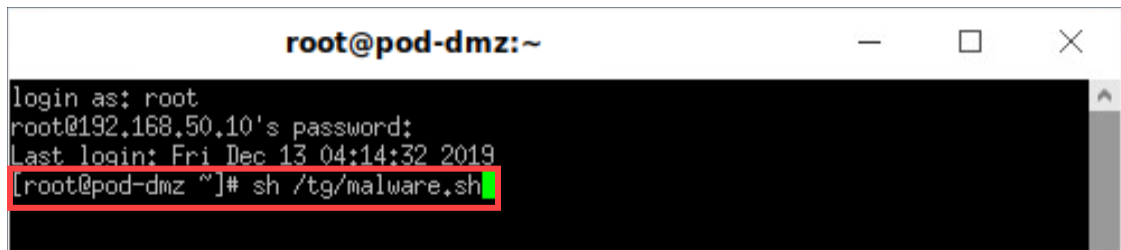


- At the *login as:* prompt, type **root**. Type **Pa10A1t0** for the password, and press **Enter**.



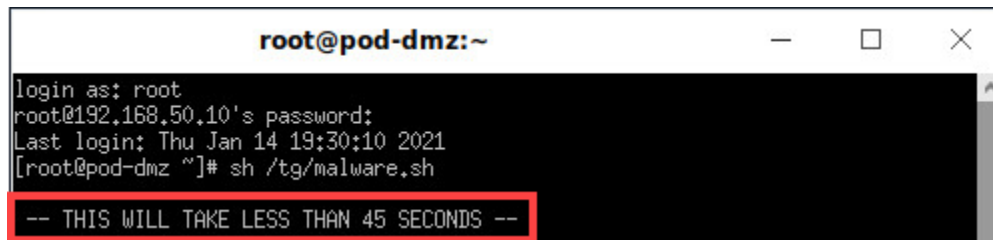
The cursor will not move while you type the password.

5. Type `sh /tg/malware.sh` and press **Enter**.



```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Fri Dec 13 04:14:32 2019  
[root@pod-dmz ~]# sh /tg/malware.sh
```

6. Allow the script to generate malware traffic. Notice it says it will take less than 45 seconds to complete. You may experience different time spans when doing this step. It is important that you allow the **malware.sh** script to finish.



```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Thu Jan 14 19:30:10 2021  
[root@pod-dmz ~]# sh /tg/malware.sh  
-- THIS WILL TAKE LESS THAN 45 SECONDS --
```

- The script will generate test malware traffic to the Firewall so that you can see malware traffic in the Firewall. You will see the following output when the script has generated the traffic.

```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Fri Dec 13 04:14:32 2019  
[root@pod-dmz ~]# sh /tg/malware.sh  
  
THIS COULD TAKE UP TO 10 MINUTES  
  
Actual: 822 packets (735581 bytes) sent in 134.03 seconds.  
Rated: 5400.0 Bps, 0.043 Mbps, 6.11 pps  
Flows: 27 flows, 0.20 fps, 822 flow packets, 0 non-flow  
Statistics for network device: ens224  
Successful packets: 822  
Failed packets: 0  
Truncated packets: 0  
Retried packets (ENOBUFFS): 0  
Retried packets (EAGAIN): 0  
Actual: 67 packets (47535 bytes) sent in 17.04 seconds.  
Rated: 2700.0 Bps, 0.021 Mbps, 3.83 pps  
Flows: 6 flows, 0.34 fps, 67 flow packets, 0 non-flow  
Statistics for network device: ens224  
Successful packets: 67  
Failed packets: 0  
Truncated packets: 0  
Retried packets (ENOBUFFS): 0  
Retried packets (EAGAIN): 0  
Actual: 372 packets (264661 bytes) sent in 0.259538 seconds.  
Rated: 1019700.0 Bps, 8.15 Mbps, 1433.31 pps  
Flows: 2 flows, 7.70 fps, 372 flow packets, 0 non-flow  
Statistics for network device: ens224  
Successful packets: 372  
Failed packets: 0  
Truncated packets: 0  
Retried packets (ENOBUFFS): 0  
Retried packets (EAGAIN): 0  
Actual: 44 packets (11666 bytes) sent in 0.118690 seconds.  
Rated: 98200.0 Bps, 0.785 Mbps, 370.71 pps  
Flows: 2 flows, 16.85 fps, 44 flow packets, 0 non-flow  
Statistics for network device: ens224  
Successful packets: 44  
Failed packets: 0  
Truncated packets: 0  
Retried packets (ENOBUFFS): 0  
Retried packets (EAGAIN): 0  
[root@pod-dmz ~]#
```

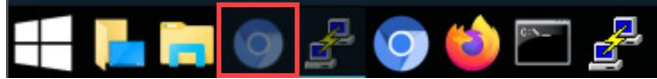


Notice that you have successfully generated malware packets by initializing the **malware.sh** file.

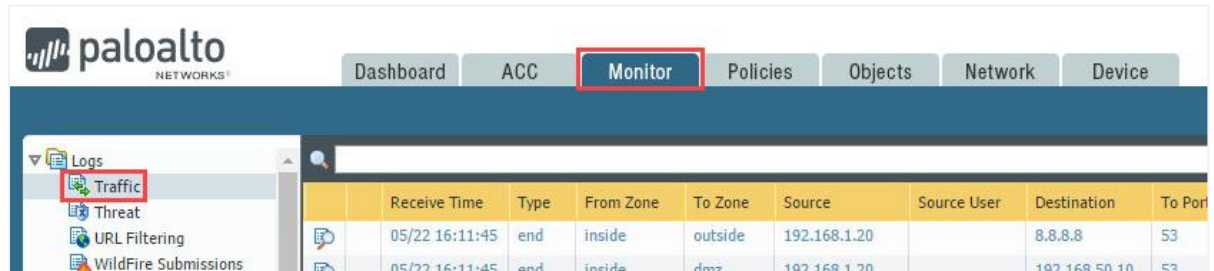
3.2 Review Traffic in the Firewall Logs

In this section, you will explore the *Traffic* logs in the Firewall.

1. Maximize *Chromium* from the taskbar.



2. Navigate to the **Monitor > Logs > Traffic**.



3. You will see traffic from the Firewall. You may need to refresh the Firewall interface for the most recent traffic by clicking the **Refresh** icon at the top-right of the web interface.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
	09/25 14:59:17	end	danger	danger	10.10.10.10		192.168.1.121	25	incomplete	allow
	09/25 14:59:11	end	danger	danger	172.16.255.1		145.120.22.109	51491	skype	allow
	09/25 14:59:11	end	danger	danger	10.0.2.15		10.0.2.3	53	dns	allow
	09/25 14:59:11	end	danger	danger	10.0.2.15		10.0.2.3	53	dns	allow
	09/25 14:59:11	end	danger	danger	172.16.255.1		67.117.28.180	56259	skype	allow
	09/25 14:59:11	end	danger	danger	172.16.255.1		69.255.24.214	24506	skype	allow
	09/25 14:58:56	end	danger	danger	172.16.255.1		95.86.252.198	6192	skype	allow
	09/25 14:58:56	end	danger	danger	192.168.3.131		65.54.95.75	80	web-browsing	allow
	09/25 14:58:56	end	danger	danger	10.0.2.15		10.0.2.3	53	dns	allow
	09/25 14:58:56	end	danger	danger	10.0.2.15		64.4.9.254	61863	insufficient-data	allow
	09/25 14:58:56	end	danger	danger	192.168.3.131		208.82.236.129	80	web-browsing	allow
	09/25 14:58:45	end	danger	danger	172.16.255.1		75.76.39.18	35877	skype	allow
	09/25 14:58:44	end	danger	danger	10.0.2.15		10.0.2.255	138	netbios-dg	allow
	09/25 14:58:44	end	danger	danger	172.16.255.1		172.16.255.255	137	netbios-ns	allow
	09/25 14:58:41	end	danger	danger	192.168.3.131		65.54.95.75	80	web-browsing	allow
	09/25 14:58:41	end	danger	danger	192.168.3.131		65.54.95.140	80	web-browsing	allow
	09/25 14:58:41	end	danger	danger	10.0.2.15		64.4.9.254	1863	insufficient-data	allow

- Look under the *Application* column and find traffic that is categorized as **web-browsing**. You may need to select the next page in the lower-left.

09/25 15:00:54	end	danger	danger	192.168.3.131	66.235.133.62	80	incomplete	allow
09/25 15:00:39	end	danger	danger	192.168.3.131	65.54.95.68	80	web-browsing	allow
09/25 15:00:39	end	danger	danger	192.168.3.131	65.54.95.140	80	web-browsing	allow

Report Groups 12 3 4 5 6 7 8 9 10 Resolve hostname Highlight Policy Actions

admin | Logout | Last Login Time: 05/21/2018 21:06:49

- Click on the **Magnifying Glass** icon on the left to view the traffic.

05/22 16:12:44	end	danger	danger	192.168.0.2	112.137.162...	80	web-browsing
----------------	-----	--------	--------	-------------	----------------	----	--------------



Due to the nature of the lab environment, you may get different results depending on the traffic log you choose.

- Review the *Detailed Log View* window.

Detailed Log View

General

Session ID 542

Action allow

Action Source from-policy

Application web-browsing

Rule Allow-Any

Rule UUID 70b46624-c194-409a-819c-7d9c3fba47f

Session End Reason tcp-fin

Category computer-and-internet-info

Device SN

IP Protocol tcp

Source

Source User

Source 192.168.1.20

Country 192.168.0.0-192.168.255.255

Port 34938

Zone inside

Interface ethernet1/2

NAT IP 203.0.113.20

NAT Port 45708

Destination

Destination User

Destination 35.222.85.5

Country United States

Port 80

Zone outside

Interface ethernet1/1

NAT IP 35.222.85.5

NAT Port 80

Flags

Captive Portal ☐

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ...	Verdict	URL	File Name
	2019/12/30 22:24:52	end	web-browsing	allow	Allow-Any	70b46...	911		comp... and-internet-info				

Close

7. You can see the details of the **Source** and **Destination**.

Detailed Log View

General	Source	Destination
Session ID 542	Source User	Destination User
Action allow	Source 192.168.1.20	Destination 35.222.85.5
Action Source from-policy	Country 192.168.0.0-192.168.255.255	Country United States
Application web-browsing	Port 34938	Port 80
Rule Allow-Any	Zone inside	Zone outside
70b46624-c194-409a-819c-7d9c3fba47f	Interface ethernet1/2	Interface ethernet1/1
Rule UUID	NAT IP 203.0.113.20	NAT IP 35.222.85.5
Session End Reason tcp-fin	NAT Port 45708	NAT Port 80
Category computer-and-internet-info		
Device SN		
IP Protocol tcp		

Flags

Captive Portal ☐

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/12/30 22:24:52	end	web-browsing	allow	Allow-Any	70b46...	911		comp... and-internet-info				

Close

8. You can see the **Application** and **Category** in the *General* section.

Detailed Log View

General	Source	Destination
Session ID 542	Source User	Destination User
Action allow	Source 192.168.1.20	Destination 35.222.85.5
Action Source from-policy	Country 192.168.0.0-192.168.255.255	Country United States
Application web-browsing	Port 34938	Port 80
Rule Allow-Any	Zone inside	Zone outside
70b46624-c194-409a-819c-7d9c3fba47f	Interface ethernet1/2	Interface ethernet1/1
Rule UUID	NAT IP 203.0.113.20	NAT IP 35.222.85.5
Session End Reason tcp-fin	NAT Port 45708	NAT Port 80
Category computer-and-internet-info		
Device SN		
IP Protocol tcp		

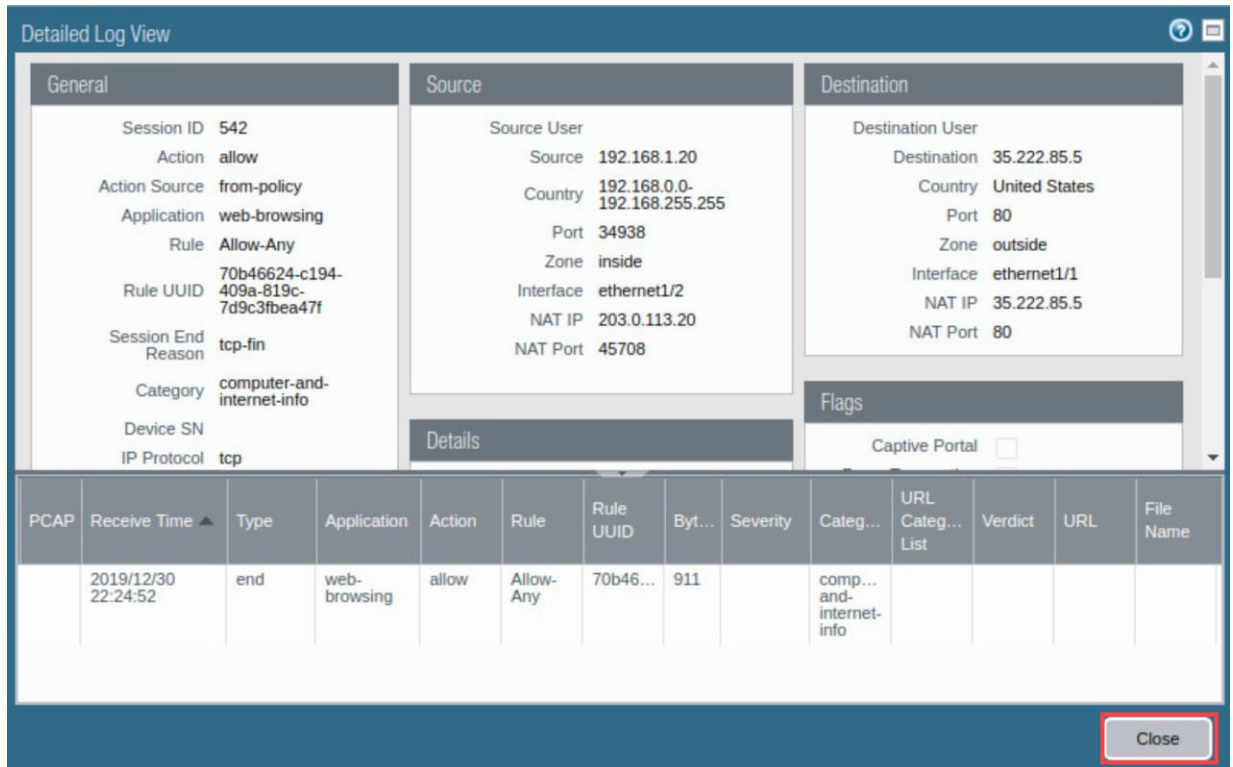
Flags

Captive Portal ☐

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/12/30 22:24:52	end	web-browsing	allow	Allow-Any	70b46...	911		comp... and-internet-info				

Close

9. Click **Close** on the *Detailed Log View* window.



The screenshot shows the 'Detailed Log View' window with the following details:

General		Source		Destination	
Session ID	542	Source User		Destination User	
Action	allow	Source	192.168.1.20	Destination	35.222.85.5
Action Source	from-policy	Country	192.168.0.0-192.168.255.255	Country	United States
Application	web-browsing	Port	34938	Port	80
Rule	Allow-Any	Zone	inside	Zone	outside
Rule UUID	70b46624-c194-409a-819c-7d9c3fba47f	Interface	ethernet1/2	Interface	ethernet1/1
Session End Reason	tcp-fin	NAT IP	203.0.113.20	NAT IP	35.222.85.5
Category	computer-and-internet-info	NAT Port	45708	NAT Port	80
Device SN					
IP Protocol	tcp				

Below the details is a table with the following columns: PCAP, Receive Time, Type, Application, Action, Rule, Rule UUID, Byt..., Severity, Categ..., URL Categ..., Verdict, URL, File Name.

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ...	Verdict	URL	File Name
	2019/12/30 22:24:52	end	web-browsing	allow	Allow-Any	70b46...	911		comp... and-internet-info				

A 'Close' button is located at the bottom right of the window.

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