



SECURITY OPERATIONS FUNDAMENTALS V2

Lab 3: Analyzing Firewall Logs

Document Version: **2022-12-23**

Copyright © 2022 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
1 Analyzing Firewall Logs	6
1.0 Load Lab Configuration	6
1.1 Generate Traffic to the Firewall	11
1.2 Review Traffic in the Firewall Logs	14

Introduction

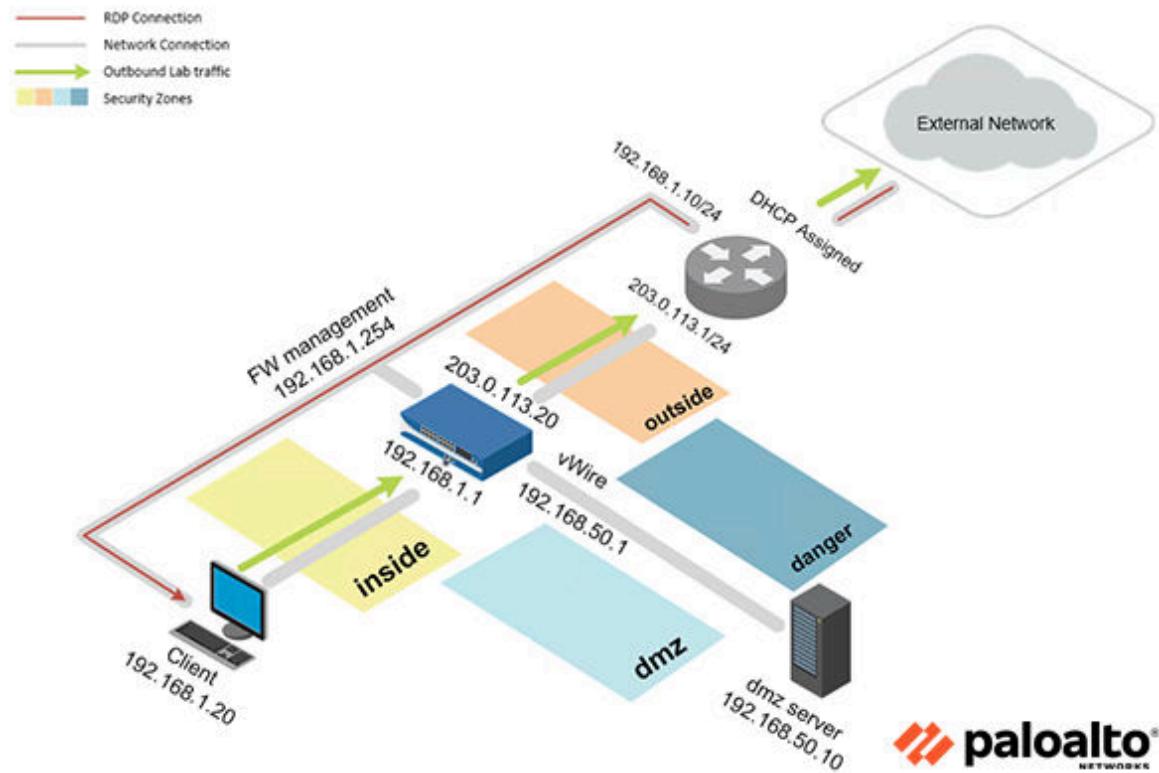
In this lab, you will generate traffic and use the Firewall logs to analyze the traffic.

Objective

In this lab, you will perform the following tasks:

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

Lab Topology

paloalto
NETWORKS

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 Analyzing Firewall Logs

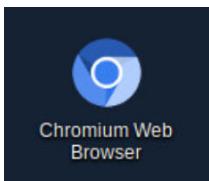
1.0 Load Lab Configuration

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

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



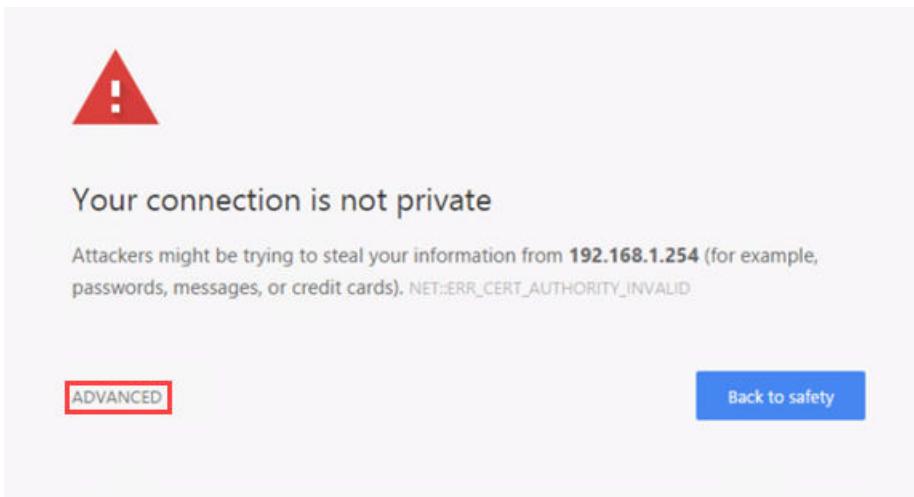
2. Log in to the client PC with the username `lab-user` and password `PaloAlt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

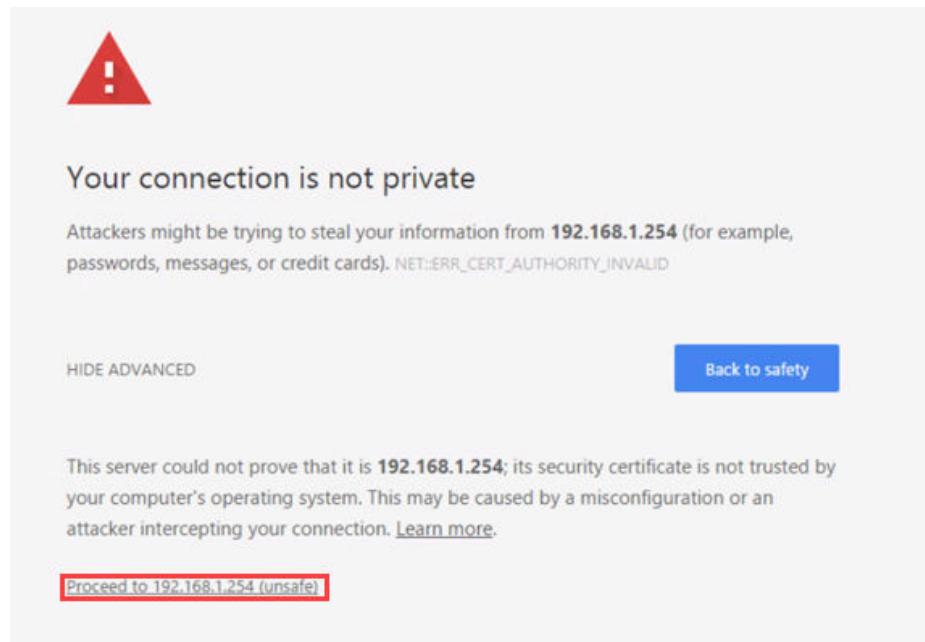


5. You will see a “*Your connection is not private*” message. Click on the **ADVANCED** link.



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.

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



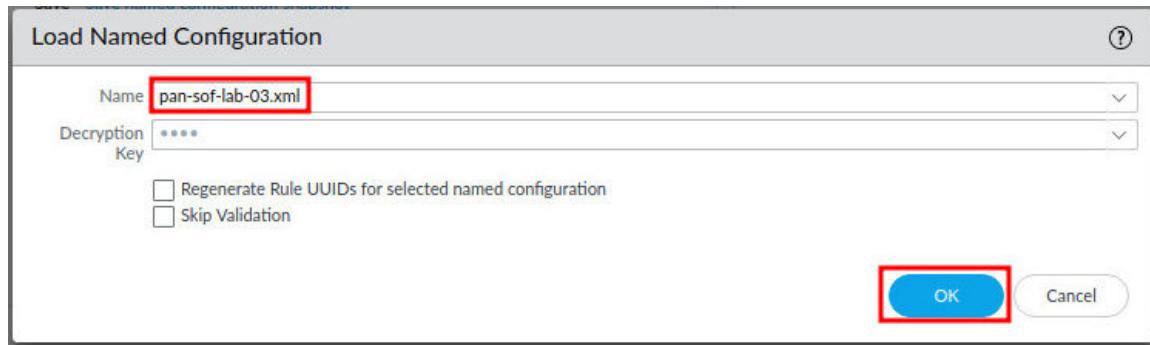
7. Log in to the Firewall web interface as username **admin**, password **PaloAlto!**.



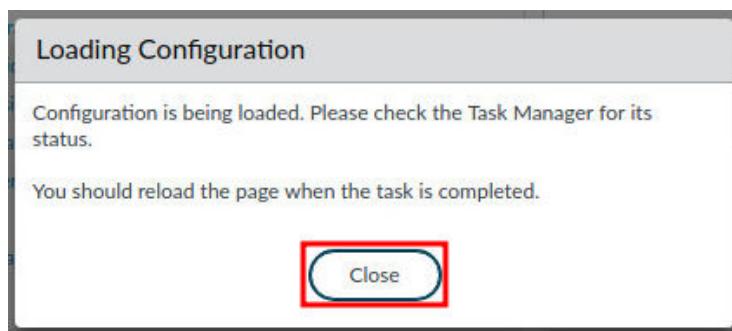
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is selected. On the left, a sidebar menu under the 'Setup' heading lists various configuration options like High Availability, Config Audit, and Certificate Management. The main content area is titled 'Configuration Management' and contains several sub-options: Revert, Save, Load, Export, and Import. The 'Load' option, which is 'Load named configuration snapshot', is highlighted with a red box. To the right, there are sections for 'Device Operations' (Reboot Device, Shutdown) and 'Miscellaneous' (Custom Log, SNMP Set).

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



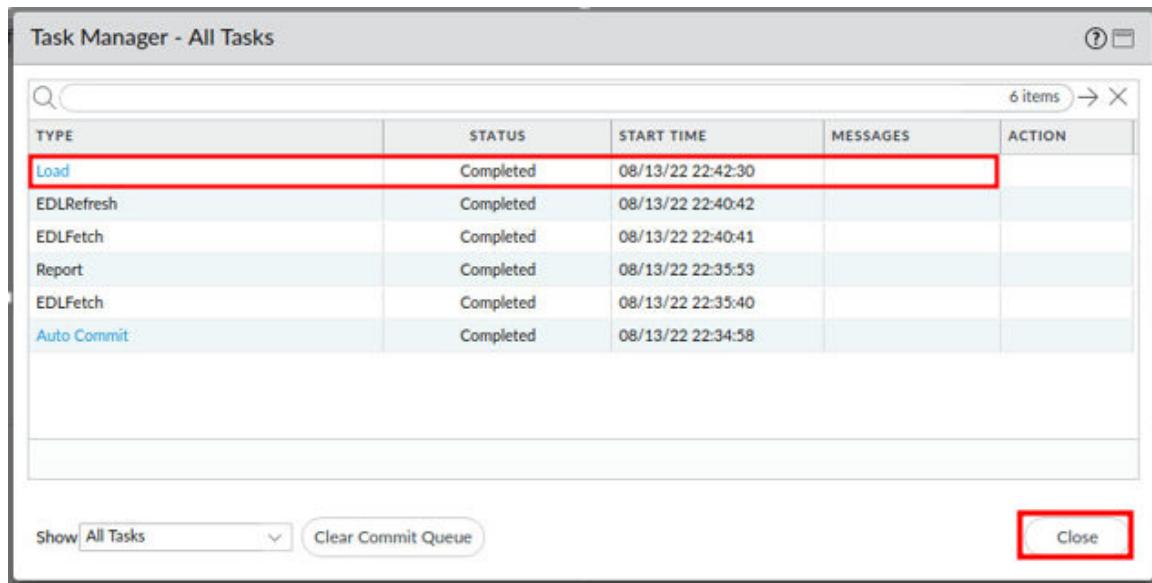
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

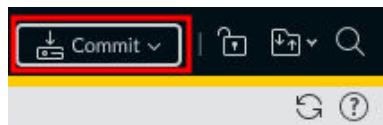


12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.

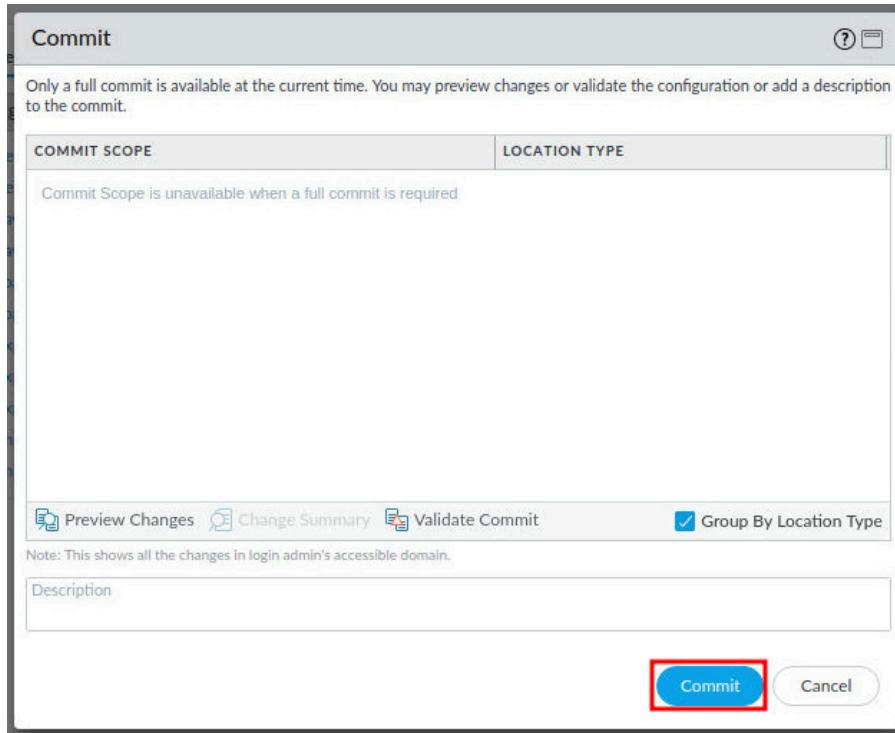


TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

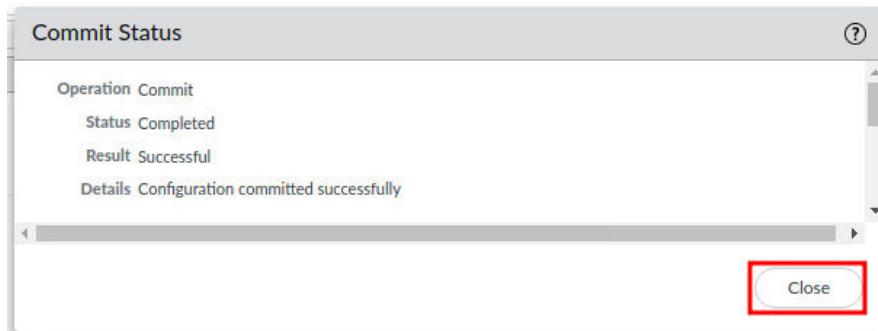
13. Click the **Commit** link located at the top-right of the web interface.



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



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

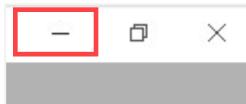


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

1.1 Generate Traffic to the Firewall

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

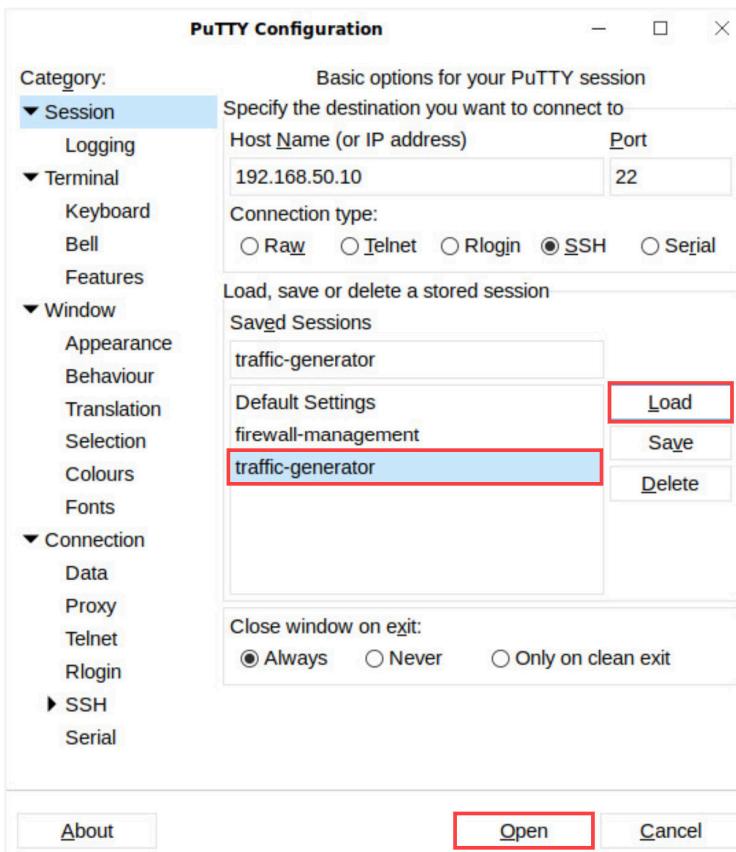
1. Minimize *Chromium* in the upper-right corner.



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



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



4. At the *login as:* prompt, type **root**. Type **PaloAlt0!** for the password, and press **Enter**.



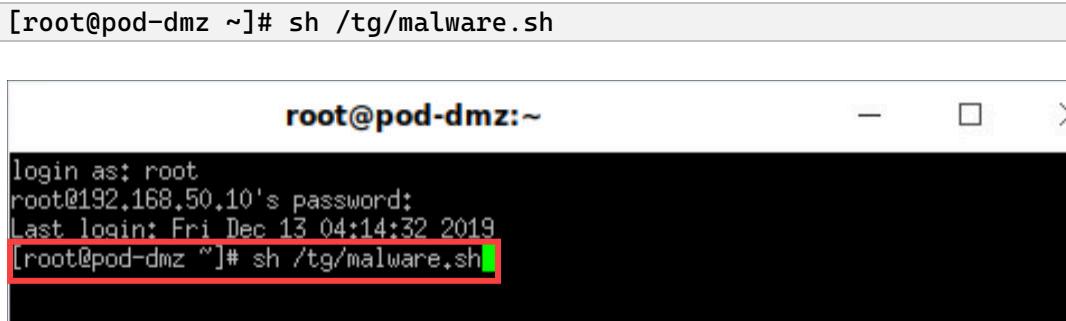
192.168.50.10 - PuTTY

```
login as: root
root@192.168.50.10's password: █
```



The cursor will not move while you type the password.

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



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

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 --
```

7. 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 (ENOBUFS): 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 (ENOBUFS): 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 (ENOBUFS): 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 (ENOBUFS): 0  
Retried packets (EAGAIN): 0  
[root@pod-dmz ~]#
```

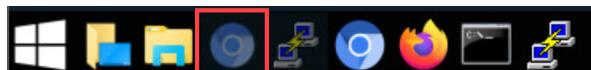


Notice that you have successfully generated malware packets by initializing the **malware.sh** file.

1.2 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. For easier navigation, you may remove columns by clicking on the drop-down arrow next to a column header, then **Columns**. Uncheck selections like **Source User**, **Source Dynamic Address Group**, **Destination Dynamic Address Group**, and **Dynamic User Group**, watch the columns dynamically disappear, then press **Esc** key to clear the popup box.

	SESSION END REASON
Any	aged-out
Any	Session End Reason

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

	09/25 20:31:42	end	inside	outside	192.168.1.20	35.224.170.84	80	web-browsing	allow
	1 2 3 4 5 6 7 8 9 10	▶	<input type="checkbox"/> Resolve hostname	<input type="checkbox"/> Highlight Policy Actions	<input type="checkbox"/> Test Policy Match	▼			



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

5. Review the *Detailed Log View* window.

Detailed Log View													
General				Source					Destination				
Session ID	273	Source User		Destination User					Destination DAG				
Action	allow	Source	192.168.1.20	Country	192.168.0.0-192.168.255.255	Port	42222	NAT IP	35.224.170.84	Country	United States		
Action Source	from-policy	Source DAG		Zone	inside	Zone	outside	NAT Port	80	Interface	ethernet1/1		
Host ID		Interface	ethernet1/2	Interface				NAT IP	35.224.170.84				
Application	web-browsing	NAT IP	203.0.113.20	NAT Port	6247			NAT Port	80				
Rule	Allow-Any												
Rule UUID	2fb482dd-0ee7-48f1-beb5-8d965998937e												
Session End Reason	tcp-fin												
Category	computer-and-internet-info												
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/09/25 20:31:42	end	web-browsing	allow	Allow-Any	2fb482... 911			compu... and-internet-info				

Close

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

Detailed Log View													
General				Source					Destination				
Session ID	273	Source User		Destination User					Destination	35.224.170.84			
Action	allow	Source	192.168.1.20	Destination DAG					Country	United States			
Action Source	from-policy	Source DAG		Port	80				Zone	outside			
Host ID		Country	192.168.0.0-192.168.255.255	Interface	ethernet1/1				Interface	ethernet1/1			
Application	web-browsing	Port	42222	NAT IP	203.0.113.20				NAT IP	35.224.170.84			
Rule	Allow-Any	Zone	inside	NAT Port	6247				NAT Port	80			
Rule UUID	2fb482dd-0ee7-48f1-beb5-8d965998937e	Interface	ethernet1/2										
Session End Reason	tcp-fin	NAT IP											
Category	computer-and-internet-info	NAT Port											
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/09/25 20:31:42	end	web-browsing	allow	Allow-Any	2fb482...	911		compu... and-internet-info				

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

Detailed Log View													
General				Source					Destination				
Session ID	273	Source User		Destination User					Country	United States			
Action	allow	Source	192.168.1.20	Destination DAG					Port	80			
Action Source	from-policy	Source DAG		Port	42222				Zone	outside			
Host ID		Country	192.168.0.0-192.168.255.255	Interface	ethernet1/2				Interface	ethernet1/1			
Application	web-browsing	Port	42222	NAT IP	203.0.113.20				NAT IP	35.224.170.84			
Rule	Allow-Any	Zone	inside	NAT Port	6247				NAT Port	80			
Rule UUID	2fb482dd-0ee7-48f1-beb5-8d965998937e	Interface	ethernet1/1										
Session End Reason	tcp-fin	NAT IP											
Category	computer-and-internet-info	NAT Port											
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/09/25 20:31:42	end	web-browsing	allow	Allow-Any	2fb482...	911		compu... and-internet-info				

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