SECURITY OPERATIONS FUNDAMENTALS V2

Lab 2: Using the Application Command Center (ACC) to Find Threats

Document Version: 2022-12-23

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
1 Using the Application Command Center to find Threats 6
1.0 Load Lab Configuration 6
1.1 Generate Malware Traffic to the Firewall 11
1.2 Find Malware Threat in the Application Command Center 14

Introduction

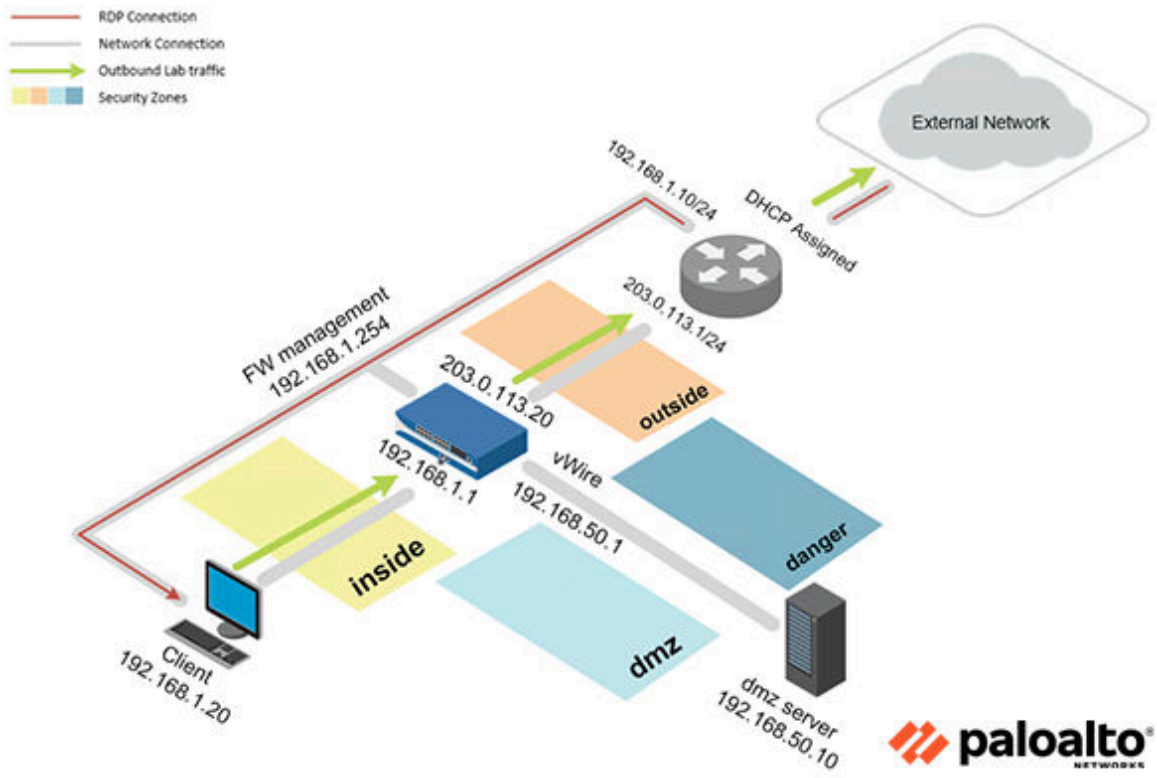
In this lab, you will generate malware traffic and use the Application Command Center to find the threat.

Objective

In this lab, you will perform the following tasks:

- Generate Malware Traffic to the Firewall
- Find Malware Threat in the Application Command Center

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.

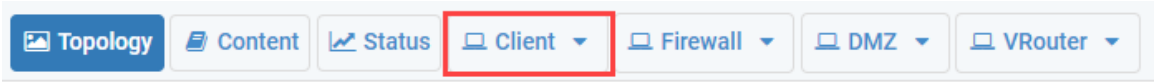
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Using the Application Command Center to find Threats

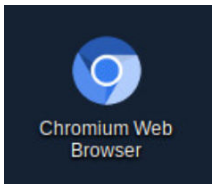
1.0 Load Lab Configuration

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

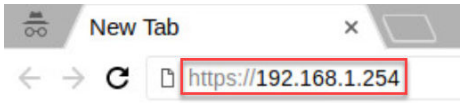
1. Click on the **Client** tab to access the client PC.



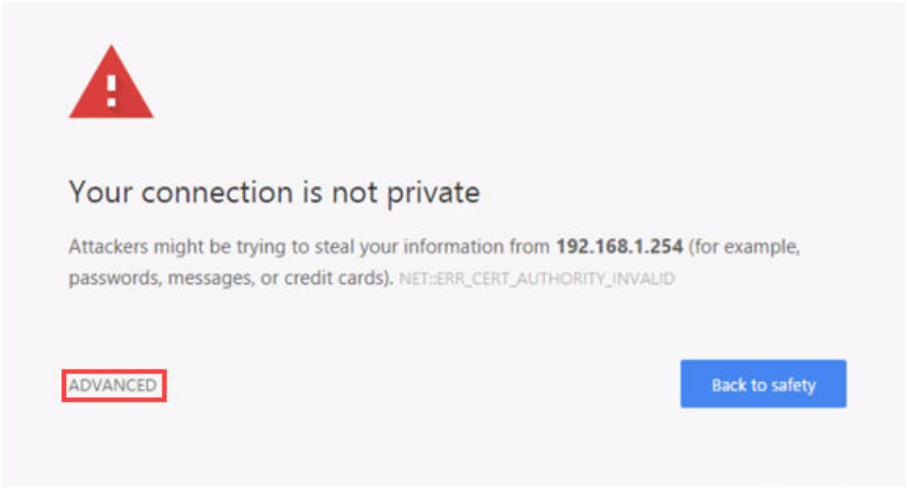
2. Log in to the client PC with the username `lab-user` and password `Pal0Alt0!`.
3. Double-click the **Chromium** icon located on the desktop.



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

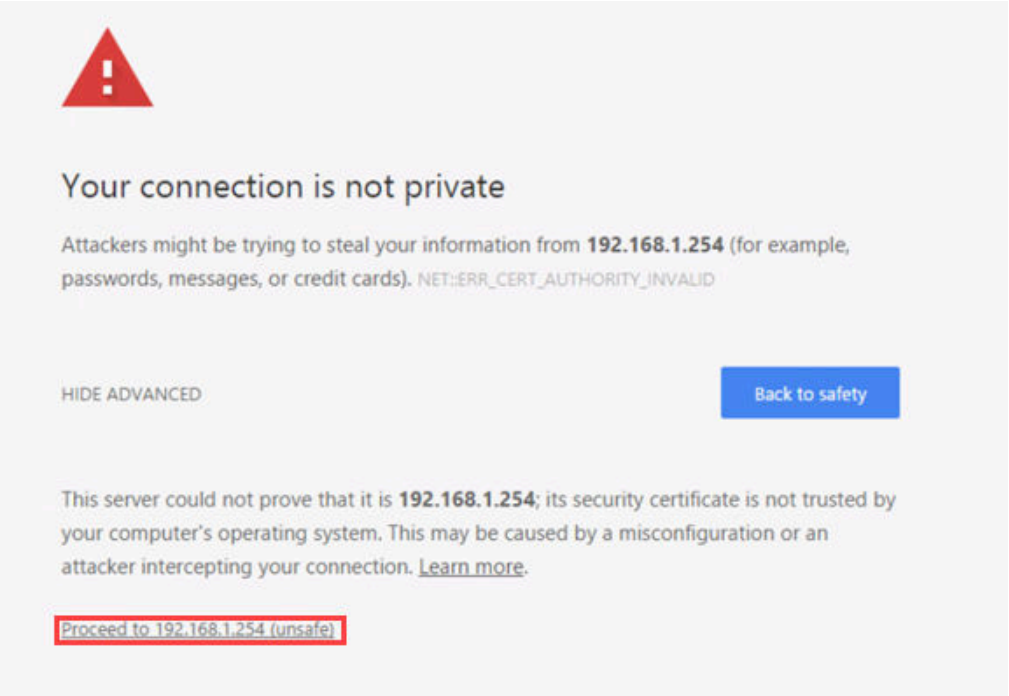


5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



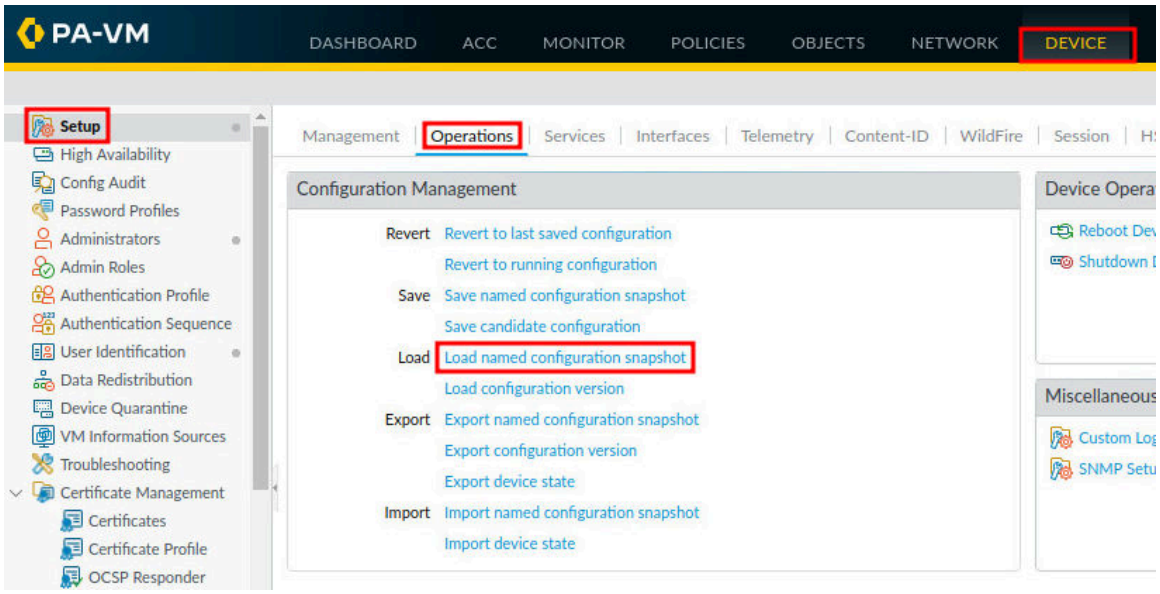
If you encounter the *"Unable to connect"* or *"502 Bad Gateway"* message while attempting to connect to the IP specified above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

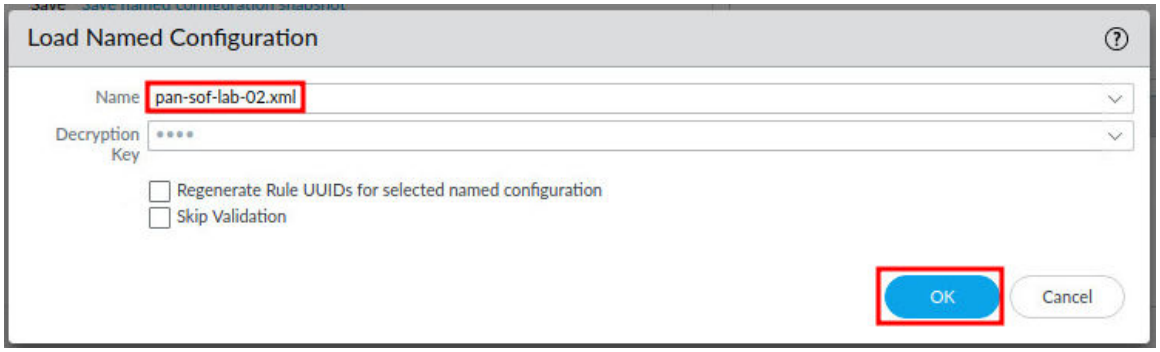


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

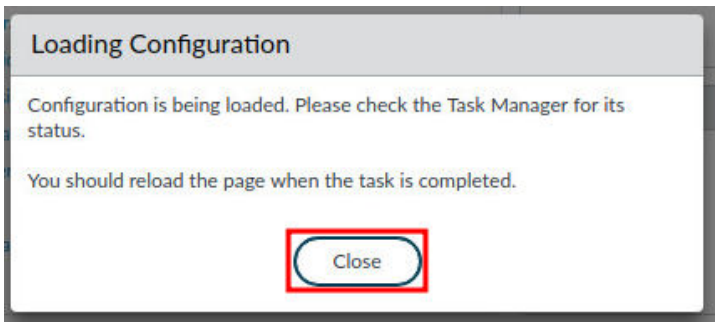
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-sof-lab-02.xml** from the *Name* dropdown box and click **OK**.

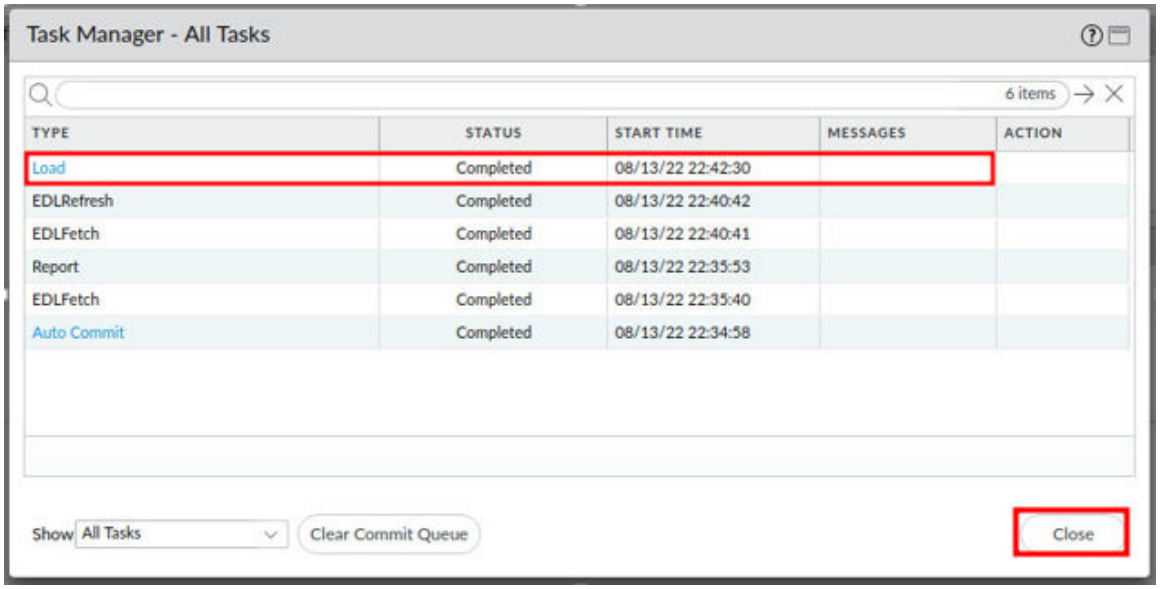


10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

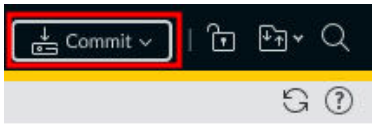


11. Click the **Tasks** icon located at the bottom-right of the web interface.

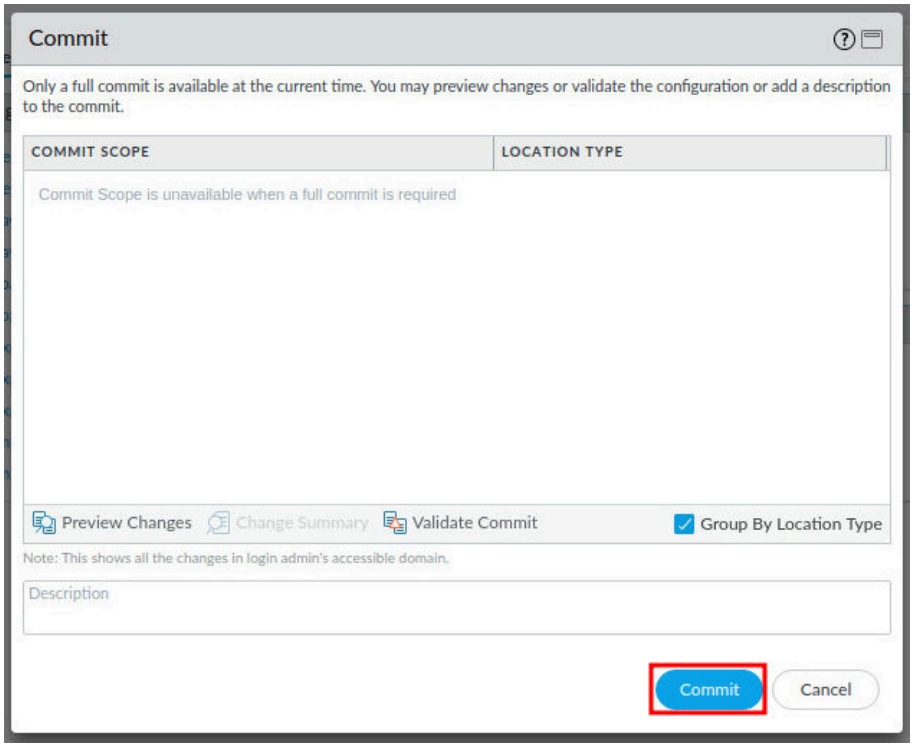
12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.



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.



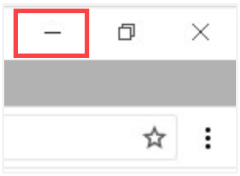
15. When the commit operation successfully completes, click **Close** to continue.

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.

1.1 Generate Malware Traffic to the Firewall

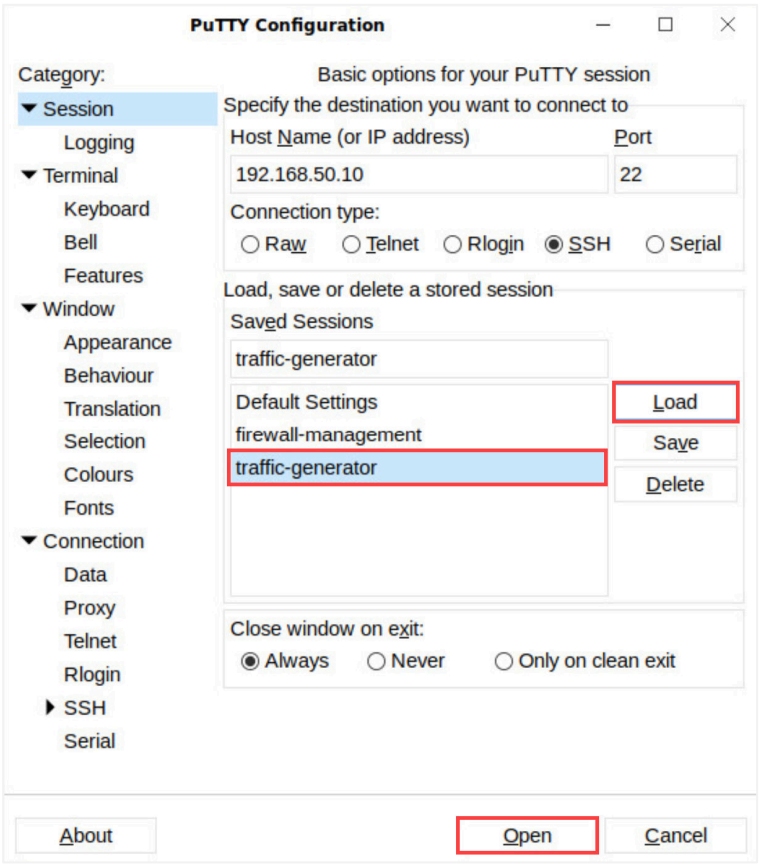
In this section, you will generate malware traffic to the Firewall using a script that is replaying previously-captured traffic.

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



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

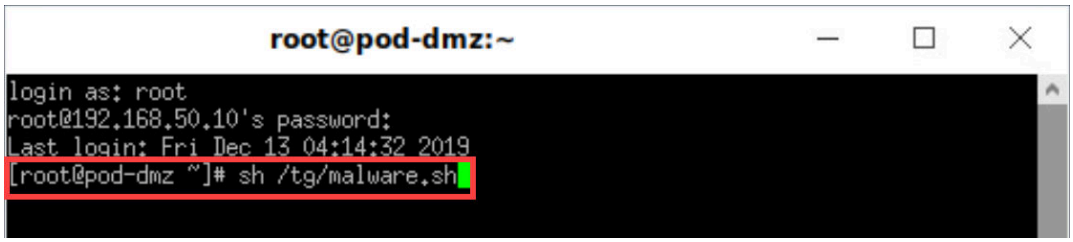


4. At the *login as:* prompt, type `root`. Type `Pal0Alt0!` for the password, and press **Enter**.

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

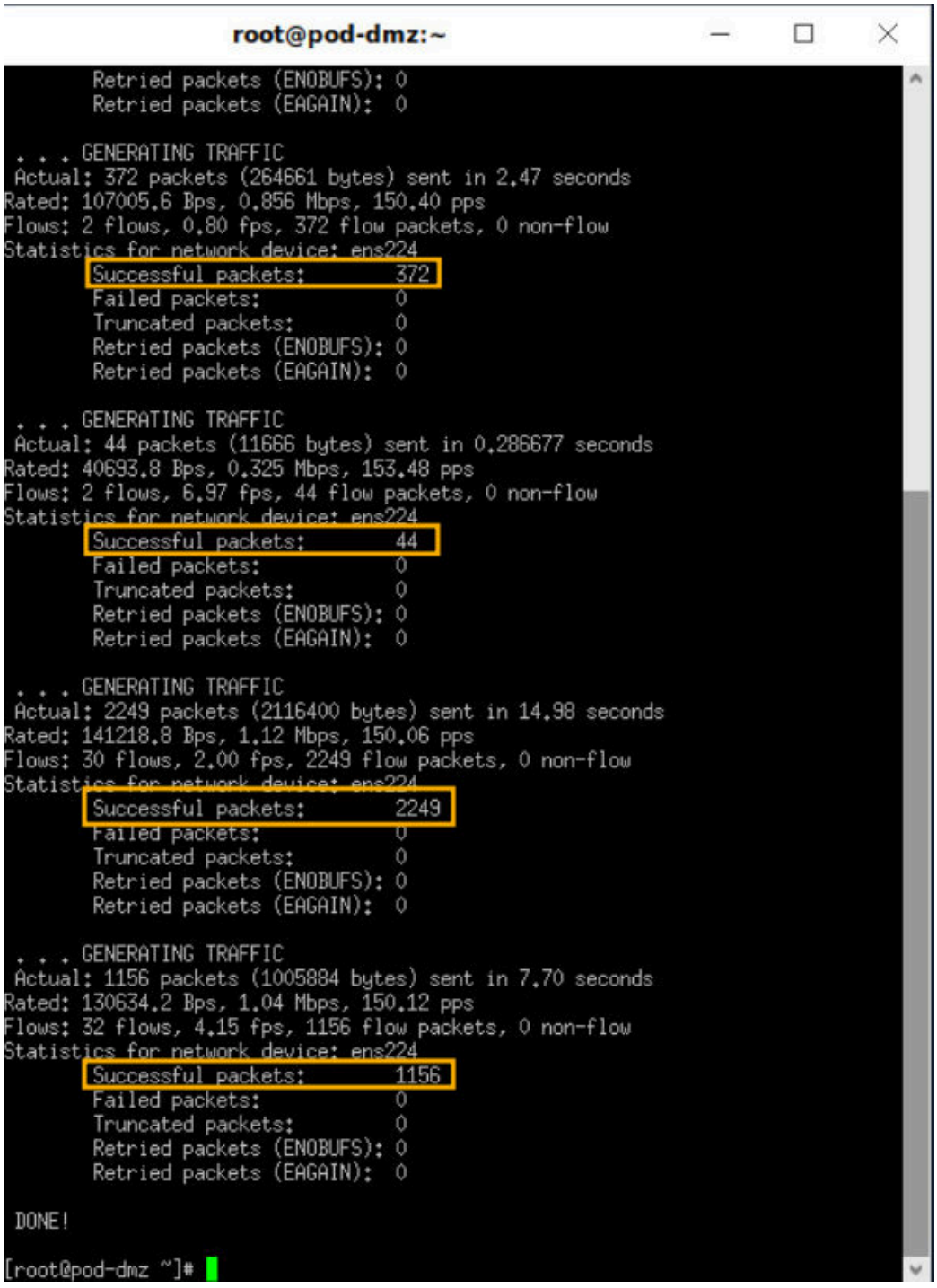
5. Type `sh /tg/malware.sh` and press **Enter**.

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



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.

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.

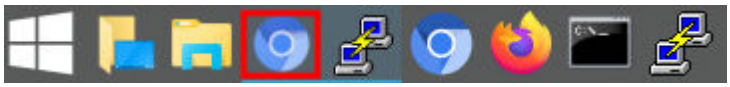


Notice that you have successfully generated malware packets by initializing the **malware.sh** file.

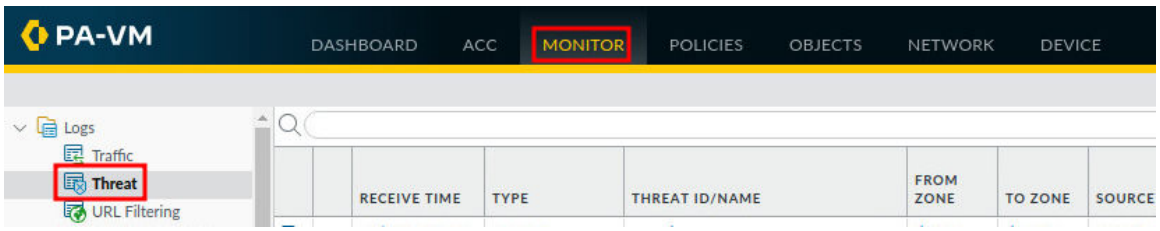
1.2 Find Malware Threat in the Application Command Center

In this section, you will review **Threat Activity** and **Blocked Activity** in the *Application Command Center*.

1. Maximize *Chromium* from the taskbar.



2. Navigate to **MONITOR > Logs > Threat**



3. Look for an entry where the column **THREAT ID/NAME** includes threats such as **Bredolab.Gen Command and Control Traffic**.

RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS
10/30 18:19:02	spyware	generic:evastrutzmann.at	danger	danger	10.12.1.1
10/30 18:18:44	spyware	Bredolab.Gen Command and Control Traffic	danger	danger	192.168.0.2
10/30 18:14:57	spyware	generic:tischlerei-kreiner.at	danger	danger	10.12.1.101
10/30 18:14:57	spyware	generic:entryinformation.info	danger	danger	10.12.1.1
10/30 18:14:57	spyware	generic:domtablesthemultihdis.info	danger	danger	10.12.1.1
10/30 18:14:50	spyware	generic:evastrutzmann.at	danger	danger	10.12.1.101

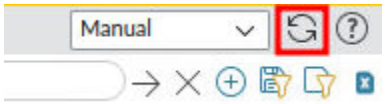
4. If you do not see the **Bredolab.Gen Command and Control Traffic** entry, you can re-run the *malware.sh* script to push malicious traffic through the firewall again.

    a. Switch back to *PuTTY* by clicking the icon in the taskbar.

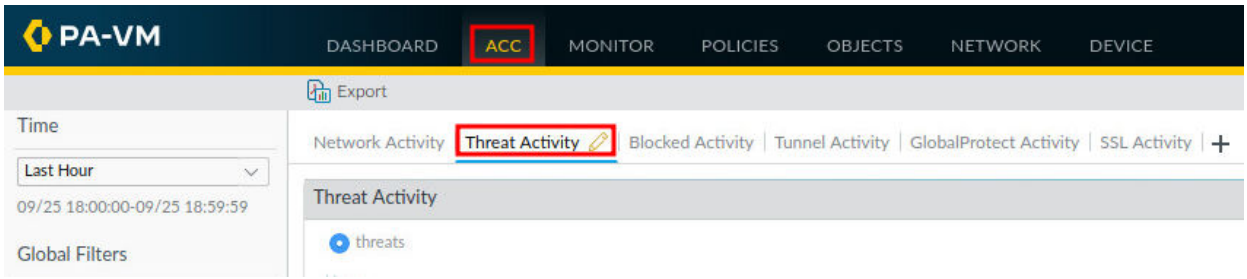
    b. Press the **up-arrow** key then press the **Enter** key to re-run the script.

c. Return to the *Chromium* window

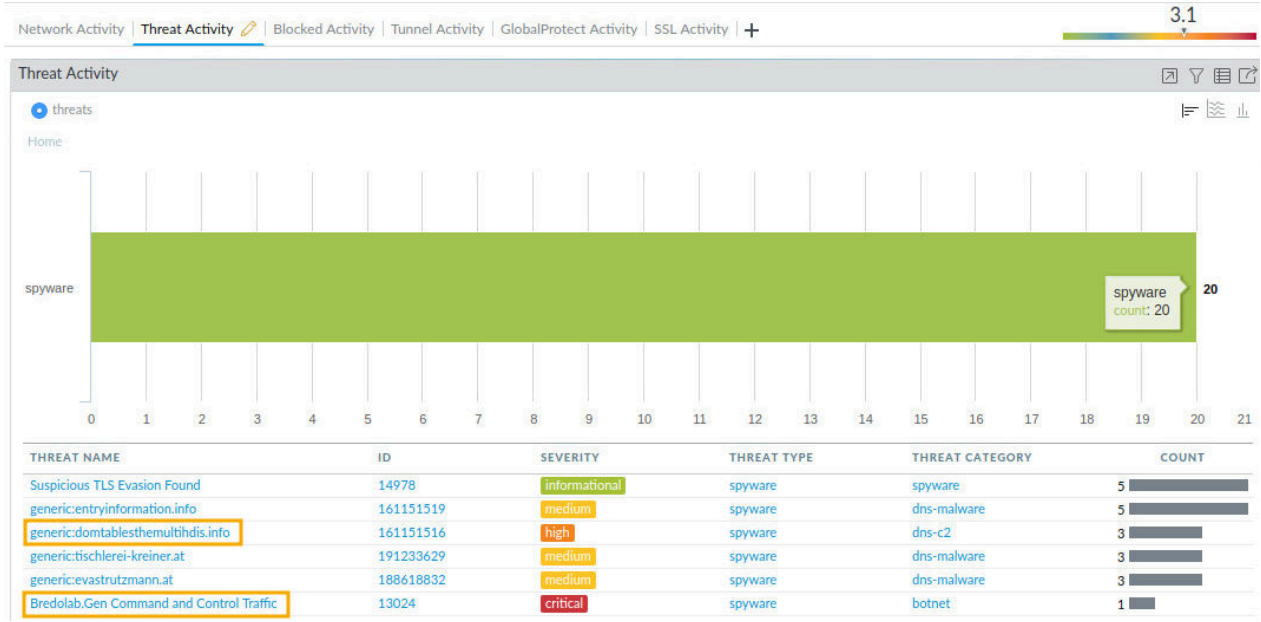
d. Refresh the threat list by clicking the *refresh* icon. (Alternatively, you could change the drop-down from *manual* to *10 seconds*, and run the script again until the *Bredolab* threat appears in the list.)



5. Navigate to **ACC > Threat Activity**.

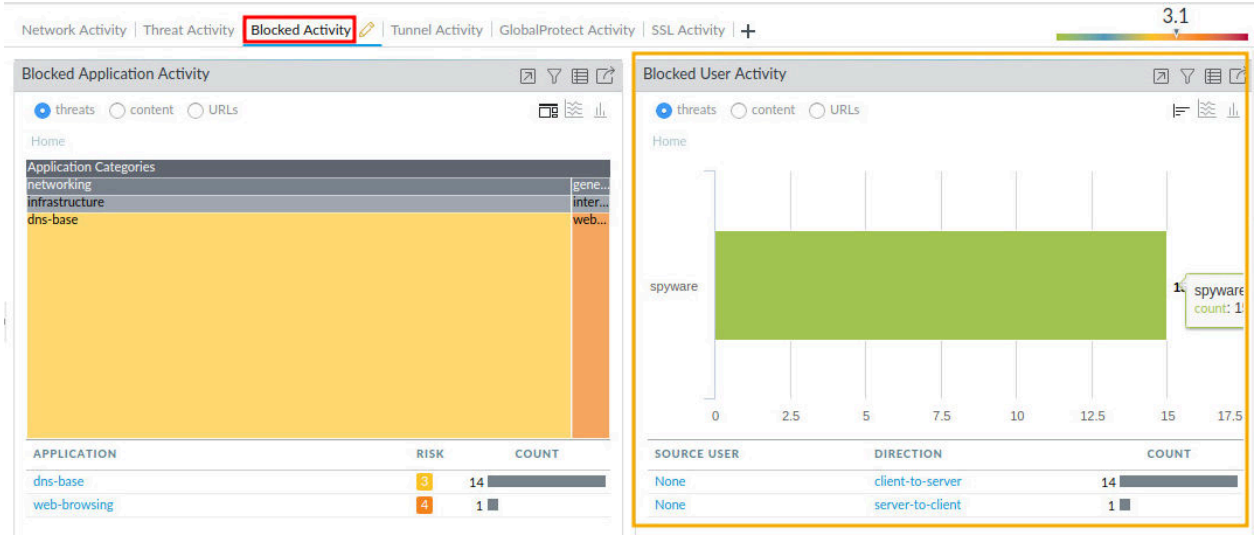


6. You should see a bar graph of the types of threats identified and a list of threats under *Threat Name*.



If you do not see any data onscreen, you may need to wait up to 5-10 minutes and click the **Refresh** icon in the upper-right. If that does not help, try clicking on the web browser's **Refresh** icon to refresh the entire browser. You may see one or multiple threats during the waiting period. The threat you are looking for is **Bredolab.Gen Command and Control Traffic.**

7. Navigate to the **Blocked Activity** tab. Observe the *Blocked User Activity* section.



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

