



CYBERSECURITY FOUNDATION

Lab 2: Malware Analysis

Document Version: **2021-01-22**

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

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

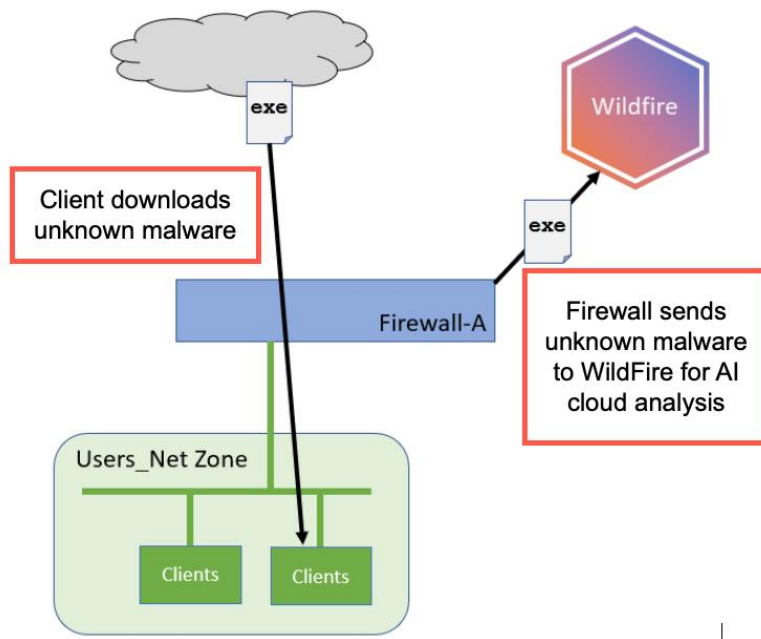
Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
2 Malware Analysis	6
2.0 Load Lab Configuration	6
2.1 Create a WildFire Analysis Profile	11
2.2 Modify a Security Profile Group	13
2.3 Test the WildFire Analysis Profile	16

Introduction

In this lab, you will create, test, and examine a WildFire security Profile.

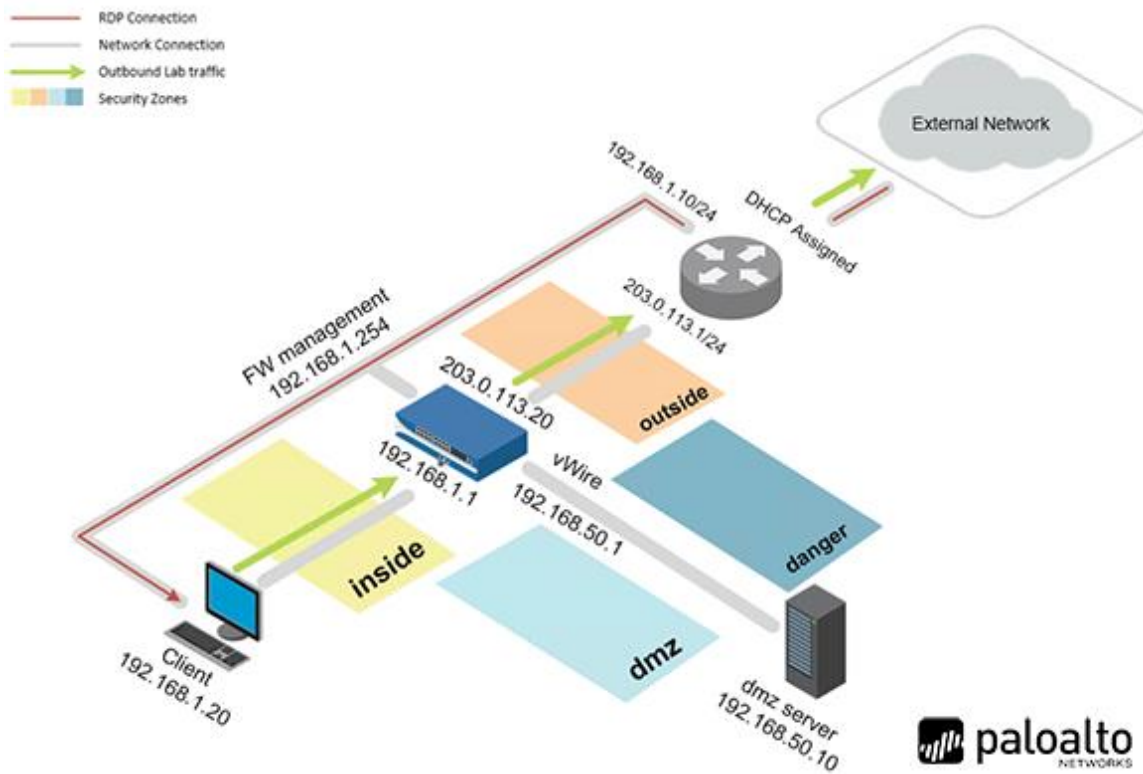


Objective

In this lab, you will perform the following tasks:

- Configure and test a WildFire Analysis Security Profile and examine the Wildfire report

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.

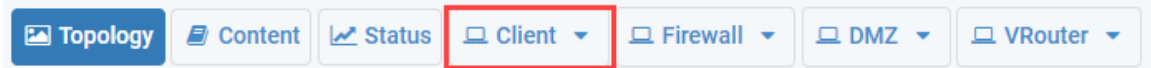
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

2 Malware Analysis

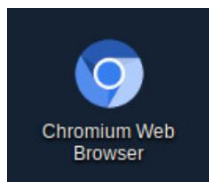
2.0 Load Lab Configuration

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

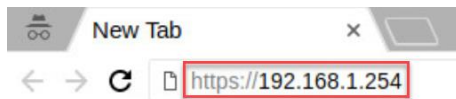
1. Click on the **Client** tab to access the Client PC.



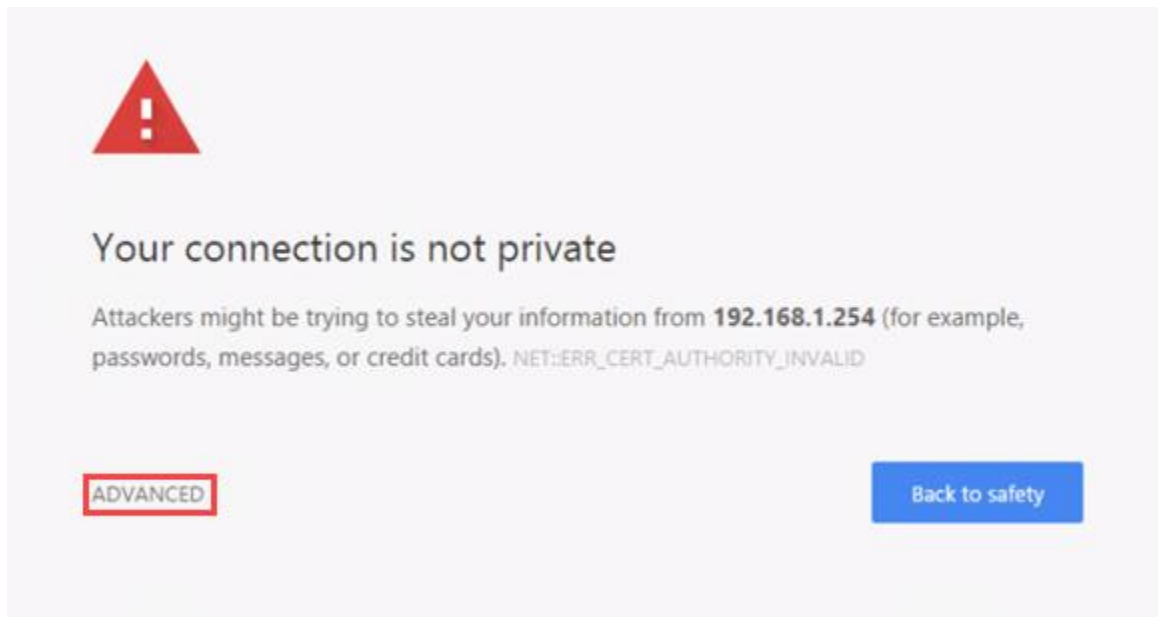
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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



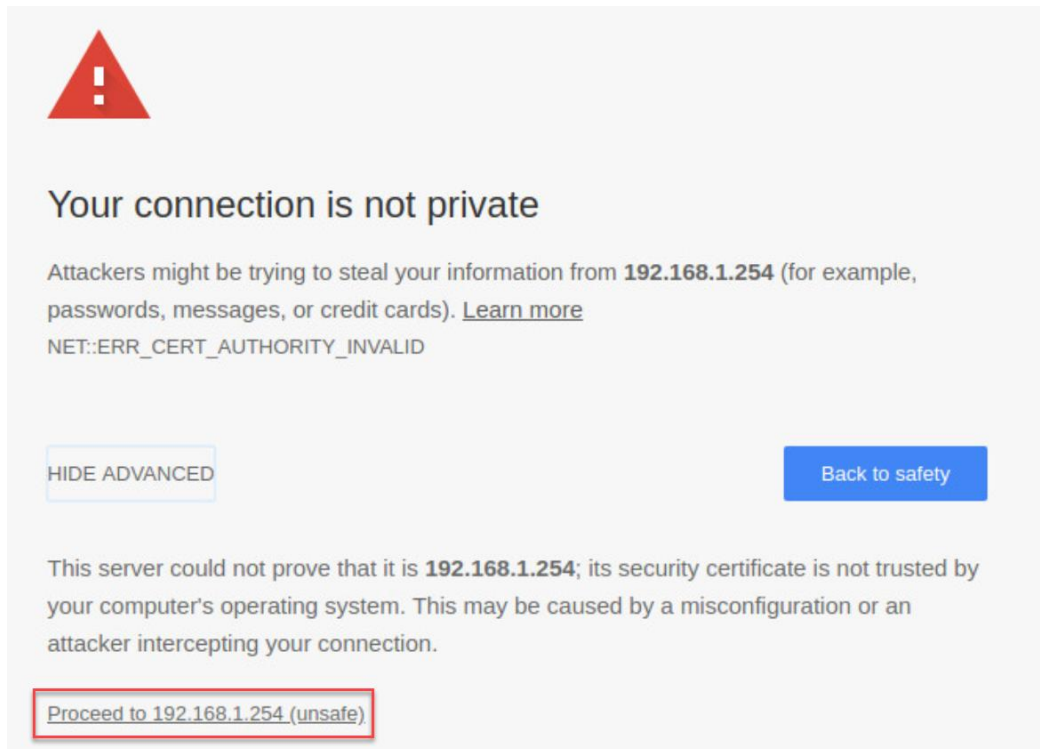
5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.





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

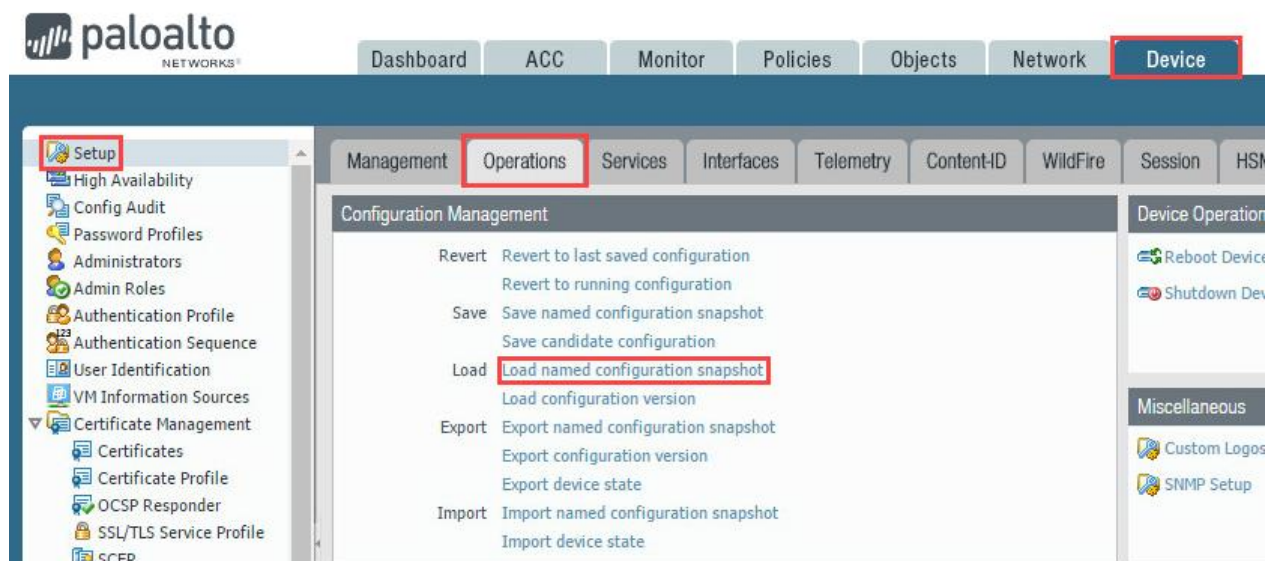
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



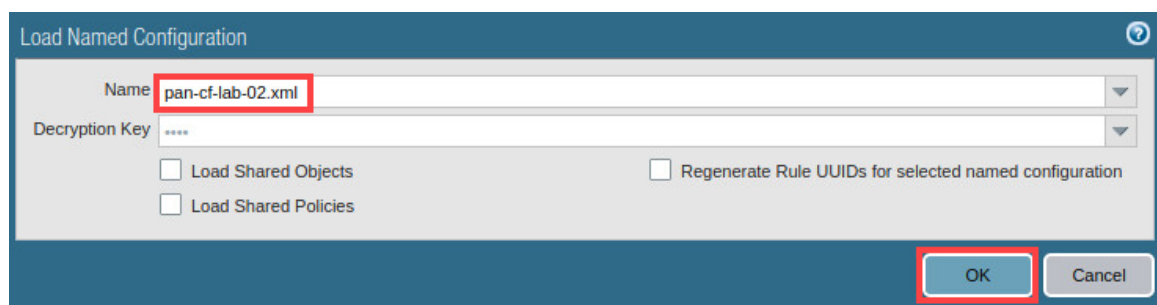
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



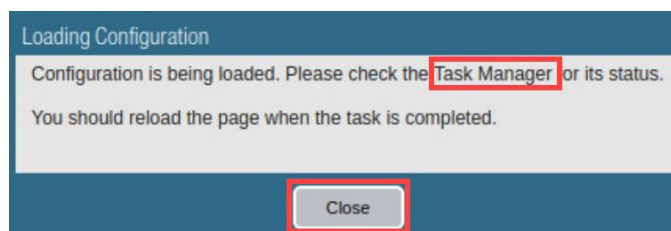
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



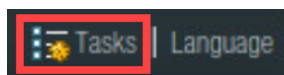
9. In the *Load Named Configuration* window, select **pan-cf-lab-02.xml** from the *Name* dropdown box and click **OK**.



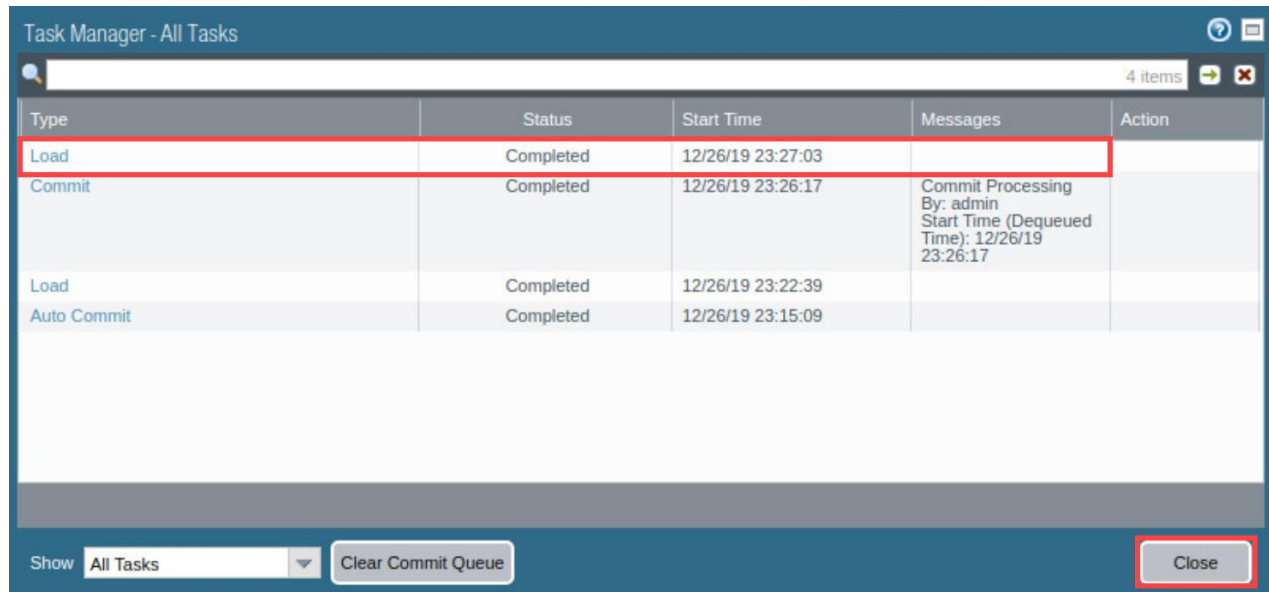
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



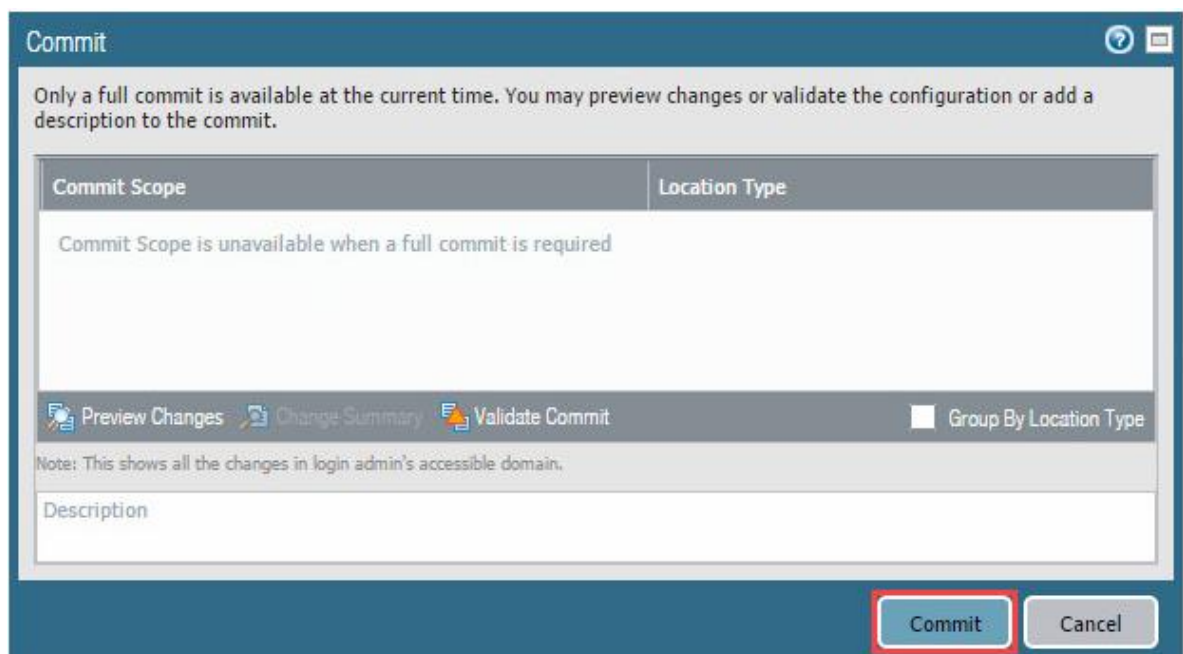
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



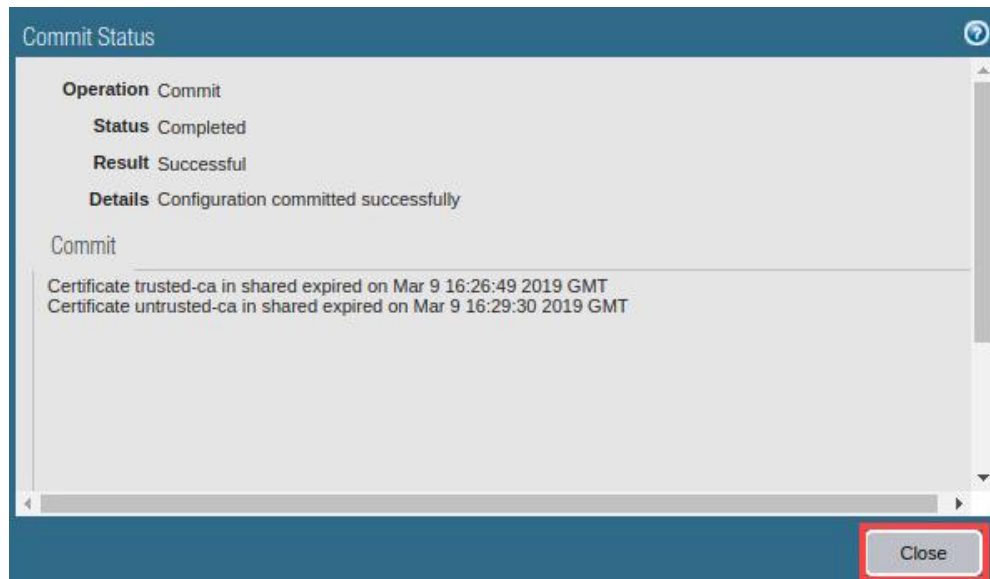
13. Click the **Commit** link located at the top-right of the web interface.



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



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



16. 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.

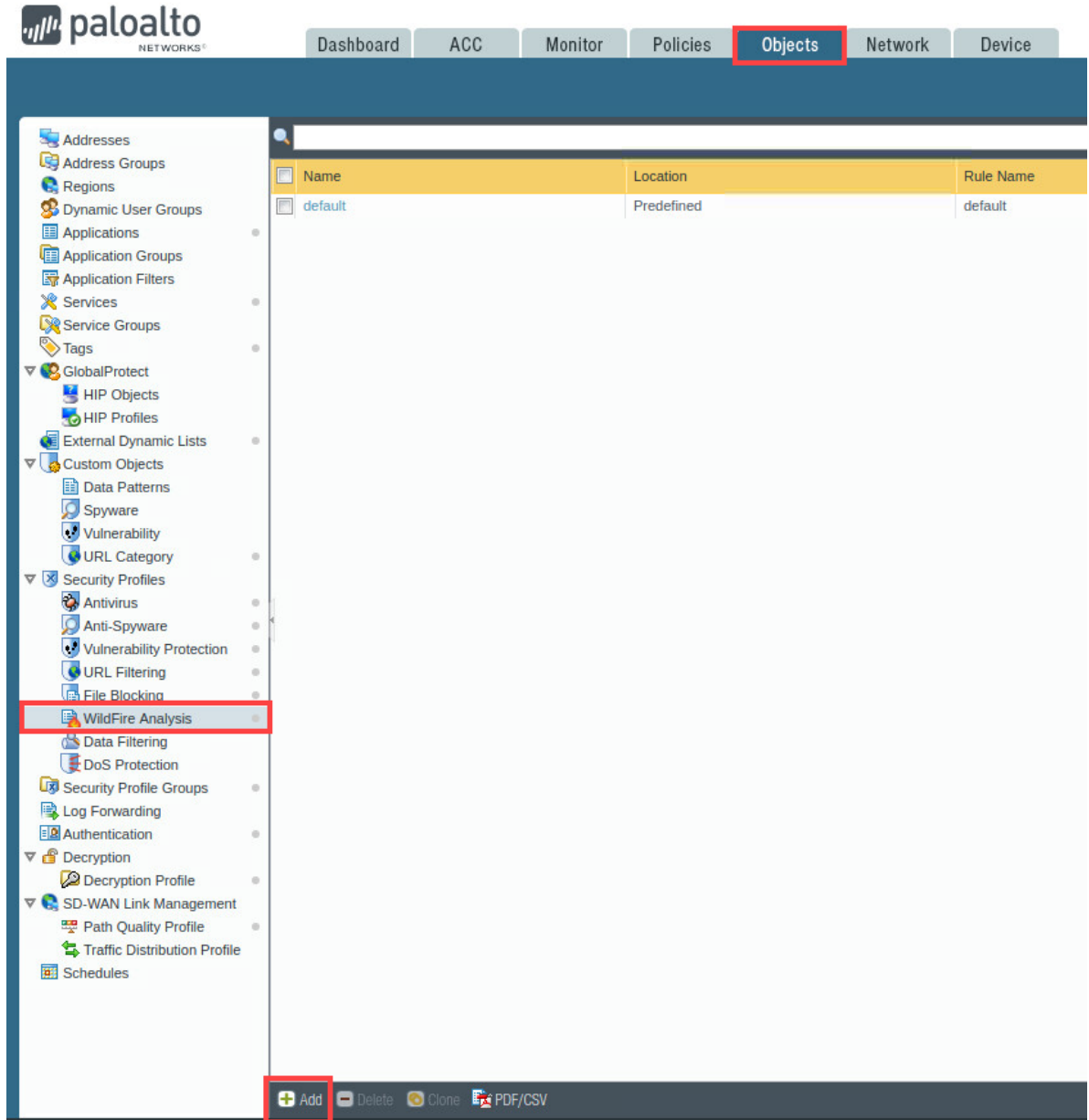


The **Warnings** displayed are normal. You will resolve those during this lab.

2.1 Create a WildFire Analysis Profile

In this section, you will create a WildFire Analysis Profile.

1. Navigate to **Objects > Security Profiles > Wildfire Analysis**. Click **Add**.

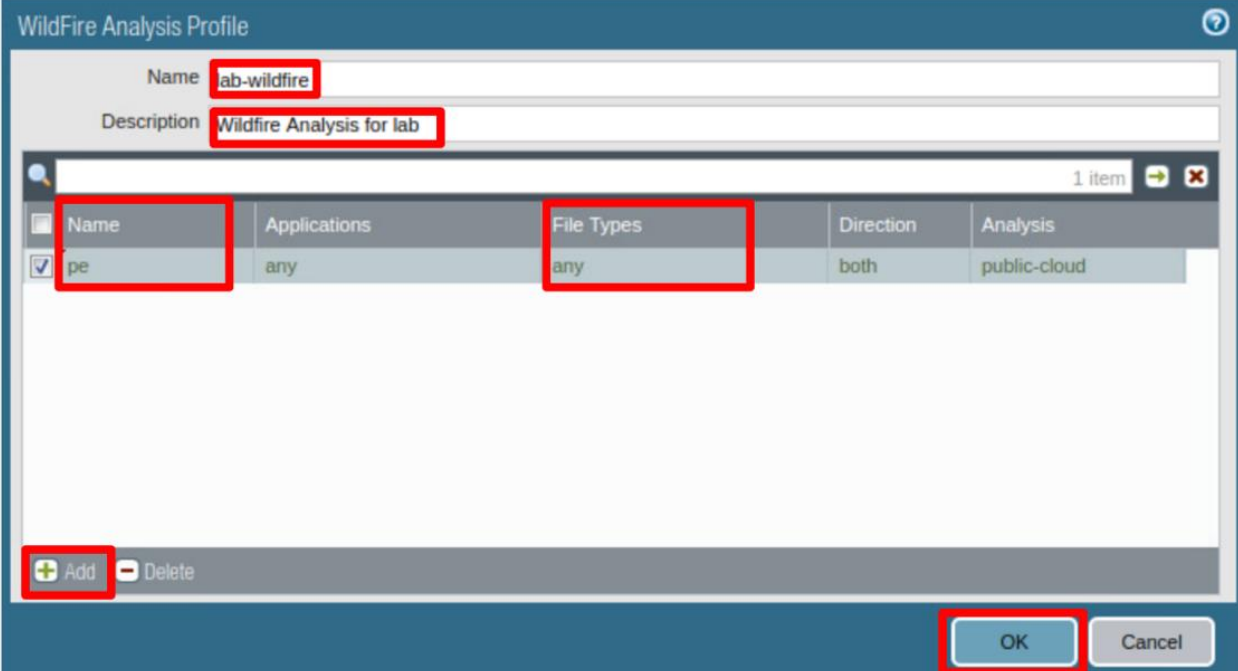


The screenshot shows the Palo Alto Networks management interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects (highlighted with a red box), Network, and Device. On the left, a sidebar menu lists various configuration categories. Under 'Security Profiles', the 'WildFire Analysis' option is highlighted with a red box. The main content area displays a table with the following data:

Name	Location	Rule Name
default	Predefined	default

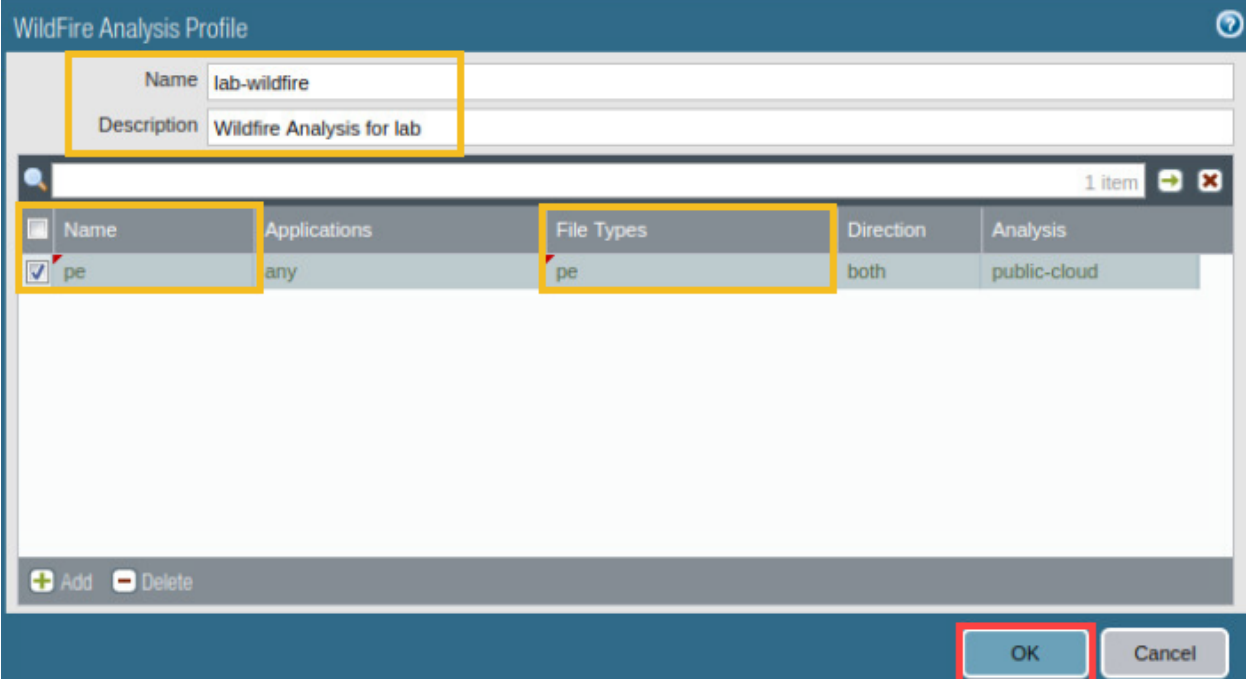
At the bottom of the interface, a toolbar contains buttons for '+ Add' (highlighted with a red box), Delete, Clone, and PDF/CSV.

2. In the *WildFire Analysis Profile* window, type **lab-wildfire** for the *Name*, **wildFire Analysis for lab** for the *Description*, and click **Add**. For the *name*, type **pe**. Under *File Types*, click **any** and click **Add**. From the dropdown menu, select **pe**. Leave all other defaults and click **OK**.



The screenshot shows the 'WildFire Analysis Profile' window. The 'Name' field is set to 'lab-wildfire' and the 'Description' field is set to 'Wildfire Analysis for lab'. Below these fields is a table with one item. The table has columns: Name, Applications, File Types, Direction, and Analysis. The row shows 'pe' for Name, 'any' for Applications, 'any' for File Types, 'both' for Direction, and 'public-cloud' for Analysis. At the bottom left, there are 'Add' and 'Delete' buttons. At the bottom right, there are 'OK' and 'Cancel' buttons.

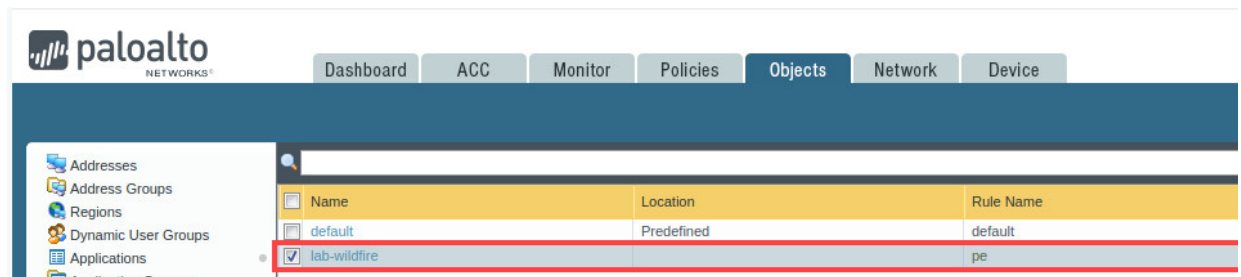
Name	Applications	File Types	Direction	Analysis
pe	any	any	both	public-cloud



The screenshot shows the 'WildFire Analysis Profile' window after updates. The 'Name' field is 'lab-wildfire' and the 'Description' field is 'Wildfire Analysis for lab'. The table now shows 'pe' for Name, 'any' for Applications, 'pe' for File Types, 'both' for Direction, and 'public-cloud' for Analysis. The 'Add' and 'Delete' buttons are at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

Name	Applications	File Types	Direction	Analysis
pe	any	pe	both	public-cloud

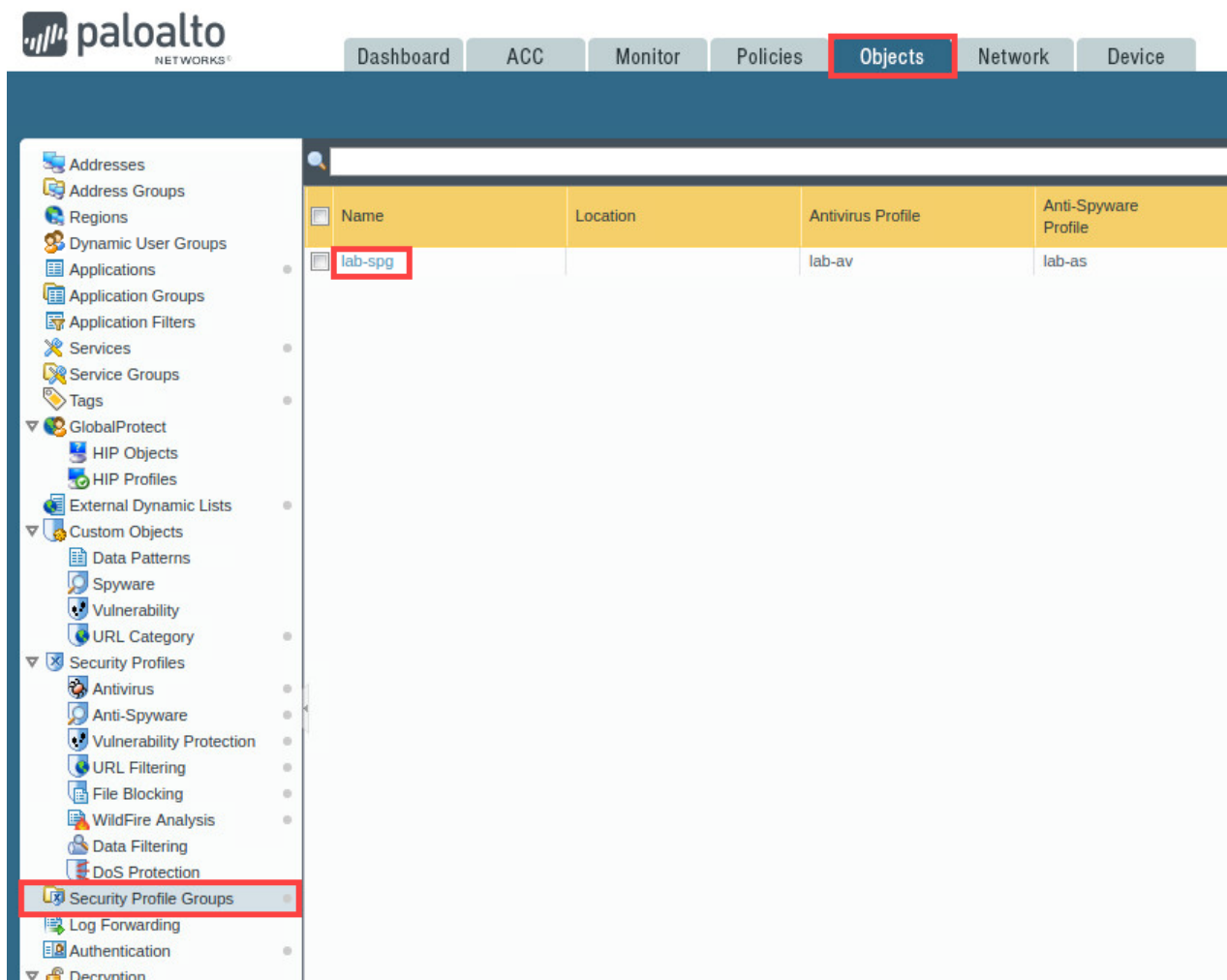
3. Verify the **lab-wildfire** object has been created.



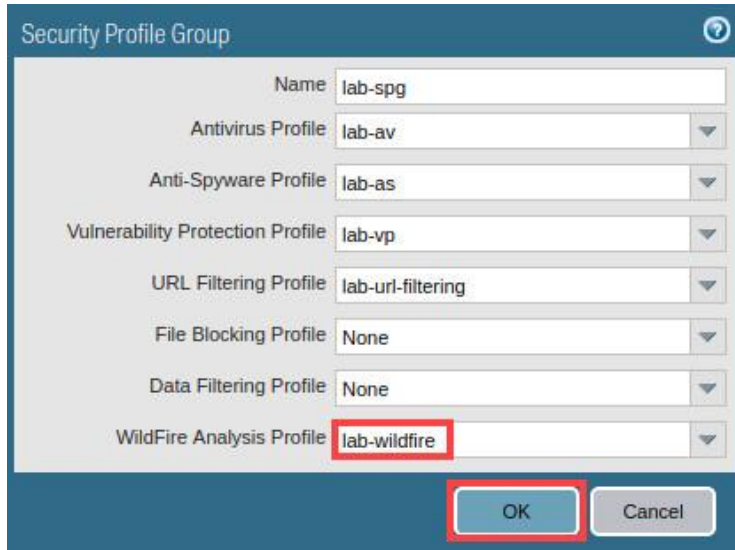
2.2 Modify a Security Profile Group

In this section, you will add the **lab-wildfire** analysis profile to the *lab-spg* security profile group.

1. Navigate to **Objects > Security Profile Groups**. Click **lab-spg** to open the *Security Profile Group*.



2. In the *Security Profile Group* window, select **lab-wildfire** for the *WildFire Analysis Profile*. Click **OK**.

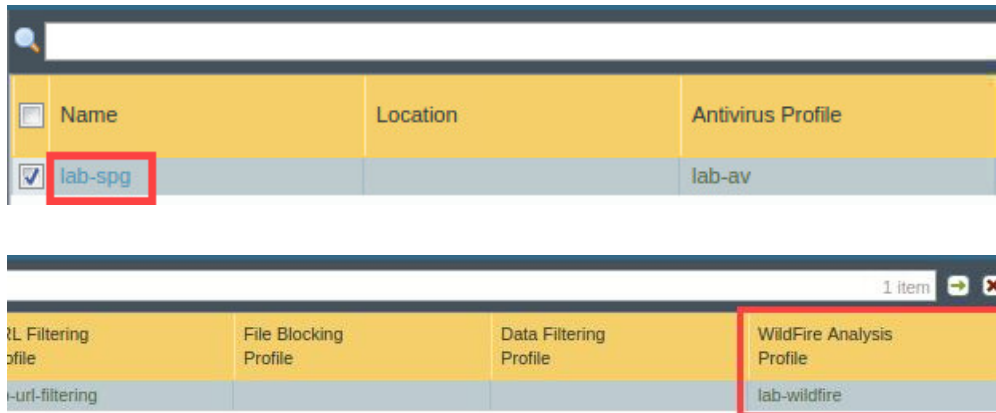


The 'Security Profile Group' window shows the following configuration:

Profile Type	Selected Profile
Name	lab-spg
Antivirus Profile	lab-av
Anti-Spyware Profile	lab-as
Vulnerability Protection Profile	lab-vp
URL Filtering Profile	lab-url-filtering
File Blocking Profile	None
Data Filtering Profile	None
WildFire Analysis Profile	lab-wildfire

At the bottom, the 'OK' button is highlighted with a red box.

3. Verify the *lab-spg* security profile group has been updated for the *WildFire Analysis Profile* to show **lab-wildfire**.



The screenshot shows two parts of the interface. The top part is a table listing security profile groups:

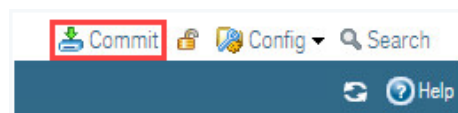
Name	Location	Antivirus Profile
lab-spg		lab-av

The 'lab-spg' entry is highlighted with a red box. The bottom part shows a detailed view of the 'lab-spg' profile:

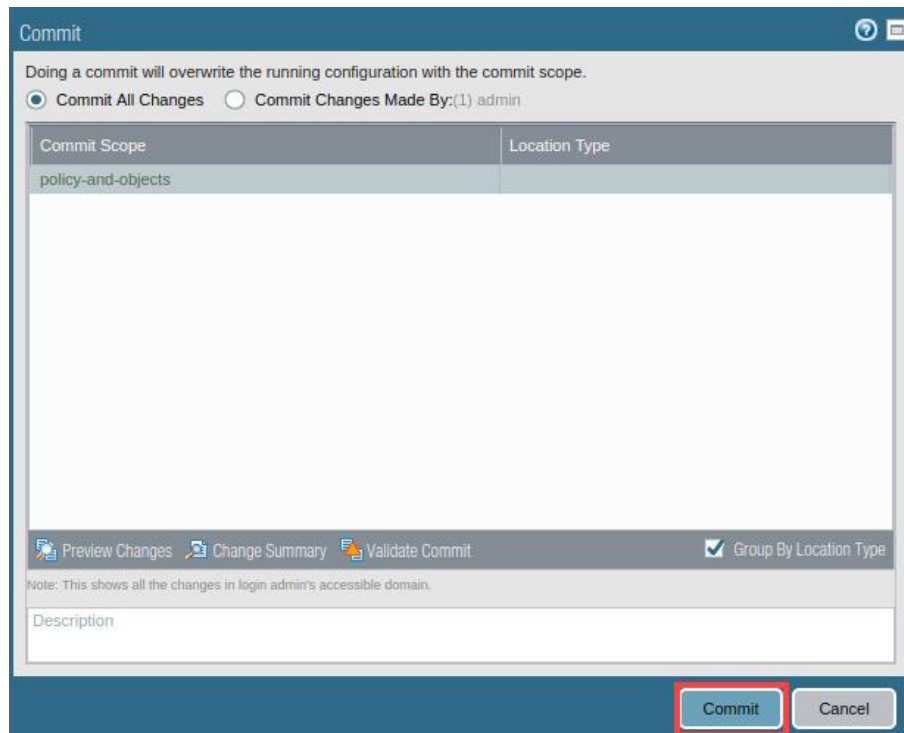
URL Filtering Profile	File Blocking Profile	Data Filtering Profile	WildFire Analysis Profile
lab-url-filtering			lab-wildfire

The 'WildFire Analysis Profile' column and its value 'lab-wildfire' are highlighted with a red box.

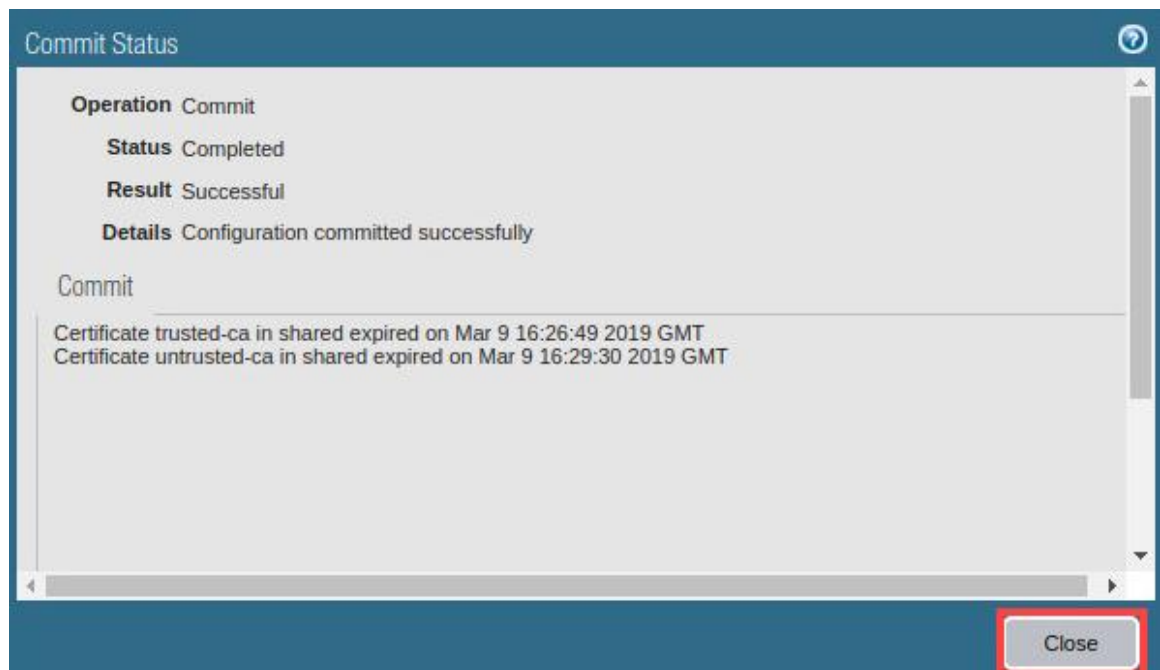
4. Click the **Commit** link located at the top-right of the web interface.



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



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



7. Open a new *Chromium* tab and continue to the next task.



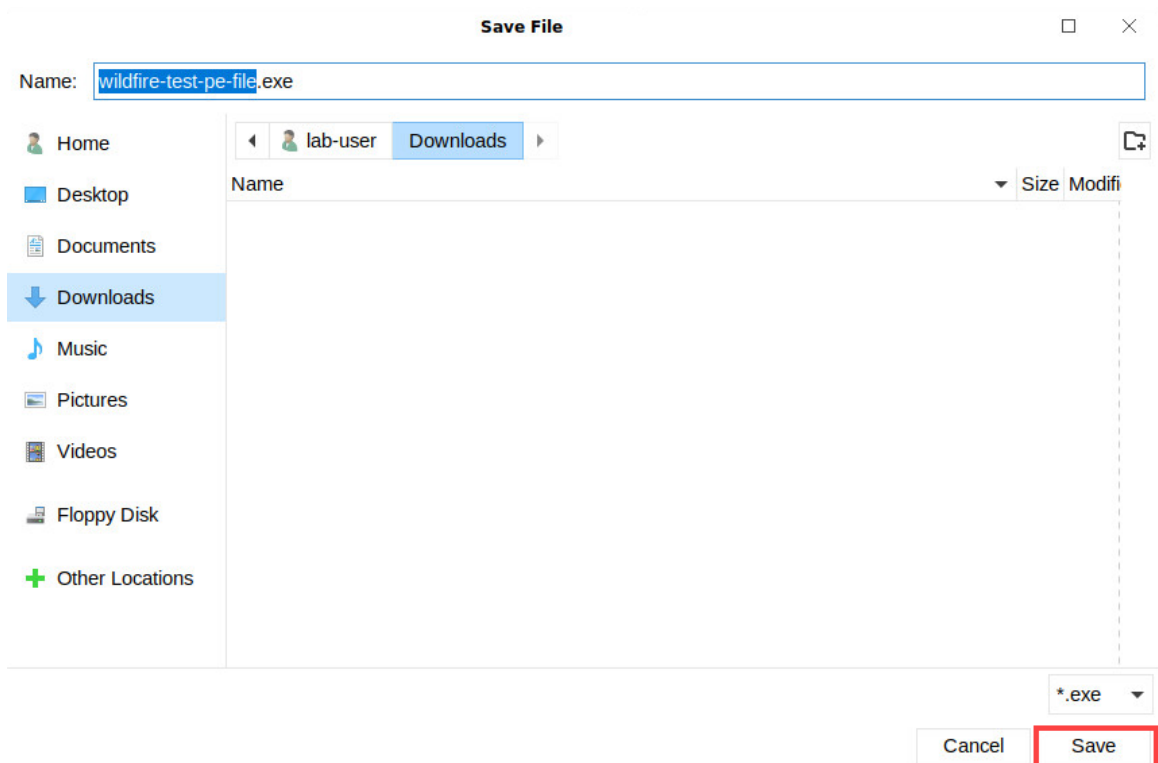
2.3 Test the WildFire Analysis Profile

In this section, you will test the WildFire Analysis Profile that you created and generate an attack file to simulate a zero-day attack.

1. On the new *Chromium* tab, enter <http://wildfire.paloaltonetworks.com/publicapi/test/pe> in the address bar and press **Enter**. Do not open the file.



2. In the *Save File* window, leave the defaults and click **Save**.



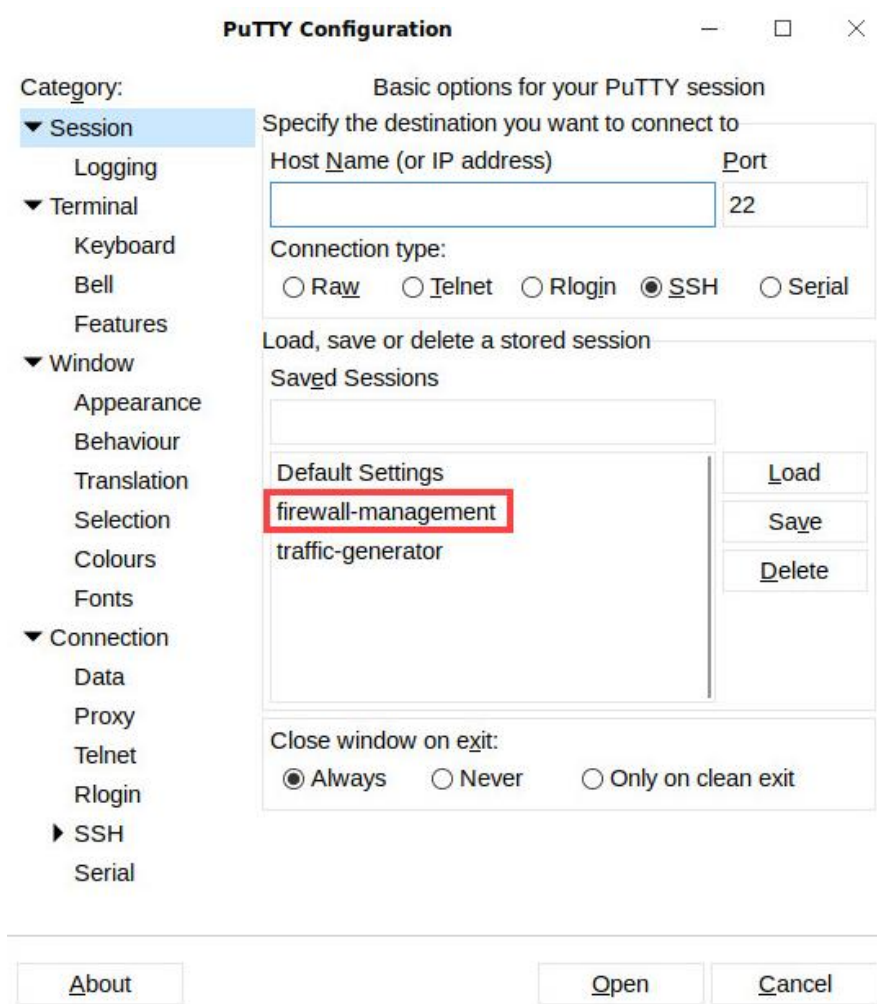
3. Close the *Chromium* tab that was used to download the attack file.



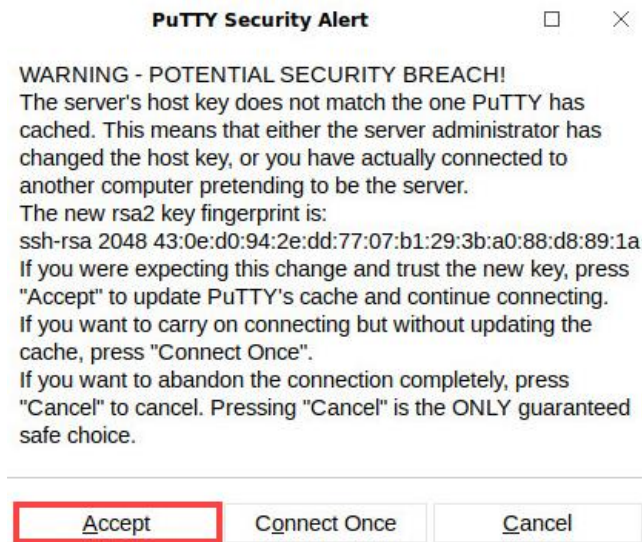
4. On the client *Desktop*, click the **Putty** icon located at the lower-left of the *Desktop*.



5. In the *Putty Configuration* window, double-click **firewall-management**.



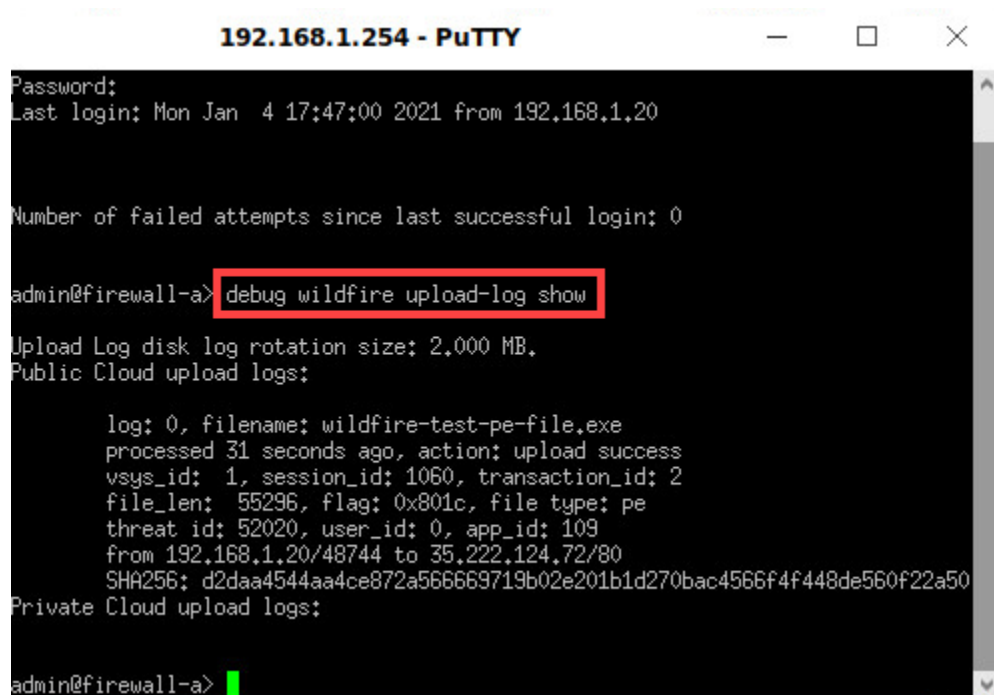
- If the *PuTTY Security Alert* window appears, click **Accept**.



- Log in as **admin** and for the *password*, type **Train1ng\$**.



8. In the 192.168.1.254 – Putty window, type `debug wildfire upload-log show` and press **Enter**.



```

192.168.1.254 - PuTTY
Password:
Last login: Mon Jan  4 17:47:00 2021 from 192,168,1,20

Number of failed attempts since last successful login: 0

admin@firewall-a> debug wildfire upload-log show

Upload Log disk log rotation size: 2,000 MB.
Public Cloud upload logs:

  log: 0, filename: wildfire-test-pe-file.exe
  processed 31 seconds ago, action: upload success
  vsys_id: 1, session_id: 1060, transaction_id: 2
  file_len: 55296, flag: 0x801c, file type: pe
  threat id: 52020, user_id: 0, app_id: 109
  from 192,168,1,20/48744 to 35,222,124,72/80
  SHA256: d2daa4544aa4ce872a566669719b02e201b1d270bac4566f4f448de560f22a50
Private Cloud upload logs:

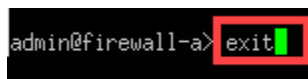
admin@firewall-a>

```

**Please
Note**

The command should display the output **log: 0, filename: wildfire-test-pe-file.exe processed...** This output verifies that the file was uploaded to the WildFire public cloud. The message might take a minute or two to appear.

9. In the 192.168.1.254 – Putty window, type `exit` and press **Enter**.

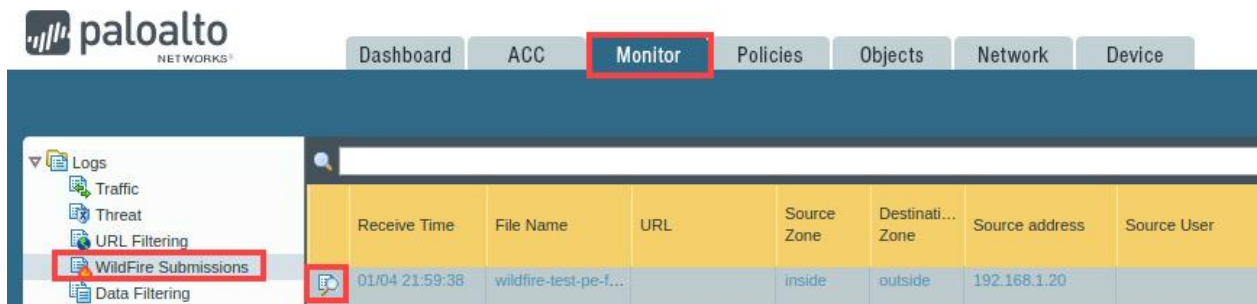


```

admin@firewall-a> exit

```

10. Navigate to **Monitor > Logs > WildFire Submissions**. It may take **5 to 10** minutes for the **wildfire-test-pe-file.exe** to appear. Click the **magnifying glass** icon next to the **wildfire-test-pe-file.exe** to see a detailed view of the Wildfire entry.



11. On the *Log Info* tab, review the information within the **General**, **Source**, and **Destination** panels.

Detailed Log View

Log Info WildFire Analysis Report

General		Source		Destination	
Session ID	623	Source User		Destination User	
Action	allow	Source	192.168.1.20	Destination	35.222.124.72
Application	web-browsing	Port	60496	Port	80
Rule	egress-outside-content-id	Zone	inside	Zone	outside
Rule UUID	c0db929f-b928-444d-91be-4551b4865eda	Interface	ethernet1/2	Interface	ethernet1/1
Verdict	malicious	NAT IP		NAT IP	
Device SN	015351000056630	NAT Port	6356	NAT Port	80
IP Protocol	tcp				
Log Action					
Generated Time: 2021/01/04 21:59:38					

PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2021/01/04 21:51:51	end	web-browsing	allow	egress-outside-content-id	c0db9...	60...		lab-decry...				
	2021/01/04 21:59:38	wildfire	web-browsing	allow	egress-outside-content-	c0db9...		high			malici...		wildfir..

Close

12. Click the *WildFire Analysis Report* Tab. Review the information regarding the *Wildfire Analysis Summary*.

Detailed Log View

Log Info WildFire Analysis Report

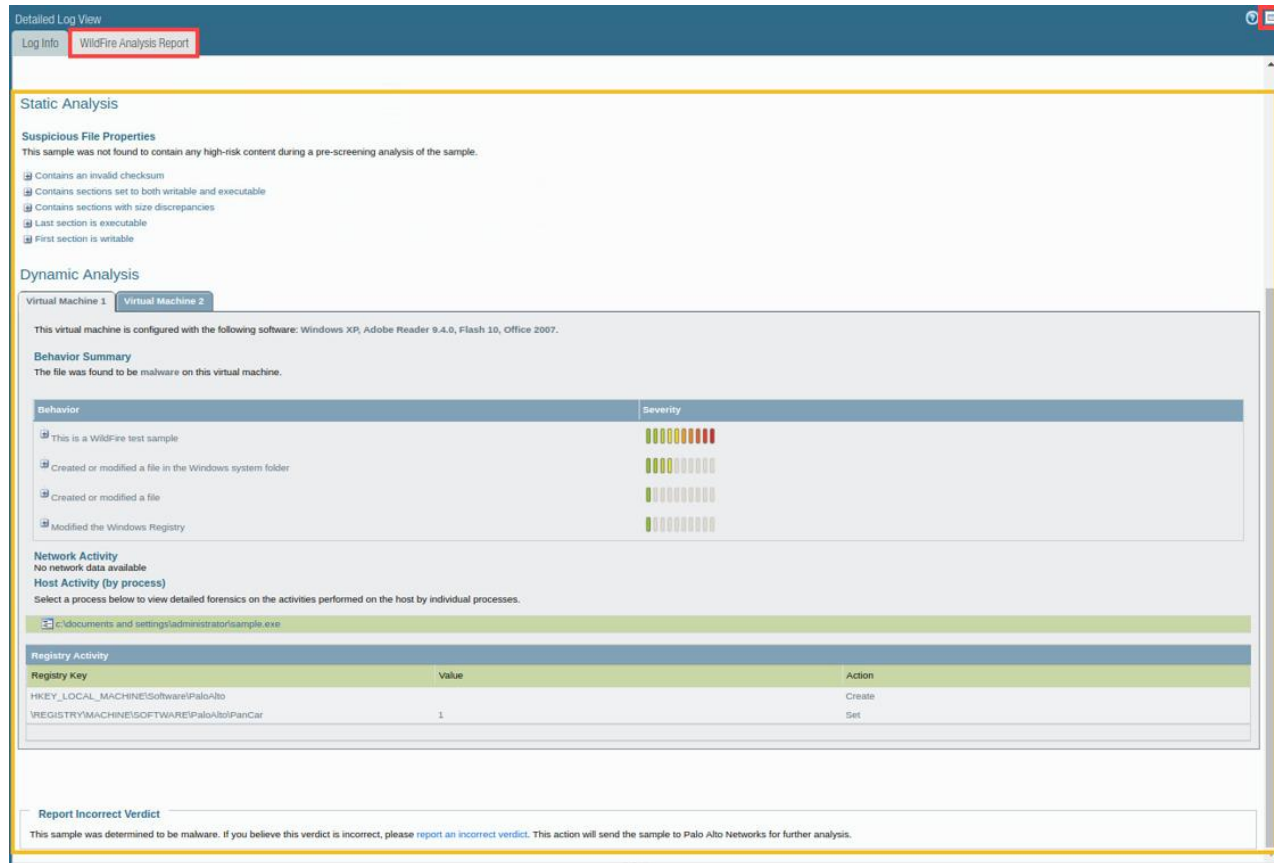
WildFire Analysis Summary [Download PDF](#)

File Information	
File Type	PE
File Signer	
SHA-256	e43c27a40fcf12b471752f1c953fdf50f5e27a79a27ad1fd2fd7e144a6fe95d1
SHA1	116e52b563274b823ba72bc40757d965a3d324f6
MD5	f88fc35d8d39bd228b316d7a26ccfcde
File Size	55296 bytes
First Seen Timestamp	2021-01-04 21:50:13 UTC
Verdict	malware
Sample File	Download File

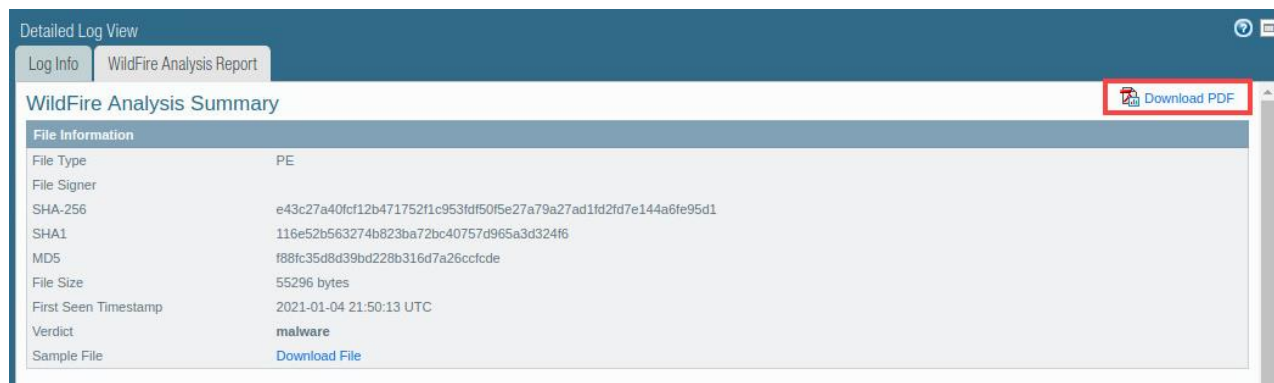
PCAP	Receive Time ▲	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2021/01/04 21:51:51	end	web-browsing	allow	egress-outside-content-id	c0db9...	60...		lab-decry...				
	2021/01/04 21:59:38	wildfire	web-browsing	allow	egress-outside-content-	c0db9...		high			malici...		wildfir..

Close

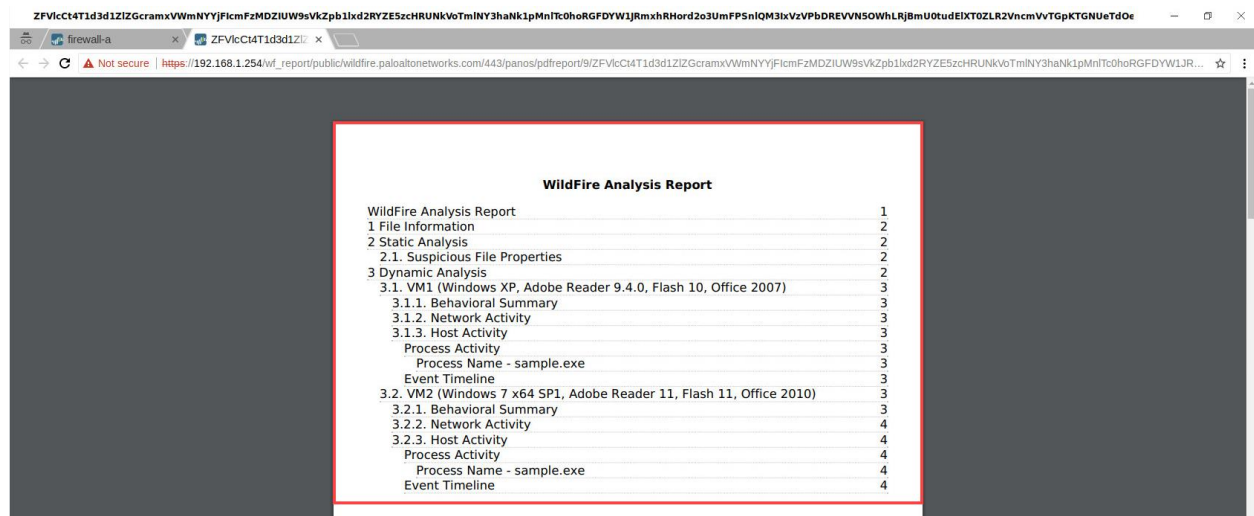
13. Scroll down the *WildFire Analysis Report* tab to see the **Static Analysis, Dynamic Analysis, Network Activity, Host Activity (by process), and Report Incorrect Verdict**. You may need to click the **expand** icon in the upper-right corner to better view the Wildfire Analysis Report.



14. Click **Download PDF** to view the *WildFire report*.



15. Once the file opens in *Chromium*, scroll through and review the **Wildfire Analysis Report**.



WildFire analysis reports provide comprehensive information on targeted users, header information from emails (if enabled), what application delivers the file, and all the URLs involved on the delivery of the file. WildFire reports contain several key pieces of information on the session information configured on the Palo Alto Networks Firewall. This is about the forwarded file and depends on the behavior observed for the file.

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