



CYBERSECURITY FOUNDATION V2

Lab 2: Malware Analysis

Document Version: 2022-12-22

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

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

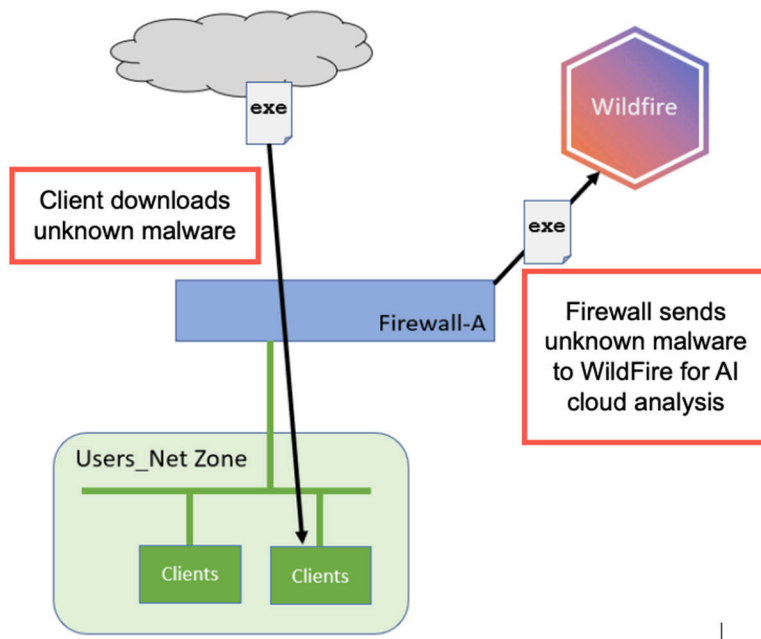
Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Malware Analysis	6
1.0 Load Lab Configuration	6
1.1 Create a WildFire Analysis Profile	11
1.2 Modify a Security Profile Group	13
1.3 Test the WildFire Analysis Profile	15

Introduction

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

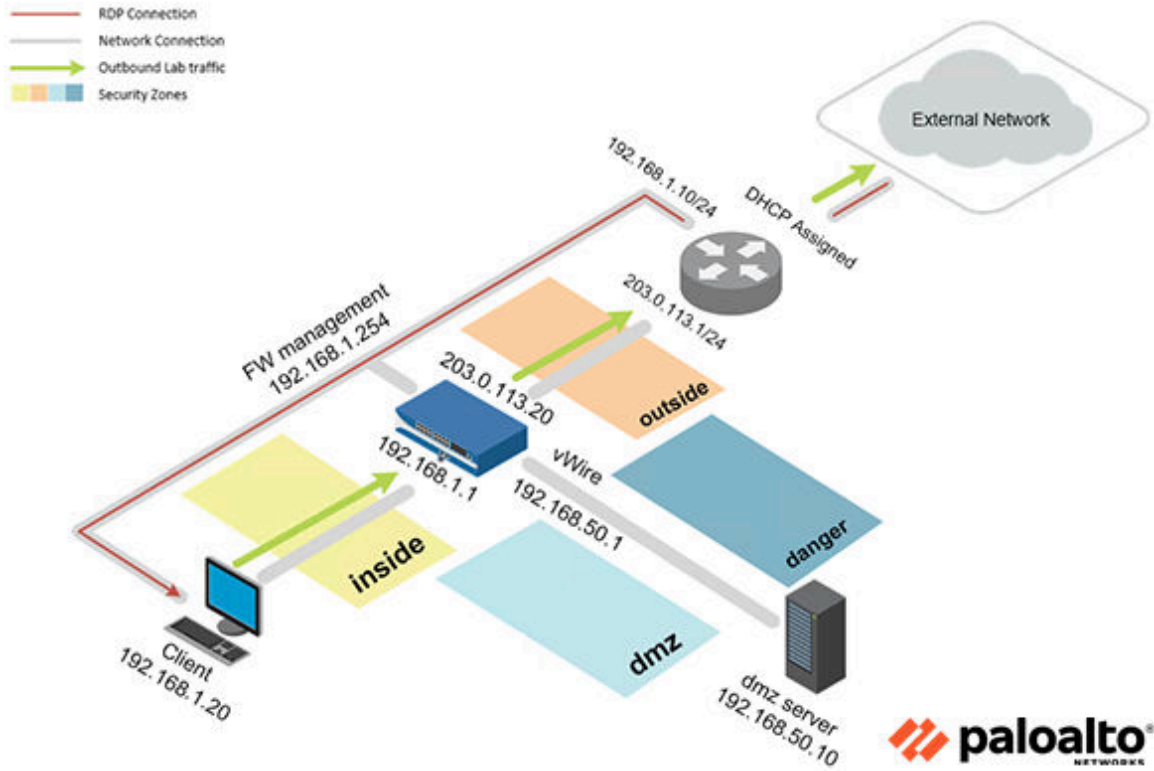


Objective

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.

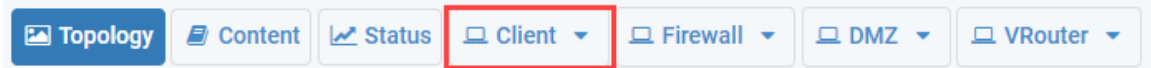
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Malware Analysis

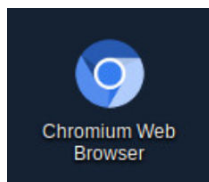
1.0 Load Lab Configuration

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

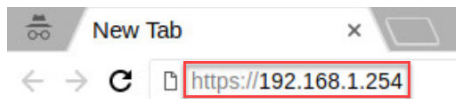
1. Click on the **Client** tab to access the Client PC.



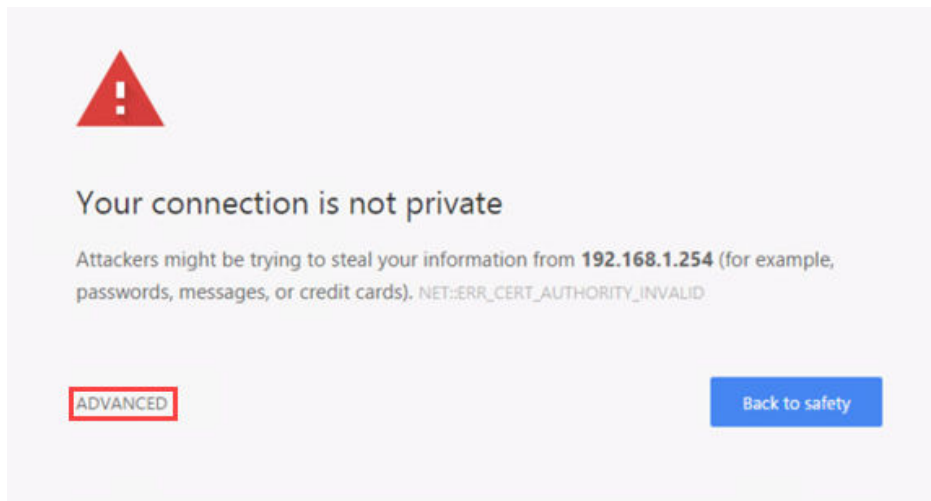
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

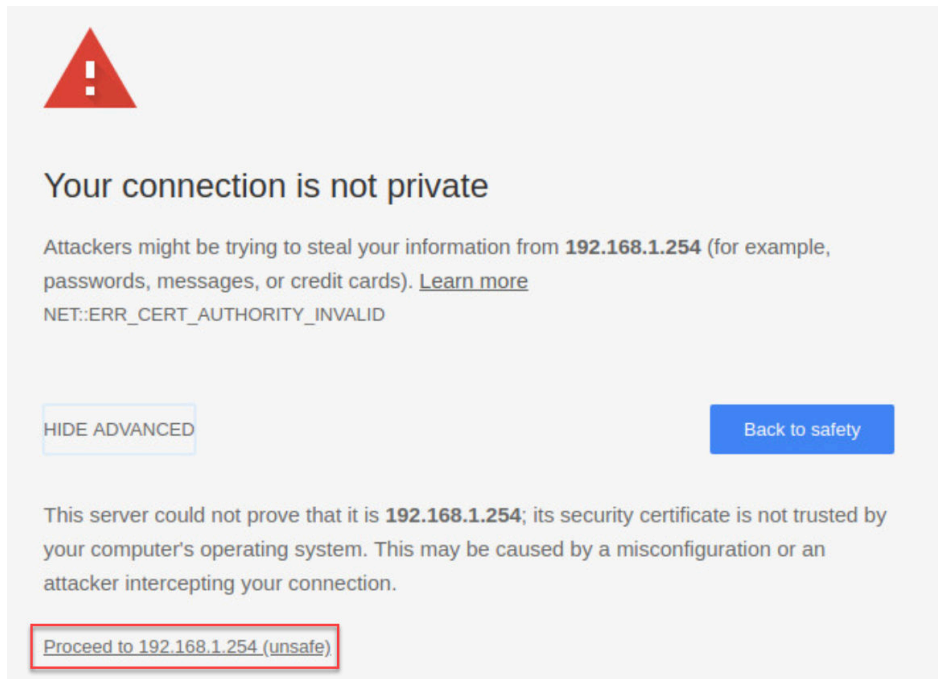


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

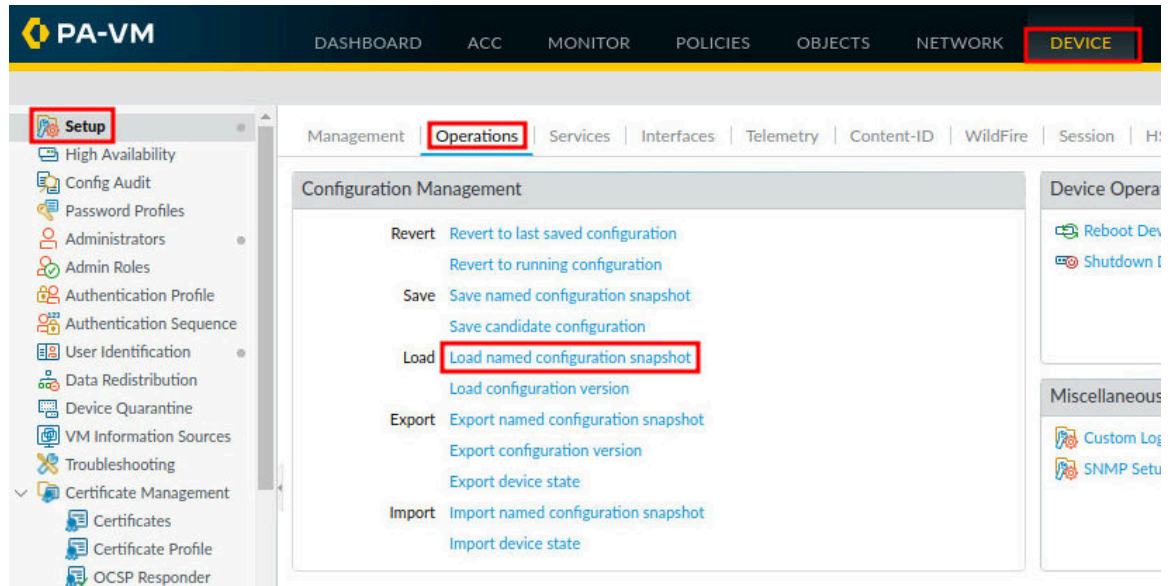
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



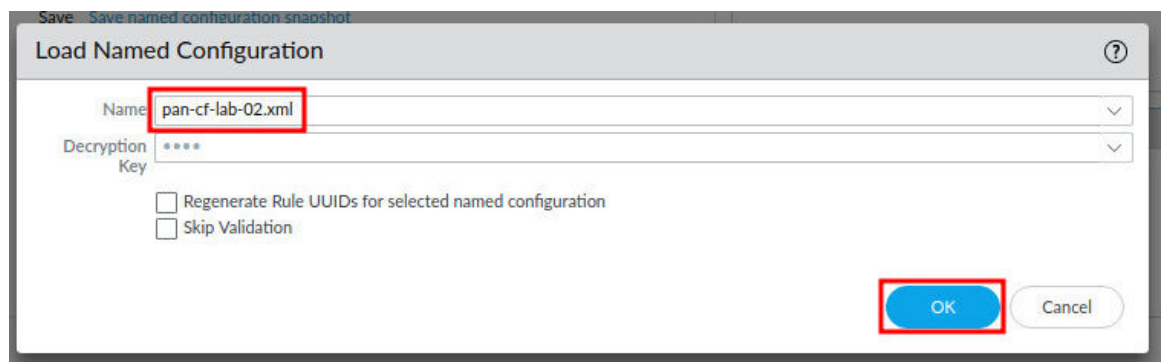
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



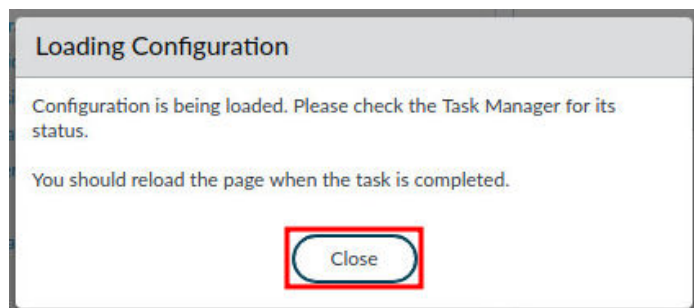
- In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



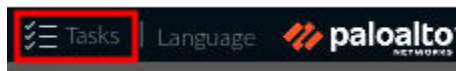
- In the *Load Named Configuration* window, select **pan-cf-lab-02.xml** from the *Name* dropdown box and click **OK**.



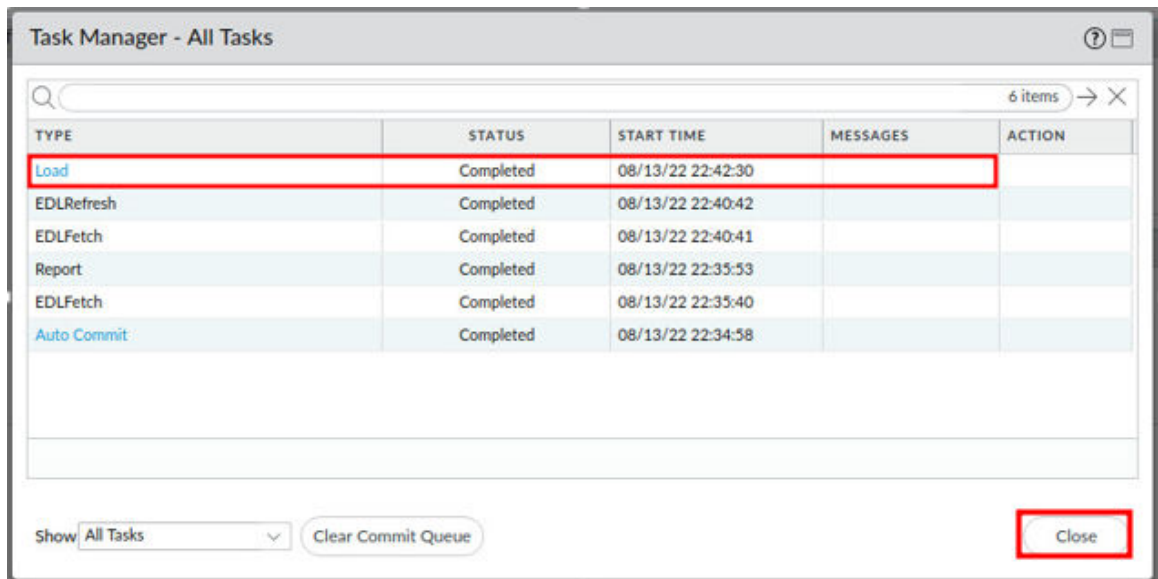
- In the *Loading Configuration* window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.



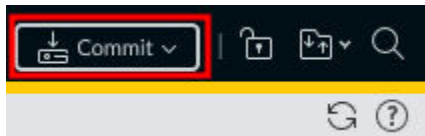
11. Click the **Tasks** icon located at the bottom-right of the web interface.



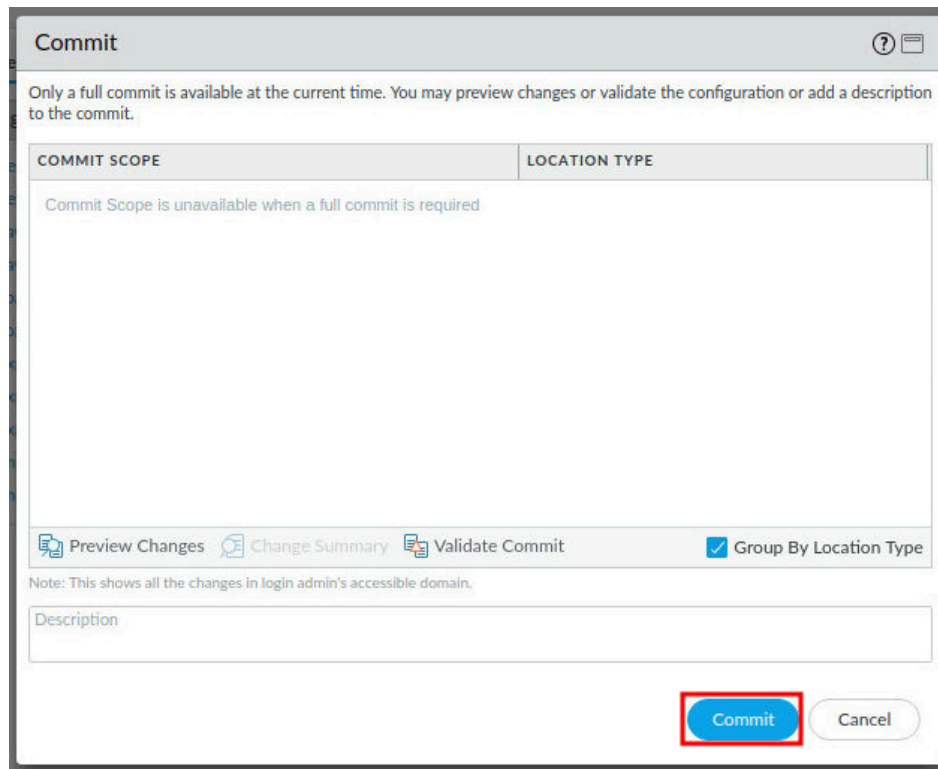
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



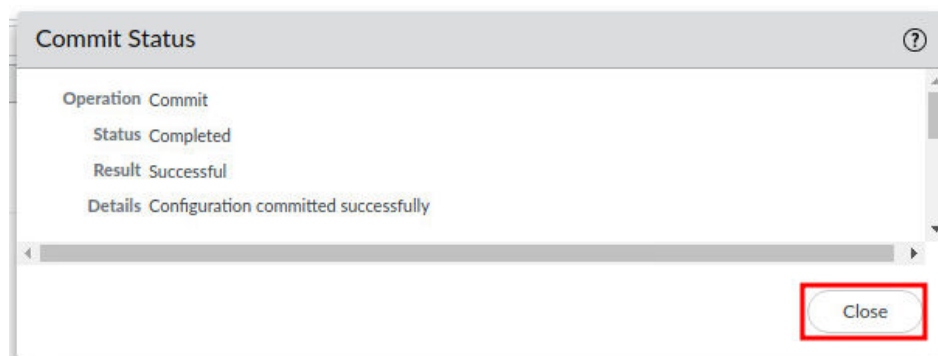
13. Click the **Commit** link located at the top-right of the web interface.



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



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

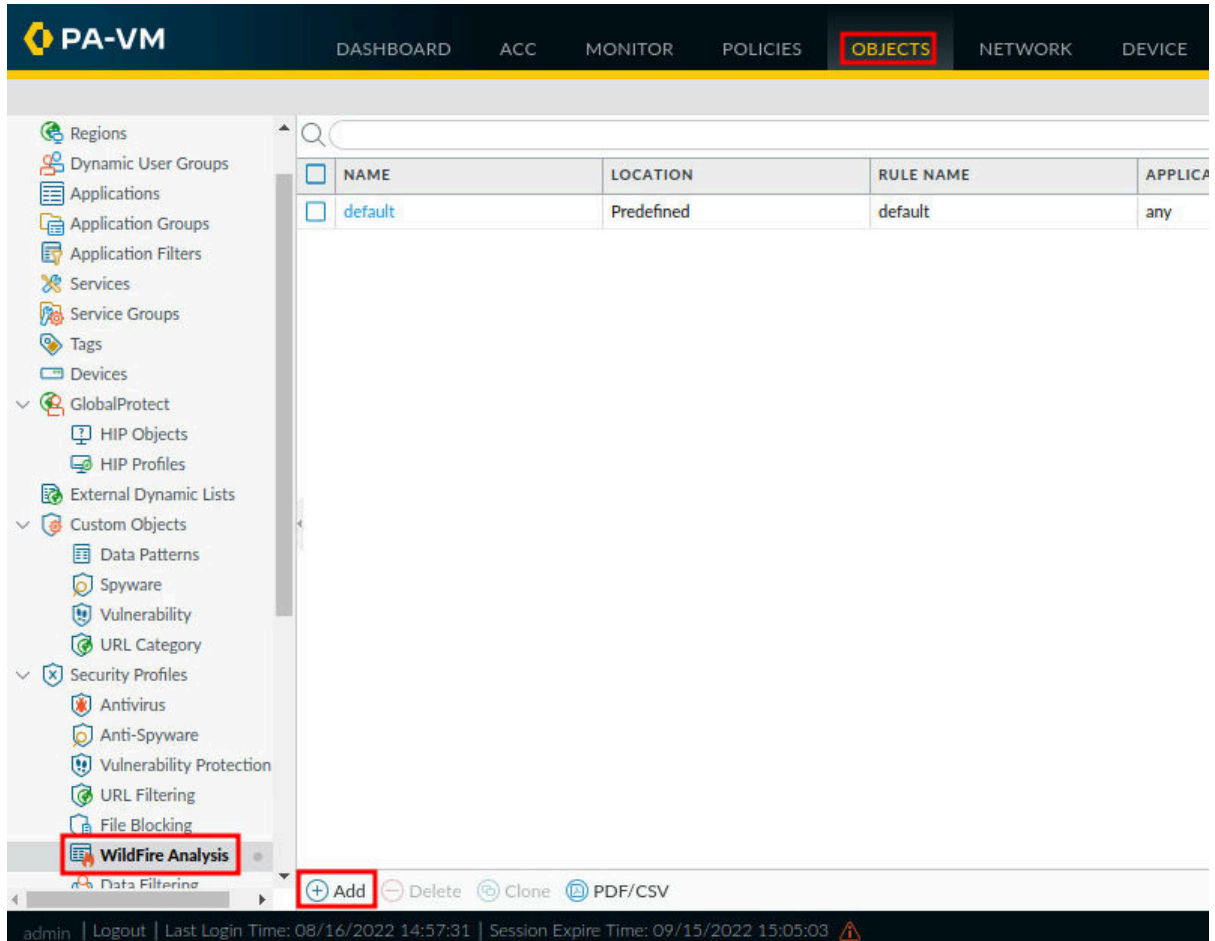


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit

1.1 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**.

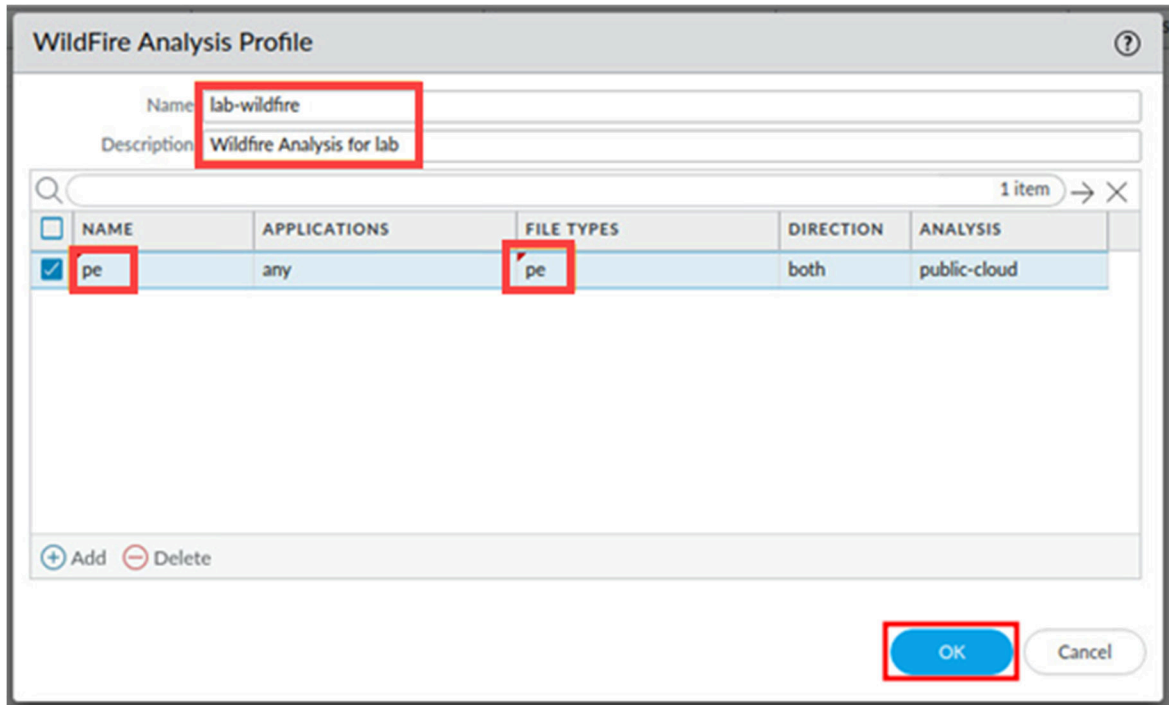


The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (highlighted with a red box), 'NETWORK', and 'DEVICE'. The left sidebar contains a tree view of configuration categories, with 'WildFire Analysis' highlighted at the bottom (indicated by a red box). The main content area displays a table with the following data:

NAME	LOCATION	RULE NAME	APPLICA
default	Predefined	default	any

Below the table, there is a '+ Add' button (highlighted with a red box), followed by 'Delete', 'Clone', and 'PDF/CSV' buttons. The footer shows the user 'admin', a 'Logout' link, and session information: 'Last Login Time: 08/16/2022 14:57:31' and 'Session Expire Time: 09/15/2022 15:05:03'.

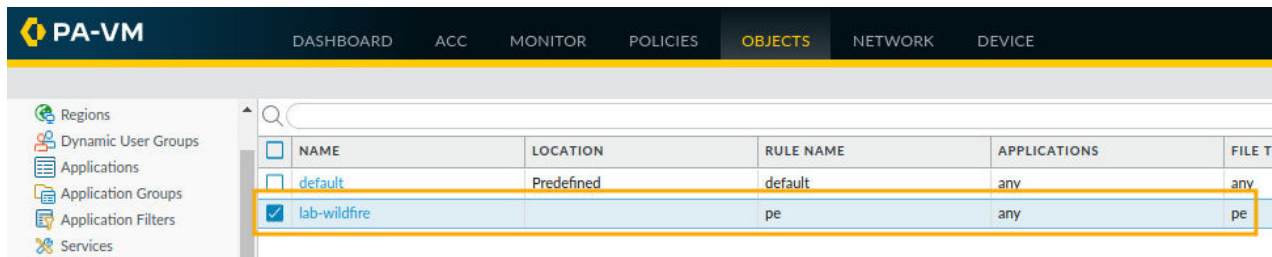
- In the *WildFire Analysis Profile* window, type `lab-wildfire` for the *Name*, *WildFire Analysis for lab* for the *Description*, and click **Add**. For the *name*, type `pe`. Under *File Types*, click **any** and click **Add**. From the dropdown menu, select **pe**. Leave all other defaults and click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



The screenshot shows the 'WildFire Analysis Profile' window. The 'Name' field contains 'lab-wildfire' and the 'Description' field contains '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' under NAME, 'any' under APPLICATIONS, 'pe' under FILE TYPES, 'both' under DIRECTION, and 'public-cloud' under ANALYSIS. At the bottom right, there is an 'OK' button and a 'Cancel' button.

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
pe	any	pe	both	public-cloud

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



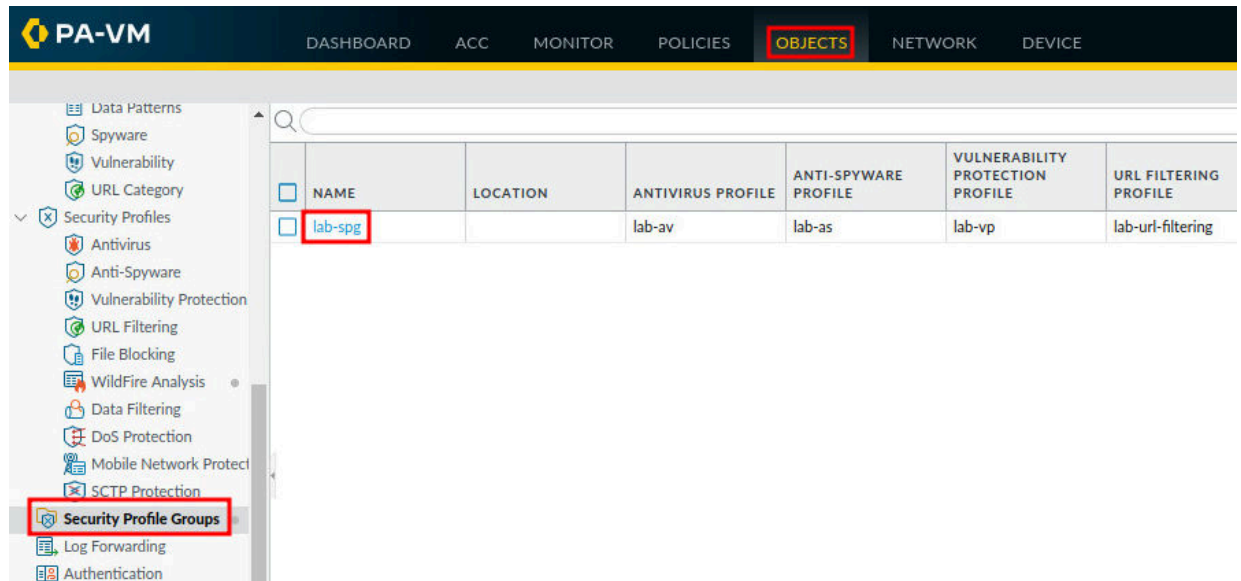
The screenshot shows the 'PA-VM' interface with the 'OBJECTS' tab selected. A table lists the objects. The 'lab-wildfire' object is highlighted with a blue selection bar.

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES
default	Predefined	default	any	any
lab-wildfire		pe	any	pe

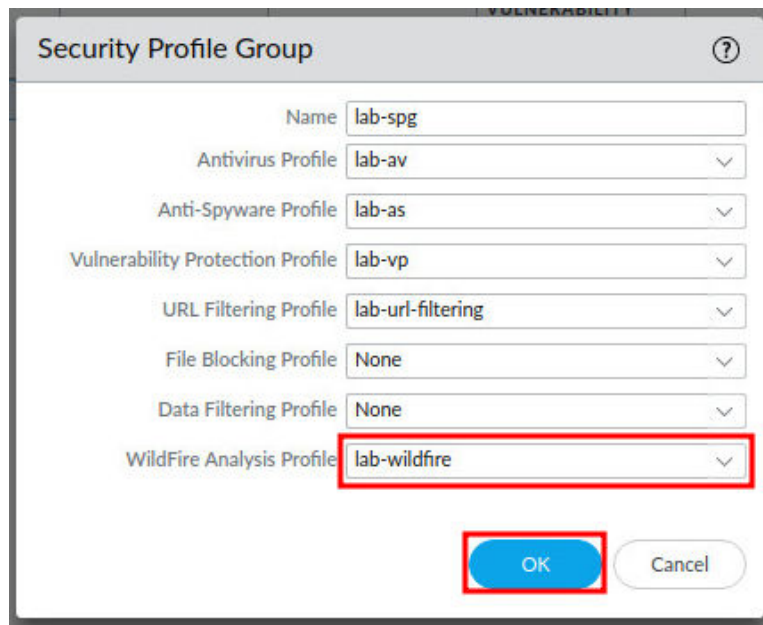
1.2 Modify a Security Profile Group

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*.



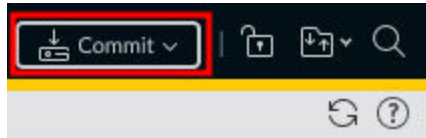
2. In the *Security Profile Group* window, select **lab-wildfire** for the *WildFire Analysis Profile*. Click **OK**.



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

1 item →									
<input type="checkbox"/>	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
<input checked="" type="checkbox"/>	lab-spg		lab-av	lab-as	lab-vp	lab-url-filtering			lab-wildfire

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.

Commit

Doing a commit will overwrite the running configuration with the commit scope.

☒ Commit All Changes
 ☐ Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

Preview Changes

Change Summary

Validate Commit

☒ Group By Location Type

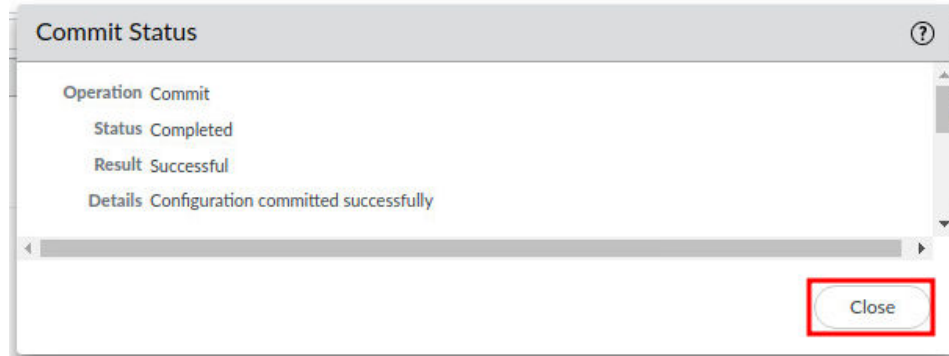
Note: This shows all the changes in login admin's accessible domain.

Description

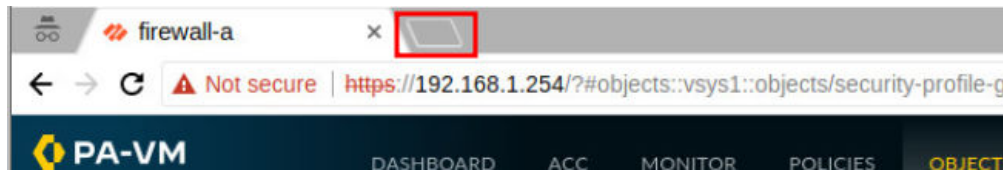
Commit

Cancel

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



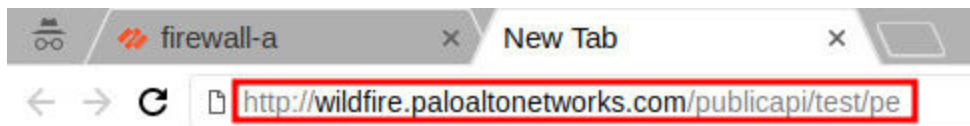
- Open a new *Chromium* tab and continue to the next task.



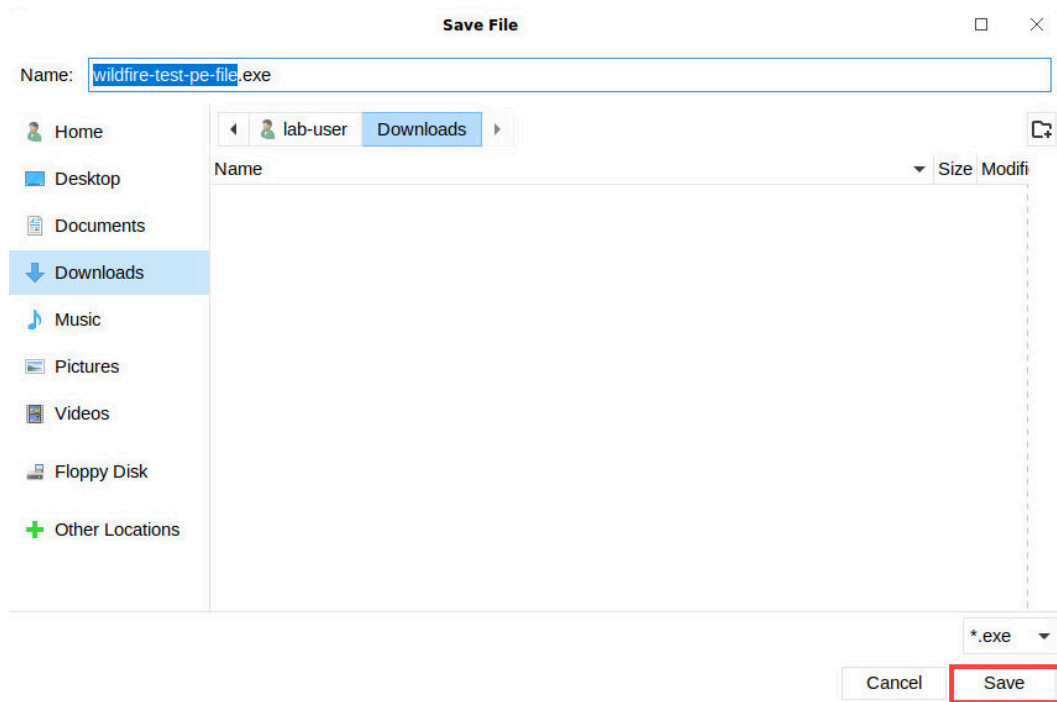
1.3 Test the WildFire Analysis Profile

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

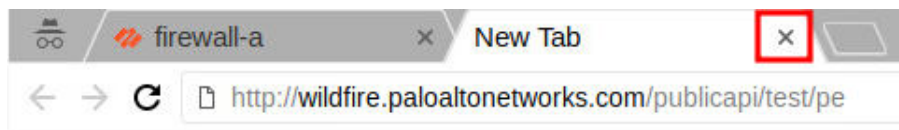
- On the new *Chromium* tab, enter `http://wildfire.paloaltonetworks.com/publicapi/test/pe` in the address bar and press **Enter**. Do not open the file.



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



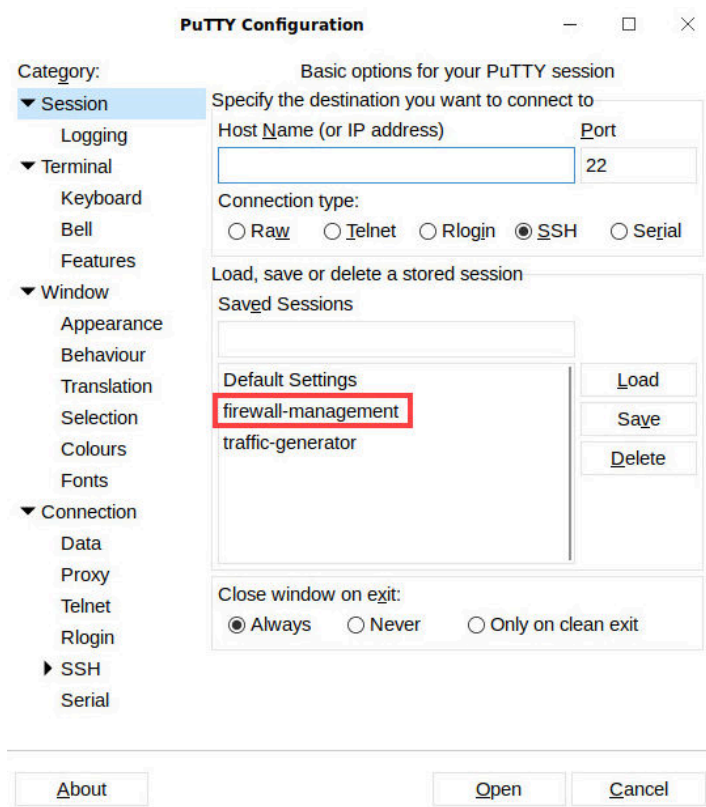
3. Close the *Chromium* tab that was used to download the attack file.



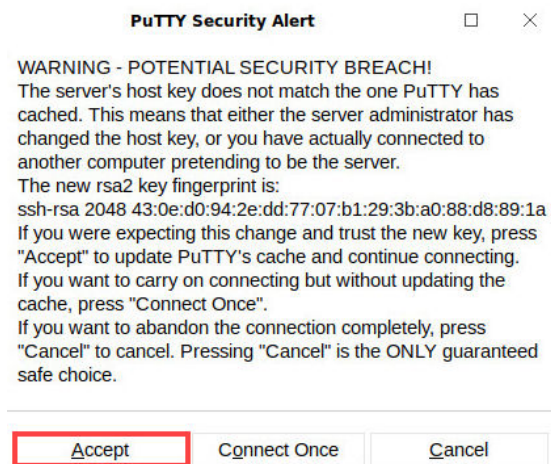
4. On the client *Desktop*, click the **Putty** icon located at the lower-left of the *Desktop*.



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



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



- When prompted for *login*, type *admin* then press **Enter**. When prompted for *Password*, type *Pa10Alt0!*.



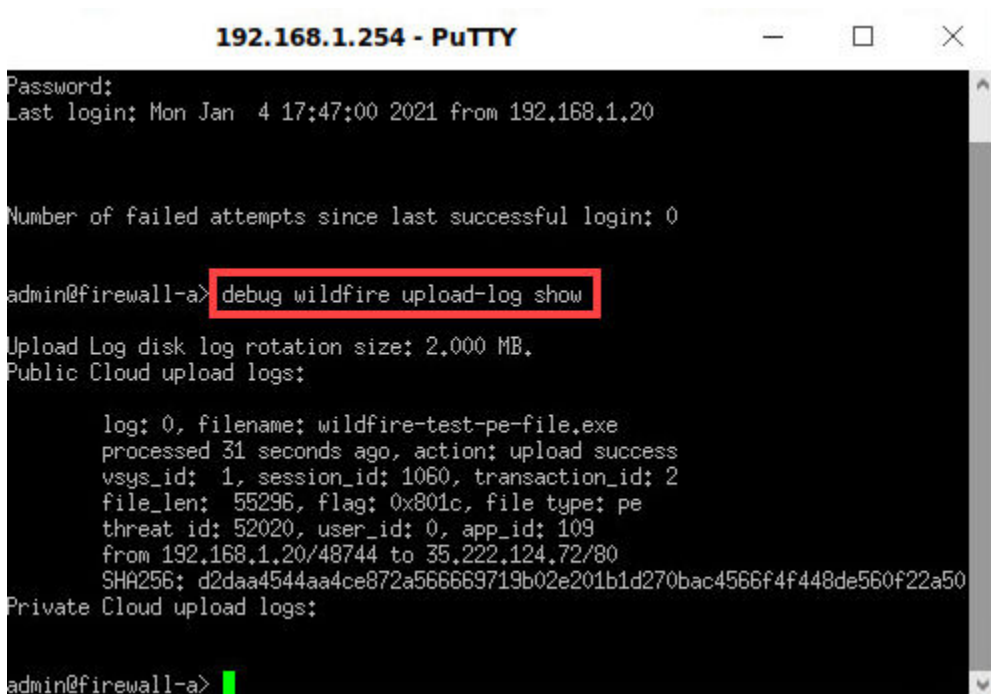
```
192.168.1.254 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Mon Jan  4 21:35:12 2021 from 192.168.1.20

Number of failed attempts since last successful login: 0

admin@firewall-a>
```

- In the *192.168.1.254 – Putty* window, enter the following CLI command

```
debug wildfire upload-log show
```



```
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>
```

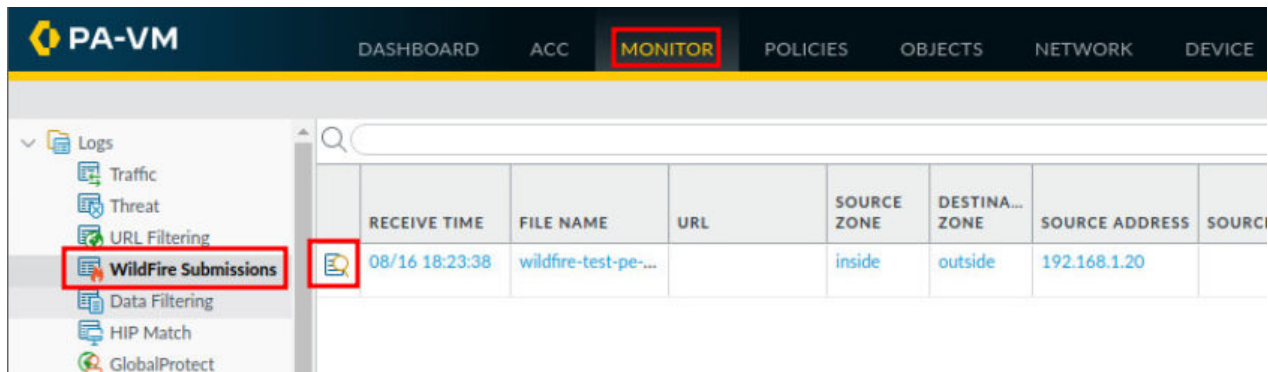
**Please
Note**

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.



The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR' (highlighted with a red box), 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. On the left sidebar, under 'Logs', 'WildFire Submissions' is highlighted with a red box. The main content area displays a table with the following data:

RECEIVE TIME	FILE NAME	URL	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	SOURCE
08/16 18:23:38	wildfire-test-pe...		inside	outside	192.168.1.20	

A magnifying glass icon is visible next to the 'wildfire-test-pe...' entry in the 'FILE NAME' column, which is also highlighted with a red box.

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	218	Source User		Destination User							
Action	allow	Source	192.168.1.20	Destination	35.222.124.72						
Application	web-browsing	Source DAG		Destination DAG							
Rule	egress-outside-content-id	Port	57026	Port	80						
Rule UUID	86b509e9-c685-4f46-8fac-479e6e9ab8b0	Zone	inside	Zone	outside						
Verdict	malicious	Interface	ethernet1/2	Interface	ethernet1/1						
Device SN	015351000081504	NAT IP		NAT IP							
		NAT Port	29205	NAT Port	80						

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/08/16 18:21:24	end	web-browsing	allow	egress-outside-content-id	86b50...	61...		lab-decrypt...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-id	86b50...		high			malicio...		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**

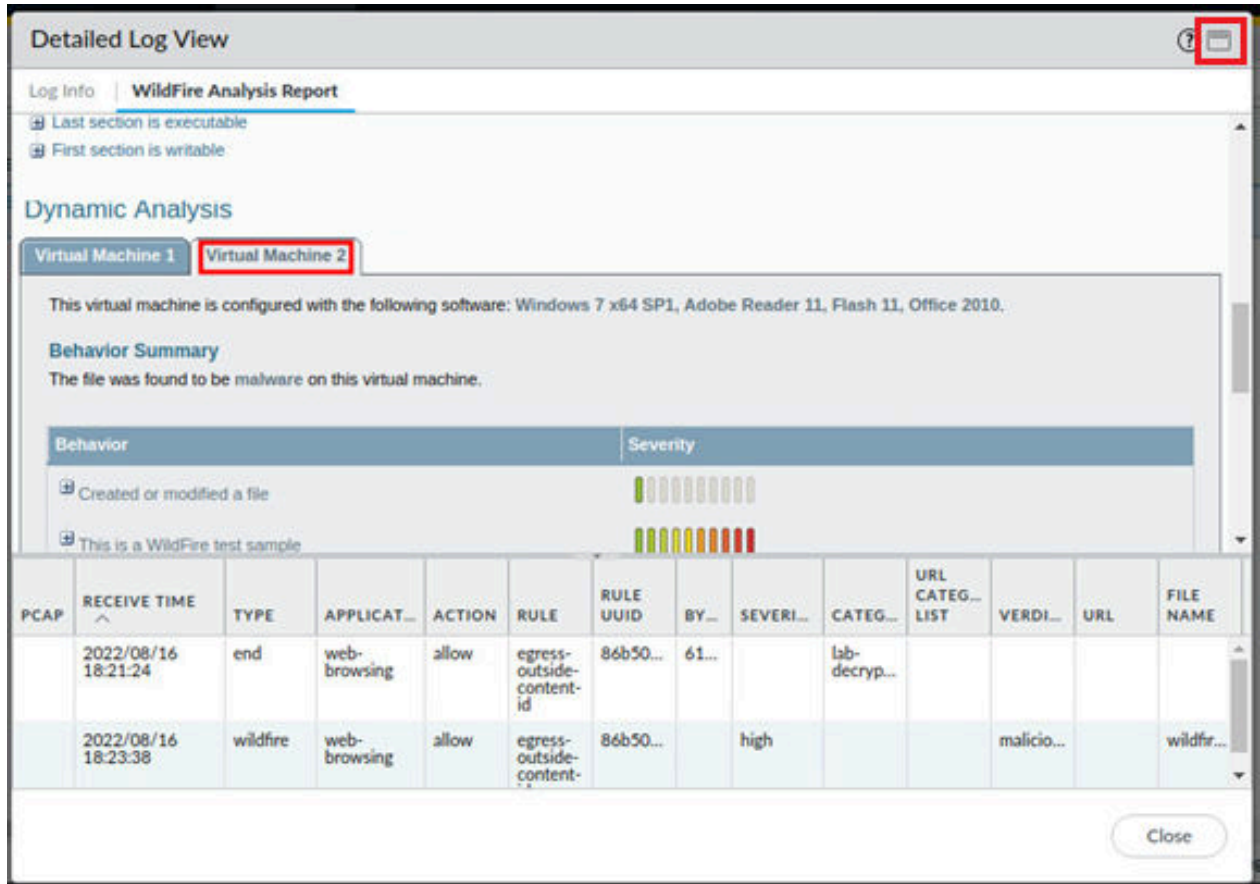
WildFire Analysis Summary [Download PDF](#)

File Information	
File Type	PE
File Signer	
SHA-256	a7f46e450e05b641f17dbccdc5ca1ea1e94b10fbc64b4f70b398911bdb6472c5
SHA1	461854d62a6a3822420e2a5c547a8680f32e7c0c
MD5	e5ec489de36be8d691c244b0c62e9558
File Size	55296 bytes
First Seen Timestamp	2022-08-16 18:18:54 UTC
Verdict	malware

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/08/16 18:21:24	end	web-browsing	allow	egress-outside-content-id	86b50...	61...		lab-decrypt...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-id	86b50...		high			malicio...		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 select the **Virtual Machine 2** tab if the report does not a file as malware in Virtual Machine 1. You may need to click the **expand** icon in the upper-right corner to better view the Wildfire Analysis Report.



Detailed Log View

Log Info | **WildFire Analysis Report**

Log Info

- Last section is executable
- First section is writable

Dynamic Analysis

Virtual Machine 1 | **Virtual Machine 2**

This virtual machine is configured with the following software: Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010.

Behavior Summary

The file was found to be malware on this virtual machine.

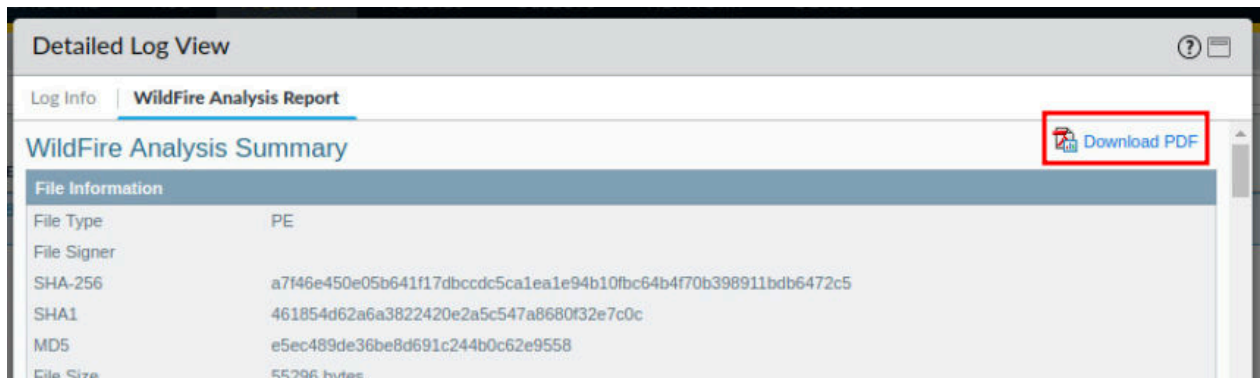
Behavior

- Created or modified a file
- This is a WildFire test sample

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/08/16 18:21:24	end	web-browsing	allow	egress-outside-content-id	86b50...	61...		lab-decrypt...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-id	86b50...		high			malicio...		wildfir...

Close

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



Detailed Log View

Log Info | **WildFire Analysis Report**

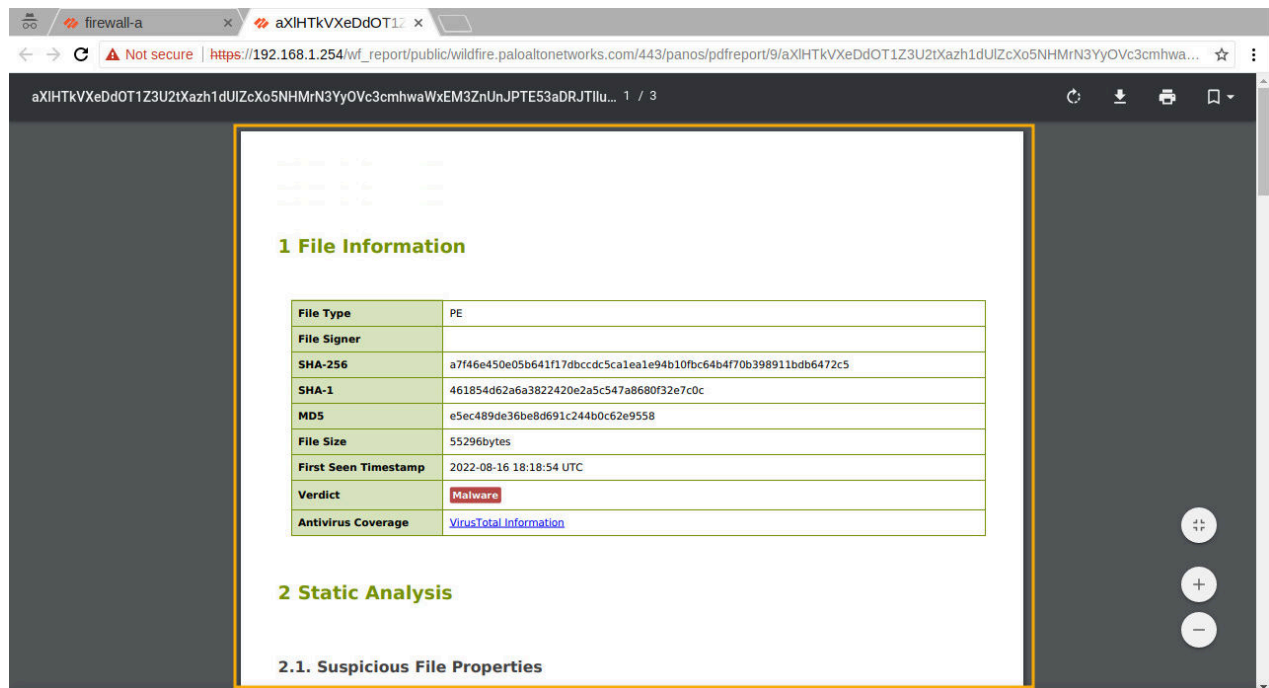
WildFire Analysis Summary

[Download PDF](#)

File Information

File Type	PE
File Signer	
SHA-256	a7f46e450e05b641f17dbccdc5ca1ea1e94b10fbc64b4f70b398911bdb6472c5
SHA1	461854d62a6a3822420e2a5c547a8680f32e7c0c
MD5	e5ec489de36be8d691c244b0c62e9558
File Size	55296 bytes

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.