CYBERSECURITY FOUNDATION V2

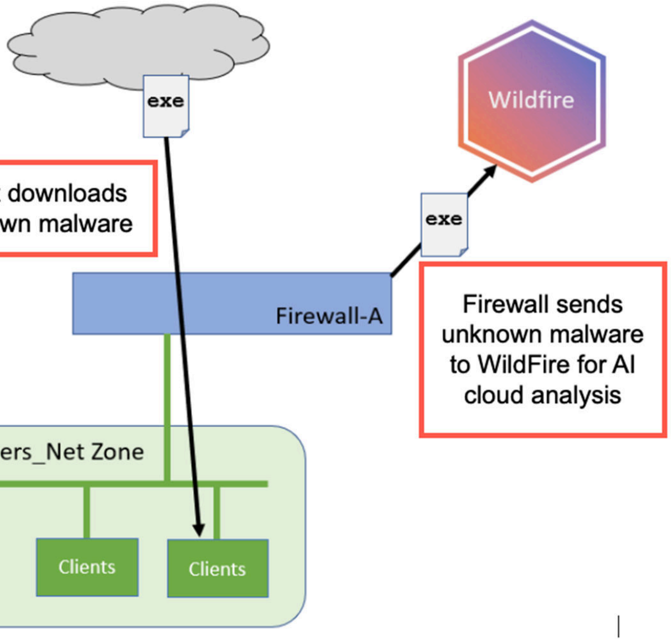
Lab 2: Malware Analysis

Document Version: 2022-12-22

Contents

Introduction

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

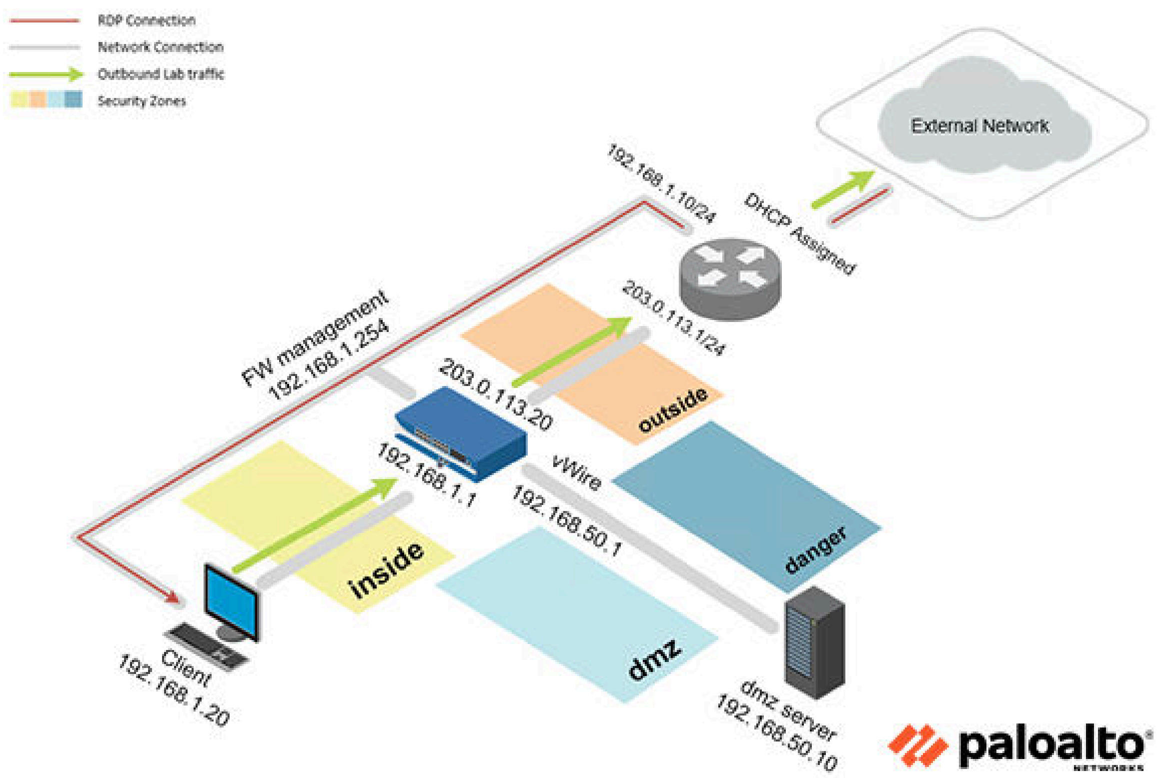

exe
Wildfire
Client downloads unknown malware
exe
Firewall-A
Firewall sends unknown malware to WildFire for AI cloud analysis
Users_Net Zone
Clients
Clients

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.

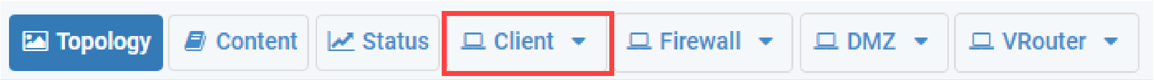
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Malware Analysis

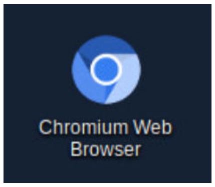
1.0 Load Lab Configuration

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

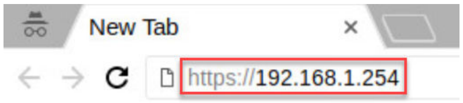
1. Click on the **Client** tab to access the Client PC.



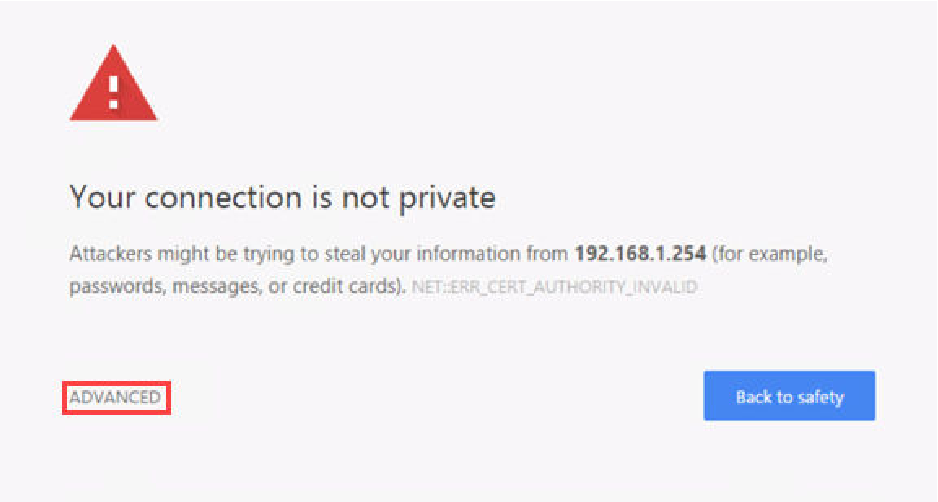
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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.

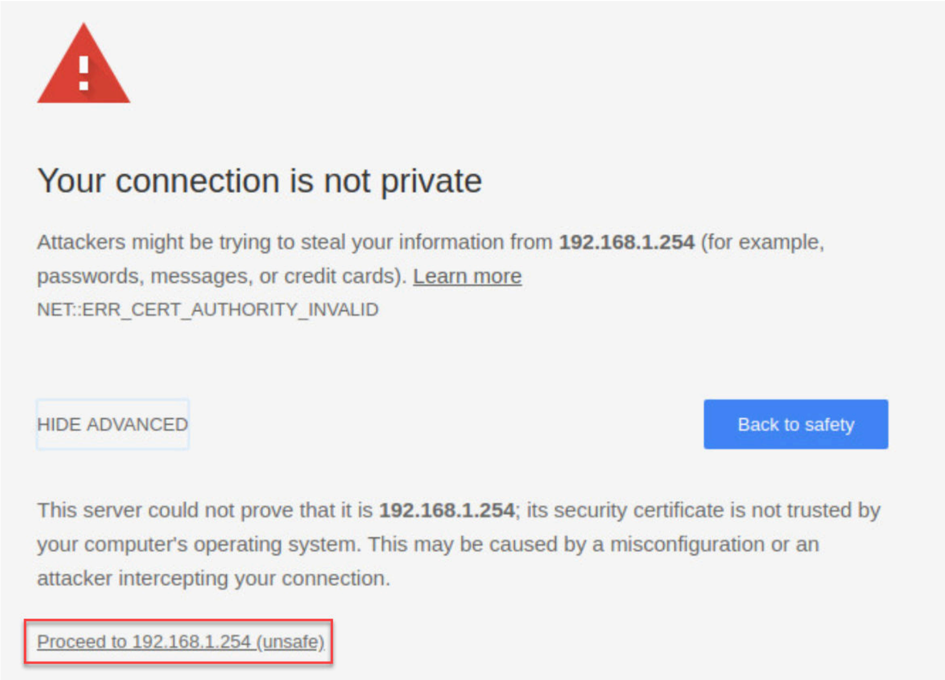


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.



Your connection is not private

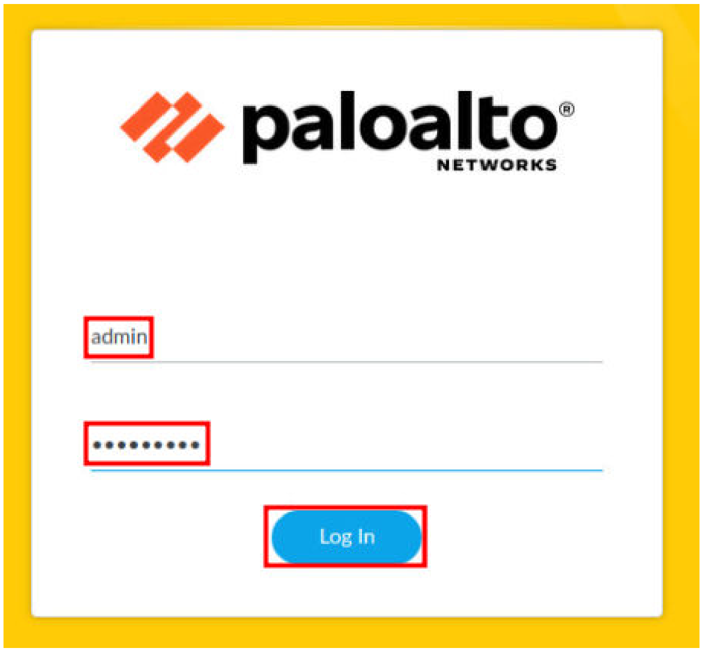
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.254 (unsafe)

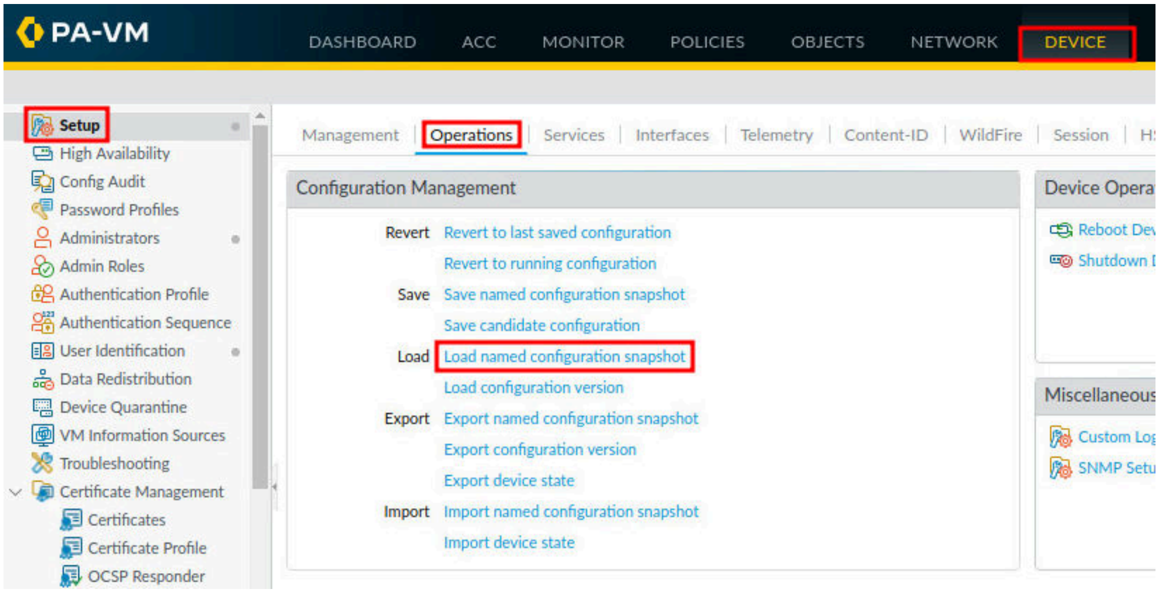
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



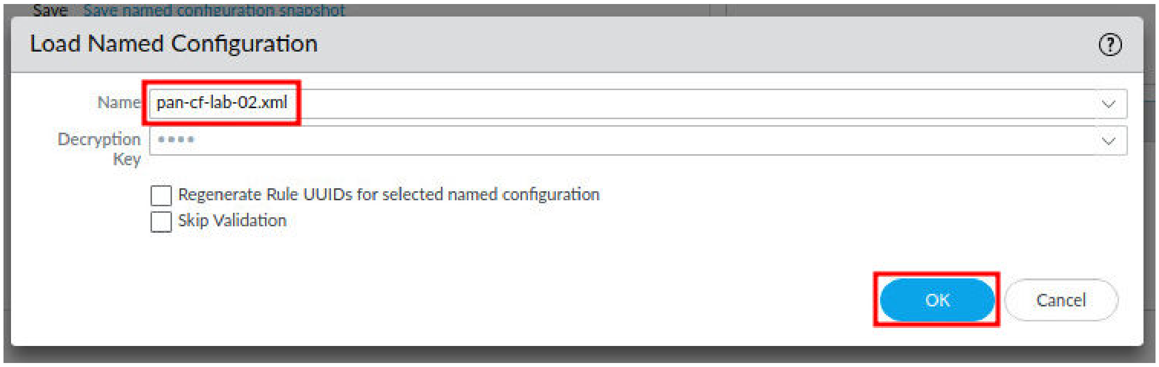
admin

•••••••••

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**.


Load Named Configuration

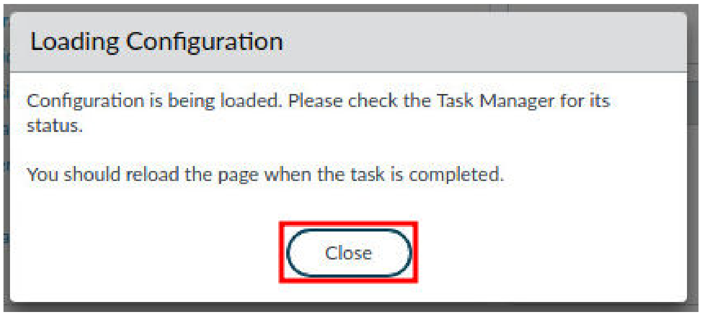
Name pan-cf-lab-02.xml

Decryption Key ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

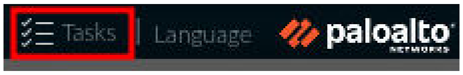
10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

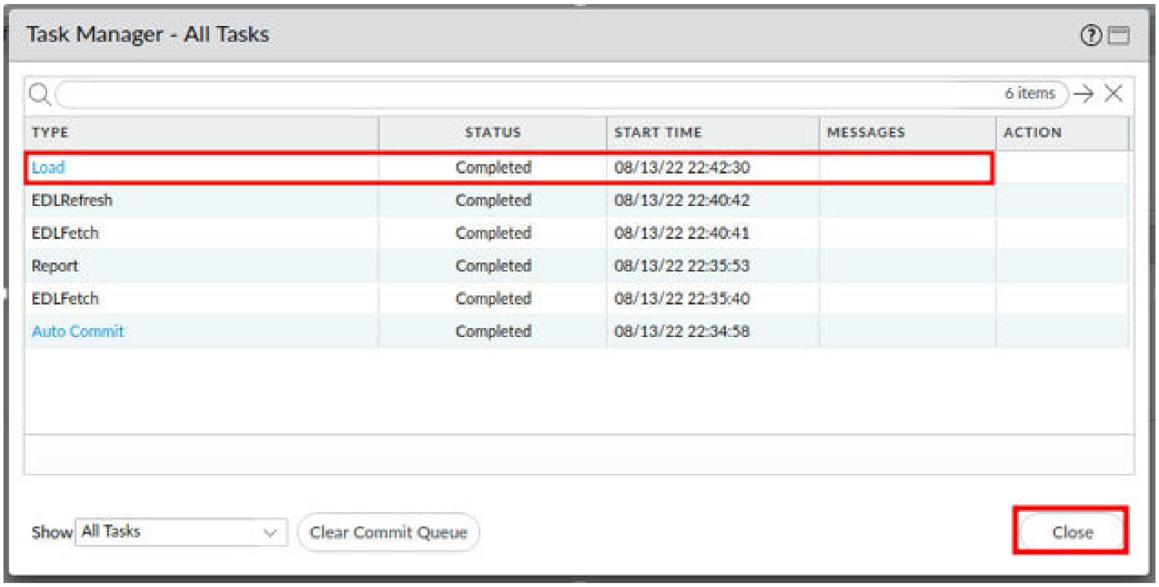
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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.**

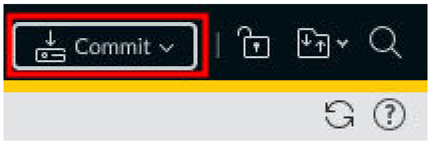


Task Manager - All Tasks

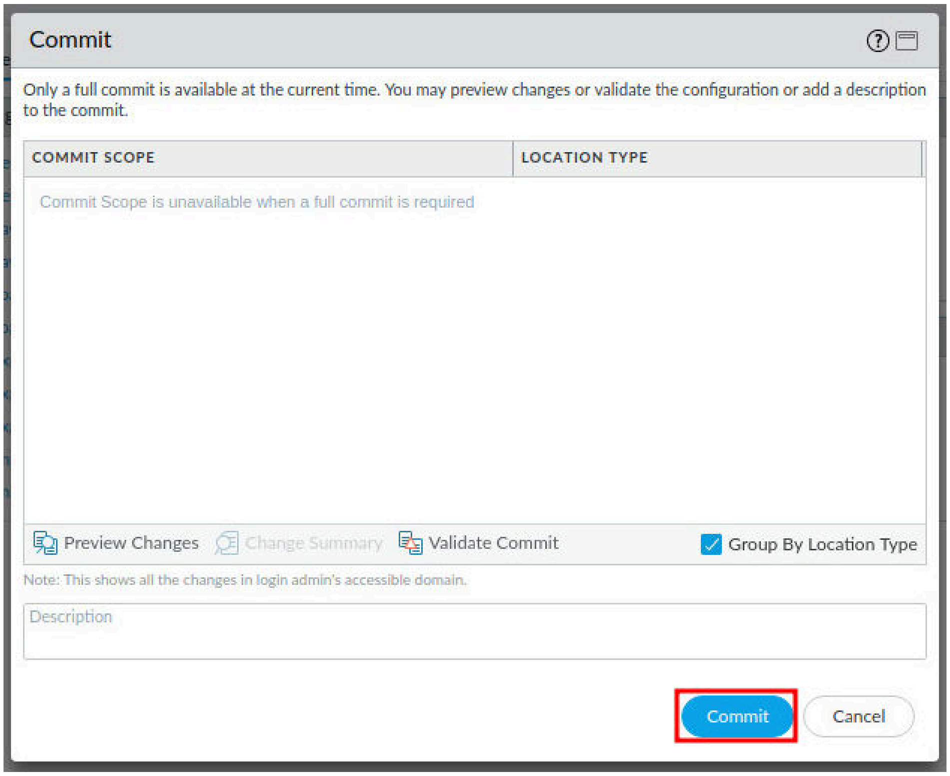
6 items

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.



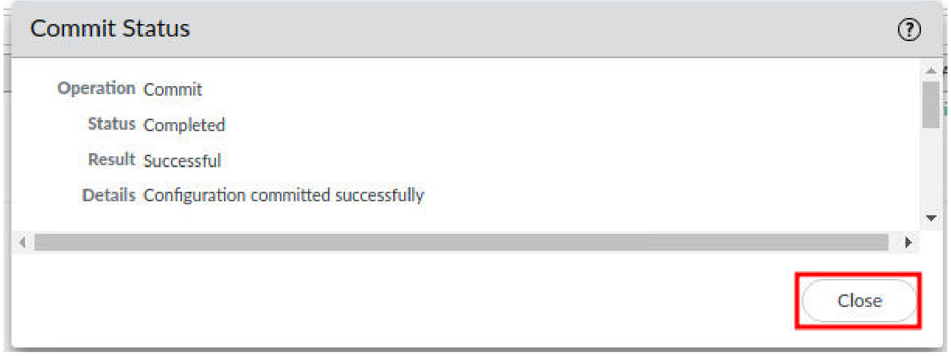
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

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

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



Commit Status

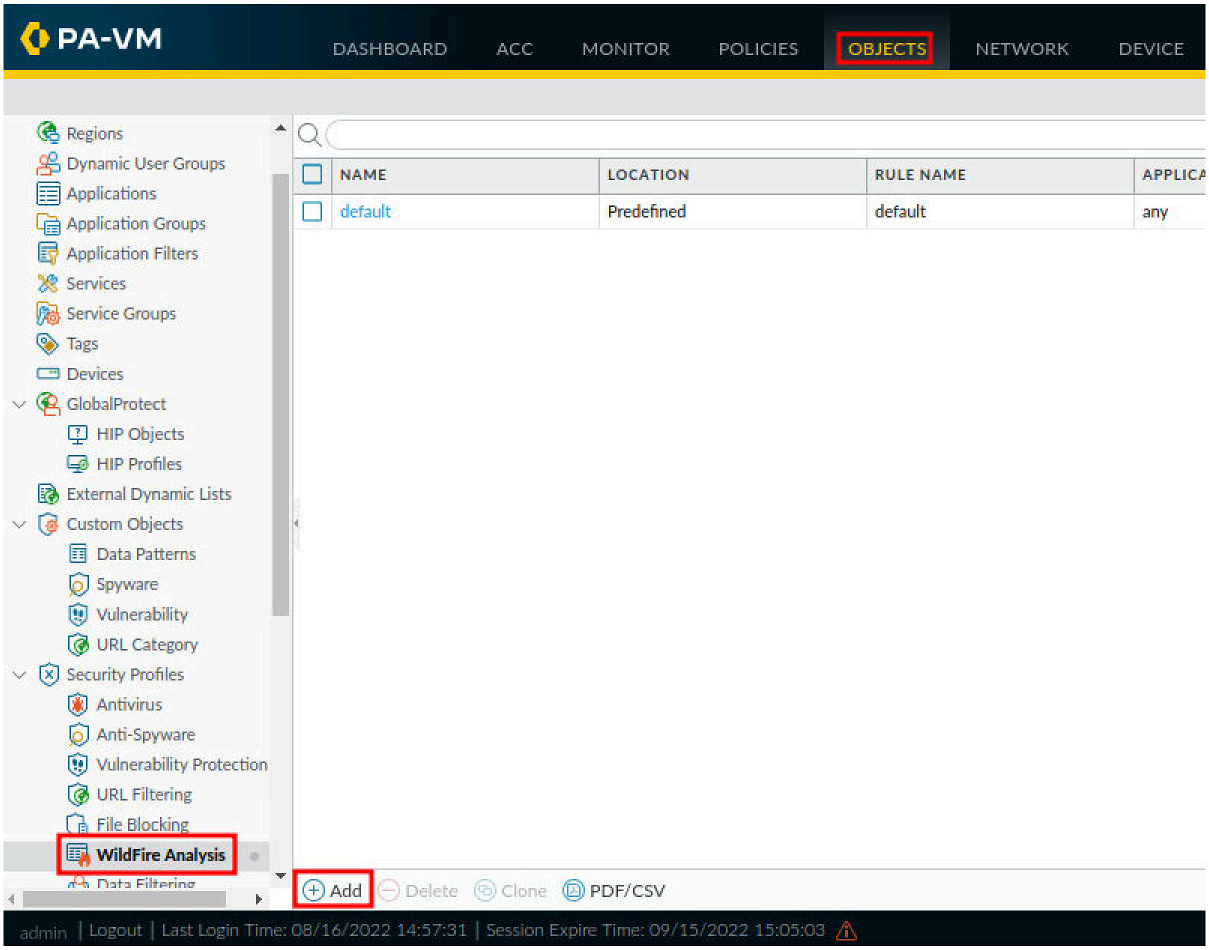
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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.

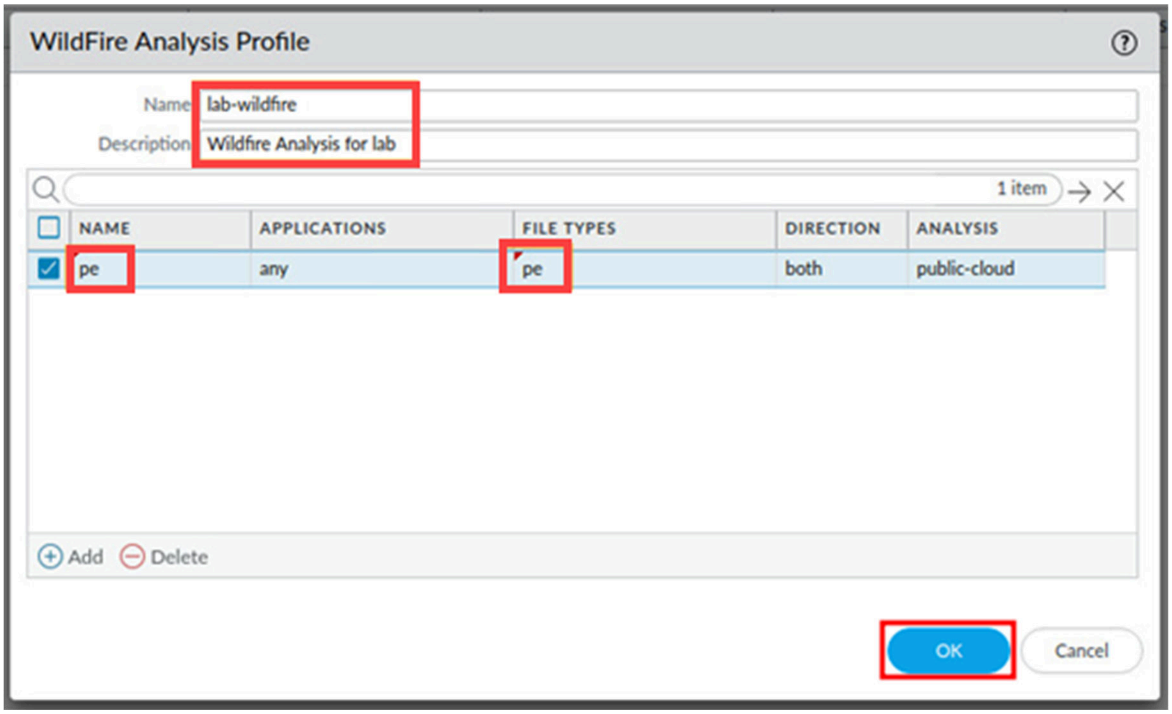
1. Navigate to **Objects > Security Profiles > Wildfire Analysis**. Click **Add**.



NAME	LOCATION	RULE NAME	APPLICA
default	Predefined	default	any

admin | Logout | Last Login Time: 08/16/2022 14:57:31 | Session Expire Time: 09/15/2022 15:05:03

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**.



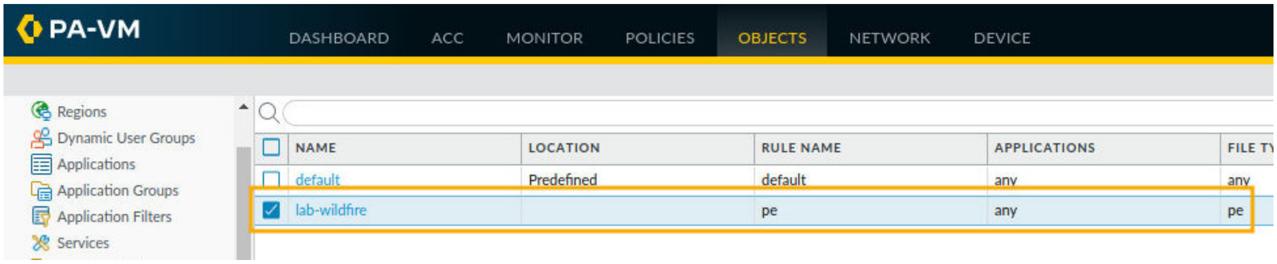
WildFire Analysis Profile

Name: lab-wildfire

Description: Wildfire Analysis for lab

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

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

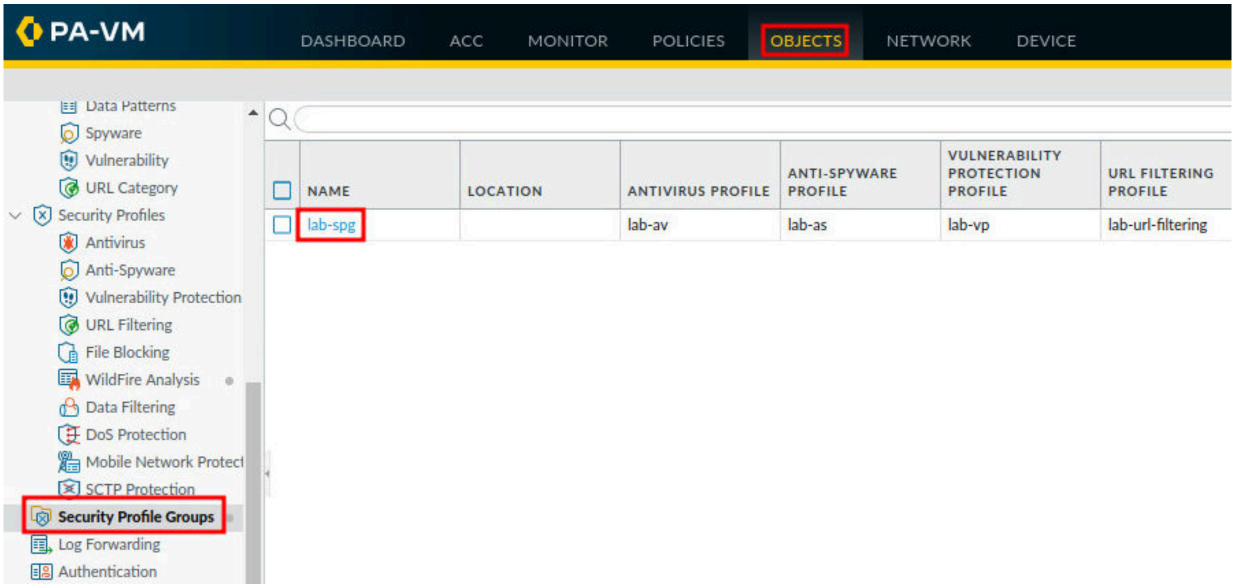


☐	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TY
☐	default	Predefined	default	any	any
☑	lab-wildfire		pe	any	pe

1.2 Modify a Security Profile Group

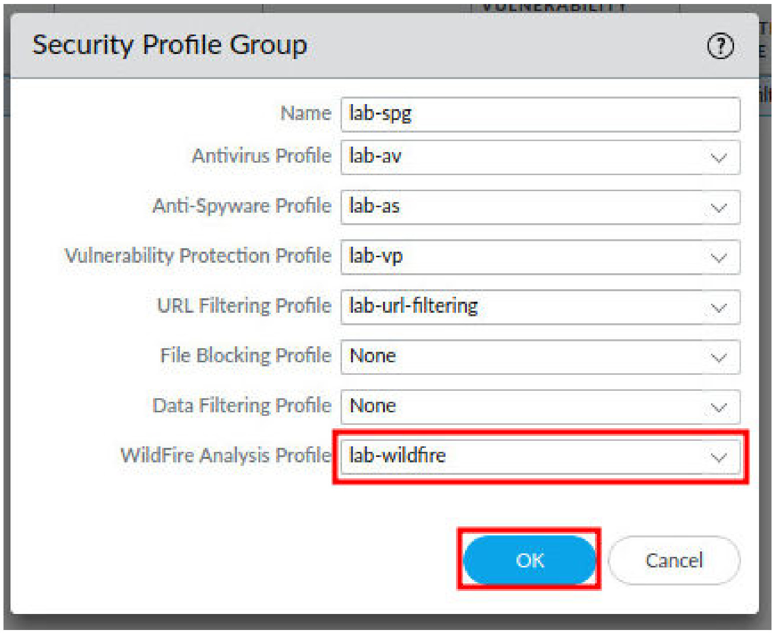
In this section, you will add the **lab-wildfire** analysis profile to the *lab-spg* security profile group.

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



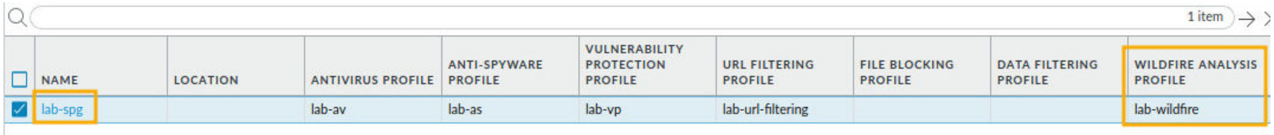
□	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE
□	lab-spg		lab-av	lab-as	lab-vp	lab-url-filtering

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



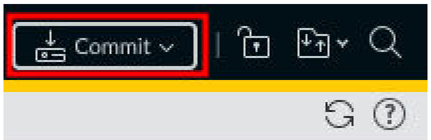
Name	lab-spg
Antivirus Profile	lab-av
Anti-Spyware Profile	lab-as
Vulnerability Protection Profile	lab-vp
URL Filtering Profile	lab-url-filtering
File Blocking Profile	None
Data Filtering Profile	None
WildFire Analysis Profile	lab-wildfire

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

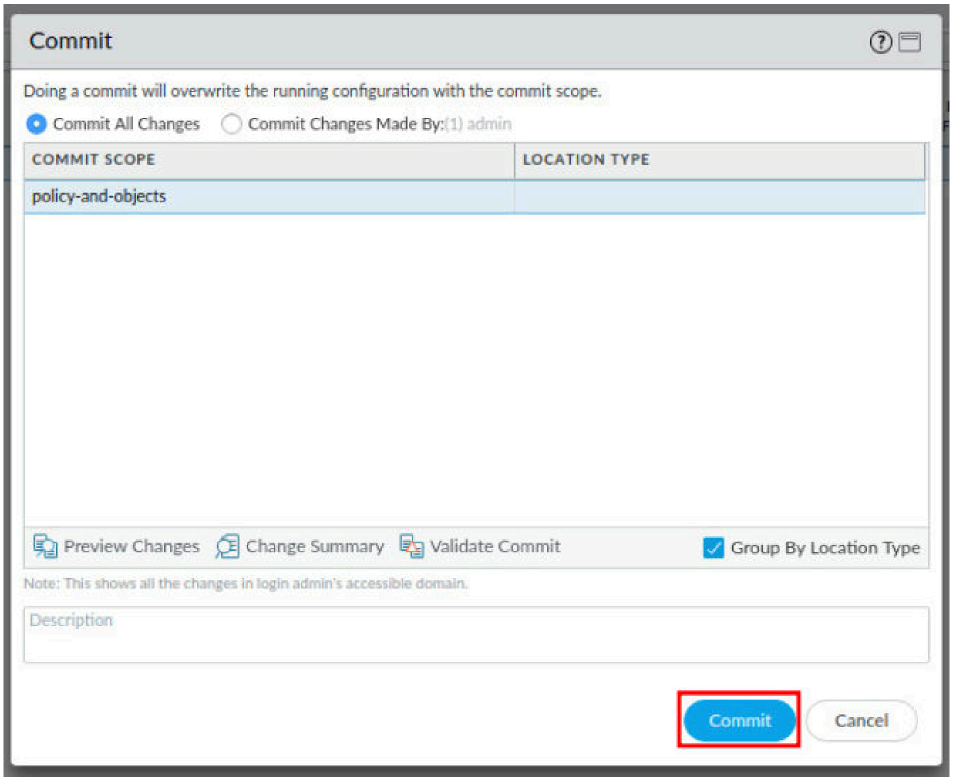


☐	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
☑	lab-spg		lab-av	lab-as	lab-vp	lab-url-filtering			lab-wildfire

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.



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

● Commit All Changes ○ Commit Changes Made By:(1) admin

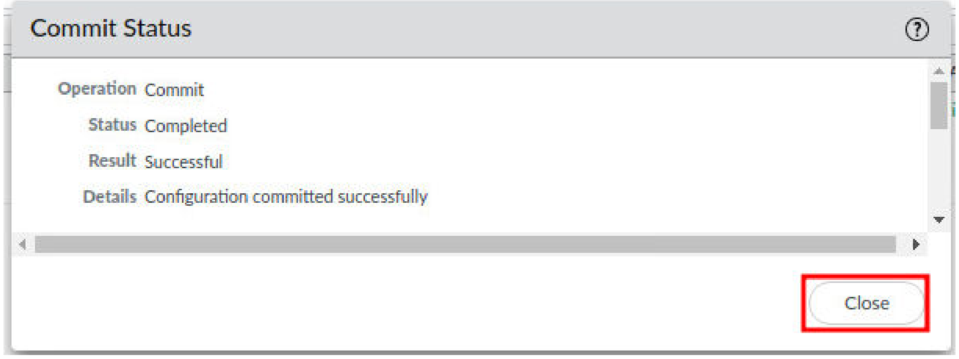
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

☑ Group By Location Type

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

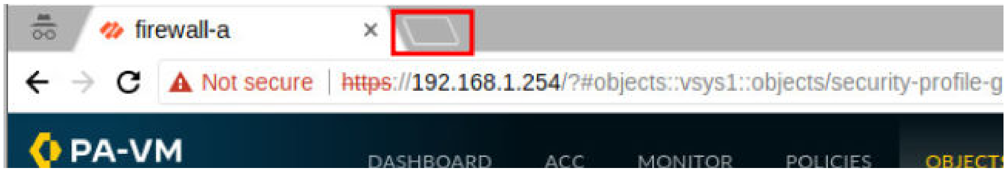
Description

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



Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

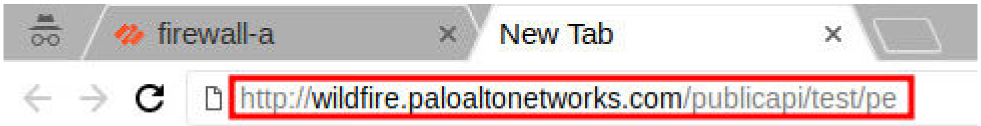
7. Open a new *Chromium* tab and continue to the next task.


firewall-a
Not secure
https://192.168.1.254/?#objects::vsys1::objects/security-profile-g
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS

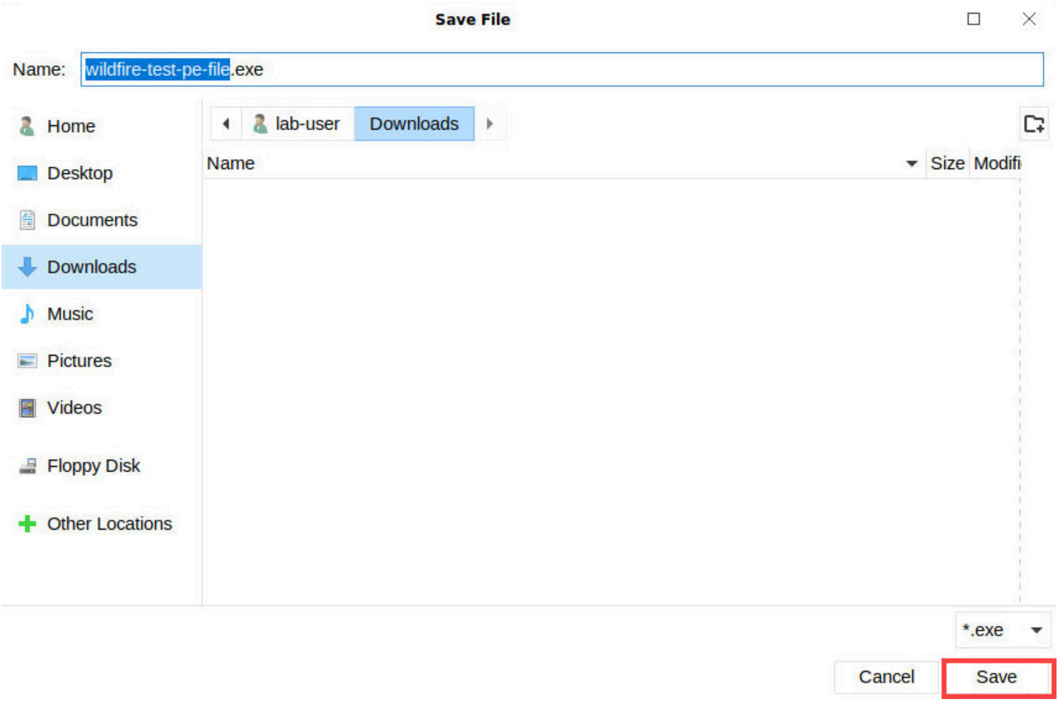
1.3 Test the WildFire Analysis Profile

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

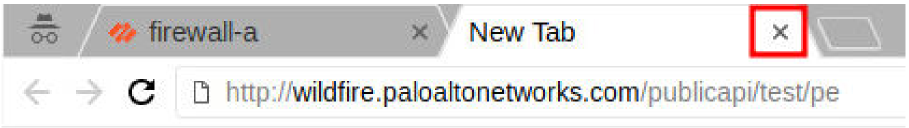
1. On the new *Chromium* tab, enter `http://wildfire.paloaltonetworks.com/publicapi/test/pe` in the address bar and press **Enter**. Do not open the file.



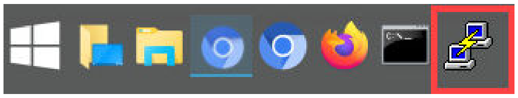
2. In the *Save File* window, leave the defaults and click **Save**.



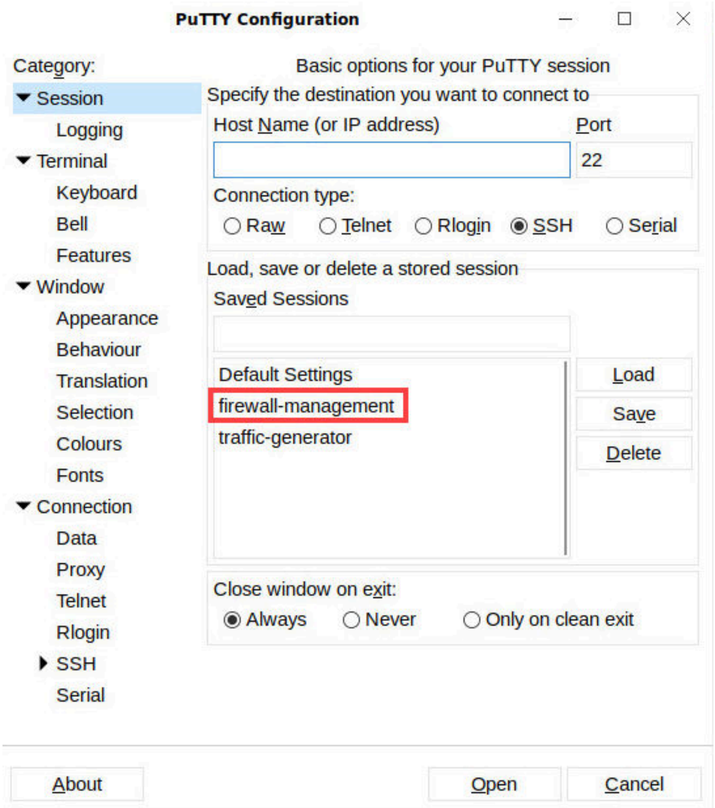
3. Close the *Chromium* tab that was used to download the attack file.



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**.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

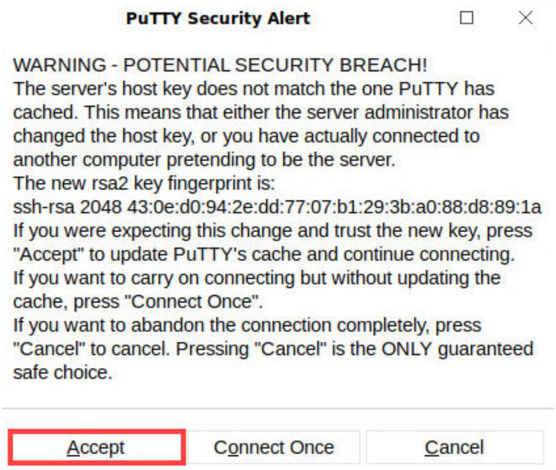
Load, save or delete a stored session

Saved Sessions

Default Settings
firewall-management
traffic-generator

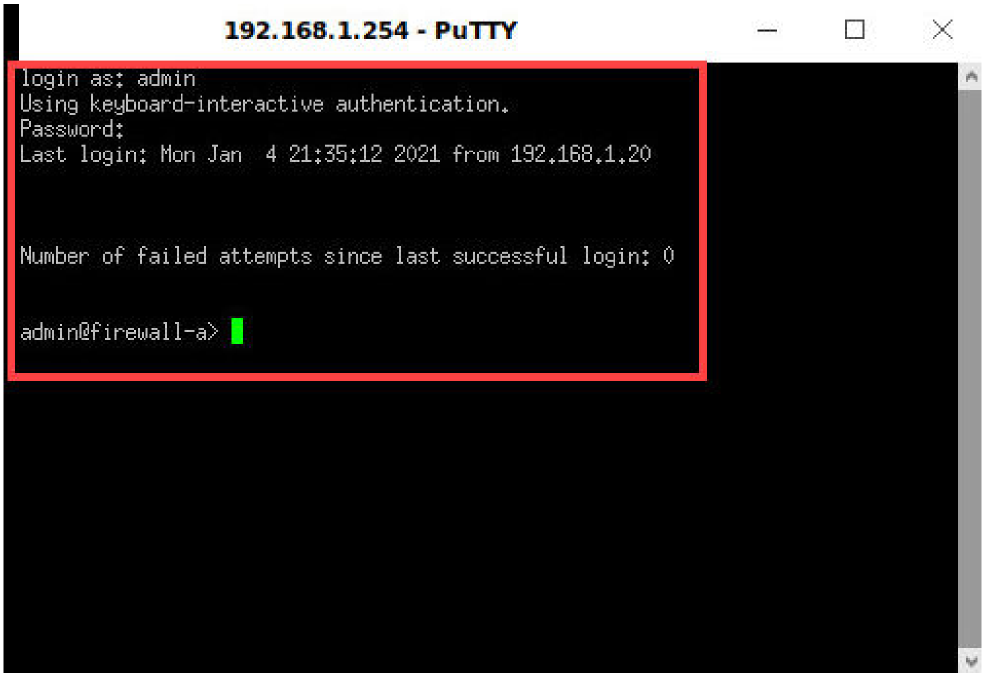
Close window on exit: ● Always ○ Never ○ Only on clean exit

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



WARNING - POTENTIAL SECURITY BREACH!
The server's host key does not match the one PuTTY has cached. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 2048 43:0e:d0:94:2e:dd:77:07:b1:29:3b:a0:88:d8:89:1a
If you were expecting this change and trust the new key, press "Accept" to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, press "Connect Once".
If you want to abandon the connection completely, press "Cancel" to cancel. Pressing "Cancel" is the ONLY guaranteed safe choice.

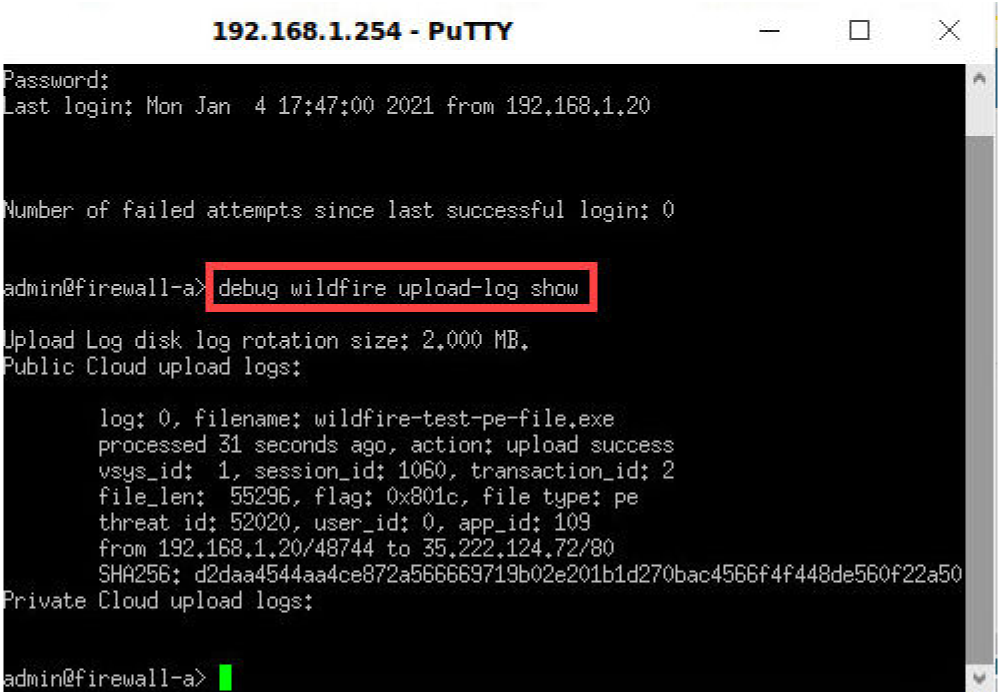
7. When prompted for *login*, type `admin` then press **Enter**. When prompted for *Password*, type `Pal0Alt0!`.



```
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>
```

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

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

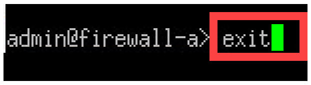


```
Password:
Last login: Mon Jan  4 17:47:00 2021 from 192.168.1.20


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

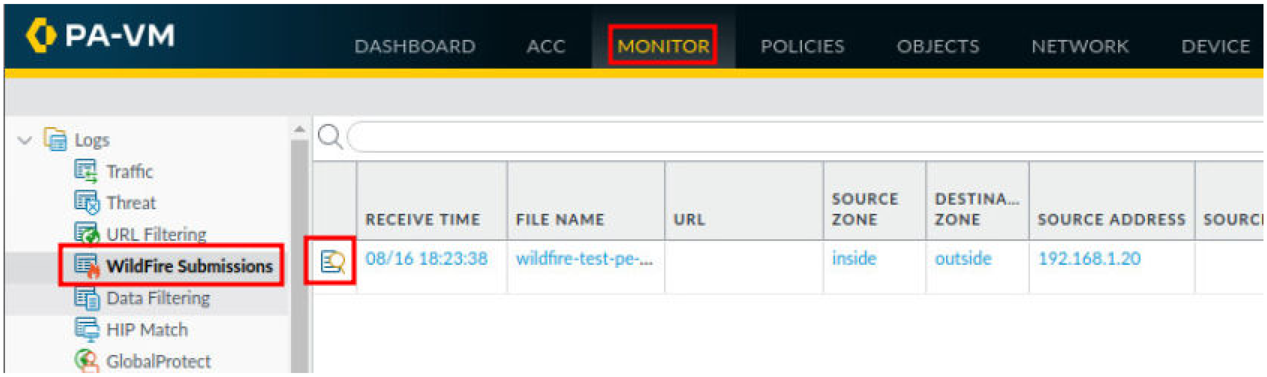
The command should display the output **`log: 0, filename: wildfire-test-pe-file.exe processed…`** This output verifies that the file was uploaded to the WildFire public cloud. The message might take a minute or two to appear.

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



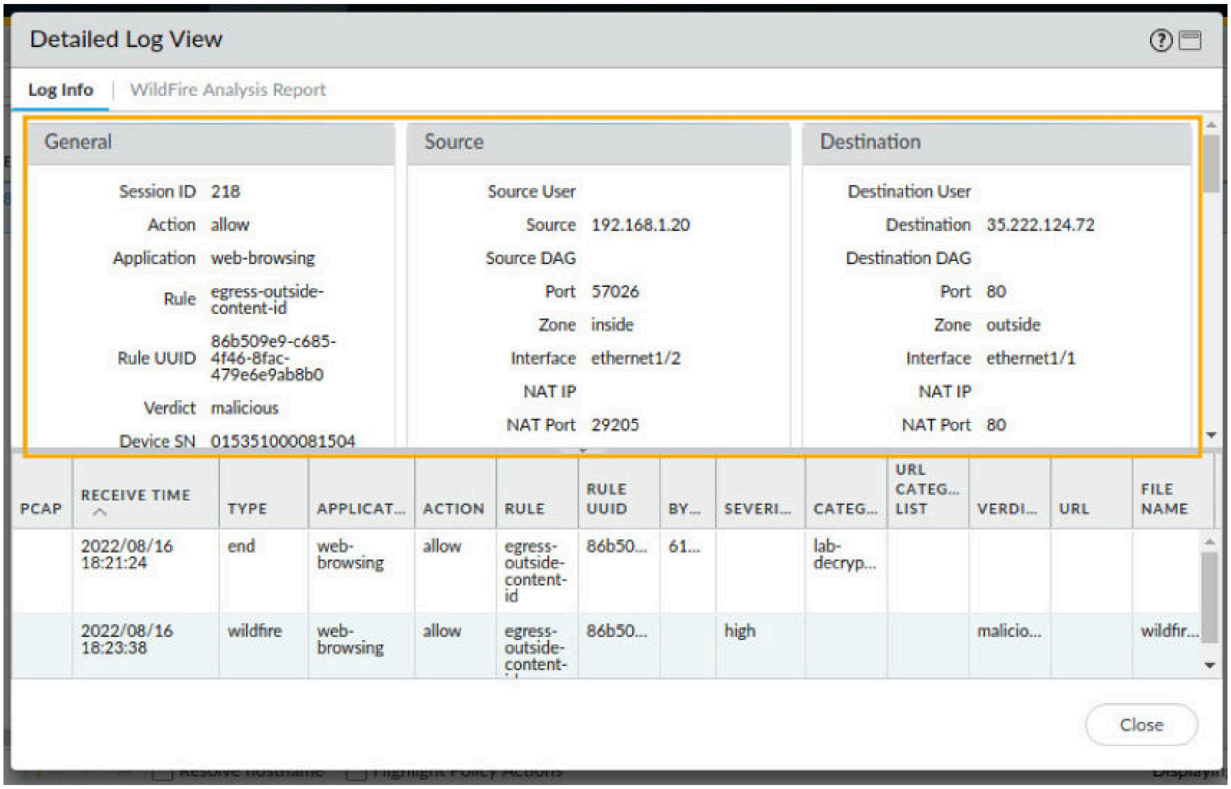
```
admin@firewall-a> exit
```

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.



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

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



Detailed Log View

General

Session ID	218
Action	allow
Application	web-browsing
Rule	egress-outside-content-id
Rule UUID	86b509e9-c685-4f46-8fac-479e6e9ab8b0
Verdict	malicious
Device SN	015351000081504

Source

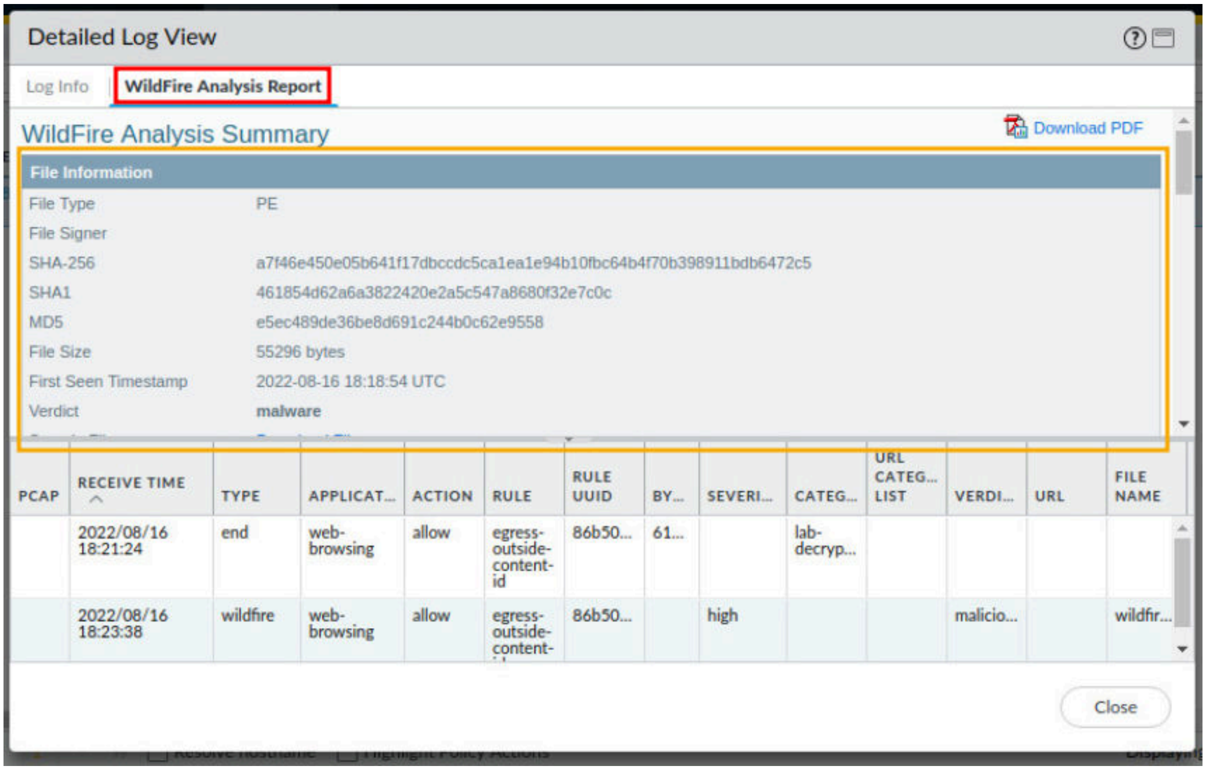
Source User	
Source	192.168.1.20
Source DAG	
Port	57026
Zone	inside
Interface	ethernet1/2
NAT IP	
NAT Port	29205

Destination

Destination User	
Destination	35.222.124.72
Destination DAG	
Port	80
Zone	outside
Interface	ethernet1/1
NAT IP	
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-decryp...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-	86b50...		high			malicio...		wildfir...

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



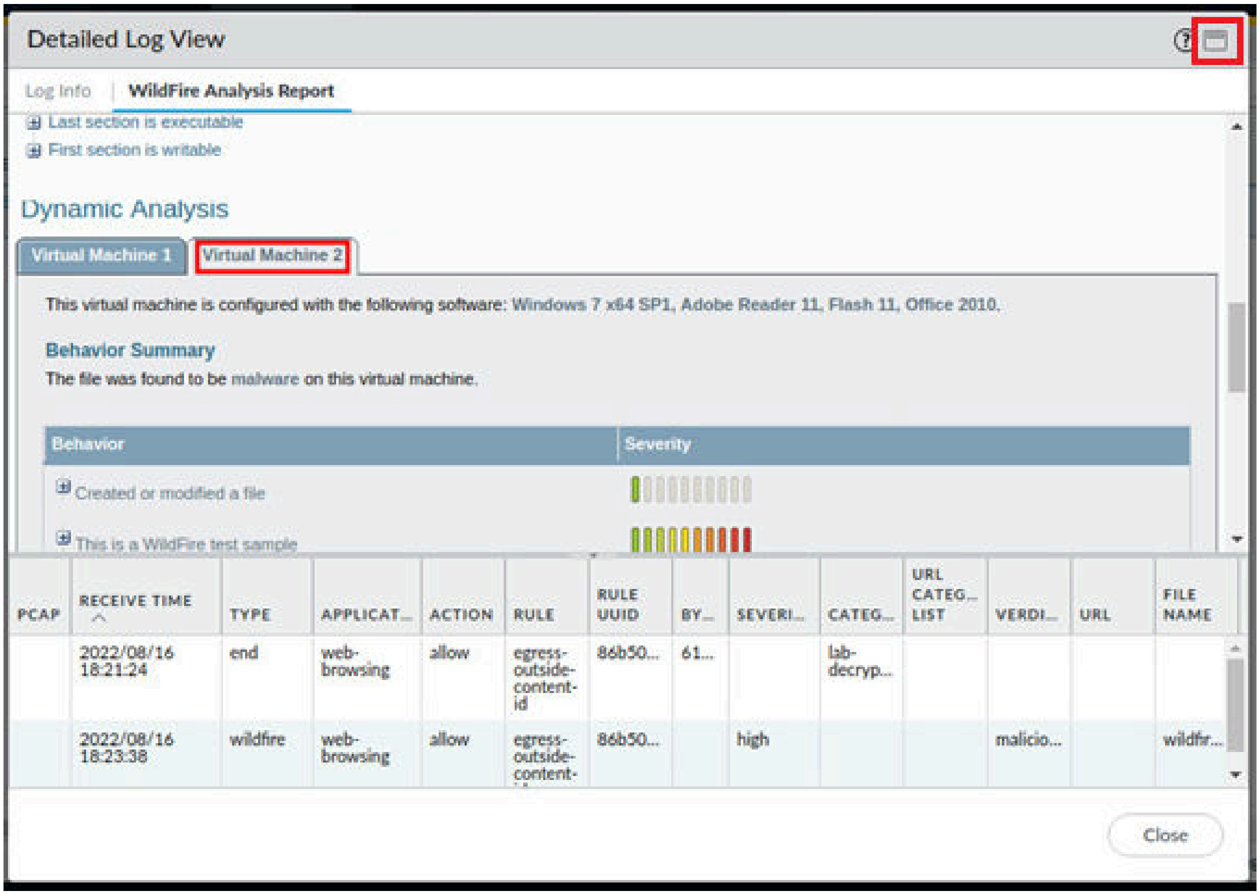
Detailed Log View

WildFire Analysis Summary

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-decryp...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-	86b50...		high			malicio...		wildfir...

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 many 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.



Dynamic Analysis

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

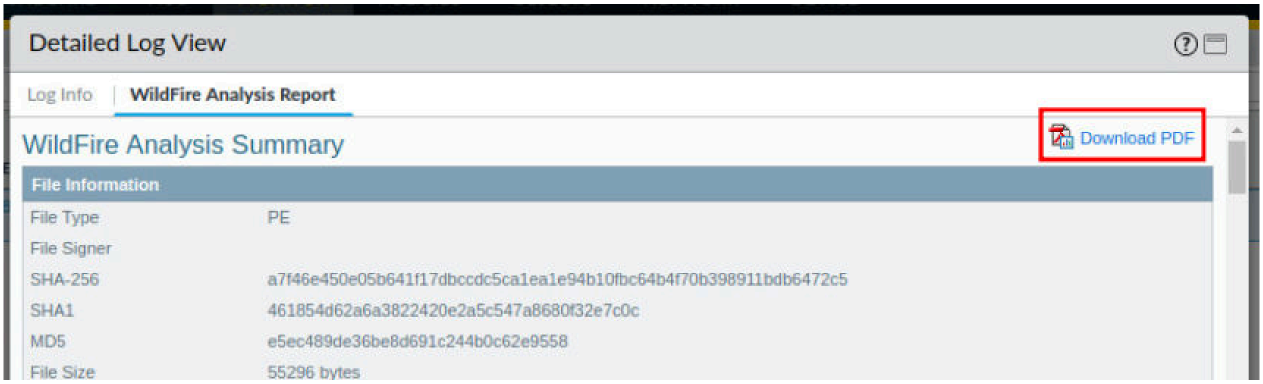
Behavior Summary

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

Behavior	Severity
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... LIST	VERDI...	URL	FILE NAME
	2022/08/16 18:21:24	end	web-browsing	allow	egress-outside-content-id	86b50...	61...		lab-decryp...				
	2022/08/16 18:23:38	wildfire	web-browsing	allow	egress-outside-content-	86b50...		high			malicio...		wildfir...

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

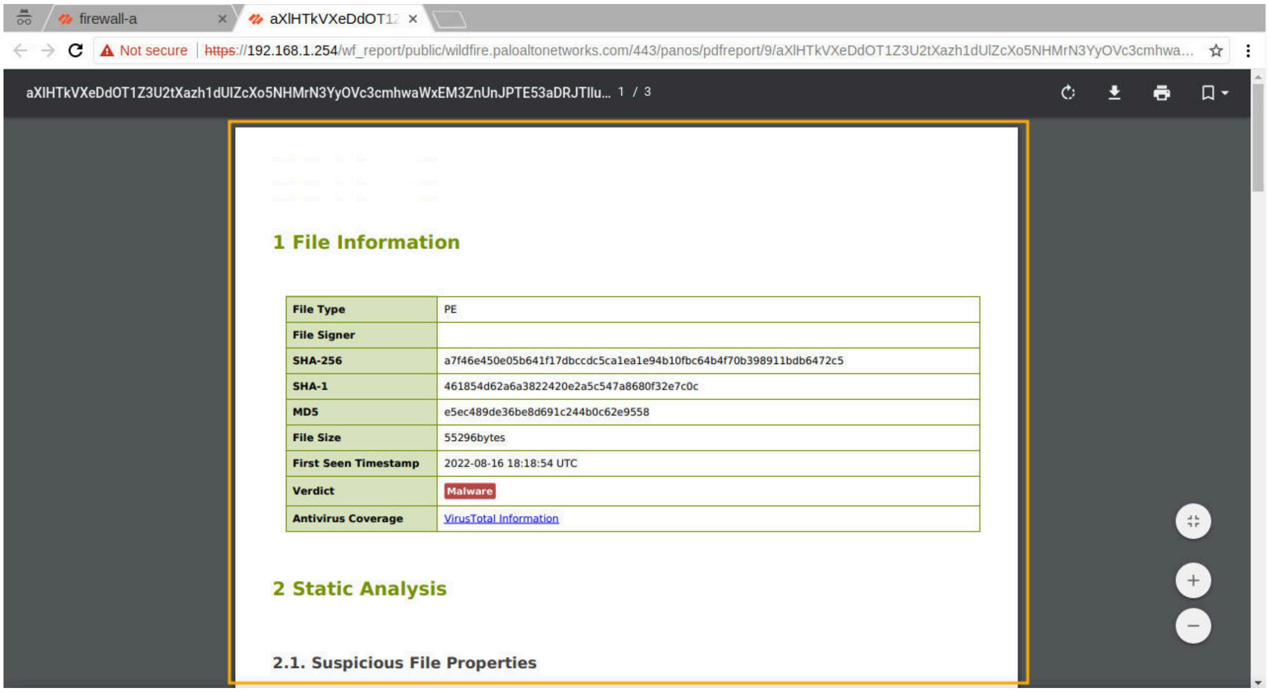


WildFire Analysis Summary

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.



firewall-a
aXlHTkVXeDdOT12
Not secure
https://192.168.1.254/wf_report/public/wildfire.paloaltonetworks.com/443/panos/pdfreport/9/aXlHTkVXeDdOT1Z3U2tXazh1dUlZcXo5NHMrN3YyOVc3cmhwa...
aXlHTkVXeDdOT1Z3U2tXazh1dUlZcXo5NHMrN3YyOVc3cmhwaWxEM3ZnUnJPTE53aDRJTllu... 1 / 3

1 File Information

File Type	PE
File Signer	
SHA-256	a7f46e450e05b641f17dbccdc5ca1ea1e94b10fbc64b4f70b398911bdb6472c5
SHA-1	461854d62a6a3822420e2a5c547a8680f32e7c0c
MD5	e5ec489de36be8d691c244b0c62e9558
File Size	55296bytes
First Seen Timestamp	2022-08-16 18:18:54 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

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.