PALO ALTO NETWORKS EDU 210

Lab 12: Blocking Unknown Malware with Wildfire

Document Version: 2022-07-18

Contents

Introduction

Your company has recently seen an increase in malicious files being downloaded by users. You have sent out informational emails explaining how much damage these types of files can do, and you have told people not to download files from “sketchy” sources.

Fortunately, you have deployed the Palo Alto Networks firewall, and you can set up a Security Profile that will send any unknown files to the WildFire cloud for analysis.

To test the Security Profile after you have configured it, you will download a test file from Palo Alto Networks. This test file is not actually malicious, but WildFire will identify it as such.

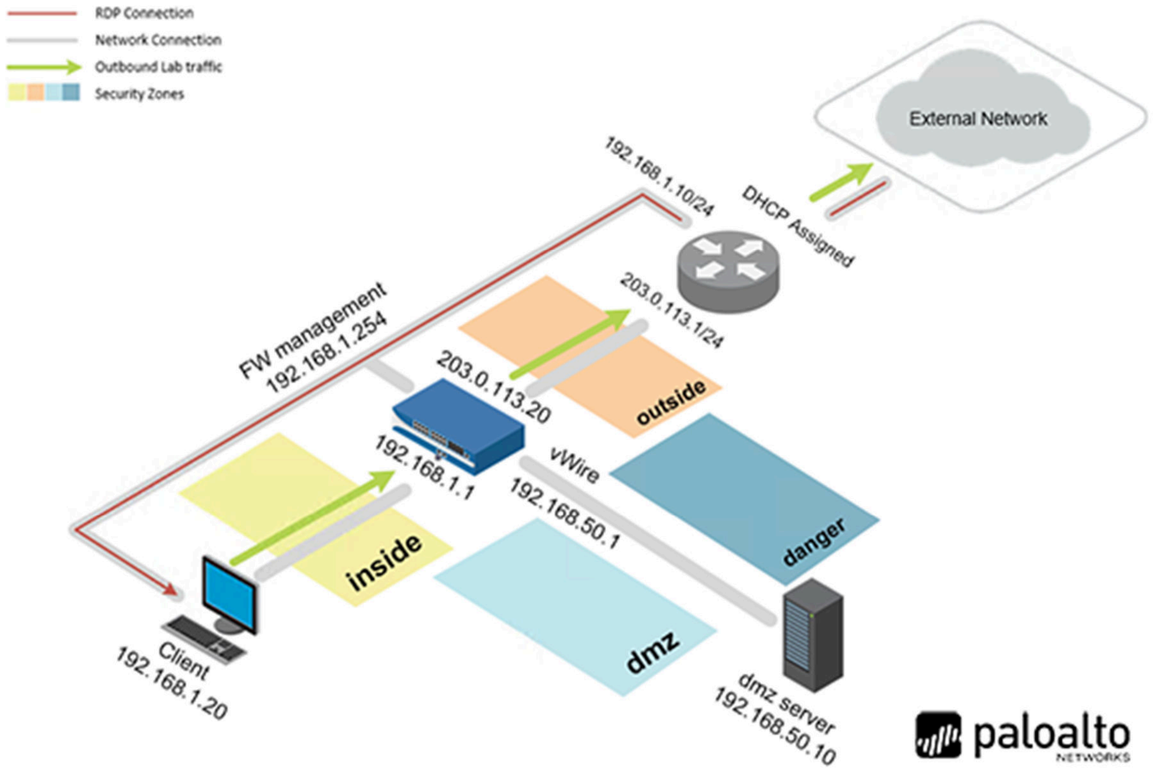
You will then examine a detailed report from WildFire with information about the file that was analyzed.

Objective

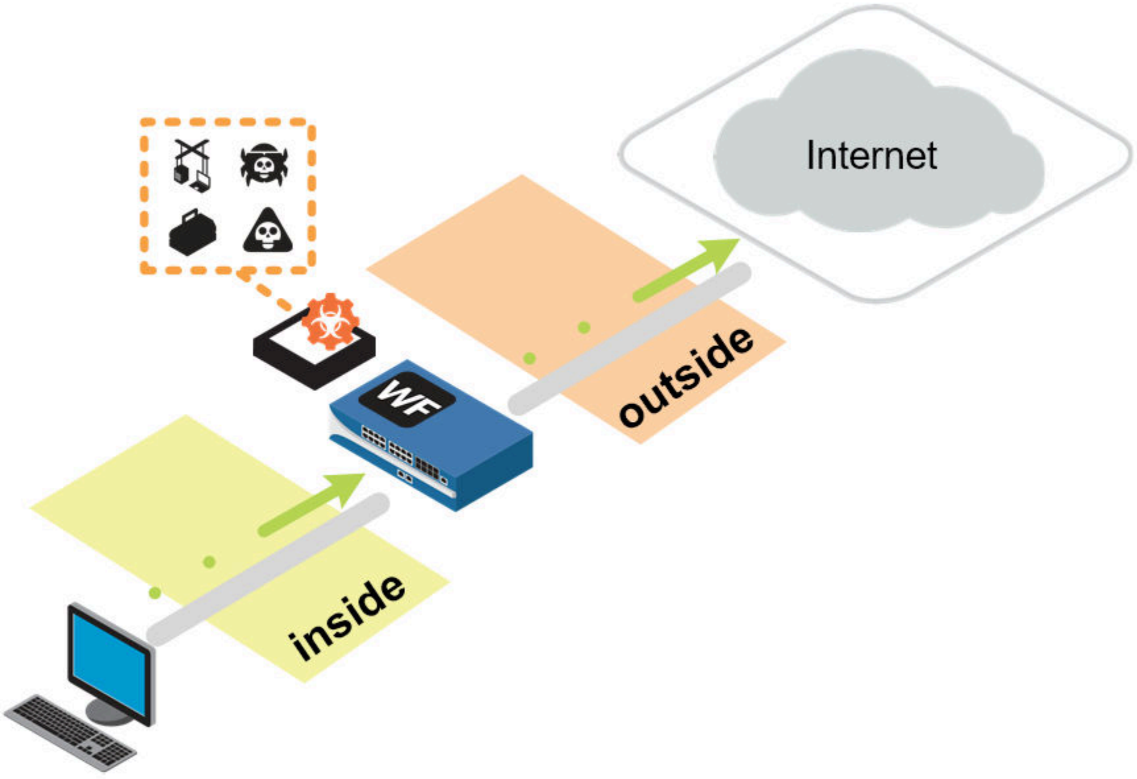
In this lab, you will perform the following tasks:

- Create a WildFire Analysis Profile
- Apply Wildfire Profile to security rules
- Test the Wildfire Analysis Profile
- Examine Wildfire analysis details

Lab Topology



Theoretical Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

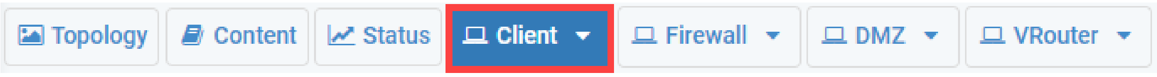
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Blocking Threats with User-ID

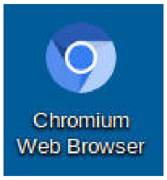
1.1 Apply a Baseline Configuration to the Firewall

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

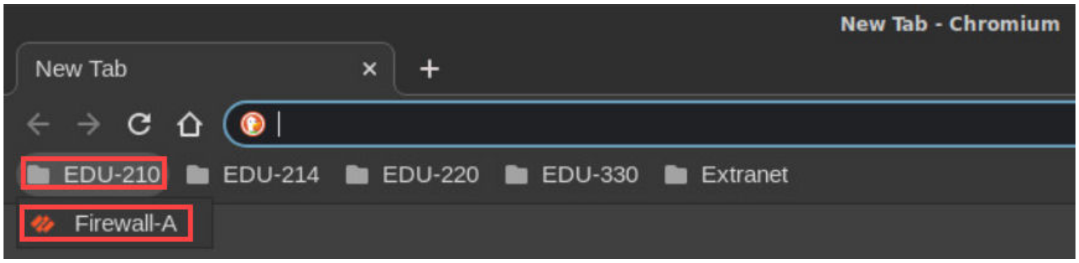
1. Click on the **Client** tab to access the Client PC.



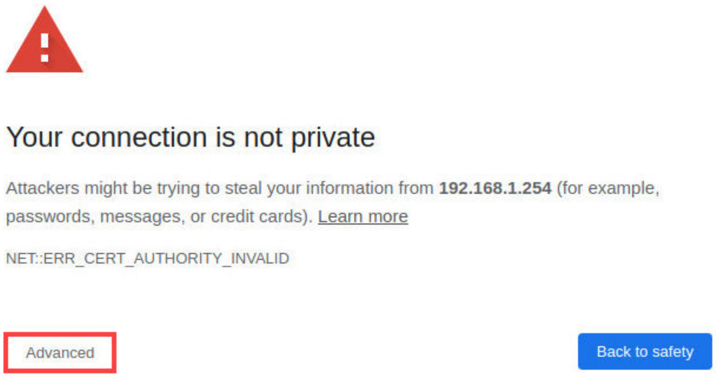
2. Double-click the **Chromium Web Browser** icon located on the desktop.



3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.



4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



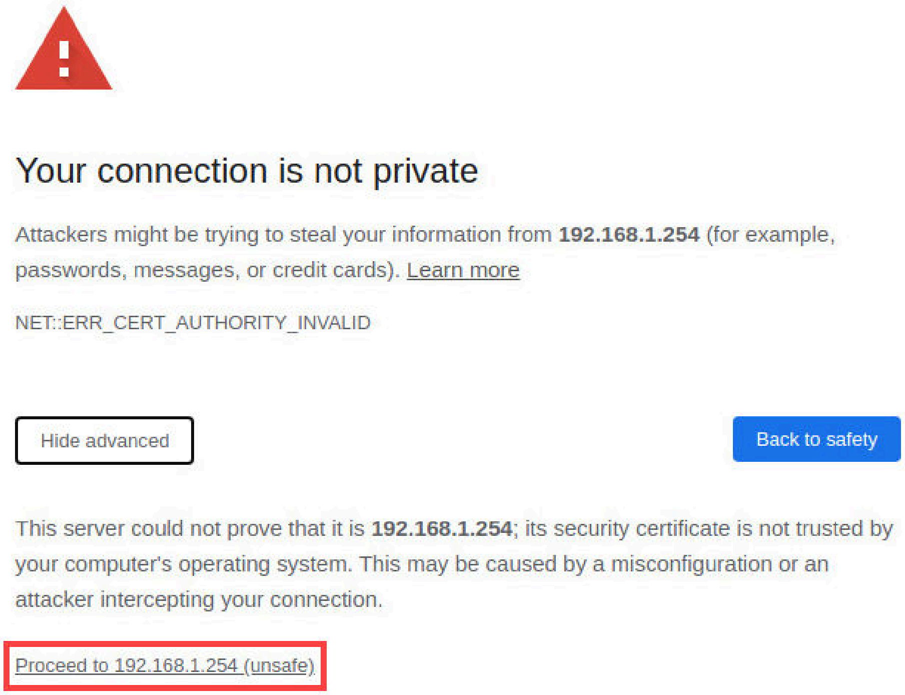
Your connection is not private

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

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.

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



Your connection is not private

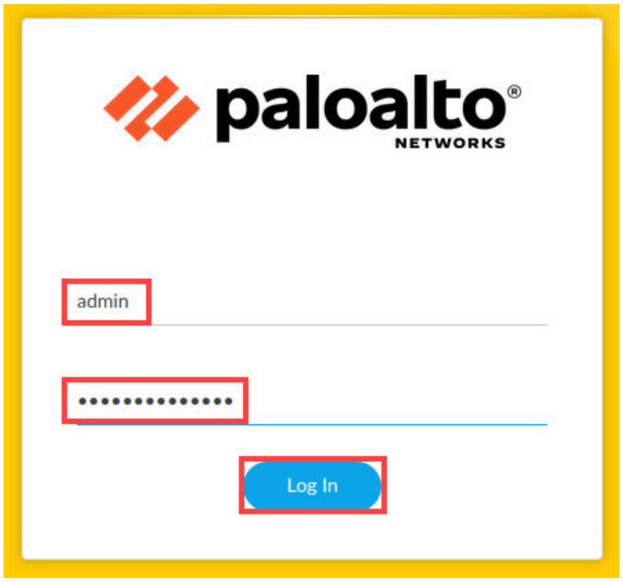
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). Learn more

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)

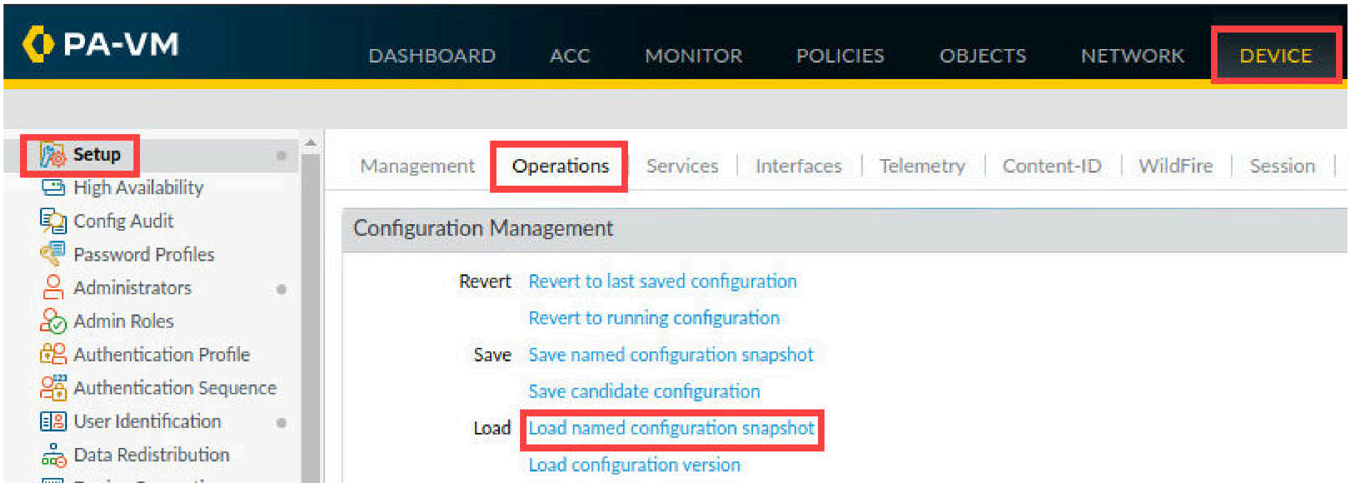
6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!`.**



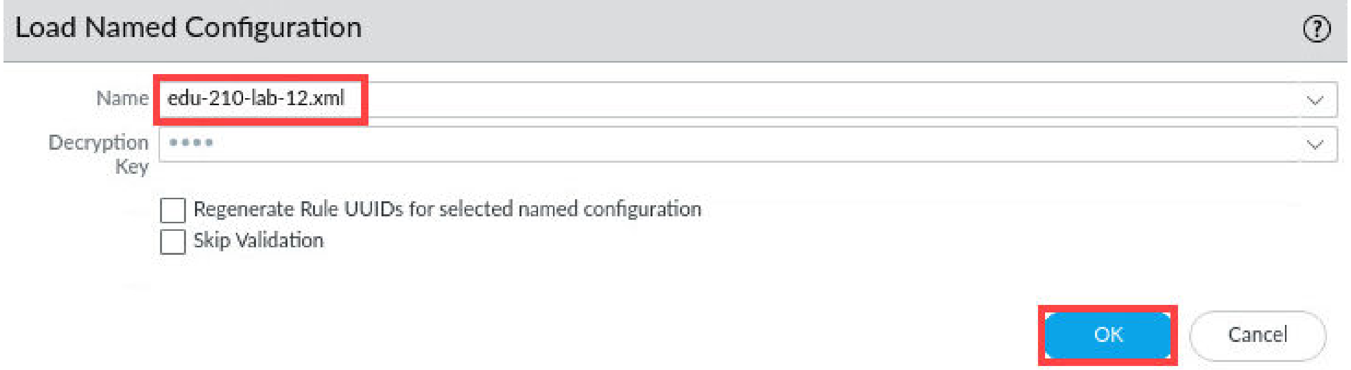
admin

••••••••••••••

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



8. In the *Load Named Configuration* window, select **edu-210-lab-12.xml** from the *Name* dropdown box and click **OK**.



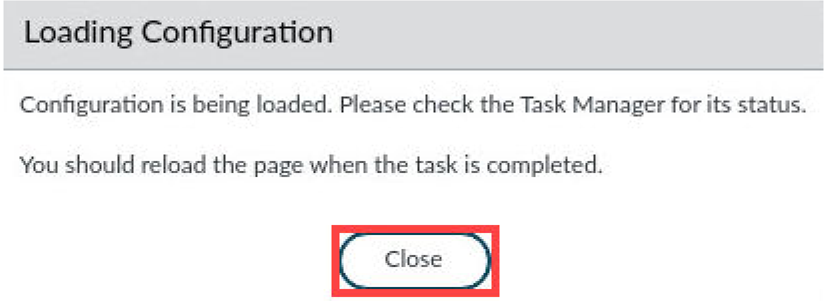
Name: edu-210-lab-12.xml

Decryption Key: ••••

□ Regenerate Rule UUIDs for selected named configuration

□ Skip Validation

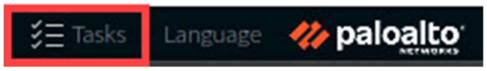
9. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



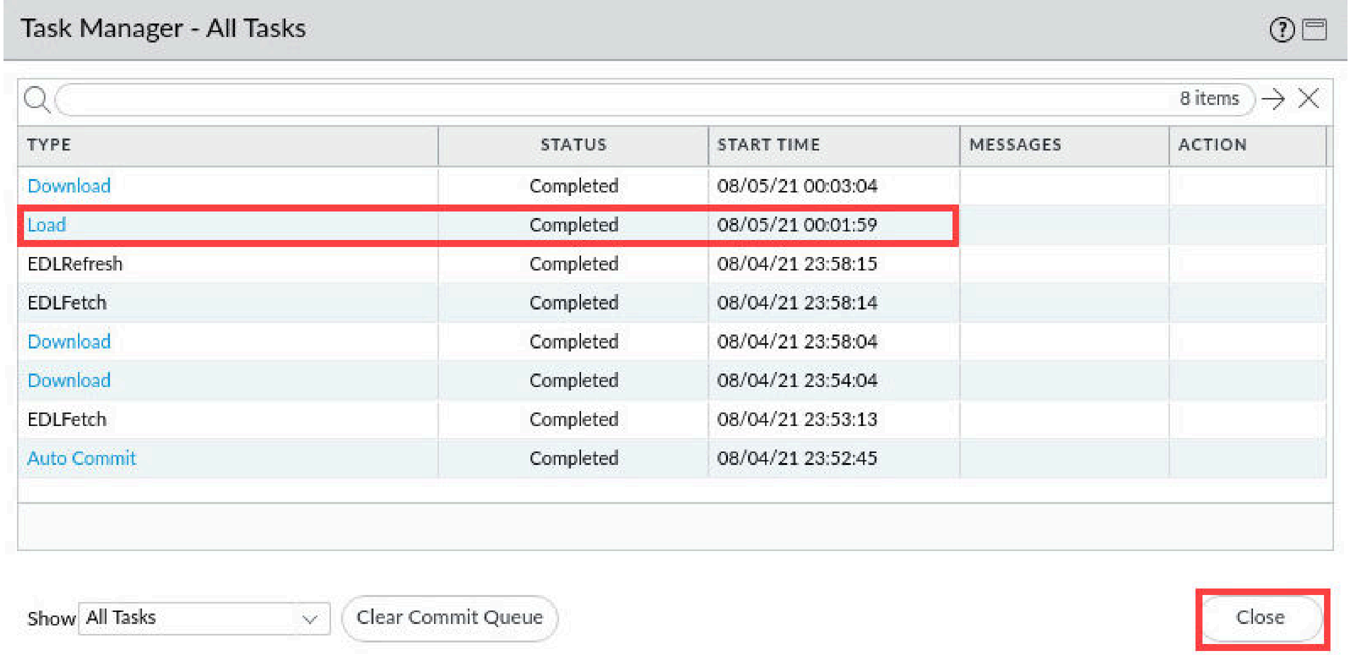
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



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



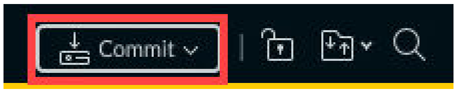
Task Manager - All Tasks

8 items

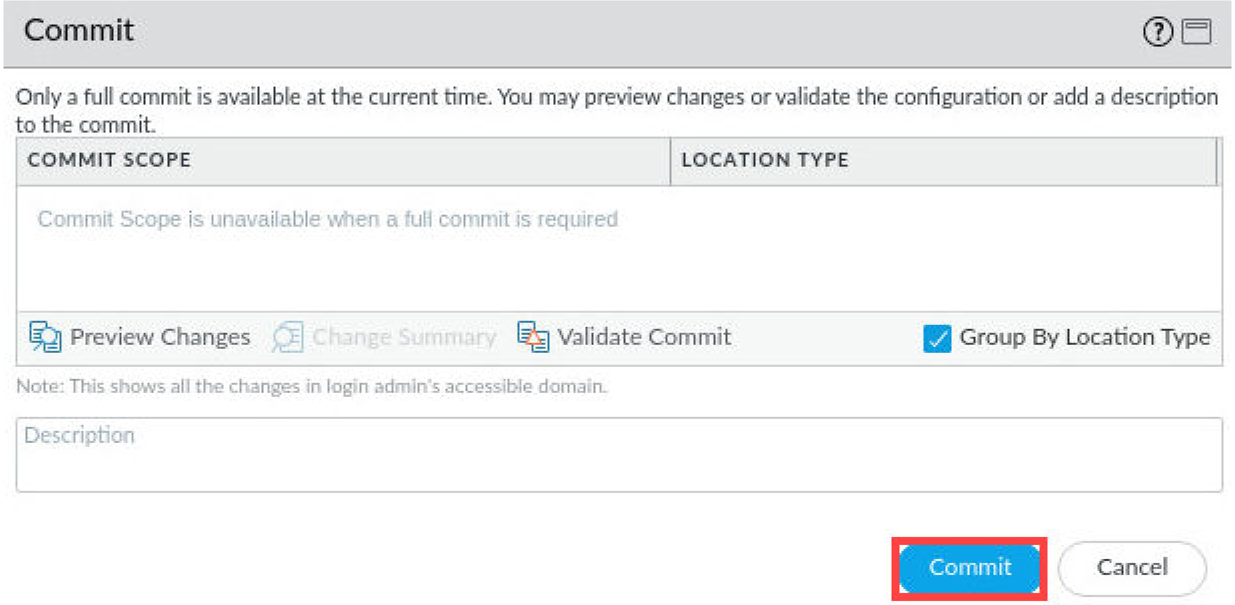
TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show All Tasks

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



13. 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.

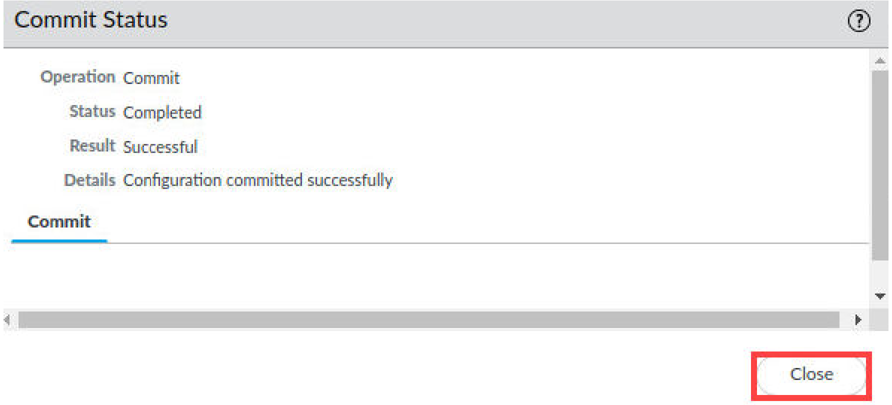
COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

☑ Group By Location Type

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

Description

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



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

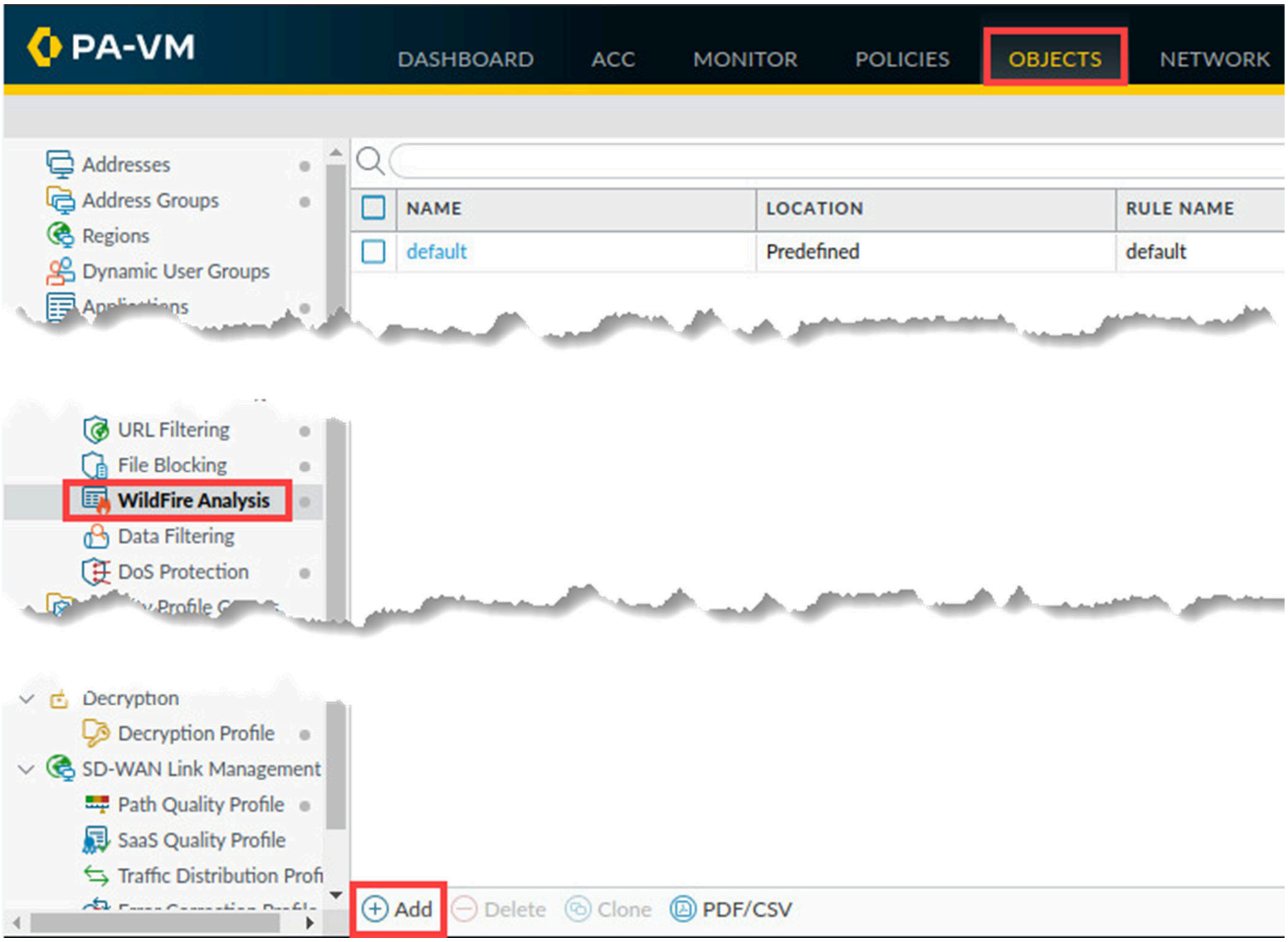
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Create a WildFire Analysis Profile

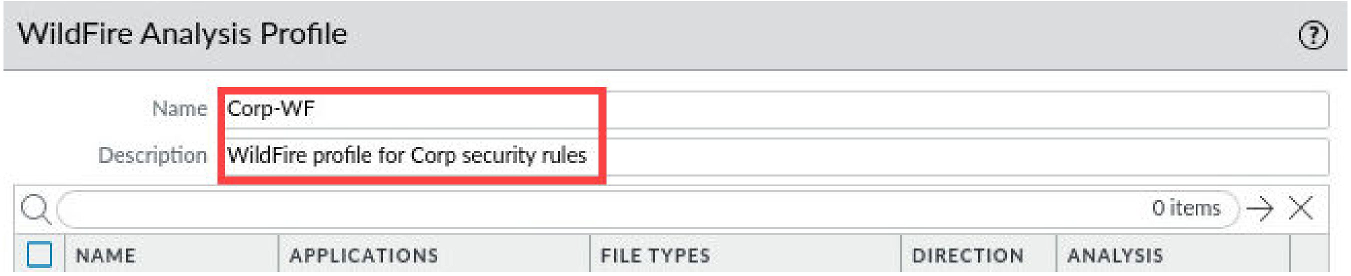
In this section, you will create a WildFire Analysis Security Profile that you can attach to Security policy rules to test files and URLs for malware.

1. In the web interface, select **Objects > Security Profiles > WildFire Analysis**. Click **Add**.



2. In the *WildFire Analysis Profile window*, configure the following.

Parameter	Value
Name	`Corp-WF`
Description	`WildFire profile for Corp security rules.`

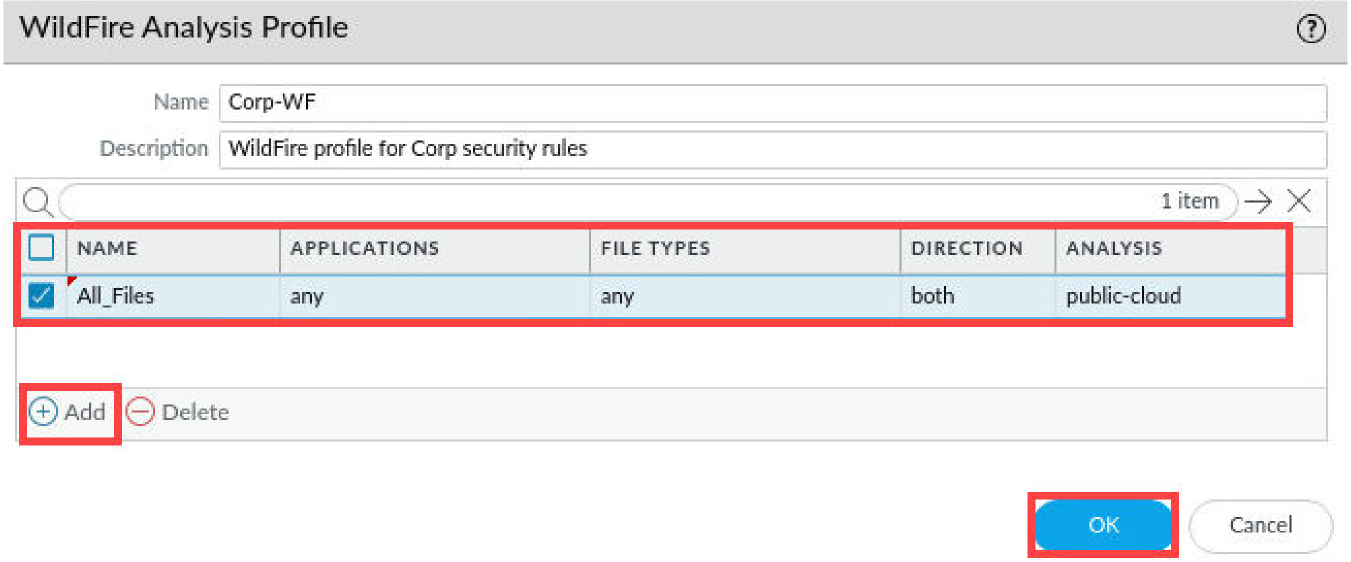

WildFire Analysis Profile

Name: Corp-WF

Description: WildFire profile for Corp security rules

3. Click **Add** and configure the following. Click **OK** to close the *WildFire Analysis Profile* window.

Parameter	**Value**
Name	**`All_Files`**
Applications	**any**
File Types	**any**
Direction	**both**
Analysis	**public-cloud**



Name Corp-WF

Description WildFire profile for Corp security rules

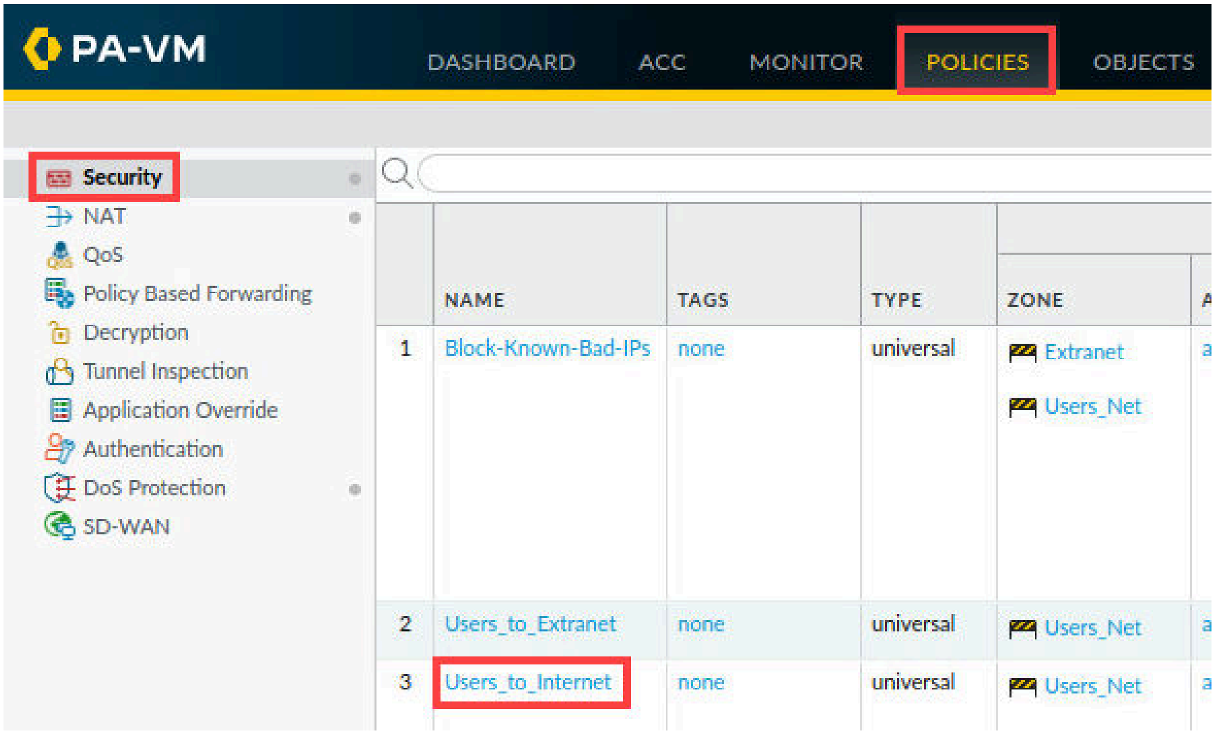
□	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
☑	All_Files	any	any	both	public-cloud

4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Apply WildFire Profile to Security Rules

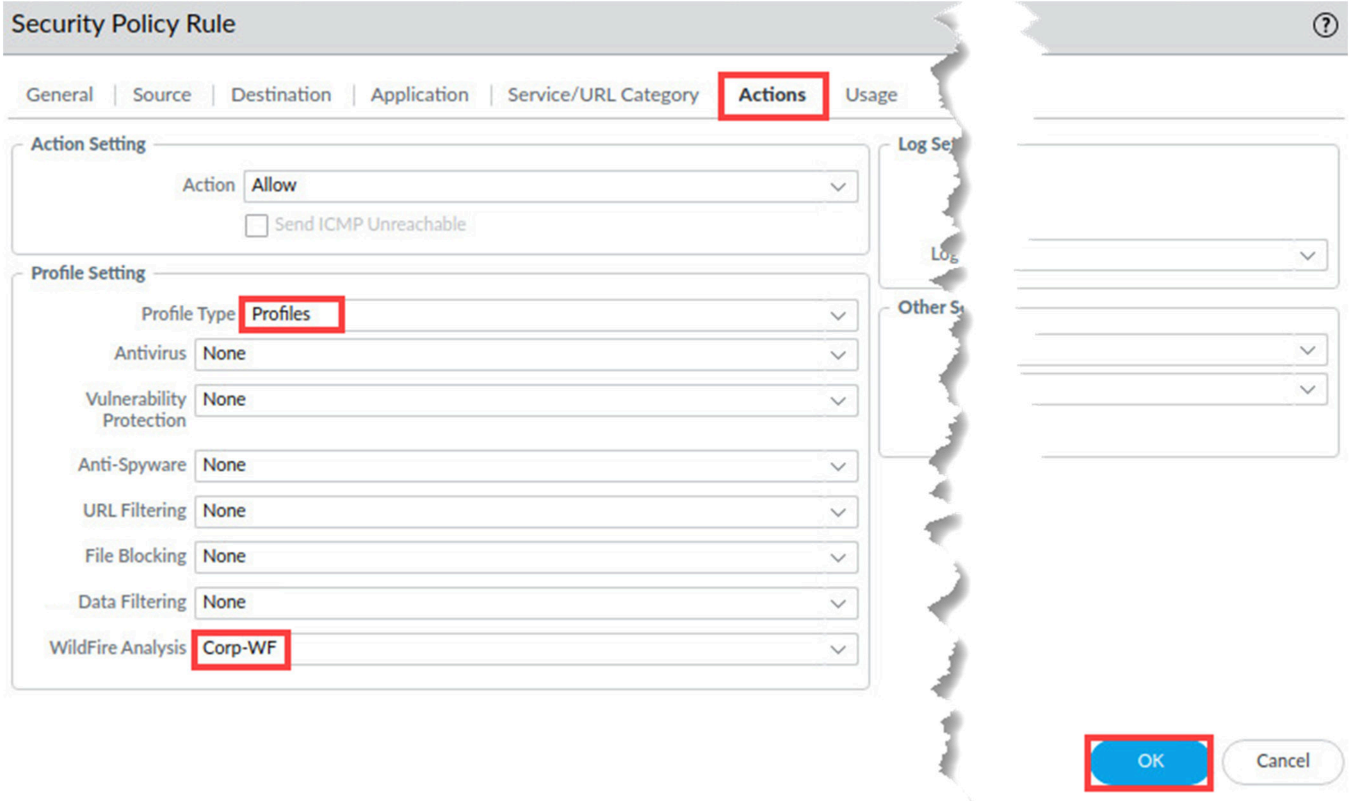
In this section, you will apply the *WildFire Analysis* profile to a security rule.

1. Select **Policies > Security**. Click on the **Users_to_Internet** rule.



	NAME	TAGS	TYPE	ZONE
1	Block-Known-Bad-IPs	none	universal	Extranet Users_Net
2	Users_to_Extranet	none	universal	Users_Net
3	Users_to_Internet	none	universal	Users_Net

2. In the *Security Policy Rule* window, select the **Actions** tab. Under *Profile Settings*, use the dropdown list to select **Profiles.** For *WildFire Analysis***,** select **Corp-WF**. Click **OK**.



Action Setting

Action: Allow

☐ Send ICMP Unreachable

Profile Setting

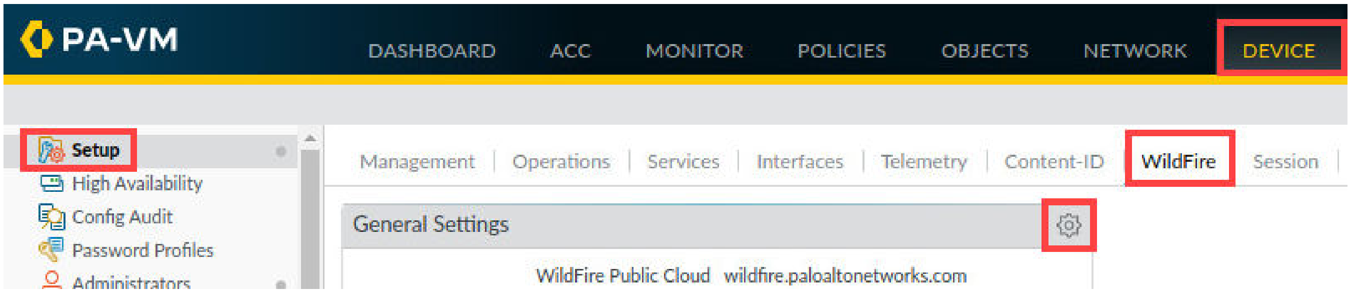
Profile Type	Profiles
Antivirus	None
Vulnerability Protection	None
Anti-Spyware	None
URL Filtering	None
File Blocking	None
Data Filtering	None
WildFire Analysis	Corp-WF

3. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.4 Update WildFire Settings

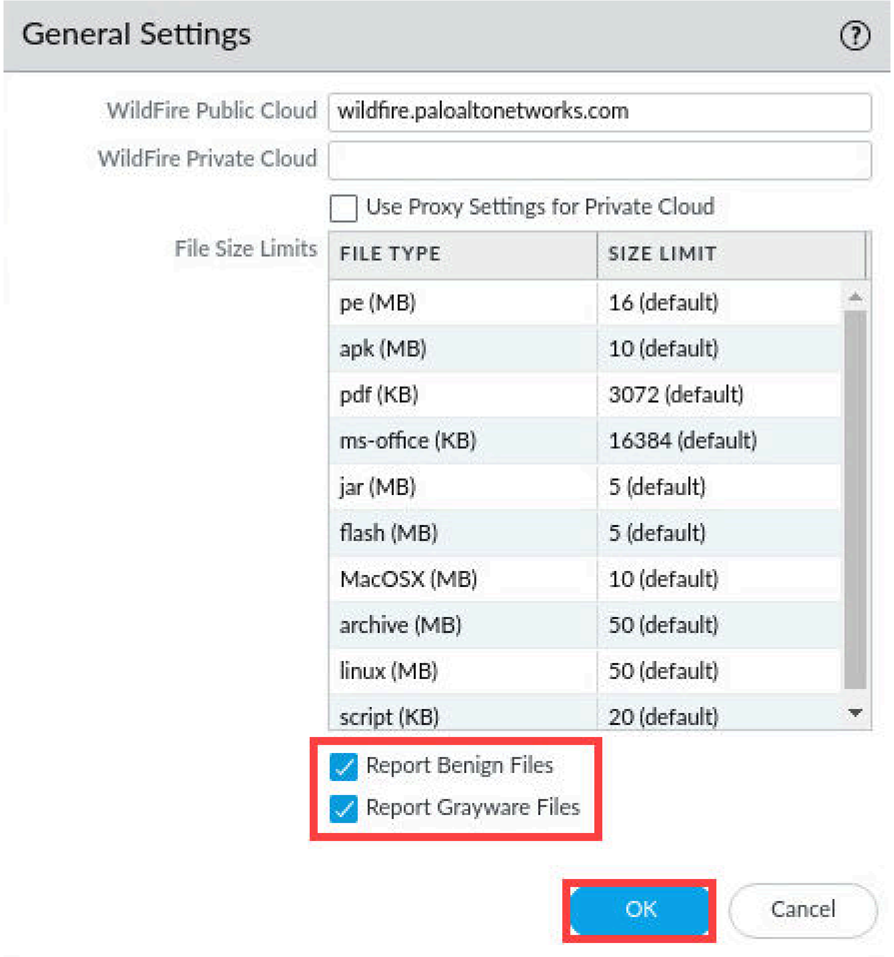
In this section, you will update the WildFire settings.

1. Select **Device > Setup > WildFire.** Click the **gear** icon to edit the **General Settings**.



WildFire Public Cloud wildfire.paloaltonetworks.com

2. In the *General Settings* window, check the boxes for **Report Benign Files** and **Report Grayware Files**. Leave the remaining settings unchanged and click **OK**.



General Settings

WildFire Public Cloud: wildfire.paloaltonetworks.com

WildFire Private Cloud:

☐ Use Proxy Settings for Private Cloud

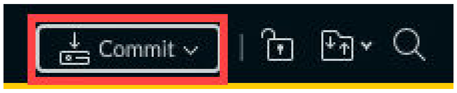
File Size Limits

FILE TYPE	SIZE LIMIT
pe (MB)	16 (default)
apk (MB)	10 (default)
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
jar (MB)	5 (default)
flash (MB)	5 (default)
MacOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

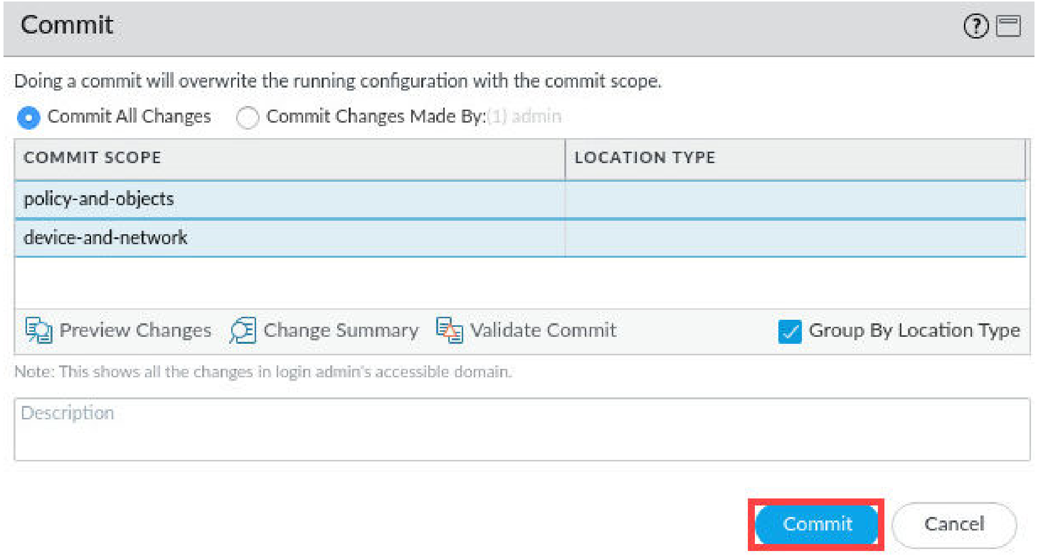
☑ Report Benign Files

☑ Report Grayware Files

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



4. 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

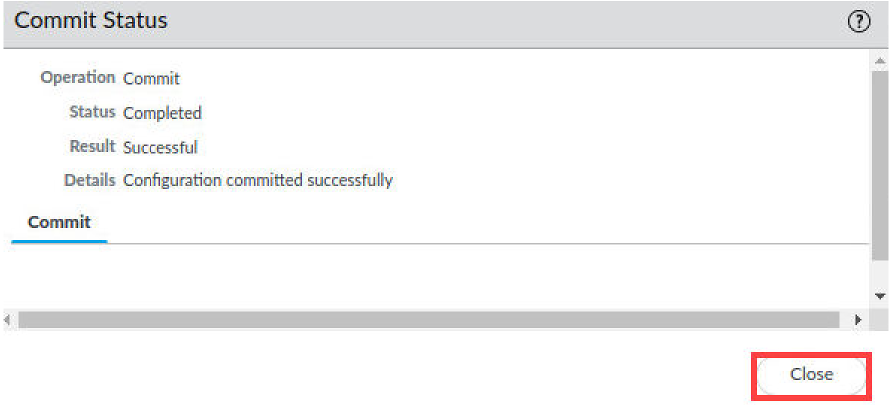
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	
device-and-network	

☑ Group By Location Type

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

Description

5. When the *Commit* operation successfully completes, click **Close** to continue.



Commit Status

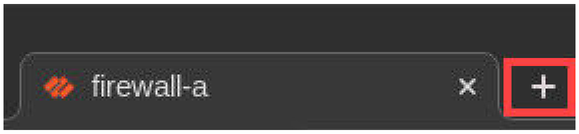
Operation	Commit
Status	Completed
Result	Successful
Details	Configuration committed successfully

6. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

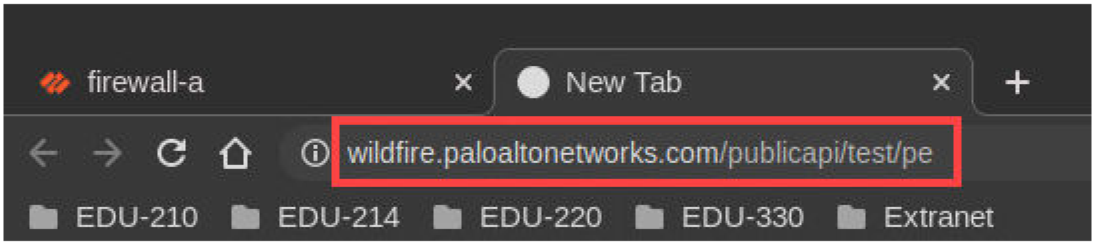
1.5 Test the WildFire Analysis Profile

In this section, you will test the Wildfire Analysis profile that you added to a security rule.

1. Open a new tab in **Chromium**.



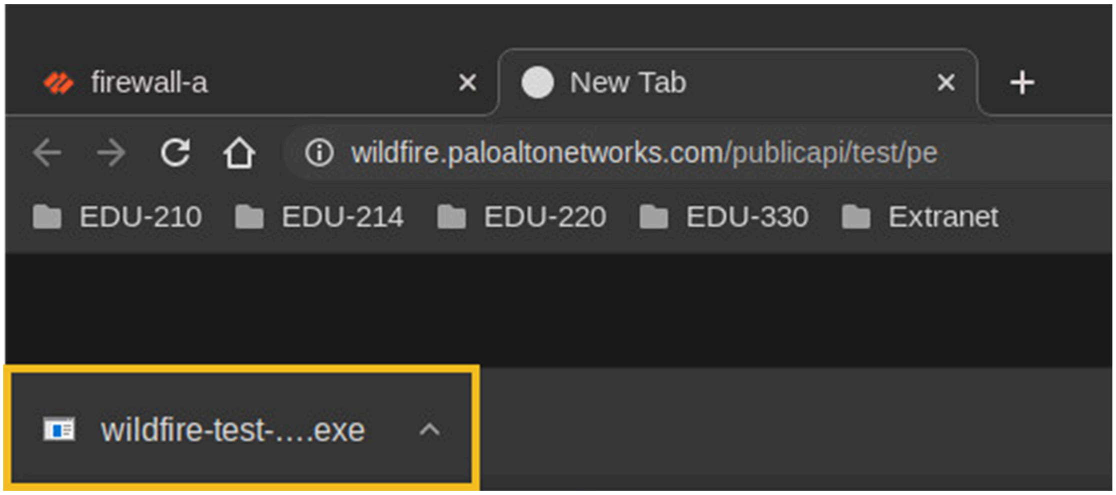
2.
3. Type **`http://wildfire.paloaltonetworks.com/publicapi/test/pe`** and press **Enter**.



Please Note

This site generates an attack file with a unique signature that simulates a zero-day attack. A wildfire-test-pe-file.exe file automatically is downloaded to the Downloads directory.

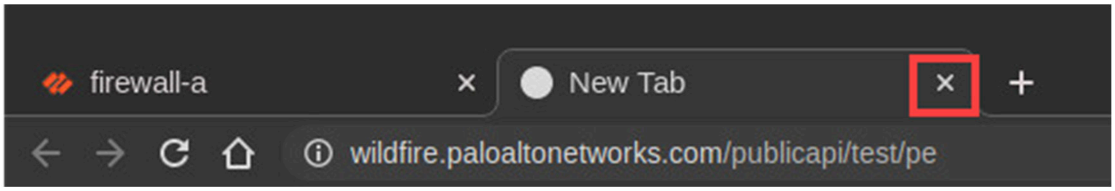
4. Verify the *wildfire-test-pe-file.exe* file successfully downloaded at the bottom of the *Chromium* window.



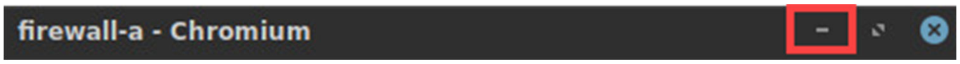
Please Note

You can also verify the wildfire-test-pe-file.exe was successfully downloaded by viewing the downloads folder.

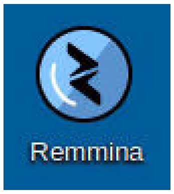
5. Close the new *chromium* tab that you opened by clicking the **X** icon.



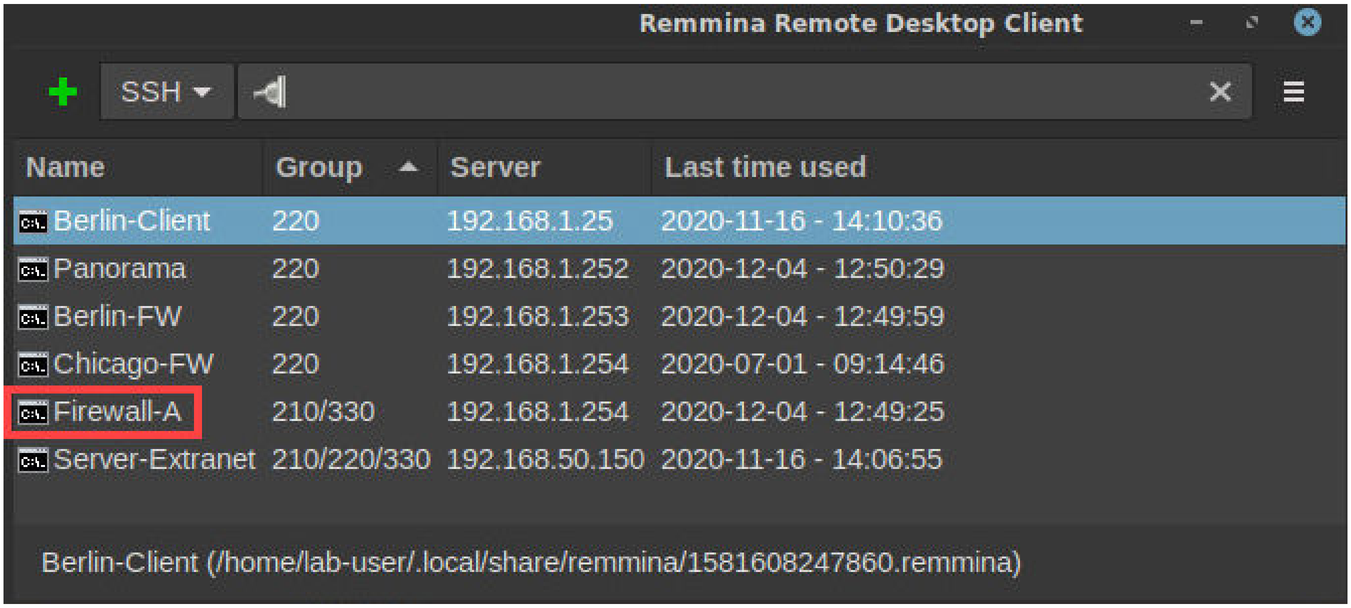
6. Minimize the *Palo Alto Networks Firewall*.



7. On the *client desktop*, open the **Remmina** application.



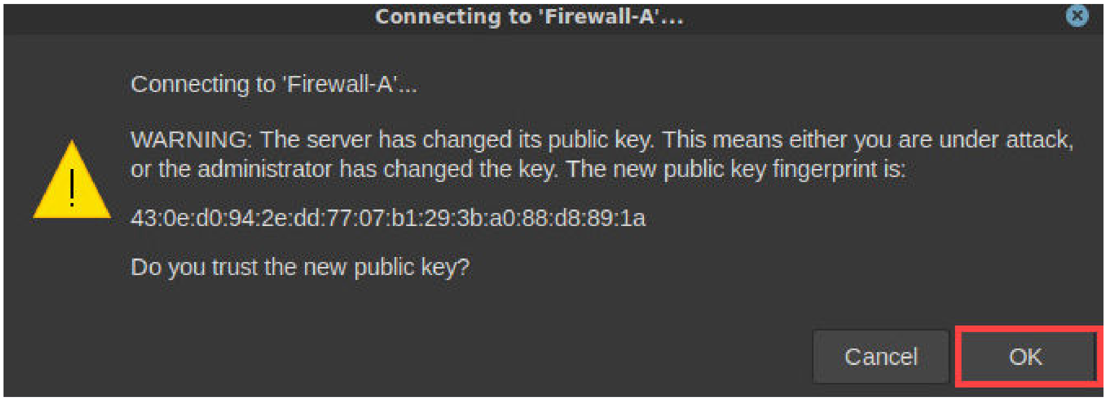
8. Double-click the entry for **Firewall-A**.



Name	Group	Server	Last time used
Berlin-Client	220	192.168.1.25	2020-11-16 - 14:10:36
Panorama	220	192.168.1.252	2020-12-04 - 12:50:29
Berlin-FW	220	192.168.1.253	2020-12-04 - 12:49:59
Chicago-FW	220	192.168.1.254	2020-07-01 - 09:14:46
Firewall-A	210/330	192.168.1.254	2020-12-04 - 12:49:25
Server-Extranet	210/220/330	192.168.50.150	2020-11-16 - 14:06:55

Berlin-Client (/home/lab-user/.local/share/remmina/1581608247860.remmina)

9. If you get *Connecting to 'Firewall-A'…* window, click **OK**.



Connecting to 'Firewall-A'...

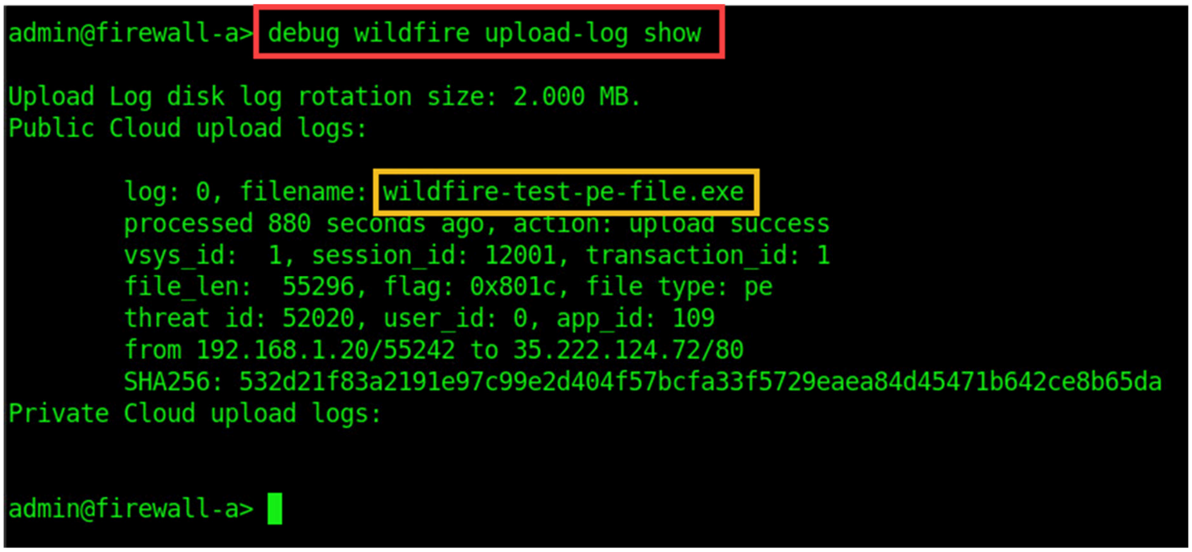
WARNING: The server has changed its public key. This means either you are under attack, or the administrator has changed the key. The new public key fingerprint is:

43:0e:d0:94:2e:dd:77:07:b1:29:3b:a0:88:d8:89:1a

Do you trust the new public key?

10. In the CLI connection to the firewall, enter the command below.

```
admin@firewall-a> debug wildfire upload-log show <Enter>
```



```
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 880 seconds ago, action: upload success
        vsys_id:  1, session_id: 12001, transaction_id: 1
        file_len:  55296, flag: 0x801c, file type: pe
        threat id: 52020, user_id: 0, app_id: 109
        from 192.168.1.20/55242 to 35.222.124.72/80
        SHA256: 532d21f83a2191e97c99e2d404f57bcfa33f5729eaea84d45471b642ce8b65da
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 display.

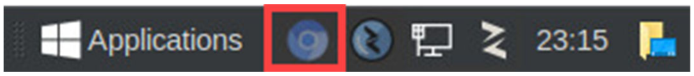
The details of the entry you see will differ from the example shown here.

11. Type **Exit** to close the SSH session to the firewall.

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

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

12. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

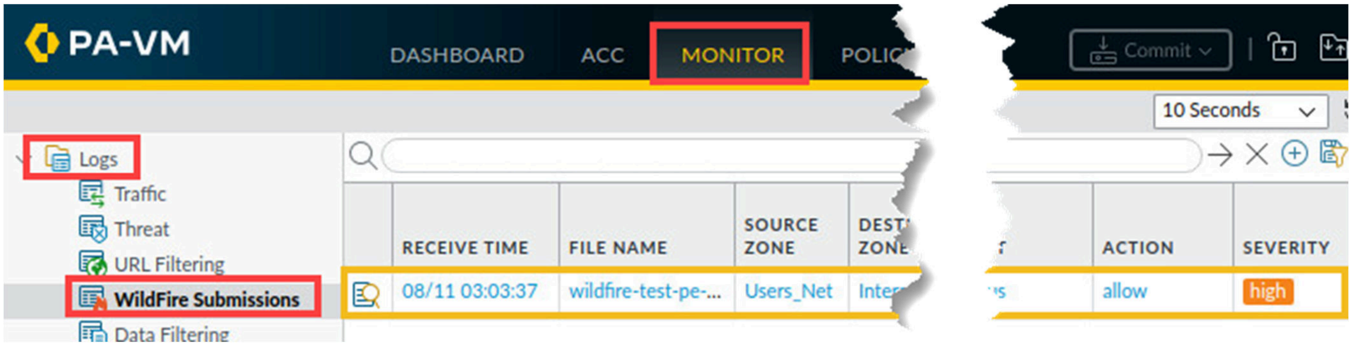


13. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.6 Examine WildFire Analysis Details

In this section, you will examine the WildFire Analysis details in the Palo Alto Networks firewall and view a PDF of the Detailed Log view.

1. Select **Monitor > Logs > Wildfire Submissions**. Verify the **wildfire-test-pe-file.exe** is visible.

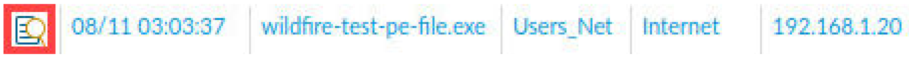


RECEIVE TIME	FILE NAME	SOURCE ZONE	DEST ZONE		ACTION	SEVERITY
08/11 03:03:37	wildfire-test-pe-...	Users_Net	Inte	s	allow	high

> **Please Note**
>
> Note that in this example several default columns have been hidden, and the details of the entry you see will differ.

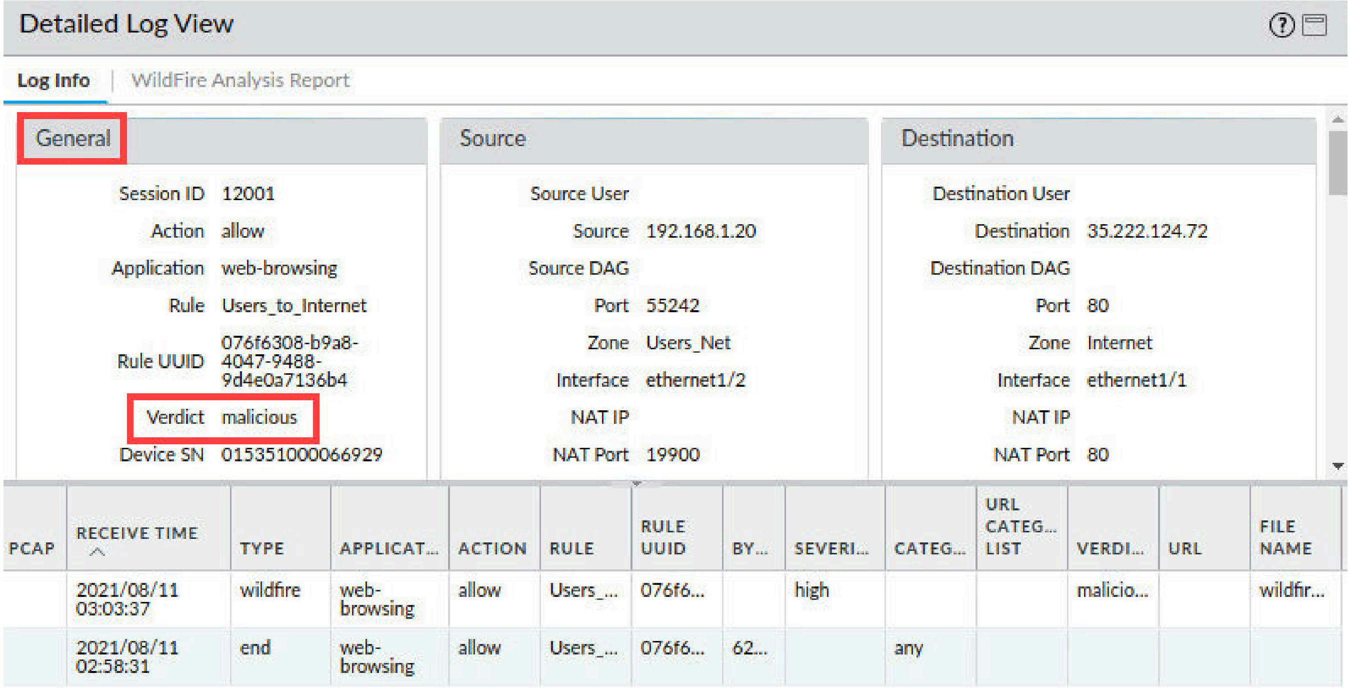
> **STOP**
>
> Analysis can take 5 to 15 minutes, and the table will remain empty until WildFire has reached a verdict about the file. Do not continue to the next step until the WildFire Submissions is showing.

2. Click the **magnifying glass** icon next to the entry to open the **Detailed Log View** of the entry.



08/11 03:03:37	wildfire-test-pe-file.exe	Users_Net	Internet	192.168.1.20

3. In the *Detailed Log View* window, under the *General* section, note the **Verdict**.



General

Session ID 12001
Action allow
Application web-browsing
Rule Users_to_Internet
Rule UUID 076f6308-b9a8-4047-9488-9d4e0a7136b4
Verdict malicious
Device SN 015351000066929

Source

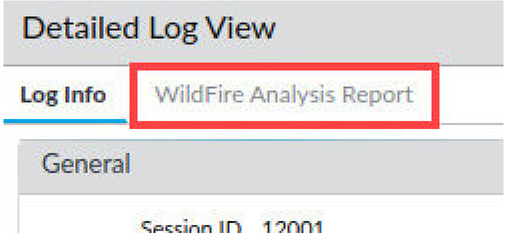
Source User
Source 192.168.1.20
Source DAG
Port 55242
Zone Users_Net
Interface ethernet1/2
NAT IP
NAT Port 19900

Destination

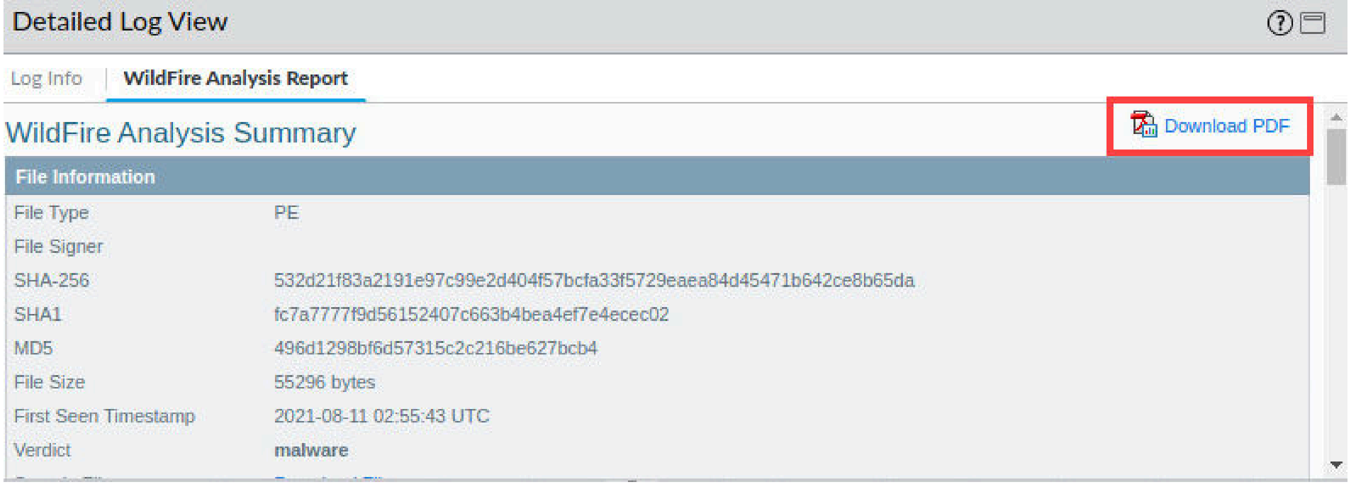
Destination User
Destination 35.222.124.72
Destination DAG
Port 80
Zone Internet
Interface ethernet1/1
NAT IP
NAT Port 80

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2021/08/11 03:03:37	wildfire	web-browsing	allow	Users_...	076f6...		high			malicio...		wildfir...
	2021/08/11 02:58:31	end	web-browsing	allow	Users_...	076f6...	62...		any				

4. Click the tab labeled **Wildfire Analysis Report** at the top of the *Detailed Log View*.



5. In the *WildFire Analysis Summary* window, click **Download PDF**. This action will open a PDF version of the *Wildfire Analysis Report* in another tab of the Chromium browser.

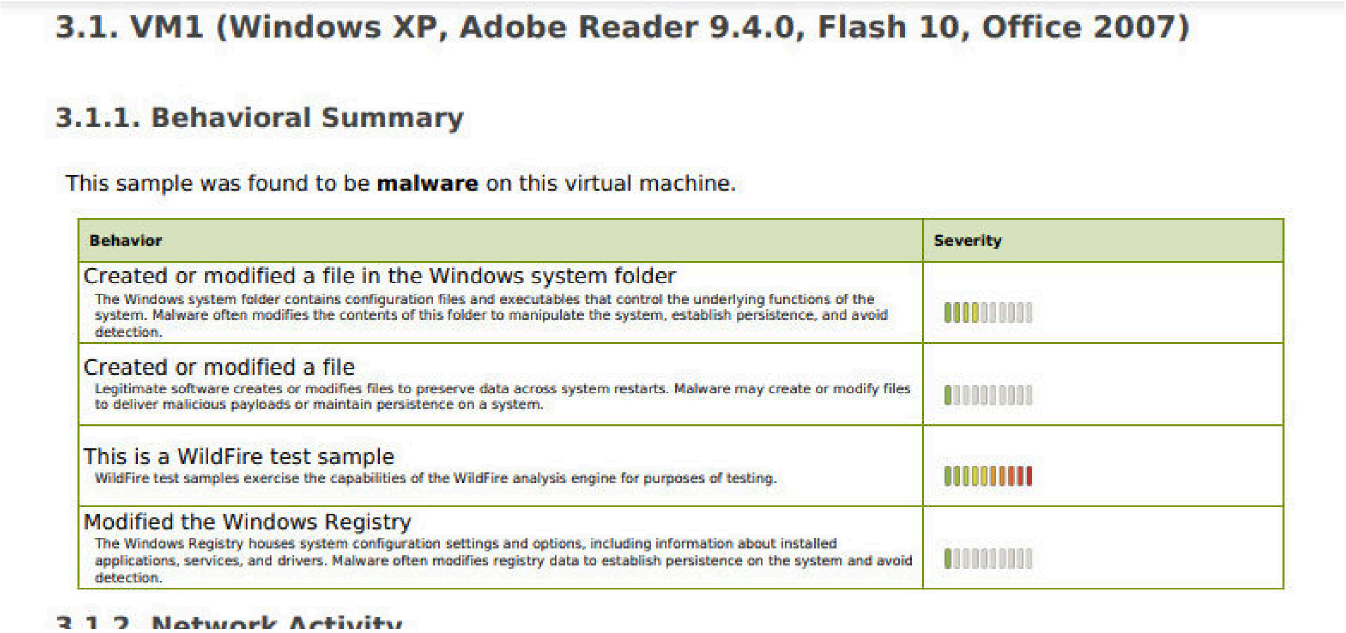


WildFire Analysis Summary

File Information

File Type PE
File Signer
SHA-256 532d21f83a2191e97c99e2d404f57bcfa33f5729eaea84d45471b642ce8b65da
SHA1 fc7a7777f9d56152407c663b4bea4ef7e4ecec02
MD5 496d1298bf6d57315c2c216be627bcb4
File Size 55296 bytes
First Seen Timestamp 2021-08-11 02:55:43 UTC
Verdict **malware**

6. Scroll through the report and view the detailed information about the WildFire analysis of the file.



3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	▮▮▮▮▯▯▯▯▯▯
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	▮▯▯▯▯▯▯▯▯▯
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	▮▮▮▮▮▮▮▮▮▮
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	▮▯▯▯▯▯▯▯▯▯

3.1.2. Network Activity

Please Note

For example, section 3.1 provides of the report details about the kind of environment that WildFire used to test the file along with specific actions that the malware file carried out.

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