



PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 10: Blocking Unknown Threats with WildFire

Document Version: **2025-10-13**

Copyright © 2025 Network Development Group, Inc.
www.netdevgroup.com

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

Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are registered trademarks of Palo Alto Networks, Inc. All other marks mentioned herein may be trademarks of their respective companies.

Contents

Introduction	3
Objective	3
Lab Topology	4
Theoretical Lab Topology	4
Lab Settings	5
Lab Guidance	5
1 Blocking Unknown Threats with Wildfire – High Level Lab Steps	6
1.1 Login and Apply a Baseline Configuration to the Firewall.....	6
1.2 Create a Wildfire Analysis Profile	6
1.3 Modify Security Profile Group	6
1.4 Update Wildfire Settings.....	6
1.5 Commit the Configuration	7
1.6 Test the Wildfire Analysis Profile.....	7
1.7 Examine WildFire Analysis Details	7
2 Blocking Unknown Threats with Wildfire – Detailed Lab Steps	8
2.1 Apply a Baseline Configuration to the Firewall	8
2.2 Create a Wildfire Analysis Profile	12
2.3 Modify Security Profile Group	13
2.4 Update WildFire Settings.....	15
2.5 Test the WildFire Analysis Profile.....	17
2.6 Examine WildFire Analysis Details.....	20

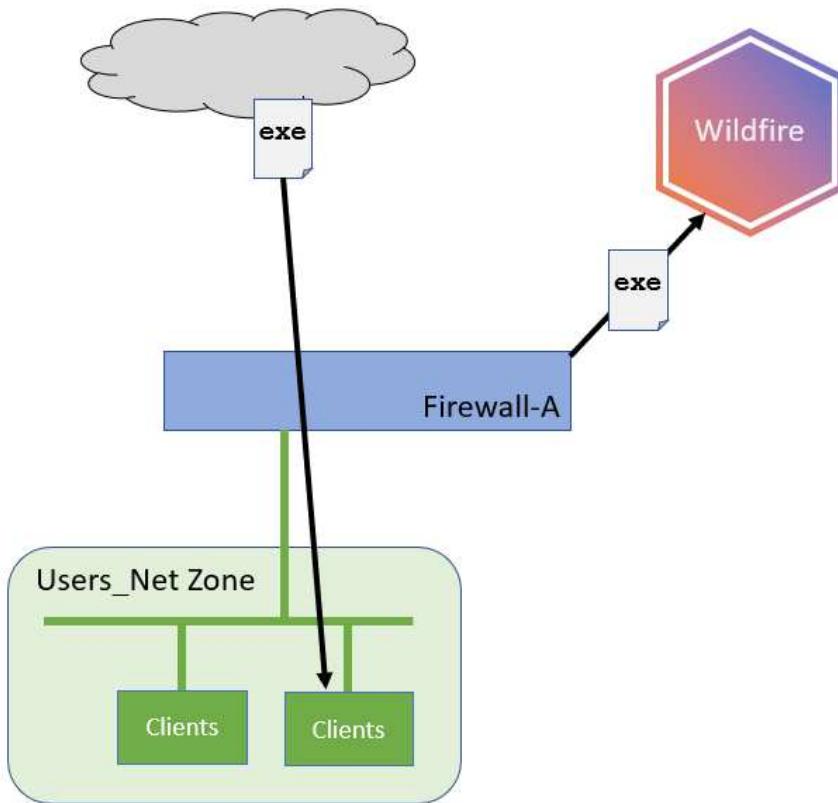
Introduction

Your company has recently seen an increase in malicious files that users are downloading. 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 questionable 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 provided by 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.

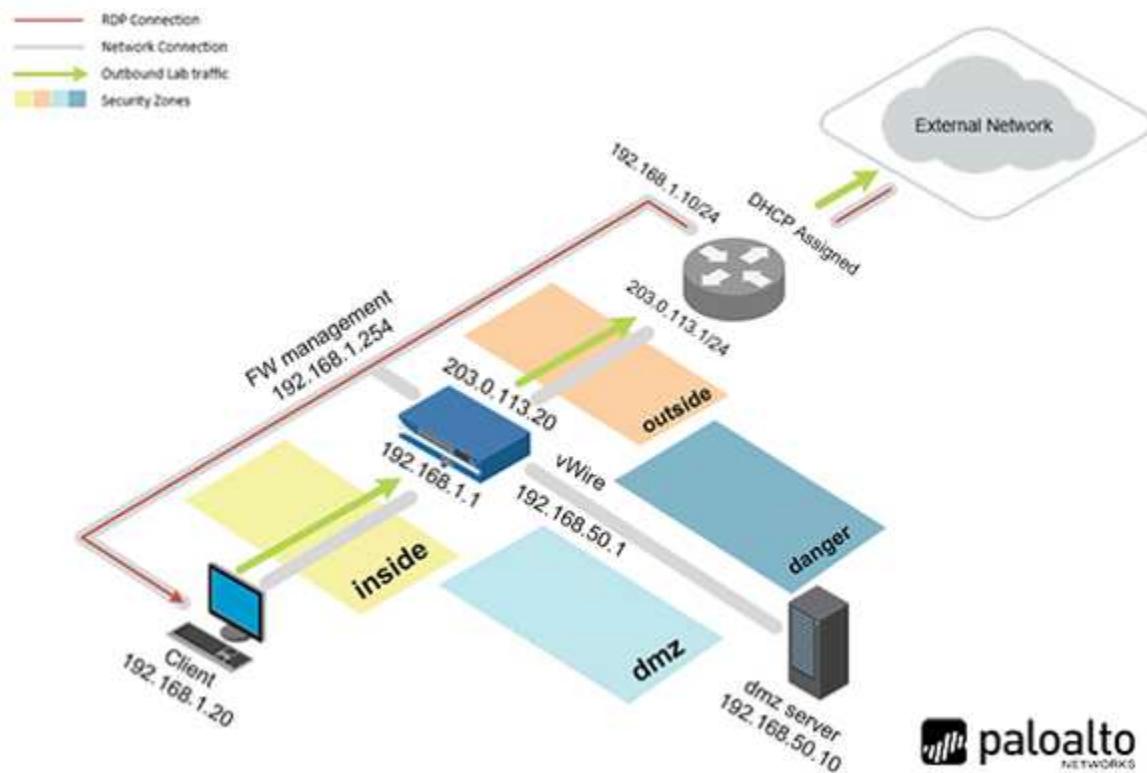


Objective

In this lab, you will perform the following tasks:

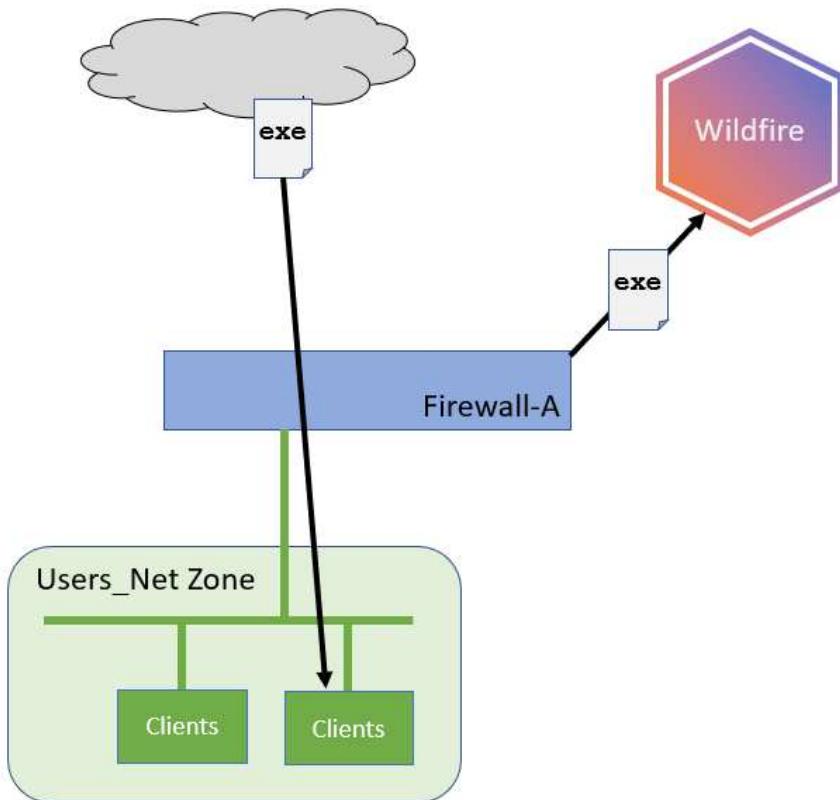
- Create a WildFire Analysis Profile.
- Apply Wildfire Profile to security rules.
- Test the Wildfire Analysis Profile.
- Examine Wildfire analysis details.

Lab Topology



paloalto
NETWORKS

Theoretical 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	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!
vRouter	192.168.1.10	root	PaloAlt0

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

Please
Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Blocking Unknown Threats with Wildfire – High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Login and Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select **lab-user**, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-10.xml** to the Firewall.

1.2 Create a Wildfire Analysis Profile

- Use the information in the tables below to create a WildFire Analysis Security Profile that you can attach to Security Policy rules to test files and URLs for malware.

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

- Click **Add** in the bottom left corner and configure the following:

Profile Details	Value
Name	All_Files
Applications	any
File Types	any
Direction	Both
Analysis	public-cloud

1.3 Modify Security Profile Group

- Add the **Corp-WF** Profile to the **Corp-Profiles-Group**.
- Disable** all but the **Corp-WF** Security Profile.

Please Note

Doing this ensures that the firewall will only use WildFire and no other Security Profiles such as Anti-Virus or Machine Learning for this lab.

1.4 Update Wildfire Settings

- Enable the options for **Report Benign Files** and **Report Grayware Files** under the **General Settings** for Wildfire.

1.5 Commit the Configuration

- Commit the changes to the firewall before proceeding.

1.6 Test the Wildfire Analysis Profile

- Use the Firefox browser and connect to:
http://192.168.50.80/wildfire-test-pe-file.exe
- Save the file when prompted.
- Use the **Remmina** application and connect to **Firewall-A**.
- Use the command **debug wildfire upload-log show** to verify that the test file was uploaded.

1.7 Examine WildFire Analysis Details

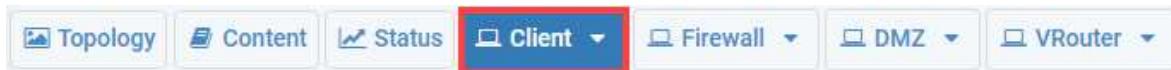
- Examine the **WildFire Submissions** log file and periodically use the **Refresh** icon until you see a new entry for the wildfire-test-pe-file.exe.
- Examine the **Detailed Log View** for the entry.
- Note the **Verdict** of the file.
- Click the link for **Download PDF** and examine the report to view detailed information about the Wildfire analysis of the file.

2 Blocking Unknown Threats with Wildfire – Detailed Lab Steps

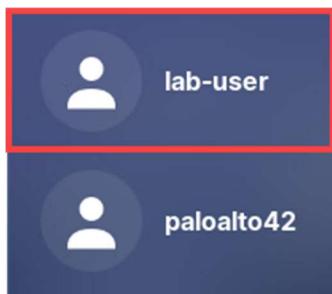
2.1 Apply a Baseline Configuration to the Firewall

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

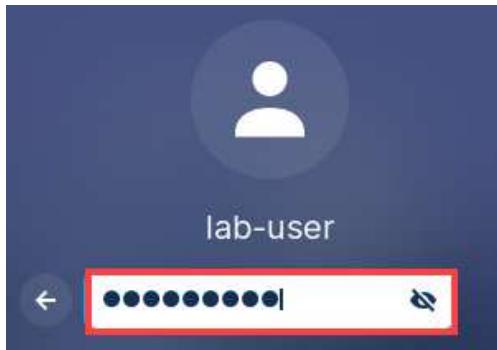
1. Click on the **Client** tab to access the Client PC.



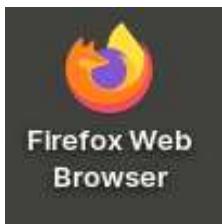
2. On the *Zorin* desktop, click **lab-user**.



3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



- Double-click the **Firefox Web Browser** icon located on the *Desktop*.



- In the *Firefox* address field, type **https://192.168.1.254** and press **Enter**.



- Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.

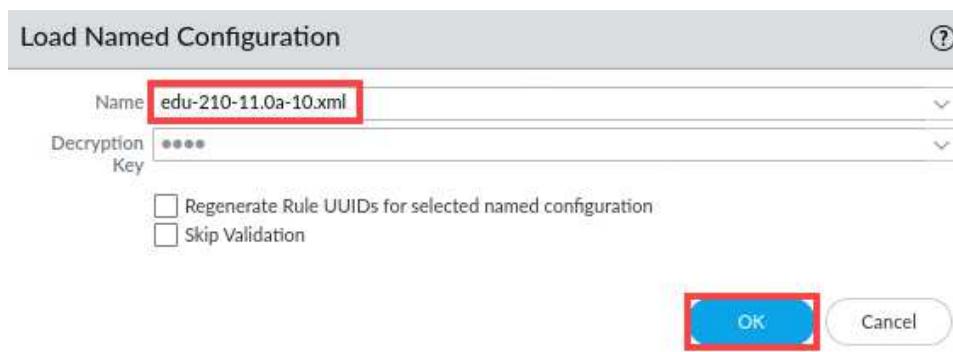


If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

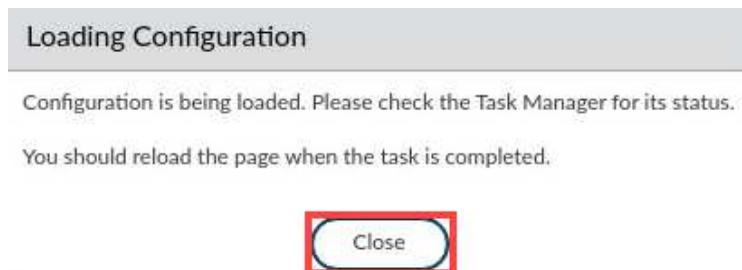
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. At the top, there's a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is highlighted with a red box. Below the navigation bar is a sidebar with a 'Setup' icon and several options: High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area has a 'Management' tab and an 'Operations' tab, which is highlighted with a red box. Under the 'Operations' tab, there's a 'Configuration Management' section. It includes options like Revert (Revert to last saved configuration, Revert to running configuration), Save (Save named configuration snapshot, Save candidate configuration), Load (Load named configuration snapshot, Load configuration version). The 'Load named configuration snapshot' option is also highlighted with a red box.

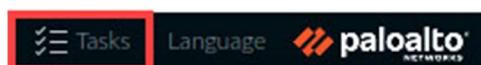
8. In the *Load Named Configuration* window, select **edu-210-11.0a-10.xml** from the *Name* drop-down box and click **OK**.



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.



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 been completed. Click **Close**

JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

Show All Tasks | Clear Commit Queue | Close

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.

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 All Changes Commit Changes Made By: (1) admin

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

Preview Changes Change Summary Validate Commit

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

Description

Commit Cancel

14. When the commit operation is complete, click **Close** to continue.

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit App Dependency

Close



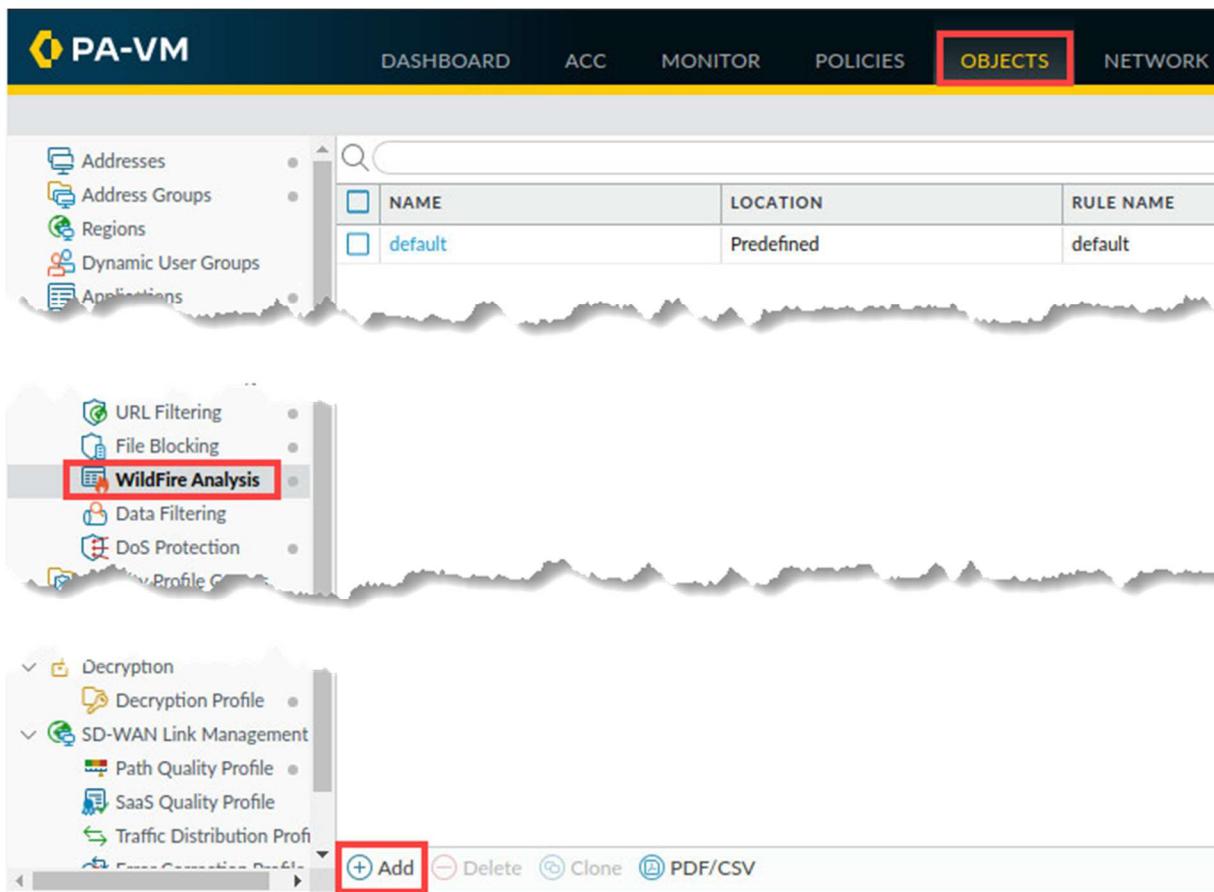
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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

2.2 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**.

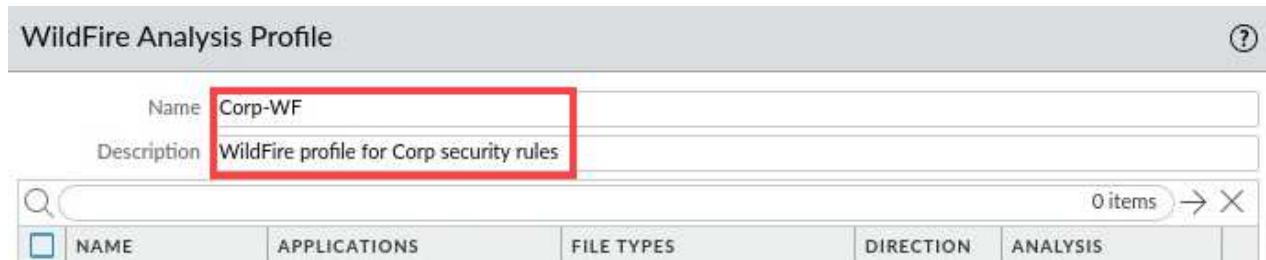


The screenshot shows the PA-VM interface with the following details:

- Header:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS** (highlighted), NETWORK.
- Left Sidebar:** Addresses, Address Groups, Regions, Dynamic User Groups, Applications.
- Middle Panel:** A table with columns NAME, LOCATION, RULE NAME. One row is listed: default, Predefined, default.
- Second Left Sidebar:** URL Filtering, File Blocking, **WildFire Analysis** (highlighted with a red box), Data Filtering, DoS Protection.
- Third Left Sidebar:** Decryption, SD-WAN Link Management, Path Quality Profile, SaaS Quality Profile, Traffic Distribution Prof.
- Bottom Bar:** + Add, Delete, Clone, PDF/CSV.

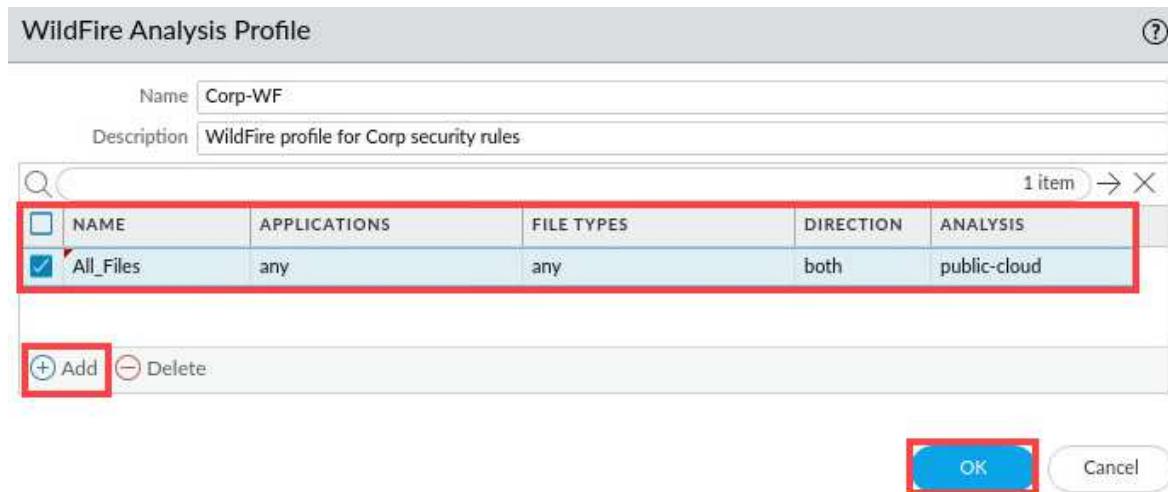
2. In the *WildFire Analysis Profile* window, configure the following.

Parameter	Value
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



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

2.3 Modify Security Profile Group

In this section, you will apply the *WildFire Analysis* profile to a Security Profile Group.

- Select **Objects > Security Profile Groups**. Click and edit the **Corp-Profiles-Group**.

- Use the drop-down list for **Wildfire Analysis Profile** to select **Corp-WF**. Set the other **Profiles** to **None**. Click **OK**.

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



Doing this ensures that the firewall will only use Wildfire and no other Security Profiles such as Anti-Virus or Inline Machine Learning.

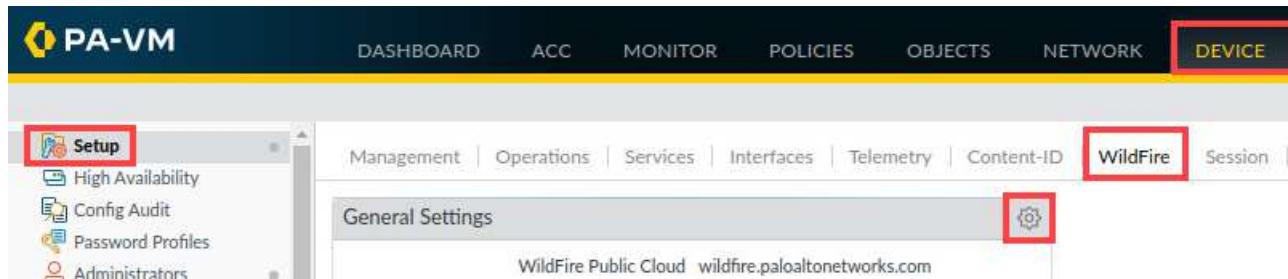
In a production environment, you want to apply all the Security Profiles for your Group. In this lab, we only want to test WildFire to see how it operates alone.

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

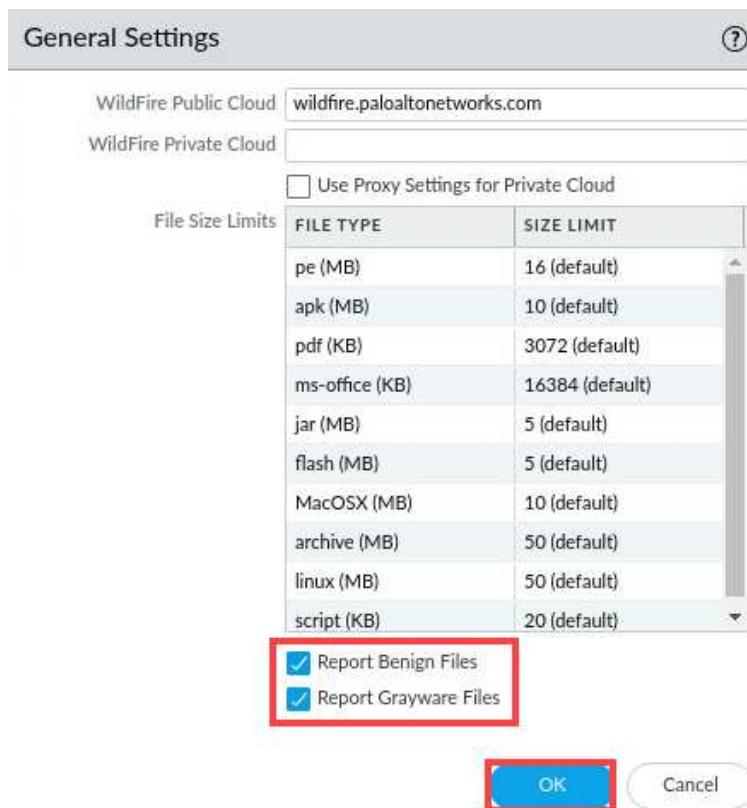
2.4 Update WildFire Settings

In this section you will update the WildFire settings.

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



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**.



The screenshot shows the 'General Settings' configuration window. It includes fields for WildFire Public Cloud (wildfire.paloaltonetworks.com) and WildFire Private Cloud, a checkbox for 'Use Proxy Settings for Private Cloud', and a 'File Size Limits' table. The table lists file types and their 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)

At the bottom, two checkboxes are checked and highlighted with a red box: 'Report Benign Files' and 'Report Grayware Files'. The window has 'OK' and 'Cancel' buttons at the bottom.

3. Navigate to Policies > Security and click Allow-PANW-Apps.

NAME	TAGS	TYPE	ZONE	ADDRESS
1 Block-Bad-URLs	none	universal	Users_Net	any
2 Block-from-Known...	none	universal	Internet	Palo Alto Networks - Bulletproof Palo Alto Networks - High risk Palo Alto Networks - Known m
3 Block-to-Known-Ba...	none	universal	Extranet Users_Net	any
4 Allow-PANW-Apps	none	universal	Users_Net	192.168.1.254
5 Users_to_Extranet	none	universal	Users_Net	any

4. In the Security Policy Rule window, on the Source tab, click Any for the Source Address. Click OK.

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input type="checkbox"/> Users_Net	<input type="checkbox"/> 192.168.1.254

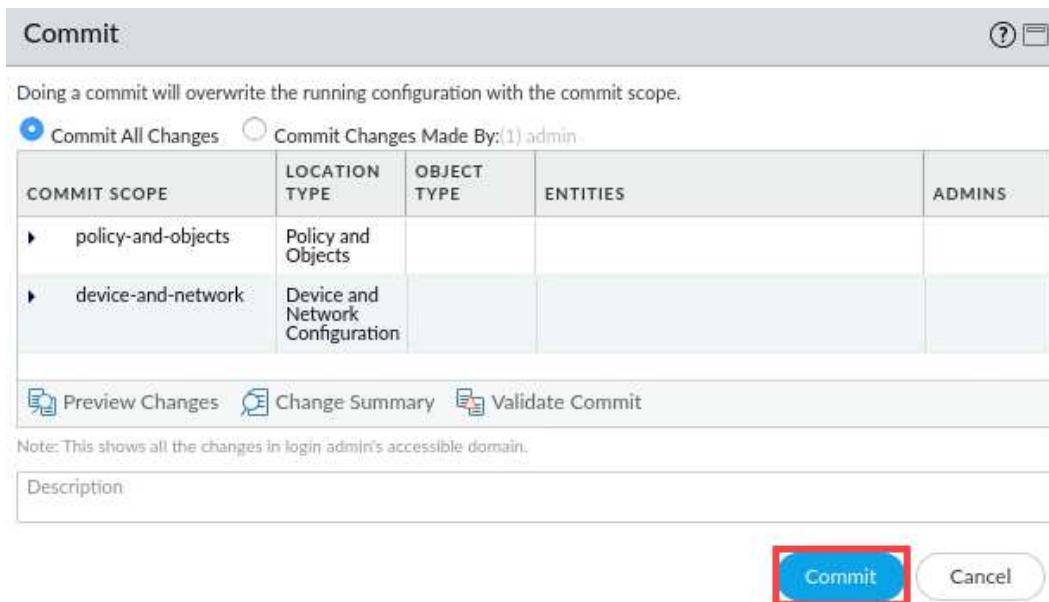
+ Add - Delete + Add - Delete Negate

OK Cancel

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



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



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

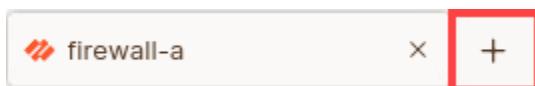


8. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.5 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 **Firefox**.



- Type <http://192.168.50.80/wildfire-test-pe-file.exe> 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.

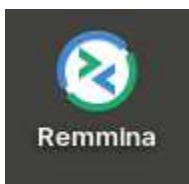
- When Firefox prompts you, click **Save**.

**Please Note**

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

- Close the new Firefox tab that you opened by clicking the X icon.



5. Minimize the *Palo Alto Networks Firewall*.6. On the client desktop, open the **Remmina** application.7. Double-click the entry for **Firewall-A**.

Name	Group	Server	Plugin	Last used
Berlin-Client		192.168.1.25	SSH	2022-11-21 - 09:01:12
Firewall-A		192.168.1.254	SSH	2022-12-16 - 07:51:14
Firewall-B		192.168.1.253	SSH	2022-11-21 - 08:51:34
Panorama		192.168.1.252	SSH	2022-12-14 - 10:34:19
Server-Extranet		192.168.50.10	SSH	2022-12-16 - 09:27:14

8. 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 108 seconds ago, action: upload success  
    vsys_id: 1, session_id: 2033, transaction_id: 1  
    file_len: 55296, flag: 0x801c, file type: pe  
    threat id: 52020, user_id: 0, app_id: 0  
    from 192.168.1.20/55378 to 35.222.124.72/80  
    SHA256: 0bf9a2e236ee7c29d3132364ec755614f1c29d0219518edda33f3dea9aa78ae1  
  
    log: 1, filename: wildfire-test-pe-file.exe  
    processed 108 seconds ago, action: upload success  
    vsys_id: 1, session_id: 2662, transaction_id: 2  
    file_len: 55296, flag: 0x801c, file type: pe  
    threat id: 52020, user_id: 0, app_id: 0  
    from 192.168.1.20/55916 to 35.222.124.72/80  
    SHA256: 4e4fa8d52ea4552bd3c04bc当地8da6384ffc54ef4eecf9810949670f57be8b0d4  
Private Cloud upload logs:
```

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.

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

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

10. Re-open the *PA-VM firewall* web interface by clicking on the **Firefox** icon on the task bar.



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

2.6 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. You may need to periodically use the refresh button in the upper right corner of the window until you see a new entry for the wildfire-test-pe-file.exe.

RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINATION ZONE	VERDICT	ACTION	SEVERITY	SENDER ADDRESS
09/21 03:38:11	wildfire-test-pe-file.exe	Users_Net	Extranet	malicious	allow	high	>_to_Extranet
09/21 03:38:11	wildfire-test-pe-file.exe	Users_Net	Extranet	malicious	allow	high	.to_Extranet

Please Note

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



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 Submission is showing.

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

	09/21 03:38:11	wildfire-test-pe-file.exe	Users_Net	Extranet	192.168.1.20	192.168.50.80
--	----------------	---------------------------	-----------	----------	--------------	---------------

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

Detailed Log View

Log Info | WildFire Analysis Report

General		Source			Destination										
Session ID	1092	Source User			Destination User										
Action	allow	Source	192.168.1.20		Destination	192.168.50.80									
Application	web-browsing	Source DAG			Destination DAG										
Rule	Users_to_Extranet	Port	46572		Port	80									
Rule UUID	f3297494-77d0-4335-a111-54a35172bcce1	Zone	Users_Net		Zone	Extranet									
Verdict	malicious	Interface	ethernet1/2		Interface	ethernet1/3									
Device SN	015351000091874	Details													
IP Protocol	tcp	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	LIST	VERDI...	URL	FILE NAME
PCAP	2023/09/21 03:33:31	end	web-browsing		allow	Users_...	f3297...	61...		any					
	2023/09/21 03:38:11	wildfire	web-browsing		allow	Users_...	f3297...		high			malicio...		wildfir...	
	2023/09/21 03:38:11	wildfire	web-browsing		allow	Users_...	f3297...		high			malicio...		wildfir...	

Close

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

Detailed Log View

Log Info | **WildFire Analysis Report**

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 Firefox browser.

Detailed Log View

Log Info | **WildFire Analysis Report**

WildFire Analysis Summary

File Information

File Type	PE
File Signer	
SHA-256	e38d71a0d5cb10244b43b2b879f3dd62a6d22243022337b35976b9c300103052
SHA1	514347c2be886ea97c8752caabef41249ea94774
MD5	9a80e32da46ec5277e0766c9f36750b3
File Size	56033 bytes
First Seen Timestamp	2023-09-21 03:33:07 UTC
Verdict	malware

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERITY	CATEGORY	URL CATEGORIES	VERDICT	URL	FILE NAME
	2023/09/21 03:33:31	end	web-browsing	allow	Users_...	f3297...	61...		any				
	2023/09/21 03:38:11	wildfire	web-browsing	allow	Users_...	f3297...		high			malicio...		wildfir...
	2023/09/21 03:38:11	wildfire	web-browsing	allow	Users_...	f3297...		high			malicio...		wildfir...

Close

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

The screenshot shows a web browser window with the URL https://192.168.1.254/wf_report/public/wildfire.paloaltonetworks.com/443/panos/pdfreport/9/ZFVlcCt4T1d3d. The left sidebar contains a navigation tree for the WildFire Analysis Report, including sections for File Information, Static Analysis (Suspicious File Properties), Dynamic Analysis (VM1 and VM2 configurations), and Host Activity (Process Activity, Network Activity, Event Timeline). The main content area displays the following details:

3.1. VM1 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

3.1.1. Behavioral Summary

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

Behavior	Severity
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.	Medium (3 bars)
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	Medium (3 bars)
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.	Medium (3 bars)
The idle time between two API events are too long. The idle time between two API events are too long.	Medium (3 bars)
Boot or Logon Autostart Execution Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems	Medium (3 bars)

3.1.2. Network Activity

No network data available.

3.1.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\|Users\|Administrator\|sample.exe)

Please Note

For example, section 3.1 provides 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.