



## **PALO ALTO NETWORKS EDU-210**



### **Lab 8: WildFire**

**Document Version: 2021-08-24**

Copyright © 2021 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks 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
Objectives.....	3
Lab Topology .....	4
Theoretical Lab Topology.....	4
Lab Settings .....	5
8 WildFire .....	6
8.0 Load Lab Configuration .....	6
8.1 Renew Expired Certificates .....	9
8.2 Create a WildFire Analysis Profile .....	11
8.3 Modify a Security Profile Group .....	14
8.4 Update WildFire Settings .....	15
8.5 Test the WildFire Analysis Profile.....	16

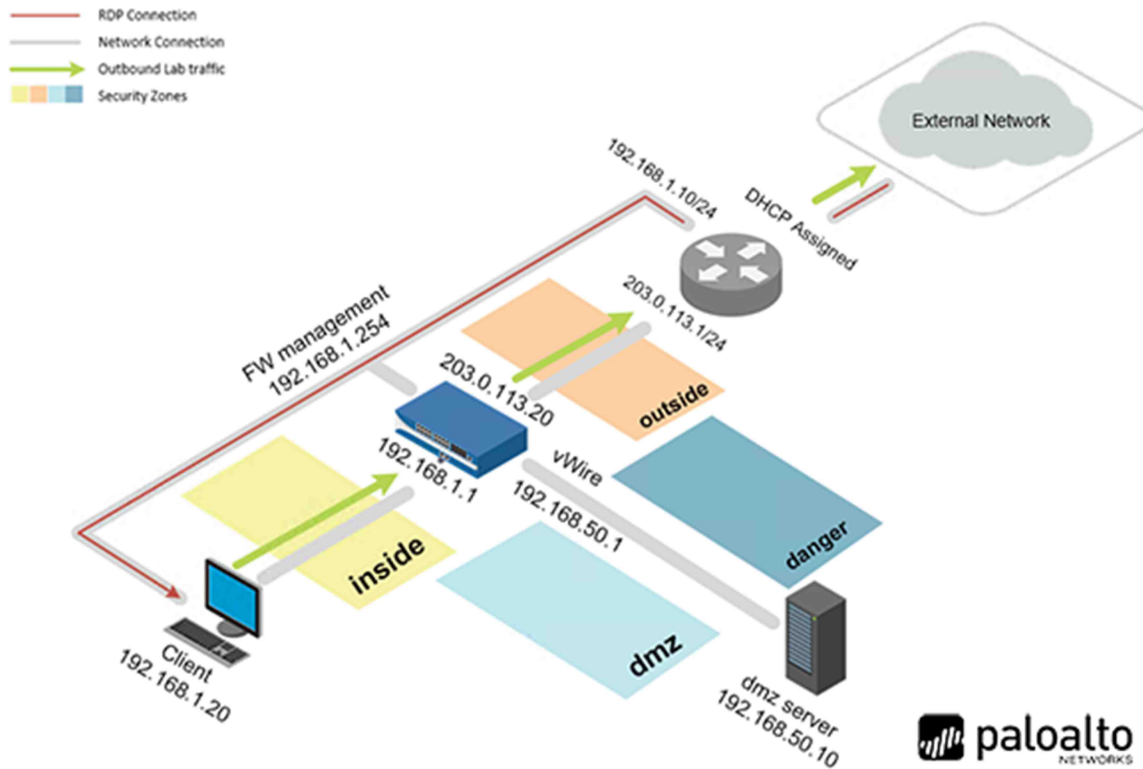
## Introduction

In this exercise, you will configure WildFire and confirm that executable files are sent to WildFire for analysis.

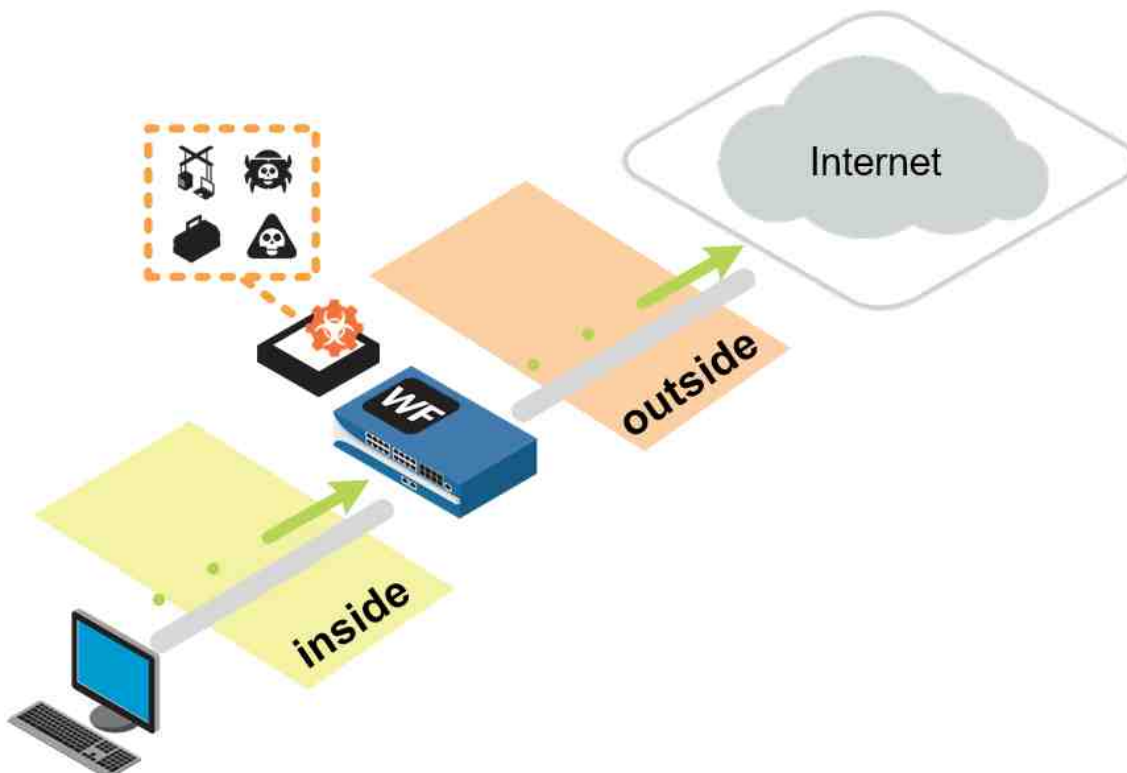
## Objectives

- ) Configure and test a WildFire Analysis Security Profile

## Lab Topology



## 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	Training\$
Firewall	192.168.1.254	admin	Training\$

## 8 WildFire

### 8.0 Load Lab Configuration

1. Launch the Client virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Log in as lab-user using the password Trai n1ng\$.



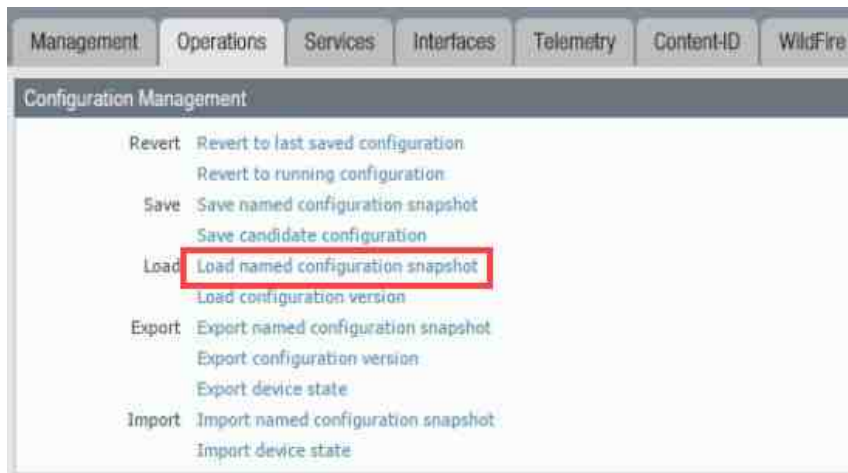
3. Launch the Chromium Web Browser and connect to <https://192.168.1.254>.
4. If a security warning appears, click Advanced and proceed by clicking on Proceed to 192.168.1.254 (unsafe).
5. Log in to the Palo Alto Networks firewall using the following:

Parameter	Value
Name	admin
Password	Trai n1ng\$

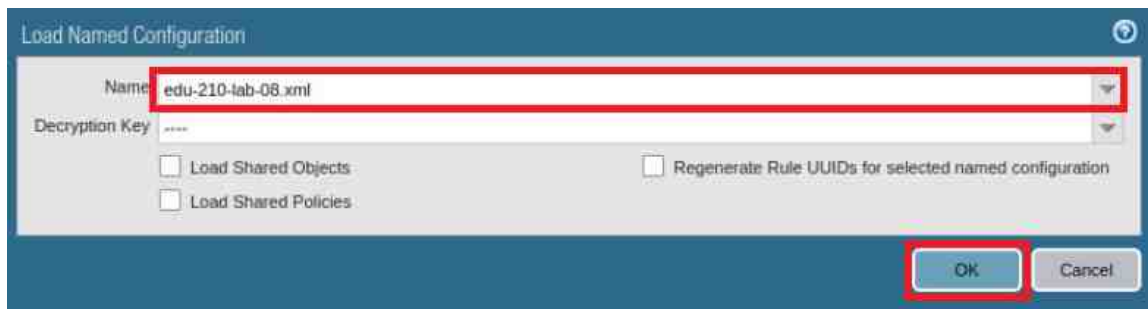
6. In the web interface, select Device > Setup > Operations.



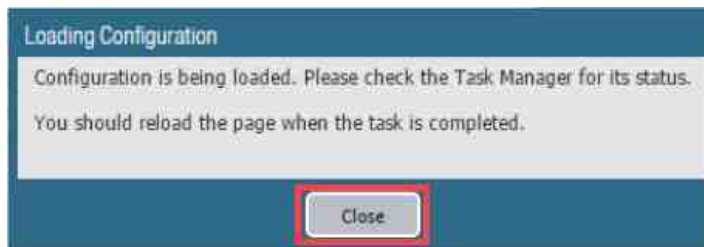
- Click Load named configuration snapshot:



- Click the dropdown list next to the Name text box and select edu-210-lab-08.xml. Click OK.



- Click Close.

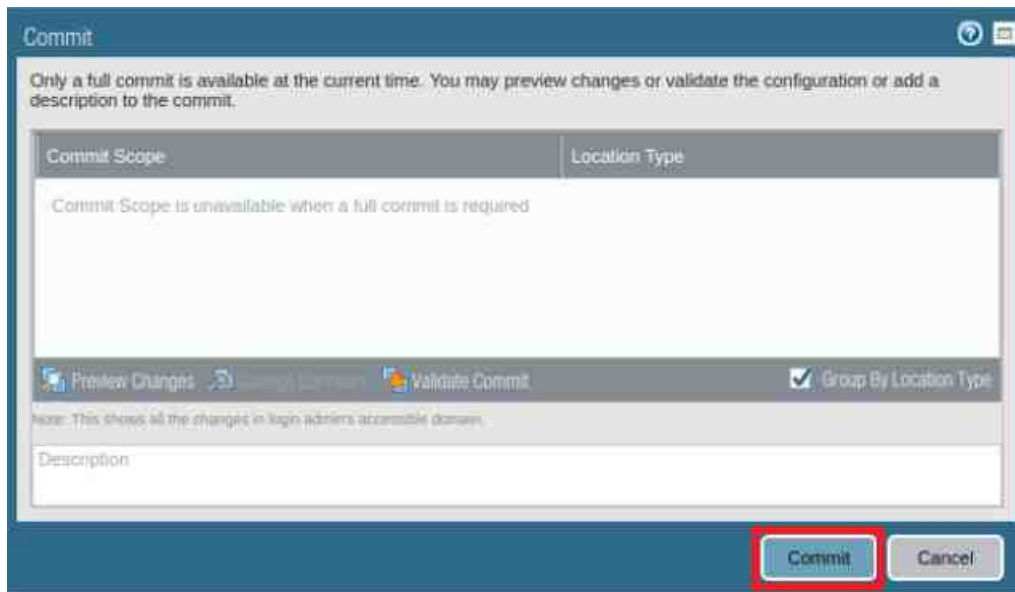


The following instructions are the steps to execute a "Commit All" as you will perform many times throughout these labs.

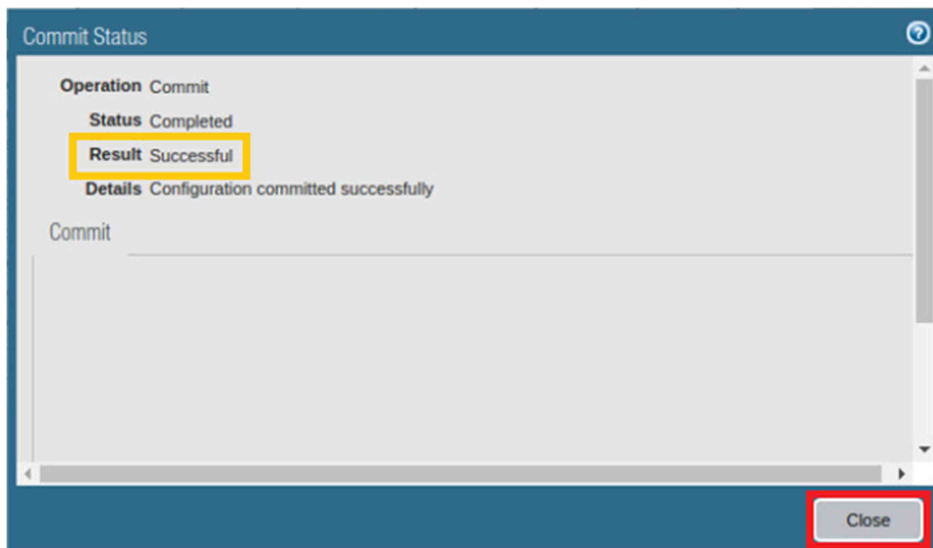
- Click the Commit link at the top-right of the web interface.



11. Click Commit and wait until the commit process is complete.



12. Once completed successfully, click Close to continue.

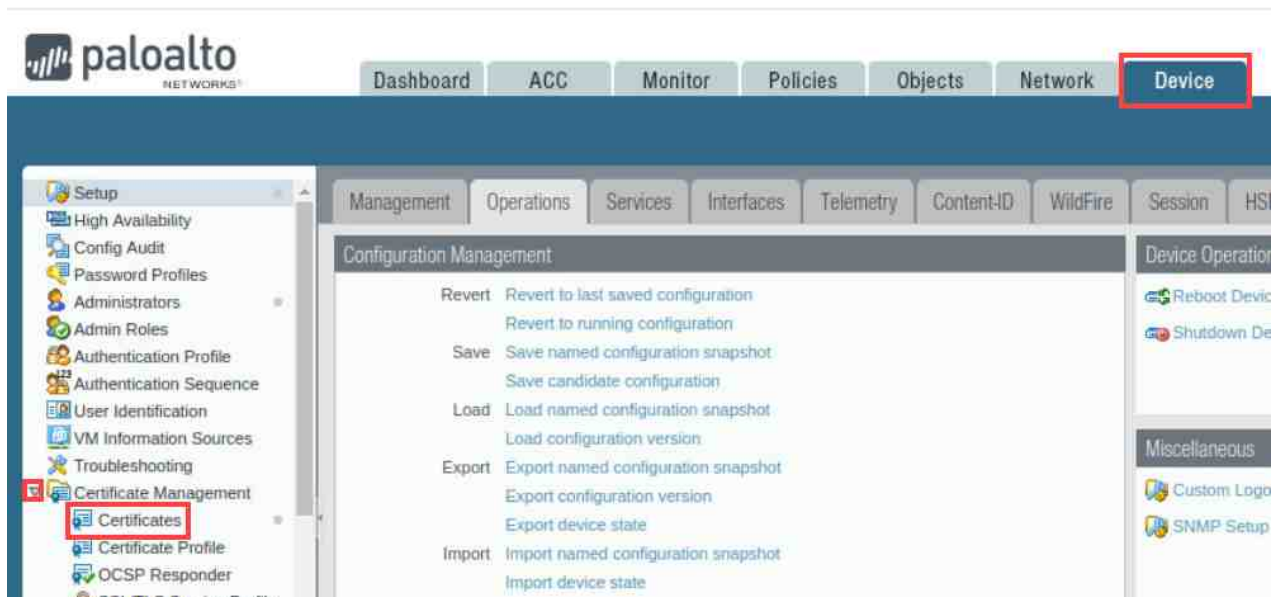


13. Leave the firewall web interface open to continue with the next task.

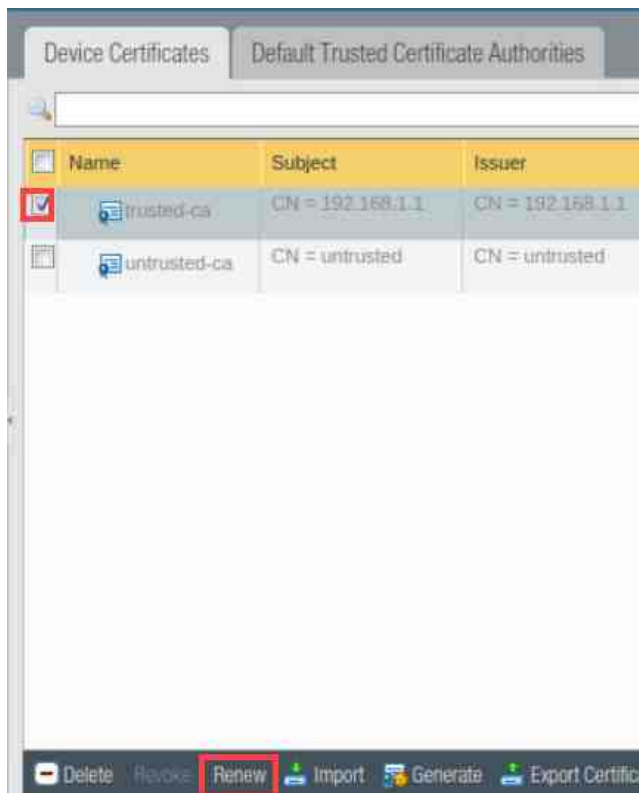


## 8.1 Renew Expired Certificates

1. In the web interface, navigate to Device > Certificate Management > Certificates.



2. Select trusted-ca from the list and click Renew to renew the certificate.



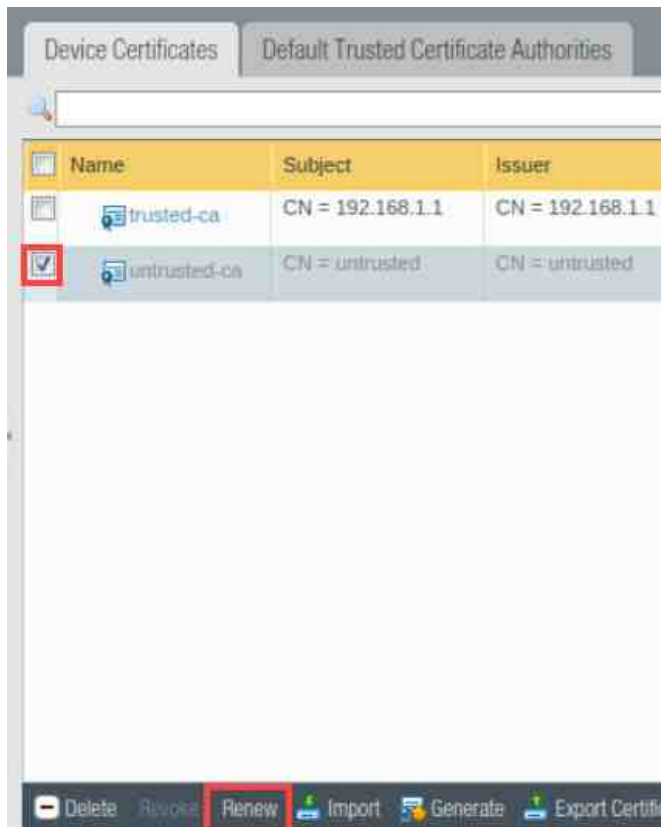
- Accept the default of 365 days and click OK.



- Click OK to confirm.



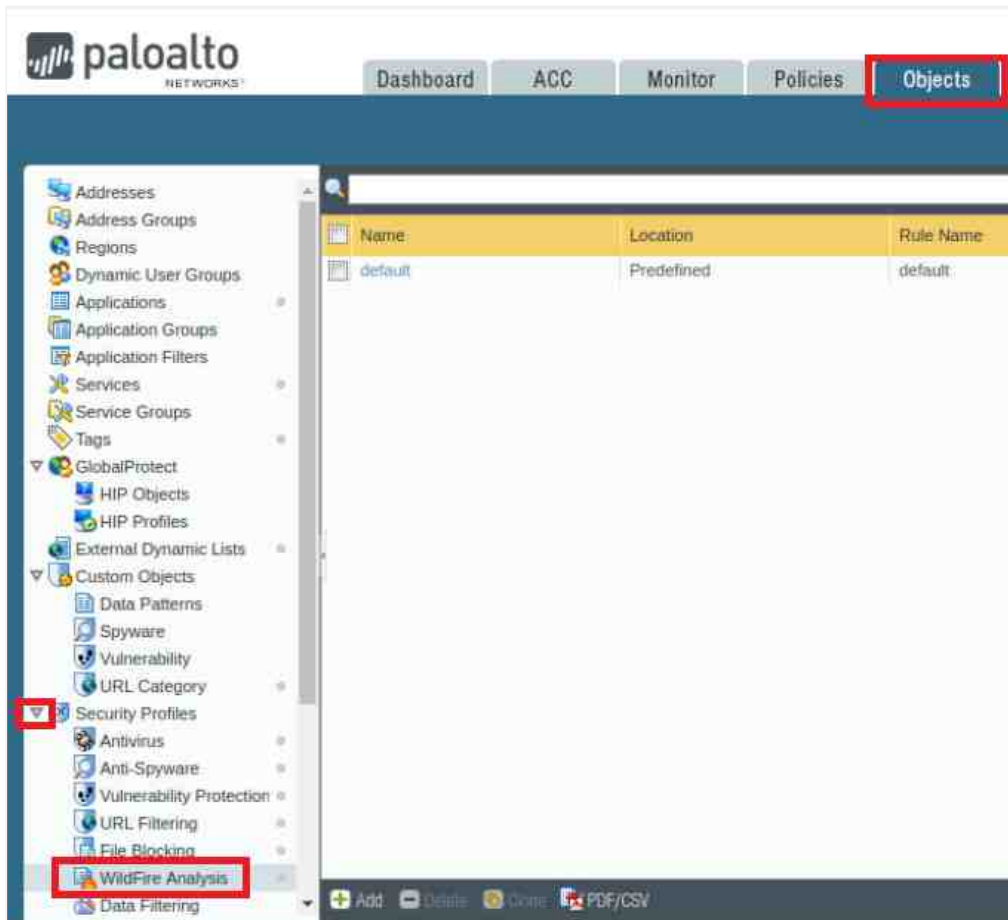
- Unselect trusted-ca from the list, then select untrusted-ca from the list, and click Renew to renew the certificate.



6. Accept the default of 365 days and click OK.
7. Click OK to confirm.
8. Leave the firewall web interface open to continue with the next task.

## 8.2 Create a WildFire Analysis Profile

1. In the web interface, navigate to Objects > Security Profiles > WildFire Analysis.

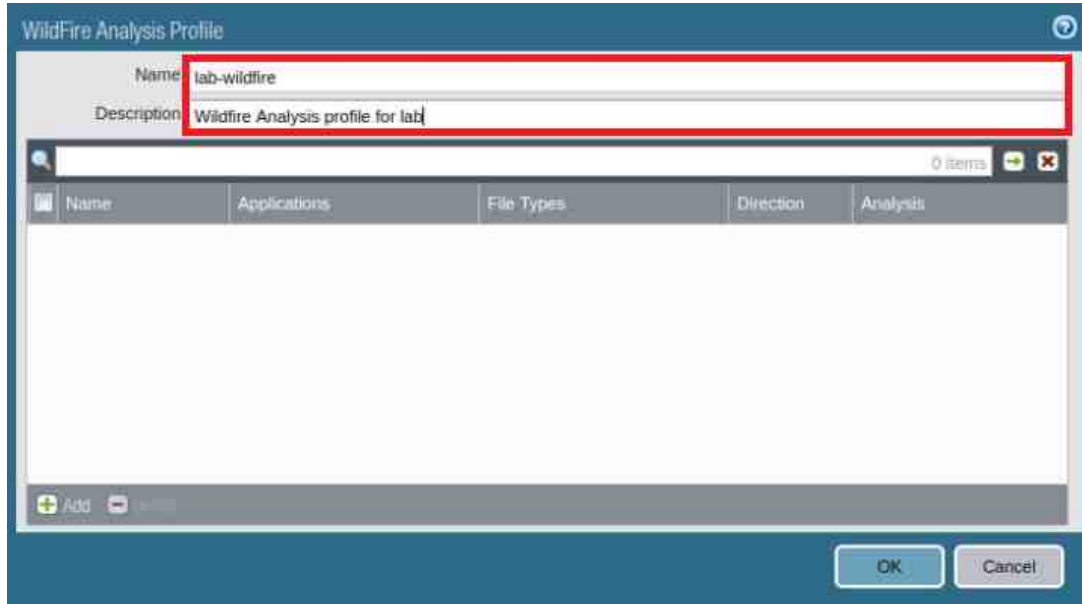


2. Click Add to open the WildFire Analysis Profile configuration window.



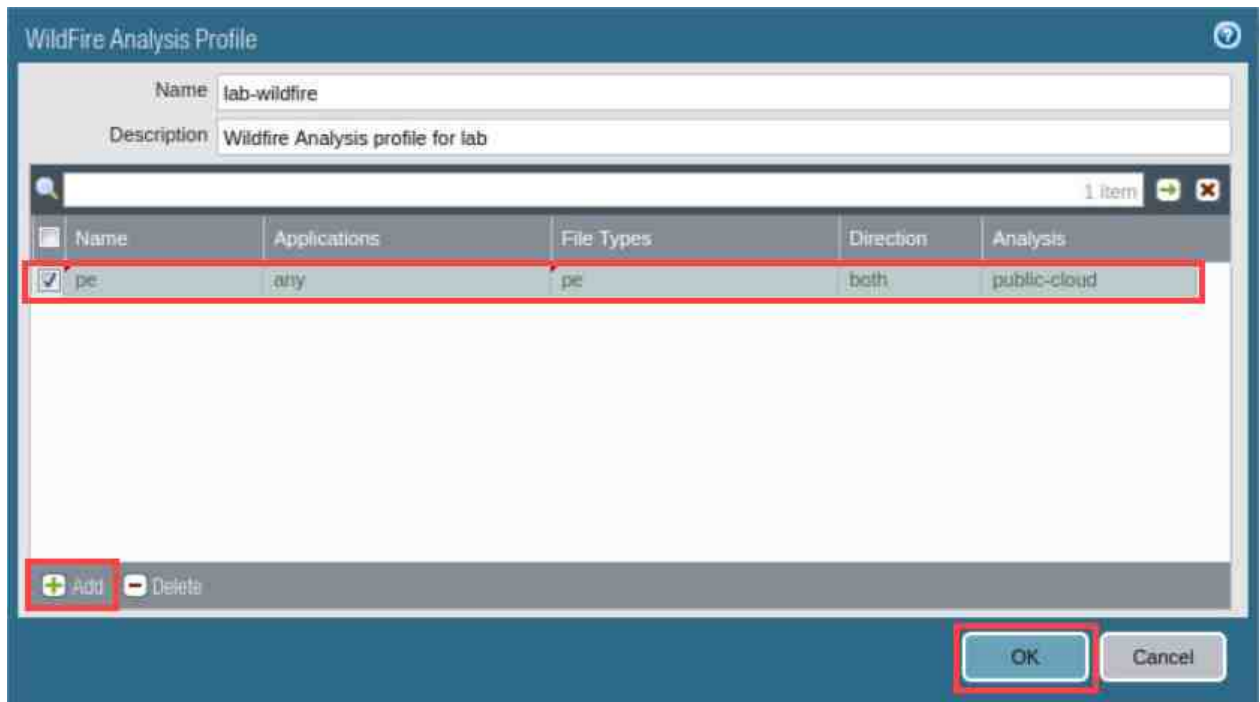
3. In the WildFire Analysis Profile window, configure the following:

Parameter	Value
Name	Type lab-wildfire
Description	Type wildfire Analysis profile for lab



- In the WildFire Analysis Profile window, click Add and configure the following. Once finished, click OK.

Parameter	Value
Name	Type pe
Applications	Verify that any is selected
File Types	Click Add and select pe
Direction	Verify that both is selected
Analysis	Verify that public-cloud is selected

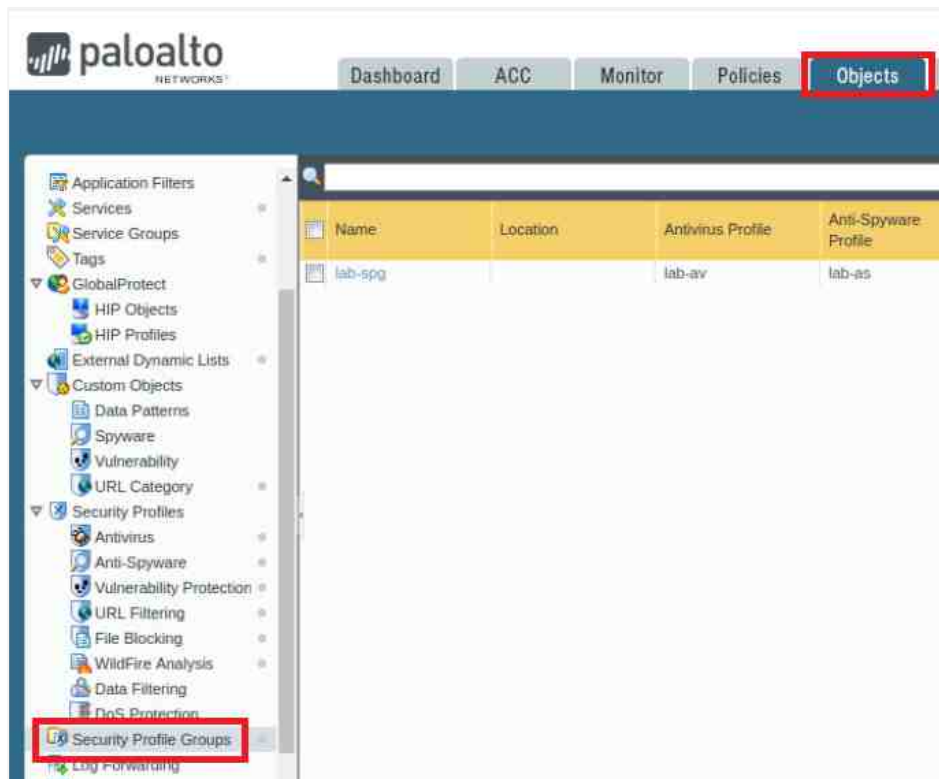


The file type pe includes .cpl, .dll, .efi, .exe, .fon, .ocx, .pif, .scr, and .sys file types.

- Leave the firewall web interface open to continue with the next task.

### 8.3 Modify a Security Profile Group


1. In the web interface, select Objects > Security Profile Groups.



2. Click on lab-spg to open the Security Profile Group.

Name	Location	Antivirus Profile	Anti-Spyware Profile	Vuln Prot
lab-spg		lab-av	lab-as	lab-vp

3. In the Security Profile Group window, add the newly created lab-wildfire from the WildFire Analysis Profile dropdown list. Click OK.

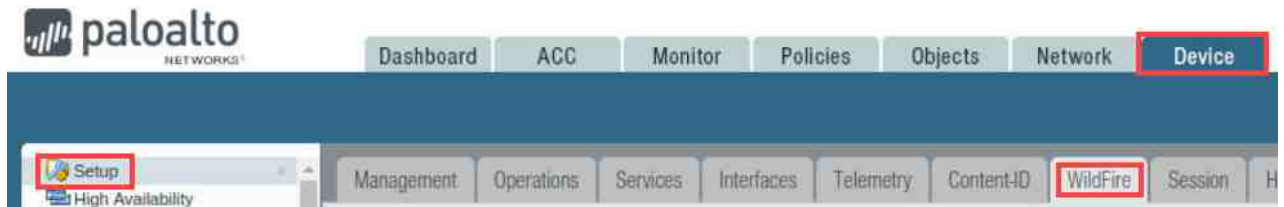


The screenshot shows the 'Security Profile Group' configuration window. The 'Name' field is set to 'lab-spg'. The 'Antivirus Profile' is set to 'lab-av', 'Anti-Spyware Profile' is set to 'lab-as', 'Vulnerability Protection Profile' is set to 'lab-vp', 'URL Filtering Profile' is set to 'lab-url-filtering', 'File Blocking Profile' is set to 'None', and 'Data Filtering Profile' is set to 'None'. The 'WildFire Analysis Profile' dropdown menu is open, showing 'lab-wildfire' selected. The 'OK' button is highlighted with a red box.

4. Leave the firewall web interface open to continue with the next task.

## 8.4 Update WildFire Settings

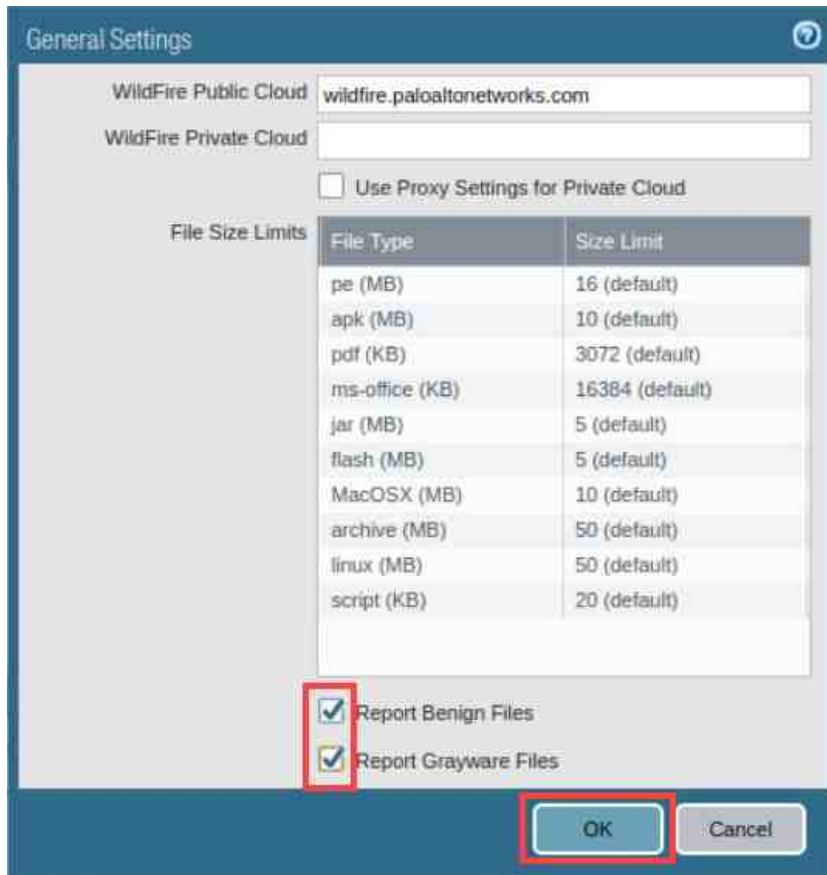
1. In the web interface, navigate to Device > Setup > WildFire.



2. Click the gear icon next to General Settings.



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



4. Commit the new configurations.
5. Leave the firewall web interface open to continue with the next task

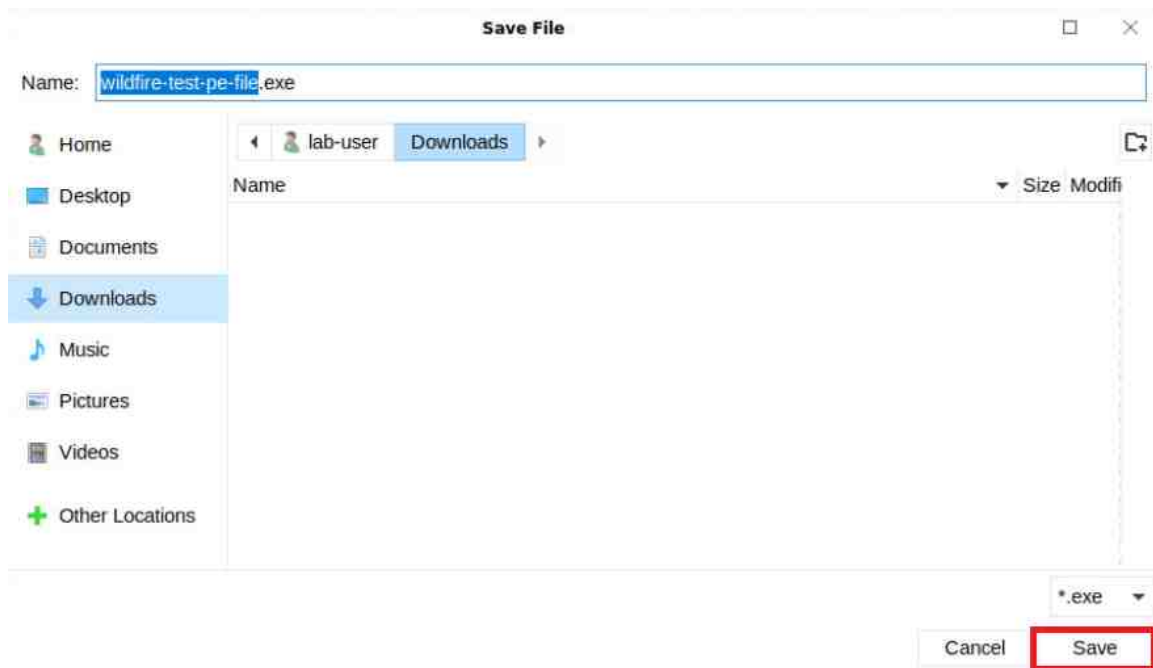
## 8.5 Test the WildFire Analysis Profile

1. Open a new tab in Chromium Web Browser and browse to <http://wildfire.paloaltonetworks.com/publicapi/test/pe>.





- This site generates an attack file with a unique signature, which simulates a zero-day attack. Without opening the file, click Save to save it to the Downloads directory.



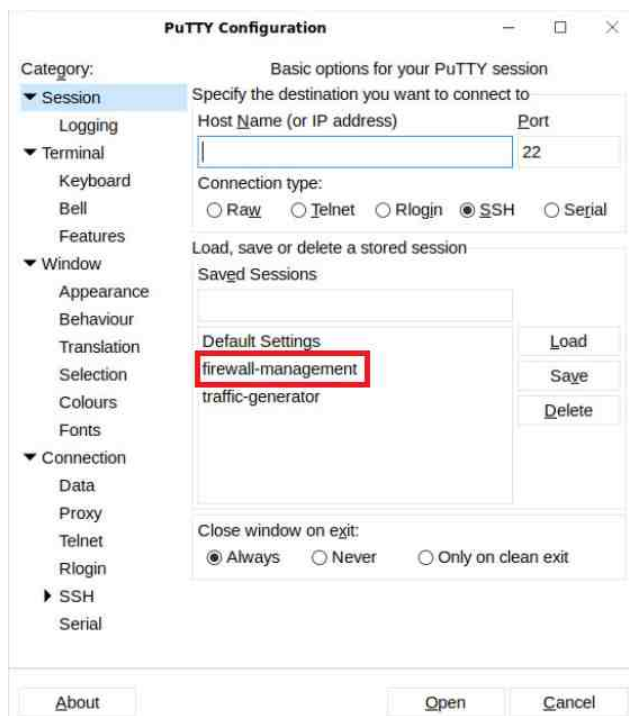
- Click the X to close the notification bar at the bottom of the browser window.



- Close the browser tab.



- On the Client desktop, open PuTTY and double-click firewall-management.



- When prompted for credentials, log in as `admin` with the password `Tra1n1ng$`.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 27 21:11:02 2020

Number of failed attempts since last successful login: 0

admin@firewall-a>
```

- Once logged in, enter the command below to 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:

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

```
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 498 seconds ago, action: upload success
  vsys_id: 1, session_id: 409, transaction_id: 2
  file_len: 55296, flag: 0x801c, file type: pe
  threat id: 52020, user_id: 0, app_id: 109
  from 192.168.1.20/46476 to 35.222.124.72/80
  SHA256: 80b8907c3f9f126f2265ea4f4dbb21f52191ae4ced4c366810486cc9883baa45

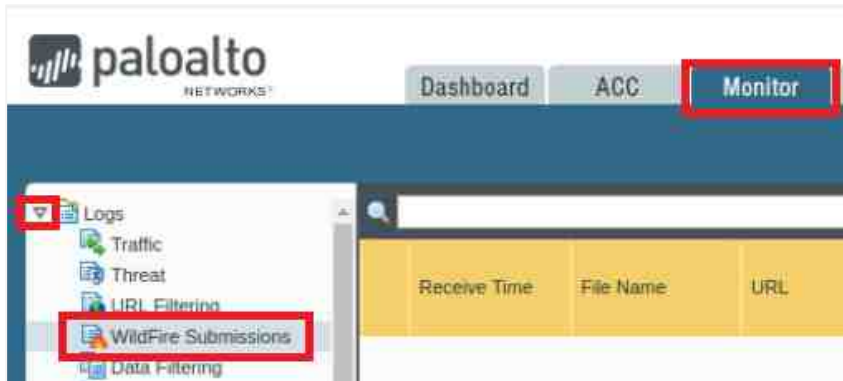
  log: 1, filename: wildfire-test-pe-file.exe
  processed 581 seconds ago, action: skipped - remote verdict pending dup
  vsys_id: 1, session_id: 341, transaction_id: 1
  file_len: 55296, flag: 0x201c, file type: pe
  threat id: 52020, user_id: 0, app_id: 109
  from 192.168.1.20/46452 to 35.222.124.72/80
  SHA256: ae06df42ed59f4157802be40b8c1044de5eadf3b7c8f081a96aa2e2d8fddf9b7

Private Cloud upload logs:

admin@firewall-a>
```

- Type `exit` followed by pressing the Enter key to close the PuTTY session.

- Change focus back to the firewall's web interface and navigate to Monitor > Logs > WildFire Submissions.



- Find the entry for wildfire-test-pe-file.exe that has been submitted to WildFire and identified as malicious.

File Name	URL	Source Zone	Destination Zone	Source address	Source User	Destination address	Dynamic User Group	Destination Port	Application	Rule	Verdict
wildfire-test-pe-f...		inside	outside	192.168.1.20		35.222.124.72		80	web-browsing	egress-outside-content-id	malicious



The WildFire analysis can take 5 to 30 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 see the Detailed Log View of the WildFire entry.

Receive Time	File Name	URL
03/16 18:41:05	wildfire-test-pe-f...	

12. In the Detailed Log View window, while on the Log Info tab, check the information within the General, Details, and Destination panels. Once finished, click Close.



The screenshot shows the 'Detailed Log View' window with the 'Log Info' tab selected. The window is divided into three main panels: General, Source, and Destination. The General panel contains session details, the Source panel shows source user and network information, and the Destination panel shows destination user and network information. Below these panels is a table of log entries, and a 'Close' button is at the bottom right.

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2020/03/16 18:29:28	end	web-browsing	allow	egress-outside-content-id	db6ad...	62...		lab-decry...				
	2020/03/16 18:41:05	wildfire	web-browsing	allow	egress-outside-content-id	db6ad...		high			malici...		wildfir..

13. The lab is now complete; you may end the reservation.