



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



### **Lab 8: WildFire**

**Document Version: 2019-11-12**

Copyright © 2019 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
1 WildFire .....	6
1.0 Load Lab Configuration .....	6
1.1 Create a WildFire Analysis Profile .....	9
1.2 Modify a Security Profile Group .....	11
1.3 Test the WildFire Analysis Profile.....	12

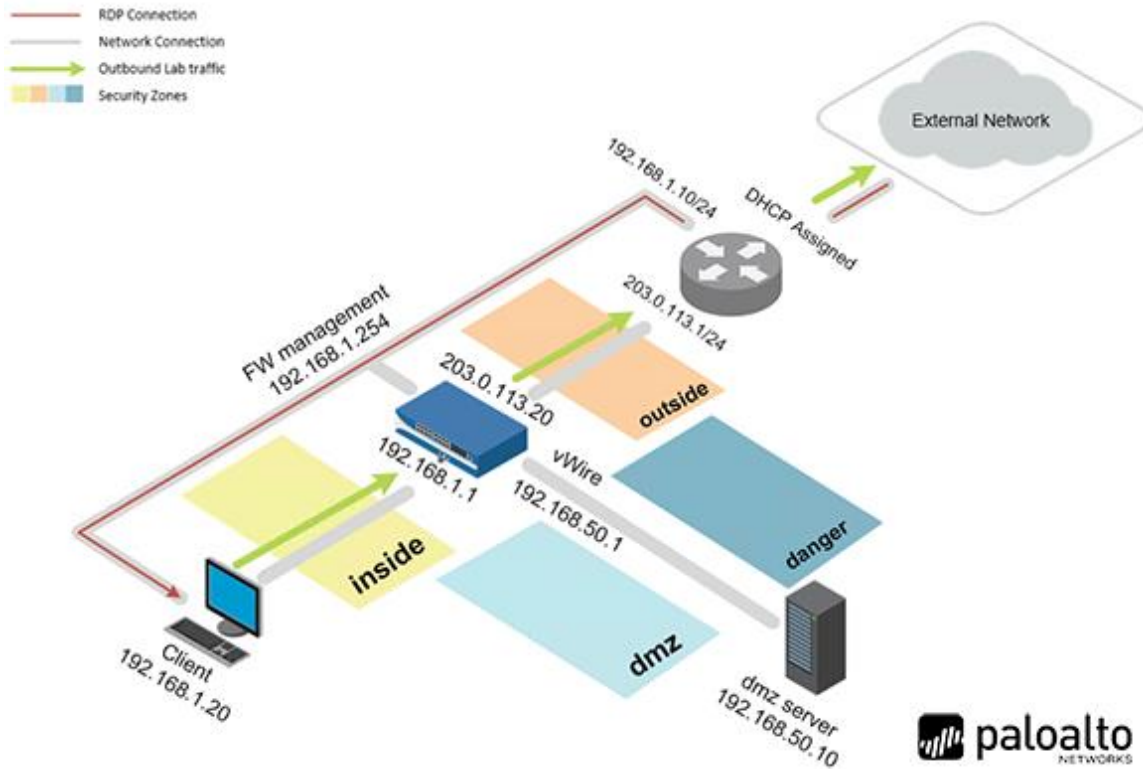
## Introduction

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

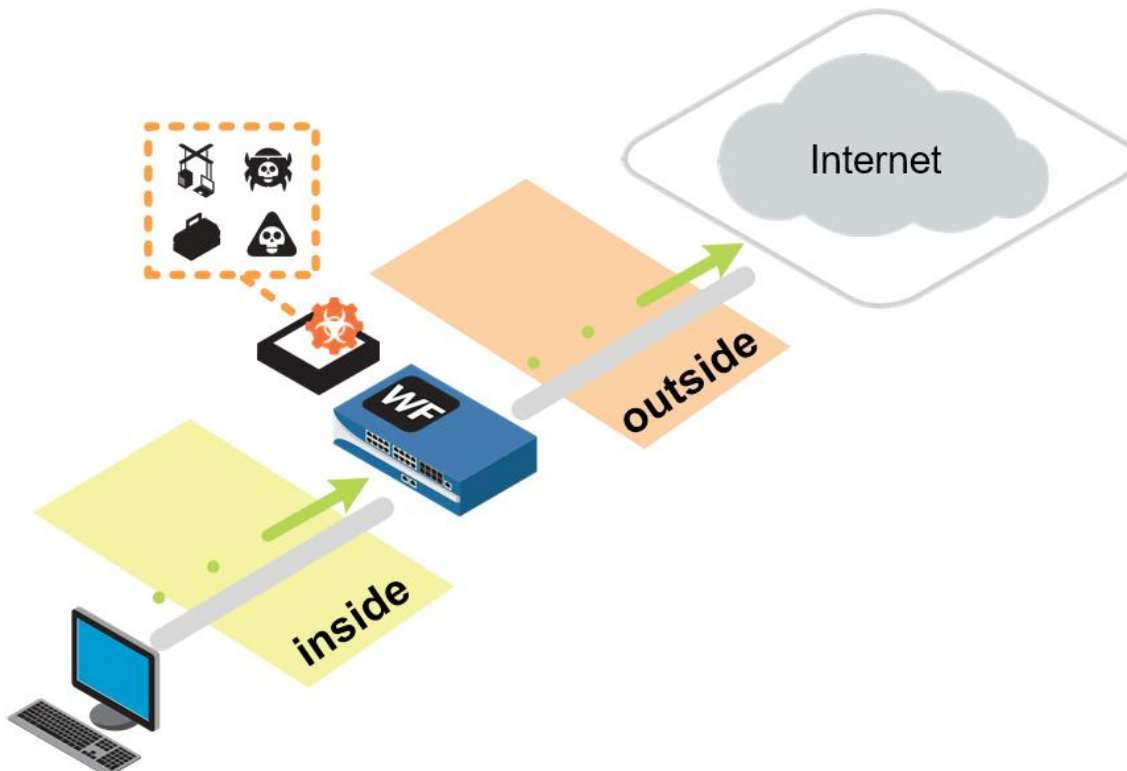
## Objectives

- 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	Pa10A1t0
Firewall	192.168.1.254	admin	admin

## 1 WildFire

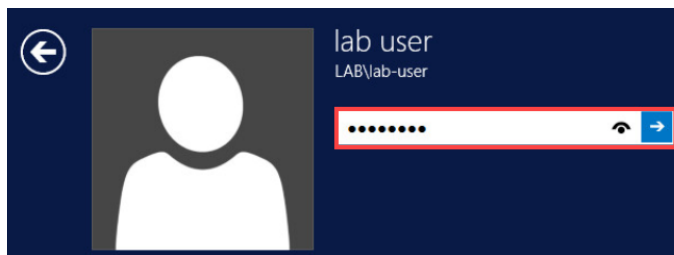
### 1.0 Load Lab Configuration

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. Click within the splash screen to bring up the login screen. Log in as **lab-user** using the password **Pa10A1t0**.



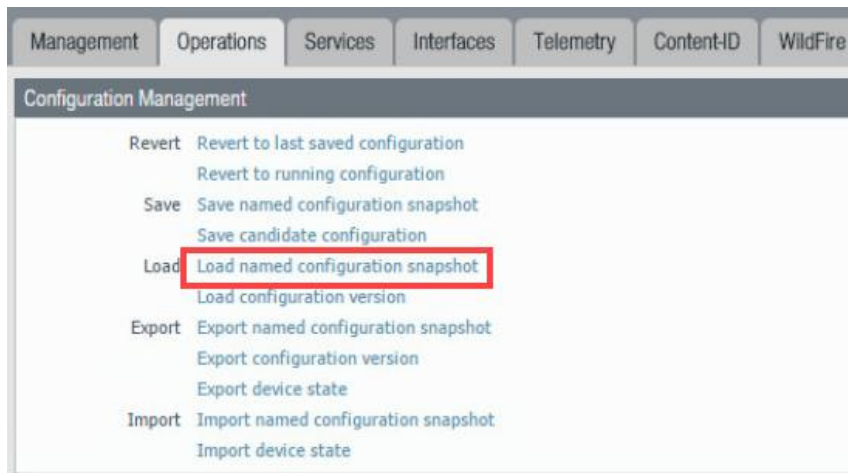
3. Launch the **Chrome** browser and connect to <https://192.168.1.254>.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

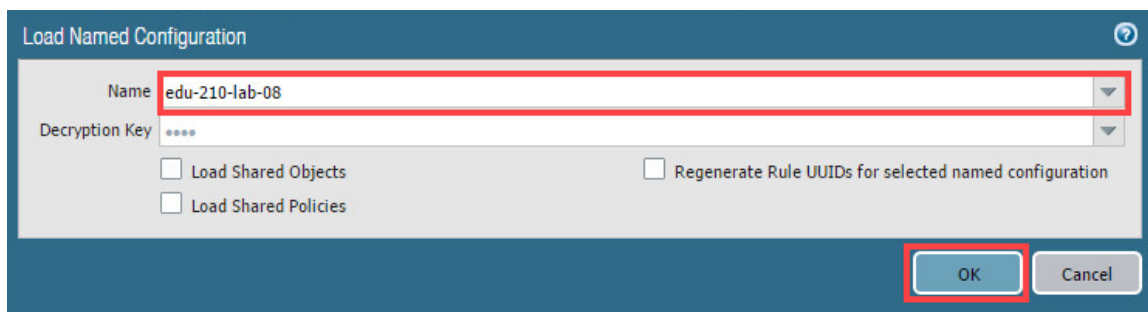
6. In the web interface, navigate to **Device > Setup > Operations**.



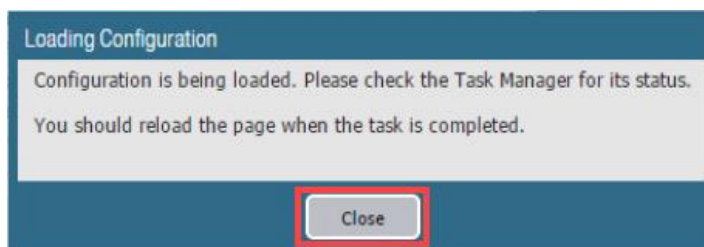
7. Click **Load named configuration snapshot**:



8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-08**. Click **OK**.



9. Click **Close**.

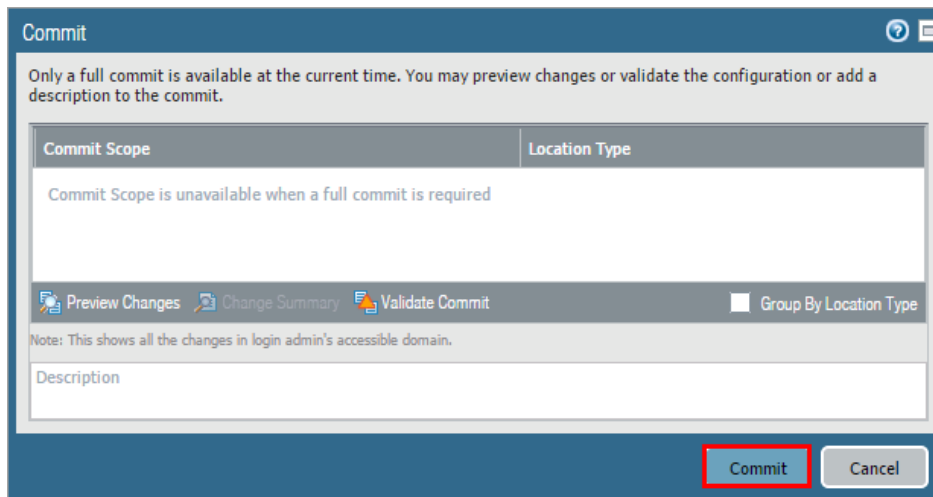


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

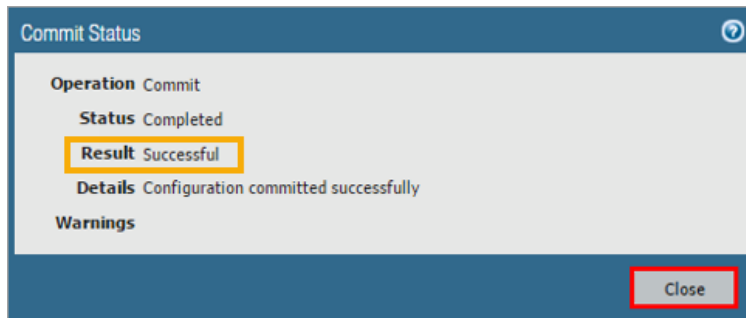
10. Click the **Commit** link at the top-right of the web interface.



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



12. Once completed successfully, click **Close** to continue.

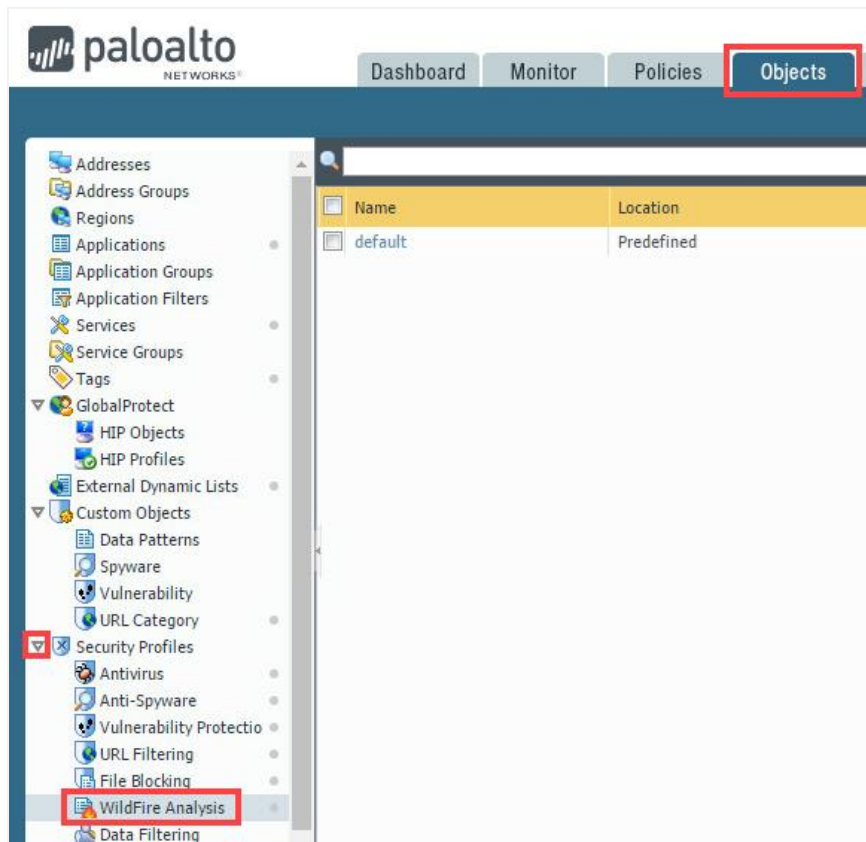


13. Leave the firewall web interface open to continue with the next task.



## 1.1 Create a WildFire Analysis Profile

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

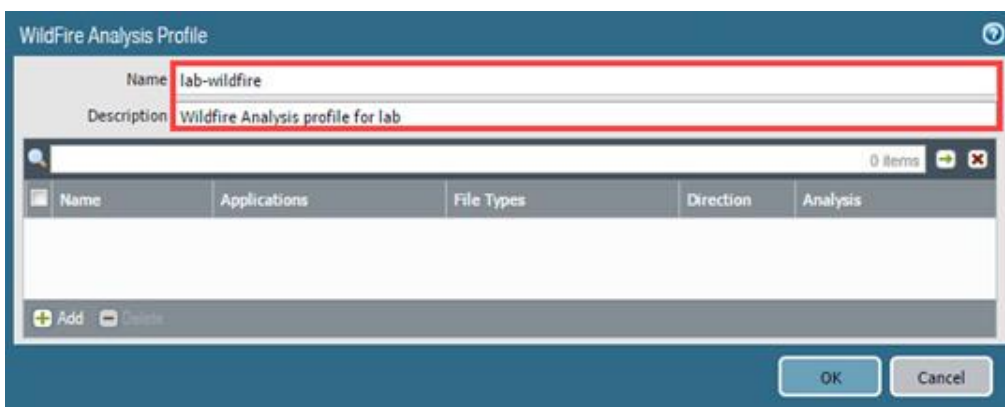


2. Click **Add** to open the *WildFire Analysis Profile* configuration window.



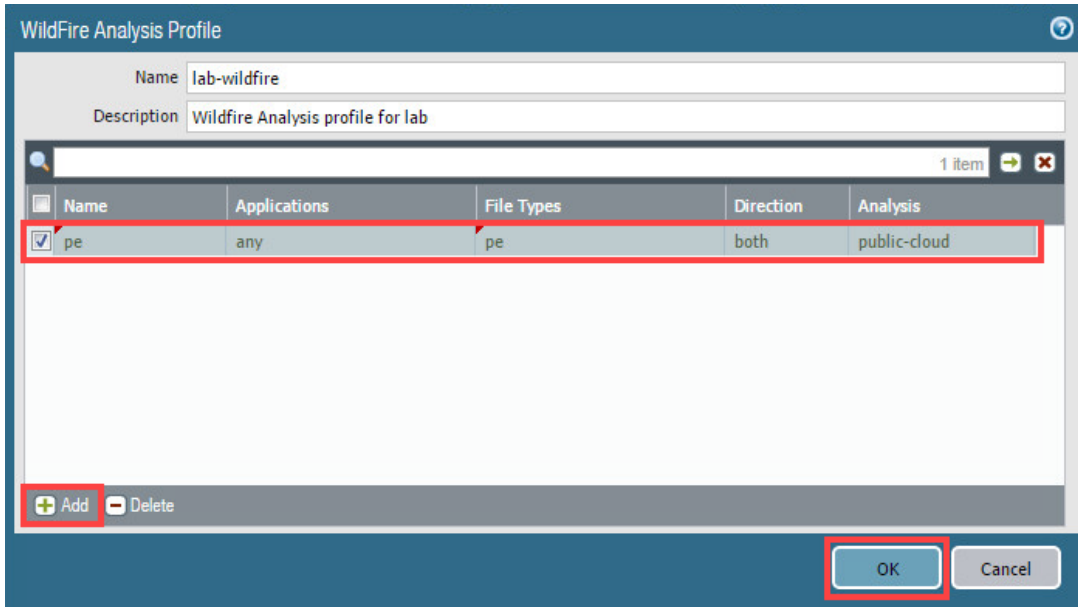
3. In the *WildFire Analysis Profile* window, configure the following:

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



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

Parameter	Value
Name	Type <b>pe</b>
Applications	Verify that <b>any</b> is selected
File Types	Click <b>Add</b> and select <b>pe</b> from the drop-down list
Direction	Verify that <b>both</b> is selected
Analysis	Verify that <b>public-cloud</b> is selected

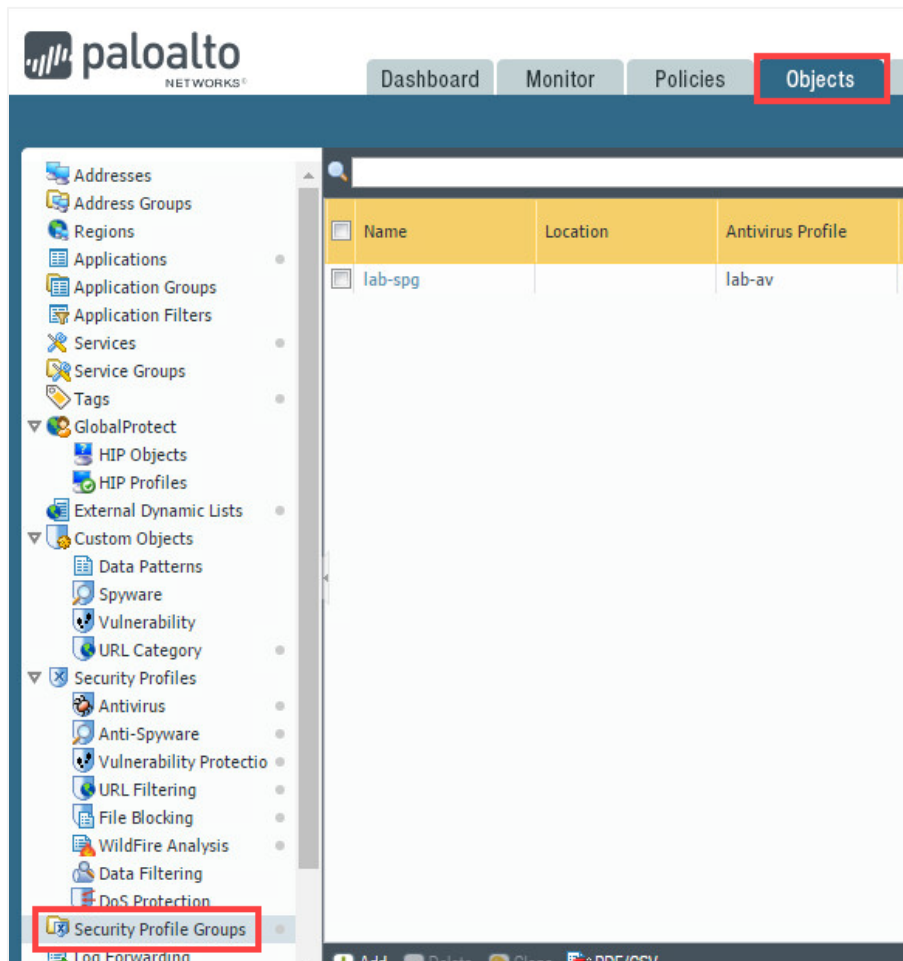



The file type **pe** includes .cpl, .dll, .efi, .exe, .fon, .ocx, .pif, .scr, and .sys file types.

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

## 1.2 Modify a Security Profile Group

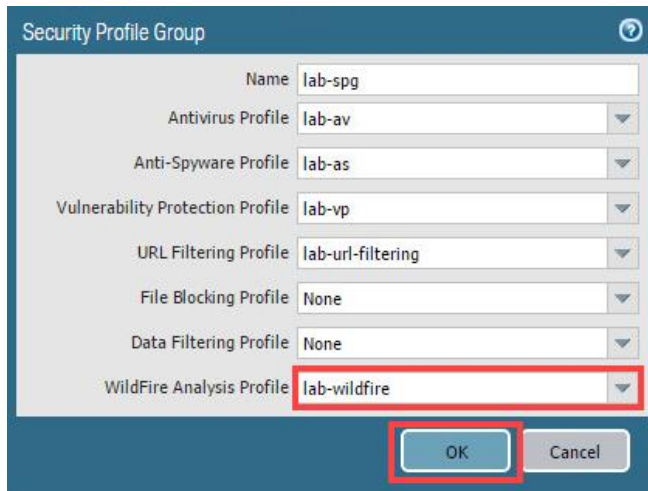
1. In the web interface, select **Objects > Security Profile Groups**.



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-

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



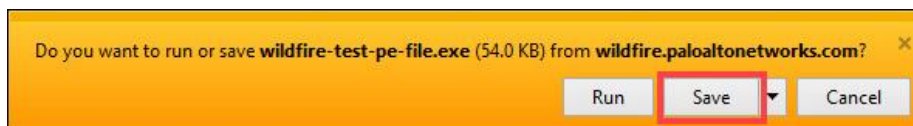
4. **Commit** all changes.
5. Leave the firewall web interface open to continue with the next task.

### 1.3 Test the WildFire Analysis Profile

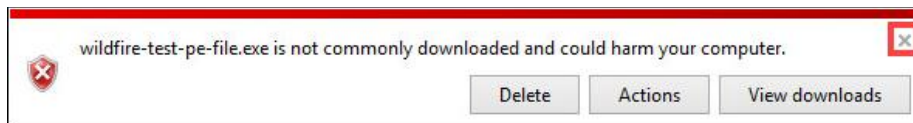
1. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to <http://wildfire.paloaltonetworks.com/publicapi/test/pe>.



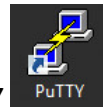
2. This site generates an attack file with a unique signature, which simulates a zero-day attack. Without opening the file, save it to the *Downloads* directory.



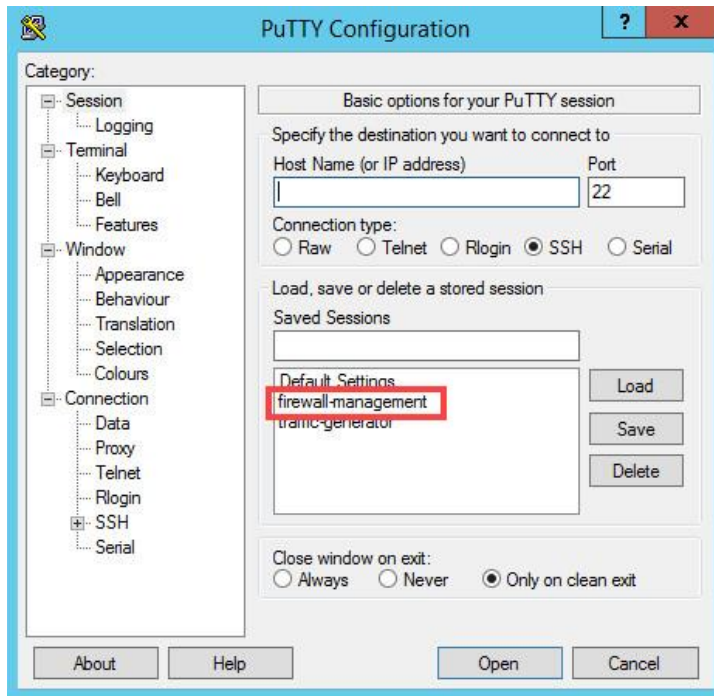
3. If prompted, close the message box stating that the *EXE* file may be harmful.



4. Close the **IE** browser.



5. On the Windows desktop, open **PuTTY** and double-click **firewall-management**.



6. When prompted for credentials, log in as **admin** with the password **admin**.

```
login as: admin
Using keyboard-interactive authentication.
Password:

Number of failed attempts since last successful login: 0

admin@firewall-a> █
```

- Once logged in, enter the command below command 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
```

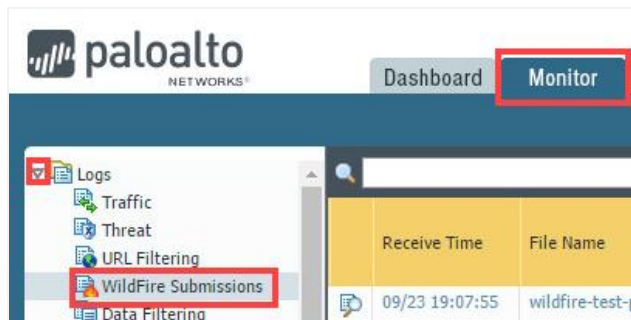
```
admin@firewall-a> debug wildfire upload-log show

Upload Log disk log rotation size: 2.000 MB.
Public Cloud upload logs:

  log: 0, filename: wildfire-test-pe-file.exe
  processed 1660 seconds ago, action: upload success
  vsys_id: 1, session_id: 506, transaction_id: 1
  file_len: 55296, flag: 0x801c, file type: pe
  threat id: 52020, user_id: 0, app_id: 109
  from 192.168.1.20/42493 to 52.70.105.11/80
  SHA256: c5ce611cbc774e8d77097255d864e9b3bbf00065f8d9e56f9ca8e32d38078f02
Private Cloud upload logs:

admin@firewall-a>
```

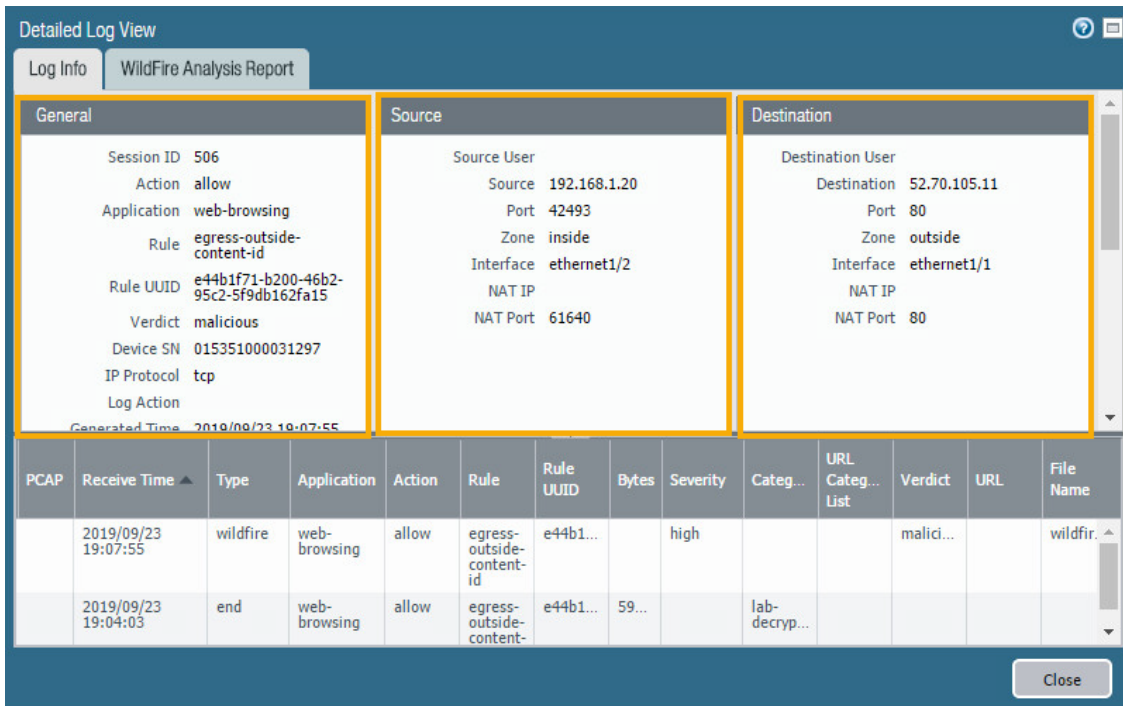
- Type **exit** followed by pressing the **Enter** key to close the *PuTTY* session.
- Change focus back to the firewall's web interface and navigate to **Monitor > Logs > WildFire Submissions**.



- After five minutes have passed, find the entry for *wildfire-test-pe-file.exe* that has been submitted to *WildFire* and identified as malicious. Click the **magnifying glass** icon next to the entry to see the *Detailed Log View* of the *WildFire* entry.

	Receive Time	File Name	Source Zone	Destinati... Zone	Source address	Destination address	Desti... Port	Application	Rule	Verdict
	09/23 19:07:55	wildfire-test-pe-file.exe	inside	outside	192.168.1.20	52.70.105.11	80	web-browsing	egress-outside-content-id	malicious

11. In the *Detailed Log View* window, while on the *Log Info* tab, check the information within the *General*, *Details*, and *Destination* panels.



**Detailed Log View**

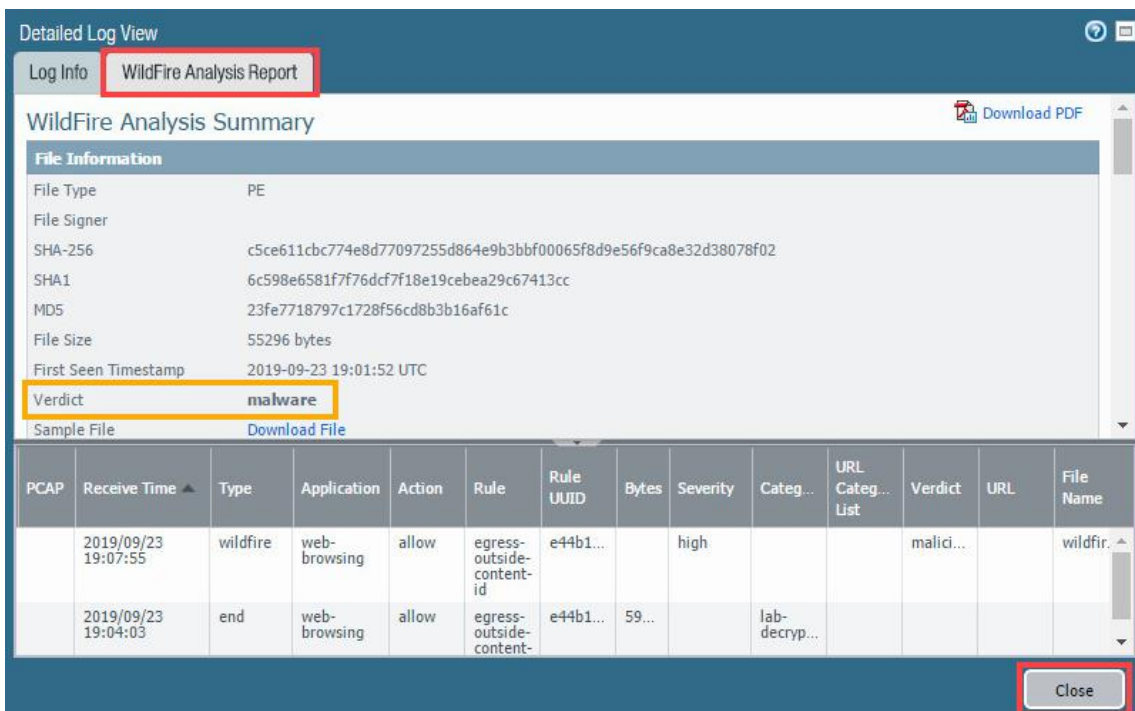
Log Info | WildFire Analysis Report

General		Source		Destination	
Session ID	506	Source User		Destination User	
Action	allow	Source	192.168.1.20	Destination	52.70.105.11
Application	web-browsing	Port	42493	Port	80
Rule	egress-outside-content-id	Zone	inside	Zone	outside
Rule UUID	e44b1f71-b200-46b2-95c2-5f9db162fa15	Interface	ethernet1/2	Interface	ethernet1/1
Verdict	malicious	NAT IP		NAT IP	
Device SN	015351000031297	NAT Port	61640	NAT Port	80
IP Protocol	tcp				
Log Action					
Generated Time	2019/09/23 19:07:55				

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/09/23 19:07:55	wildfire	web-browsing	allow	egress-outside-content-id	e44b1...		high			malici...		wildfir...
	2019/09/23 19:04:03	end	web-browsing	allow	egress-outside-content-id	e44b1...	59...		lab-decrypt...				

Close

12. Click the **WildFire Analysis Report** tab and review the available information. Notice that the verdict for this file is malware. Scroll down to view more information such as *Static Analysis*, *Dynamic Analysis*, *Network Activity*, *Host Activity* (by process), and *Report Incorrect Verdict*. Once finished, click **Close**.



**Detailed Log View**

Log Info | **WildFire Analysis Report**

WildFire Analysis Summary

Download PDF

File Information	
File Type	PE
File Signer	
SHA-256	c5ce611cbc774e8d77097255d864e9b3bbf00065f8d9e56f9ca8e32d38078f02
SHA1	6c598e6581f7f76dcf7f18e19cebea29c67413cc
MD5	23fe7718797c1728f56cd8b3b16af61c
File Size	55296 bytes
First Seen Timestamp	2019-09-23 19:01:52 UTC
Verdict	<b>malware</b>
Sample File	<a href="#">Download File</a>

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/09/23 19:07:55	wildfire	web-browsing	allow	egress-outside-content-id	e44b1...		high			malici...		wildfir...
	2019/09/23 19:04:03	end	web-browsing	allow	egress-outside-content-id	e44b1...	59...		lab-decrypt...				

Close

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