PALO ALTO NETWORKS - EDU-210

Lab 8: WildFire

Document Version: 2017-09-29

Contents

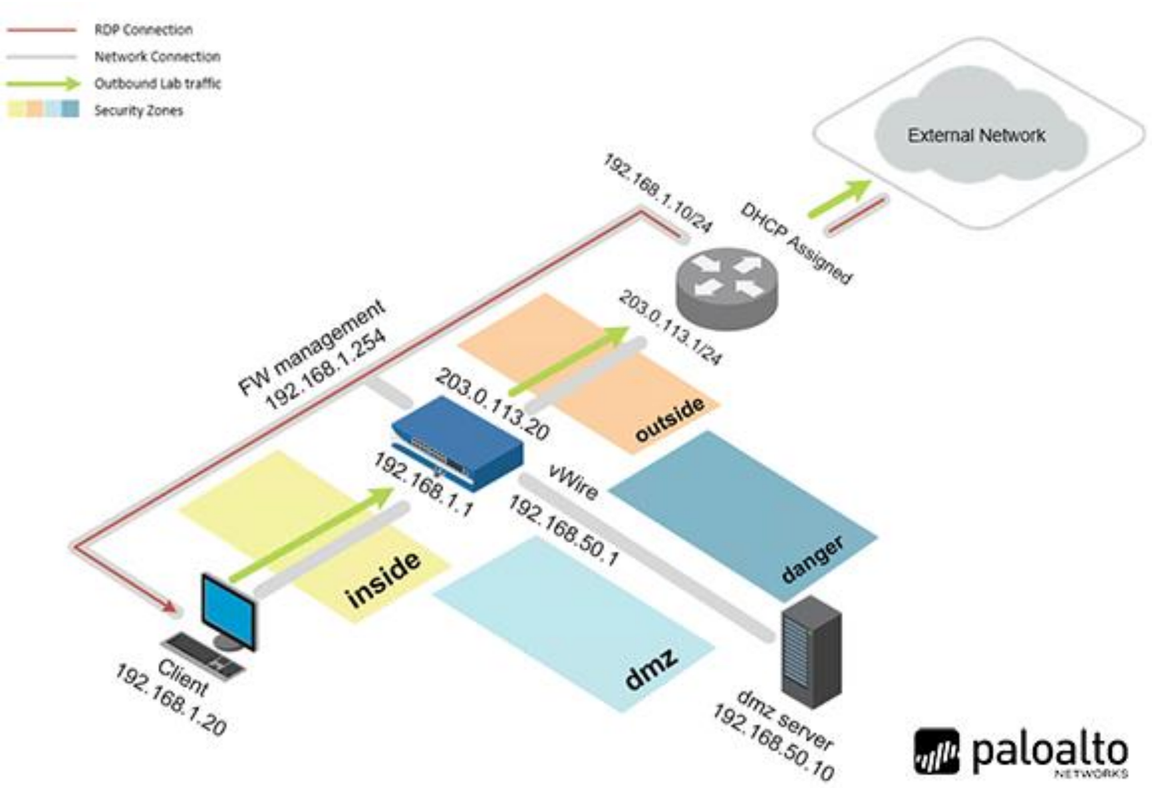
Introduction

Today about 45% of all web sites are encrypted using SSL and about 90% of the applications used within an organization are web-based ssl or ssl enabled. To correctly identify the application or inspect the traffic for threats we first need to be able to decrypt that information. In this exercise you will begin testing ssl decryption, in order to evaluate how to implement decryption within your environment.

Objectives

- Create Security zones two different ways and observe the time saved.
- Create Interface Management Profiles to allow ping and responses pages.
- Configure Ethernet interfaces to observe DHCP client options and static configuration.
- Create a virtual router and attach configured Ethernet interfaces.
- Test connectivity with automatic default route configuration and static configuration.

Lab Topology



Lab Settings

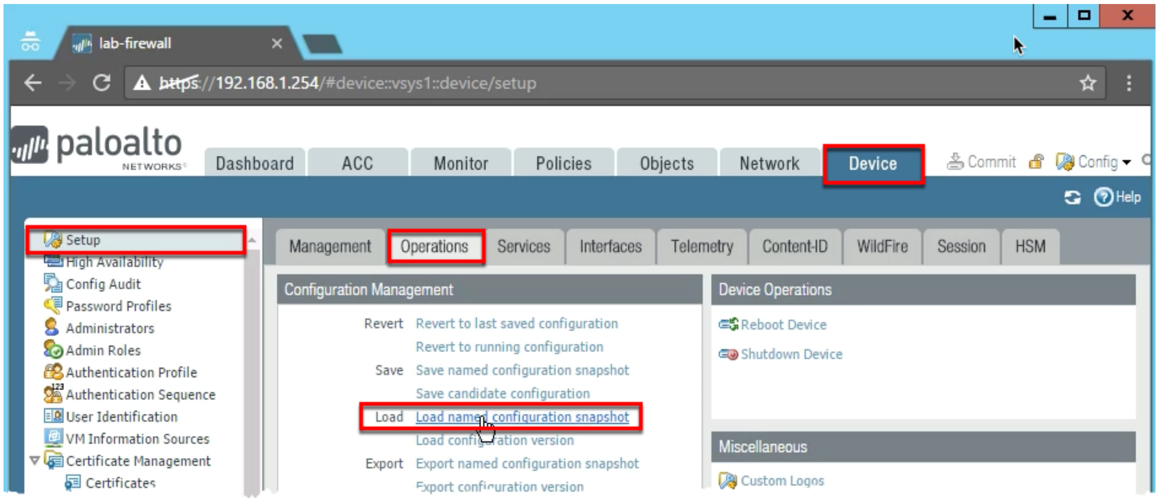
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

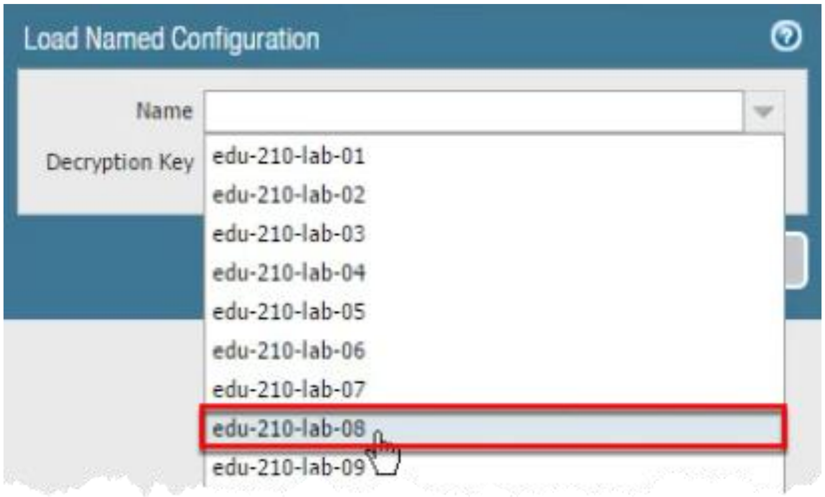
8 Lab: WildFire

8.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



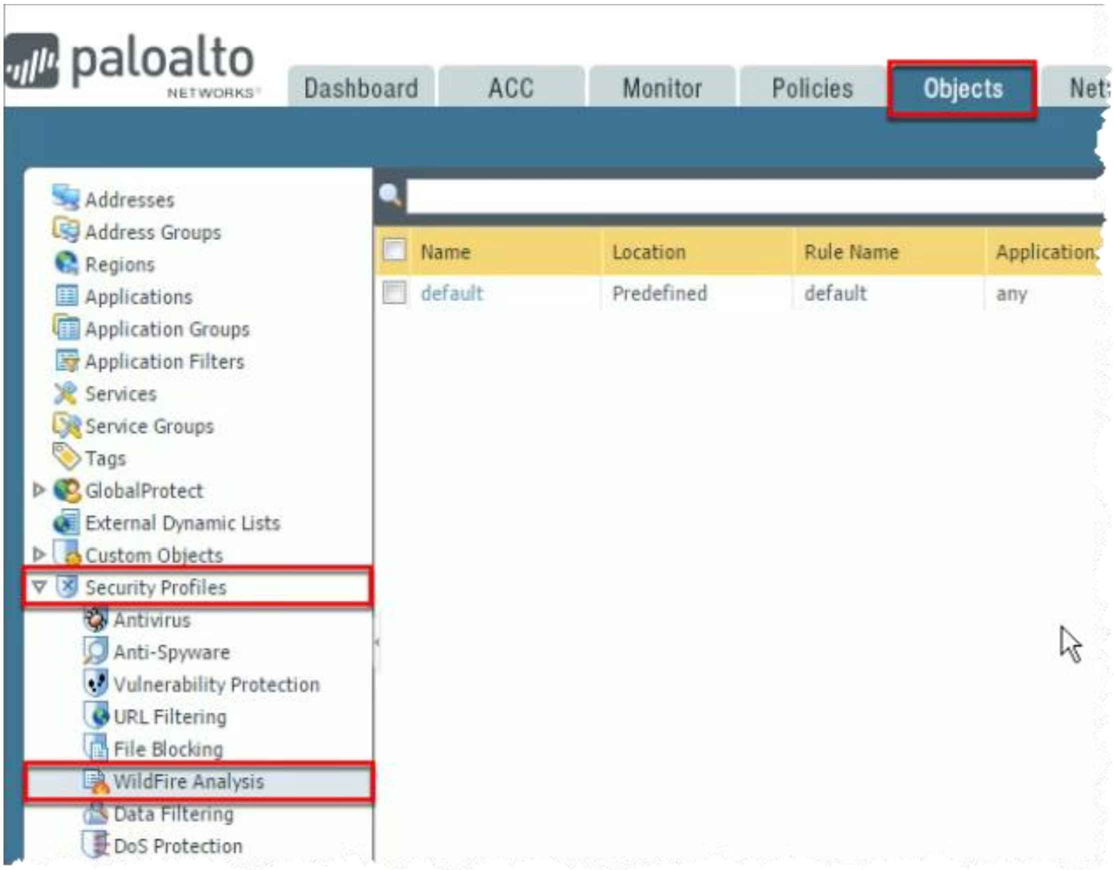
3. Select **edu-210-lab-07** and click **OK**.



4. Click **Close**.
5. **Commit** all changes.

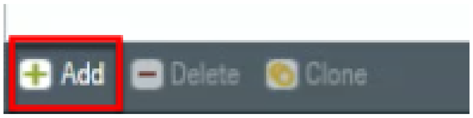
8.1 Create a WildFire Analysis Profile

1. In the WebUI select **Objects > Security Profiles > WildFire Analysis**.



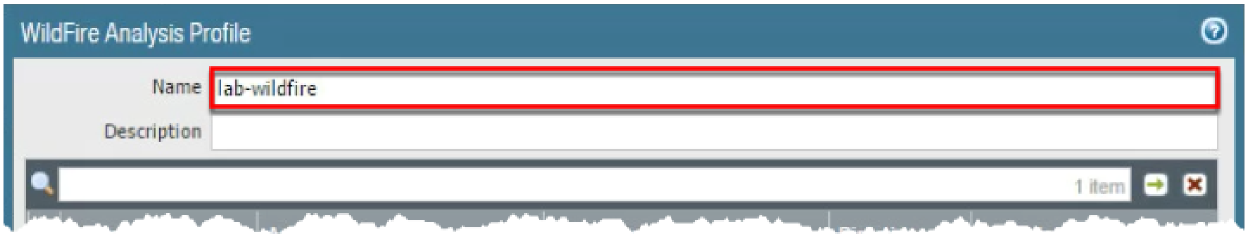
Name	Location	Rule Name	Application
default	Predefined	default	any

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



3. Configure the following:

Parameter	Value
Name	`lab-wildfire`



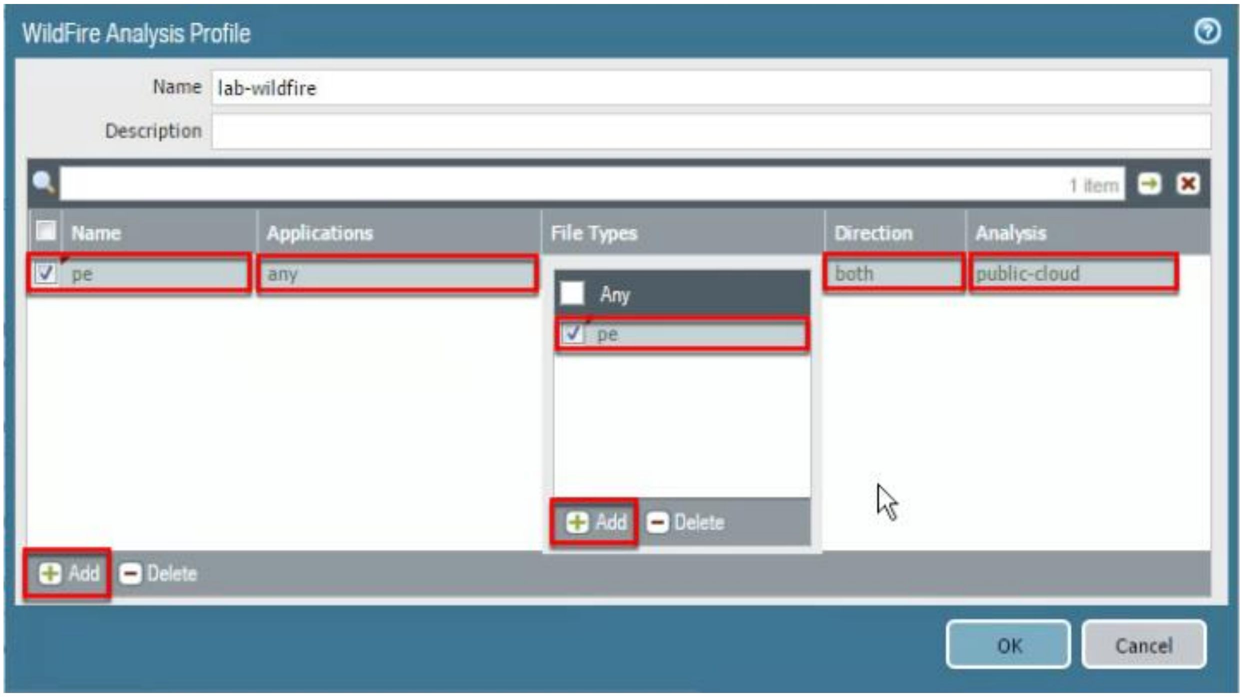
WildFire Analysis Profile

Name: lab-wildfire

Description:

4. Click **Add** and configure the following:

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



WildFire Analysis Profile

Name: lab-wildfire

Description:

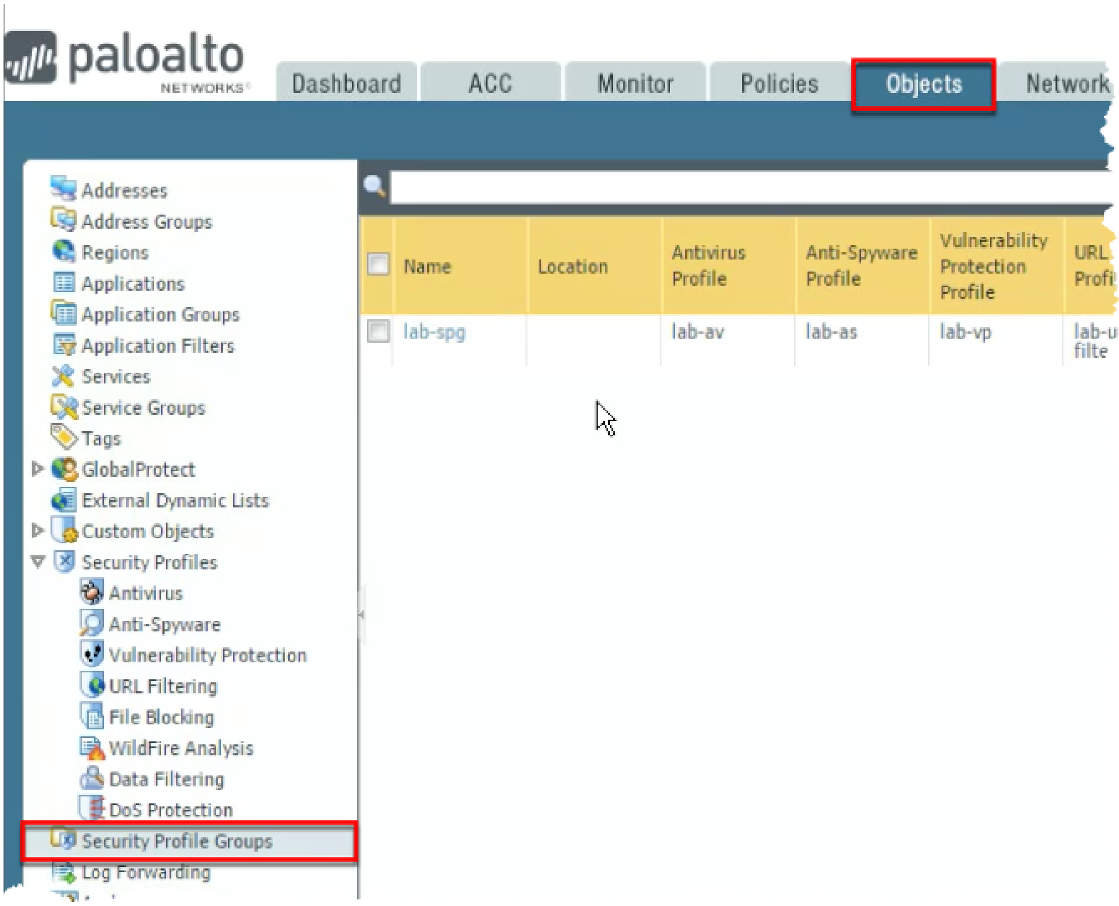
Name	Applications	File Types	Direction	Analysis
☑ pe	any	□ Any ☑ pe	both	public-cloud

Note: The file type `pe` includes both .exe and `.dll` file types.

5. Click **OK** to close the WildFire Analysis Profile configuration window.

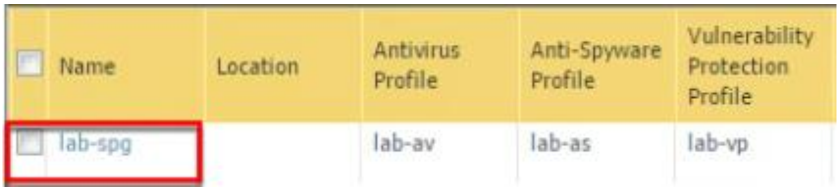
8.2 Modify Security Profile Group

1. In the WebUI select **Objects > Security Profile Groups**.



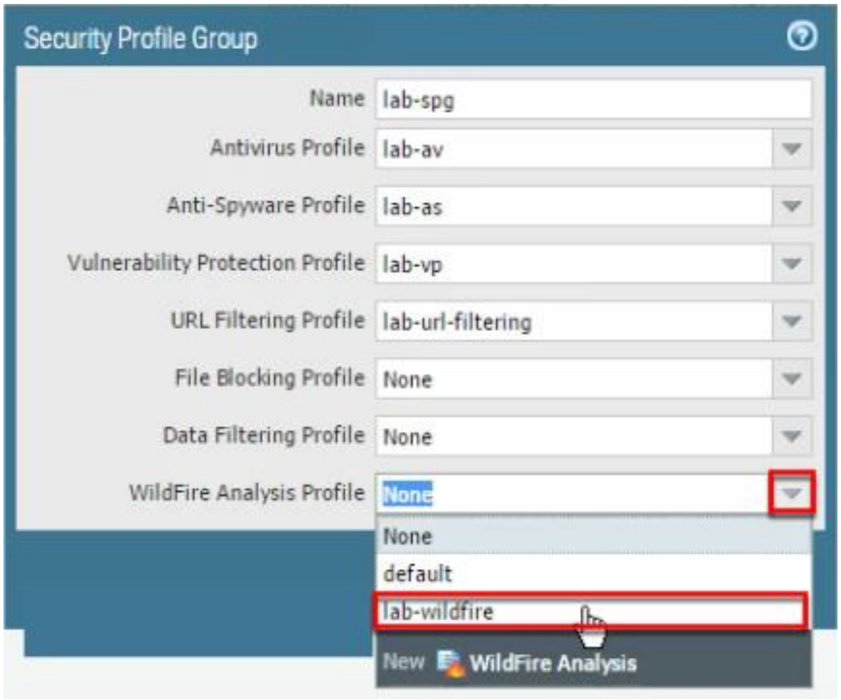
□	Name	Location	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile	URL Profi
□	lab-spg		lab-av	lab-as	lab-vp	lab-u filte

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



□	Name	Location	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile
□	lab-spg		lab-av	lab-as	lab-vp

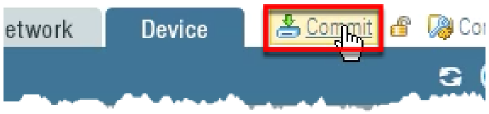
3. Add the newly created lab-wildfire WildFire Analysis Profile:


Security Profile Group

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: None

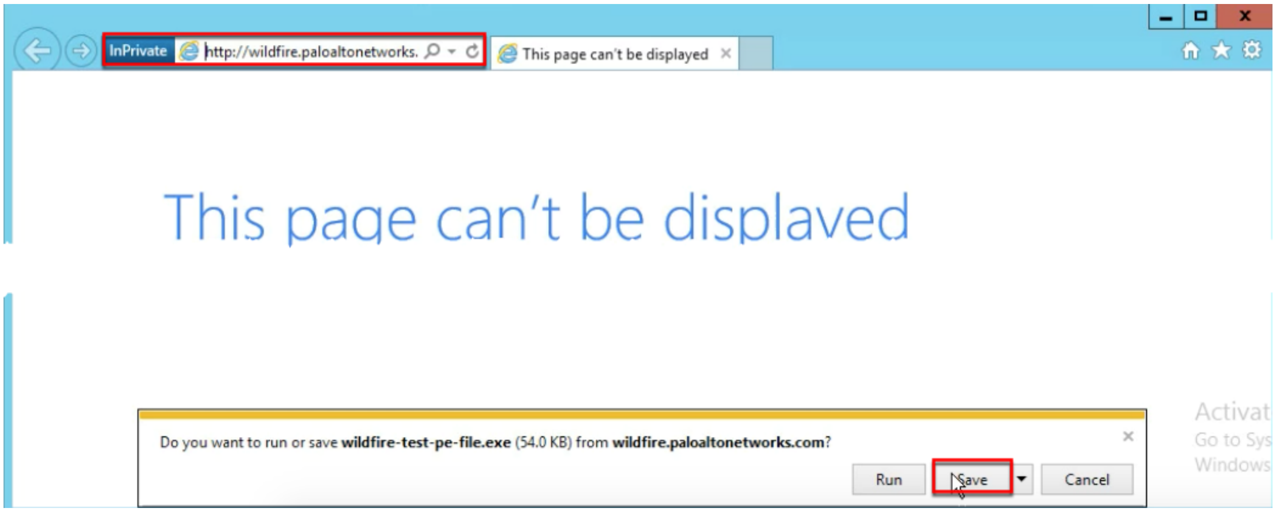
4. Click **OK**.

5. **Commit** all changes.



8.3 Test the WildFire Analysis Profile

1. Open a new browser in private/incognito mode 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.
2. Without opening the file, save it to the Downloads directory.



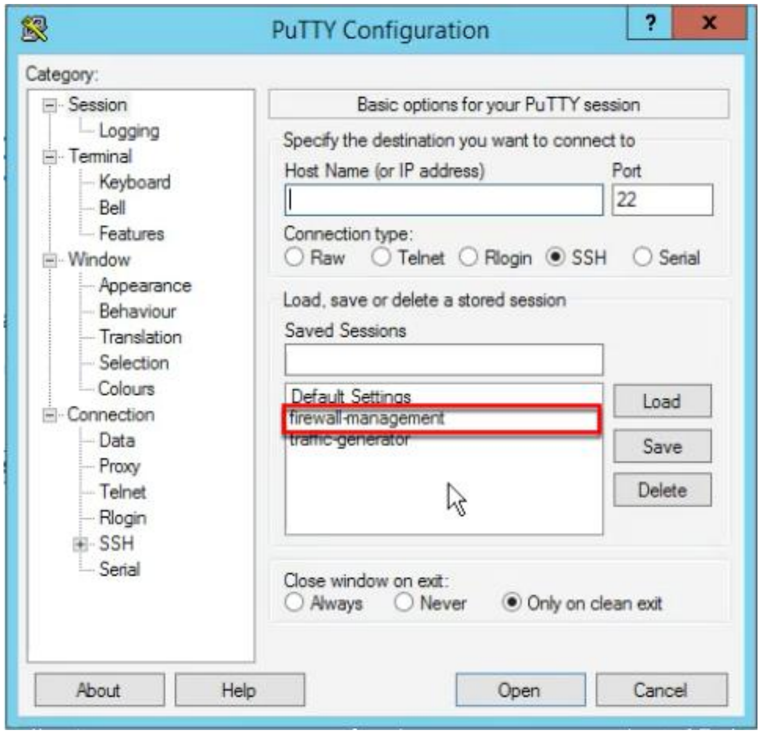
InPrivate http://wildfire.paloaltonetworks.

This page can't be displayed

This page can't be displayed

Do you want to run or save **wildfire-test-pe-file.exe** (54.0 KB) from **wildfire.paloaltonetworks.com**?

3. To verify that the file was uploaded to the public WildFire cloud, open **PuTTY** and double-click firewall-management to log in to the firewall with admin/admin.



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

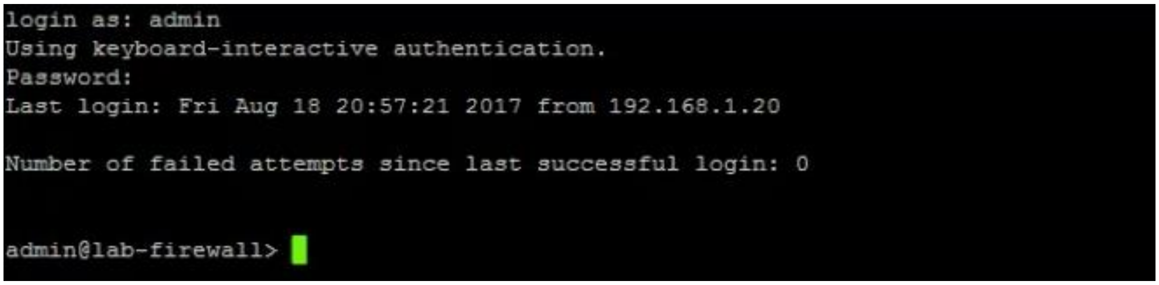
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

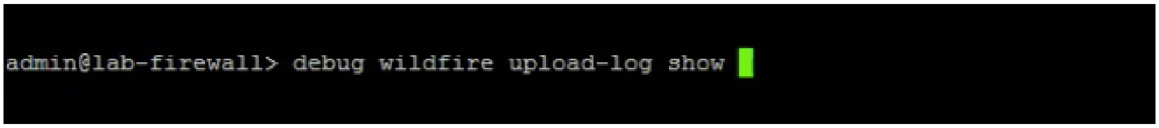
Default Settings
firewall-management
traffic-generator

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

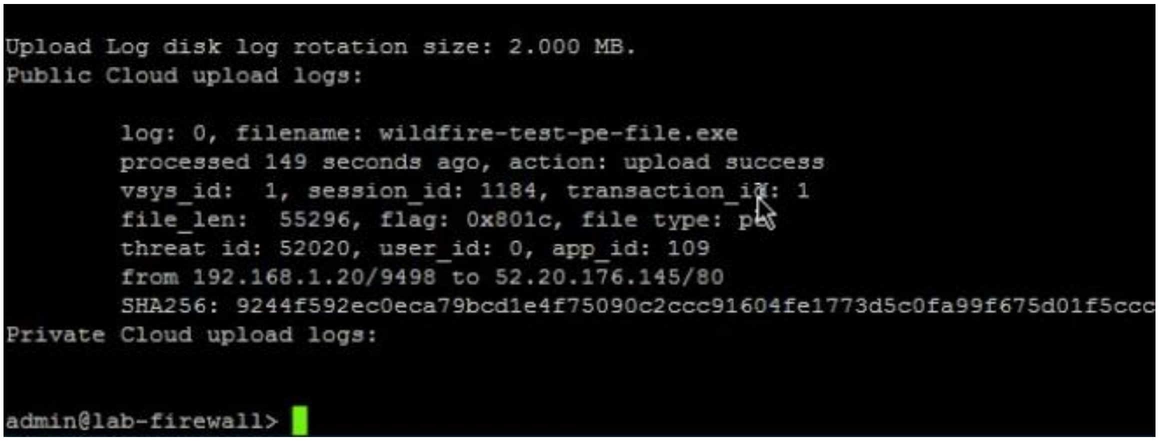


```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 18 20:57:21 2017 from 192.168.1.20

Number of failed attempts since last successful login: 0


admin@lab-firewall>
```

4. When you are logged in, enter the **`debug wildfire upload-log show`** 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:

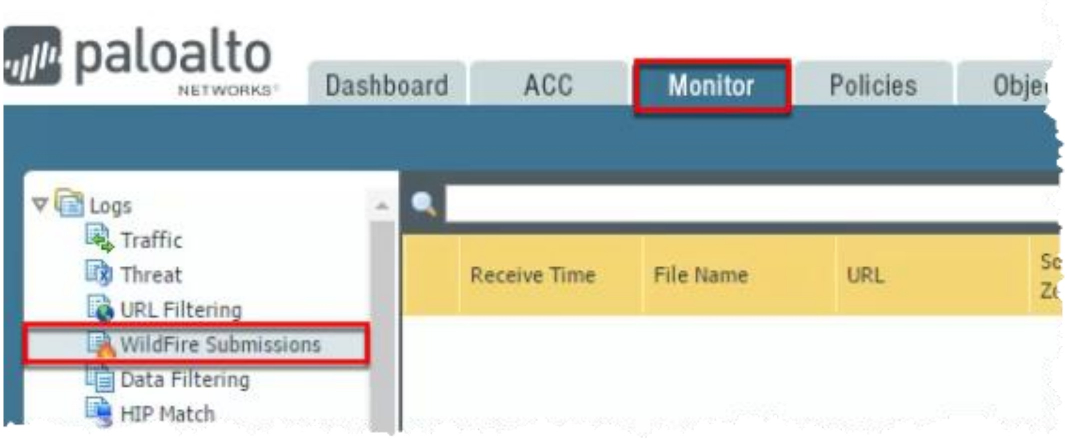


```
admin@lab-firewall> debug wildfire upload-log show
```



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

        log: 0, filename: wildfire-test-pe-file.exe
        processed 149 seconds ago, action: upload success
        vsys_id:  1, session_id: 1184, transaction_id: 1
        file_len:  55296, flag: 0x801c, file type: pe
        threat id: 52020, user_id: 0, app_id: 109
        from 192.168.1.20/9498 to 52.20.176.145/80
        SHA256: 9244f592ec0eca79bcd1e4f75090c2ccc91604fe1773d5c0fa99f675d01f5ccc
Private Cloud upload logs:


admin@lab-firewall>
```

5. Select **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.



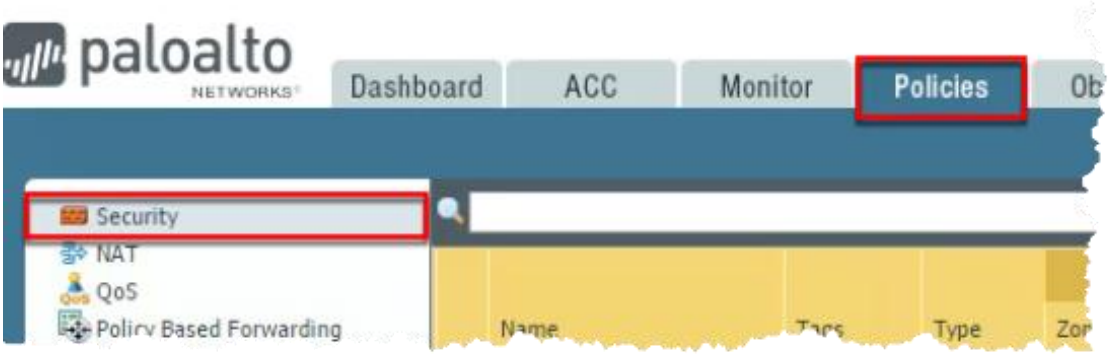
6. Click the **magnifying glass** icon next to the entry to see the Detailed Log View of the WildFire entry:

7. On the Log Info tab, check the information within the General, Details, and Destination panels. Then look at the information in the WildFire Analysis Report tab.

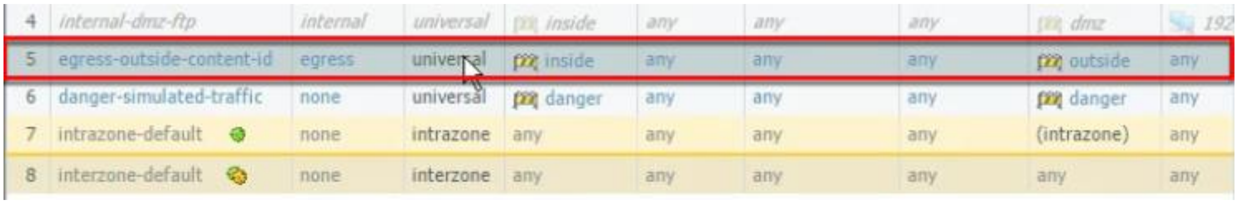
8. Log out and close the **PuTTY** session.

8.4 Disable Security Policy Rule

1. Select **Policies > Security**.

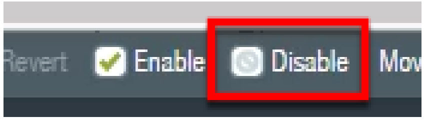


2. Select but do not open **egress-outside-content-id**.

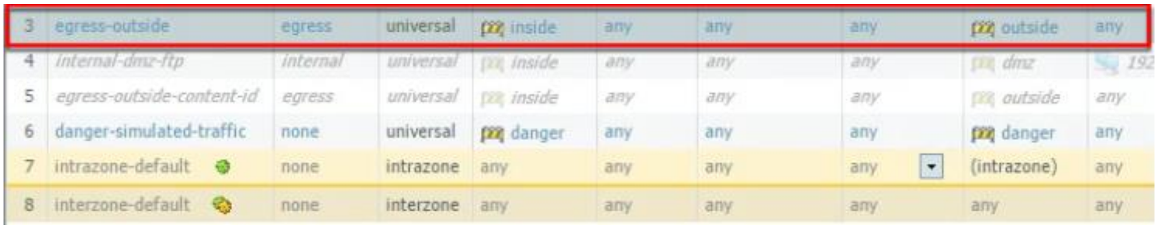


4	*internal-dmz-ftp*	*internal*	*universal*	*inside*	*any*	*any*	*any*	*dmz*	*192*
5	egress-outside-content-id	egress	universal	inside	any	any	any	outside	any
6	danger-simulated-traffic	none	universal	danger	any	any	any	danger	any
7	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
8	interzone-default	none	interzone	any	any	any	any	any	any

3. Click **Disable**.

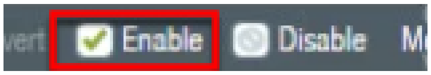


4. Select but do not open **egress-outside**.

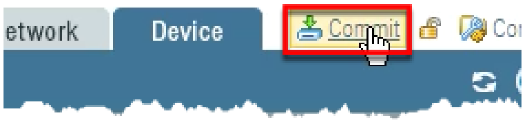


3	egress-outside	egress	universal	inside	any	any	any	outside	any
4	internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	192
5	egress-outside-content-id	egress	universal	inside	any	any	any	outside	any
6	danger-simulated-traffic	none	universal	danger	any	any	any	danger	any
7	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
8	interzone-default	none	interzone	any	any	any	any	any	any

5. Click **Enable**.



6. **Commit** all changes.



Stop. This is the end of the WildFire lab.