PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 10: Blocking Unknown Threats with WildFire

Document Version: 2025-10-13

Contents

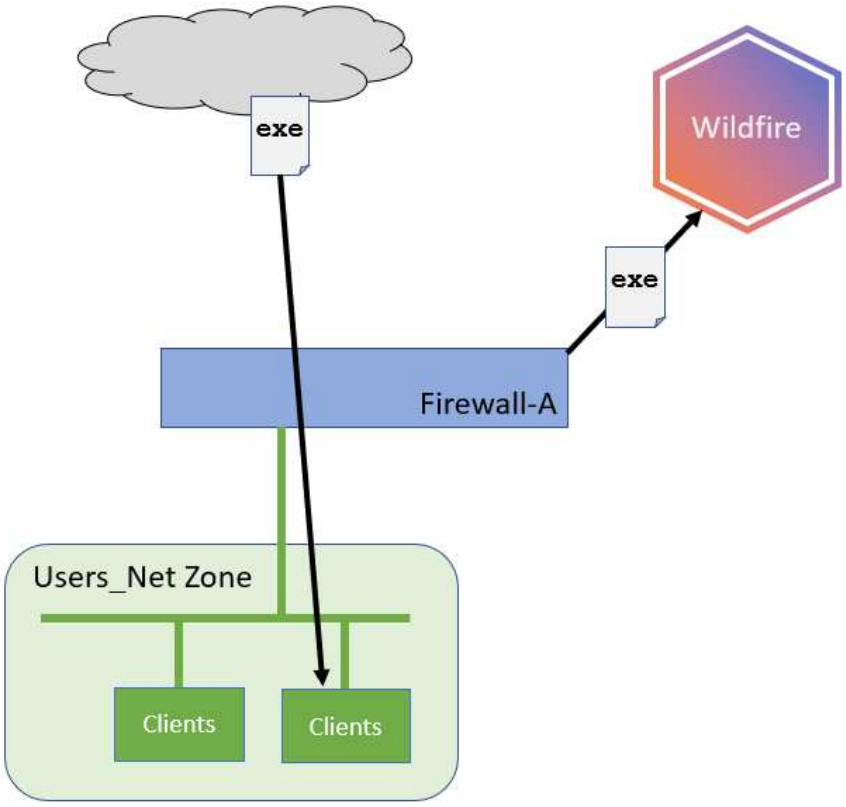
Introduction

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.

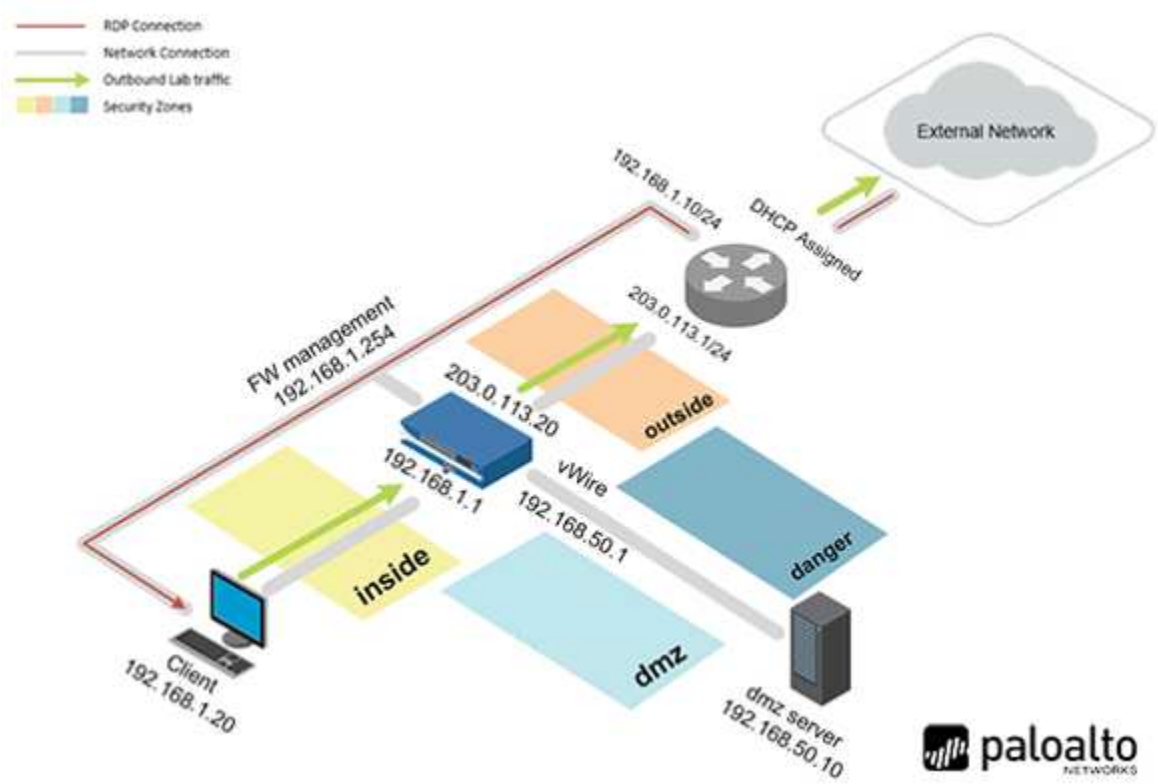


Objective

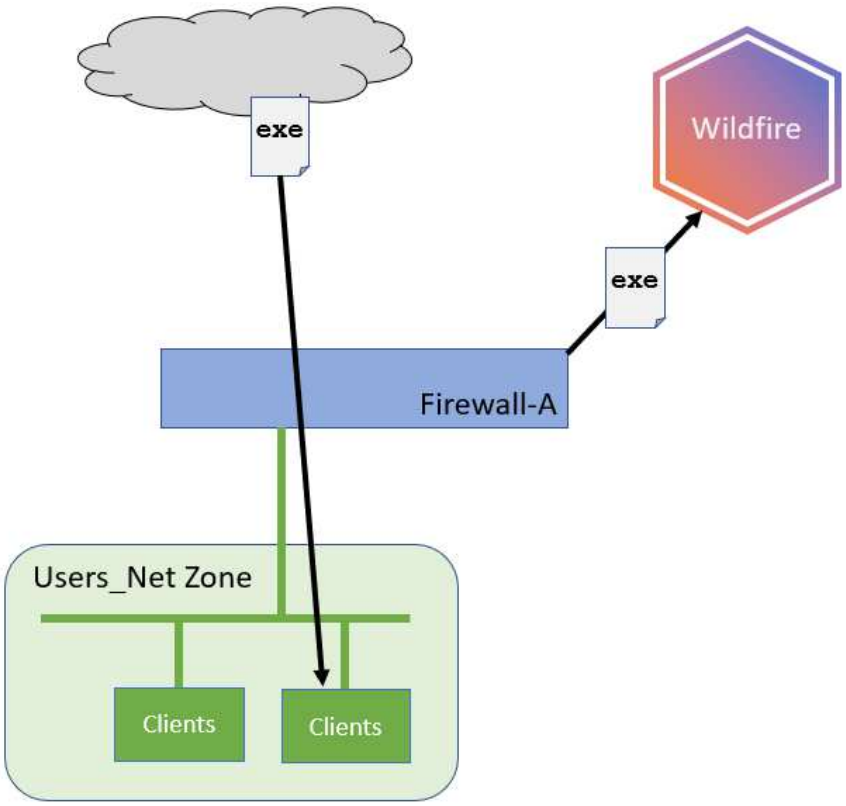
In this lab, you will perform the following tasks:

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

Lab Topology



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`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

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.

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.

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

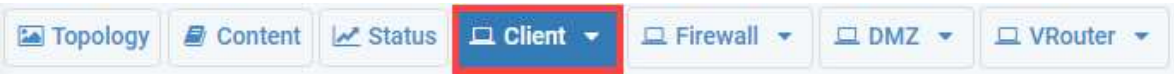
- Examine the **WildFire Submissions** log file and periodically use the **Refresh** icon until you see a new entry for the wildfire-test-pe-file.exe.
- Examine the **Detailed Log View** for the entry.
- Note the **Verdict** of the file.
- Click the link for **Download PDF** and examine the report to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

2 Blocking Unknown Threats with Wildfire – Detailed Lab Steps

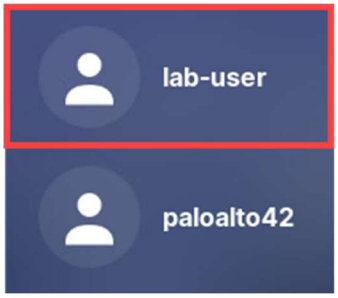
2.1 Apply a Baseline Configuration to the Firewall

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.



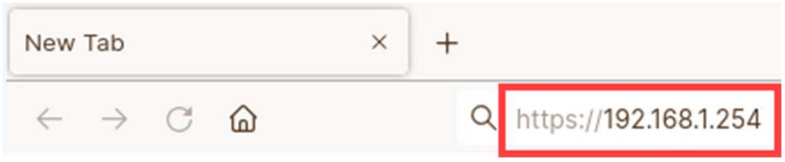
2. On the *Zorin* desktop, click **lab-user.**



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

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

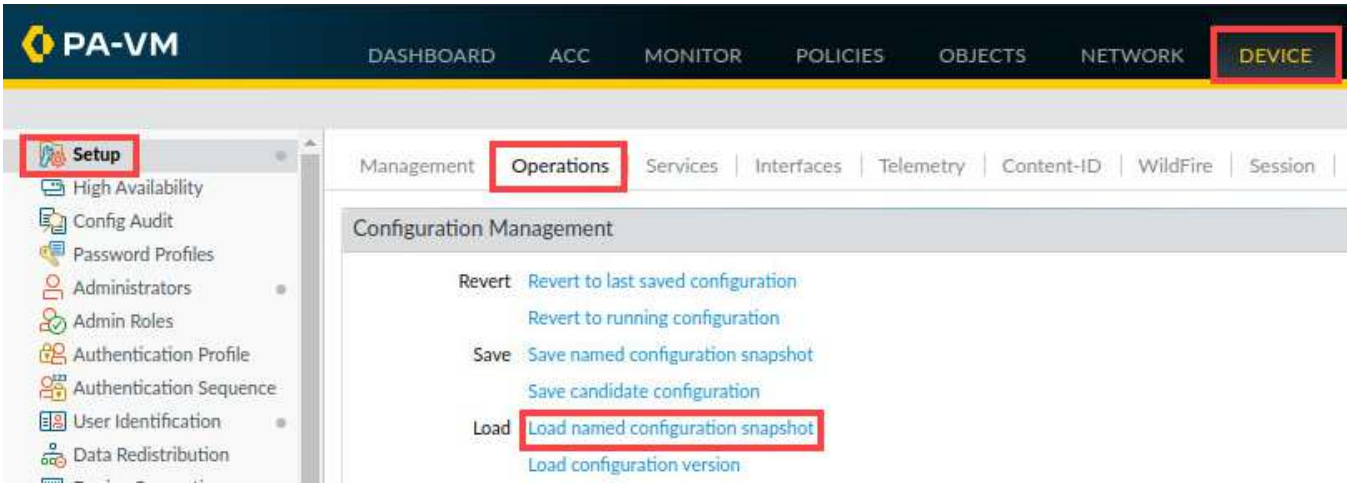
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



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

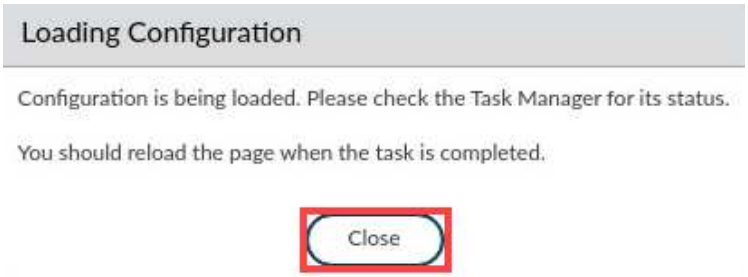
If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

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

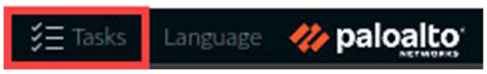


8. In the *Load Named Configuration* window, select **edu-210-11.0a-10.xml** from the *Name* drop-down box and click **OK**.

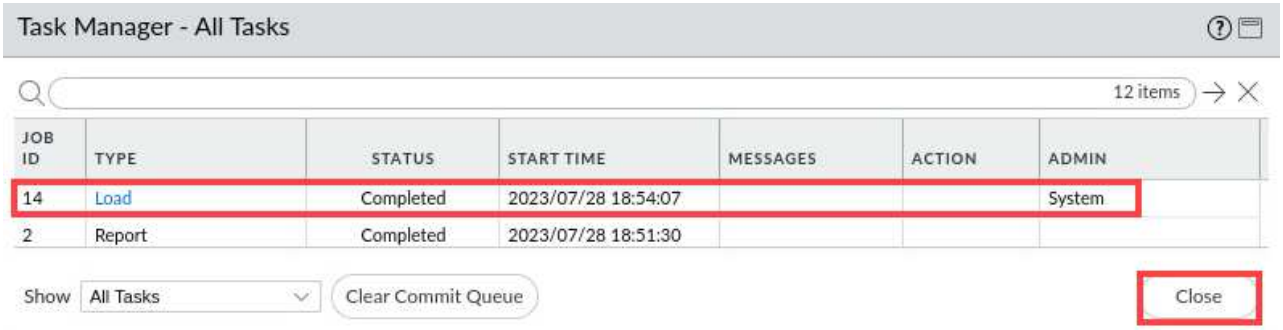
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

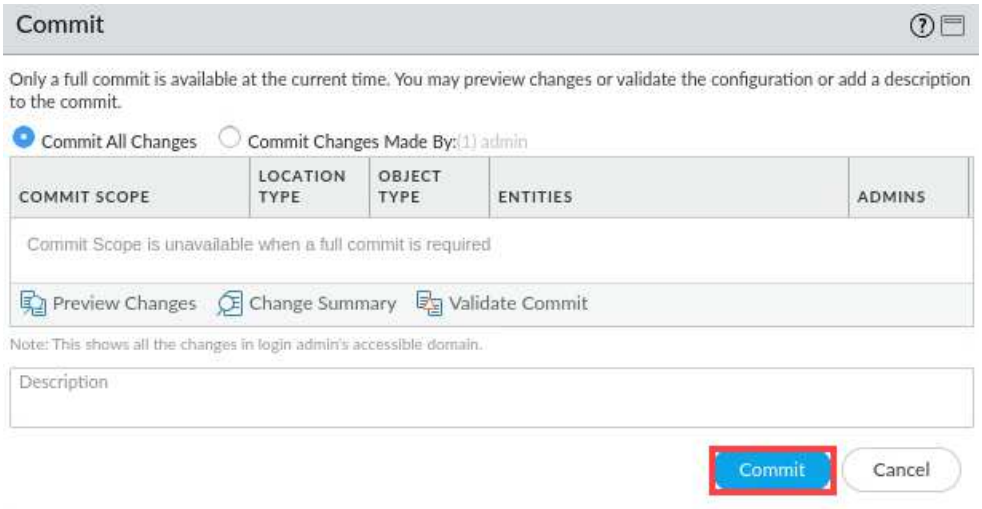


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**



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.



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

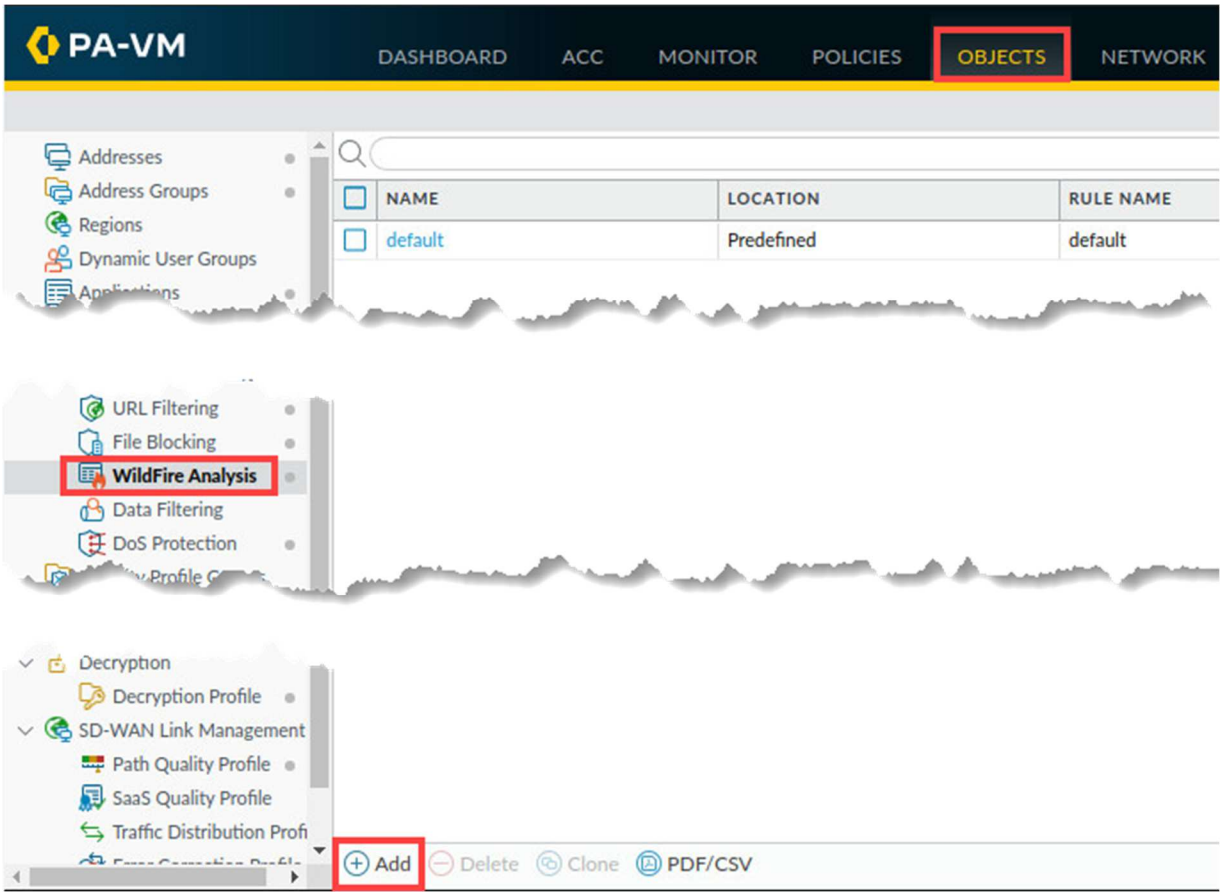
The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

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**.

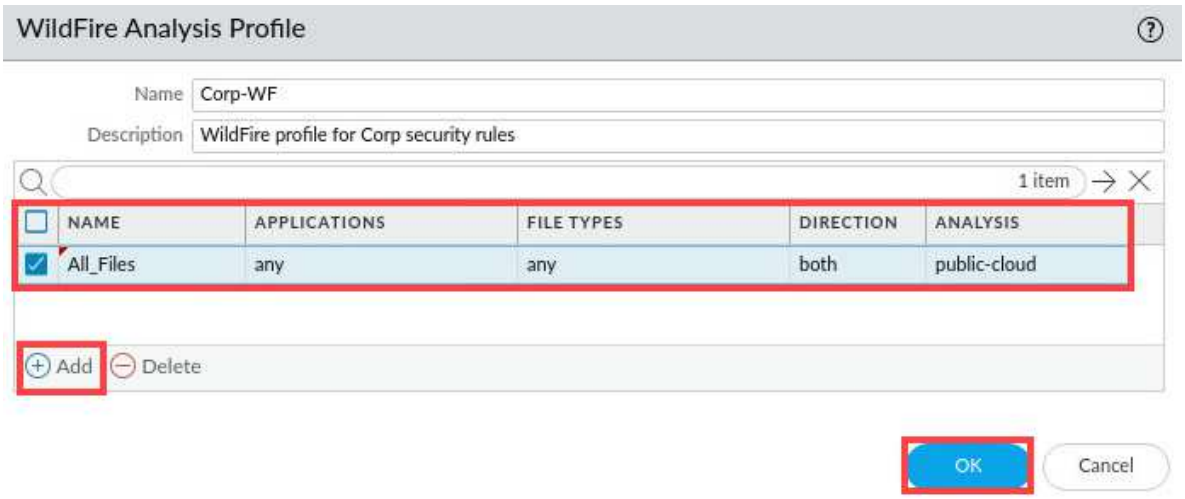


2. In the *WildFire Analysis Profile* window, configure the following.

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**

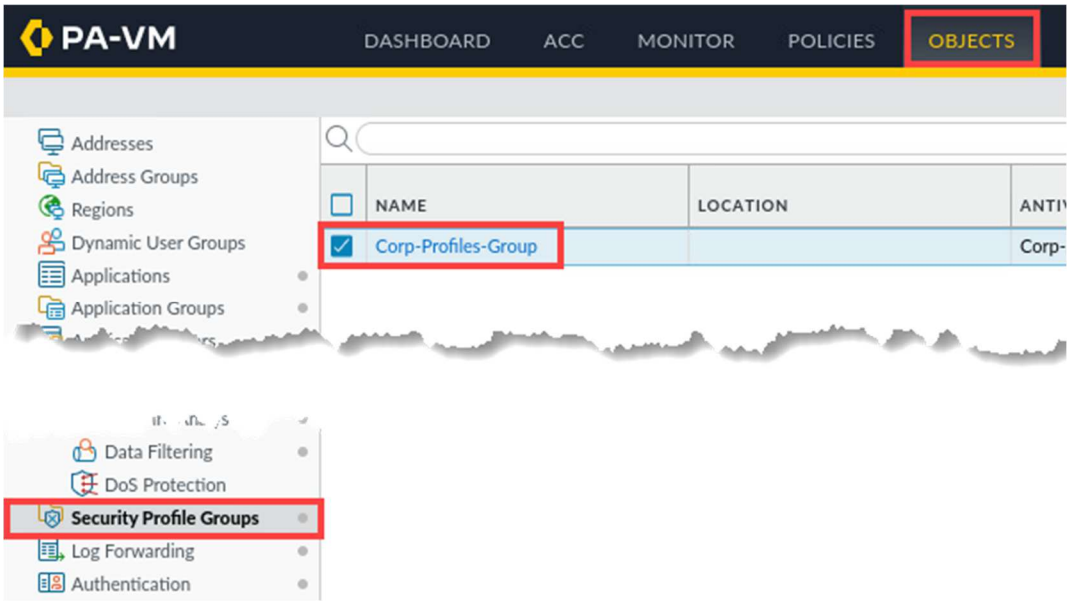


4. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

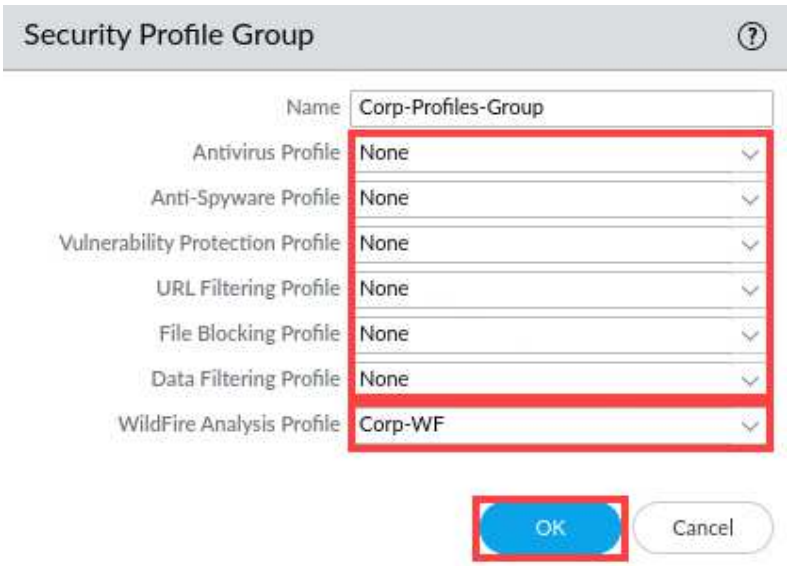
2.3 Modify Security Profile Group

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

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



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



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

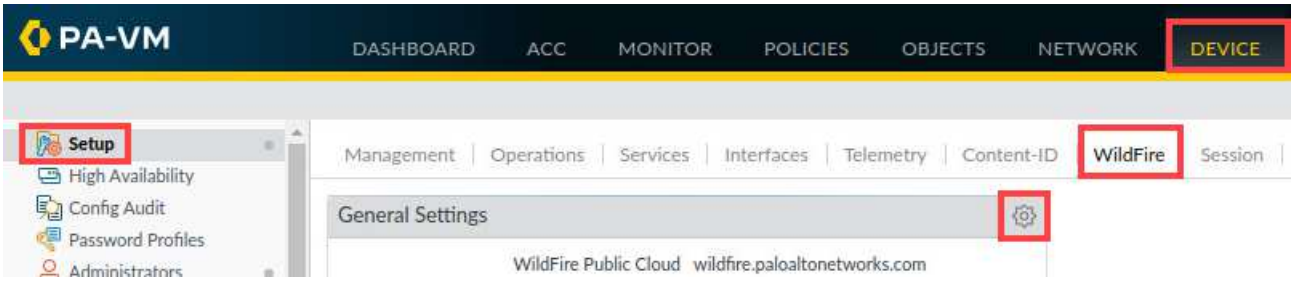
In a production environment, you want to apply all the Security Profiles for your Group. In this lab, we only want to test WildFire to see how it operates alone.

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

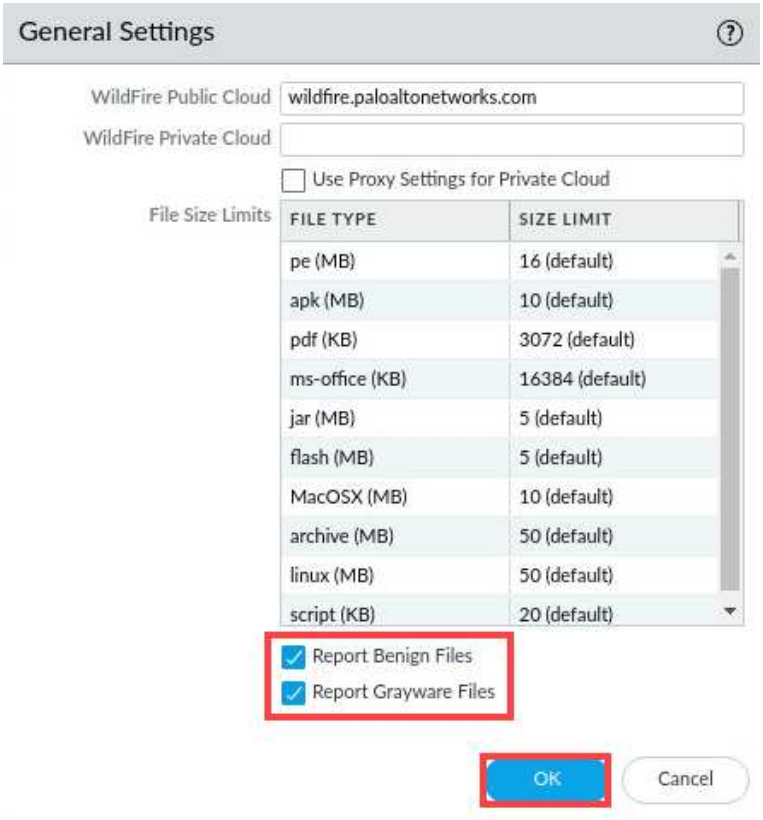
2.4 Update WildFire Settings

In this section you will update the WildFire settings.

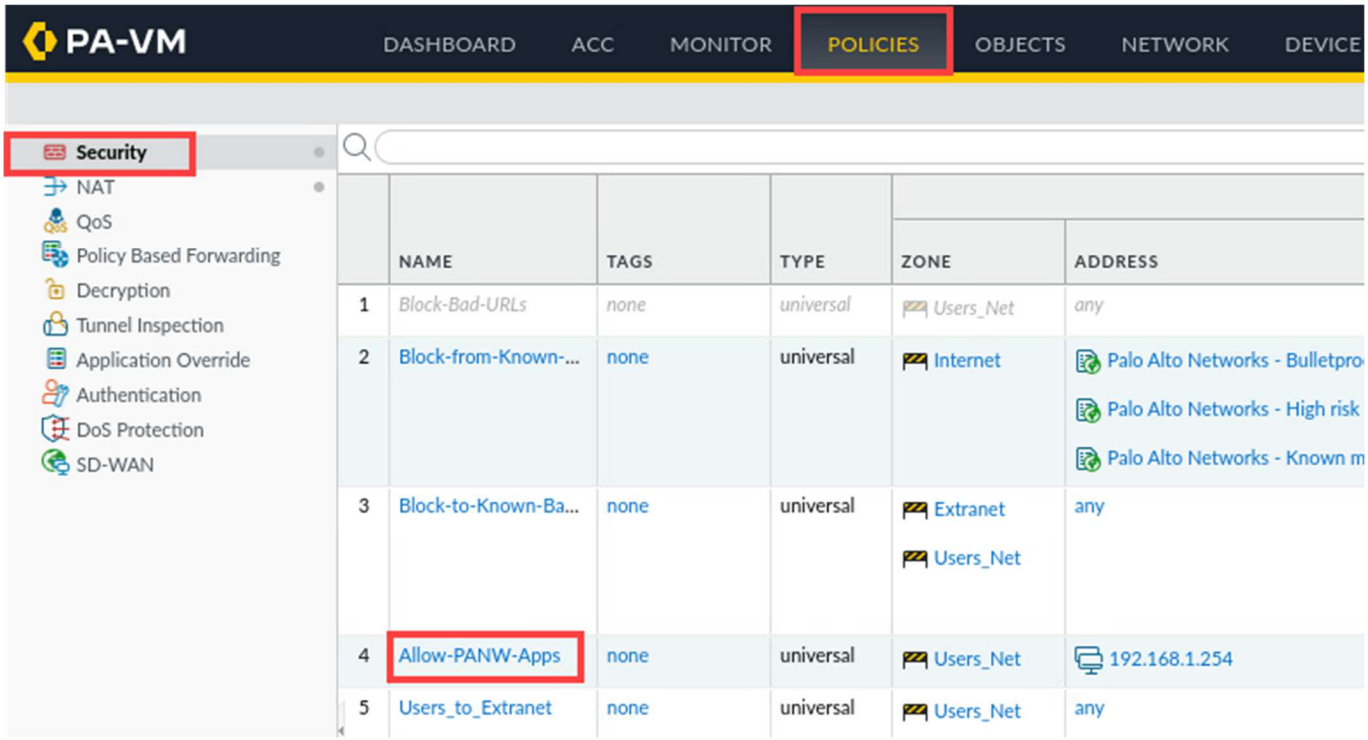
1. Select **Device > Setup > WildFire.** Click the **gear** icon to edit the **General Settings**.



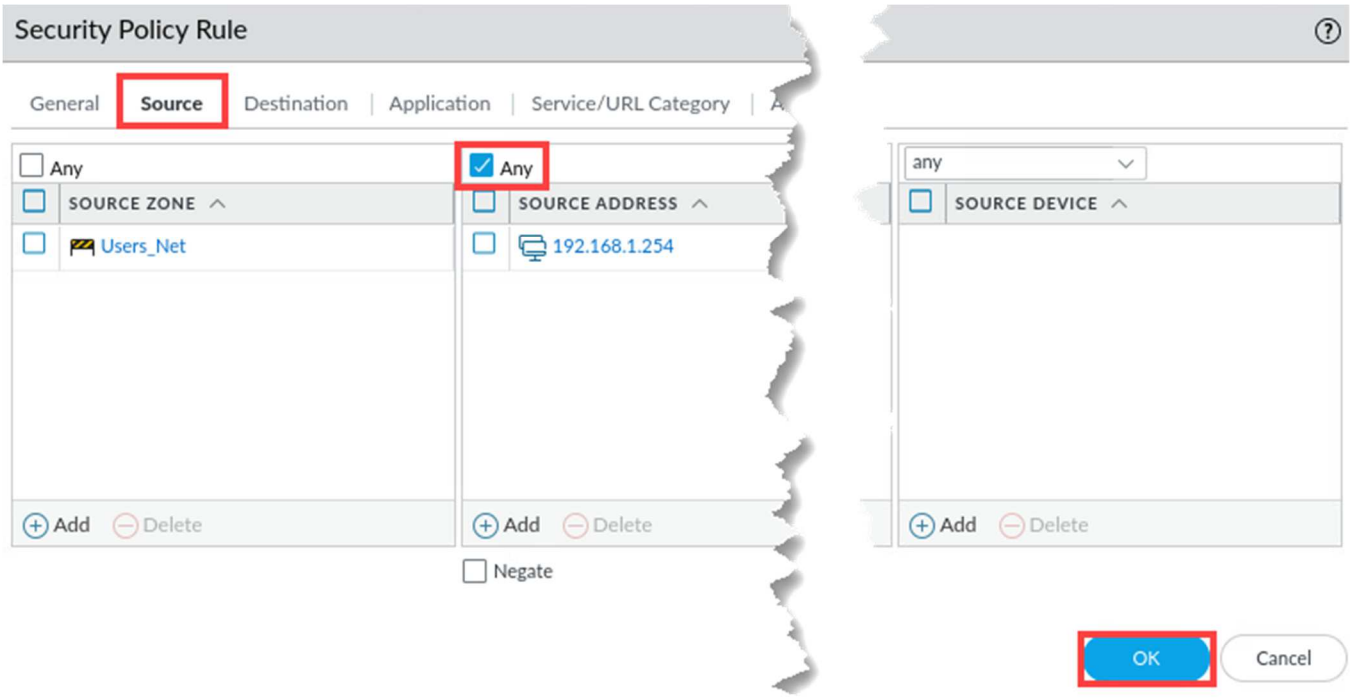
2. In the *General Settings* window, check the boxes for **Report Benign Files** and **Report Grayware Files**. Leave the remaining settings unchanged and click **OK**.



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

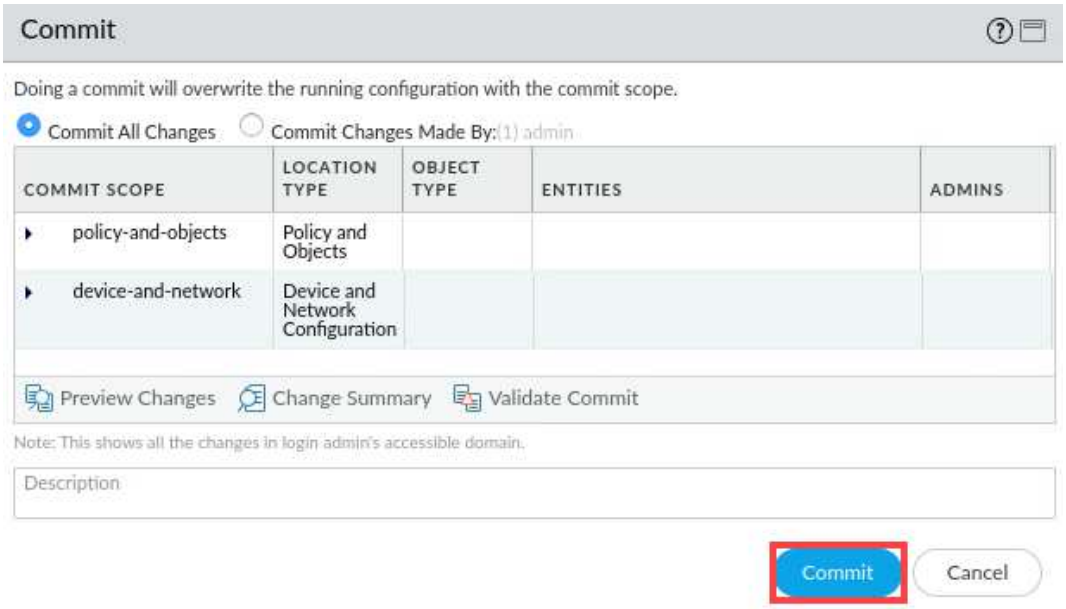


4. In the *Security Policy Rule* window, on the **Source** tab, click **Any** for the *Source Address*. Click **OK**.



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**.

2. 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.

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

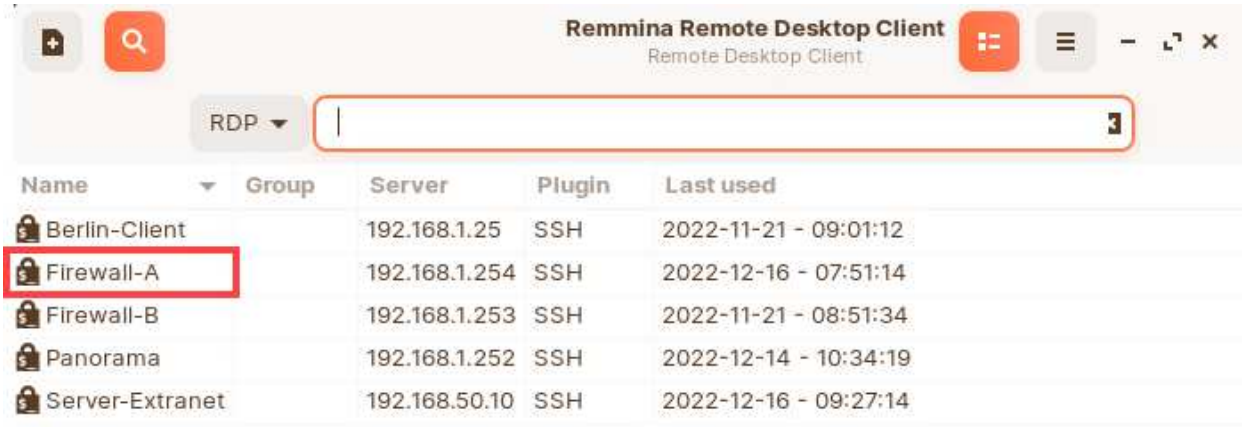
Please Note You can also verify the wildfire-test-pe-file.exe was successfully downloaded by viewing the downloads folder.

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

5. Minimize the *Palo Alto Networks Firewall*.

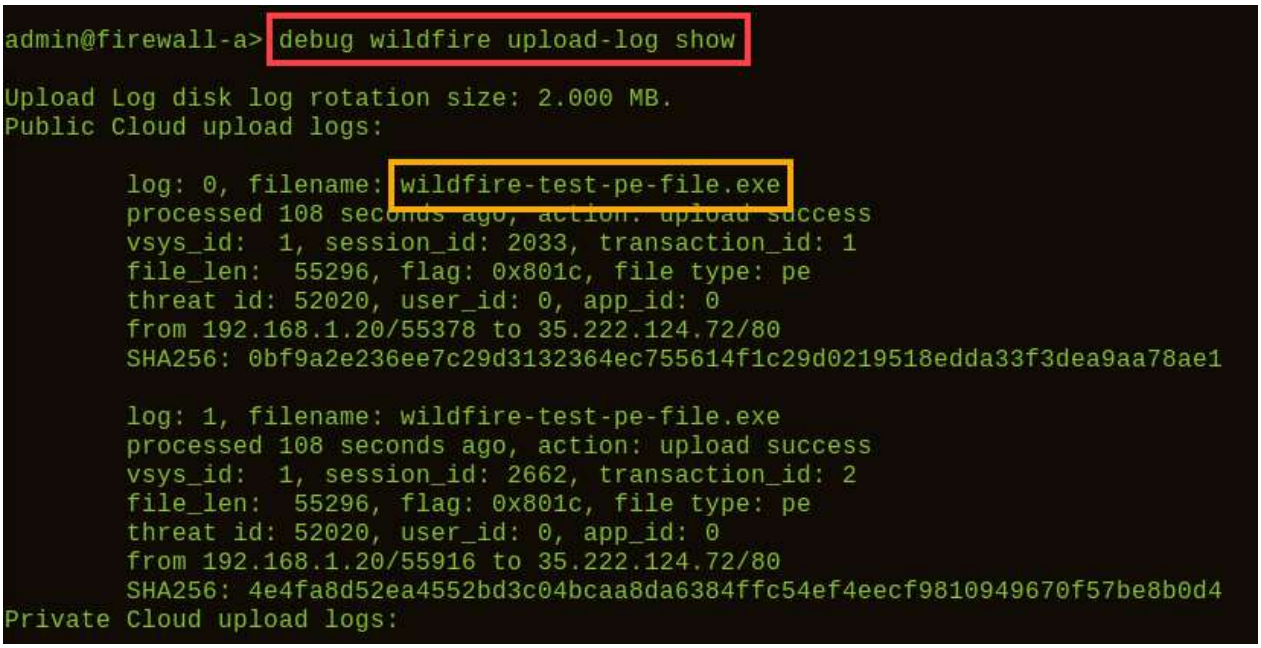
6. On the client desktop, open the **Remmina** application.

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



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

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

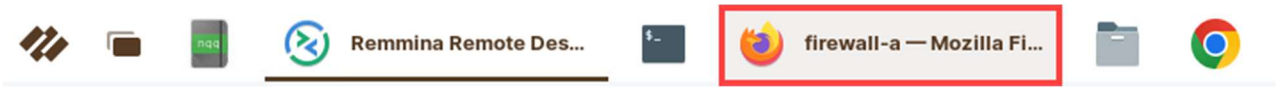


> **Please Note**
>
> The command should display the output log: 0, filename: wildfire-test-pe-file.exe processed. This output verifies that the file was uploaded to the WildFire public cloud. The message might take a minute or two to display.
>
> The details of the entry you see will differ from the 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.

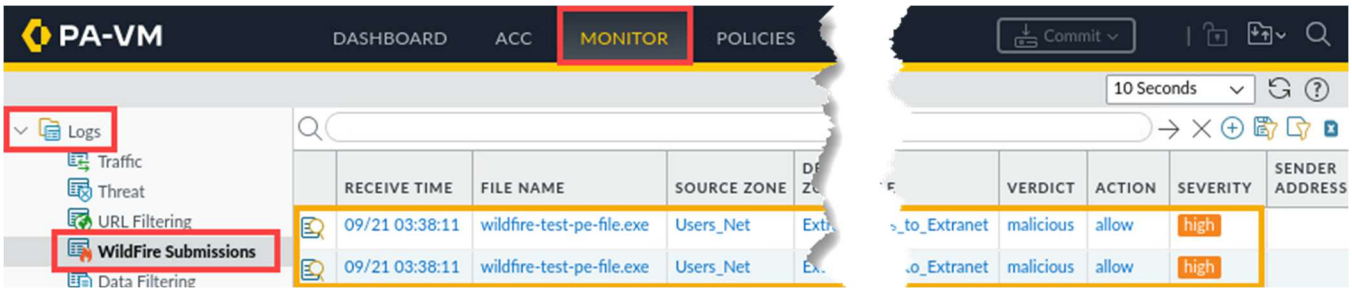


11. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

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.

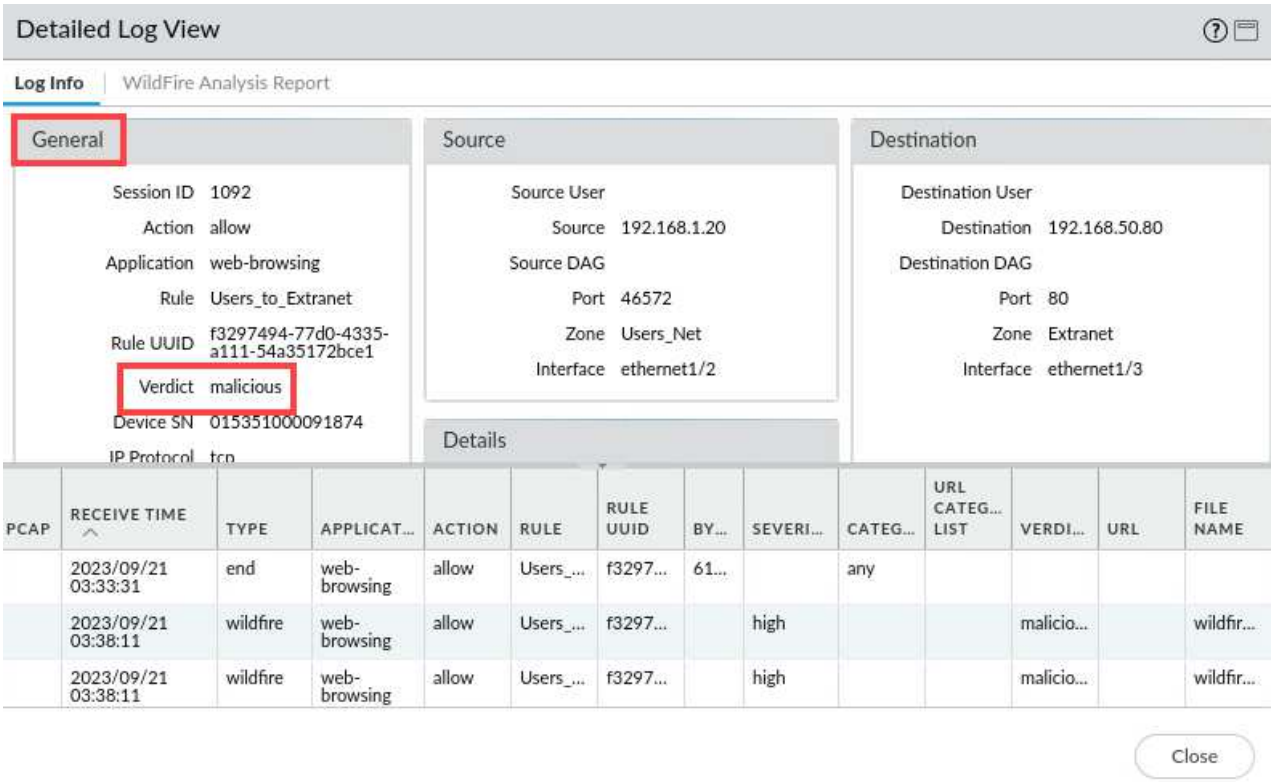


> **Please Note**
>
> Note that in this example several default columns have been hidden, and the details of the entry you see will differ.

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.

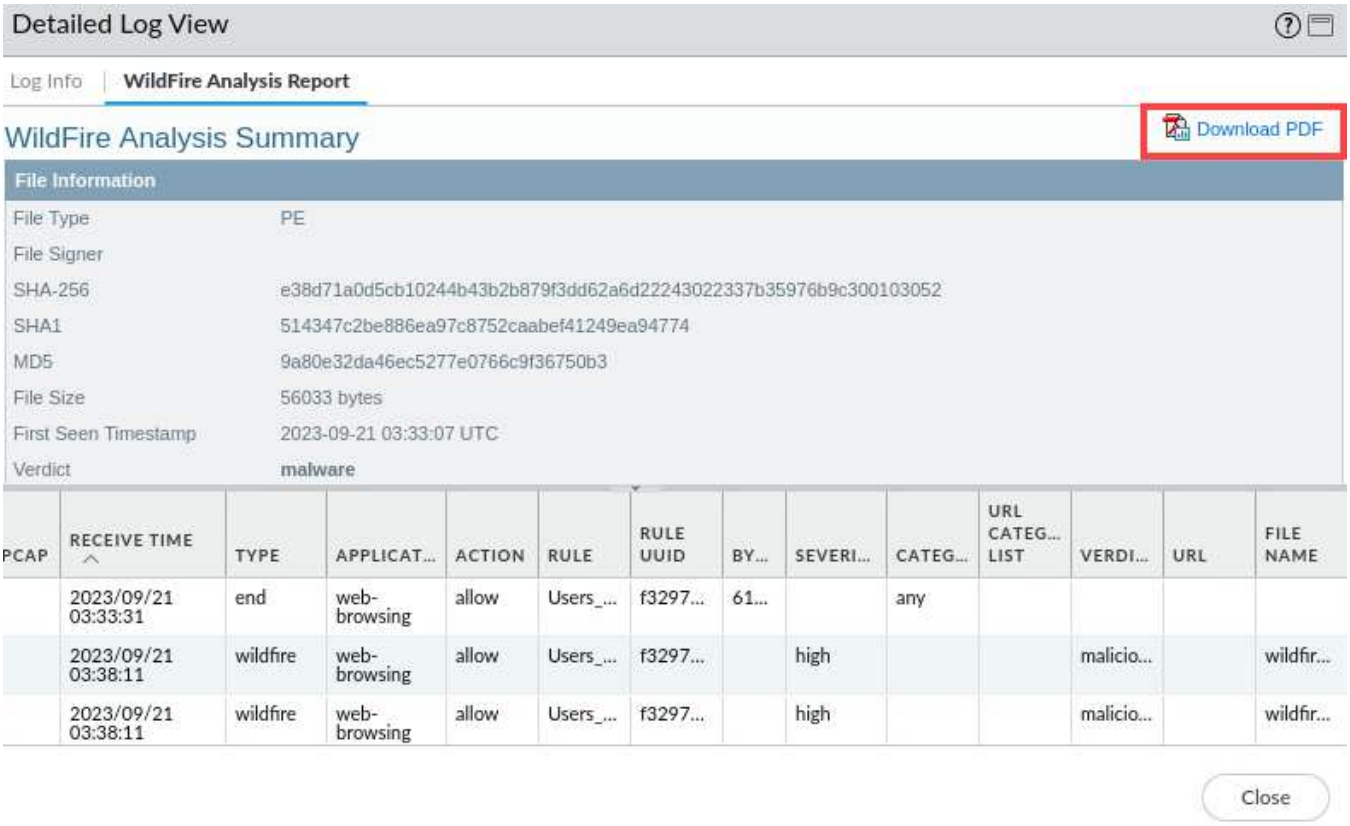
2. Click the **magnifying glass** icon next to the entry to open the **Detailed Log View** of the entry.

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

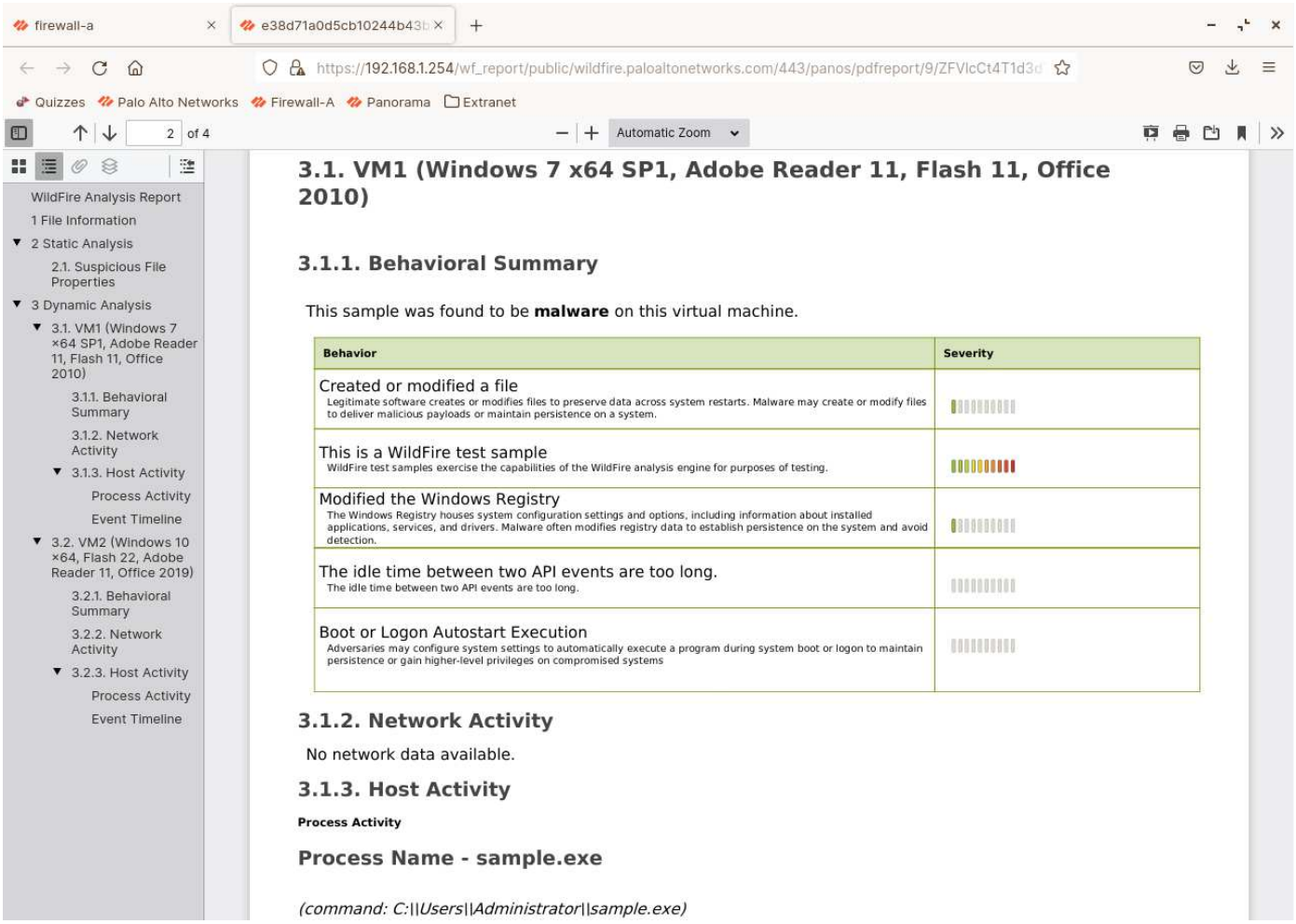


4. Click the tab labeled **Wildfire Analysis Report** at the top of the Detailed Log View.

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 Firefox browser.



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



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.