12 - Blocking Unknown Malware with Wildfire

1.2 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. 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.

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.

1.3 Apply WildFire Profile to Security Rules

In this section, you will apply the WildFire Analysis profile to a security rule.

1. Select Policies > Security. Click on the Users_to_Internet rule.
2. In the Security Policy Rule window, select the Actions tab. Under Profile Settings, use the dropdown list to select Profiles. For WildFire Analysis, select Corp-WF. Click OK.
3. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.4 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. Click the Commit link located at the top-right of the web interface.
4. In the Commit window, click Commit to proceed with committing the changes.
5. When the Commit operation successfully completes, click Close to continue.
6. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.5 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 Chromium.
2. Type http://wildfire.paloaltonetworks.com/publicapi/test/pe and press Enter.
3. Verify the wildfire-test-pe-file.exe file successfully downloaded at the bottom of the Chromium window.

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

5. Close the new chromium tab that you opened by clicking the X icon.
6. Minimize the Palo Alto Networks Firewall.
7. On the client desktop, open the Remmina application.
8. Double-click the entry for Firewall-A.
9. If you get Connecting to 'Firewall-A'… window, click OK.
10. In the CLI connection to the firewall, enter the command below.
    - `admin@firewall-a> debug wildfire upload-log show <Enter>`

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.

11. Type Exit to close the SSH session to the firewall.
    - `admin@firewall-a> exit <Enter>`
12. Reopen the PA-VM firewall web interface by clicking on the Chromium icon in the taskbar.
13. Leave the Palo Alto Networks Firewall open and continue to the next task.

1.6 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.
2. Click the magnifying glass icon next to the entry to open the Detailed Log View of the entry.

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 Submissions is showing.

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 Chromium browser.
6. Scroll through the report and view the detailed information about the WildFire analysis of the file.
7. The lab is now complete; you may end your reservation.

For example, section 3.1 provides of the report details about the kind of environment that WildFire used to test the file along with specific actions that the malware file carried out.