BLOCKING UNKNOWN THREATS WITH WILDFIRE

IF I AM PUTTING MYSELF OUT THERE AND TAKING SOME OF THESE RISKS, THEN I WANT TO DO IT PROPERLY

- WildFire® concepts
- Configure and manage WildFire
- WildFire reporting

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

© 2022 Palo Alto Networks, Inc.

Learning Objectives

After you complete this module,
you should be able to:

- Describe WildFire purposes and operation
- Describe WildFire license and deployment choices
- Configure and update WildFire
- View WildFire reports and logs

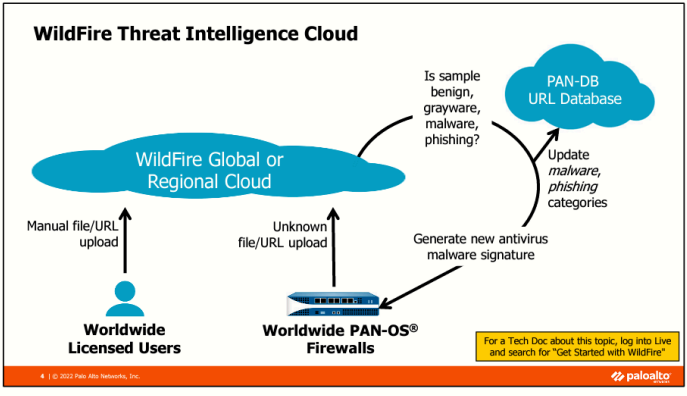
This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

- Describe WildFire purposes and operation
- Describe WildFire license and deployment choices
- Configure and update WildFire
- View WildFire reports and logs

This section describes WildFire concepts and devices.

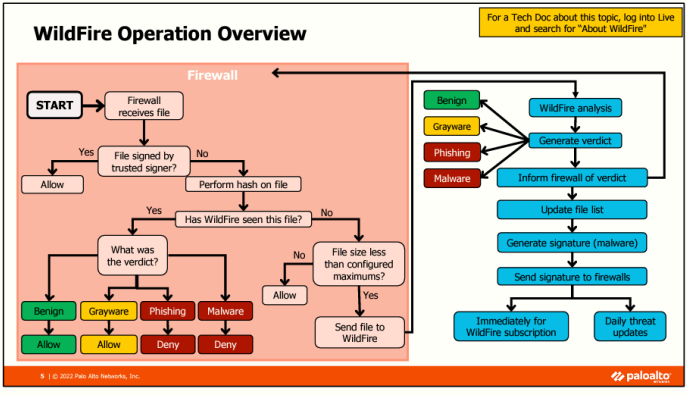
© 2022 Palo Alto Networks, Inc.



Modern malware has evolved from simple viruses to highly evasive and adaptable network applications that allow hackers to launch increasingly sophisticated and targeted attacks. This new breed of malware is at the core of many of today's most sophisticated intrusions. As malware has become more powerful, it has become more targeted and customized for specific networks. This customization helps it to avoid traditional signature-based anti-malware solutions.

Palo Alto Networks firewalls worldwide automatically forward unknown files and URL links found in emails to the WildFire global threat intelligence cloud or one of three WildFire regional clouds in Europe, Japan, and Singapore for analysis. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds. WildFire signatures and verdicts then are shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location where the malware was first detected. Licensed WildFire users worldwide can also use the WildFire XML API or WildFire Dashboard to upload files to WildFire for analysis manually. For more information about the WildFire XML API, log into Live and search for "WildFire API Reference" or see *WildFire API Reference Guide* at https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-api.html.

WildFire is a cloud-based, virtual sandbox that evaluates unknown files and URL links found in emails. The evaluation occurs for Android, Linux, macOS, Windows XP, Windows 7, and Windows 10. After the analysis is complete, files and links are labeled benign, grayware, malware, or phishing. Suppose a malware or a phishing URL is found. In that case, WildFire creates a new antivirus signature or adds the URL to the PAN-DB Phishing URL category and then makes these updates available within minutes for download by firewalls around the world.



The flowchart provides an overview of how a firewall works with WildFire technology.

When the firewall encounters a file, it will check whether a trusted signer signs it. If the answer is yes, the firewall trusts that the file does not have hidden malware and allows the file to be delivered. If the answer is no, the firewall creates a hash number for the file and uses the hash to work with WildFire to determine if the file has already been sent to WildFire.

If the file has been sent to WildFire, the firewall uses the previous verdict. If the file has not been sent to WildFire, the firewall determines if the file's size is less than the maximum firewall-to-WildFire transmission size configured on the firewall. If the file exceeds the maximum size, the firewall allows the file to be delivered and not sent to WildFire. If the file size is less than the configured maximum, then the file is sent to WildFire for analysis.

WildFire analyzes the file and generates a verdict. The firewall is informed of the verdict. WildFire then updates its file list and generates a malware signature. The signature is made available within minutes to WildFire-licensed firewalls around the world. Unlicensed firewalls can retrieve the new signature within 24 to 48 hours through typically scheduled content updates.

WildFire Verdict Descriptions

Verdict	Description
Benign	• Safe and does not exhibit malicious behavior.
Grayware	• No security threat but might display obtrusive behavior. • Examples include adware, spyware, and browser helper objects (BHOs).
Malware	• Malicious in nature and intent and can pose a security threat. • Examples include viruses, worms, trojans, remote access tools (RATs), rootkits, and botnets.
Phishing	• An attempt to trick users into revealing their login information. • Based on properties and behaviors the website displays.

6 | © 2022 Palo Alto Networks, Inc.

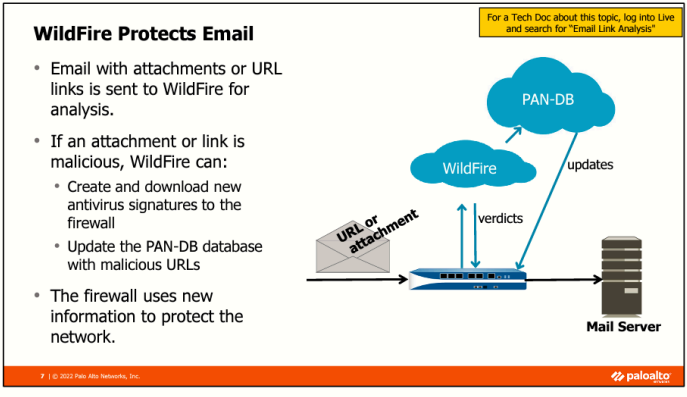
WildFire gives a benign verdict to safe files or URLs and poses no threat to your organization.

The *grayware* verdict was introduced in PAN-OS 7.0 to identify executables that behave similarly to malware but are not malicious in nature or intent. The verdict enables a security incident responder to distinguish grayware from malicious files and prioritize accordingly quickly. Antivirus signatures are not generated for grayware, but you can configure your firewall to log grayware events to assess whether such events warrant further action.

A *malware* verdict indicates that WildFire has determined that the file or URL is malicious in nature and intent and can pose a security threat to your organization. If a current signature does not exist, WildFire will create one and make it available to firewalls worldwide. WildFire also will update the PAN-DB URL Filtering database with malicious URLs.

Beginning with PAN-OS 8.0, the *phishing* verdict was introduced to classify phishing links found in emails separately from emailed links found to be exploits or malware. When the firewall detects an unknown link in an email, it forwards the link to WildFire for analysis. WildFire classifies the link as phishing based on the accompanying website's properties and behaviors. Palo Alto Networks security researchers also manually review certain links to check for phishing activity. Phishing links are added to the PAN-DB database and are used to block future phishing attacks.

File verdicts appear in the web interface WildFire Submissions log and in the WildFire portal, both of which are described later in this module.

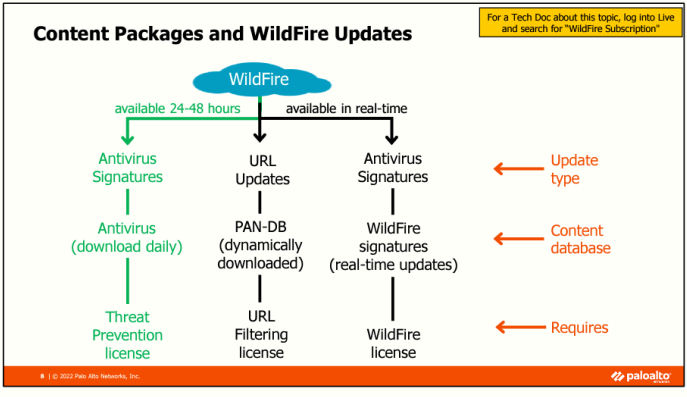


The firewall sends emails with attachments or URL links to WildFire for analysis. Neither the firewall nor WildFire stores or enables the viewing of email contents.

When WildFire detects a malicious file, it immediately creates a new antivirus signature that can be downloaded in real-time by Palo Alto Networks firewalls worldwide. This new antivirus signature can help to prevent further compromise of other machines in your network and across the globe.

Suppose WildFire determines that a URL link included in the email is malicious. In that case, it quickly updates the Antivirus content database and the PAN-DB database to prevent further compromise of other hosts around the world. If the URL link was found to be specifically a phishing website, the URL is added to the Advanced URL Filtering *phishing* category in the PAN-DB database. If you have a WildFire and PAN-DB license, your firewall can block access to newly discovered malware and phishing sites as soon as signatures are generated.

If WildFire determines that a file attachment or URL link is malicious, it includes the email header information in the WildFire Submissions log that it returns to the firewall. If User-ID technology is enabled, you can use the log information to find and remediate the threats received by your users quickly. If User-ID matches a name in the WildFire log, the log's Email Header section contains a link. If you click the link, the ACC tab opens, filtered by the user or group of users.

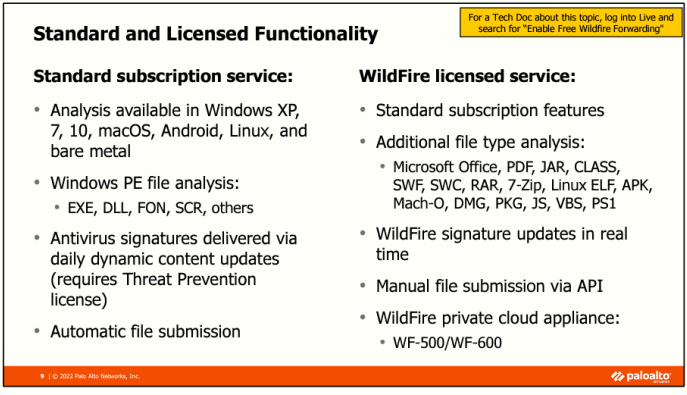


WildFire analysis is used to create new antivirus signatures. It also is used to update the URLs and URL categories listed in the PAN-DB URL Filtering database.

Antivirus signatures are made available within 24 to 48 hours as content updates to the Antivirus content database. You can schedule daily downloads of the Antivirus content database. A Threat Prevention license enables firewall access to the Antivirus content database.

Antivirus signatures also are made available in real-time as content updates to the WildFire signatures content database on the firewall. You can schedule a firewall to check for new WildFire antivirus signatures in real-time. A WildFire license enables firewall access to the WildFire antivirus signatures.

URL updates are made available within 5 minutes as content updates to the PAN-DB URL Filtering database. You do not need to schedule PAN-DB downloads because new URL information is downloaded dynamically by the firewall as needed. A URL Filtering license enables firewall access to the PAN-DB URL Filtering database.



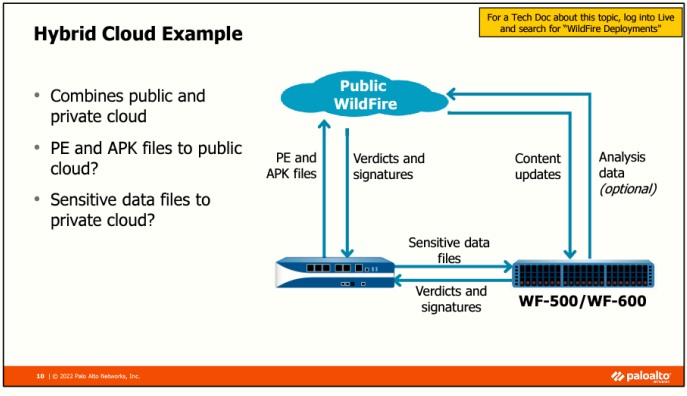
Every type of Palo Alto Networks firewall with a Threat Prevention license running PAN-OS 4.1 or later has access to the standard WildFire subscription service. The standard subscription service includes file and URL analysis on various virtual machine-based operating systems. If WildFire detects that malware is attempting to detect the presence of a virtual machine, WildFire also can perform analysis in a bare-metal machine environment. The standard service enables firewalls to automatically submit unknown Windows Portable Executable (or PE) files for analysis. Windows PE file types include EXE, DLL, SCR, and FON. New signatures and protections are made available daily to the firewalls through the regular dynamic content updates.

Palo Alto Networks firewalls with a WildFire license are entitled to the standard subscription features and additional features. A firewall may submit more file types for analysis. Other file types are Microsoft Office files, PDF files, Java JAR and CLASS files, Adobe Flash SWF and SWC files, RAR, 7-Zip, Linux ELF, and Android APK files. The macOS Mach-O, DMG, and PKG files also are supported. WildFire also can analyze JS, VBS, and PS1 files.

WildFire can create new signatures in real-time. WildFire licensed firewalls have access to those signatures, enabling near real-time protection against the latest threats detected anywhere in the world. The 5-minute WildFire content update time applies to PAN-OS 7.1 and later. In previous versions, the content update time was 15 minutes. There are two different content package formats for WildFire content updates: content packages for 7.1 and later and content packages for 7.0 and earlier. These content packages contain the same set of signatures.

A license also enables users to programmatically submit files for analysis to WildFire using the WildFire XML API. For more information about the WildFire XML API, log into Live and search for "WildFire API Reference" or see *WildFire API Reference Guide* at https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-api.html.

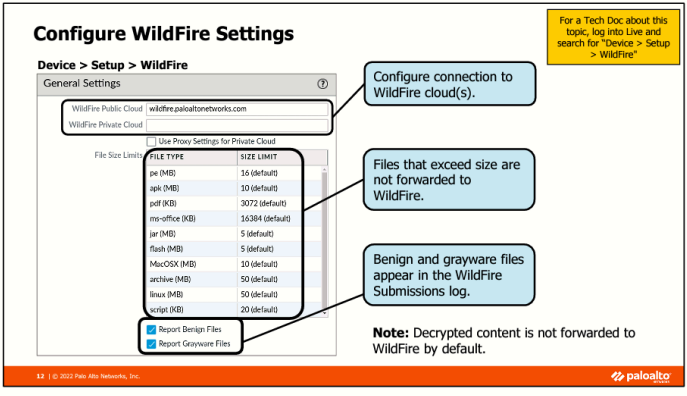
A WildFire license entitles a firewall to use the WF-500/WF-600 appliance as a WildFire private cloud service.



A hybrid cloud combines public and private cloud solutions. If you use a WF-500/WF-600 appliance, you can configure a WildFire hybrid cloud that enables the WF-500/WF-600 to analyze sensitive file types locally. In contrast, other less sensitive file types, such as PE files, are forwarded to the WildFire public cloud. You also can forward file types that are not supported on the WF-500/WF-600, such as APK files, to the WildFire public cloud. If the public and private cloud solutions are used together, the private-cloud analysis prevails when overlapping configurations exist.

This section describes how to configure and mange WildFire on your firewall.

© 2022 Palo Alto Networks, Inc.



Use **Device > Setup > WildFire** to configure WildFire settings on the firewall.

By default, the **WildFire Public Cloud** setting is configured with the URL value wildfire.paloaltonetworks.com, the global WildFire cloud. Other URL values also are available in different geographies to satisfy performance and data locality requirements. For Europe, use the URL value eu.wildfire.paloaltonetworks.com. Data submitted to the European WildFire cloud never is forwarded to the global WildFire cloud in the United States. For Japan, use the value wildfire.paloaltonetworks.jp. Only malicious files submitted to the Japanese WildFire cloud are submitted to the worldwide WildFire cloud.

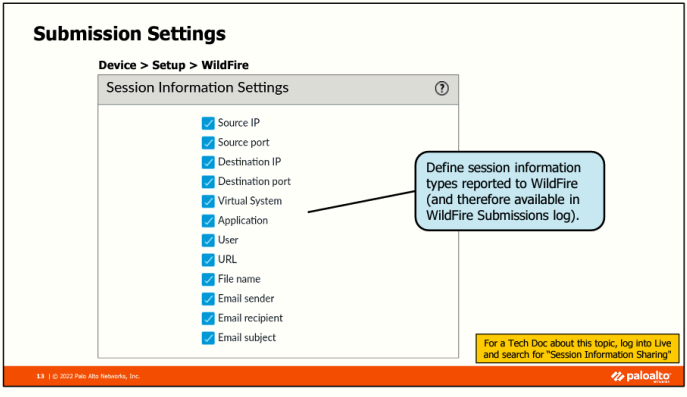
If you have configured a WF-500/WF-600 private cloud appliance, enter its IP address or domain name as the WildFire Private Cloud field value.

You also can configure size limits for files forwarded to WildFire for analysis. The default and maximum size limits were increased with PAN-OS 9.0. The updated default file sizes are designed to include the vast majority of malware you will likely encounter. Files larger than the specified size are not sent to WildFire.

The **Report Benign Files** and **Report Grayware Files** checkboxes are not enabled by default. If you allow them, WildFire includes analyzed benign and grayware files in the report it returns to the firewall. A report appears as an entry in the WildFire Submissions log. Even if these two options are enabled, WildFire does not report back to the firewall about any benign or grayware URLs analyzed within the email because the size of these reports could be prohibitively large.

Suppose you have configured SSL or SSH decryption. In that case, the firewall does not forward any decrypted content to WildFire for analysis until you enable the **Allow forwarding of decrypted content** option at **Device > Setup > Content-ID > Content-ID Settings**.

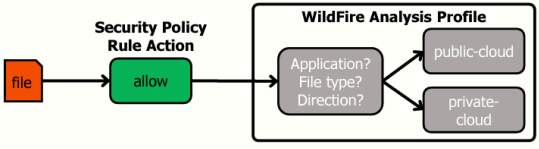
For more information on this topic, log into Live and search for "WildFire best practices" or see the following documentation for additional information on WildFire file size best practices: https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html.



The **Session Information Settings** options specify which types of session information are sent to WildFire. All options are selected by default. Because this information is submitted to WildFire, WildFire can include this information in the report that it returns to the firewall, which means that this information is available in the firewall's WildFire Submissions log or the WildFire portal.

WildFire Analysis

Profile implements additional security checks on files in allowed traffic.

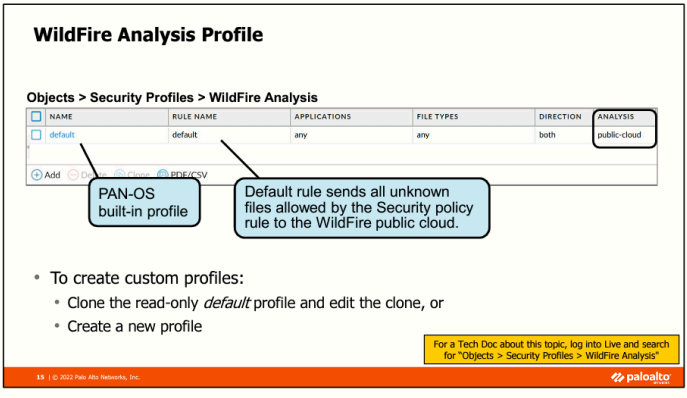


For a Tech Doc about this topic, log into Live and search for "WildFire Best Practices"

WildFire Analysis Profiles are objects added to Security policy rules that are configured with an action of "allow." WildFire Analysis Profiles are unnecessary for Security policy rules configured with the "deny" action because no further processing is needed if the network traffic is blocked. As with Security policy rules, WildFire Analysis Profiles are applied to all packets over the life of a session.

The WildFire Analysis Profiles represent additional security checks on files in allowed network traffic. WildFire Analysis Profiles enable you to have more granular control over allowed traffic. For example, you can configure a firewall to submit files to WildFire only when they match specific file types and are transferred in a particular direction by a specific application. The files submitted to WildFire are logged to the log found at **Monitor > Logs > WildFire Submissions**.

© 2022 Palo Alto Networks, Inc.



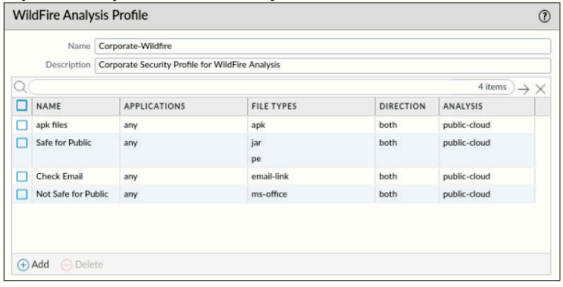
A Palo Alto Networks firewall includes a predefined, read-only *default* WildFire Analysis Profile. Suppose the default profile is assigned to a Security policy rule. In that case, the profile sends all unknown files from any applications allowed by the rule to the WildFire public cloud for analysis. Beginning with PAN-OS 8.0, blocked files also are submitted to WildFire.

To create a custom WildFire Analysis Profile, clone the *default* profile and edit the clone. Or you can create a new WildFire Analysis Profile. Use customized WildFire Analysis Profiles to minimize the number of files analyzed by WildFire between more-trusted zones or maximize the number of files analyzed between less-trusted zones. In a Zero Trust configuration, no zone is completely trusted.

Creating a WildFire Analysis Profile

For a Tech Doc about this topic, log into Live and search for "Forward Files for WildFire Analysis"

Objects > Security Profiles > WildFire Analysis > Add

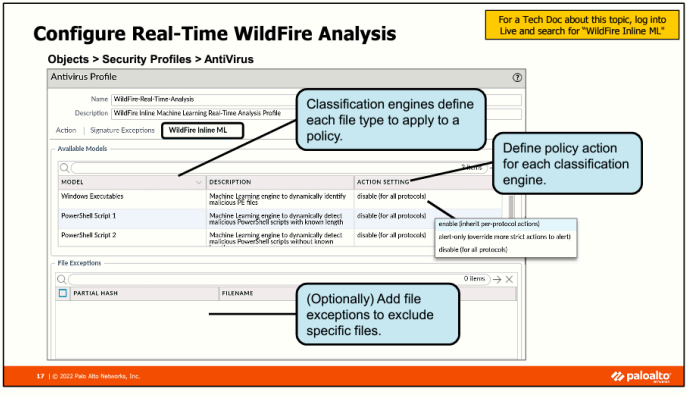


Use a WildFire Analysis Profile to specify which application file types to send to WildFire for analysis. You can determine which traffic to forward to a WildFire public or private cloud-based application, file type, and transmission direction.

In the example, APK files being transferred in any direction are sent to the WildFire public cloud for analysis because a WildFire private cloud cannot analyze them. The JAR and PE file types being transferred are sent to the WildFire public cloud because they typically do not contain confidential information. The profile also ensures that the WildFire public cloud analyzes any URL links found in an email. The first two rules could have been combined without affecting WildFire's operation.

In some instances, an organization might determine that its Microsoft documents or PDFs might have sensitive information that the organization does not want to be forwarded to the public cloud. In the example, the *ms-office* and *pdf* files are sent to a WildFire private cloud to keep these files securely in the local network.

Note: By default, the firewall will not automatically forward files to WildFire detected during SSL Decryption. To enable the firewall to forward decrypted SSL traffic for WildFire analysis. You must edit Allow Forwarding of Decrypted Content in the Content-ID settings. For more information, log into Live and search for "Forward Decrypted SSL traffic for WildFire Analysis" or see the documentation at: https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/submit-files-for-wildfire-analysis/forward-decrypted-ssl-traffic-for-wildfire-analysis.html.



With the release of PAN-OS 10.0, you can configure real-time WildFire analysis on the firewall. Real-time WildFire analysis prevents malware variants of portable executables from entering your network in real-time by using a firewall-based classification engine built on the WildFire Cloud analysis technology. The real-time WildFire analysis classification engines are configured through an Antivirus Profile and require an active WildFire subscription. The real-time classification engines currently support PowerShell scripts and Windows executables.

To configure real-time WildFire analysis on the firewall, you create a new or update an existing Antivirus Security Profile to use the WildFire analysis classification engine. Next, you define a policy action for each classification engine you added to the Antivirus Profile. Policy actions can be configured to:

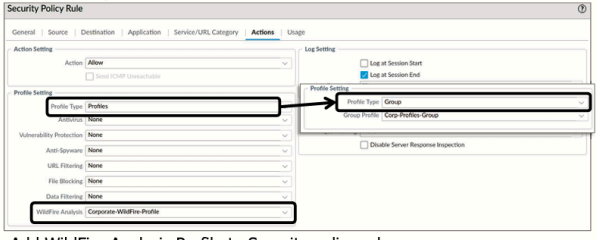
- **Enable (inherit per-protocol actions)**: Traffic is inspected according to your selections in the **WildFire Inline ML Action** column in the decoders section of the **Action** tab.
- **Alert-only (override more strict actions to alert)**—Traffic is inspected according to your selections in the WildFire Inline ML Action column in the decoders section of the Action tab. Any action with a severity level higher than alert (drop, reset-client, reset-server, reset-both) will be overridden to alert, allowing traffic to pass while generating and saving an alert in the threat logs.
- **Disable**: WildFire allows traffic to pass without any policy action.

Optionally, file exceptions can be added to an antivirus policy to exclude specific files, such as false positives. To add a file exception, add the file hash, filename, and description of the file you want to exclude from enforcement.

WildFire real-time analysis is not supported on the VM-50 and VM-50 lite virtual appliances.

Attach WildFire Analysis Profiles to Security Rules

Policies > Security > Add



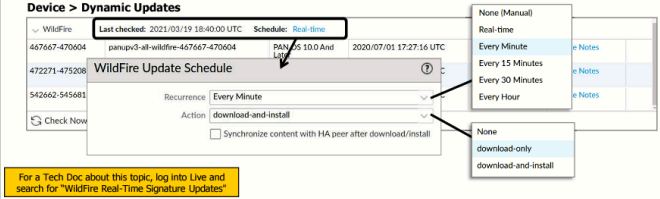
- Add WildFire Analysis Profile to Security policy rule, or
- Add WildFire Analysis Profile to Group Profile and add group to Security policy rule.

To assign a WildFire Analysis Profile to a Security policy rule, select **Profiles** as the **Profile Type** and add the WildFire Analysis Profile you created. You also can add a WildFire Analysis Profile to a Security Profile group. If the profile is part of a group, select **Group** for the **Profile Type** and add the group's name.

Note: If a file type is matched in the File Blocking Profile and WildFire Analysis Profile, and if the **File Blocking Profile** action is set to "block," the file is not forwarded to WildFire.

WildFire Update Schedule

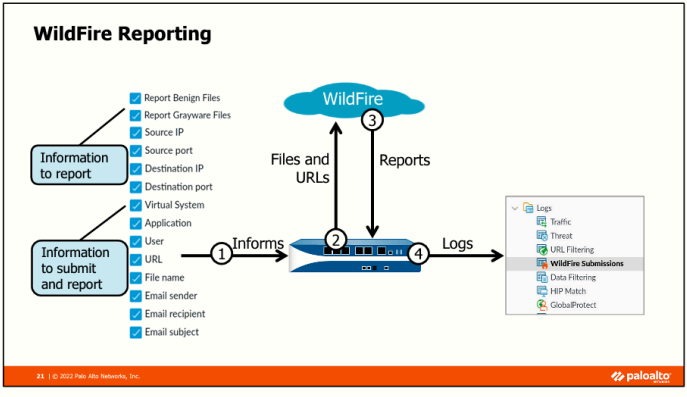
- Schedule poll period for WildFire antivirus signature updates:
  - Requires a WildFire license
  - Without a license, WildFire antivirus signatures still are added to the daily Antivirus content package.



Any new WildFire antivirus signatures created by WildFire are available for download from WildFire in real-time. If you have a WildFire license, you can configure how frequently your firewall wants to poll WildFire for new antivirus signatures. The example shows that you can configure your firewall to poll in real-time or up to once an hour.

If you do not have a WildFire license, your firewall can still access the new antivirus signatures developed by WildFire. WildFire transfers any new antivirus signatures to the Antivirus content package within 24 to 48 hours. You can configure your firewall to download the Antivirus content package daily.

This section describes WildFire reporting and how to report an incorrect verdict.

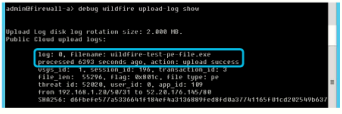


WildFire reports its findings to the firewall each time WildFire analyzes a file or URL link. You can configure both the types of information submitted to WildFire and the amount of data returned to the firewall in the report.

Information reported back to the firewall is recorded by the firewall in the WildFire Submissions log.

Verify Submissions and View Reports

```
> debug wildfire upload-log show
```



CLI command to verify successful file upload

View returned report information.

Monitor > Logs > WildFire Submissions

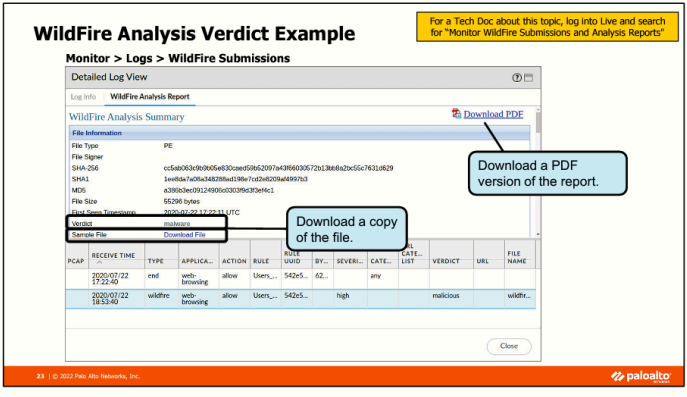
	RECEIVE TIME	FILE NAME	SOURCE ZONE	SOURCE ADDRESS	APPLICATION	RULE	VERDICT	SEVERITY
	07/10 17:04:24	wildfire-test-pe-file.exe	Users_Net	192.168.1.20	web-browsing	Users_to_Internet	malicious	high

For a Tech Doc about this topic, log into Live and search for "Verify WildFire Submissions"

22 | © 2022 Palo Alto Networks, Inc.

To verify successful file upload to WildFire, use the CLI and enter **`debug wildfire upload-log show`**. The output from the command should display something similar in format to what is shown in the example. Notice the status "upload success" and the file's name, which in the example is wildfire-test-pe-file.exe. This information confirms that the file was uploaded to the WildFire public cloud.

Files that contain malware should always be reported in the WildFire Submissions log. Benign or grayware files might be reported in the WildFire Submissions log, depending on how you have configured your firewall. The WildFire verdict is reported in the **Verdict** column. Your configuration of the firewall's WildFire settings will determine whether the information is available in many of the columns.

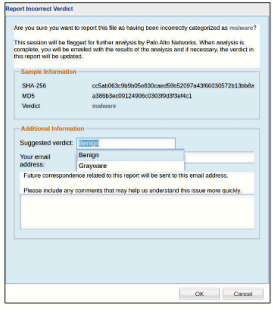


To display a detailed report about a submitted file, click the **magnifying glass** icon to the left of a log entry. The **Detailed Log View** window opens for that entry. Click the **WildFire Analysis Report** tab to display the details of the analysis by the WildFire technology.

Use the log entry and the WildFire analysis to find the targeted users, the applications used, and the malicious behavior observed.

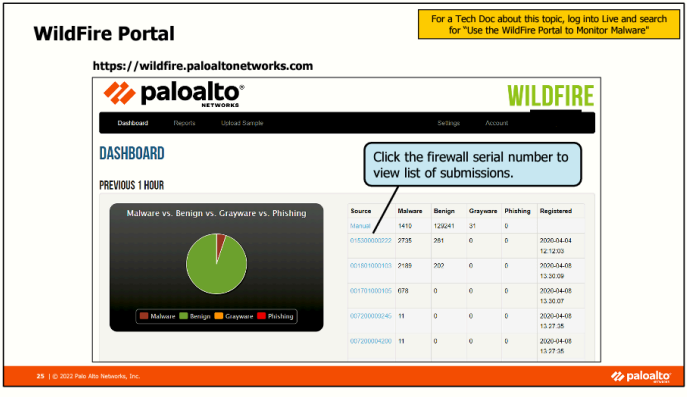
To print the analysis, click **Download PDF** and print the PDF document. The PDF includes a detailed timeline of the actions taken by the malware.

Report Incorrect Verdict: Web Interface



- You can submit verdict change requests to Palo Alto Networks:
  - From web interface or WildFire portal
- From web interface:
  1. Select **Monitor > Logs > WildFire Submissions**.
  2. Find entry and click its detailed view icon.
  3. Click **WildFire Analysis Report** tab.
  4. Click **Select Incorrect Verdict** link.
  5. Suggest new verdict.

WildFire reports indicate whether WildFire analysis showed a file to be benign, grayware, or malware. If you think that WildFire incorrectly categorized a file, you can use the web interface or the WildFire portal to request a new verdict from Palo Alto Networks. The example here shows the web interface form to request a new verdict.



The detailed analysis of the submitted files is available through the WildFire portal. To access the WildFire portal, go to https://wildfire.paloaltonetworks.com and log in using your Palo Alto Networks Support credentials or your WildFire account.

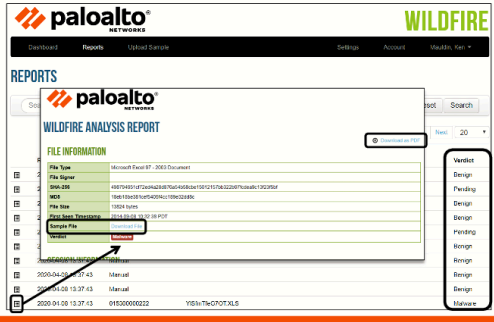
The browser opens to display the **Dashboard**, which lists summary information for all the firewalls associated with your WildFire account or Support account. The display includes the number of files that were found to be associated with malware, grayware, phishing, or was found to be benign. The **Dashboard** also reports summary information for the files submitted manually by a user using the WildFire XML API.

Click a firewall's serial number to display only the list of file submissions associated with a specific firewall. The **Reports** page will open, but the list of submissions will be filtered to include only those files submitted by that firewall.

You also can use the WildFire portal and click **Upload Sample** to upload one or more files for analysis manually. You can either directly upload the file to WildFire or specify a URL for the file.

WildFire Dashboard Reports

For a Tech Doc about this topic, log into Live and search for "WildFire Analysis Reports—Close Up"

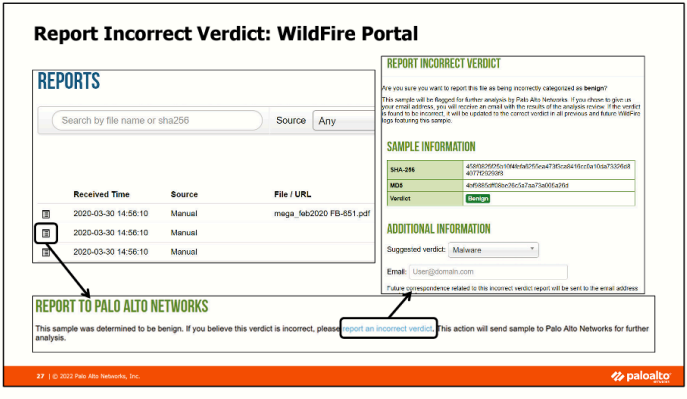


To display the entire list of submitted files, click the **Reports** button at the top of the WildFire portal. Search filter options are available at the top of the page to limit the number of submitted files displayed. The portal includes pagination controls if the number of entries exceeds the size of the page.

To display an Analysis report for an individual file, click the **details** icon to the left of the filename.

Use the WildFire portal to find the targeted users, the applications that were used, and the malicious behavior observed. The WildFire portal also can be configured to send email notifications when results are available for review. To configure email settings, click **Settings** in the portal.

To print a detailed report, use the print option on your browser.



You also can request a new verdict using the WildFire portal. Click the **details** icon next to a WildFire report. Scroll down in the browser page that opens and click the **report an incorrect verdict** link. In the window that opens, add information to the fields in the form and click **Submit**.

Module Summary

Now that you have completed this module, you should be able to:

- Describe WildFire purposes and operation
- Describe WildFire license and deployment choices
- Configure and update WildFire
- View WildFire reports and logs

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"Wildfire Versus Malware"

© 2022 Palo Alto Networks, Inc.

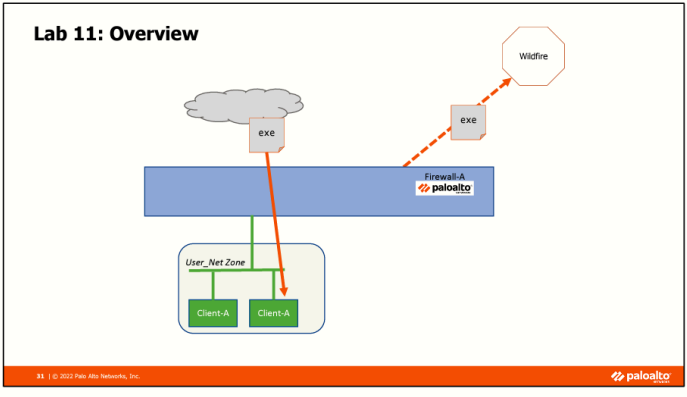
Review Questions

1. Which file type can a firewall send to WildFire when the firewall does not have a WildFire subscription?
   a. PDF
   b. JAR
   c. APK
   d. EXE

2. Which WildFire verdict might indicate obtrusive behavior but not a security threat?
   a. benign
   b. grayware
   c. malware
   d. phishing

3. True or false? When a malicious file or link is detected in an email, WildFire can update antivirus signatures in the PAN-DB database.
   a. true
   b. false

4. Assume you have a WildFire subscription. Which file state or condition might result in a file not being analyzed by WildFire?
   a. executable file signed by a trusted signer
   b. file size limit exceeded
   c. file already has WildFire hash
   d. file located in a JAR or RAR archive



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 11: Blocking Unknown Threats with WildFire

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

© 2022 Palo Alto Networks, Inc.

Answers to Review Questions

1. d
2. b
3. b (false)
4. d