WILDFIRE

EDU-210 Version A
PAN-OS® 9.0

DETECT UNKNOWN THREATS

- WildFire® concepts
- Configuring and managing WildFire
- WildFire reporting

Agenda

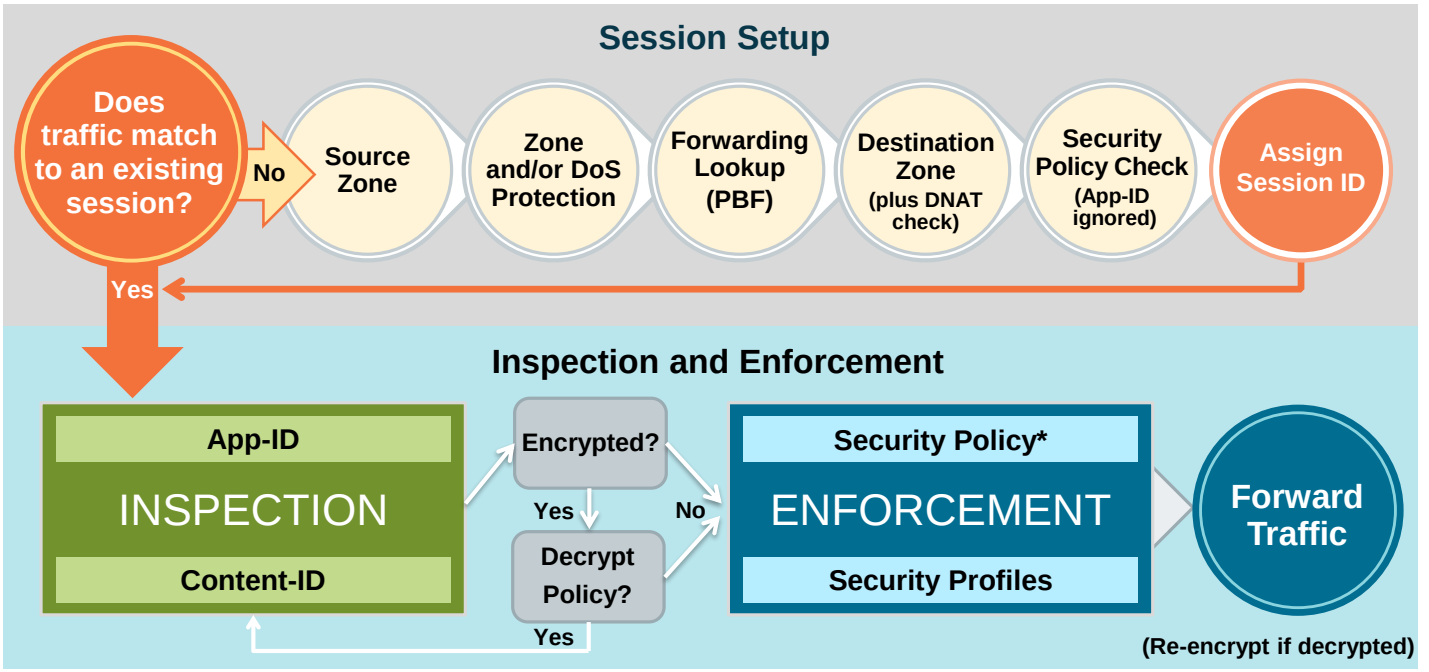
After you complete this module, you should be able to:

- Describe how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure Session Information Settings to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

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

- Describe how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure **Session Information Settings** to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall. The course will reference this diagram to address where specific concepts fit into the packet processing sequence.

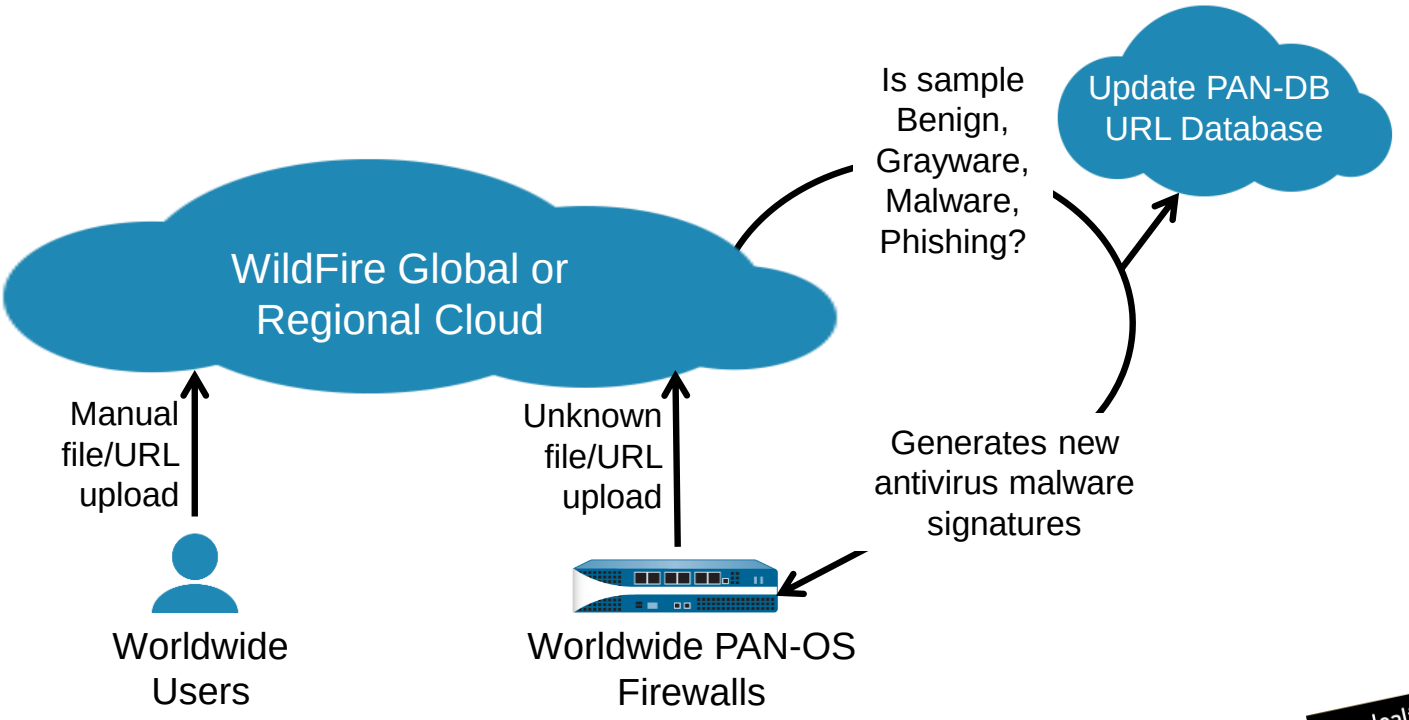
For more information about the packet handling sequence inside of a PAN-OS® device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.

WildFire concepts

Configuring and managing WildFire

WildFire reporting

WildFire Threat Intelligence Cloud

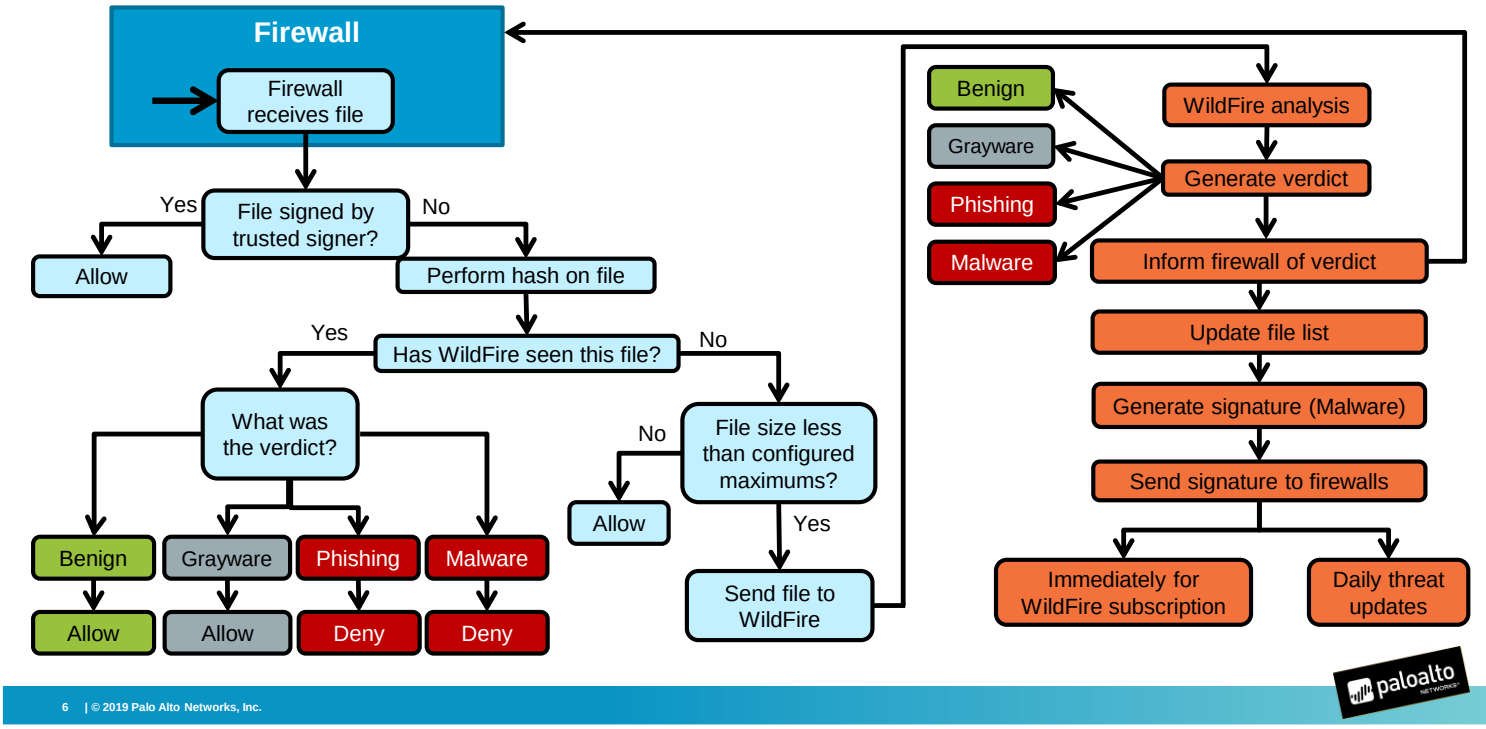


Modern malware has evolved from being simple replication of viruses to being highly evasive and adaptable network applications that allow hackers to launch increasingly sophisticated and targeted attacks. This new breed of malware is at the core of many of today's most sophisticated intrusions. As malware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

Palo Alto Networks firewalls across the world automatically forward unknown files and URL links found in emails to the WildFire Threat Intelligence Global Cloud or to one of three WildFire regional clouds for analysis. The three regional clouds are in Europe, Japan, and Singapore. 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, which enables WildFire users worldwide to benefit from malware coverage regardless of the location where the malware was first detected. WildFire users worldwide also can use the WildFire XML API or WildFire Dashboard to manually upload files to WildFire for analysis. For more information about the WildFire XML API, see the *WildFire API Reference Guide* at https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-api.html.

WildFire is a cloud-based, virtual sandbox used to evaluate unknown files and URL links found in emails. The evaluation occurs for Android, Linux, Mac OSX, Windows XP, Windows 7, and Windows 10. After analysis is complete, files and links are labeled as Benign, Grayware, Malware, or Phishing. If malware or a phishing URL is found, WildFire creates a new antivirus signature or adds the URL to the PAN-DB Phishing URL category and then makes these updates available in minutes for download by firewalls around the world.

WildFire Operation Overview



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

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

If the file has been sent to WildFire, then the previous verdict is used by the firewall. If the file has not been sent to WildFire, then 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, then the firewall allows the file to be delivered and the file is 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 in minutes to WildFire-licensed firewalls around the world. Unlicensed firewalls can retrieve the new signature within 24 to 48 hours through normally 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	▪ Based on properties and behaviors the website displays

A Benign verdict is given by WildFire to files or URLs that have been found to be safe and pose no threat to your organization.

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

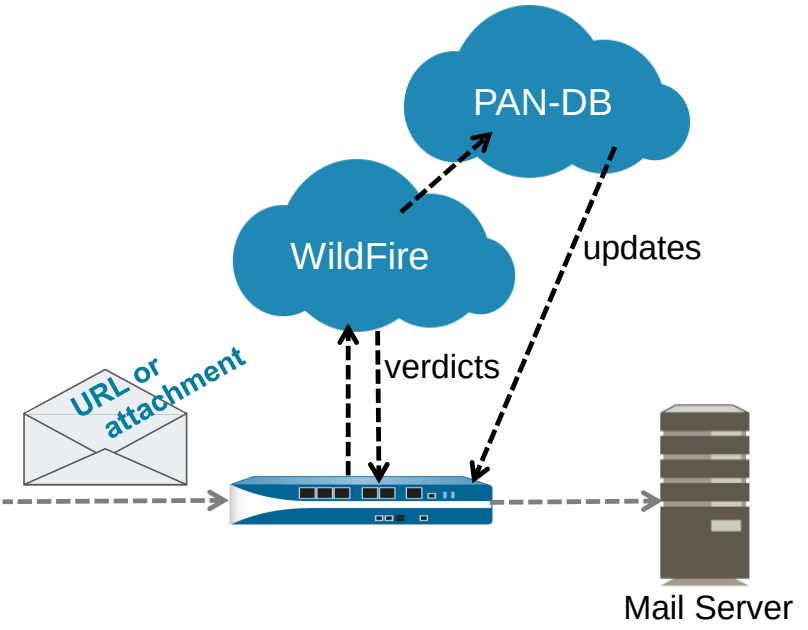
A Malware verdict indicates that WildFire has determined that the file or URL is malicious in nature and intent and can pose a security threat to your organization. If a current signature does not exist, WildFire will create one and make it available to firewalls around the world. WildFire also will 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 properties and behaviors that the accompanying website displays, and 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.

WildFire Protects Email

- Email with attachments or URL links sent to WildFire for analysis
- If an attachment or link is malicious, WildFire can:
  - Create and download new antivirus signatures to the firewall
  - Update the PAN-DB database with malicious URLs
- The firewall uses new information to protect the network.



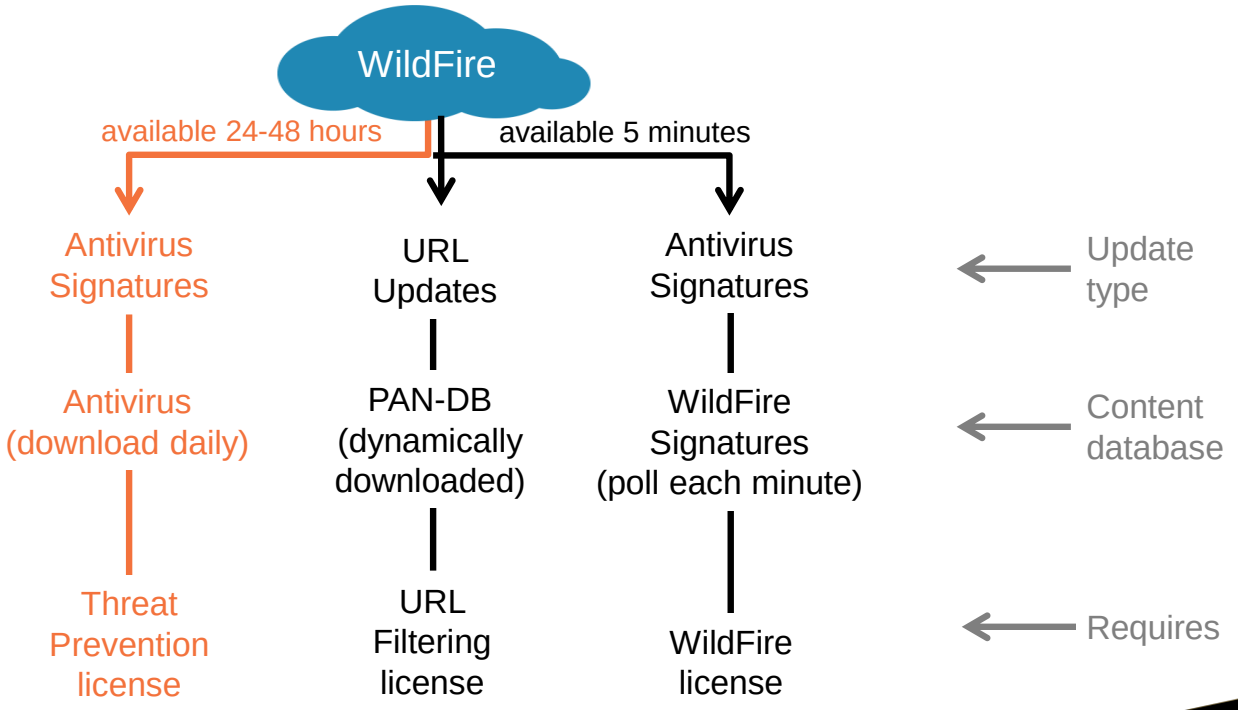
The firewall sends email with attachments or URL links to WildFire for analysis. Neither the firewall nor WildFire stores or enables the viewing of email contents.

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

If WildFire determines that a URL link included in the email is malicious, it quickly updates the antivirus 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 URL 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 in as few as 5 minutes.

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 quickly find and remediate the threats received by your users. If User-ID matches a name in the WildFire log, the log's Email Header section contains a link. If you clink the link, the **ACC** tab opens, filtered by the user or group of users.

Content Packages and WildFire Updates



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. Firewall access to the Antivirus content database is enabled by a Threat Prevention license.

Antivirus signatures also are made available within 5 minutes 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 intervals as frequent as every minute. Firewall access to the WildFire antivirus signatures is enabled by a WildFire license.

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. Firewall access to the PAN-DB URL Filtering database is enabled by a URL Filtering license.

Standard and Licensed Functionality

Standard subscription service:

- Windows XP and 7 analysis
- Windows PE file analysis:
  - EXE, DLL, FON, SCR, others
- Antivirus signatures delivered via daily dynamic content updates (requires Threat Prevention license)
- Automatic file submission

WildFire licensed service:

- Standard subscription features
- Additional file type analysis:
  - Microsoft Office, PDF, JAR, CLASS, SWF, SWC, APK, Mach-O, DMG, RAR, 7-Zip, Linux ELF, and PKG files
- WildFire signature updates every 5 minutes
- API file submission
- WildFire private cloud appliance:
  - WF-500

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 Windows XP and Windows 7 virtual machines. 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 normal dynamic content updates.

Palo Alto Networks firewalls with a WildFire license are entitled to the standard subscription features and additional features. More file types may be submitted by a firewall for analysis. Additional 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. Flash files or Flash content embedded in webpages are analyzed. The Mac OS-X Mach-O, DMG, and PKG files also are supported.

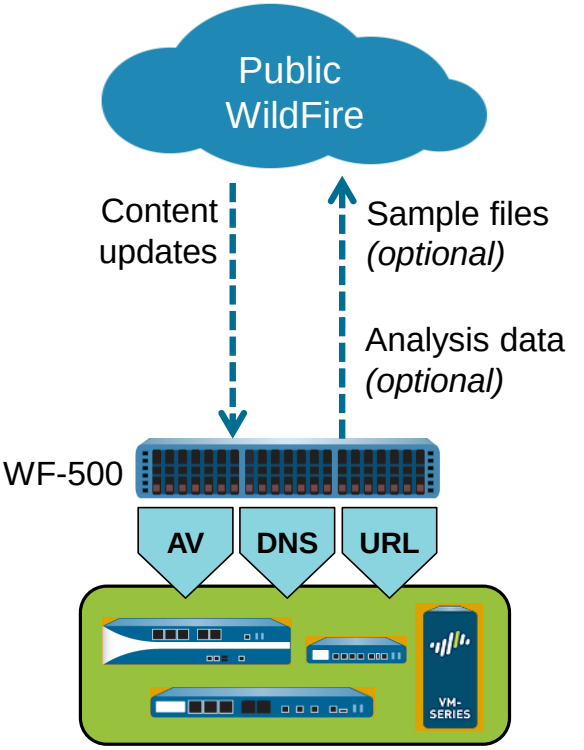
WildFire can create new signatures every 5 minutes. WildFire licensed firewalls have access to those signatures, which enables near real-time protection against the latest threats detected anywhere in the world. The 5-minute WildFire content update time applies to PAN-OS 7.1 and later. In previous versions 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, see the *WildFire API Reference Guide* at https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-api.html.

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

WildFire Private Cloud

- WF-500 appliance:
  - Only Windows XP and 7 virtual environments
- Locally analyzes unknown files, and files or URLs found in email:
  - Files never leave your network
  - No APK files
- Locally generates antivirus signatures and categorizes URLs
- Signatures updated every 5 minutes
- Supports the WildFire XML API
- Does not support the Phishing verdict



The WF-500 appliance is a WildFire private cloud solution. It supports Windows XP and Windows 7 virtual environments and requires that you install a Window 7 64-bit image on the appliance.

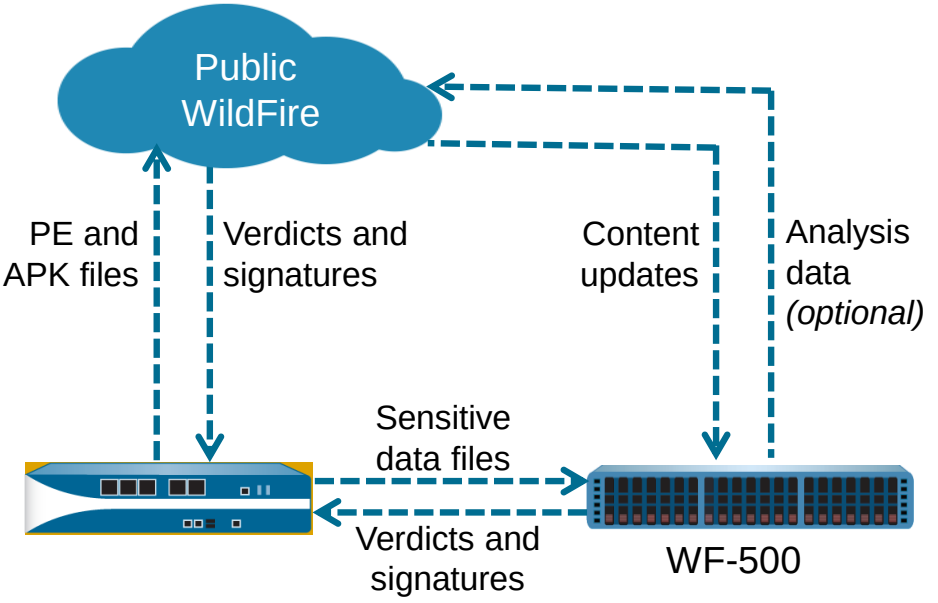
The WF-500 appliance analyzes files forwarded from your Palo Alto Networks firewalls or from the WildFire XML API. Beginning with PAN-OS 6.1, the WF-500 appliance can generate signatures locally and categorize URLs. Because the WildFire private cloud is a local sandbox benign, grayware, and phishing files that are analyzed never leave your network. By default, the WF-500 appliance never sends malware files outside of your network. However, you can choose to automatically forward malware files to the WildFire public cloud for signature generation. In this case, the WildFire public cloud re-analyzes the file, generates a signature to identify the malware, and distributes the signature worldwide. You also can choose to send a Malware report, but not the actual file.

The WF-500 appliance supports the WildFire XML API. For more information about the WildFire XML API, see the *WildFire API Reference Guide* at https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-api.html.

Daily content updates for the WF-500 appliance provide additional cloud intelligence, which leads to more accurate results. The content updates help improve WF-500 analysis accuracy by providing daily updates to trusted code-signing certificates, malware domain lists, new signatures, and other useful information. Just as with firewall content packages, you can configure automatic download and installation of the WF-500 content packages or you can manually download and install the content packages. Content updates can be installed directly from an internet connection, or through another host with an internet connection.

Hybrid Cloud Example

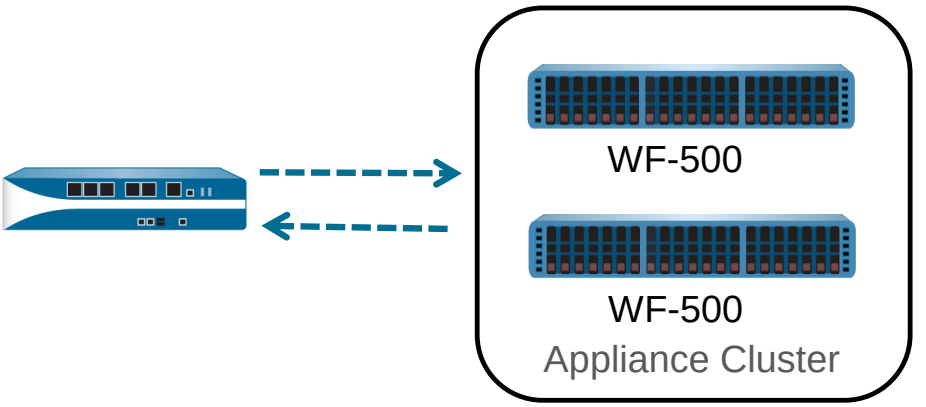
- Combines public and private cloud
- PE and APK files to public cloud?
- Sensitive data files to private cloud?



A hybrid cloud combines the public and private cloud solutions. If you use a WF-500 appliance, you can configure a WildFire hybrid cloud that enables the WF-500 to analyze sensitive file types locally, while 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, 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.

WildFire Appliance Cluster

- Combines multiple WildFire appliances for fault tolerance
- Useful when the WildFire public cloud cannot be used
- Can group up to 20 appliances



You can configure and manage up to 20 WildFire appliances as a WildFire appliance cluster on a single network. WildFire appliance clusters are especially useful in environments where you cannot use the WildFire public cloud. WildFire appliance clusters can support a larger firewall deployment on a single network than a standalone WildFire appliance supports. Clusters also provide fault tolerance and a single signature package that is distributed to all firewalls connected to the cluster.

Beginning with PAN-OS 8.1, you can enable encryption in WildFire appliance clusters to maintain the confidentiality of transmitted content, including user samples. Enablement of encryption allows you to configure custom and predefined client certificates, and server certificates, to establish encrypted appliance-to-appliance communication. You also can operate clusters in a FIPS/CC-compliant environment when they are configured using FIPS/CC-compliant certificates.

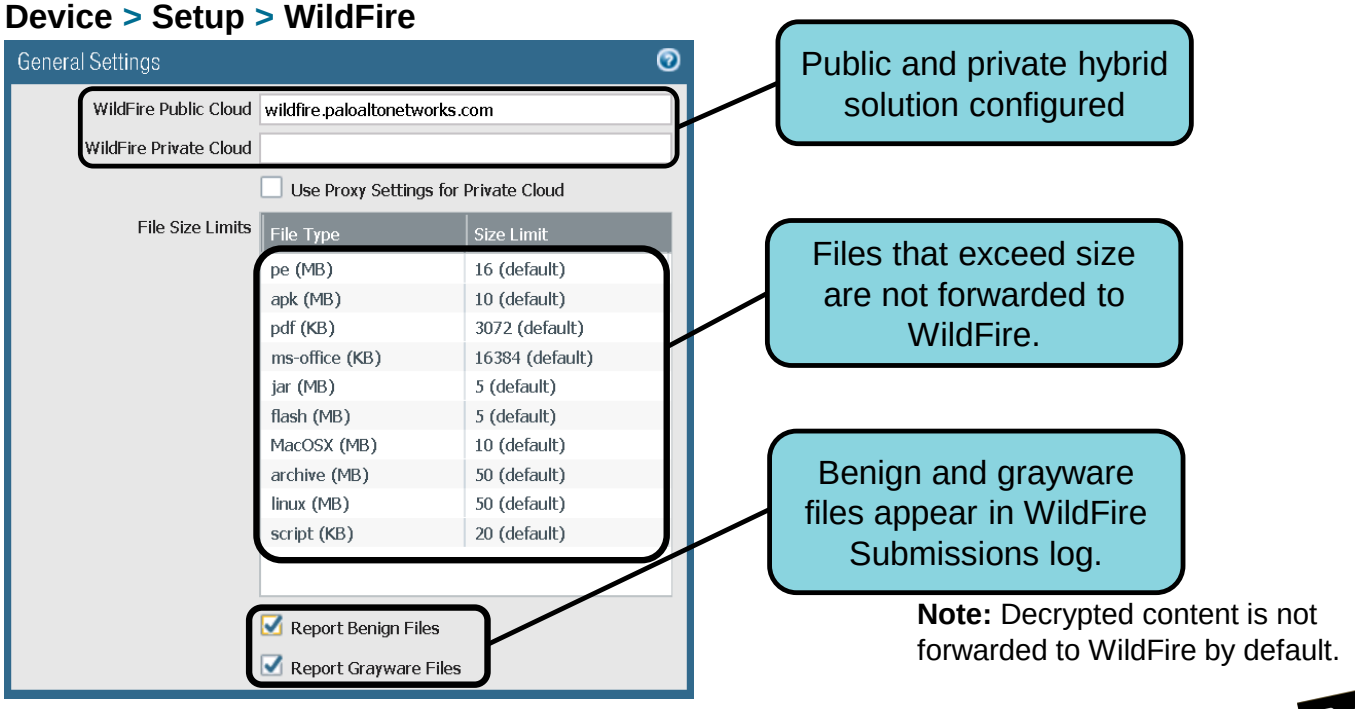
WildFire concepts

Configuring and managing WildFire

WildFire reporting

Configuring WildFire Settings

Device > Setup > WildFire



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, which is the global WildFire cloud. Other URL values also are available in other 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 forwarded to the global WildFire cloud.

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

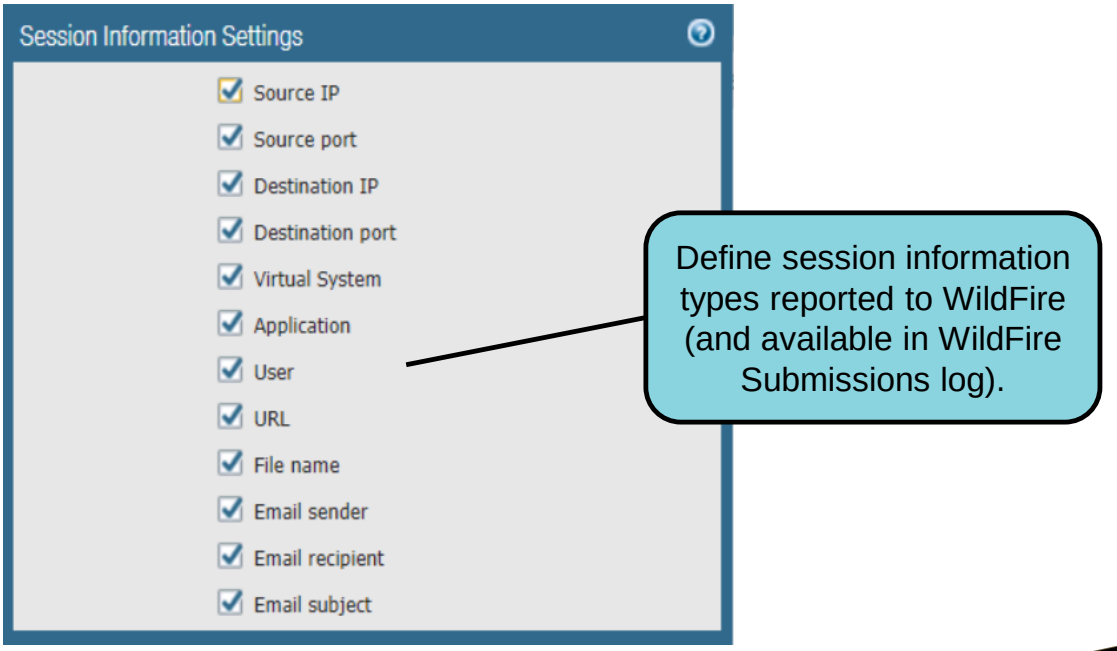
You also can configure size limits for files forwarded to WildFire for analysis. The default and maximum size limits have been increased with the release of PAN-OS 9.0. The updated default file sizes are designed to include the vast majority of malware that you are likely to encounter. Files larger than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

The **Report Benign Files** and **Report Grayware Files** check boxes are not enabled by default. If you enable them, then 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 email because the size of these reports could be prohibitively large.

If you have configured SSL or SSH decryption, 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**.

Submission Settings

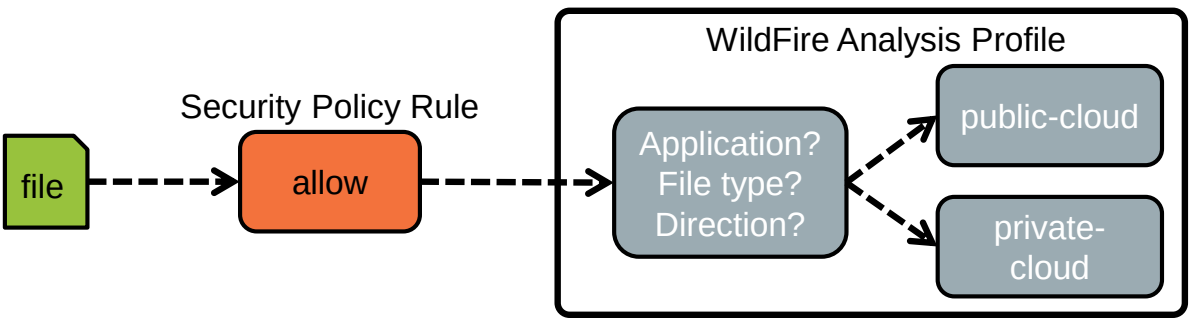
Device > Setup > WildFire



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 in the WildFire portal.

WildFire Analysis Profile

- Profile implements additional security checks on files in allowed traffic.

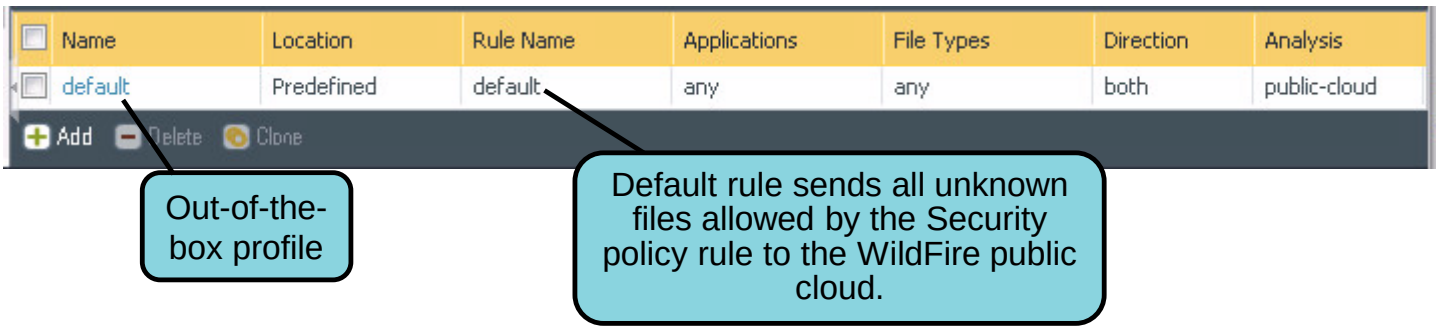


WildFire Analysis Profiles are objects that are added to Security policy rules that are configured with an action of "allow." WildFire Analysis Profiles are not necessary for Security policy rules configured with the "deny" action because no further processing is needed if the network traffic will be 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 to be performed 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 specific direction by a specific application. The files submitted to WildFire are logged to the log found at **Monitor > Logs > WildFire Submissions**.

WildFire Analysis Profile (Cont.)

Objects > Security Profiles > WildFire Analysis



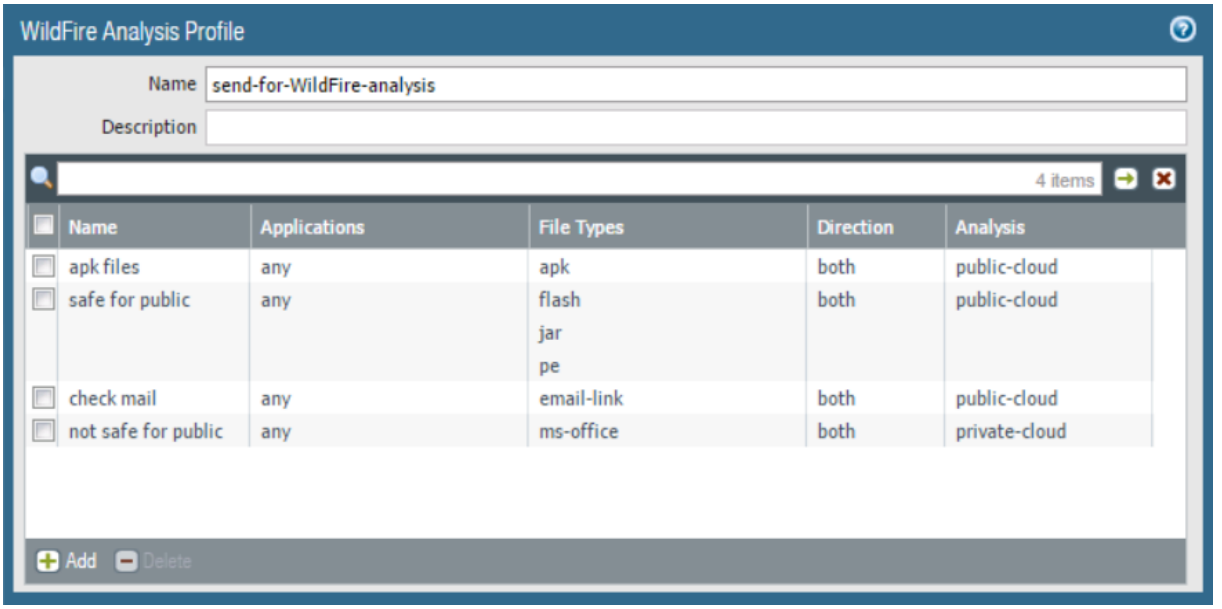
- To create customized profiles:
  - Clone the default read-only profile and edit the clone, or
  - Add a new profile

A Palo Alto Networks firewall includes a predefined, read-only default WildFire Analysis Profile. If the default profile is assigned to a Security policy rule, then 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 customized 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 to 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

Objects > Security Profiles > WildFire Analysis > Add



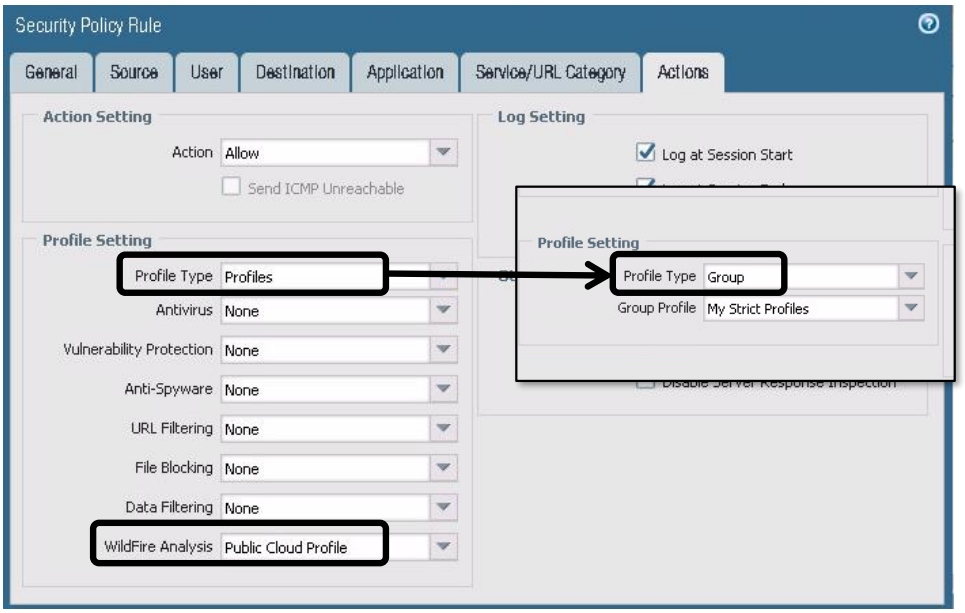
Use a WildFire Analysis Profile to specify which application file types to send to WildFire for analysis. You can specify which traffic to forward to a WildFire public or private cloud based on application, file type, and transmission direction.

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

In some instances an organization might determine that its Microsoft documents or PDFs might have sensitive information that the organization does not want 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.

Attaching WildFire Analysis Profiles to Security Rules

Policies > Security > Add



- Assign WildFire Analysis Profile to security rule
- Add WildFire Analysis Profile to Group Profile and add group to security rule

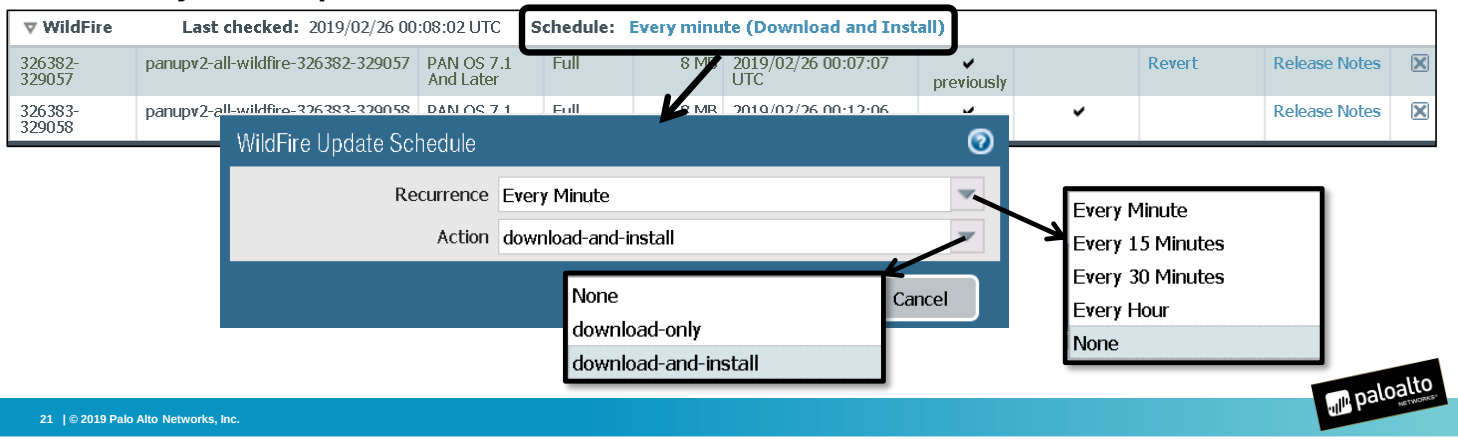
To assign a WildFire Analysis Profile to a Security policy rule, select **Profiles** as the **Profile Type**, then add the WildFire Analysis Profile you created. You also can add a WildFire Analysis Profile to a Security Profile Group. If the profile is part of a group, select **Group** for the **Profile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

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,” then 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 into the daily Antivirus content package.

Device > Dynamic Updates



Any new WildFire antivirus signatures created by WildFire are available for download from WildFire in as little as 5 minutes. If you have a WildFire license, you can configure how frequently you want your firewall to poll WildFire for new antivirus signatures. The example shows that you can configure your firewall to poll as often as every minute.

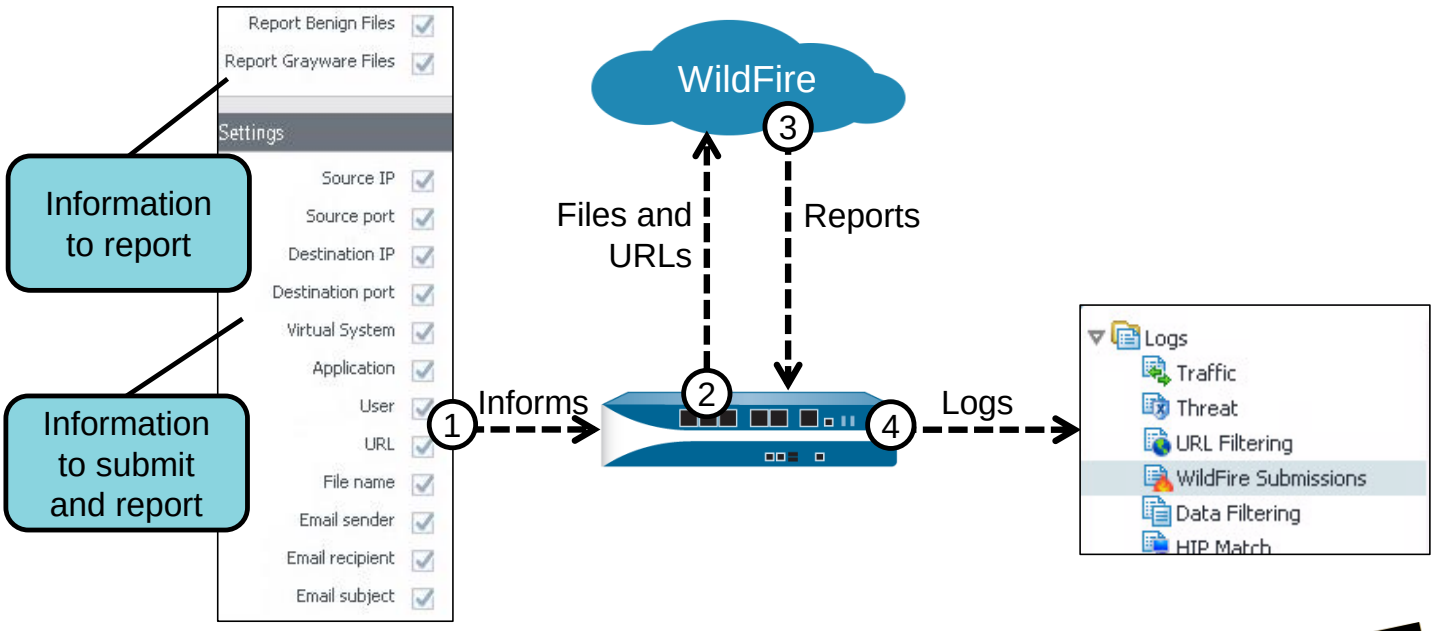
If you do not have a WildFire license, your firewall still can access the new antivirus signatures developed by WildFire. WildFire transfers any new antivirus signatures to the Antivirus content package within 24 to 48 hours. You can configure your firewall to download the Antivirus content package daily.

WildFire concepts

Configuring and managing WildFire

WildFire reporting

WildFire Reporting



Each time that WildFire technology analyzes a file or URL link, it reports its findings to the firewall. You can configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report.

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

Verifying Submissions and Viewing Reports

```
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 6393 seconds ago, action: upload success
        vsys_id: 1, session_id: 196, transaction_id: 3
        file_len: 55296, flag: 0x801c, file type: pe
        threat id: 52020, user_id: 0, app_id: 109
        from 192.168.1.20/50731 to 52.20.176.145/80
        SHA256: d6fbefe577a5336641f184ef4a3136889fed8fd0a3774165f01cd202549b637
```

- CLI command to verify successful file upload:
  - **`debug wildfire upload-log show`**
- View returned report information

Monitor > Logs > WildFire Submissions

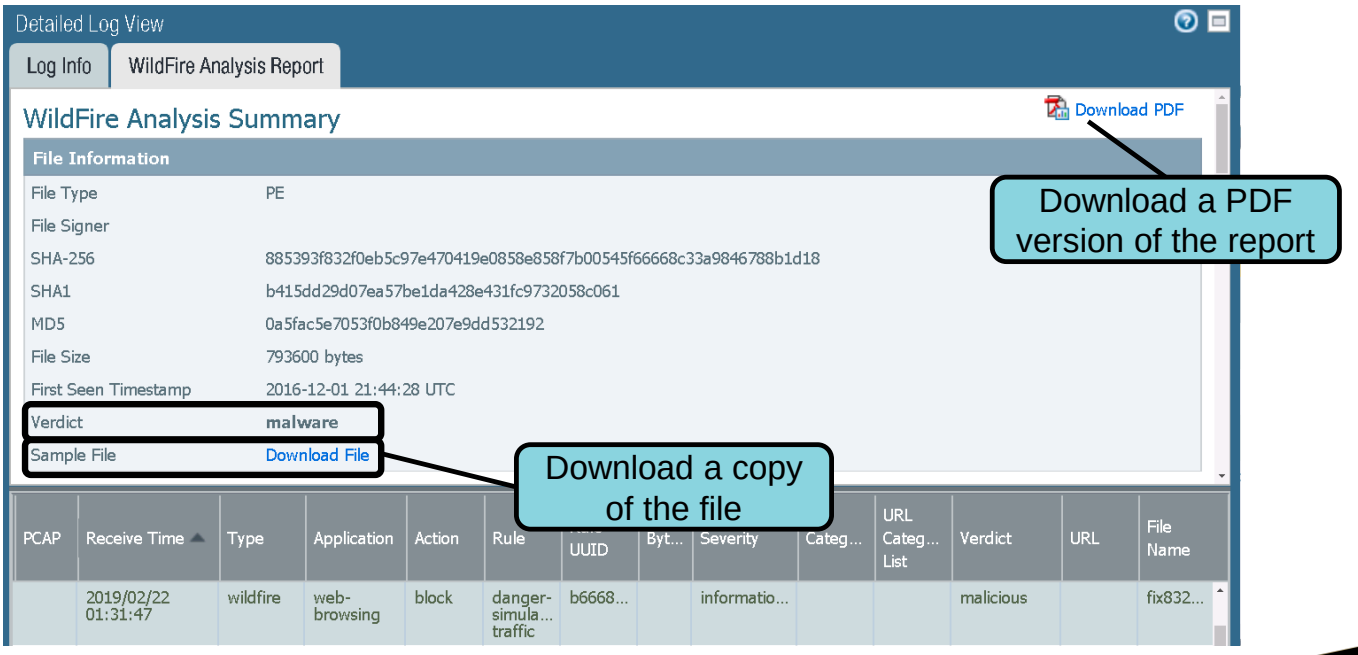
	Receive Time	File Name	Source Zone	Destination Zone	Source address	Destination address	Desti... Port	Application	Rule	Verdict	Action
	02/22 01:31:47	fix832922.ms	danger	danger	10.12.1.101	194.58.100.59	80	web-browsing	danger-simulated-traffic	malicious	block
	02/22 01:31:47	89yg7g87byi	danger	danger	10.5.3.101	72.52.179.2	80	web-browsing	danger-simulated-traffic	malicious	block
	02/22 01:31:47	locky.exe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	danger-simulated-traffic	malicious	allow

To verify successful file upload to WildFire, use the CLI and enter the command **`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 name of the file, 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 always should be reported in the WildFire Submissions log. Benign files or files that contain grayware 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 information is available in many of the columns.

WildFire Analysis Verdict Example

Monitor > Logs > WildFire Submissions

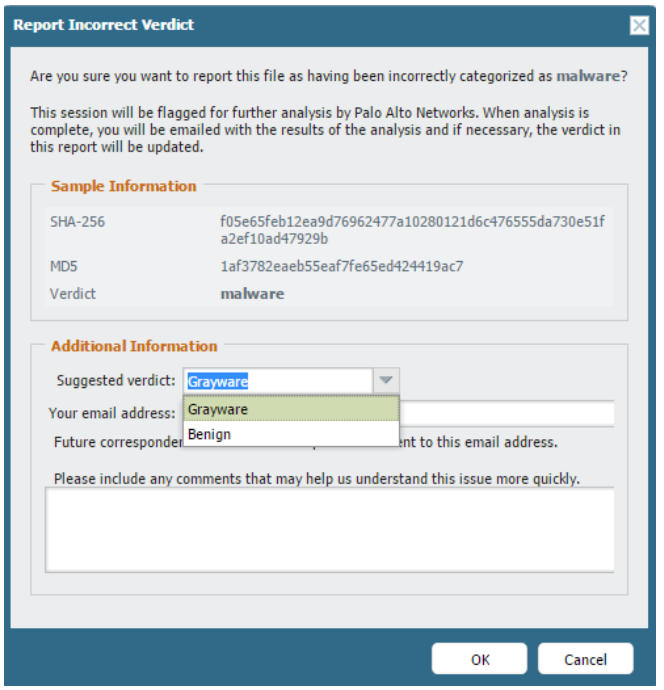


To display a detailed report about a submitted file, click the **magnifying glass** icon to the left of a log entry. The **Detailed Log View** window opens for that entry. Click the **WildFire Analysis Report** tab to display the details of the analysis by the WildFire technology.

Use the log entry and the WildFire analysis to find the users that were targeted, the applications that were used, and the malicious behavior that was 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

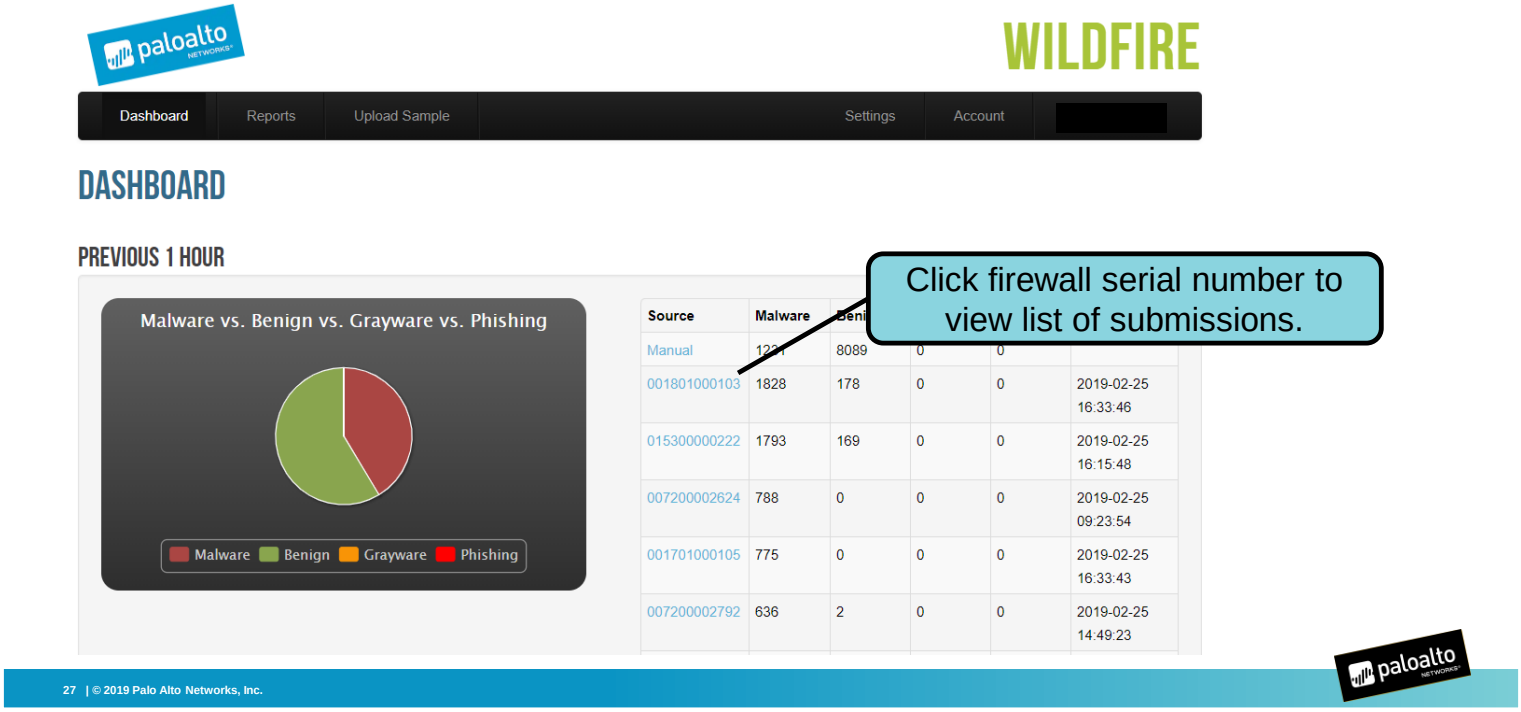


- You can submit verdict change request to Palo Alto Networks:
  - From web interface or WildFire portal
- From web interface:
  - Select Monitor > Logs > WildFire Submissions.
  - Find entry and click its detailed view icon.
  - Click WildFire Analysis Report tab.
  - Click Select Incorrect Verdict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

WildFire reports indicate whether WildFire analysis showed a file to be Benign, Grayware, or Malware. If you think that a file was incorrectly categorized by WildFire, you can use the web interface or the WildFire portal to request a new verdict from Palo Alto Networks. The example here displays the web interface form used to request a new verdict.

WildFire Portal

https://wildfire.paloaltonetworks.com



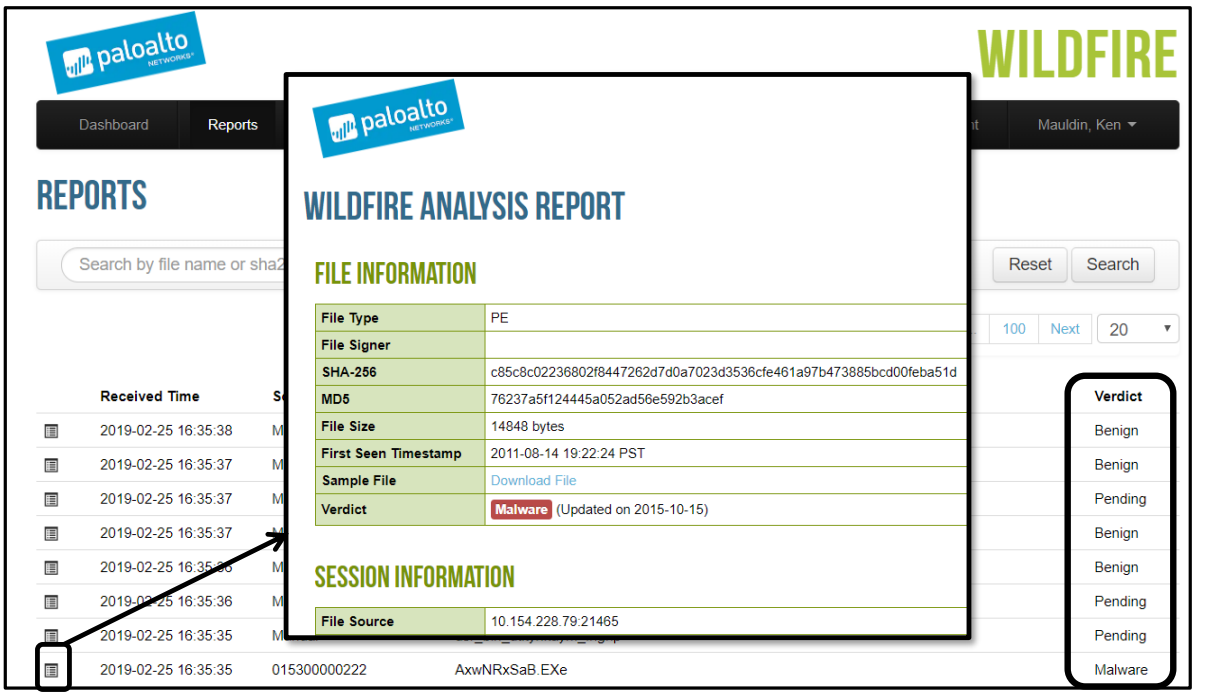
Results of the detailed analysis of the submitted files are available through the WildFire portal. To access the WildFire portal, go to https://wildfire.paloaltonetworks.com and log in using your Palo Alto Networks Support credentials or your WildFire account.

The browser opens to display the **Dashboard**, which lists summary information for all of 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, or phishing, or were found to be benign. The dashboard also reports summary information for the files that were submitted manually by a user using the WildFire XML API.

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

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

WildFire Dashboard Reports



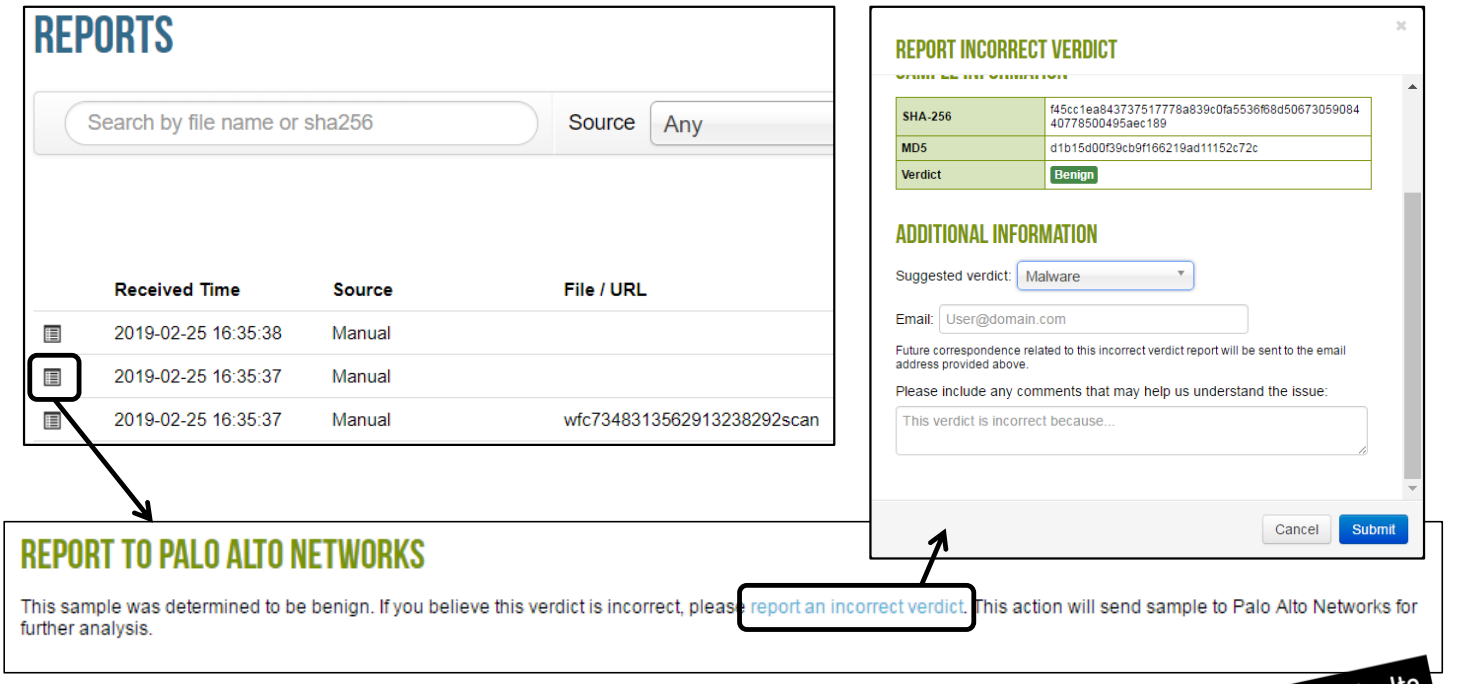
To display the entire list of submitted files, click the **Reports** button at the top of the WildFire portal. Search filter options are available at the top of the page to allow you to limit the number of submitted files that are displayed. The portal includes pagination controls if the number of entries 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 users that were targeted, the applications that were used, and the malicious behavior that was 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.

Report Incorrect Verdict: WildFire Portal



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 how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure Session Information Settings to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

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

- Describe how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure **Session Information Settings** to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

Questions?

Review Questions

1. Which three attributes are true regarding WildFire? (Choose three.)
   a. Identifies threats by signatures, which are available for download by Palo Alto Networks firewalls in as little as 5 minutes.
   b. Provides the ability to identify malicious behaviors in executable files by running them in a virtual environment and observing their behaviors.
   c. Triggered by “block” or “forward” actions in a File Blocking Security Profile
   d. Uploads files for analysis to a WildFire solution maintained in the customer’s environment and/or a hosted public cloud environment.
2. Which four options are possible WildFire analysis verdicts? (Choose four.)
   a. Benign
   b. Grayware
   c. Malware
   d. Phishing
   e. Spyware
3. True or false? When a malicious file or link is detected in an email, WildFire can update antivirus signatures and the PAN-DB database.
   a. true
   b. false
4. Which three file types can be sent to WildFire without a WildFire license? (Choose three.)
   a. dll
   b. exe
   c. pdf
   d. scr
   e. xml

WildFire Lab (Pages 163-169 in the Lab Guide)

- Load a firewall lab configuration
- Create and test a WildFire Analysis Profile

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b, d
2. a, b, c, d
3. a (true)
4. a, b, d

This page intentionally left blank