WildFire What's New Guide
Contact Information
Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation
• For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
• To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
• Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright
Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2018-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised
February 12, 2019
# Table of Contents

**Latest WildFire Cloud Features** ................................................................. 5  
Real Time WildFire Verdicts and Signatures for Documents.......................... 7  
Script Sample Analysis.................................................................................. 8  
ELF Malware Test File.................................................................................. 10  
Email Link Analysis Enhancements............................................................. 11  
Sample Removal Request........................................................................... 12  
Updated WildFire Cloud Data Retention Period......................................... 14  
DEX File Analysis....................................................................................... 15  
Network Traffic Profiling........................................................................... 16  
Additional Malware Test Files................................................................... 17  
Dynamic Unpacking.................................................................................... 18  
Windows 10 Analysis Environment............................................................. 19  
Archive (RAR/7z) and ELF File Analysis..................................................... 20  
WildFire Analysis of Blocked Files.............................................................. 21  
WildFire Phishing Verdict........................................................................... 22

**WildFire Features in PAN-OS 9.0** ........................................................... 25  
Increased WildFire File Fowarding Capacity............................................... 27  
WildFire Appliance Archive Support.......................................................... 29

**WildFire Features in PAN-OS 8.1** ............................................................ 31  
WildFire Appliance-to-Appliance Encryption............................................. 33

**WildFire Features in PAN-OS 8.0** ............................................................ 37  
Panorama Centralized Management for WildFire Appliances..................... 39  
WildFire Appliance Clusters......................................................................... 40  
Preferred Analysis for Documents or Executables....................................... 41  
Verdict Changes............................................................................................ 42  
Verdict Checks with the WildFire Global Cloud.......................................... 44

**WildFire Release History** ....................................................................... 45  
WildFire Release Listing............................................................................... 47
Latest WildFire Cloud Features

The following list shows all of the new features that were added to the WildFire Cloud. Each section provides context for the new feature, with steps to get started.

New Cloud Features: January 2019

> Real Time WildFire Verdicts and Signatures for Documents

New Cloud Features: December 2018

> Script Sample Analysis
> ELF Malware Test File

New Cloud Features: October 2018

> Email Link Analysis Enhancements

New Cloud Features: August 2018

> Sample Removal Request
> Updated WildFire Cloud Data Retention Period
> DEX File Analysis

New Cloud Features: July 2018

> Network Traffic Profiling

New Cloud Features: May 2018

> Dynamic Unpacking
> Additional Malware Test Files

New Cloud Features: March 2018

> Windows 10 Analysis Environment
> Archive (RAR/7z) and ELF File Analysis
> WildFire Analysis of Blocked Files
> WildFire Phishing Verdict
Real Time WildFire Verdicts and Signatures for Documents

WildFire protections and verdicts for Microsoft office documents are now available immediately after the WildFire cloud completes static analysis. Products and services that integrate with WildFire can also access the immediate verdicts to coordinate enforcement to prevent successful attacks. Additional information about a malicious file is available in the WildFire sample analysis report when WildFire completes dynamic analysis.
Script Sample Analysis

To use this feature, be sure to download and install the latest PAN-OS content release. PAN-OS Applications and Threats content release 8.101 enables you to specify file forwarding of script files. For more information about the update, refer to the Applications and Threat Content Release Notes.

To download the release notes, log in to the Palo Alto Networks Support Portal, click Dynamic Updates and select the release notes listed under Apps + Threats.

The WildFire public cloud can now analyze and classify script files with verdicts using static and dynamic analysis. When a malicious script is discovered, the WildFire cloud generates and distributes C2 and DNS signatures to firewalls to prevent successful script-based attacks. Because C2 and DNS signatures look at key network behaviors contained within samples, these signatures can detect activity in previously unknown malicious scripts. To ensure that you are protected from the latest threats, always keep your firewalls up-to-date with the latest content and software updates from Palo Alto Networks.

- The WildFire appliance does not support script file analysis at this time.
- Only firewalls operating PAN-OS 8.1 and later can forward scripts to the WildFire public cloud.

The WildFire cloud is capable of analyzing the following script types:

- JScript (.js)
- VBScript (.vbs)
- PowerShell Script (.ps1)

To forward script files for analysis, the WildFire Analysis Profile on the firewall must be configured to forward the script file type or Any unknown files to the WildFire public cloud.

1. Enable file type forwarding.
   1. Select Objects > Security Profiles > WildFire Analysis and Add or modify a profile to define traffic to forward for WildFire analysis.
   2. Add or modify a profile rule, select file type, and set the rule to forward the new Any file type. You can also specify the script file type if you want to forward only scripts.

   Profile rules with the file type set to Any forward all file types for WildFire analysis.

   3. Select Destination and set the profile rule to forward the files to the public-cloud.
   4. Click OK to save the new or modified WildFire Analysis profile.

2. Attach the WildFire Analysis profile to a security policy rule—traffic matched to the policy rule is forwarded for WildFire Analysis.

   1. Select Policies > Security and Add or modify a security policy rule.
   2. Select Actions and set the Profile Type to Profiles.
   3. Select the newly-created WildFire Analysis profile.
   4. Click OK to save the security policy rule.

   For detailed steps to configure a WildFire Analysis profile and to attach the profile to a security policy rule, see Forward Files for WildFire Analysis.
3. Select **Monitor > WildFire Submissions** to find WildFire verdicts and analysis reports for script files that have been submitted by the firewall.

You can also submit script files directly to the WildFire public cloud for analysis. With a WildFire subscription, you can manually and programmatically submit a daily total of 1,000 files. Each submission counts as a single upload regardless of the content.

1. **Manually submit** files to the WildFire public cloud for analysis. You can then view the WildFire sample analysis report and verdict (malicious, grayware or benign) on the WildFire portal.

2. **Use the WildFire API** to submit files to the WildFire public cloud. You can use the WildFire API to retrieve verdicts and analysis reports for the files. You can also specify script as the target analysis environment when you retrieve a packet capture through the WildFire API.
ELF Malware Test File

Palo Alto Networks now provides an ELF sample malware file to test your WildFire deployment. The new file can be downloaded using a direct download link using your browser or through the WildFire API. Download one of the new sample files and verify that it gets forwarded to WildFire for analysis.

**STEP 1 |** Download one of the new malware test files. Select from either direct or API download.

- **Direct Download:**
  - If you have SSL decryption enabled on the firewall, use the following URL: https://wildfire.paloaltonetworks.com/publicapi/test/elf
  - If you do not have SSL decryption enabled on the firewall, use the following URL instead: http://wildfire.paloaltonetworks.com/publicapi/test/elf

- **API Download:** Make a GET request to the /test resource with the file type you want to retrieve. Use the -JO option to retain the Content-Disposition filename, as shown in the following cURL command example:

  `curl -JO 'https://wildfire.paloaltonetworks.com/publicapi/test/elf'`

  The response saves the malware test file to your local system. Each time you download the test file, it has a different SHA-256 hash value.

**STEP 2 |** On the firewall web interface, select Monitor > WildFire Submissions to confirm that the file was forwarded for analysis.

It might take about five minutes for analysis results to be displayed for the file on the WildFire Submissions page. The verdict for the test file will always display as malware.

**STEP 3 |** (Optional) Verify that the files have been properly forwarded.
Email Link Analysis Enhancements

Improved WildFire analysis reports for email links that are classified as phishing by the WildFire public cloud or PAN-DB are now available on the WildFire portal, firewalls, and through the API. If you have configured your firewall to forward email links, no additional configuration is required to take advantage of the improved functionality.

Email links analyzed using a WildFire dynamic analysis virtual environment and/or PAN-DB are shown in your WildFire Analysis Report, under the Dynamic Analysis heading. You can select the virtual machines that were used to analyze a file and view the details of behaviors detected in the email link.

To enable the firewall to forward links included in emails for WildFire analysis, see Forward Files for WildFire Analysis.

• You can view the WildFire sample analysis report and verdict (malicious, grayware or benign) on the WildFire portal or the firewall.

• You can use the WildFire API to retrieve verdicts and analysis reports for email links.
Sample Removal Request

Unique samples sent to the WildFire cloud for analysis can now be deleted at the discretion of the user. This allows users who are subject to data protection policies, including those who must comply with GDPR, to permanently dispose of sample data based on their organization's retention policies. Sample data includes session / upload data and the sample file itself.

STEP 1 | Create a text file with a list of SHA256 or MD5 hashes of the samples to be deleted. Each hash must be on an individual line in the file and can include up to 100 samples.

Only files that are unique to your environment can be deleted. If files are found to be available in other public or private feeds, only the session and upload data for a given account is removed.

STEP 2 | Log in to the WildFire cloud using your Palo Alto Networks support credentials or your WildFire account.

STEP 3 | Select Settings on the menu bar.

STEP 4 | Click Choose File and select the hash list text file that you created in step 1 and then Remove Samples. You will receive a confirmation upon a successful file upload.

STEP 5 | After the samples are removed from the WildFire cloud, you will receive a confirmation email with the details of the request. This includes a list of the samples that were requested to be deleted, and the removal status of each sample. This process can take up to 7 days.
Samples that do not exist or are not unique to your environment will return statuses of Not found and Rejected, respectively.

<table>
<thead>
<tr>
<th>Hash</th>
<th>Status</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>6d2ef77b3b8b4329cb1f0eeb5e0821993a84e3cc0e50232bf51a06967c6e1c</td>
<td>Deleted</td>
<td></td>
</tr>
</tbody>
</table>
Updated WildFire Cloud Data Retention Period

Palo Alto Network's data retention policies for samples submitted to the WildFire cloud have been updated. Files sent to the WildFire cloud for processing and analysis are retained until processing takes place. Once analyzed, files categorized as benign are now retained for 14 days in case the analysis decision is reversed. As before, files determined to be malicious are retained for 10 years. Furthermore, signatures and sample reports for corresponding files, which do not include personal information, will continue to be stored indefinitely.
DEX File Analysis

The WildFire public cloud can now analyze Dalvik executable (DEX) files with malicious, benign, or grayware verdicts. Individual DEX files not forwarded by the firewall to Wildfire for analysis. Instead, DEX files can be uploaded for analysis using the WildFire API or the WildFire portal (With a WildFire subscription, you can manually and programatically submit a daily total of 1,000 files). DEX files contained within APK files are analyzed as part of the APK file analysis. As with all malicious samples, the WildFire public cloud generates and distributes a signature to firewalls to prevent future instances of the file from penetrating your network. Signatures generated by DEX file analysis are matched against DEX files passing through the firewall, as well as those contained within APK files. No additional configuration needs to be made in order to take advantage of this feature.

- The WF-500 appliance does not support DEX file analysis.

- Manually upload DEX files to the WildFire public cloud for analysis. You can then view the WildFire sample analysis report and verdict (malicious, grayware or benign) on the WildFire portal.

- Use the WildFire API to submit DEX files to the WildFire public cloud. You can continue to use the WildFire API to retrieve verdicts and analysis reports for DEX files.
Network Traffic Profiling

Network traffic profiles detect malicious traffic patterns that might otherwise be misclassified as benign, such as communications with legitimate sites used as part of a command and control mechanism. The WildFire cloud dynamic analysis environment now has a network traffic profile detection module that performs deep inspection of PCAPs produced during sample analysis. Network traffic profiles are created through PCAP analysis by looking for 10 or more networking session attributes, which in turn is used by the WildFire cloud to detect known and variants of known malware using a one-to-many profile match. No configuration changes or PAN-OS updates are required to enable network traffic profiling. All changes and updates have been made in the WildFire Cloud.

When the analysis environment identifies a malicious traffic pattern, a new behavior is shown under the Behavioral Summary section of the WildFire analysis report with the description **One or more malicious network patterns were triggered.**

### 3 Dynamic Analysis

#### 3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

#### 3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used SSL</td>
<td></td>
</tr>
<tr>
<td>SSL is a certificate-based cryptographic protocol for secure communication over the Internet. Malware often communicates over SSL to hide its traffic from network security systems, like most firewalls and IPSes, that do not offer SSL decryption.</td>
<td></td>
</tr>
<tr>
<td>Created or modified a file in the Windows system folder</td>
<td></td>
</tr>
<tr>
<td>The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.</td>
<td></td>
</tr>
<tr>
<td>Created or modified a file</td>
<td></td>
</tr>
<tr>
<td>Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.</td>
<td></td>
</tr>
<tr>
<td>Attempted to sleep for a long period</td>
<td></td>
</tr>
<tr>
<td>Malware analysis environments have a limited amount of time in which to execute code and deliver a verdict. To subvert this process, malware often delays execution, or “sleeps,” for a long period, allowing it to avoid detection.</td>
<td></td>
</tr>
<tr>
<td>One or more malicious network patterns were triggered</td>
<td></td>
</tr>
<tr>
<td>One or more malicious network patterns were triggered.</td>
<td></td>
</tr>
</tbody>
</table>
Additional Malware Test Files

Palo Alto Networks now provides two additional sample malware files to test your WildFire deployment. These new malware samples include an APK and MacOSX file and can be downloaded using a direct download link using your browser or through the WildFire API. Download one of the new sample files and verify that it gets forwarded to WildFire for analysis.

**STEP 1 |** Download one of the new malware test files. Select from either direct or API download.

- **Direct Download:**
  - If you have SSL decryption enabled on the firewall, use one of the following URLs:
    - APK—https://wildfire.paloaltonetworks.com/publicapi/test/apk
    - MacOSX—https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - If you do not have SSL decryption enabled on the firewall, use one of the following URLs instead:
    - APK—http://wildfire.paloaltonetworks.com/publicapi/test/apk
    - MacOSX—http://wildfire.paloaltonetworks.com/publicapi/test/macos
- **API Download:** Make a GET or Post request to the /test resource with the file type you want to retrieve and as well as the -JO option to use the Content-Disposition filename as provided by the server as shown in the following cURL command:
  - APK—
    ```
curl -JO 'https://wildfire.paloaltonetworks.com/publicapi/test/apk'
    
```
  - MacOSX—
    ```
curl -JO 'https://wildfire.paloaltonetworks.com/publicapi/test/macos'
    
```

The response saves the malware test file to your local system. Each time you download the test file, it has a different SHA-256 hash value.

**STEP 2 |** On the firewall web interface, select Monitor > WildFire Submissions to confirm that the file was forwarded for analysis.

It might take about five minutes for analysis results to be displayed for the file on the WildFire Submissions page. The verdict for the test file will always display as malware.

**STEP 3 |** (Optional) Verify that the files have been properly forwarded.
Dynamic Unpacking

The WildFire public cloud now unpacks and deobfuscates files that have been encoded using custom and open source file compression or packing tools. This provides improved coverage by analyzing files that might have previously dropped as a result of code obfuscation. No additional configuration is required to analyze files using dynamic unpacking; it is automatically performed based on file characteristics detected by WildFire.

Additional information about dynamic unpacking:

- WildFire analysis results for files that are decompressed using dynamic unpacking are shown under the static analysis heading of the WildFire Analysis Report. The following example shows two new behaviors associated with dynamic unpacking.

- Dynamic unpacking does not have an analysis platform number, as it uses a combination of static and dynamic analysis.
- Dynamic unpacking behaviors are listed under the Suspicious File Properties heading of the WildFire Analysis Report.
Windows 10 Analysis Environment

The WildFire public cloud can now analyze files using the Windows 10 VM, further increasing the threat prevention coverage capabilities of WildFire. No additional configuration is required to take advantage of the new VM.

This virtual analysis environment is configured using the following system attributes:

**Platform ID 66**: Windows 10 x64, Flash 22, Adobe Reader 11, and Office 2010.

*The Windows 10 VM does not support analysis of 32-bit PE files.*

*The WildFire appliance does not support the Windows 10 analysis environment.*

Files analyzed using the new VM will be shown in your WildFire Analysis Report, under the Dynamic Analysis heading. You can select the virtual machines that were used to analyze a file and view the details of behaviors detected in the file.

For more information about submitting files for analysis, refer to: Submit Files for Wildfire Analysis
Archive (RAR/7z) and ELF File Analysis

To use this feature, be sure to download and install the latest PAN-OS content release. PAN-OS Applications and Threats content release 745 enables you to specify file forwarding of archive (.rar and 7zip) and linux (ELF) file types. For more information about the update, refer to the Applications and Threat Content Release Notes.

To download the release notes, log in to the Palo Alto Networks Support Portal, click Dynamic Updates and select the release notes listed under Apps + Threats.

The WildFire public cloud can now analyze and classify linux (ELF) and archive (RAR and 7-Zip) files with malicious, benign, or grayware verdicts. As with all malicious samples, WildFire public cloud generates and distributes a signature to firewalls to prevent future instances of the file from penetrating your network. Keep in mind, the WildFire appliance does not support ELF and archive file analysis.

Archive and ELF file types are sent in their entirety to the WildFire cloud when submitted for analysis, as they are not decoded by the firewall.

The following new file types are supported for WildFire public cloud analysis:

- Archive Files:
  - RAR—Supports Roshal Archive (.rar) files.
  - 7-Zip—Supports (.7z) files.
  - The archive file verdict is determined by the highest severity verdict of the archive contents.
  - Archive files that are multi-part or password protected cannot be analyzed.
- ELF—Supports Executable and Linkable Format (.elf) files.
WildFire Analysis of Blocked Files

If you enabled WildFire forwarding on your firewall, the firewall now submits blocked files that match antivirus signatures for WildFire analysis, in addition to unknown files. This allows WildFire to extract valuable information from new malware variants. Malware signatures often match multiple variants of the same malware family, and as such, block new malware variants that the firewall has never seen before. Sending these blocked malware samples for WildFire analysis allows WildFire to analyze them for additional URLs, domain names, and IP addresses that must be blocked. Since all WildFire analysis data is also available on AutoFocus, you can now use WildFire and AutoFocus to get a more complete perspective of all threats targeting your network, including blocked threats; this improves the efficacy of your security operations, incident response, and threat analysis.

Because blocked files are now forwarded to WildFire for analysis, you now have visibility into files that the firewall has successfully blocked. On the firewall, you can now view WildFire Submissions log details for blocked files, which include the threat log entry for a file and the threat ID matched to a file (for more information, refer to Globally Unique Threat IDs). Both the firewall and the WildFire portal also provide access to the WildFire analysis report for a blocked file so you can learn about its behavior when it executed in a WildFire analysis environment.

The firewall forwards blocked files to the WildFire public cloud based on your existing WildFire forwarding settings (Objects > Security Profiles > WildFire Analysis). The firewall doesn't forward files that are blocked based on your file blocking settings.
WildFire Phishing Verdict

The new WildFire phishing verdict classifies credential phishing links found in emails separately from emailed links found to be exploits or malware. When the firewall detects a link in an email, it forwards the link to WildFire for analysis. WildFire classifies the link as phishing based on properties and behaviors the accompanying website displays and assigns the link the new phishing verdict. Phishing links are logged as WildFire Submissions to indicate that the firewall detected such a link in an email.

Firewalls with an active WildFire license that are connected to the WildFire public cloud and are configured to forward email links for analysis will automatically start receiving phishing verdicts after the upgrade to PAN-OS 8.0. Firewalls with both a WildFire license and a PAN-DB URL Filtering license can block access to phishing sites within five minutes of initial discovery.

For Firewalls in a WildFire Private Cloud Deployment:
The WildFire appliance does not support the new Phishing verdict. However, firewalls connected to a WildFire appliance that also have an active PAN-DB URL Filtering license can still benefit from phishing protection. For these firewalls, continue to step (Optional) To prevent users from inadvertently leaking corporate credentials to attackers, block access to phishing sites and block users from submitting usernames and passwords to untrusted and unsanctioned sites. to block users from accessing newly-discovered phishing sites.

STEP 1 | Check that the firewall has an active WildFire license and is connected to WildFire.

Blocking access to phishing sites requires a PAN-DB URL Filtering license, in addition to the WildFire license.

1. Select Device > Licenses to confirm that the WildFire License is active. If you are also planning to block access to phishing sites, confirm that the PAN-DB URL Filtering license is active.
2. Select Device > Setup > WildFire and confirm that the WildFire Public Cloud is set to:
   ```
   wildfire.paloaltonetworks.com
   ```
3. Alternatively, you can connect the firewall to a WildFire regional cloud in the European Union (EU) or in Japan.

STEP 2 | Verify that the firewall is enabled to forward email links for WildFire analysis.

1. Select Objects > Security Profiles > WildFire Analysis and confirm that at least one profile is configured to forward email-link or any File Types for WildFire analysis.
2. Select Policies > Security to confirm that the WildFire Analysis profile is attached to a security policy rule:
STEP 3 | Monitor phishing links.

- View links the firewall forwarded that WildFire found to be phishing links:

  Select **Monitor > WildFire Submissions**. The Verdict column displays Phishing for entries that record a phishing link. You can add the following filter to display only logs for phishing links:

  (verdict eq phishing)

- View phishing activity on the firewall ACC:

  Select **ACC > Threat Activity**, view WildFire Activity By Type and select **phishing**.

- View all phishing links WildFire has identified:

  The WildFire portal displays the total number of WildFire submissions that were found to be phishing links in the last hour and the last 24 hours:

  Select **Reports**, filter by **Verdict**, and select **Phishing** to find the analysis reports for phishing links.

  If you are submitting links to a regional WildFire cloud for analysis, instead use the WildFire EU portal or the WildFire Japan portal.

STEP 4 | Forward phishing logs as SNMP traps, syslog messages, or email notifications.

1. Select **Objects > Log Forwarding** and **Add** or modify a log forwarding profile to define the logs you want to forward.
2. **Add** a rule to the profile.
3. Set the **Log Type** to wildfire.
4. Add the **Filter** (verdict eq phishing).
5. Continue to define or update the profile, and click **OK** to save the profile when you’re done.
6. Apply the new or updated log forwarding settings to traffic:
   1. Select **Policies > Security** and **Add** or modify a security policy rule.
   2. Select **Actions** and in the Log Setting section, attach the new or updated **Log Forwarding** profile to the security policy rule.
   3. Click **OK** to save the security policy rule.

STEP 5 | (Optional) To prevent users from inadvertently leaking corporate credentials to attackers, block access to phishing sites and block users from submitting usernames and passwords to untrusted and unsanctioned sites.

1. Select **Objects > URL Filtering** and **Add** or modify a URL Filtering profile.
2. Select **Categories** and filter the list of URL categories to find the phishing category.
3. Set the **Site Access** for phishing websites to **Block** to prevent users from accessing sites that aim to steal usernames and passwords.
4. Enable the new **Credential Phishing Prevention** feature to stop users from submitting credentials to untrusted sites, without blocking their access to these sites.
5. Apply the new or updated URL Filtering profile to traffic:
1. Select Policies > Security and Add or modify a security policy rule.
2. Select Actions and in the Profile Setting section, set the Profile Type to profiles.
3. Attach the new or updated URL Filtering profile to the security policy rule.
4. Click OK to save the security policy rule.
WildFire Features in PAN-OS 9.0

The following topics describe how to configure and operate the latest updates to the WildFire PAN-OS 9.0 release:

> Increased WildFire File Forwarding Capacity
> WildFire Appliance Archive Support

For additional information about this release, including a complete feature listing, known issues, and changes to default behavior, refer to the PAN-OS 9.0 Release Information.
Increased WildFire File Forwarding Capacity

The maximum and default WildFire file forwarding sizes and rates are increased in PAN-OS® 9.0 to provide optimal visibility and detection. Based on Palo Alto Network’s data analytics, the new default capacities protect against the majority of threats, and is a best practice to use the new default values.

The forwarding capacities for Traps, Aperture, and Magnifier have not changed. For additional information about the file forwarding capacity of these products and other public/API integrations, refer to the product documentation.

<table>
<thead>
<tr>
<th>File Type</th>
<th>PAN-OS 9.0 Default File Forwarding Sizes</th>
<th>PAN-OS 9.0 Size Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>pe</td>
<td>16MB</td>
<td>1-50MB</td>
</tr>
<tr>
<td>apk</td>
<td>10MB</td>
<td>1-50MB</td>
</tr>
<tr>
<td>pdf</td>
<td>3,072KB</td>
<td>100-51,200KB</td>
</tr>
<tr>
<td>ms-office</td>
<td>16,384KB</td>
<td>200-51,200KB</td>
</tr>
<tr>
<td>jar</td>
<td>5MB</td>
<td>1-20MB</td>
</tr>
<tr>
<td>flash</td>
<td>5MB</td>
<td>1-10MB</td>
</tr>
<tr>
<td>MacOSX</td>
<td>10MB</td>
<td>1-50MB</td>
</tr>
<tr>
<td>archive</td>
<td>50MB</td>
<td>1-50MB</td>
</tr>
<tr>
<td>linux</td>
<td>50MB</td>
<td>1-50MB</td>
</tr>
</tbody>
</table>

The default forwarding values might change over time based on the current version of PAN-OS or the content release version. To view the file size ranges and defaults:

- **Web Interface**—From the Device > Setup > WildFire > General Settings window, select and clear a Size Limit field, and then press enter to update the field.
- **CLI**—From a terminal emulator, connect to the firewall CLI and issue the following command: `show wildfire file-size-limits`.

**STEP 1** | Log in to the firewall and verify the WildFire file forwarding size limits.
As a WildFire best practice, Palo Alto Networks recommends using the default file forwarding sizes. These values are designed to include the vast majority of malware that are likely to be encountered in real-world scenarios. Very large files that are beyond the size limits are excluded.

STEP 2 | Commit your configuration updates.

STEP 3 | Verify that the firewall is forwarding files to the WildFire public cloud.
WildFire Appliance Archive Support

The WildFire appliance can now analyze and classify archive (RAR and 7-Zip) files with malicious, benign, or grayware verdicts. Previously this feature was only present in the WildFire cloud. This analysis capability has now been expanded to include WildFire appliances running PAN-OS 9.0 and later.

- When any file contained within an archive is determined to be malicious, the archive file is considered malicious by WildFire.
- Archive files that are multi-part or password protected cannot be analyzed.

The WildFire appliance is capable of analyzing the following archive file types:

- RAR—Supports Roshal Archive (.rar) files.
- 7-Zip—Supports (.7z) files.

To forward archive files for analysis, the WildFire Analysis Profile on the firewall must be configured to forward the archive file type or Any unknown files to the WildFire private cloud.

1. Enable file type forwarding.
   1. Select Objects > Security Profiles > WildFire Analysis and Add or modify a profile to define traffic to forward for WildFire analysis.
   2. Add or modify a profile rule, select file type, and set the rule to forward the new Any file type. You can also specify the archive file type if you want to forward only archives.

   Profile rules with the file type set to Any forward all file types for WildFire analysis.

   3. Select Destination and set the profile rule to forward the files to the private-cloud.
   4. Click OK to save the new or modified WildFire Analysis profile.

2. Attach the WildFire Analysis profile to a security policy rule—traffic matched to the policy rule is forwarded for WildFire Analysis.
   1. Select Policies > Security and Add or modify a security policy rule.
   2. Select Actions and set the Profile Type to Profiles.
   3. Select the newly-created WildFire Analysis profile.
   4. Click OK to save the security policy rule.

   For detailed steps to configure a WildFire Analysis profile and to attach the profile to a security policy rule, see Forward Files for WildFire Analysis.

3. Select Monitor > WildFire Submissions to find WildFire verdicts and analysis reports for archive files that have been submitted by the firewall.
WildFire Features in PAN-OS 8.1

The following topics describe how to configure and operate the latest updates to the WildFire PAN-OS 8.1 release:

> WildFire Appliance-to-Appliance Encryption

For additional information about this release, including a complete feature listing, known issues, and changes to default behavior, refer to the PAN-OS 8.1 Release Information.
WildFire Appliance-to-Appliance Encryption

You can now encrypt WildFire® communications between appliances deployed in a cluster. Prior to 8.1 and by default, WildFire appliances send data using cleartext when communicating with management appliances as well as WildFire cluster peers. You can use either predefined or custom certificates to authenticate connections between WildFire appliance peers using the IKE/IPsec protocol. The predefined certificates meet current FIPS/CC/UACPL-approved certification and compliance requirements. If you want to use custom certificates instead, you must select a FIPS/CC/UACPL-compliant certificate or you will not be able to import the certificate.

You can configure WildFire appliance-to-appliance encryption locally using the WildFire CLI or centrally through Panorama. Keep in mind, all WildFire appliances within a given cluster must run a version of PAN-OS that supports encrypted communications.

If the WildFire appliances in your cluster uses FIPS/CC mode, encryption is automatically enabled using predefined certificates.

Before configuring WildFire appliance-to-appliance encryption, be sure to review your existing WildFire secure communications configuration. If you previously configured the WildFire appliance and the firewall for secure communications using a custom certificate, you can use that custom certificate and the requisite DNS name for configuring secure communications between WildFire appliances.

It is imperative that you use the correct, matching DNS name in the register firewall to: field in Panorama. Failure to do so will prevent appliance-to-appliance encryption from working as intended.

The following tables describe the high-level tasks involved in configuring WildFire appliance-to-appliance encryption. For detailed instructions on these tasks, refer to the WildFire Administration Guide for the full installation procedure.

Table 1: WildFire Appliance-to-Appliance Encryption Installation Tasks Using Panorama

<table>
<thead>
<tr>
<th>Configuration Using Custom Certificates through Panorama</th>
<th>Configuration Using Predefined Certificates through Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. In the Panorama &gt; Managed WildFire Clusters &gt; WildFire Cluster page:</td>
<td>1. In the Panorama &gt; Managed WildFire Clusters &gt; WildFire Cluster page:</td>
</tr>
<tr>
<td>• Configure the DNS name used for authentication found in the custom certificate.</td>
<td>• Enable Secure Cluster Communication.</td>
</tr>
<tr>
<td>• Enable customize secure server communication and configure the SSL/TLS Service Profile and certificate profile to define the custom certificate for encrypted communication between WildFire peers.</td>
<td>• Enable HA Traffic Encryption.</td>
</tr>
<tr>
<td>• Import or generate a custom certificate. If you are generating a custom certificate, be sure to use the same DNS stated in the certificate.</td>
<td></td>
</tr>
</tbody>
</table>
Table 2: WildFire Appliance-to-Appliance Encryption Installation Tasks Using the CLI

1. In the Panorama > Managed WildFire Clusters > WildFire Cluster page:
   - Configure the DNS name used for authentication found in the custom certificate.
   - Enable customize secure server communication and configure the SSL/TLS Service Profile and certificate profile to define the custom certificate for encrypted communication between WildFire peers.
   - Import or generate a custom certificate. If you are generating a custom certificate, be sure to use the same DNS stated in the certificate.

2. Configure the firewall secure communication settings to use the custom certificate. This enables the WildFire cluster to communicate with the firewall using encryption.

3. From the WildFire appliance cluster active-controller CLI:
   - Make sure you configure the appliance to use custom certificates only, so that it does not use the predefined certificate.
   - Enable secure cluster communication.
<table>
<thead>
<tr>
<th>Configuration Using Custom Certificates through the WildFire CLI</th>
<th>Configuration Using Predefined Certificates through the CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enable HA traffic encryption.</td>
<td></td>
</tr>
</tbody>
</table>
**WildFire Features in PAN-OS 8.0**

The following topics describe how to configure and operate the latest updates to the WildFire PAN-OS 8.0 release:

- Panorama Centralized Management for WildFire Appliances
- WildFire Appliance Clusters
- Preferred Analysis for Documents or Executables
- Verdict Changes
- Verdict Checks with the WildFire Global Cloud

For additional information about this release, including a complete feature listing, known issues, and changes to default behavior, refer to the PAN-OS 8.0 Release Information.
Panorama Centralized Management for WildFire Appliances

Beginning with release 8.0.1, you can now manage WildFire appliances and WildFire appliance clusters with Panorama. Panorama can manage up to 200 WildFire appliances as WildFire appliance cluster nodes, standalone WF-500 appliances, or a combination of cluster nodes and standalone appliances. Panorama can manage a maximum of ten WildFire appliance clusters.

Compared to managing WildFire appliances and appliance clusters individually using the local CLI, using Panorama provides centralized management and monitoring of multiple appliances and appliance clusters. Centralized management enables you to push common configurations, configuration updates, and software upgrades to all or a subset of the managed WildFire appliances, which makes it easy to ensure that WildFire appliances and appliance clusters have consistent configurations.
WildFire Appliance Clusters

Beginning with this release, you can now configure and manage up to twenty WildFire appliances as a WildFire appliance cluster on a single network. This is especially useful in environments where you cannot use the WildFire public cloud. WildFire appliance clusters support larger firewall deployments on a single network than a standalone WildFire appliance supports. Additionally, clusters provide fault tolerance and a single signature package that is distributed to all firewalls that are connected to the cluster.

You can manage clusters locally, using the WildFire appliance CLI, or centrally, from a Panorama M-Series or virtual appliance. A WildFire cluster environment includes:

- From 2 to 20 WildFire appliances that you want to group and manage as a cluster. At a minimum, a cluster must have two WildFire appliances configured in a high-availability (HA) pair.
- Firewalls that connect to the cluster for traffic analysis and signature generation.
- (Optional) One or two Panorama appliances for centralized cluster management if you choose not to manage the cluster locally. To provide HA, use two Panorama appliances configured as an HA pair.

At a minimum, a cluster must have two WildFire appliances configured as a high-availability (HA) pair. WildFire appliances that you add to a WildFire appliance cluster become cluster nodes.

STEP 1 | Create a WildFire appliance cluster and add WildFire appliances to the cluster.
Configure the cluster member nodes and roles, configure HA, and verify the configuration. You can Configure a Cluster and Add Nodes Locally or Configure a Cluster and Add Nodes on Panorama.

STEP 2 | Configure basic WildFire appliance cluster settings.
Configure the connection to the WildFire public cloud, data retention policies, signature generation, the preferred analysis environment, DNS settings, and so on. You can Configure Basic Cluster Settings Locally or Configure Basic Cluster Settings on Panorama.

STEP 3 | Remove a WildFire appliance from a cluster.
Safely remove a node from a WildFire appliance cluster. You can Remove a Node from a Cluster Locally, however, removing a node from a cluster using Panorama is not supported.

With the introduction of managing WildFire appliance clusters on Panorama, you can also manage individual standalone WildFire appliances on Panorama.
Preferred Analysis for Documents or Executables

A single virtual machine (VM) image runs on the WildFire appliance; when you Upgrade the WildFire Appliance Software, you can choose for the WildFire appliance to use the VM image that most reflects your network environment. Each available VM image represents a single operating system and supports several different analysis environments based on that operating system. You can now dedicate all analysis environments to support certain file types: either documents (Microsoft Office files and PDFs) or portable executables (PEs). This feature is helpful if you are using the WildFire appliance to analyze specific file types; for example, if you’ve deployed a WildFire hybrid cloud to analyze documents locally and PEs in the WildFire global cloud. In this case, you could dedicate all analysis environments to documents. Previously, analysis environments were statically allocated and the resources available for document and executable analysis were evenly divided; you could not adjust the allocation of analysis resources even when the WildFire appliance was configured to analyze only one type of file.

STEP 1 | Confirm that the firewall is configured to forward only the file type to which you want to dedicate WildFire analysis environments.

1. In the firewall web interface, select Objects > Security Profiles > WildFire Analysis.
2. Confirm that the WildFire Analysis profile set to forward files to the WildFire private cloud for analysis is configured to forward documents or executables.
3. Select Policies > Security and confirm that the WildFire Analysis profile is attached to a security policy rule. Traffic the rule allows is forwarded to the WildFire appliance for private cloud analysis based on the WildFire Analysis profile settings.

STEP 2 | Allocate WildFire appliance resources to analyze either documents or executables.

Use the following CLI command:

```bash
admin@WF-500# set deviceconfig setting wildfire preferred-analysis-environment documents | executables | default
```

and choose from one of the following options:

- **documents**—Dedicate analysis resources to concurrently analyze 25 documents, 1 PE, and 2 email links.
- **executables**—Dedicate analysis resources to concurrently analyze 25 PEs, 1 documents, and 2 email links.
- **default**—The appliance concurrently analyzes 16 documents, 10 portable executables (PE), and 2 email links.

STEP 3 | Confirm that all WildFire appliances processes are running.

```bash
admin@WF-500> show system software status
```
Verdict Changes

You can now use the WildFire appliance to change a verdict for a sample. Verdict changes apply only to those samples submitted to the WildFire appliance, and the verdict for the same sample remains unchanged in the WildFire global cloud.

The WildFire private cloud content package is updated to reflect any verdict changes that you make (on the firewall, select Device > Dynamic Updates > WF-Private to enable WildFire private cloud content updates). When you change a sample verdict to malicious, the WildFire appliance generates a new signature to detect the malware and adds that signature to the WildFire private cloud content package. When you change a sample verdict to benign, the WildFire appliance removes the signature from the WildFire private cloud content package.

- Change a sample verdict:

```
admin@WF-500# submit wildfire local-verdict-change hash <sha256 hash> comment <comment> verdict <verdict>
```

- **hash**—Provide the SHA-256 hash of the file for which you want to change the verdict.
- **verdict**—Enter the new file verdict: 0 indicates a benign sample; 1 indicates malware; 2 indicates grayware, and 4 indicates phishing.
- **comment**—Include a comment to describe the verdict change.

- See samples with changed verdicts:

```
admin@WF-500# show wildfire global local-verdict-change all | <sha256 hash>
```

- **all**—See all samples with changed verdicts. The output includes the original verdict and the new verdict.
- **<sha256 hash>**—Check a specific sample for a changed verdict. The output includes the original verdict and the new verdict.

- Use the API to change a sample verdict:

Make a request to the new resource submit/local-verdict-change and include the API key, the file hash, the new verdict you want to apply to the sample, and a descriptive comment of the change:

```
curl -X POST -H "Content-Type: multipart/form-data" -F "apikey=apikey" -F "hash=sha-256-hash" -F "verdict=0" -F "comment=comment-for-verdict-change" "https://wf-500/publicapi/submit/local-verdict-change"
```

Use the following parameters when changing a WildFire appliance verdict for a file:

- **apikey**—Enter your API key.
- **hash**—Provide the SHA-256 hash of the file for which you want to change the verdict.
- **verdict**—Enter the new file verdict: 0 indicates a benign sample, 1 indicates malware, 2 indicates grayware, and 4 indicates phishing.
- **comment**—Include a comment to describe the verdict change.

The following XML response verifies a successful verdict change. Example:
Use the API to see samples with changed verdicts:

Make a request to the new resource `get/verdicts/changed` and include the API key and a start date for the query. Samples with changed verdicts from the specified start date to the present date is shown in this list:

```
curl -F "apikey=apikey" -F "date=YYYY-MM-DD" "https://wf-500/publicapi/get/verdicts/changed"
```

The `verdict` element value can be one of the following:

- 0—benign
- 1—malware
- 2—grayware
- 4—phishing

The XML response contains the WildFire verdict along with the related hash values for each sample with changed verdicts within the specified time-frame. Example:

```
<wildfire>
  <get-verdict-info>
    <sha256>afe6b95ad95bc689c356f34ec8d9094c495e4af57c932ac413b65ef132063acc</sha256>
    <verdict>1</verdict>
    <md5>0e4e3c2d84a9bc726a50b3c91346fbb1</md5>
  </get-verdict-info>
  ...........
  <get-verdict-info>
    <sha256>9739eb4207fe251d40f05187cbfd16081f97b246ebcc6010660244a84a9391b0</sha256>
    <verdict>2</verdict>
    <md5>481e625e50211e5eaf6ed8f54f8cf83</md5>
  </get-verdict-info>
</wildfire>
```
The WildFire appliance can now leverage WildFire global cloud intelligence to deliver quick verdicts for known samples. This allows the WildFire appliance to dedicate analysis resources to samples that are truly unknown to both your private network and the global WildFire community. Before analyzing a sample locally, the WildFire appliance checks if the WildFire global cloud has already analyzed the sample (the WildFire appliance sends only the sample hash to the WildFire global cloud—it does not send the raw file or any additional sample data). If the sample is known to the WildFire global cloud, the WildFire appliance retrieves the sample verdict and analysis report and delivers them promptly to the firewall that detected the sample. If the sample is unknown to the WildFire global cloud, the WildFire appliance analyzes the sample locally. In either case, the WildFire appliance locally generates a signature to detect the malware, and delivers the signature to the firewall as part of the WildFire private cloud content update.

The WildFire appliance continues to periodically synchronize verdicts and analysis reports for locally-analyzed samples so that they match the verdicts and analysis reports the WildFire global cloud provides—this ensures that analysis information for locally-analyzed samples stays up-to-date with worldwide WildFire submissions and the latest threat intelligence. In cases where the WildFire global cloud and the WildFire appliance record a different verdict for a sample, the WildFire global cloud verdict takes precedence and changes the local verdict.

The following CLI command enables the WildFire appliance to perform verdict lookups and synchronize verdicts with the WildFire global cloud. This feature is disabled by default; set the command to `yes` to enable the feature.

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence cloud-query [yes | no]
```

Another new WildFire appliance feature supports **Verdict Changes for locally-analyzed samples**. If you change the verdict for a sample, the new verdict continues to apply to the locally-submitted sample, even if the WildFire global cloud has recorded a different verdict for the same sample.
WildFire Release History

The following section lists past major releases of WildFire and the associated documentation set for that version.

> WildFire Release Listing
## WildFire Release Listing

<table>
<thead>
<tr>
<th>Release Version</th>
<th>Release Notes</th>
<th>Documentation List</th>
</tr>
</thead>
</table>
| WildFire 8.0    | PAN-OS 8.0 Release Notes | • WildFire 8.0 Administration Guide  
                   |                | • WildFire 8.0 API Reference Guide  
                   |                | • WildFire 8.0 New Features Guide  
                   |                | • WildFire WF-500 Hardware Reference Guide |
| WildFire 7.1    | PAN-OS 7.1 Release Notes | • WildFire 7.1 Administration Guide  
                   |                | • WildFire 7.1 API Reference Guide  
                   |                | • WildFire 7.1 New Features Guide  
                   |                | • WildFire WF-500 Hardware Reference Guide |
| WildFire 7.0    | EoL. Documentation is no longer updated. Refer to EoL Software Documentation page to access reference materials. | |
| WildFire 6.1    | PAN-OS 6.1 Release Notes | • WildFire 6.1 Administration Guide  
                   |                | • WildFire 6.1 New Features Guide  
                   |                | • WildFire WF-500 Hardware Reference Guide |
| WildFire 6.0    | EoL. Documentation is no longer updated. Refer to EoL Software Documentation page to access reference materials. | |