Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes how to configure your Palo Alto Networks firewalls to submit samples to the WildFire cloud and how to manage a WF-500 appliance for use in private cloud or hybrid cloud deployments:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://docs.paloaltonetworks.com or search the documentation.

- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.

- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.

- For the most current PAN-OS and WildFire 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
# Table of Contents

**WildFire Overview** .......................................................... 5  
About WildFire. ................................................................. 6  
WildFire Concepts. ............................................................. 7  
WildFire Deployments ......................................................... 11  
WildFire File Type Support .................................................. 13  
WildFire Subscription ........................................................ 14  
Get Started with WildFire .................................................... 15

**Set Up and Manage a WF-500 Appliance** .......................... 19  
About the WF-500 Appliance ................................................. 20  
Configure the WF-500 Appliance ........................................... 21  
Set Up the WF-500 Appliance VM Interface .......................... 27  
  Virtual Machine Interface Overview .................................. 27  
  Configure the VM Interface on the WF-500 Appliance .......... 28  
  Connect the Firewall to the WF-500 Appliance VM Interface . 29  
Enable WF-500 Appliance Analysis Features ....................... 31  
  Set Up WF-500 Appliance Content Updates ......................... 31  
  Enable Local Signature and URL Category Generation .......... 33  
Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud ........................................... 35  
Upgrade a WF-500 Appliance ............................................... 36

**Submit Files for WildFire Analysis** ................................. 39  
WildFire Best Practices ....................................................... 40  
Forward Files for WildFire Analysis ..................................... 42  
Forward Decrypted SSL Traffic for WildFire Analysis .......... 46  
Verify WildFire Submissions ............................................... 47  
  Test a Sample Malware File ............................................ 47  
  Verify File Forwarding .................................................. 47  
Manually Upload Files to the WildFire Portal ....................... 52  
Submit Malware or Reports from the WF-500 Appliance .......... 53  
Firewall File Forwarding Capacity by Platform ..................... 54

**Monitor WildFire Activity** ............................................... 55  
About WildFire Logs and Reporting ..................................... 56  
Use the Firewall to Monitor Malware .................................. 57  
  Configure WildFire Submissions Log Settings ................. 57  
  Monitor WildFire Submissions and Analysis Reports ........ 59  
  Set Up Alerts for Malware ............................................. 61  
Use the WildFire Portal to Monitor Malware ......................... 63  
  Configure WildFire Portal Settings ................................ 63
## Table of Contents

Add WildFire Portal Users ................................................................. 64  
View Reports on the WildFire Portal ................................................. 65  
WildFire Analysis Reports—Close Up .............................................. 66  
WildFire Example ........................................................................... 69  

Use the WildFire API ....................................................................... 75  

Use the WF-500 Appliance CLI ....................................................... 77  
WF-500 Appliance Software CLI Concepts ....................................... 78  
WF-500 Appliance Software CLI Structure ...................................... 78  
WF-500 Appliance Software CLI Command Conventions .................. 78  
WF-500 Appliance CLI Command Messages .................................... 79  
WF-500 Appliance Command Option Symbols .................................. 80  
WF-500 Appliance Privilege Levels ............................................... 81  
WildFire CLI Command Modes ...................................................... 82  
WF-500 Appliance CLI Configuration Mode ................................. 82  
WF-500 Appliance CLI Operational Mode ..................................... 86  
Access the WF-500 Appliance CLI ................................................. 87  

Use the WF-500 Appliance CLI ....................................................... 88  
Access WF-500 Appliance Operational and Configuration Modes ...... 88  
Display WF-500 Appliance Software CLI Command Options .......... 88  
Restrict WF-500 Appliance CLI Command Output ............................ 89  
Set the Output Format for WF-500 Appliance Configuration Commands ............................................. 90  
WF-500 Appliance Configuration Mode Command Reference .......... 91  
set deviceconfig setting wildfire ................................................. 91  
set deviceconfig system update-schedule ..................................... 93  
set deviceconfig system vm-interface ......................................... 94  
WF-500 Appliance Operational Mode Command Reference .............. 96  
create wildfire api-key ................................................................. 96  
delete wildfire api-key ............................................................... 97  
delete wildfire-metadata ............................................................ 98  
edit wildfire api-key ................................................................. 99  
load wildfire api-key ................................................................. 100  
request system raid ................................................................. 101  
request system wildfire-vm-image ............................................. 102  
request wf-content ................................................................. 103  
save wildfire api-key .............................................................. 104  
set wildfire portal-admin .......................................................... 105  
show system raid ................................................................. 106  
show wildfire ................................................................. 107  
test wildfire registration .......................................................... 111
WildFire® Overview

WildFire® provides detection and prevention of zero-day malware using a combination of malware sandboxing and signature-based detection and blocking of malware. WildFire extends the capabilities of Palo Alto Networks next-generation firewalls to identify and block targeted and unknown malware.

▲ About WildFire
▲ WildFire Concepts
▲ WildFire Deployments
▲ WildFire File Type Support
▲ WildFire Subscription
▲ Get Started with WildFire
About WildFire

The WildFire Virtual Environment identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block the malware. When a Palo Alto Networks firewall detects an unknown sample (a file or a link included in an email), the firewall can automatically forward the sample for WildFire analysis. Based on the properties, behaviors, and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire determines the sample to be benign, grayware, or malicious. WildFire then generates signatures to recognize the newly-discovered malware, and makes the latest signatures globally available every five minutes. All Palo Alto Networks firewalls can then compare incoming samples against these signatures to automatically block the malware first detected by a single firewall.

To learn more about WildFire, or to get started with WildFire now, see the following topics:

- Review WildFire Concepts to learn more about the types of samples you can submit for WildFire analysis, WildFire verdicts, and WildFire signatures.
- Learn more about WildFire Deployments deployments you can set up with the firewall. You can submit samples you would like to have analyzed to a Palo Alto Networks-hosted WildFire cloud, a locally-hosted WildFire private cloud, or you can use a hybrid cloud, where the firewall submits certain samples to the public cloud and certain samples to a private cloud.
- Get Started with WildFire to define the samples that you want to submit for analysis, and to begin submitted samples to a WildFire cloud.
WildFire Concepts

▲ Samples
▲ Firewall Forwarding
▲ Session Information Sharing
▲ Virtual Environment
▲ Verdicts
▲ File Analysis
▲ Email Link Analysis
▲ Compressed and Encoded File Analysis
▲ WildFire Signatures

Samples

Samples are all file types and email links the firewall forwards for WildFire analysis. See Email Link Analysis and Email Link Analysis for details on the file types and links that a firewall can submit for WildFire analysis.

Firewall Forwarding

The firewall forwards unknown samples for WildFire analysis based on the configured WildFire Analysis profile settings (Objects > Security Profiles > WildFire Analysis). In addition to detecting links included in emails, files that are attached to emails, and browser-based file downloads, the firewall leverages Palo Alto Networks App-ID feature to detect file transfers within applications. For samples that the firewall detects, the firewall checks the sample hash against WildFire signatures to determine if WildFire has previously analyzed the sample. If the sample is identified as malware, it is blocked. If the sample remains unknown after comparing it against existing WildFire signatures, the firewall forwards the sample for WildFire analysis.

By default, the firewall also forwards information about the session in which an unknown sample was detected. To manage the session information that the firewall forwards, select Device > Setup > WildFire and edit Session Information Settings.

Session Information Sharing

In addition to forwarding unknown samples for analysis, the firewall also forwards information about the unknown sample's network session. Palo Alto Networks uses session information to learn more about the context of the suspicious network event, indicators of compromise related to the malware, affected hosts and clients, and applications used to deliver the malware.
The firewall is enabled to forward session information by default; however, you can adjust the default settings and choose what type of session information the firewall forwards to WildFire. On the firewall, select Device > Setup > WildFire and select or clear the following Session Information Settings:

- **Source IP**—Forward the source IP address that sent the unknown file.
- **Source Port**—Forward the source port that sent the unknown file.
- **Destination IP**—Forward the destination IP address for the unknown file.
- **Destination Port**—Forward the destination port for the unknown file.
- **Virtual System**—Forward the virtual system that detected the unknown file.
- **Application**—Forward the user application that transmitted the unknown file.
- **User**—Forward the targeted user.
- **URL**—Forward the URL associated with the unknown file.
- **Filename**—Forward the name of the unknown file.
- **Email sender**—Forward the sender of an unknown email link (the name of the email sender also appears in WildFire logs and reports).
- **Email recipient**—Forward the recipient of an unknown email link (the name of the email recipient also appears in WildFire logs and reports).
- **Email subject**—Forward the subject of an unknown email link (the email subject also appears in WildFire logs and reports).

**Virtual Environment**

Multiple virtual machines run in the WildFire public cloud to represent a variety of operating systems and applications. WildFire executes samples in a virtual environment and observes sample behavior for signs of malicious activities, such as changes to browser security settings, injection of code into other processes, modification of files in the Windows system folder, or attempts by the sample to access malicious domains. The WildFire public cloud also analyzes files across application versions in order to identify malware intended to uniquely target specific versions of client applications (the WildFire private cloud does not support multi-version analysis, and does not analyze application-specific files are analyzed across several versions of the application). For links that the firewall extracts from email messages and forwards to WildFire, WildFire visits the links to determine if the corresponding web page hosts any exploits. When WildFire completes analysis, it generates a detailed forensics report that summarizes sample behaviors and assigns a verdict of malware, benign, or grayware to the sample.

WildFire runs virtual environments with each of the following operating systems:

- Microsoft Windows XP 32-bit
- Microsoft Windows 7 32-bit (Supported as an option for WF-500 appliance only)
- Microsoft Windows 7 64-bit
- Microsoft Windows 10 64-bit (WildFire Cloud Analysis only)
- Android (WildFire Cloud Analysis only)
- Linux (WildFire Cloud Analysis only)
Verdicts

WildFire delivers verdicts to identify samples it analyzes as safe, malicious, or unwanted (grayware is considered obtrusive but not malicious):

- **Benign**—The sample is safe and does not exhibit malicious behavior.
- **Grayware**—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).
- **Malicious**—The sample is malware and poses a security threat. Malware can include viruses, worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For files identified as malware, WildFire generates and distributes a signature to prevent against future exposure to the threat.

File Analysis

A Palo Alto Networks firewall configured with a WildFire analysis profile forwards samples for WildFire analysis based on file type (including email links). Additionally, the firewall decodes files that have been encoded or compressed up to four times (such as files in ZIP format); if the decoded file matches WildFire Analysis profile criteria, the firewall forwards the decoded file for WildFire analysis.

While the firewall can forward all the file types listed below, WildFire analysis support can vary depending on the WildFire cloud to which you are submitted samples. Review WildFire File Type Support to learn more.

**File Types Supported for WildFire Forwarding:**

- **apk**—Android Application Package (APK) files. APK files are not supported for WildFire private cloud analysis using a WF-500 appliance.
- **flash**—Adobe Flash applets and Flash content embedded in web pages.
- **jar**—Java applets (JAR/class files types).
- **ms-office**—Microsoft Office files, including documents (DOC, DOCX, RTF), workbooks (XLS, XLSX), and PowerPoint (PPT, PPTX) presentations, and Office Open XML (OOXML) 2007+ documents.
- **pe**—Portable Executable (PE) files. PEs include executable files, object code, DLLs, and FON (fonts). A subscription is not required to forward PE files for WildFire analysis, but is required for all other supported file types.
- **pdf**—Portable Document Format (PDF) files.
- **MacOSX**—Mach-O, DMG, and PKG files are supported with content version 599. You can also manually or programmatically submit all Mac OS X supported file types for analysis (including application bundles, for which the firewall does not support automatic forwarding).
- **email-link**—HTTP/HTTPS links contained in SMTP and POP3 email messages. See Email Link Analysis.
- **archive**—Roshal Archive (RAR) and 7-Zip (7z) archive files. Password-protected and multi-volume archives are that are split into several smaller files cannot be submitted for analysis.
Email Link Analysis

A Palo Alto Networks firewall can extract HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links for WildFire analysis. The firewall only extracts links and associated session information (sender, recipient, and subject) from email messages; it does not receive, store, forward, or view the email message.

WildFire visits submitted links to determine if the corresponding web page hosts any exploits. A link that WildFire finds to be malicious is:

- Recorded on the firewall as a WildFire Submissions log entry. The WildFire analysis report that details the behavior and activity observed for the link is available for each WildFire Submissions log entry. The log entry also includes the email header information—email sender, recipient, and subject—so that you can identify the message and delete it from the mail server, or mitigate the threat if the email has been delivered or opened.
- Added to PAN-DB and the URL is categorized as malware.

The firewall forwards email links in batches of 100 email links or every two minutes (depending on which limit is hit first). Each batch upload to WildFire counts as one upload toward the upload per-minute capacity for the given firewall platform (Firewall File Forwarding Capacity by Platform).

If a link included in an email corresponds to a file download instead of a URL, the firewall forwards the file only if the corresponding file type is enabled for WildFire analysis.

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

Compressed and Encoded File Analysis

By default, the firewall decodes files that have been encoded or compressed up to four times, including files that have been compressed using the ZIP format. The firewall then inspects and enforces policy on the decoded file; if the file is unknown, the firewall forwards the decoded file for WildFire analysis.

WildFire Signatures

WildFire can discover zero-day malware in web traffic (HTTP/HTTPS), email protocols (SMTP, IMAP, and POP), and FTP traffic and can quickly generate signatures to identify and protect against future infections from the malware it discovers. WildFire will automatically generate a signature based on the malware payload of the sample and tests it for accuracy and safety. Because malware evolves rapidly, the signatures that WildFire generates address multiple variants of the malware. WildFire generates and makes new signatures available every five minutes. Firewalls with an active WildFire license can retrieve the latest signatures every five minutes. If you do not have a WildFire subscription, signatures are made available within 24-48 hours as part of the antivirus update for firewalls with an active Threat Prevention license.

As soon as the firewall downloads and installs the new signature, the firewall blocks files that contain that malware (or a variant of the malware).
WildFire Deployments

You can set up a Palo Alto Networks firewall to submit unknown samples to the Palo Alto Networks-hosted WildFire global cloud, to a locally-hosted WildFire private cloud, or you can enable the firewall to forward certain samples to a WildFire global cloud and certain samples to a WildFire private cloud:

- **WildFire Global Cloud**
- **WildFire Private Cloud**
- **WildFire Hybrid Cloud**

### WildFire Global Cloud

A Palo Alto Networks firewall with can forward unknown files and email links to the WildFire global cloud or to one of three WildFire regional clouds that Palo Alto Networks owns and maintains. Choose the WildFire cloud to which you want to submit samples for analysis based on your location and your organization’s needs:

- **WildFire Global Cloud**
  
  The WildFire global cloud is a public cloud environment hosted in the United States.

  Use the following URL to submit files to the WildFire global cloud for analysis and to access the WildFire global portal: wildfire.paloaltonetworks.com.

- **WildFire EU Cloud**

  The WildFire EU cloud is a regional public cloud environment hosted in The Netherlands. It is designed to adhere to European Union (EU) data privacy regulations and samples submitted to the WildFire Europe cloud remain within EU borders.

  Use the following URL to submit files to the WildFire Europe cloud for analysis and to access the WildFire Europe cloud portal: eu.wildfire.paloaltonetworks.com.

- **WildFire Japan Cloud**

  The WildFire Japan cloud is a regional public cloud environment hosted in Japan.

  Use the following URL to submit files to the WildFire Japan cloud for analysis and to access the WildFire Japan cloud portal: jp.wildfire.paloaltonetworks.com.

- **WildFire Singapore Cloud**

  The WildFire Singapore cloud is a regional public cloud environment hosted in Singapore.

  Use the following URL to submit files to the WildFire Singapore cloud for analysis and to access the WildFire Singapore cloud portal: sg.wildfire.paloaltonetworks.com.

Each WildFire cloud—global and regional—analyzes samples and generates malware signatures independently of the other WildFire clouds. WildFire signatures are then shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location the malware was first detected. Review WildFire File Type Support to learn more about the file types that each cloud analyzes. If you have a WF-500 appliance, you can enable a WildFire Hybrid Cloud deployment, where the firewall can forward certain files to a WildFire public cloud, and other files to a WildFire private cloud for local analysis.
WildFire Private Cloud

In a Palo Alto Networks private cloud deployment, Palo Alto Networks firewalls forward files to a WF-500 appliance on your corporate network that is being used to host a private cloud analysis location. A WildFire private cloud can receive and analyze files from up to 100 Palo Alto Networks firewalls.

Because the WildFire private cloud is a local sandbox, benign and grayware files it analyzes never leave your network. By default, the private cloud also does not send discovered malware outside of your network; however, you can choose to automatically forward malware to the WildFire public cloud for signature generation and distribution. In this case, the WildFire public cloud re-analyzes the sample, generates a signature to identify the sample, and distributes the signature to all Palo Alto Networks firewalls with Threat Prevention and WildFire licenses.

If you do not want the WildFire private cloud to forward even malicious samples outside of your network, you can:

- Enable the WF-500 appliance to forward the malware report (and not the sample itself) to the WildFire public cloud. WildFire reports provide statistical information that helps Palo Alto Networks assess the pervasiveness and propagation of the malware. For more details, see Submit Malware or Reports from the WF-500 Appliance.
- Manually Upload Files to the WildFire Portal (instead of automatically forwarding all malware) or Use the WildFire API to submit files to the WildFire public cloud.

You can also Enable Local Signature and URL Category Generation on the WF-500 appliance. Signatures the WF-500 appliance generates are distributed to connected firewalls so that the firewalls can effectively block the malware the next time it is detected.

Android Application Package (APK) files are not supported for WildFire private cloud analysis.

WildFire Hybrid Cloud

A firewall in a WildFire hybrid cloud deployment can forward certain samples to the Palo Alto Networks-hosted WildFire global cloud and other samples to a WildFire private cloud hosted by a WF-500 appliance. A WildFire hybrid cloud deployment allows the flexibility to analyze private documents locally and inside your network, while the WildFire public cloud analyzes files from the Internet. For example, forward Payment Card Industry (PCI) and Protected Health Information (PHI) data exclusively to the WildFire private cloud for analysis, while forwarding Portable Executables (PEs) to the WildFire public cloud for analysis. In a WildFire hybrid cloud deployment, offloading files to the public cloud for analysis allows you benefit from a prompt verdict for files that have been previously processed in the WildFire public cloud, and also frees up the WF-500 appliance capacity to process sensitive content. Additionally, you can forward certain file types to the WildFire public cloud that are not currently supported for WF-500 appliance analysis, such as Android Application Package (APK) files.

In a WildFire hybrid cloud deployment, there might be some cases where a single file matches your criteria for both public cloud analysis and private cloud analysis; in these cases, the file is submitted only to the private cloud for analysis as a cautionary measure.

To set up hybrid cloud forwarding, see Forward Files for WildFire Analysis.
WildFire File Type Support

The following table lists the file types that are supported for analysis in the WildFire cloud environments.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Links contained in emails</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Android application package (APK) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>Adobe Flash files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>Java Archive (JAR) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft Office files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Portable executable (PE) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Portable document format (PDF) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mac OS X files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>Archive (RAR and 7z) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>Linux (ELF) files</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
</tbody>
</table>

Looking for more?
- For details on each WildFire cloud analysis environment, see WildFire Deployments.
- For details about each file type supported for WildFire analysis, see File Analysis.
WildFire Subscription

The basic WildFire service is included as part of the Palo Alto Networks next generation firewall and does not require a WildFire subscription. With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis, and can retrieve WildFire signatures only with antivirus and/or Threat Prevention updates which are made available every 24-48 hours.

A WildFire subscription unlocks the following WildFire features:

- **WildFire Dynamic Updates**—The WildFire public cloud and a WildFire private cloud can generate and distribute new WildFire signatures every five minutes, and you can set the firewall to retrieve and install these signatures every minute (this allows the firewall to get the latest signatures within a minute of availability). Select Device > Dynamic Updates to **Enable the firewall to get the latest WildFire signatures**. Depending on your WildFire deployment, you can set up one or both of the following signature package updates:
  - **WildFire**—Get the latest signatures from the WildFire public cloud.
  - **WF-Private**—Get the latest signatures from a WF-500 appliance that is configured to **locally generate signatures and URL categories**.

- **WildFire Advanced File Type Support**—In addition to PEs, forward advanced file types for WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), archive files, and HTTP/HTTPS email links contained in SMTP and POP3 email messages (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), and archive (RAR/7-Zip) files).

- **WildFire API**—Access to the **WildFire API**, which enables direct programmatic access to the WildFire public cloud or a WildFire private cloud. Use the WildFire API to submit files for analysis and to retrieve the subsequent WildFire analysis reports. The WildFire API supports up to 1,000 file submissions and up to 10,000 queries a day.

- **WildFire Private and Hybrid Cloud Support**—Forward files to a WF-500 appliance. WildFire private cloud and WildFire hybrid cloud deployments both require the firewall to be able to submit samples to a WF-500 appliance. Enabling a WF-500 appliance requires only a support license.
Get Started with WildFire

The following steps provide a quick workflow to get started with WildFire®. If you’d like to learn more about WildFire before getting started, take a look at the WildFire Overview and review WildFire Best Practices.

<table>
<thead>
<tr>
<th>Get Started with WildFire</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Get your WildFire Subscription. If you do not have a WildFire subscription, you can still forward PEs for WildFire analysis.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2** Decide which of the WildFire Deployments works for you:  
  - WildFire global cloud—Forward samples to the WildFire global cloud, or to one of two regional clouds hosted in Europe and Japan.  
  - WildFire private cloud—(Requires a WF-500 appliance) Forward samples to a local WF-500 appliance that resides on your network.  
  - WildFire hybrid cloud—(Requires a WF-500 appliance) Forward some samples to the WildFire public cloud and some samples to a WildFire private cloud. |  |
| **Step 3** (WildFire private and hybrid cloud only) Set Up and Manage a WF-500 Appliance, including upgrading the WF-500 appliance to the latest release version. Firewalls connected to the appliance must be running the same release version. |  |
| **Step 4** Confirm your WildFire license is active on the firewall. | 1. Log in to the firewall.  
  2. Select Device > Licenses and check that the WildFire License is active.  
  If the WildFire License is not displayed, select one of the License Management options to activate the license. |  |
| **Step 5** Connect the firewall to WildFire and configure WildFire settings. | 1. Select Device > Setup > WildFire and edit General Settings.  
  2. Use the WildFire Private Cloud and WildFire Public Cloud fields to Specify the WildFire Deployments to which you want to forward samples.  
  3. Define the size limits for files the firewall forwards and configure WildFire logging and reporting settings. It is a recommended WildFire best practice to set the **File Size** for PEs to the maximum size limit of 10 MB, and to leave the **File Size** for all other file types set to the default value.  
  4. Click OK to save the WildFire General Settings. |
### Get Started with WildFire

**Step 6** Enable the firewall to get the latest WildFire signatures. New WildFire signatures are made available every five minutes to detect and identify malware.

1. **Select Device > Dynamic Updates:**
   - *(WildFire public and hybrid cloud)* Check that WildFire updates are displayed.
   - *(WildFire private and hybrid cloud)* Check that **WF-Private** updates are displayed. For the firewall to receive signatures from a WF-500 appliance, you must enable the WF-500 appliance to **locally generate signatures and URL categories**.
   - Select **Check Now** to retrieve the latest signature update packages.

2. Set the **Schedule** to download and install the latest WildFire signatures.

3. Use the **Recurrence** field to set the frequency at which the firewall checks for new updates to **Every Minute**. As new WildFire signatures are available every five minutes, this setting ensures the firewall retrieves these signatures within a minute of availability.

4. Enable the firewall to **Download and Install** these updates as the firewall retrieves them.

5. **Click OK.**

**Step 7** Start scanning traffic for threats, including malware that WildFire identifies.

Attach the **default** Antivirus profile to a security policy rule to scan traffic the rules allows based on WildFire antivirus signatures (select **Policies > Security** and add or modify the defined **Actions** for a rule).

**Step 8** Start submitting samples for WildFire analysis.

1. **Define traffic to forward for WildFire analysis.** (Select **Objects > Security Profiles > WildFire Analysis** and modify or **Add** a WildFire Analysis profile).
   - As a best practice, use the WildFire Analysis default profile to ensure complete WildFire coverage for traffic the firewall allows. If you still decide to create a custom WildFire Analysis profile, set the profile to forward **Any** file type—this enables the firewall to automatically start forwarding newly-supported file types for analysis.

2. For each profile rule, set the **WildFire Deployments Destination** to which you want the firewall to forward samples for analysis—**public-cloud** or the **private-cloud**.

3. **Attach the WildFire Analysis profile to a security policy rule.** Traffic matched to the policy rule is forwarded for WildFire analysis (**Policies > Security** and **Add** or modify a security policy rule).

**Step 9** Enable the firewall to **Forward Decrypted SSL Traffic for WildFire Analysis.** This is a **recommended WildFire best practice.**
## Get Started with WildFire

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Confirm that the firewall is successfully forwarding samples.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• If you enabled logging of benign files in Step 4, select <strong>Monitor &gt; WildFire Submissions</strong> and check that entries are being logged for benign files submitted to WildFire. (If you'd like to disable logging of benign files after confirming that the firewall is connected to WildFire, select <strong>Device &gt; Setup &gt; WildFire</strong> and clear <strong>Report Benign Files</strong>).</td>
</tr>
<tr>
<td></td>
<td>• Other options to <strong>Verify File Forwarding</strong> allow you to confirm that the firewall forwarded a specific sample, view samples the firewall forwards according to file type, and to view the total number of samples the firewall forwards.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Test a Sample Malware File</strong> to test your complete WildFire configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Investigate WildFire analysis results.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Find WildFire analysis results:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use the Firewall to Monitor Malware</strong> and view WildFire analysis reports for a sample.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View Reports on the WildFire Portal</strong> for all samples submitted to the WildFire public cloud, including samples that you manually submitted to the WildFire public cloud.</td>
</tr>
<tr>
<td></td>
<td>• Use the WildFire API to retrieve sample verdicts and reports from a WF-500 appliance.</td>
</tr>
<tr>
<td></td>
<td>• Assess the risk of malware you find on your network with the <strong>AutoFocus</strong> threat intelligence portal. AutoFocus layers data from global WildFire submissions with statistics to identify pervasive and targeted malware, both on your network, within our industry, and globally.</td>
</tr>
</tbody>
</table>

| Step 12 | Review and implement **WildFire Best Practices**. |
Set Up and Manage a WF-500 Appliance

This topic describes how to configure a WF-500 appliance in order to host a WildFire® private cloud to analyze files on your network. The following topics describe readying the WF-500 appliance to receive files for analysis, how to manage the appliance, and how to enable the appliance to locally generate threat signatures and URL categories.

▲ About the WF-500 Appliance
▲ Configure the WF-500 Appliance
▲ Set Up the WF-500 Appliance VM Interface
▲ Enable WF-500 Appliance Analysis Features
▲ Upgrade a WF-500 Appliance
About the WF-500 Appliance

The WF-500 appliance provides an on-premises WildFire private cloud, enabling you to analyze suspicious files in a sandbox environment without requiring the firewall to send files out of network. To use the WF-500 appliance to host a WildFire private cloud, configure the firewall to submit samples to the WF-500 appliance for analysis. The WF-500 appliance sandboxes all files locally and analyzes them for malicious behaviors using the same engine the WildFire public cloud uses. Within minutes, the private cloud returns analysis results to the firewall WildFire Submissions logs.

You can continue to enable a WF-500 appliance to:

- Locally generate antivirus and DNS signatures for discovered malware, and to assign a URL category to malicious links. You can then enable connected firewalls to retrieve the latest signatures and URL categories every five minutes.
- Submit malware to the WildFire public cloud. The WildFire public cloud re-analyzes the sample and generates a signature to detect the malware—this signature can be made available within minutes to protect global users.
- Submit locally-generated malware reports (without sending the raw sample content) to the WildFire public cloud, to contribute to malware statistics and threat intelligence.

You can configure up to 100 Palo Alto Networks firewalls, each with valid WildFire subscriptions, to forward to a single WF-500 appliance. Beyond the WildFire firewall subscriptions, no additional WildFire subscription is required to enable a WildFire private cloud deployment.

WF-500 Appliance Interfaces

The WF-500 appliance has two interfaces:

- **MGT**—Receives all files forwarded from the firewalls and returns logs detailing the results back to the firewalls. See Configure the WF-500 Appliance.
- **Virtual Machine Interface (VM interface)**—Provides network access for the WildFire sandbox systems to enable sample files to communicate with the Internet, which allows WildFire to better analyze the behavior of the sample. When the VM interface is configured, WildFire can observe malicious behaviors that the malware would not normally perform without network access, such as phone-home activity. However, to prevent malware from entering your network from the sandbox, configure the VM interface on an isolated network with an Internet connection. You can also enable the Tor option to hide the public IP address used by your company from malicious sites that are accessed by the sample. For more information on the VM interface, see Set Up the WF-500 Appliance VM Interface.

Obtain the information required to configure network connectivity on the MGT port and the VM interface from your network administrator (IP address, subnet mask, gateway, hostname, DNS server). All communication between the firewalls and the appliance occurs over the MGT port, including file submissions, WildFire log delivery, and appliance administration. Therefore, ensure that the firewalls have connectivity to the MGT port on the appliance. In addition, the appliance must be able to connect to updates.paloaltonetworks.com to retrieve its operating system software updates.
Configure the WF-500 Appliance

This section describes the steps required to integrate a WF-500 appliance into a network and perform basic setup.

<table>
<thead>
<tr>
<th>Configure the WF-500 Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
</tbody>
</table>

- **Console Port**—This is a 9-pin male serial connector. Use the following settings on the console application: 9600-8-N-1. Connect the provided cable to the serial port on the management computer or USB-To-Serial converter.

- **MGT Port**—This is an Ethernet RJ-45 port. By default, the MGT port IP address is 192.168.1.1. The interface on your management computer must be on the same subnet as the MGT port. For example, set the IP address on the management computer to 192.168.1.5.

2. Power on the appliance.

   The appliance will power on as soon as you connect power to the first power supply and a warning beep will sound until you connect the second power supply. If the appliance is already plugged in and is in the shutdown state, use the power button on the front of the appliance to power on.
### Step 3  Register the WF-500 appliance.
1. Obtain the serial number from the S/N tag on the appliance, or run the following command and refer to the *serial* field:
   ```
   admin@WF-500> show system info
   ``
2. From a browser, navigate to the Palo Alto Networks Support Portal and log in.
3. Register the device as follows:
   - If this is the first Palo Alto Networks device that you are registering and you do not have a login, click **Register** at the bottom of the page.
     To register, provide an email address and the serial number of the device. When prompted, set up a username and password for access to the Palo Alto Networks support community.
   - For existing accounts, log in and then click **My Devices**. Scroll down to the **Register Device** section at the bottom of the screen and enter the serial number of the device, the city and postal code, and then click **Register Device**.
4. To confirm WildFire registration on the WF-500 appliance, log in to the appliance with an SSH client or by using the Console port. Enter a username/password of admin/admin and enter the following command on the appliance:
   ```
   admin@WF-500> test wildfire registration
   ```
   The following output indicates that the appliance is registered with one of the Palo Alto Networks WildFire cloud servers.
   ```
   Test wildfire
   wildfire registration: successful
   download server list: successful
   select the best server:
   cs-s1.wildfire.paloaltonetworks.com
   ```

### Step 4  Reset the admin password.
1. Set a new password by running the command:
   ```
   admin@WF-500> set password
   ```
2. Type the old password, press enter and then enter and confirm the new password. Commit the configuration to ensure that the new password is saved in the event of a restart.
3. Type `exit` to log out and then log back in to confirm that the new password is set.
Configure the WF-500 Appliance

Set Up and Manage a WF-500 Appliance

Configure the WF-500 Appliance (Continued)

Step 5 Configure the management interface settings.

This example uses the following values:

- IPv4 address - 10.10.0.5/22
- Subnet Mask - 255.255.252.0
- Default Gateway - 10.10.0.1
- Hostname - wildfire-corp1
- DNS Server - 10.0.0.246

1. Log in to the appliance with an SSH client or by using the Console port and enter configuration mode:
   admin@WF-500> configure

2. Set the IP information:
   admin@WF-500# set deviceconfig system ip-address 10.10.0.5 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting servers primary 10.0.0.246
   Configure a secondary DNS server by replacing primary with secondary in the above command, excluding the other IP parameters. For example:
   admin@WF-500# set deviceconfig system dns-setting servers secondary 10.0.0.247

3. Set the hostname (wildfire-corp1 in this example):
   admin@WF-500# set deviceconfig system hostname wildfire-corp1

4. Commit the configuration to activate the new management (MGT) port configuration:
   admin@WF-500# commit

5. Connect the MGT interface port to a network switch.

6. Put the management PC back on your corporate network, or whatever network is required to access the appliance on the management network.

7. From your management computer, use an SSH client to connect to the new IP address or hostname assigned to the MGT port on the appliance. In this example, the IP address is 10.10.0.5.

Step 6 Activate the appliance with the WildFire authorization code that you received from Palo Alto Networks.

Though it will function without an auth-code, the WF-500 appliance cannot retrieve software or content updates without a valid auth-code.

1. Change to operational mode:
   admin@WF-500# exit

2. Fetch and install the WildFire license:
   admin@WF-500> request license fetch auth-code <auth-code>

3. Verify the license:
   admin@WF-500> request support check
   Information about the support site and the support contract date is displayed. Confirm that the date displayed is valid.
Configure the WF-500 Appliance

Step 7 Set the WF-500 clock.

There are two ways to do this. You can either manually set the date, time, and timezone or you can configure the WF-500 appliance to synchronize its local clock with a Network Time Protocol (NTP) server.

- To set the clock manually, enter the following commands:
  
  admin@WF-500> set clock date <YY/MM/DD> time <hh:mm:ss>
  
  admin@WF-500> configure
  
  admin@WF-500# set deviceconfig system timezone <timezone>

  The time stamp that will appear on the WildFire detailed report will use the time zone set on the appliance. If administrators in various regions will view reports, consider setting the time zone to UTC.

- To configure the WF-500 to synchronize with an NTP server, enter the following commands:

  admin@WF-500> configure

  admin@WF-500# set deviceconfig system ntp-servers

  primary-ntp-server ntp-server-address <NTP primary server IP address>

  admin@WF-500# set deviceconfig system ntp-servers

  secondary-ntp-server ntp-server-address <NTP secondary server IP address>

  The WF-500 appliance does not prioritize the primary or secondary NTP server; it synchronizes with either server.

Step 8 (Optional for NTP configuration) Set up NTP authentication.

- Disable NTP authentication:

  admin@WF-500# set deviceconfig system ntp-servers

  primary-ntp-server authentication-type none

- Enable symmetric key exchange (shared secrets) to authenticate the NTP server time updates:

  admin@WF-500# set deviceconfig system ntp-servers

  primary-ntp-server authentication-type symmetric-key

  Continue to enter the key-ID (1 - 65534), choose the algorithm to use in NTP authentication (MD5 or SHA1), and then enter and confirm the authentication algorithm authentication-key.

- Use autokey (public key cryptography) to authenticate the NTP server time updates:

  admin@WF-500# set deviceconfig system ntp-servers

  primary-ntp-server authentication-type autokey

Step 9 Choose the virtual machine image for the appliance to use to analyze files.

The image should be based on the attributes that most accurately represent the software installed on your end user computers. Each virtual image contains different versions of operating systems and software, such as Windows XP or Windows 7 32-bit or 64-bit and specific versions of Adobe Reader, and Flash. Although you configure the appliance to use one virtual machine image configuration, the appliance uses multiple instances of the image to improve performance.

- To view a list of available virtual machines to determine which one best represents your environment:

  admin@WF-500> show wildfire vm-images

- View the current virtual machine image by running the following command and refer to the Selected VM field:

  admin@WF-500> show wildfire status

- Select the image that the appliance will use for analysis:

  admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>

  For example, to use vm-1:

  admin@WF-500# set deviceconfig setting wildfire active-vm vm-1
| Step 10 | Enable the WF-500 appliance to observe malicious behaviors where the file being analyzed seeks network access. | Set Up the WF-500 Appliance VM Interface. |
| Step 11 | (Optional) Enable the WF-500 appliance to get daily Palo Alto Networks content updates to facilitate and improve malware analysis. | Enable WF-500 Appliance Analysis Features |
| Step 12 | (Optional) Enable the WF-500 appliance to generate DNS and antivirus signatures and URL categories, and to distribute new signatures and URL categorizations to connected firewalls. | Enable Local Signature and URL Category Generation |
| Step 13 | (Optional) Automatically submit malware the WildFire private cloud discovers to the WildFire public cloud, to support global protection against the malware. | Submit Malware to the WildFire Public Cloud. |
| Step 14 | (Optional) If you do not want to forward malware samples outside of the WildFire private cloud, instead submit WildFire analysis reports to the WildFire public cloud. If you do not want to submit locally-discovered malware to the WildFire public cloud, it is a best practice to enable malware analysis report submissions to improve and refine WildFire threat intelligence. | Submit Analysis Reports to the WildFire Public Cloud. |
| Step 15 | (Optional) Allow additional users to manage the WF-500 appliance. You can assign two role types: superuser and superreader. Superuser is equivalent to the admin account, and superreader only has read access. In this example, you will create a superreader account for the user bsimpson: 1. Enter configuration mode: admin@WF-500> configure 2. Create the user account: admin@WF-500# set mgt-config users bsimpson <password> 3. Enter and confirm a new password. 4. Assign the superreader role: admin@WF-500# set mgt-config users bsimpson permissions role-based superreader yes |
Step 16 Configure RADIUS authentication for administrator access.

1. Create a RADIUS profile using the following options:
   ```
   admin@WF-500# set shared server-profile radius <profile-name>
   (Configure the RADIUS server and other attributes.)
   ```

2. Create an authentication profile:
   ```
   admin@WF-500# set shared authentication-profile <profile-name> method radius server-profile <server-profile-name>
   ```

3. Assign the profile to a local admin account:
   ```
   admin@WF-500# set mgt-config users username authentication-profile authentication-profile-name>
   ```
Set Up the WF-500 Appliance VM Interface

The virtual machine interface (vm-interface) provides external network connectivity from the sandbox virtual machines in the WF-500 appliance to enable observation of malicious behaviors in which the file being analyzed seeks network access. The following sections describe the VM interface and the steps required for configuring it. You can optionally enable the Tor feature with the VM interface, which will mask any malicious traffic sent from the WF-500 appliance through the VM interface, so the malware sites that the traffic may be sent to cannot detect your public-facing IP address.

This section also describes the steps required to connect the VM interface to a dedicated port on a Palo Alto Networks firewall to enable Internet connectivity.

- Virtual Machine Interface Overview
- Configure the VM Interface on the WF-500 Appliance
- Connect the Firewall to the WF-500 Appliance VM Interface

Virtual Machine Interface Overview

The VM interface (labeled 1 on the back of the appliance) is used by WildFire to improve malware detection capabilities. The interface allows a sample running on the WildFire virtual machines to communicate with the Internet so that the WF-500 appliance can better analyze the behavior of the sample file to determine if it exhibits characteristics of malware.

While it is recommended that you enable the VM interface, it is very important that you do not connect the interface to a network that allows access to any of your servers/hosts because malware that runs in the WildFire virtual machines could potentially use this interface to propagate itself.

This connection can be a dedicated DSL line or a network connection that only allows direct access from the VM interface to the Internet and restricts any access to internal servers/client hosts.

The following illustration shows two options for connecting the VM interface to the network.
Option-1 (recommended) — Connect the VM interface to an interface in a dedicated zone on a firewall that has a policy to the Internet and has no access to any of your internal servers/hosts. This is important because malware that runs in the WildFire virtual machines can potentially use this interface to propagate itself. This is the recommended option because the firewall logs will provide visibility into any traffic that is generated by the VM interface.

Option-2 — Use a dedicated Internet provider connection, such as a DSL, to connect the VM interface to the Internet. Ensure that there is no access from this connection to internal servers/hosts. Although this is a simple solution, traffic generated by the malware out the VM interface will not be logged unless you place a firewall or a traffic monitoring tool between the WF-500 appliance and the DSL connection.

Configure the VM Interface on the WF-500 Appliance

This section describes the steps required to configure the VM interface on the WF-500 appliance using the Option 1 configuration detailed in the Virtual Machine Interface Example. After configuring the VM interface using this option, you must also configure an interface on a Palo Alto Networks firewall through which traffic from the VM interface is routed as described in Connect the Firewall to the WF-500 Appliance VM Interface.

By default, the VM interface has the following settings:

- IP Address: 192.168.2.1
- Netmask: 255.255.255.0
- Default Gateway: 192.168.2.254
- DNS: 192.168.2.254
If you plan on enabling this interface, configure it with the appropriate settings for your network. If you do not plan on using this interface, leave the default settings. Note that this interface must have network values configured or a commit failure will occur.

### Configure the VM Interface

**Step 1** Set the IP information for the VM interface on the WF-500 appliance. The following settings are used in this example:
- IPv4 address - 10.16.0.20/22
- Subnet Mask - 255.255.252.0
- Default Gateway - 10.16.0.1
- DNS Server - 10.0.0.246

The VM interface cannot be on the same network as the management interface (MGT).

1. Enter configuration mode:
   ```
   admin@WF-500> configure
   ```
2. Set the IP information for the VM interface:
   ```
   admin@WF-500# set deviceconfig system vm-interface
   ip-address 10.16.0.20 netmask 255.255.252.0
   default-gateway 10.16.0.1 dns-server 10.0.0.246
   ```
   You can only configure one DNS server on the VM interface. As a best practice, use the DNS server from your ISP or an open DNS service.

**Step 2** Enable the VM interface.

1. Enable the VM interface:
   ```
   admin@WF-500# set deviceconfig setting wildfire
   vm-network-enable yes
   ```
2. Commit the configuration:
   ```
   admin@WF-500# commit
   ```

**Step 3** Test connectivity of the VM interface.

Ping a system and specify the VM interface as the source. For example, if the VM interface IP address is 10.16.0.20, run the following command where `ip-or-hostname` is the IP or hostname of a server/network that has ping enabled:

```
admin@WF-500> ping source 10.16.0.20 host ip-or-hostname
```

For example:

```
admin@WF-500> ping source 10.16.0.20 host 10.16.0.1
```

**Step 4** (Optional) Send any malicious traffic that the malware generates to the Internet. The Tor network masks your public facing IP address, so the owners of the malicious site cannot determine the source of the traffic.

1. Enable the Tor network:
   ```
   admin@WF-500# set deviceconfig setting wildfire
   vm-network-use-tor
   ```
2. Commit the configuration:
   ```
   admin@WF-500# commit
   ```

**Step 5** Connect the Firewall to the WF-500 Appliance VM Interface.

### Connect the Firewall to the WF-500 Appliance VM Interface

The following example workflow describes how to connect the VM interface to a port on a Palo Alto Networks firewall. Before connecting the VM interface to the firewall, the firewall must already have an Untrust zone connected to the Internet. In this example, you configure a new zone named `wf-vm-zone` that will contain the interface used to connect the VM interface on the appliance to the firewall. The policy associated with the `wf-vm-zone` will only allow communication from the VM interface to the Untrust zone.
Configure the Firewall to Control Traffic for the WF-500 Appliance VM Interface

**Step 1** Configure the interface on the firewall that the VM interface will connect to and set the virtual router.

The wf-vm-zone should only contain the interface (ethernet1/3 in this example) used to connect the VM interface on the appliance to the firewall. This is done to avoid having any traffic generated by the malware from reaching other networks.

1. From the web interface on the firewall, select **Network > Interfaces** and then select an interface, for example **Ethernet1/3**.
2. In the **Interface Type** drop-down, select **Layer3**.
3. On the **Config** tab, from the **Security Zone** drop-down box, select **New Zone**.
4. In the Zone dialog **Name** field, enter **wf-vm-zone** and click **OK**.
5. In the **Virtual Router** drop-down box, select **default**.
6. To assign an IP address to the interface, select the **IPv4** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example **10.16.0.0/22**.
7. To save the interface configuration, click **OK**.

**Step 2** Create a security policy on the firewall to allow access from the VM interface to the Internet and block all incoming traffic. In this example, the policy name is WildFire VM Interface. Because you will not create a security policy from the Untrust zone to the wf-vm-interface zone, all inbound traffic is blocked by default.

1. Select **Policies > Security** and click **Add**
2. In the **General** tab, enter a **Name**.
3. In the **Source** tab, set the **Source Zone** to **wf-vm-zone**.
4. In the **Destination** tab, set the **Destination Zone** to **Untrust**.
5. In the **Application** and **Service/ URL Category** tabs, leave the default as **Any**.
6. In the **Actions** tab, set the **Action Setting** to **Allow**.
7. Under **Log Setting**, select the **Log at Session End** check box.

If there are concerns that someone might inadvertently add other interfaces to the wf-vm-zone, clone the WildFire VM Interface security policy and then in the **Action** tab for the cloned rule, select **Deny**. Make sure this new security policy is listed below the WildFire VM interface policy. This will override the implicit intra-zone allow rule that allows communications between interfaces in the same zone and will deny/block all intra-zone communication.

**Step 3** Connect the cables.

Physically connect the VM interface on the WF-500 appliance to the port you configured on the firewall (Ethernet 1/3 in this example) using a straight through RJ-45 cable. The VM interface is labeled 1 on the back of the appliance.

**Step 4** Verify that the VM interface is transmitting and receiving traffic.

1. View the VM interface settings:
   ```
   admin@WF-500> show interface vm-interface
   ```

2. Verify that received/transmitted counters are incrementing. You can run the following command to generate ping traffic from the VM interface to an external device:
   ```
   admin@WF-500> ping source vm-interface-ip host <gateway-ip>
   ```
   **For example:**
   ```
   admin@WF-500> ping source 10.16.0.20 host 10.16.0.1
   ```
Enable WF-500 Appliance Analysis Features

- Set Up WF-500 Appliance Content Updates
- Enable Local Signature and URL Category Generation
- Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud

Set Up WF-500 Appliance Content Updates

Configure daily content updates for the WF-500 appliance. WF-500 content updates provide the appliance with threat intelligence to facilitate accurate malware detection, improve appliance capability to differentiate malicious samples from benign samples, and ensure that the appliance has the most recent information needed to generate signatures.

- Install WF-500 Content Updates Directly from the Update Server
- Install WF-500 Content Updates from an SCP-Enabled Server

Install WF-500 Content Updates Directly from the Update Server

### Install Threat Intelligence Content Updates Directly from the Update Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1. | Log in to the WF-500 appliance and run the following command to display the current content version:  
admin@wf-500> show system info | match wf-content-version  
2. | Confirm that the appliance can communicate with the Palo Alto Networks Update Server and view available updates:  
admin@wf-500> request wf-content upgrade check  
The command queries the Palo Alto Networks Update Server and provides information about available updates and identifies the version that is currently installed on the appliance.  
<table>
<thead>
<tr>
<th>Version</th>
<th>Size</th>
<th>Released on</th>
<th>Downloaded</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-253</td>
<td>57MB</td>
<td>2014/09/20 20:00:08 PST</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>2-39</td>
<td>44MB</td>
<td>2014/02/12 14:04:27 PST</td>
<td>yes</td>
<td>current</td>
</tr>
</tbody>
</table>

If the appliance cannot connect to the update server, you will need to allow connectivity from the appliance to the Palo Alto Networks Update Server (updates.paloaltonetworks.com), or download and install the update using SCP as described in Install WF-500 Content Updates from an SCP-Enabled Server.
### Install Threat Intelligence Content Updates Directly from the Update Server (Continued)

#### Step 2  Download and install the latest content update.

1. **Download the latest content update:**
   ```bash
   admin@wf-500> request wf-content upgrade download latest
   ```

2. **View the status of the download:**
   ```bash
   admin@wf-500> show jobs all
   You can run `show jobs pending` to view pending jobs. The following output shows that the download (job id 5) has finished downloading (Status FIN):  
   ```
<table>
<thead>
<tr>
<th>Enqueued</th>
<th>ID</th>
<th>Type</th>
<th>Status</th>
<th>Result</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>03:42:20</td>
<td>5</td>
<td>Downld</td>
<td>FIN</td>
<td>OK</td>
<td>03:42:23</td>
</tr>
</tbody>
</table>
   ```

3. **After the download is complete, install the update:**
   ```bash
   admin@wf-500> request wf-content upgrade install version latest
   Run the `show jobs all` command again to monitor the status of the install.
   ```

#### Step 3  Verify the content update.

Run the following command and refer to the `wf-content-version` field:
```bash
admin@wf-500> show system info
```

The following shows an example output with content update version 2-253 installed:
```bash
admin@wf-500> show system info
hostname: wf-500
ip-address: 10.5.164.245
netmask: 255.255.255.0
default-gateway: 10.5.164.1
mac-address: 00:25:90:c3:ed:56
vm-interface-ip-address: 192.168.2.2
vm-interface-netmask: 255.255.255.0
vm-interface-default-gateway: 192.168.2.1
vm-interface-dns-server: 192.168.2.1
time: Mon Apr 21 09:59:07 2014
uptime: 17 days, 23:19:16
family: m
model: WP-500
serial: abcd3333
sw-version: 6.1.0
wf-content-version: 2-253
wfm-release-date: 2014/08/20 20:00:08
logdb-version: 6.1.2
platform-family: m
```

#### Step 4  (Optional)  Schedule content updates to be installed on a daily or weekly basis.

1. **Schedule the appliance to download and install content updates:**
   ```bash
   admin@WF-500# set deviceconfig system update-schedule wf-content recurring [daily | weekly] action [download-and-install | download-only]
   For example, to download and install updates daily at 8:00 am:
   ```
   ```bash
   admin@WF-500# set deviceconfig system update-schedule wf-content recurring daily action download-and-install at 08:00
   ```

2. **Commit the configuration**
   ```bash
   admin@WF-500# commit
   ```
Install WF-500 Content Updates from an SCP-Enabled Server

The following procedure describes how to install threat intelligence content updates on a WF-500 appliance that does not have direct connectivity to the Palo Alto Networks Update Server. You will need a Secure Copy (SCP)-enabled server to temporarily store the content update.

**Install Threat Intelligence Content Updates from an SCP-Enabled Server**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Retrieve the content update file from the update server.</th>
</tr>
</thead>
</table>
| 1. Log in to the Palo Alto Networks Support Portal and click Dynamic Updates.  
2. In the WF-500 Appliance section, locate the latest WF-500 appliance content update and download it.  
3. Copy the content update file to an SCP-enabled server and note the file name and directory path. |

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Install the content update on the WF-500 appliance.</th>
</tr>
</thead>
</table>
| 1. Log in to the WF-500 appliance and download the content update file from the SCP server:  
admin@WF-500> scp import wf-content from username@host:path  
For example:  
admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/updates/panup-all-wfmeta-2-253.tgz  
If your SCP server is running on a non-standard port or if you need to specify the source IP, you can also define those options in the `scp import` command.  
2. Install the update:  
admin@WF-500> request wf-content upgrade install file panup-all-wfmeta-2-253.tgz  
3. View the status of the installation:  
admin@WF-500> show jobs all |

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Verify the content update.</th>
</tr>
</thead>
</table>
| Verify the content version:  
admin@wf-500> show system info | match wf-content-version  
The following output now shows version 2-253:  
wf-content-version: 2-253 |

**Enable Local Signature and URL Category Generation**

The WF-500 appliance can generate signatures locally based on the samples received from connected firewalls and the WildFire API, as an alternative to sending malware to the public cloud for signature generation. The appliance can generate the following types of signatures for the firewalls to use to block malware and any associated command and control traffic:

- **Antivirus signatures**—Detect and block malicious files. WildFire adds these signatures to WildFire and Antivirus content updates.
- **DNS signatures**—Detect and block callback domains for command and control traffic associated with malware. WildFire adds these signatures to WildFire and Antivirus content updates.
- **URL categories**—Categorizes callback domains as malware and updates the URL category in PAN-DB.
Configure the firewalls to retrieve the signatures generated by the WF-500 appliance as frequently as every five minutes. You can also send the malware sample to the WildFire public cloud, in order to enable the signature to be distributed globally through Palo Alto Networks content releases.

Even if you're using the WF-500 appliance for local file analysis, you can also enable connected firewalls to receive the latest signatures distributed by the WildFire public cloud.

Enable the WF-500 Appliance to Generate and Distribute Signature and URL Categories

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set Up WF-500 Appliance Content Updates.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This allows the WF-500 appliance to receive the latest threat intelligence from Palo Alto Networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Enable signature and URL category generation.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Log in to the appliance and type <code>configure</code> to enter configuration mode.</td>
</tr>
<tr>
<td></td>
<td>2. Enable all threat prevention options:</td>
</tr>
<tr>
<td></td>
<td><code>admin@WF-500# set deviceconfig setting wildfire signature-generation av yes dns yes url yes</code></td>
</tr>
<tr>
<td></td>
<td>3. Commit the configuration:</td>
</tr>
<tr>
<td></td>
<td><code>admin@WF-500# commit</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Set the schedule for connected firewalls to retrieve the signatures and URL categories the WF-500 appliance generates.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It is a best practice to configure your firewalls to retrieve content updates from both the WildFire public cloud and WF-500 appliance. This ensures that your firewalls receive signatures based on threats detected worldwide, in addition to the signatures generated by the local appliance.</td>
</tr>
<tr>
<td></td>
<td>• For multiple firewalls managed by Panorama:</td>
</tr>
<tr>
<td></td>
<td>Launch Panorama and select <strong>Panorama &gt; Device Deployment &gt; Dynamic Updates</strong>, click <strong>Schedules</strong>, and <strong>Add</strong> scheduled content updates for managed devices. For details on using Panorama to set up managed firewalls to receive signatures and URL categories from a WF-500 appliance, see <strong>Schedule Content Updates to Devices Using Panorama</strong>.</td>
</tr>
<tr>
<td></td>
<td>• For a single firewall:</td>
</tr>
<tr>
<td></td>
<td>a. Log in to the firewall web interface and select <strong>Device &gt; Dynamic Updates</strong>. For firewalls configured to forward files to a WF-500 appliance (in either a WildFire private cloud or hybrid cloud deployment), the WF-Private section is displayed.</td>
</tr>
<tr>
<td></td>
<td>b. Set the <strong>Schedule</strong> for the firewall to <strong>download and install content updates</strong> from the WF-500 appliance.</td>
</tr>
</tbody>
</table>
Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud

Enable the WF-500 appliance to automatically submit malware samples to the WildFire public cloud. The WildFire public cloud further analyzes the malware and generates a signature to identify the sample. The signature is then added to WildFire signature updates, and distributed to global users to prevent future exposure to the threat. If you do not want to forward malware samples outside of your network, you can instead choose to submit only WildFire reports for the malware discovered on your network, in order to contribute to and refine WildFire statistics and threat intelligence.

<table>
<thead>
<tr>
<th>Enable the WF-500 Appliance to Submit Malware or Reports to the WildFire Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Submit Malware to the WildFire Public Cloud.</td>
</tr>
<tr>
<td>1. Execute the following CLI command from the WF-500 appliance to enable the appliance to automatically submit malware samples to the WildFire public cloud:</td>
</tr>
<tr>
<td><code>admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes</code></td>
</tr>
<tr>
<td>If the firewall that originally submitted the sample for WildFire private cloud analysis has packet captures (PCAPs) enabled, the PCAPs for the malware will also be forwarded to the WildFire public cloud.</td>
</tr>
<tr>
<td>2. Go to the WildFire portal to view analysis reports for malware automatically submitted to the WildFire public cloud. When malware is submitted to the WildFire public cloud, the public cloud generates a new analysis report for the sample.</td>
</tr>
<tr>
<td>• Submit Analysis Reports to the WildFire Public Cloud</td>
</tr>
<tr>
<td>To automatically submit malware reports to the WildFire public cloud (and not the malware sample), execute the following CLI command on the WF-500 appliance:</td>
</tr>
<tr>
<td><code>admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-report yes</code></td>
</tr>
<tr>
<td>If you have enabled the WF-500 appliance to automatically submit malware to the WildFire public cloud, you do not need to enable this option—the WildFire public cloud will generate a new analysis report for the sample.</td>
</tr>
<tr>
<td>Reports submitted to the WildFire public cloud cannot be viewed on the WildFire portal. The WildFire portal displays only WildFire public cloud reports.</td>
</tr>
<tr>
<td>• Verify Malware and Report Submission Settings</td>
</tr>
<tr>
<td>Check to confirm that cloud intelligence is enabled to either submit malware or submit reports to the WildFire public cloud by running the following command:</td>
</tr>
<tr>
<td><code>admin@WF-500&gt; show wildfire status</code></td>
</tr>
<tr>
<td>Refer to the Submit sample and Submit report fields.</td>
</tr>
</tbody>
</table>
Upgrade a WF-500 Appliance

Use the following workflow to upgrade the WF-500 appliance operating system. The appliance can only use one environment at a time to analyze samples, so after upgrading the appliance, review the list of available VM images and then choose the image that best fits your environment. In the case of Windows 7, if your environment has a mix of Windows 7 32-bit and Windows 7 64-bit systems, it is recommended that you choose the Windows 7 64-bit image, so WildFire will analyze both 32-bit and 64-bit PE files. Although you configure the appliance to use one virtual machine image configuration, the appliance uses multiple instances of the image to perform file analyses.

<table>
<thead>
<tr>
<th>Upgrade the WF-500 Appliance to PAN-OS 7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Download the 7.1 software version to the WF-500 appliance. You cannot skip any major release versions when upgrading the WF-500 appliance. For example, if you want to upgrade from PAN-OS 6.1 to PAN-OS 7.1, you must first install PAN-OS 7.0. The WF-500 appliance does not support PAN-OS 7.1.1. However, if you'd like to upgrade connected firewalls to PAN-OS 7.1.1, you can continue to do so after upgrading the WF-500 appliance to PAN-OS 7.1.0.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Install the 7.1 software version on the WF-500 appliance.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Confirm that the installation was successful.</td>
</tr>
</tbody>
</table>

Log in to the WF-500 appliance and download the 7.1.0 software version:
```
admin@WF-500> request system software download version 7.1.0
```
To check the status of the download, use the following command:
```
admin@WF-500> show jobs all
```

Install the WF-500 appliance operating system image (downloaded in **Step 1**) by running the following command:
```
admin@WF-500> request system software install version 7.1.0
```

1. Confirm that the upgrade is complete. Run the following command and look for the job type **Install** and status **FIN**:
```
admin@WF-500> show jobs all
```

2. Restart the appliance:
```
admin@WF-500> request restart system
```

3. Verify that the `sw-version` field shows 7.1:
```
admin@WF-500> show system info | match sw-version
```
### Upgrade the WF-500 Appliance to PAN-OS 7.1 (Continued)

| Step 4 (Optional) Enable the Windows 7 64-bit sandbox environment. | 1. View the active virtual machine image by running the following command and refer to the *Selected VM field*:  
   `admin@WF-500> show wildfire status`
   
   2. View a list of available virtual machines images:  
   `admin@WF-500> show wildfire vm-images`
      
      The following output shows that *vm-5* is the Windows 7 64-bit image:  
      
      *vm-5*
      Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010. Support PE, PDF, Office 2010 and earlier
   
   3. Select the image to be used for analysis:  
   `admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>`
      
      For example, to use *vm-5*, run the following command:  
      `admin@WF-500# set deviceconfig setting wildfire active-vm vm-5`
   
   4. Commit the configuration:  
   `admin@WF-500# commit`

| Step 5 Upgrade the firewalls connected to the appliance. | Upgrade firewalls to PAN-OS 7.1 and continue to [Forward Files for WildFire Analysis](#) |

---

---

© Palo Alto Networks, Inc.  
WildFire 7.1 Administrator’s Guide  •  37
Submit Files for WildFire Analysis

The following topics describe how to submit files for WildFire® analysis. You can set up Palo Alto Networks firewalls to automatically forward unknown files to the WildFire public cloud or a WildFire private cloud, and you can also manually submit files for analysis using the WildFire portal. Samples submitted for WildFire analysis receive a verdict of benign, grayware, or malware, and a detailed analysis report is generated for each sample.

- WildFire Best Practices
- Forward Files for WildFire Analysis
- Forward Decrypted SSL Traffic for WildFire Analysis
- Verify WildFire Submissions
- Manually Upload Files to the WildFire Portal
- Submit Malware or Reports from the WF-500 Appliance
- Firewall File Forwarding Capacity by Platform
WildFire Best Practices

- Follow the best practices to secure your network from Layer 4 and Layer 7 evasions to ensure reliable content identification and analysis. Specifically make sure to implement the best practices for TCP settings (Device > Setup > Session > TCP Settings) and Content-ID settings (Device > Setup > Content-ID > Content-ID Settings).

- Make sure that you also have an active Threat Prevention subscription. Together, WildFire and Threat Prevention enable comprehensive threat detection and prevention.

- The WildFire cloud generates and distributes new WildFire signatures every five minutes, but you can configure the firewall to download signature updates every minute to ensure that you get the latest version within a minute of availability.

- If the firewall is configured to decrypt SSL traffic, enable the firewall to Forward Decrypted SSL Traffic for WildFire Analysis. Only a superuser can enable this option.

- Use the default WildFire Analysis profile to define the traffic the firewall should forward for WildFire analysis (Objects > Security Profiles > WildFire Analysis). The default WildFire Analysis profile ensures complete WildFire coverage for all traffic your security policy allows—it specifies that all supported file types across all applications are forwarded for WildFire analysis, regardless of whether the files are uploaded or downloaded.

  If you choose to create a custom WildFire Analysis profile, it is a best practice to still set the profile to forward any file type. This allows the firewall to automatically begin forwarding file types as they become supported for WildFire analysis.

  For details on applying a WildFire Analysis profile to firewall traffic, review how to Forward Files for WildFire Analysis.

- While you are configuring the firewall to forward files for WildFire analysis, review the file Size Limit for all supported file types. Set the Size Limit for portable executables (PEs) to the maximum supported file size limit: 10 MB. Leave the Size Limit for all other file types set to the default limit. (Select Device > Setup > WildFire and edit the General Settings to adjust file size limits based on file type. Click the Help icon to find the default size limit for each file type).

  About the Default File Size Limits for WildFire Forwarding

  The default file size limits on the firewall are designed to include the large majority of malware in the wild (which is smaller than the default size limits) and exclude large files that are very unlikely to be malicious and can impact WildFire forwarding capacity. Because the firewall has a specific capacity reserved to forward files for WildFire analysis, forwarding high numbers of large files might cause the firewall to skip forwarding some files. This condition might occur when the maximum file size limits are configured for a file type that is traversing the firewall at a high rate. In this case, a potentially malicious file might not be forwarded for WildFire analysis. Consider this possible condition if you would like to increase the size limit for files other than PEs beyond the default size limit.

  The following graph is a representative illustration of the distribution of file sizes for malware, as observed by the Palo Alto Networks threat research team. The firewall default file sizes settings can be increased to the maximum file size setting to gain a relatively small increase in the malware catch rate for each file type.
Recommended File Size Limits to Catch Uncommonly Large Malicious Files

If you are specifically concerned about uncommonly large malicious files, you might want to increase file size limits beyond the default settings. In these cases, the following settings are recommended to catch rare, very large malicious files.

Select Device > Setup > WildFire, and edit General Settings to adjust the Size Limit for each file type:

- pe—10 MB
- apk—30 MB
- pdf—1,000 KB
- ms-office—2,000 KB
- jar—5 MB
- flash—5 MB
- MacOSX—1 MB
- archive—10 MB
Forward Files for WildFire Analysis

Configure Palo Alto Networks firewalls to forward unknown files or email links for analysis. Use the WildFire Analysis profile to define files to forward to the WildFire cloud (use the public cloud or a private cloud), and then attach the profile to a security rule to trigger inspection for zero-day malware.

Specify traffic to be forwarded for analysis based on the application in use, the file type detected, links contained in email messages, or the transmission direction of the sample (upload, download, or both). For example, you can set up the firewall to forward Portable Executables (PEs) or any files that users attempt to download during a web-browsing session.

If you are using a WF-500 appliance to host a WildFire private cloud, you can extend WildFire analysis resources to a WildFire Hybrid Cloud, by configuring the firewall to continue to forward sensitive files to your WildFire private cloud for local analysis, and forward less sensitive or unsupported file types to the WildFire public cloud.

Before you begin:
- If another firewall resides between the firewall you are configuring to forward files and the WildFire cloud or WF-500 appliance, make sure that the firewall in the middle allows the following ports:
  - The WildFire public cloud uses port 443 for registration and file submissions.
  - The WF-500 appliance uses port 443 for registration and 10443 for file submissions.
- (PA-7000 Series Firewalls Only) To enable a PA-7000 Series firewall to forward files and email links for WildFire analysis, you must first configure a data port on an NPC as a Log Card interface.

### Configure a Firewall to Forward Files and Email Links to WildFire

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Specify the WildFire Deployments to which you want to forward samples.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Device &gt; Setup &gt; WildFire and edit the General Settings based on your WildFire cloud deployment (public, private, or hybrid).</td>
<td></td>
</tr>
<tr>
<td><strong>WildFire Public Cloud:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Enter the WildFire Public Cloud URL:</td>
<td></td>
</tr>
<tr>
<td>• United States: wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Europe: eu.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Japan: jp.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Singapore: sg.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>2. Make sure the WildFire Private Cloud field is clear.</td>
<td></td>
</tr>
<tr>
<td><strong>WildFire Private Cloud:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Enter the IP address or FQDN of the WF-500 appliance in the WildFire Private Cloud field.</td>
<td></td>
</tr>
<tr>
<td>2. Clear the WildFire Public Cloud field.</td>
<td></td>
</tr>
<tr>
<td><strong>WildFire Hybrid Cloud:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Enter the WildFire Public Cloud URL:</td>
<td></td>
</tr>
<tr>
<td>• United States: wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Europe: eu.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Japan: jp.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• Singapore: sg.wildfire.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>2. Enter the IP address or FQDN of the WF-500 appliance in the WildFire Private Cloud field.</td>
<td></td>
</tr>
</tbody>
</table>
### Configure a Firewall to Forward Files and Email Links to WildFire (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Define the size limits for files the firewall forwards and configure WildFire logging and reporting settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Continue editing WildFire General Settings (&lt;Device &gt; Setup &gt; WildFire).</td>
</tr>
<tr>
<td></td>
<td>- Review the File Size Limits for files forwarded from the firewall.</td>
</tr>
<tr>
<td></td>
<td>It is recommended WildFire best practice to set the File Size for PEs to the maximum size limit of 10 MB, and to leave the File Size for all other file types set to the default value.</td>
</tr>
<tr>
<td></td>
<td>- Select Report Benign Files to allow logging for files that receive a WildFire verdict of benign.</td>
</tr>
<tr>
<td></td>
<td>- Select Report Grayware Files to allow logging for files that receive a WildFire verdict of grayware.</td>
</tr>
<tr>
<td></td>
<td>- Define what session information is recorded in WildFire analysis reports by editing the Session Information Settings. By default, all session information is displayed in WildFire analysis reports. Clear the check boxes to remove the corresponding fields from WildFire analysis reports and click <strong>OK</strong> to save the settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>(Panorama Only) Configure Panorama to gather additional information about samples collected from firewalls running a PAN-OS version prior to PAN-OS 7.0. Some WildFire Submissions log fields introduced in PAN-OS 7.0 are not populated for samples submitted by firewalls running earlier software versions. If you are using Panorama to manage firewalls running software versions earlier than PAN-OS 7.0, Panorama can communicate with WildFire to gather complete analysis information for samples submitted by those firewalls from the defined WildFire Server (the WildFire global cloud, by default) to complete the log details.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select <strong>Panorama &gt; Setup &gt; WildFire</strong> and enter a <strong>WildFire Server</strong> if you'd like to modify the default setting to instead allow Panorama to gather details from the WildFire cloud hosted in Japan or from a WF-500 appliance.</td>
</tr>
</tbody>
</table>
Step 4  Define traffic to forward for WildFire analysis.

If you have a WF-500 appliance set up, you can use both the private cloud and the public cloud in a hybrid cloud deployment. Analyze sensitive files locally on your network, while sending all other unknown files to the WildFire public cloud for comprehensive analysis and prompt verdict returns.

1. Select Objects > Security Profiles > WildFire Analysis. Add a new WildFire analysis profile, and give the profile a descriptive Name.

2. Add a profile rule to define traffic to be forwarded for analysis and give the rule a descriptive Name, such as local-PDF-analysis.

3. Define for the profile rule to match to unknown traffic and to forward samples for analysis based on:
   - Applications—Forward files for analysis based on the application in use.
   - File Types—Forward files for analysis based on file types, including links contained in email messages. For example, select PDF to forward unknown PDFs detected by the firewall for analysis.
   - Direction—Forward files for analysis based the transmission direction of the file (upload, download, or both). For example, select both to forward all unknown PDFs for analysis, regardless of the transmission direction.

4. Set the Analysis location to which the firewall forwards files matched to the rule.
   - Select public-cloud to forward matching samples to the WildFire public cloud for analysis.
   - Select private-cloud to forward matching samples to a WildFire private cloud for analysis.

   For example, to analyze PDFs that could contain sensitive or proprietary information without sending these documents out of your network, set the Analysis location for the rule local-PDF-analysis to private-cloud.

5. (Optional) Continue to add rules to the WildFire analysis profile as needed. For example, you could add a second rule to the profile to forward Android application package (APK), Portable Executable (PE), and Flash files to the WildFire public cloud for analysis.

6. Click OK to save the WildFire analysis profile.
## Configure a Firewall to Forward Files and Email Links to WildFire (Continued)

**Step 5**  
Attach the WildFire Analysis profile to a security policy rule. Traffic allowed by the security policy rule is evaluated against the attached WildFire analysis profile; the firewalls forwards traffic matched to the profile for WildFire analysis.

1. Select **Policies > Security** and **Add** or modify a policy rule.  
2. Click the **Actions** tab within the policy rule.  
3. In the Profile Settings section, select **Profiles** as the **Profile Type** and select a **WildFire Analysis** profile to attach to the policy rule.

![Profile Settings](image)

**Step 6**  
Make sure to enable the firewall to also **Forward Decrypted SSL Traffic for WildFire Analysis**.  
This is a **recommended WildFire best practice**.

**Step 7**  
Review and implement **WildFire Best Practices**.

**Step 8**  
Click **Commit** to apply the WildFire settings.

**Step 9**  
Choose what to do next...

- **Verify WildFire Submissions** to confirm that the firewall is successfully forwarding files for WildFire analysis.  
- **(WildFire Private Cloud Only) Submit Malware or Reports from the WF-500 Appliance**. Enable this feature to automatically forward malware identified in your WildFire private cloud to the WildFire public cloud. The WildFire public cloud re-analyzes the sample and generates a signature if the sample is malware. The signature is distributed to global users through Wildfire signature updates.  
- **Monitor WildFire Activity** to assess alerts and details reported for malware.
# Forward Decrypted SSL Traffic for WildFire Analysis

Enable the firewall to forward decrypted SSL traffic for WildFire analysis. Traffic that the firewall decrypts is evaluated against security policy rules; if it matches the WildFire analysis profile attached to the security rule, the decrypted traffic is forwarded for WildFire analysis before the firewall re-encrpts it. Only a super user can enable this option.

Forwarding decrypted SSL traffic for WildFire analysis is a **WildFire best practice.**

## Forward Decrypted SSL Traffic

<table>
<thead>
<tr>
<th>On a firewall that does not have multiple virtual systems enabled:</th>
<th>1. If you have not already, enable the firewall to perform <strong>decryption</strong> and <strong>Forward Files for WildFire Analysis</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Select <strong>Device &gt; Setup &gt; Content-ID</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Edit the Content-ID settings and <strong>Allow Forwarding of Decrypted Content</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong> to save the changes.</td>
</tr>
<tr>
<td>On a firewall with virtual systems enabled:</td>
<td>1. If you have not already, enable decryption and <strong>Forward Files for WildFire Analysis</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Device &gt; Virtual Systems</strong>, click the virtual system you want to modify, and <strong>Allow Forwarding of Decrypted Content</strong>.</td>
</tr>
</tbody>
</table>
Verify WildFire Submissions

Test your WildFire setup using malware test samples, and also verify that the firewall is correctly forwarding files for WildFire analysis.

▲ Test a Sample Malware File
▲ Verify File Forwarding

Test a Sample Malware File

Palo Alto Networks provides a sample malware file that you can use to test a WildFire configuration. Take the following steps to download the malware sample file, verify that the file is forwarded for WildFire analysis, and view the analysis results.

Use a Sample Malware File to Test the WildFire Configuration

Step 1 Download the malware test file: http://wildfire.paloaltonetworks.com/publicapi/test/pe. If you have SSL decryption enabled on the firewall, use the following URL instead: https://wildfire.paloaltonetworks.com/publicapi/test/pe.

The test file is named wildfire-test-pe-file.exe and each test file has a unique SHA-256 hash value.

You can also use the WildFire API to retrieve a malware test file. See the WildFire API Reference for details.

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.

Verify File Forwarding

After the firewall is set up to Forward Files for WildFire Analysis, use the following options to verify the connection between the firewall and the WildFire public or private cloud, and to monitor file forwarding.

Several of the options to verify that a firewall is forwarding samples for WildFire analysis are CLI commands; for details on getting started with and using the CLI, refer to the PAN-OS CLI Quick Start Guide.
Verify File Forwarding

- Verify that the firewall is communicating with a WildFire server(s).

Use the `test wildfire registration` command to verify that the firewall is connected to a WildFire private cloud, the WildFire public cloud, or both.

The following example output is for a firewall in a WildFire Private Cloud deployment:

```
admin@VM-FW> test wildfire registration
This test may take a few minutes to finish.
Do you want to continue? (y or n)
Test wildfire Public Cloud
Testing cloud server wildfire.paloaltonetworks.com ... wildfire registration: failed

Test wildfire Private Cloud
Testing cloud server X.X.X.X ... wildfire registration: successful
download server list: successful
select the best server: X.X.X.X:XXXX
```

The example output confirms that the firewall is connected to the WildFire private cloud, and is not connected to the WildFire public cloud (public cloud registration fails).

If the firewall is configured in a WildFire Hybrid Cloud deployment, check that the firewall is successfully registered with and connected to both the WildFire public cloud and a WildFire private cloud.
Verify File Forwarding (Continued)

- Verify the status of the firewall connection to the WildFire public and/or private cloud, including the total number of files forwarded by the firewall for analysis.

Use the `show wildfire status` command to:
- Check the status of the WildFire public and/or private cloud to which the firewall is connected. The status `Idle` indicates that the WildFire cloud (public or private) is ready to receive files for analysis.
- Confirm the configured size limits for files forwarded by the firewall (`Device > Setup > WildFire`).
- Monitor file forwarding, including how the total count of files forwarded by the firewall for WildFire analysis. If the firewall is in a WildFire hybrid cloud deployment, the number of files forwarded to the WildFire public cloud and the WildFire private cloud are also displayed.

The following example shows the `show wildfire status` output for a firewall in a WildFire private cloud deployment:

```
admin@WM-FW> show wildfire status

Connection info:
  Signature verification: enable
  Server selection: enable
  File cache: enable

WildFire Public Cloud:
  Server address: wildfire.paloaltonetworks
  Status: Disabled due to config
  Best server:
  Device registered: no
  Through a proxy: no
  Valid wildfire license: yes
  Service route IP address: X.X.X.X

WildFire Private Cloud:
  Server address: X.X.X.X
  Status: Idle
  Best server: X.X.X.X:XXXXXX
  Device registered: yes
  Through a proxy: no
  Valid wildfire license: yes
  Service route IP address: X.X.X.X

File size limit info:
  pe 9 MB
  apk 49 MB
  pdf 1000 KB
  ms-office 9500 KB
  jar 9 MB
  flash 10 MB
  MacOX 1 MB

Forwarding info:
  file idle time out (second): 90
  total concurrent files: 0
  Public Cloud:
    total files forwarded: 0
    file forwarded in last minute: 0
    concurrent files: 0
  Private Cloud:
    total files forwarded: 0
    file forwarded in last minute: 0
    concurrent files: 0

To view forwarding information for only the WildFire public cloud or WildFire private cloud, use the following commands:
- `show wildfire status channel public`
- `show wildfire status channel private`
```
### Verify WildFire Submissions
### Submit Files for WildFire Analysis

<table>
<thead>
<tr>
<th>View samples forwarded by the firewall according to file type (including email links).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this option to confirm that email links are being forwarded for WildFire analysis, since only email links that receive a malware verdict are logged as <strong>WildFire Submissions</strong> entries on the firewall, even if logging for benign and grayware samples is enabled. This is due to the sheer number of WildFire Submissions entries that would be logged for benign email links.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use the <code>show wildfire statistics</code> command to confirm the file types being forwarded to the WildFire public or private cloud:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The command displays the output of a working firewall and shows counters for each file type that the firewall forwards for WildFire analysis. If a counter field shows 0, the firewall is not forwarding that file type.</td>
</tr>
<tr>
<td>• Confirm that email links are being forwarded for analysis by checking that the following counters do not show zero:</td>
</tr>
<tr>
<td>• <strong>FWD_CNT_APPENDED_BATCH</strong>—Indicates the number of email links added to a batch waiting for upload to WildFire.</td>
</tr>
<tr>
<td>• <strong>FWD_CNT_LOCAL_FILE</strong>—Indicates the total number of email links uploaded to WildFire.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verify that a specific sample was forwarded by the firewall and check that status of that sample.</th>
</tr>
</thead>
<tbody>
<tr>
<td>This option can be helpful when troubleshooting to:</td>
</tr>
<tr>
<td>• Confirm that samples that have not yet received a WildFire verdict were correctly forwarded by the firewall. Because <strong>WildFire Submissions</strong> are logged on the firewall only when WildFire analysis is complete and the sample has received a WildFire verdict, use this option to verify the firewall forwarded a sample that is currently undergoing WildFire analysis.</td>
</tr>
<tr>
<td>• Track the status for a single file or email link that was allowed according to your security policy, matched to a WildFire Analysis profile, and then forwarded for WildFire analysis.</td>
</tr>
<tr>
<td>• Check that a firewall in a <strong>WildFire Hybrid Cloud</strong> deployment is forwarding the correct file types and email links to either the WildFire public cloud or a WildFire private cloud.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Execute the following CLI commands on the firewall to view samples the firewall has forwarded WildFire analysis:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• View all samples forwarded by the firewall by with the CLI command <code>debug wildfire upload-log</code>.</td>
</tr>
<tr>
<td>• View only samples forwarded to the WildFire public cloud with the CLI command <code>debug wildfire upload-log channel public</code>.</td>
</tr>
<tr>
<td>• View only samples forwarded to the WildFire private cloud with the CLI command <code>debug wildfire upload-log channel private</code>.</td>
</tr>
</tbody>
</table>

The following example shows the output for the three commands listed above when issued on a firewall in a WildFire public cloud deployment:

```
user@firewall> debug wildfire upload-log channel public
Public Cloud upload logs:
```

```
0:1, filename: support-login.svf
processed 363950 seconds ago, action: skipped - remote benign dup
vpi_id: 1, session_id: 36456, transaction_id: 260
file_len: 51156, flags: 0x010, file_type: Flash
thread_id: 52146, start: 1276, end: 872
from XX.XX.XX.XX/XXX to XX.XX.XX.XX/XXX
SHA256: 62f1a236073a9db94a7707ccf88d83ac96a7da4494c63ba90badf0250b3b84d9d
```

```
0:1, filename: GSN_B Because_12.03.2014_900x350.svf
processed 711500 seconds ago, action: skipped - remote benign dup
vpi_id: 1, session_id: 239049, transaction_id: 260
file_len: 39206, flags: 0x010, file_type: Flash
thread_id: 52145, start: 20853, end: 272
from XX.XX.XX.XX/XXX to XX.XX.XX.XX/XXX
SHA256: c552e212be7422a3a257c1831ed2f1633275ece9856a500d9b70f733233e5d6e7
```
<table>
<thead>
<tr>
<th>Verify File Forwarding (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor samples successfully submitted for WildFire analysis.</td>
</tr>
</tbody>
</table>

Using the firewall web interface, select **Monitor > Logs > WildFire Submissions**. All files forwarded by a firewall to the WildFire public or private cloud for analysis are logged on the WildFire Submissions page.

- **Check the WildFire verdict for a sample:**
  By default, only samples that receive malware verdicts are displayed as **WildFire Submissions** entries. To enable logging for benign and/or grayware samples, select **Device > Setup > WildFire > Report Benign Files/ Report Grayware Files**.

  Enable logging for benign files as a quick troubleshooting step to verify that the firewall is forwarding files. Check the **WildFire Submissions** logs to verify that files are being submitted for analysis and receiving WildFire verdicts (in this case, a benign verdict).

- **Confirm the analysis location for a sample:**
  The **WildFire Cloud** column displays the location to which the file was forwarded and where it was analyzed (public cloud or private cloud). This is useful when deploying a **WildFire Hybrid Cloud**.
Manually Upload Files to the WildFire Portal

All Palo Alto Networks customers with a support account can use the Palo Alto Networks WildFire portal to manually submit up to five samples a day for WildFire analysis. If you have a WildFire subscription, you can manually submit samples to the portal as part of your 1000 sample uploads daily limit; however, keep in mind that the 1000 sample daily limit also includes WildFire API submissions.

### Upload Samples the WildFire Portal

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Manually upload files or URLs to the WildFire portal for analysis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Click <strong>Upload Sample</strong> on the menu bar.</td>
</tr>
<tr>
<td></td>
<td>• To submit files for analysis, select <strong>File Upload</strong> and <strong>Open</strong> the files you want to submit for WildFire analysis. Click <strong>Start</strong> to begin WildFire analysis of a single file, or click <strong>Start Upload</strong> to submit all the files you added for WildFire analysis.</td>
</tr>
<tr>
<td></td>
<td>• To submit a URL for analysis, click <strong>URL Upload</strong>, enter a URL, and <strong>Submit</strong> for WildFire analysis.</td>
</tr>
<tr>
<td>3.</td>
<td>Close the <strong>Uploaded File Information</strong> pop-up.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>View the WildFire verdict and analysis results for the file.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WildFire takes approximately five minutes to complete a file analysis.</td>
</tr>
<tr>
<td></td>
<td>Because a manual upload is not associated with a specific firewall, manual uploads do not show session information in the reports.</td>
</tr>
<tr>
<td>2.</td>
<td>In the Previous 1 Hour section, select <strong>Manual</strong> under the source column to view analysis information for the latest manually-submitted samples.</td>
</tr>
<tr>
<td>3.</td>
<td>Find the files or URLs you uploaded and click the detail icon to the left of the Received Time.</td>
</tr>
</tbody>
</table>
Submit Malware or Reports from the WF-500 Appliance

Enable the WF-500 appliance cloud intelligence feature to automatically submit malware samples discovered in the WildFire private cloud to the WildFire public cloud. The WildFire public cloud further analyzes the malware and generates a signature to identify the sample. The signature is then added to WildFire signature updates, and distributed to global users to prevent future exposure to the threat. If you do not want to forward malware samples outside of your network, you can instead choose to submit only WildFire reports for the malware discovered on your network to contribute to WildFire statistics and threat intelligence.

### Enable the WF-500 Appliance to Submit Malware or Reports to the WildFire Public Cloud

- **Submit Malware to the WildFire Public Cloud**
  
  Execute the following CLI command from the WF-500 appliance to enable the appliance to automatically submit malware samples to the WildFire public cloud:

  `admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes`

  If the firewall that originally submitted the sample for WildFire private cloud analysis has packet captures (PCAPs) enabled, the PCAPs for the malware will also be forwarded to the WildFire public cloud.

- **Submit Malware Reports to the WildFire Public Cloud**
  
  If the WF-500 appliance is enabled to Submit Malware to the WildFire Public Cloud, you do not need to also enable the appliance to submit malware reports to the public cloud. When malware is submitted to the WildFire public cloud, the public cloud generates a new malware report for the sample.

  To enable the WF-500 appliance to automatically submit malware reports to the WildFire public cloud (and not the malware sample), execute the following CLI command on the WF-500 appliance:

  `admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-report yes`

- **Verify Cloud Intelligence Settings**
  
  Check to confirm that cloud intelligence is enabled to either submit malware or submit malware reports to the WildFire public cloud by running the following command:

  `admin@WF-500> show wildfire status`

  Refer to the Submit sample and Submit report fields.
Firewall File Forwarding Capacity by Platform

File forwarding capacity is the maximum rate per minute at which each Palo Alto Networks firewall platform can submit files to the WildFire cloud or a WF-500 appliance for analysis. If the firewall reaches the per-minute limit, it queues any remaining samples.

The Reserved Drive Space column in the following table lists the amount of drive space on the firewall that is reserved for queuing files. If the firewall reaches the drive space limit, it cancels forwarding of new files to WildFire until more space in the queue is available.

The speed at which the firewall can forward files to WildFire also depends on the bandwidth of the upload link to the WildFire systems.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Maximum Files Per Minute</th>
<th>Reserved Drive Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-100</td>
<td>5</td>
<td>100MB</td>
</tr>
<tr>
<td>VM-200</td>
<td>10</td>
<td>200MB</td>
</tr>
<tr>
<td>VM-300</td>
<td>20</td>
<td>200MB</td>
</tr>
<tr>
<td>PA-200</td>
<td>5</td>
<td>100MB</td>
</tr>
<tr>
<td>PA-500</td>
<td>10</td>
<td>200MB</td>
</tr>
<tr>
<td>PA-2000 Series</td>
<td>20</td>
<td>200MB</td>
</tr>
<tr>
<td>PA-3020</td>
<td>50</td>
<td>200MB</td>
</tr>
<tr>
<td>PA-3050/3060</td>
<td>50</td>
<td>500MB</td>
</tr>
<tr>
<td>PA-4020</td>
<td>20</td>
<td>200MB</td>
</tr>
<tr>
<td>PA-4050/4060</td>
<td>50</td>
<td>500MB</td>
</tr>
<tr>
<td>PA-5000 Series</td>
<td>50</td>
<td>500MB</td>
</tr>
<tr>
<td>PA-7000 Series</td>
<td>100</td>
<td>1GB</td>
</tr>
</tbody>
</table>
Monitor WildFire Activity

Depending on your WildFire® deployment—public, private, or hybrid—you can view samples submitted to WildFire and analysis results for each sample using the WildFire portal, by accessing the firewall that submitted the sample (or Panorama, if you are centrally managing multiple firewalls), or by using the WildFire API.

After WildFire has analyzed a sample and delivered a verdict of malware, grayware, or benign, a detailed analysis report is generated for the sample. WildFire analysis reports viewed on the firewall that submitted the sample also include details for the session during which the sample was detected. For samples identified as malware, the WildFire analysis report includes details on existing WildFire signatures that might be related to the newly-identified malware and information on file attributes, behavior, and activity that indicated the sample was malicious.

See the following topics for details on how to monitor WildFire submissions, to WildFire analysis reports for samples, and to set up alerts and notifications based on submissions and analysis results:

▲ About WildFire Logs and Reporting
▲ Use the Firewall to Monitor Malware
▲ Use the WildFire Portal to Monitor Malware
▲ WildFire Analysis Reports—Close Up
▲ WildFire Example

The AutoFocus threat intelligence portal provides a different lens through which to view WildFire analysis details for a sample. AutoFocus layers statistics over WildFire analysis data to indicate high-risk artifacts found during sample analysis (such as an IP address or a domain).
About WildFire Logs and Reporting

You can Monitor WildFire Activity on the firewall, with the WildFire portal, or with the WildFire API.

For each sample WildFire analyzes, WildFire categorizes the sample as malware, grayware, or benign and details sample information and behavior in the WildFire analysis report. WildFire analysis reports can be found on the firewall that submitted the sample and the WildFire cloud (public or private) that analyzed the sample, or can be retrieved using the WildFire API:

- **On the firewall**—All samples submitted by a firewall for WildFire analysis are logged as WildFire Submissions entries (Monitor > WildFire Submissions). For each WildFire submission entry you can open a detailed log view to view the WildFire analysis report for the sample or to download the report as a PDF.

- **On the WildFire portal**—Monitor WildFire activity, including the WildFire analysis report for each sample, which can also be downloaded as a PDF. In a WildFire private cloud deployment, the WildFire portal provides details for samples that are manually uploaded to the portal and samples submitted by a WF-500 appliance with cloud intelligence enabled.

  The option to view WildFire analysis reports on the portal is only supported for WF-500 appliances with the cloud intelligence feature is enabled.

- **With the WildFire API**—Retrieve WildFire analysis reports from a WF-500 appliance or from the WildFire public cloud.
Use the Firewall to Monitor Malware

Samples forwarded by the firewall are added as entries to the WildFire Submissions logs. A detailed WildFire analysis report is displayed in the expanded view for each WildFire Submissions entry.

Configure WildFire Submissions Log Settings

Configure the following options for WildFire Submissions logs:

- Enable Logging for Benign and Grayware Samples
- Include Email Header Information in WildFire Logs and Reports
- Include User-ID Information in WildFire Logs and Reports

Enable Logging for Benign and Grayware Samples

Logging for benign and grayware samples is disabled by default. Email links that receive benign or grayware verdicts are not logged.

Include Email Header Information in WildFire Logs and Reports

Use the following steps to include email header information—email sender, recipient(s), and subject—in WildFire logs and reports.

Session information is forwarded to the WildFire cloud along with the sample, and used to generate the WildFire analysis report. Neither the firewall nor the WildFire cloud receive, store, or view actual email contents.

Include Email Header Information in WildFire Logs and Reports

Step 1 Select Device > Setup > WildFire.

Session information can help you to quickly track down and remediate threats detected in email attachments or links, including how to identify recipients who have downloaded or accessed malicious content.
Include Email Header Information in WildFire Logs and Reports

Step 2 Edit the Session Information Settings section and enable one or more of the options (Email sender, Email recipient, and Email subject).

Step 3 Click OK to save.

Include User-ID Information in WildFire Logs and Reports

Enable the firewall to match User-ID information with email header information, so that the User-ID for the recipient of a malicious email attachment or link is identified for a WildFire entry.

Include User-ID Information in WildFire Logs and Reports

Step 1 Select Device > User Identification > Group Mapping Settings.

Step 2 Select the desired group mapping profile to modify it.

Step 3 In the Server Profile tab in the Mail Domains section, populate the Domain List field:

- **Mail Attributes**—This field is automatically populated after you fill in the Domain List field and click OK. The attributes are based on your LDAP server type (Sun/RFC, Active Directory, and Novell).
- **Domain List**—Enter the list of email domains in your organization using a comma separated list up to 256 characters.

When email header information is matched to a User-ID, the Recipient User-ID field in the Email Headers section of the detailed log view will link to a filtered ACC for that user or user group.

![Diagram showing the detailed log view with emphasis on Email Headers.](image-url)
Monitor WildFire Submissions and Analysis Reports

Samples that firewalls submit for WildFire analysis are displayed as entries in the **WildFire Submissions** log on the firewall web interface. For each WildFire entry, you can open an expanded log view which displays log details and the WildFire analysis report for the sample.

**Monitor WildFire Submissions and Reports**

**Step 1**  Forward Files for WildFire Analysis.

**Step 2**  Configure WildFire Submissions Log Settings.

**Step 3**  To view samples submitted by a firewall to a WildFire public, private, or hybrid cloud, select **Monitor > WildFire Submissions**. When WildFire analysis of a sample is complete, the results are sent back to the firewall that submitted the sample and are accessible in the WildFire Submissions logs. The Verdict column indicates whether the sample is benign, malicious, or grayware.
Monitor WildFire Submissions and Reports (Continued)

Step 4 For any entry, select the Log Details icon to open a detailed log view for each entry:

The detailed log view displays Log Info and the WildFire Analysis Report for the entry. If the firewall has packet captures (PCAPs) enabled, the sample PCAPs are also displayed.

For all samples, the WildFire analysis report displays file and session details. For malware samples, the WildFire analysis report is extended to include details on the file attributes and behavior that indicated the file was malicious.

Step 5 (Optional) Download PDF of the WildFire Analysis Report.
Set Up Alerts for Malware

You can configure a Palo Alto Networks firewall to send an alert when WildFire identifies a malicious file or email link. You can configure alerts for benign and grayware files as well, but not for benign and grayware email links. This example describes how to configure an email alert; however, you could also configure log forwarding to set up alerts to be delivered as syslog messages, SNMP traps, or Panorama alerts.

**Set Up Email Alerts for Malware**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure an email server profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Device &gt; Server Profiles &gt; Email</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Add</strong> and then enter a <strong>Name</strong> for the profile. For example, WildFire-Email-Profile.</td>
</tr>
<tr>
<td>3.</td>
<td><em>(Optional)</em> Select the virtual system to which this profile applies from the <strong>Location</strong> drop-down.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Add</strong> to add a new email server entry and enter the information required to connect to the Simple Mail Transport Protocol (SMTP) server and send email (up to four email servers can be added to the profile):</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server</strong>—Name to identify the mail server (1-31 characters). This field is just a label and does not have to be the host name of an existing SMTP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Display Name</strong>—The name to show in the From field of the email.</td>
</tr>
<tr>
<td></td>
<td>• <strong>From</strong>—The email address where notification emails are sent from.</td>
</tr>
<tr>
<td></td>
<td>• <strong>To</strong>—The email address to which notification emails are sent.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Additional Recipient(s)</strong>—Enter an email address to send notifications to a second recipient.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gateway</strong>—The IP address or host name of the SMTP gateway to use to send the emails.</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>OK</strong> to save the server profile.</td>
</tr>
<tr>
<td>6.</td>
<td>Click <strong>Commit</strong> to save the changes to the running configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Test the email server profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Monitor &gt; PDF Reports &gt; Email Scheduler</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Add</strong> and select the new email profile from the <strong>Email Profile</strong> drop-down.</td>
</tr>
<tr>
<td>3.</td>
<td>Click the <strong>Send test</strong> email button and a test email should be sent to the recipients defined in the email profile.</td>
</tr>
</tbody>
</table>
### Set Up Email Alerts for Malware (Continued)

**Step 3** Configure a log forwarding profile, to enable WildFire logs to be forwarded to Panorama, an email account, SNMP, and/or a syslog server.

In this example you will set up email logs for when a sample is determined to be malicious. You can also enable Benign and Grayware logs to be forwarded, which will produce more activity if you are testing.

1. Select **Objects > Log Forwarding**.
2. **Add** and name the profile, for example, WildFire-Log-Forwarding.
3. In **WildFire Settings**, choose the email profile from the Email column for **Malicious** as shown below.

   ![Log Forwarding Profile](image)

   To forward logs to Panorama, select the check boxes under the Panorama column for Benign, Grayware, and/or Malicious. For SNMP and Syslog, select the drop-down and choose the appropriate profile or click **New** to configure a new profile.

4. Click **OK** to save the changes.

**Step 4** Add the log forwarding profile to a security policy being used for WildFire forwarding (with a WildFire Analysis profile attached).

The WildFire Analysis profile defines the traffic that the firewall forwards for WildFire analysis. To set up a WildFire analysis profile and attach it to a security policy rule, see **Forward Files for WildFire Analysis**.

1. Select **Policies > Security** and click on the policy that is used for WildFire forwarding.
2. In the **Actions** tab **Log Setting** section, select the **Log Forwarding** profile you configured.
3. Click **OK** to save the changes and then **Commit** the configuration.
Use the WildFire Portal to Monitor Malware

Log in to the Palo Alto Networks WildFire portal using your Palo Alto Networks support credentials or your WildFire account. The portal opens to display the dashboard, which lists summary report information for all of the firewalls associated with the specific WildFire subscription or support account. For each device listed, the portal displays statistics for the number of malware samples that have been detected, benign samples that have been analyzed, and the number of pending files that are waiting to be analyzed. Your WildFire portal account displays data for all samples submitted by firewalls on your network that are connected to the WildFire public cloud, as well as data for samples manually submitted to the portal. Additionally, if you have enabled a WF-500 appliance to forward malware to the WildFire public cloud for signature generation and distribution, reports for those malware samples can also be accessed on the portal.

See the following sections for details on using the WildFire portal to monitor WildFire activity:

- Configure WildFire Portal Settings
- Add WildFire Portal Users
- View Reports on the WildFire Portal

Configure WildFire Portal Settings

This section describes the settings that can be customized for a WildFire cloud account, such as time zone and email notifications for each firewall connected to the account. You can also delete firewall logs stored in the cloud.

<table>
<thead>
<tr>
<th>Customize the WildFire Portal Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Use the WildFire Portal to Monitor Malware

Monitor WildFire Activity

Customize the WildFire Portal Settings (Continued)

Step 4  (Optional) Configure email notifications based on WildFire analysis verdicts.

1. In the Configure Alerts section, select Malware, Grayware, and/or Benign check boxes to receive email notifications based on those verdicts:
   - Select the verdict check boxes in the All row to receive verdict notifications for all samples uploaded to the WildFire cloud.
   - Select the verdict check boxes in the Manual row to receive verdict notifications for all samples that are manually uploaded to the WildFire public cloud using the WildFire portal.
   - Select the verdict check boxes for one or several firewall serial numbers to receive verdict notifications for samples submitted by those firewalls.

2. Select Update Notification to enable verdict notifications to be emailed to the email address associated with your support account.

Add WildFire Portal Users

WildFire portal accounts are created by a super user (the registered owner of a Palo Alto Networks device) to give additional users the ability to log in to the WildFire cloud and view device data for which they are granted access by the super user. A WildFire user can be a user associated with an existing Palo Alto Networks account or a user not associated with a Palo Alto Networks support account, to whom you can allow access to just the WildFire public clouds and a specific set of firewall data.

Add WildFire Portal Users

Step 1  Select the account for which you want to add users who can access the WildFire portal.

1. Log in to the Palo Alto Networks Support Portal.
2. Under Manage Account, click on Users and Accounts.
3. Select an existing account or sub-account.

Step 2  Add a WildFire user.

1. Click Add WildFire User.
2. Enter the email address for the user you would like to add. The only restriction when adding a user is that the email address cannot be from a free web-based email account (such as Gmail, Hotmail, and Yahoo). If an email address is entered for a domain that is not supported, a pop-up warning is displayed.
Monitor WildFire Activity

Use the WildFire Portal to Monitor Malware

Add WildFire Portal Users (Continued)

**Step 3** Assign firewalls to the new user account and access the WildFire cloud.

Select the firewall(s) by serial number for which you want to grant access and fill out the optional account details. Users with an existing support account will receive an email with a list of the firewalls that are now available for WildFire report viewing. If the user does not have a support account, the portal sends an email with instructions on how to access the portal and how to set a new password.

The new user can now log in to the WildFire cloud and view WildFire reports for the firewalls to which they have been granted access. Users can also configure automatic email alerts for these devices in order to receive alerts on files analyzed. They can choose to receive reports on malicious and/or benign files.

---

**View Reports on the WildFire Portal**

The WildFire portal displays reports for samples that are submitted from firewalls, manually uploaded, or uploaded using the WildFire API. Select **Reports** to display the latest reports for samples analyzed by the WildFire cloud. For each sample listed, the report entry shows the date and time the sample was received by the cloud, the serial number of the firewall that submitted the file, the file name or URL, and the verdict delivered by WildFire (benign, grayware, or malware).

Use the search option to search for reports based on the file name or the sample hash value. You can also narrow the results displayed by viewing only reports for samples submitted by a specific **Source** (view only results submitted manually or by a specific firewall) or for samples that received a specific WildFire **Verdict** (any, benign, malware, grayware, or pending).

To view an individual report from the portal, click the **Reports** icon to the left of the report name. To save the detailed report, click the **Download as PDF** button on the upper right of the report page. For details on WildFire analysis reports, see WildFire Analysis Reports—Close Up.

The following shows a list of sample files submitted by a specific firewall:
WildFire Analysis Reports—Close Up

Access WildFire analysis reports on the firewall, the WildFire portal, and the WildFire API.

WildFire analysis reports display detailed sample information, as well as information on targeted users, email header information (if enabled), the application that delivered the file, and all URLs involved in the delivery or phone-home activity of the file. WildFire reports contain some or all of the information described in the following table based on the session information configured on the firewall that forwarded the file and depending on the observed behavior for the file.

When viewing a WildFire report for a file that was manually uploaded to the WildFire portal or by using the WildFire API, the report will not show session information because the traffic did not traverse the firewall. For example, the report would not show the Attacker/Source and Victim/Destination.

<table>
<thead>
<tr>
<th>Report Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Information</td>
<td>• <strong>File Type</strong>—Flash, PE, PDF, APK, JAR/Class, archive, linux, or MS Office. This field is named URL for HTTP/HTTPS email link reports and will display the URL that was analyzed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>File Signer</strong>—The entity that signed the file for authenticity purposes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hash Value</strong>—A file hash is much like a fingerprint that uniquely identifies a file to ensure that the file has not been modified in any way. The following lists the hash versions that WildFire generates for each file analyzed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA-1</strong>—Displays the SHA-1 value for the file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA-256</strong>—Displays the SHA-256 value for the file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MD5</strong>—Displays the MD5 information for the file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>File Size</strong>—The size (in bytes) of the file that WildFire analyzed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>First Seen Timestamp</strong>—If the WildFire system has analyzed the file previously, this is the date/time that it was first observed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Verdict</strong>—Displays the analysis verdict:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Benign</strong>—The file is safe and does not exhibit malicious behavior.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Grayware</strong>—The file behaves similarly to malware, but does not pose a direct security threat. Grayware includes executables that display obtrusive behavior, but are not malicious in intent or nature. Examples of grayware include adware, spyware, and Browser Helper Objects (BHOs).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Malware</strong>—WildFire identified the file as malware and generates a signature to protect against future exposure.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sample File</strong>—Click the Download File link to download the sample file to your local system. Note that you can only download files with the malware verdict, not benign.</td>
</tr>
</tbody>
</table>
Monitor WildFire Activity

WildFire Analysis Reports—Close Up

<table>
<thead>
<tr>
<th>Report Heading</th>
<th>Description</th>
</tr>
</thead>
</table>
| Coverage Status    | Click the **Virus Total** link to view endpoint antivirus coverage information for samples that have already been identified by other vendors. If the file has never been seen by any of the listed vendors, file not found appears. In addition, when the report is rendered on the firewall, up-to-date information about what signature and URL filtering coverage that Palo Alto Networks currently provides to protect against the threat will also be displayed in this section. Because this information is retrieved dynamically, it will not appear in the PDF report. The following coverage information is provided for active signatures:  
• **Coverage Type**—The type of protection provided by Palo Alto Networks (virus, DNS, WildFire, or malware URL).  
• **Signature ID**—A unique ID number assigned to each signature that Palo Alto Networks provides.  
• **Detail**—The well-known name of the virus.  
• **Date Released**—The date that Palo Alto Networks released coverage to protect against the malware.  
• **Latest Content Version**—The version number for the content release that provides protection against the malware. |
| Session Information| Contains session information based on the traffic as it traversed the firewall that forwarded the sample. To define the session information that WildFire will include in the reports, select **Device > Setup > WildFire> Session Information Settings**. The following options are available:  
• Source IP  
• Source Port  
• Destination IP  
• Destination Port  
• Virtual System (If multi-vsyst is configured on the firewall)  
• Application  
• User (If User-ID is configured on the firewall)  
• URL  
• Filename  
• Email sender  
• Email recipient  
• Email subject |
| Dynamic Analysis   | If a file is low risk and WildFire can easily determine that it is safe, only a static analysis is performed, instead of a dynamic analysis. When a dynamic analysis is performed, this section contains tabs for each virtual environment that the sample was run in when it was analyzed in the WildFire cloud. For example, Virtual Machine 1 tab may have Windows XP, Adobe Reader 9.3.3, and Office 2003 and Virtual Machine 2 may have similar attributes, but with Office 2007. When a file goes through a full dynamic analysis, it is run in each virtual machine and the results of each environment can be viewed by clicking any of the Virtual Machine tabs. On the WF-500 appliance, only one virtual machine is used for the analysis, which you select based on virtual environment attributes that best match your local environment. For example, if most users have Windows 7 32-bit, that virtual machine would be selected. |

© Palo Alto Networks, Inc. WildFire 7.1 Administrator’s Guide • 67
WildFire Analysis Reports—Close Up

Monitor WildFire Activity

### Behavior Summary

Each Virtual Machine tab summarizes the behavior of the sample file in the specific environment. Examples include whether the sample created or modified files, started a process, spawned new processes, modified the registry, or installed browser helper objects.

The Severity column indicates the severity of each behavior. The severity gauge will show one bar for low severity and additional bars for higher severity levels. This information is also added to the dynamic and static analysis sections.

The following describes the various behaviors that are analyzed:

- **Network Activity**—Shows network activity performed by the sample, such as accessing other hosts on the network, DNS queries, and phone-home activity. A link is provided to download the packet capture.

- **Host Activity (by process)**—Lists activities performed on the host, such as registry keys that were set, modified, or deleted.

- **Process Activity**—Lists files that started a parent process, the process name, and the action the process performed.

- **File**—Lists files that started a child process, the process name, and the action the process performed.

- **Mutex**—If the sample file generates other program threads, the mutex name and parent process is logged in this field.

- **Activity Timeline**—Provides a play-by-play list of all recorded activity of the sample. This will help in understanding the sequence of events that occurred during the analysis.

The activity timeline information is only available in the PDF export of the WildFire reports.

### Submit Malware

Use this option to manually submit the sample to Palo Alto Networks. The WildFire cloud will then re-analyze the sample and generate a signatures if it determines that the sample is malicious. This is useful on a WF-500 appliance that does not have signature generation or cloud intelligence enabled, which is used to forward malware from the appliance to the WildFire cloud.

### Report an Incorrect Verdict

Click this link to submit the sample to the Palo Alto Networks threat team if you feel the verdict is a false positive or false negative. The threat team will perform further analysis on the sample to determine if it should be reclassified. If a malware sample is determined to be safe, the signature for the file is disabled in an upcoming antivirus signature update or if a benign file is determined to be malicious, a new signature is generated. After the investigation is complete, you will receive an email describing the action that was taken.
WildFire Example

The following example scenario summarizes the full WildFire® lifecycle. In this example, a sales representative from Palo Alto Networks downloads a new software sales tool that a sales partner uploaded to Dropbox. The sales partner unknowingly uploaded an infected version of the sales tool install file and the sales rep then downloads the infected file.

This example will demonstrate how a Palo Alto Networks firewall in conjunction with WildFire can discover zero-day malware downloaded by an end user, even if the traffic is SSL encrypted. After WildFire identifies the malware a log is sent to the firewall and the firewall alerts the administrator who then contacts the user to eradicate the malware. WildFire then generates a new signature for the malware and firewalls with a Threat Prevention or WildFire subscription automatically downloads the signature to protect against future exposure. Although some file sharing web sites have an antivirus feature that checks files as they are uploaded, they can only protect against known malware.

This example uses a web site that uses SSL encryption. In this case, the firewall has decryption enabled, including the option to forward decrypted content for analysis. To enable decrypted content to be forwarded to the WildFire cloud, see Forward Files for WildFire Analysis.

**WildFire Example**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>The sales person from the partner company uploads a sales tool file named sales-tool.exe to his Dropbox account and then sends an email to the Palo Alto Networks sales person with a link to the file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>The Palo Alto sales person receives the email from the sales partner and clicks the download link, which takes her to the Dropbox site. She then clicks Download to save the file to her desktop.</td>
</tr>
</tbody>
</table>
WildFire Example (Continued)

Step 3  
The firewall that is protecting the Palo Alto sales rep has a WildFire Analysis profile rule attached to a security policy rule that will look for files in any application that is used to download or upload any of the supported file types. The firewall can also be configured to forward the email-link file type, which enables the firewall to extract HTTP/HTTPS links contained in SMTP and POP3 email messages. As soon as the sales rep clicks download, the firewall forwards the sales-tool.exe file to WildFire, where the file is analyzed for zero-day malware. Even though the sales rep is using Dropbox, which is SSL encrypted, the firewall is configured to decrypt traffic, so all traffic can be inspected. The following screen shots show the WildFire Analysis profile rule, the security policy rule configured with the WildFire analysis profile rule attached, and the option to allow forwarding of decrypted content enabled.

Step 4  
At this point, WildFire has received the file and is analyzing it for more than 200 different malicious behaviors. **Verify File Forwarding** to check that the firewall has correctly forwarded a file or email links for WildFire analysis.
Monitor WildFire Activity

WildFire Example

Step 5  Within approximately five minutes, WildFire has completed the file analysis and then sends a WildFire log back to the firewall with the analysis results. In this example, the WildFire log shows that the file is malicious.

Step 6  The firewall is configured with a log forwarding profile that will send WildFire alerts to the security administrator when malware is discovered.
WildFire Example (Continued)

Step 7  The security administrator identifies the user by name (if User-ID is configured), or by IP address if User-ID is not enabled. At this point, the administrator can shut down the network or VPN connection that the sales representative is using and will then contact the desktop support group to work with the user to check and clean the system.

By using the WildFire detailed analysis report, the desktop support person can determine if the user system is infected with malware by looking at the files, processes, and registry information detailed in the WildFire analysis report. If the user runs the malware, the support person can attempt to clean the system manually or re-image it.

For details on the WildFire report fields, see WildFire Analysis Reports—Close Up.

**FILE INFORMATION**

<table>
<thead>
<tr>
<th>File Type</th>
<th>PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-256</td>
<td>8c10655a42bc8943c70b5f6066f737a01777406fa72025738a851a66588e5020</td>
</tr>
<tr>
<td>MD5</td>
<td>1b656532e34c52b36e5e202f7f121ed729951086</td>
</tr>
<tr>
<td>File Size</td>
<td>122880 bytes</td>
</tr>
<tr>
<td>First Seen Timestamp</td>
<td>2011-10-28 21:15:58 UTC</td>
</tr>
<tr>
<td>Verdict</td>
<td>Malware</td>
</tr>
</tbody>
</table>

**SESSION INFORMATION**

| File Source  | 60.1.13.47361 |
| File Destination | 10.154.10.90.26 |
| User-ID       | unknown |
| Timestamp     | 2016-01-12 18:15:58 UTC |
| Serial Number | 007200000024 |
| Email Sender  | eywe4EUEVRV7u904INYVOCTjMjGMnXOAPUzzGBmAERO.org |
| Email Recipient | 693438EoOQ@3ozj2oLtgihOUMjPc.us |
| Email Subject | PCTSUIfV559KRDvauM31VjRyu/ApprovBeRT |
| Firewall Hostname/IP | [/T-9/16] |
| Virtual System | 1 |
| Application   | smtp |
| URL           | unknown |
| File Name     | utzX3M44a |

**COVERAGE STATUS**

The table below lists all coverage related to this malware sample. For endpoint antivirus coverage information for this sample, visit VirusTotal

<table>
<thead>
<tr>
<th>Coverage Type</th>
<th>Signature ID</th>
<th>Detail</th>
<th>Date Released</th>
<th>Latest Content Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>virus</td>
<td>2005655</td>
<td>WomWin32 Rootайл</td>
<td>2011-07-25 17:04:05</td>
<td>1674</td>
</tr>
<tr>
<td>wildfire</td>
<td>3007347</td>
<td>WomWin32 Rootайл</td>
<td>2012-03-21 15:30:59</td>
<td>83181</td>
</tr>
</tbody>
</table>
Step 8  Now that the administrator has identified the malware and the user system is being checked, how do you protect from future exposure? Answer: In this example, the administrator set a schedule on the firewall to download and install WildFire signatures every 15 minutes and to download and install Antivirus updates once per day. In less than an hour and a half after the sales rep downloaded the infected file, WildFire identified the zero-day malware, generated a signature, added it to the WildFire update signature database provided by Palo Alto Networks, and the firewall downloaded and installed the new signature. This firewall and any other Palo Alto Networks firewall configured to download WildFire and antivirus signatures is now protected against this newly discovered malware. The following screenshot shows the WildFire update schedule:

All of this occurs well before most antivirus vendors are even aware of the zero-day malware. In this example, within a very short period of time, the malware is no longer considered zero-day because Palo Alto Networks has already discovered it and has provided protection to customers to prevent future exposure.
Use the WildFire API

The WildFire® API enables you to send file analysis jobs to WildFire and query for report data through a simple XML API interface and is supported on the WildFire public cloud and for the WF-500 appliance. See the WildFire API Reference for details on using the WildFire API.
Use the WildFire API
Use the WF-500 Appliance CLI

This section describes the CLI commands that are specific to the WildFire® appliance software. All other commands, such as configuring interfaces, committing the configuration, and setting system information are identical to PAN-OS and are also shown in the hierarchy. For information on the PAN-OS commands, refer to the PAN-OS 7.1 CLI Quick Start.

▲ WF-500 Appliance Software CLI Concepts
▲ WildFire CLI Command Modes
▲ Access the WF-500 Appliance CLI
▲ Use the WF-500 Appliance CLI
▲ WF-500 Appliance Configuration Mode Command Reference
▲ WF-500 Appliance Operational Mode Command Reference
WF-500 Appliance Software CLI Concepts

This section introduces and describes how to use the WF-500 appliance software command line interface (CLI):

- WF-500 Appliance Software CLI Structure
- WF-500 Appliance Software CLI Command Conventions
- WF-500 Appliance CLI Command Messages
- WF-500 Appliance Command Option Symbols
- WF-500 Appliance Privilege Levels

WF-500 Appliance Software CLI Structure

The WF-500 appliance software CLI is used to manage the appliance. The CLI is the only interface to the appliance. Use it to view status and configuration information and modify the appliance configuration. Access the WF-500 appliance software CLI over SSH or by direct console access using the console port.

The WF-500 appliance software CLI operates in two modes:

- **Operational mode**—View the state of the system, navigate the WF-500 appliance software CLI, and enter configuration mode.
- **Configuration mode**—View and modify the configuration hierarchy.

WF-500 Appliance Software CLI Command Conventions

The basic command prompt incorporates the user name and hostname of the appliance:

```
username@hostname>
```

**Example:**

```
admin@WF-500>
```

When entering Configuration mode, the prompt changes from > to #:

```
username@hostname>(Operational mode)
```

```
username@hostname> configure
```

Entering configuration mode

```
[edit]
```

```
username@hostname# (Configuration mode)
```

In Configuration mode, the current hierarchy context is shown by the [edit...] banner presented in square brackets when a command is issued.
WF-500 Appliance CLI Command Messages

Messages may be displayed when issuing a command. The messages provide context information and can help in correcting invalid commands. In the following examples, the message is shown in bold.

Example: Unknown command
username@hostname# **application-group**
Unknown command: application-group
[edit network]
username@hostname#

Example: Changing modes
username@hostname# **exit**
Exiting configuration mode
username@hostname>

Example: Invalid syntax
username@hostname> **debug** 17
Unrecognized command
Invalid syntax.
username@hostname>

The CLI checks the syntax of each command. If the syntax is correct, it executes the command and the candidate hierarchy changes are recorded. If the syntax is incorrect, an invalid syntax message is presented, as in the following example:

username@hostname# **set deviceconfig setting wildfire cloud-intelligence submit-sample yes**
Unrecognized command
Invalid syntax.
[edit]
username@hostname#
WF-500 Appliance Command Option Symbols

The symbol preceding an option can provide additional information about command syntax.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>This option is required.</td>
</tr>
<tr>
<td>&gt;</td>
<td>There are additional nested options for this command.</td>
</tr>
<tr>
<td>+</td>
<td>There are additional command options for this command at this level.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>Although the double quote is not a command option symbol, it must be used when entering multi-word phrases in CLI commands. For example, to create an address group named Test Group and to add the user named user1 to this group, you must surround the group name with double quotes as follows: set address-group &quot;Test Group&quot; user1. If you do not put a double quote surrounding the group name, the CLI would interpret the word Test as the group name and the following error would be displayed: “test is not a valid name”. A single quote would also be invalid in this example.</td>
</tr>
</tbody>
</table>

The following examples show how these symbols are used.

Example: In the following command, the keyword from is required:

username@hostname> scp import configuration ?
+ remote-port   SSH port number on remote host
* from          Source (username@host:path)
username@hostname> scp import configuration
Example: This command output shows options designated with + and >.
username@hostname# set rulebase security rules rule1 ?
+ action               action
+ application          application
+ destination          destination
+ disabled             disabled
+ from                 from
+ log-end              log-end
+ log-setting          log-setting
+ log-start            log-start
+ negate-destination   negate-destination
+ negate-source        negate-source
+ schedule             schedule
+ service              service
+ source               source
+ to                   to
Use the WF-500 Appliance CLI

> profiles
<Enter>
[edit]
username@hostname# set rulebase security rules rule1

Each option listed with + can be added to the command.

The profiles keyword (with >) has additional options:

username@hostname# set rulebase security rules rule1 profiles ?
+ virus Help string for virus
+ spyware Help string for spyware
+ vulnerability Help string for vulnerability
+ group Help string for group
<Enter> Finish input
[edit]
username@hostname# set rulebase security rules rule1 profiles

WF-500 Appliance Privilege Levels

Privilege levels determine which commands the user is permitted to execute and the information the user is permitted to view.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>superreader</td>
<td>Has complete read-only access to the appliance.</td>
</tr>
<tr>
<td>superuser</td>
<td>Has complete read-write access to the appliance.</td>
</tr>
</tbody>
</table>
WildFire CLI Command Modes

The following topics describe the modes used to interact with the WF-500 appliance software CLI:

- WF-500 Appliance CLI Configuration Mode
- WF-500 Appliance CLI Operational Mode

WF-500 Appliance CLI Configuration Mode

Entering commands in configuration mode modifies the candidate configuration. The modified candidate configuration is stored in the appliance memory and maintained while the appliance is running.

Each configuration command involves an action, and may also include keywords, options, and values.

This section describes Configuration mode and the configuration hierarchy:

- Configuration Mode Command Usage
- Configuration Hierarchy
- Navigate the Hierarchy

Configuration Mode Command Usage

Use the following commands to store and apply configuration changes:

- **save**—Saves the candidate configuration in the non-volatile storage on the appliance. The saved configuration is retained until overwritten by subsequent `save` commands. Note that this command does not make the configuration active.
- **commit**—Applies the candidate configuration to the appliance. A committed configuration becomes the active configuration for the device.
- **set**—Changes a value in the candidate configuration.
- **load**—Assigns the last saved configuration or a specified configuration to be the candidate configuration.

> When exiting configuration mode without issuing the `save` or `commit` command, the configuration changes could be lost if the appliance loses power.
Maintaining a candidate configuration and separating the save and commit steps confers important advantages when compared with traditional CLI architectures:

- Distinguishing between the `save` and `commit` concepts allows multiple changes to be made at the same time and reduces system vulnerability.
- Commands can easily be adapted for similar functions. For example, when configuring two Ethernet interfaces, each with a different IP address, you can edit the configuration for the first interface, copy the command, modify only the interface and IP address, and then apply the change to the second interface.
- The command structure is always consistent.

Because the candidate configuration is always unique, all authorized changes to the candidate configuration are consistent with each other.

Configuration Hierarchy

The configuration for the appliance is organized in a hierarchical structure. To display a segment of the current hierarchy level, use the `show` command. Entering `show` displays the complete hierarchy, while entering `show` with keywords displays a segment of the hierarchy. For example, when running the command `show` from the top level of configuration mode, the entire configuration is displayed. When running the command `edit mgt-config` and you enter `show`, or by running `show mgt-config`, only the mgt-config part of the hierarchy displays.
Hierarchy Paths

When entering commands, the path is traced through the hierarchy as follows:

```
  deviceconfig
    setting system ...
    management wildfire ...
    auto-submit cloud-server vm-network-enable ...
    no yes
```

For example, the following command assigns the primary DNS server 10.0.0.246 for the appliance:

```
[edit]
username@hostname# set deviceconfig system dns-setting servers primary 10.0.0.246
```

This command generates a new element in the hierarchy and in the output of the following `show` command:

```
[edit]
username@hostname# show deviceconfig system dns-settings
dns-setting {
  servers {
    primary 10.0.0.246
  }
}
[edit]
username@hostname#
```
Navigate the Hierarchy

The [edit...] banner presented below the Configure mode command prompt line shows the current hierarchy context.

- **[edit]** indicates that the relative context is the top level of the hierarchy, whereas
- **[edit deviceconfig]** indicates that the relative context is at the deviceconfig level.

Use the commands listed in to navigate through the configuration hierarchy.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit</td>
<td>Sets the context for configuration within the command hierarchy.</td>
</tr>
<tr>
<td>up</td>
<td>Changes the context to the next higher level in the hierarchy.</td>
</tr>
<tr>
<td>top</td>
<td>Changes the context to the highest level in the hierarchy.</td>
</tr>
</tbody>
</table>

The `set` command issued after using the `up` and `top` commands starts from the new context.
WF-500 Appliance CLI Operational Mode

At the initial login to the device, the WF-500 appliance software CLI opens in Operational mode. Operational mode commands involve actions that are executed immediately. They do not involve changes to the configuration, and do not need to be saved or committed.

Operational mode commands are of several types:

- **Network access**—Open a window to another host. SSH is supported.
- **Monitoring and troubleshooting**—Perform diagnosis and analysis. Includes `debug` and `ping` commands.
- **Display commands**—Display or clear current information. Includes `clear` and `show` commands.
- **WF-500 appliance software CLI navigation commands**—Enter Configure mode or exit the WF-500 appliance software CLI. Includes `configure`, `exit`, and `quit` commands.
- **System commands**—Make system-level requests or restart. Includes `set` and `request` commands.
Access the WF-500 Appliance CLI

This section describes how to access WF-500 appliance software CLI:

- Establish a Direct Console Connection
- Establish an SSH Connection

Establish a Direct Console Connection

Use the following settings for direct console connection:

- Data rate: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: None

Establish an SSH Connection

To access the WF-500 appliance software CLI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Use terminal emulation software to establish an SSH console connection with the WF-500 appliance.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the administrative user name. The default is admin.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the administrative password. The default is admin. The WF-500 appliance software CLI opens in Operational mode, and the CLI prompt is displayed: <code>username@hostname&gt;</code></td>
</tr>
</tbody>
</table>
Use the WF-500 Appliance CLI

Access WF-500 Appliance Operational and Configuration Modes

When logging in, the WF-500 appliance software CLI opens in Operational mode. You can navigate between Operational and Configuration modes at any time.

- To enter Configuration mode from Operational mode, use the `configure` command:

  ```
  username@hostname> configure
  Entering configuration mode
  [edit]
  username@hostname#
  ```

- To leave Configuration mode and return to Operational mode, use the `quit` or `exit` command:

  ```
  username@hostname# quit
  Exiting configuration mode
  username@hostname>
  ```

To enter an Operational mode command while in Configuration mode, use the `run` command. For example, to show system resources from `configure` mode, use `run show system resources`.

Display WF-500 Appliance Software CLI Command Options

Use `?` (or Meta-H) to display a list of command options, based on context:

- To display a list of operational commands, enter `?` at the command prompt.

  ```
  username@hostname> ?
  clear     Clear runtime parameters
  configure Manipulate software configuration information
  debug     Debug and diagnose
  exit      Exit this session
  grep      Searches file for lines containing a pattern match
  less      Examine debug file content
  ping      Ping hosts and networks
  quit      Exit this session
  request   Make system-level requests
  scp       Use ssh to copy file to another host
  set       Set operational parameters
  show      Show operational parameters
  ssh       Start a secure shell to another host
  tail      Print the last 10 lines of debug file content
  username@hostname>
  ```
Use the WF-500 Appliance CLI

To display the available options for a specified command, enter the command followed by `?`.

Example:

```
username@hostname> ping ?
+ bypass-routing    Bypass routing table, use specified interface
+ count             Number of requests to send (1..2000000000 packets)
+ do-not-fragment   Don't fragment echo request packets (IPv4)
+ inet              Force to IPv4 destination
+ interface         Source interface (multicast, all-ones, unrouted packets)
+ interval          Delay between requests (seconds)
+ no-resolve        Don't attempt to print addresses symbolically
+ pattern           Hexadecimal fill pattern
+ record-route      Record and report packet's path (IPv4)
+ size              Size of request packets (0..65468 bytes)
+ source            Source address of echo request
+ tos               IP type-of-service value (0..255)
+ ttl               IP time-to-live value (IPv6 hop-limit value) (0..255 hops)
+ verbose           Display detailed output
+ wait              Delay after sending last packet (seconds)
<host>              Hostname or IP address of remote host
```

Restrict WF-500 Appliance CLI Command Output

Some operational commands include an option to restrict the displayed output. To restrict the output, enter a pipe symbol followed by `except` or `match` and the value that is to be excluded or included:

Example:

The following sample output is for the show system info command:

```
username@hostname> show system info
hostname: WF-500
ip-address: 192.168.2.20
netmask: 255.255.255.0
default-gateway: 192.168.2.1
mac-address: 00:25:90:95:84:76
vm-interface-ip-address: 10.16.0.20
vm-interface-netmask: 255.255.252.0
vm-interface-default-gateway: 10.16.0.1
vm-interface-dns-server: 10.0.0.247
uptime: 0 days, 0:02:35
family: m
model: WF-500
serial: 009707000118
sw-version: 5.1.0
logdb-version: 5.0.2
platform-family: m
```

The following sample displays only the system model information:
username@hostname> **show system info | match model**
model: WF-500

username@hostname>

**Set the Output Format for WF-500 Appliance Configuration Commands**

Change the output format for the configuration commands by using the `set cli config-output-format` command in Operational mode. Options include the default format, JSON (JavaScript Object Notation), set format, and XML format. The default format is a hierarchal format where configuration sections are indented and enclosed in curly brackets.
WF-500 Appliance Configuration Mode Command Reference

This section contains command reference information for the following Configuration mode commands that are specific to the WF-500 appliance software. All other commands that are part of the WF-500 appliance software are identical to PAN-OS as described in the PAN-OS 7.1 CLI Quick Start.

▲ set deviceconfig setting wildfire
▲ set deviceconfig system update-schedule
▲ set deviceconfig system vm-interface

set deviceconfig setting wildfire

Description

Configure Wildfire settings on the WF-500 appliance. You can configure forwarding of malicious files, define the cloud server that receives malware infected files, and enable or disable the vm-interface.

Hierarchy Location

set deviceconfig settings

Syntax

wildfire {
  active-vm;
  cloud-server <value>;
  vm-network-enable {no | yes};
  vm-network-use-tor {enable | disable};
  cloud-intelligence {
    submit-report {no | yes};
    submit-sample {no | yes};
  }
  signature-generation {
    av {no | yes};
    dns {no | yes};
    url {no | yes};
    {
    }
  }
}
Options

+ active-vm — Select the virtual machine environment that WildFire will use for sample analysis. Each vm has a different configuration, such as Windows XP, a specific versions of Flash, Adobe reader, etc. To view which VM is selected, run the following command: show wildfire status and view the Selected VM field. To view the VM environment information, run the following command: show wildfire vm-images.

+ cloud-server — Hostname for the cloud server that the appliance will forward malicious samples/reports to for a re-analysis. The default cloud server is wildfire-public-cloud. To configure forwarding, use the following command: set deviceconfig setting wildfire cloud-intelligence.

+ vm-network-enable — Enable or disable the vm-network. When enabled, sample files running in the virtual machine sandbox can access the Internet. This helps WildFire better analyze the behavior of the malware to look for things like phone home activity.

+ vm-network-use-tor — Enable or disable the Tor network for the vm-interface. When this option is enabled, any malicious traffic coming from the sandbox systems on the WF-500 appliance during sample analysis is sent through the Tor network. The Tor network will mask your public facing IP address, so the owners of the malicious site cannot determine the source of the traffic.

+ cloud-intelligence — Configure the appliance to submit WildFire reports or samples to the Palo Alto Networks WildFire cloud. The submit report option will send reports for malicious samples to the cloud for statistical gathering. The submit sample option will send malicious samples to the cloud. If submit-sample enabled, there is no need to enable submit-report because the sample is re-analyzed in the cloud and a new report and signature is generated if the sample is malicious.

+ signature-generation — Enable the appliance to generate signatures locally, eliminating the need to send any data to the public cloud in order to block malicious content. The WF-500 appliance will analyze files forwarded to it from Palo Alto Networks firewalls or from the WildFire API and generate antivirus and DNS signatures that block both the malicious files as well as associated command and control traffic. When the appliance detects a malicious URL, it sends the URL to PAN-DB and PAN-DB assigns it the malware category.

Sample Output

The following shows an example output of the WildFire settings.

```
admin@WF-500# show deviceconfig setting wildfire
wildfire {
  active-vm vm-5;
  cloud-intelligence {
    submit-sample yes;
    submit-report no;
  }
  cloud-server wildfire-public-cloud;
  signature-generation {
    av yes;
    dns yes;
    url yes;
  }
}
```
Required Privilege Level

superuser, deviceadmin

set deviceconfig system update-schedule

Description

Schedule content updates on a WF-500 appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign.

Hierarchy Location

set deviceconfig system update-schedule

Syntax

wf-content recurring {
  daily at <value> action {download-and-install | download-only};
  weekly {
    action {download-and-install | download-only};
    at <value>;
    day-of-week {friday | monday | saturday | sunday | thursday | tuesday | wednesday};
  }
}

Options

> wf-content — WF-500 content updates.
> daily — Schedule update every day.
+ action — Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
+ at — Time specification hh:mm (e.g. 20:10).
> hourly — Schedule update every hour.
+ action — Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
+ at — Minutes past the hour.
> weekly — Schedule update once a week.
+ action — Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
WF-500 Appliance Configuration Mode Command Reference

Sample Output

admin@WF-500# show
update-schedule {
    wf-content {
        recurring {
            weekly {
                at 19:00;
                action download-and-install;
                day-of-week friday;
            }
        }
    }
}

Required Privilege Level

superuser, deviceadmin

set deviceconfig system vm-interface

Description

The vm-interface is used by malware running on the WF-500 appliance virtual machine sandbox to access the Internet. Activating this port is recommended and will help WildFire better identify malicious activity if the malware accesses the Internet for phone-home or other activity. It is important that this interface has an isolated connection to the Internet. For more information, see Set Up the WF-500 Appliance VM Interface.

After configuring the vm-interface, enable it by running the following command:

set deviceconfig setting wildfire vm-network-enable yes

Hierarchy Location

set deviceconfig system
Use the WF-500 Appliance CLI

WF-500 Appliance Configuration Mode Command Reference

Syntax

```
set vm-interface {
  default-gateway <ip_address>;
  dns-server <ip_address>;
  ip-address <ip_address>;
  link-state;
  mtu;
  netmask <ip_address>;
  speed-duplex;
}
```

Options

```
admin@WF-500# set vm-interface
+ default-gateway — Default gateway for the VM interface
+ dns-server — dns server for the VM interface
+ ip-address — IP address for VM interface
+ link-state — Set the link state to up or down
+ mtu — Maximum Transmission Unit for the VM interface
+ netmask — IP netmask for the VM interface
+ speed-duplex — Speed and duplex for the VM interface
```

Sample Output

```
The following shows a configured vm-interface.
vm-interface {
  ip-address 10.16.0.20;
  netmask 255.255.252.0;
  default-gateway 10.16.0.1;
  dns-server 10.0.0.246;
}
```

Required Privilege Level

```
superuser, deviceadmin
```
WF-500 Appliance Operational Mode Command Reference

This section contains command reference information for the following Operational mode commands that are specific to the WF-500 appliance software. All other commands that are part of the WF-500 appliance software are identical to PAN-OS; refer to the PAN-OS 7.1 CLI Quick Start for information on those commands.

- create wildfire api-key
- delete wildfire api-key
- delete wildfire-metadata
- edit wildfire api-key
- load wildfire api-key
- request system raid
- request system wildfire-vm-image
- request wf-content
- save wildfire api-key
- set wildfire portal-admin
- show system raid
- show wildfire
- test wildfire registration

create wildfire api-key

Description

Generate API keys on a WF-500 appliance that you will use on an external system to submit samples to the appliance, query reports, or retrieve samples and Packet Captures (PCAPS) from the appliance.

Syntax

create {
  wildfire {
    api-key {
      key <value>;
      name <value>;
    }
  }
}
Options

+ key — Create an API key by manually entering a key value. The value must be 64 alpha characters (a-z) or numbers (0-9). If you do not specify the key option, the appliance generates a key automatically.
+ name — Optionally enter a name for the API key. An API key name is simply used to label the keys to make it easier to identify keys assigned for specific uses and has no impact on the functionality of the key.

Sample Output

The following output shows that the appliance has three API keys and one key is named my-api-key.

```
admin@WF-500> show wildfire api-keys all
+--------+----------------+---------------------+---------------------+
| Apikey | Name | Status  | Create Time         | Last Used Time      |
+---------------------------------------------------------------------+
| <API KEY> |             | Enabled | 2014-06-24 16:38:50 |                     |
| <API KEY> | test2-api-key | Enabled | 2014-08-04 17:00:42 |
```

Required Privilege Level

superuser, deviceadmin

delete wildfire api-key

Description

Delete an API key from the WF-500 appliance. Systems configured to use the API to perform API functions on the appliance will no longer be able to access the appliance after you delete the key.

Syntax

```
delete {
  wildfire {
    api-key {
      key <value>;
    }
  }
}
```
Options

+ key <value> — The key value for the key that you want to delete. To view a list of API keys, run the following command: admin@WF-500> show wildfire api-keys all

Sample Output

admin@WF-500> delete wildfire-api-key key <API KEY>
APIKey <API KEY> deleted

Required Privilege Level

superuser, deviceadmin

delete wildfire-metadata

Description

Delete content updates on the WF-500 appliance. For more information on content updates and how to install them, see request wf-content.

Syntax

delete {
    wildfire-metadata update <value>;
    }

Options

+ update <value> — Define the content update that you want to delete.

Sample Output

The output that follows shows the deletion of an update named panup-all-wfmeta-2-181.candidate.tgz.
admin@WF-500> delete wildfire-metadata update panup-all-wfmeta-2-181.candidate.tgz
successfully removed panup-all-wfmeta-2-181.candidate.tgz
Required Privilege Level
superuser, deviceadmin

edit wildfire api-key

Description
Modify an API key name or the key status (enabled/disabled) on a WF-500 appliance.

Syntax
edit {
wildfire {
api-key [name | status] key <value>;
}
}

Options
+ name—Change the name of an API key
+ status—Enable or disable an API key
* key—Specify the key to modify

Sample Output
The key value in this command is required. For example, to change the name of a key named stu to stu-key1, enter the following command:

```
admin@WF-500> edit wildfire api-key name stu-key1 key <API KEY>
```
To change the status of stu-key1 to disabled, enter the following command:

```
admin@WF-500> edit wildfire api-key status disable key <API KEY>
```
Example output that shows that stu-key1 is disabled:

```
admin@WF-500> show wildfire api-keys all
------------------------------------------------------------------|----------|----------|---------------------
Apikey                 | Name     | Status   | Create Time         | Last Used Time |
<API KEY>              | stu-key1 | Disabled | 2014-08-21 07:23:34 | 07:23:34       |
```
load wildfire api-key

Description

After importing API keys to the WF-500 appliance, you must use the load command to make the keys available for use. Use this command to replace all existing API keys, or you can merge the keys in the import file with the existing key database.

Syntax

load {
    wildfire {
        from <value> mode [merge | replace];
    }
}

Options

* from — Specify the API key filename that you want to import. The key files use the .keys file extension. For example, my-api-keys.keys. To view a list of keys that are available for import, enter the following command:

```
admin@WF-500> load wildfire api-key from ?
```

+ mode — Optionally enter the mode for the import (merge/replace). For example, to replace the key database on the appliance with the contents of the new key file, enter the following command:

```
admin@WF-500> load wildfire api-key mode replace from my-api-keys.keys
```

If you do not specify the mode option, the default action will merge the keys.

Required Privilege Level

superuser, deviceadmin
request system raid

Description

Use this option to manage the RAID pairs installed in the WF-500 appliance. The WF-500 appliance ships with four drives in the first four drive bays (A1, A2, B1, B2). Drives A1 and A2 are a RAID 1 pair and drives B1 and B2 are a second RAID 1 pair.

Hierarchy Location

request system

Syntax

raid {
   remove <value>;
   OR...
   copy {
      from <value>;
      to <value>;
   }
   OR...
   add {

Options

> add—Add a drive into the corresponding RAID Disk Pair
> copy—Copy and migrate from one drive to other drive in the bay
> remove—Drive to remove from RAID Disk Pair

Sample Output

The following output shows a WF-500 appliance with a correctly configured RAID.

admin@WF-500> show system raid

<table>
<thead>
<tr>
<th>Disk Pair</th>
<th>Available</th>
<th>Disk id</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Pair A</td>
<td>Available</td>
<td>A1</td>
<td>Present</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A2</td>
<td>Present</td>
</tr>
<tr>
<td>Disk Pair B</td>
<td>Available</td>
<td>B1</td>
<td>Present</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B2</td>
<td>Present</td>
</tr>
</tbody>
</table>
Required Privilege Level

superuser, deviceadmin

**request system wildfire-vm-image**

Perform upgrades on the WF-500 appliance virtual machine (VM) sandbox images used to analyze files. To retrieve new VM images from the Palo Alto Networks Update Server, you must first download the image manually, host it on an SCP enabled server, and then retrieve the image from the appliance using the SCP client. After downloading the image to the appliance, you can then install it using this command.

**Hierarchy Location**

request system

**Syntax**

```
request {
  system {
    wildfire-vm-image {
      upgrade install file <value>;
    }
  }
}
```

**Options**

> wildfire-vm-image—Install Virtual Machine (VM) images.

+ upgrade install file—Perform an upgrade to the VM image. After the file option, type ? to view a list of available VM images. For example, run the following command to list available images:

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

**Sample Output**

To list available VM images, run the following command:

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

To install a VM image (Windows 7 64-bit in this example), run the following command:

```
admin@WF-500> request system wildfire-vm-image upgrade install file WFWin7_64Base_m-1.0.0_64base
```
Required Privilege Level

superuser, deviceadmin

**request wf-content**

Perform content updates on a WF-500 appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign. To schedule content updates to install automatically, see `set deviceconfig system update-schedule` and to delete content updates on the WF-500 appliance, see `delete wildfire-metadata`.

Hierarchy Location

request

**Syntax**

```plaintext
request wf-content
{
  downgrade install {previous | <value>};
  upgrade
  {
    check
    download latest
    info
    install {
      file <filename>
      version latest;
    }
  }
}
```

**Options**

> downgrade — Installs a previous content version. Use the previous option to install the previously installed content package or enter a value to downgrade to a specific content package number.
> upgrade — Performs content upgrade functions
> check — Obtain information on available content packages from the Palo Alto Networks Update Server
> download — Download a content package
> info — Show information about available content packages
> install — Install a content package
> file — Specify the name of the file containing the content package
Sample Output

To list available content updates, run the following command:

admin@WF-500> request wf-content upgrade check

<table>
<thead>
<tr>
<th>Version</th>
<th>Size</th>
<th>Released on</th>
<th>Downloaded</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-217</td>
<td>58MB</td>
<td>2014/07/29 13:04:55 PDT</td>
<td>yes</td>
<td>current</td>
</tr>
<tr>
<td>2-188</td>
<td>58MB</td>
<td>2014/07/01 13:04:48 PDT</td>
<td>yes</td>
<td>previous</td>
</tr>
<tr>
<td>2-221</td>
<td>59MB</td>
<td>2014/08/02 13:04:55 PDT</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

Required Privilege Level

superuser, deviceadmin

save wildfire api-key

Description

Use the save command to save all API keys on the WF-500 appliance to a file. You can then export the key file for backup purposes or to modify the keys in bulk. For details on using the WildFire API on a WF-500 appliance, see the WildFire API Reference.

Hierarchy Location

save

Syntax

save {
   wildfire {
      api-key to <value>;
   }
}

Options

* to — Enter the filename for key export. For example, to export all of the API keys on the WF-500 to a file named my-wf-keys, enter the following command:
save wildfire api-key to my-wf-keys

Required Privilege Level

superuser, deviceadmin

set wildfire portal-admin

Description

Sets the portal admin account password that an administrator will use to view WildFire analysis reports generated by a WF-500 appliance. The account name (admin) and password is required when viewing the report on the firewall or from Panorama in Monitor > WildFire Submissions > View WildFire Report. The default username and password is admin/admin.

The portal admin account is the only account that you configure on the appliance to view reports from the firewall or Panorama. You cannot create new accounts or change the account name. This is not the same admin account used to manage the appliance.

Hierarchy Location

set wildfire

Syntax

set {
  wildfire {
    portal-admin {
      password <value>;
    }
  }
}

Sample Output

The following shows the output of this command.

set wildfire portal-admin password

Enter password:

Confirm password:
Required Privilege Level

superuser, deviceadmin

show system raid

Description

Show the RAID configuration of the appliance. The WF-500 appliance ships with four drives in the first four drive bays (A1, A2, B1, B2). Drives A1 and A2 are a RAID 1 pair and drives B1 and B2 are a second RAID 1 pair.

Hierarchy Location

show system

Syntax

raid {
    detail;
}

Options

No additional options.

Sample Output

The following shows the RAID configuration on a functioning WF-500 appliance.

admin@WF-500> show system raid detail

<table>
<thead>
<tr>
<th>Disk Pair A</th>
<th>Available</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clean</td>
<td></td>
</tr>
<tr>
<td>Disk id A1</td>
<td>Present</td>
<td></td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size        : 953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>partition_1 : active sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>partition_2 : active sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk id A2</td>
<td>Present</td>
<td></td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size        : 953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>partition_1 : active sync</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use the WF-500 Appliance CLI

**show wildfire**

**Description**

Shows various information about the WF-500 appliance, such as available API keys, registration information, activity, recent samples that the appliance analyzed, and the virtual machine that is selected to perform analysis.

**Hierarchy Location**

show wildfire

**Syntax**

api-keys
  all {
    details;
  }
key <value>;
}
last-device-registration all |
latest {
  analysis {
    filter malicious|benign;
    sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|Status;
    sort-direction asc|desc;

partition_2  : active sync
Disk Pair B                           Available
Status                clean
Disk id B1                           Present
  model        : ST91000640NS
  size         : 953869 MB
  partition_1  : active sync
  partition_2  : active sync
Disk id B2                           Present
  model        : ST91000640NS
  size         : 953869 MB
  partition_1  : active sync
  partition_2  : active sync

Required Privilege Level

superuser, superreader
limit 1-20000;
days 1-7;

}  
OR...
samples {
    filter malicious|benign;
    sort-by SHA256|Create Time|File Name|File Type|File Size|Malicious|Status;
    sort-direction asc|desc;
    limit 1-20000;
    days 1-7;
}  
OR...
sessions {
    filter malicious|benign;
    sort-by SHA256|Create Time|Src IP|Src Port|Dst IP|Dst Port|File|Device ID|App|Malicious|Status;
    sort-direction asc|desc;
    limit 1-20000;
    days 1-7;
}  
OR...
uploads {
    sort-by SHA256|Create Time|Finish Time|Status;
    sort-direction asc|desc;
    limit 1-20000;
    days 1-7;
}
sample-status {
    sha256 {
        equal <value>;
    }
}

statistics days <1-31>;
status |  
vm-images |  }  

Options

 administrative@WF-500> show wildfire
> api-keys — Show details about the API keys generated on the WF-500 appliance. You can view the last time the key was used, the key name, status (Enabled or Disabled), and the date/time the key was generated.
> last-device-registration — Show list of latest registration activities.
> latest — Show latest 30 activities, which include the last 30 analysis activities, the last 30 files that were analyzed, network session information on files that were analyzed and files that were uploaded to the public cloud server.
> sample-status — Show wildfire sample status. Enter the SHA or MD5 value of the file to view the current analysis status.
> statistics — Display basic wildfire statistics.
Use the WF-500 Appliance CLI

> status — Display the status of the appliance as well as configuration information such as the Virtual Machine (VM) used for sample analysis, whether or not samples/reports are sent to the cloud, vm network, and registration information.

> vm-images — Display the attributes of the available virtual machine images used for sample analysis. To view the current active image, run the following command: `admin@WF-500> show wildfire status` and view the Select VM field.

Sample Output

The following shows the output for this command.

```
admin@WF-500> show wildfire api-keys all
+------------------------------------------------------------------+-------------|
<table>
<thead>
<tr>
<th>Apikey</th>
<th>Name</th>
<th>Status</th>
<th>Create Time</th>
<th>Last Used Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;API KEY&gt;</td>
<td>my-api-key-stu</td>
<td>Enabled</td>
<td>2014-06-24 16:38:50</td>
<td></td>
</tr>
</tbody>
</table>
+------------------------------------------------------------------+-------------|

admin@WF-500> show wildfire last-device-registration all
+--------------+---------------------+-------------+------------+----------+--------+
| Device ID    | Last Registered     | Device IP   | SW Version | HW Model | Status |
|--------------|---------------------|-------------|------------|----------|--------+
+--------------+---------------------+-------------+------------+----------+--------+

admin@WF-500> show wildfire latest
> analysis Show latest 30 analysis
> samples    Show latest 30 samples
> sessions   Show latest 30 sessions
> uploads    Show latest 30 uploads

admin@WF-500> show wildfire sample-status sha256 equal 809bad2d3fbd1c8ef47ba9c5a0fe8a691103f094bc8d7e0cbeb480870fd78c

Sample information:
+---------------------+---------------------------------------------------------------+
| Create Time         | File Name                                                     |
| File Type          | File Size | Malicious | Status            |
+---------------------+---------------------------------------------------------------+
| 2014-08-04 11:49:41 | 25047801_20130919175646000_970x66_Adobe_Marketing_RM_AUTO.swf | Adobe Flash File | 64502 | No | analysis complete |
+---------------------+---------------------------------------------------------------+

Session information:
+----------------------------------+
| Create Time | Src IP | Src Port | Dst IP | Dst Port | File | Device ID | App   | Malicious | Status |
| 2014-08-04 11:49:41 | 10.10.10.50 | 80 | 192.168.2.10 | 64108 | 25047801_20130919175646000_970x66_Adobe_Marketing_RM_AUTO.swf | 001606000114 | flash | No | completed |
+----------------------------------+

Analysis information:
```
<table>
<thead>
<tr>
<th>Submit Time</th>
<th>Start Time</th>
<th>Finish Time</th>
<th>Malicious</th>
<th>VM Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td></td>
<td></td>
<td></td>
<td>Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010</td>
</tr>
</tbody>
</table>

admin@WF-500> show wildfire statistics

Last one hour statistics :
Total sessions submitted : 0
Samples submitted : 0
  analyzed : 0
  pending : 0
  malicious : 0
  benign : 0
  error : 0
uploaded : 0

Last 24 hours statistics :
Total sessions submitted : 13
Samples submitted : 13
  analyzed : 13
  pending : 0
  malicious : 0
  benign : 13
  error : 0
uploaded : 0

admin@WF-500> show wildfire status

Connection info:
  Wildfire cloud: s1.wildfire.paloaltonetworks.com
  Status: Idle
  Submit sample: disabled
  Submit report: disabled
  Selected VM: vm-5
  VM internet connection: disabled
  VM network using Tor: disabled
  Best server: s1.wildfire.paloaltonetworks.com
  Device registered: yes
  Service route IP address: 10.3.4.99
  Signature verification: enable
  Server selection: enable
  Through a proxy: no
test wildfire registration

Description

Performs a test to check the registration status of a WF-500 appliance or Palo Alto Networks firewall to a WildFire server. If the test is successful, the IP address or server name of the WildFire server is displayed. A successful registration is required before a WF-500 appliance or firewall can forward files to the WildFire server.

Syntax

test {
  wildfire {
    registration;
  }
}

Options

No additional options.

Sample Output

The following shows a successful output on a firewall that can communicate with a WF-500 appliance. If this is a WF-500 appliance pointing to the Palo Alto Networks WildFire cloud, the server name of one of the cloud servers is displayed in the select the best server: field.

Test wildfire
  wildfire registration: successful
  download server list:  successful
  select the best server:  ca-s1.wildfire.paloaltonetworks.com

Required Privilege Level

superuser, superreader