Palo Alto Networks®
WildFire Administrator's Guide

WildFire Appliance Software 5.1

Contact Information

Corporate Headquarters:

Palo Alto Networks

3300 Olcott Street

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

About this Guide

This guide describes the administrative tasks required to use and maintain the Palo Alto Networks WildFire feature. Topics covered include licensing information, configuring firewalls to forward files for inspection, viewing reports, and how to configure and manage the WF-500 WildFire appliance.

Refer to the following sources for more information:

- Palo Alto Networks Administrator's Guide—For information on the additional capabilities and for instructions on configuring the features on the firewall
- https://live.paloaltonetworks.com—For access to the knowledge base, complete documentation set, discussion forums, and videos.
- https://support.paloaltonetworks.com—For contacting support, for information on the support programs, or to manage your account or devices.

To provide feedback on the documentation, please write to us at:

documentation@paloaltonetoworks.com

Palo Alto Networks, Inc.
www.paloaltonetworks.com

P/N 810-000148-00A

Table of Contents

1 WildFire Overview

This chapter provides an overview of the WildFire feature, including supported deployments, subscription requirements, and descriptions of the steps to take if malware is detected in your environment. It includes the following sections:

About WildFire

Modern malware is at the heart of many of today's most sophisticated network attacks and is increasingly customized to avoid traditional security solutions. Palo Alto Networks has developed an integrated approach that addresses the full malware life cycle, which includes preventing infections, identifying zero-day malware (that is, malware that has not previously been identified by other antivirus vendors) or targeted malware (malware targeting a specific industry or corporation), as well as pinpointing and disrupting active infections.

The Palo Alto Networks WildFire engine exposes zero-day and targeted malware through direct observation in a virtual environment within the WildFire system. The WildFire feature also makes extensive use of Palo Alto Networks App-ID technology by identifying file transfers within all applications, not just email attachments or browser-based file downloads.

The key benefits of the Palo Alto Networks WildFire feature is that it can discover zero-day malware and can quickly generate signatures to protect against future infections of all of the malware it discovers. The firewall can provide instant alerts whenever malware is detected on your network by sending email alerts, syslog alerts, or SNMP traps. This allows you to quickly identify the user who downloaded the malware and eradicate it before it causes extensive damage or propagates to other users. In addition, every signature generated by WildFire is automatically propagated to all Palo Alto Networks firewalls protected with a Threat Prevention and/or WildFire subscription, which provides automatic protection from malware even if it was not found in your network. Palo Alto Networks is currently discovering and generating signatures for thousands of zero-day malware very week and this number continues to grow.

How Does WildFire Work?

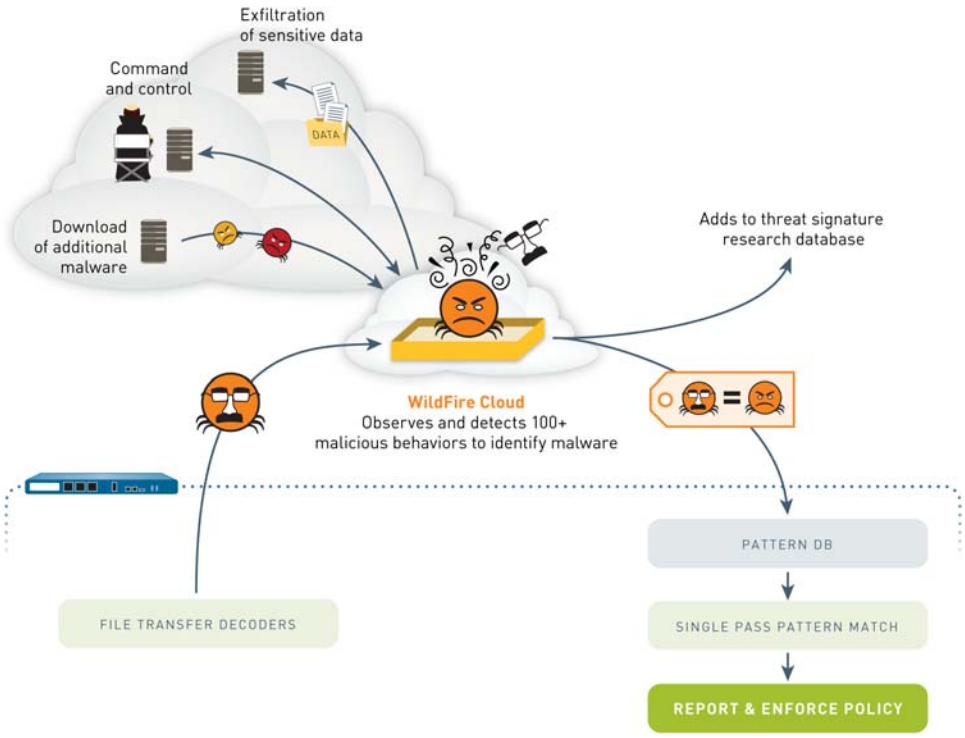
To configure your firewall to use WildFire, you must configure a file blocking profile to send files to WildFire by setting the forward action on the Win32 Portable Executable (PE) file type. Alternatively, the continue-and-forward action can be selected to prompt the user before downloading the file over HTTP. Because the WildFire setting is configured using a file blocking profile, which is then attached to a firewall policy, you have very granular control over the conditions under which files are sent to WildFire. For example, you may choose to only forward attachments for web-based email, or only from websites of certain URL categories.

Whenever a file is transferred over a session that matches a security rule with a forwarding profile, the firewall checks with WildFire to see if the file is new. If the file is new, the firewall automatically forwards the file to WildFire, even if it is contained within a ZIP file or over compressed HTTP. The firewall can also be configured to forward files inside of decrypted SSL sessions. When WildFire receives the file, it analyzes it in its virtualized sandbox to determine if the file exhibits signs of malicious behaviors, changes to browser security settings, injection of code into other processes, modification of files in the Windows system folder, or domains that the sample may have visited. When the WildFire engine completes the analysis it generates a detailed forensics report that summarizes the activities performed by the sample on the host and the network and automatically assigns a verdict of malware or benign.

In addition, when the WildFire engine identifies a sample as malware, it passes it to the WildFire signature generator, which automatically generates 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 will address multiple variants of the malware. The new signature is then distributed within 30-60 minutes to all Palo Alto Networks firewalls equipped with a WildFire subscription, or the following day as part of the antivirus update for firewalls equipped with a Threat Prevention subscription only. As soon as the firewall is updated with the

new signature, any files that contain that malware or a variant of it will automatically be dropped. Information gathered by WildFire during the analysis of malware is also used to fortify other Threat Prevention features, such as the PAN-DB malware URL categories, DNS signatures, antivirus, and anti-spyware signatures. Palo Alto Networks also develops signatures for command and control traffic, enabling immediate disruption in the communications of any malware inside the network. For details on signatures and the benefits of having a WildFire subscription, see "What are the Benefits of the WildFire Subscription?" on page 5.

The following diagram illustrates the WildFire workflow:



What is in the WildFire Reports?

For each file WildFire analyzes, it produces a detailed behavioral report within minutes of the file submission. Depending on how the file was submitted to WildFire and what subscriptions are active on the firewall, these reports are available in the firewall's WildFire logs, from the WildFire portal (https://wildfire.paloaltonetworks.com), or though WildFire API queries. The reports show detailed behavioral information about the file, information on the targeted user, the application that delivered the file, and all URLs involved in the delivery or phone-home activity of the file. For details on how to access the reports and descriptions of the report fields, see "View WildFire Reports" on page 50.

What Actions Do I Take After Malware is Detected?

When malware is discovered on your network, it is important to take quick action to prevent spread of the malware to other systems. To ensure immediate alerts to malware discovered on your network, configure your firewalls to send email notifications, SNMP Traps, and/or syslogs whenever WildFire returns a malware verdict on a file forwarded from a firewall. This allows you to quickly view the WildFire analysis report and identify the user who downloaded the malware, determine if the user ran the infected file, and assess whether the malware attempted to spread itself to other hosts on the network. If you determine that the user ran the file, you can quickly disconnect the computer from the network to prevent the malware from spreading and follow incident response and remediation processes as required. For information on WildFire reports and an example of WildFire in action, see "Monitor, Track, and Prevent Malware on Your Network" on page 45.

What Deployments are Available?

Palo Alto Networks next-generation firewalls support the following WildFire deployments:

- **Palo Alto Networks WildFire Cloud:** In this deployment, the firewall forwards files to the hosted WildFire environment that is owned and maintained by Palo Alto Networks. As WildFire detects new malware, it generates new signatures within the hour. Firewalls equipped with a WildFire subscription can receive the new signatures within 30-60 minutes; firewalls with only a Threat Prevention subscription can receive the new signatures in the next antivirus signature update within 24-48 hours. For more information, see "What are the Benefits of the WildFire Subscription?" on page 5.

- **WildFire Appliance:** In this deployment, you install a WF-500 WildFire appliance on your corporate network and configure your firewalls to forward files to it instead of to the Palo Alto Networks WildFire cloud (the default). This deployment prevents the firewall from having to send any files outside of your network for analysis. By default, the appliance will not send any files out of your network unless you explicitly enable the auto-submit feature, which will automatically forward any malware it detects to the Palo Alto Networks WildFire cloud where the files are analyzed to generate antivirus signatures. The antivirus signatures are then distributed to all Palo Alto Networks firewalls with a threat prevention and/or WildFire subscription. A single WildFire appliance can receive and analyze files from up to 100 Palo Alto Networks firewalls.

The main differences between the Palo Alto Networks WildFire cloud and the WildFire appliance are as follows:

  - The WildFire Appliance enables on-premises sandboxing of malware so that benign files never leave the customer network. By default, the WildFire appliance does not forward any files to the WildFire cloud and therefore signatures are not generated for malware detected by the appliance. If you want WildFire signatures for the malware detected on your network, you can enable the auto-submit feature on the appliance. With this option enabled, the appliance sends any malware it detects to the WildFire cloud for signature generation.
  - The WildFire API, which is available with all WildFire subscriptions, is available to all WildFire subscribers and can be used with the public cloud, but cannot be used with the WF-500 appliance.
  - Manual submission of samples can be performed on the public cloud through the web portal (wildfire.paloaltonetworks.com), but there is no local web portal for the WF-500 appliance.

What are the Benefits of the WildFire Subscription?

WildFire provides detection and prevention of zero-day malware using a combination of malware sandboxing and signature-based detection and blocking of malware. To use WildFire to gain visibility into zero-day malware, all that is required is to configure a file blocking profile to enable the firewall to forward samples to WildFire for analysis. No subscription is required to use WildFire for sandboxing files sent from Palo Alto Networks firewalls to the WildFire cloud.

In order to perform detection and blocking of known malware after the malware has been detected by WildFire, a Threat Prevention and/or WildFire subscription is required. The Threat Prevention subscription enables the firewall to receive daily antivirus signature updates, which provides coverage for all malware samples detected by WildFire globally to all customers with a Threat Prevention subscription. The Threat Prevention subscription also provides access to weekly content updates that include new vulnerability protection and anti-spyware signatures.

To receive the full benefits of the WildFire service, each firewall must have a WildFire subscription, which provides the following benefits:

- **WildFire Dynamic Updates**—Provide new malware signatures on a sub-hourly basis, configurable through **Device > Dynamic Updates**. Within an hour of detecting new malware, WildFire creates a new malware signature and distributes it through the WildFire dynamic updates, which the firewall can poll every 15, 30, or 60 minutes. The firewall can be configured to take specific actions on malware signatures separate from the regular antivirus signature actions in the antivirus profile. The WildFire signatures delivered in the dynamic update include signatures generated for malware detected in files submitted to WildFire by all Palo Alto Networks WildFire customers, not just the file samples that your firewalls send to WildFire.

It takes approximately 30 to 60 minutes for a WildFire signature to be generated after malware is discovered and to make the signatures available to WildFire subscribers. Firewalls equipped with a WildFire subscription can poll for new malware signatures every 15, 30, or 60 minutes. For example, if the firewall is set to poll for WildFire signature updates every 30 minutes, it may not receive a signature for one of your submitted files until the second polling interval after it was discovered because of the time it takes to generate the signature. If the firewall only has a Threat Prevention subscription, it will still receive signatures generated by WildFire after the WildFire signatures are rolled into the antivirus updates, which occurs about every 24-48 hours.

For files analyzed by a WF-500 WildFire appliance, signatures can only be generated for malware detected on your network if you have explicitly enabled the auto-submit feature (unless the same malware was observed by another customer and submitted the same sample to the WildFire public cloud). When auto-submit is enabled, the appliance will forward all discovered malware to the Palo Alto Networks WildFire cloud where they will be used to generate an antivirus signature to detect and block future instances of the malware.

- **Integrated WildFire Logs**—When WildFire finishes analyzing a file, it sends a WildFire log back to the firewall that submitted the file. These logs are viewed from **Monitor > Logs > WildFire** and provides direct access to the full analysis report from the WildFire system by clicking the **View WildFire Report** button. Having the WildFire log data on the firewall makes the threat logs as actionable as the threat logs, and allow you to configure SNMP, syslog, email alerts, and forwarding to Panorama. Without the WildFire subscription, WildFire logs are only accessible using the WildFire web portal at wildfire.paloaltonetworks.com.

- **WildFire API**—The WildFire subscription provides access to the WildFire API, allowing for direct programmatic access to the WildFire service on the Palo Alto Networks WildFire cloud. You can use the WildFire API to submit files to the WildFire cloud and to retrieve reports for the submitted files. The WildFire API supports up to 100 file submissions per day and up to 1000 queries per day. Note that you cannot use the WildFire API to submit files to the WildFire appliance.
- **WildFire Appliance**—Only firewalls with a valid WildFire subscription can forward files to a WildFire appliance for analysis. Firewalls that only have a Threat Prevention subscription installed can forward files to the WildFire cloud, but not to a WildFire appliance.

2 Analyze Files Using the WF-500 WildFire Appliance

This chapter describes the WF-500 WildFire appliance and how to configure and manage the appliance to prepare it to receive files for analysis. In addition, this chapter provides steps for configuring a Palo Alto Networks firewall to forward files to a WildFire appliance for file analysis.

- About the WF-500 WildFire Appliance
- Configure the WF-500 WildFire Appliance
- Forward Files to a WF-500 WildFire Appliance

About the WF-500 WildFire Appliance

The WF-500 WildFire appliance provides an on-premises WildFire private cloud, enabling you to analyze suspicious files in a sandbox environment without requiring the files to be sent outside of the network. To use a WF-500 appliance in place of the WildFire public cloud, configure the WildFire cloud setting on the firewall to point to your WF-500 appliance rather than to the **default-cloud** setting. The WF-500 appliance sandboxes all files locally and analyzes them for malicious behaviors using the same engine that is used by the WildFire public cloud system. Within minutes, the appliance returns the results of the analysis back to the firewall in the WildFire log.

By default, the WF-500 appliance does not send any files to the Palo Alto Networks WildFire cloud. However, malware must be sent to the WildFire public cloud in order to receive antivirus signatures for the malware discovered by the appliance. The WF-500 appliance has an automatic submission feature that will allow it to only send confirmed malware to the public cloud for signature generation. The signatures are then distributed to all customers who receive WildFire and antivirus signature updates from Palo Alto Networks. You can configure up to 100 Palo Alto Networks firewalls to forward to a single WildFire appliance; each firewall must have a valid WildFire subscription in order to forward files to a WildFire appliance.

The WildFire appliance has two interfaces:

- **MGT**—Receives all files forwarded from the firewalls and returns logs detailing the results back to the firewalls.
- **Virtual Machine Interface (vm-interface)**—Provides network access for the analysis sandboxes to enable WildFire to better analyze the behavior of the files running in its sandbox because it allows it to observe some malicious behaviors that would not be exhibited without network access, such as phone-home activity. However, to prevent malware from entering your network from the sandbox, you must be sure to configure this interface on an isolated network with an Internet connection to allow malware running on the virtual machines to communicate with the Internet. For more information on the vm-interface, see "Set Up the Virtual Machine Interface" on page 16.

  You must configure this interface before you will be able to commit any changes to the appliance.

Configure the WF-500 WildFire Appliance

This section describes the steps required to configure a WildFire appliance on a network and how to configure a Palo Alto Networks firewall to forward files to it for analysis.

This section contains the following topics:

Before You Begin

- Rack mount and cable the WF-500 WildFire appliance. Refer to the *WF-500 WildFire Appliance Hardware Reference Guide*.
- Obtain the information required to configure network connectivity on the MGT port and the virtual machine 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 appliance's MGT port. In addition, the appliance must be able to connect to the updates.paloaltonetworks.com site to retrieve its operating system software updates.
- Have a computer ready with either a console cable or Ethernet cable to connect to the device for the initial configuration.

Perform the Initial Configuration

This section describes the steps required to install a WF-500 WildFire appliance on a network and perform basic setup.

INTEGRATE THE WILDFIRE APPLIANCE INTO A NETWORK		
Step 1	Perform the tasks in the "Before You Begin" on page 9 section.	• Device is rack mounted • IP information ready (MGT interface and vm-interface IP address, subnet mask, gateway, hostname, DNS server) • Management computer is connected to the MGT port on the appliance or the console port
Step 2	Register the WildFire appliance.	1. Obtain the serial number from the S/N tag on the appliance, or run the following CLI command: `admin@WF-500> show system info` 2. From a browser, navigate to https://support.paloaltonetworks.com. 3. Register the device as follows: • If this is the first Palo Alto Networks device that you are registering and you do not yet have a login, click **Register** on the right side 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 **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**.
Step 3	Connect the management computer to the appliance using the MGT or Console port and power on the appliance.	1. Connect to the console port or the MGT port. Both are located on the back of the appliance. • **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 management computer's IP address to 192.168.1.5. 2. Power on the appliance. **Note** The appliance will power on as soon as power is supplied to the first power supply. A warning beep will sound until both power supplies are connected. 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.

INTEGRATE THE WILDFIRE APPLIANCE INTO A NETWORK (CONTINUED)		
Step 4	Reset the admin password.	1. Log in to the appliance with an SSH client or by using the Console port. Enter a username/password of admin/admin. 2. Set a new password by running the command: `admin@WF-500# set password` Type the old password, press enter and then enter and confirm the new password. There is no need to commit the configuration because this is an operational command. 3. Type `exit` to log out and then log back in to confirm that the new password is set.

Step 5	Set the IP information for the MGT interface and the hostname for the appliance. All firewalls that will send files to the WF-500 appliance will use the MGT port, so ensure that this interface is accessible from those firewalls.
	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`
		Note If desired, 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 for this example):
		`admin@WF-500# set deviceconfig system hostname wildfire-corp1`

Step 6	(Optional) Configure additional user accounts for managing the WildFire appliance. Two roles can be assigned: superuser and superreader. Superuser is equivalent to the admin account, and superreader only has read-only access.	In this example, we will create a superreader account for the user bsimpson:
		1. Enter configuration mode by running the following command:
		`admin@WF-500> configure`
		2. To create the user account, enter the following command:
		`admin@WF-500# set mgt-config users bsimpson password`
		3. Enter and confirm a new password.
		4. To assign the superreader role, enter the following command and then press enter:
		`admin@WF-500# set mgt-config users bsimpson permissions role-based superreader yes`

INTEGRATE THE WILDFIRE APPLIANCE INTO A NETWORK (CONTINUED)		

Step 7	Activate the appliance with the WildFire authorization code that you received from Palo Alto Networks.	1. Go to operational mode to run the following commands:
		`admin@WF-500> exit`
		2. Fetch and install the WildFire license:
		`admin@WF-500> request license fetch auth-code auth-code`
		3. Press enter to fetch and install the license.
		4. Verify the license:
		`admin@WF-500> request license info`
		An active license with a date later than the current date will be displayed.

Step 8	Set the current date/time and timezone.	1. Set the date and time:
		`admin@WF-500> set clock date YY/MM/DD time hh:mm:ss`
		2. Enter configuration mode:
		`admin@WF-500> configure`
		3. Set the local time zone:
		`admin@WF-500# set deviceconfig system timezone timezone`
		Note The time stamp that will appear on the WildFire detailed report will use the time zone set on the appliance. If you have multiple people viewing these reports, you may want to set the time zone to UTC.

Step 9	(Optional) Configure auto-submit to enable the WildFire appliance to forward files that contain malware to the Palo Alto Networks WildFire cloud. The WildFire cloud system will then generate signatures, which are distributed via the WildFire and antivirus signature updates.
	Note This option is disabled by default.
		1. To enable auto-submit, run the command:
		`admin@WF-500# set deviceconfig setting wildfire auto-submit yes`
		2. To confirm the setting, run the following command from operational mode:
		`admin@WF-500> show wildfire status`

Step 10	Commit the configuration and connect to the appliance using the new IP address. If the management computer is connected to the MGT port, the connection will be lost after the commit because the interface will now be on a different network.	1. Commit the configuration: `admin@WF-500# commit` 2. Connect the MGT interface port to a network switch. 3. Put the management PC back on your corporate network if necessary. 4. From the management computer, connect to the new IP address or hostname of the MGT port using an SSH client. In this example, the new IP address is 10.10.0.5.

INTEGRATE THE WILDFIRE APPLIANCE INTO A NETWORK (CONTINUED)	
Step 11 Set a password for the portal admin account. This account is used when accessing WildFire reports from a firewall. The default username and password is admin/admin. **Note** The portal admin account is the only account used for viewing reports from the logs. Only the password can be changed for this account and additional accounts cannot be created. This is not the same admin account used to manage the appliance.	To change the WildFire portal admin account password: 1. `admin@WF-500# set wildfire portal-admin password` 2. Press enter and type and confirm the new password.

Where to Go Next:

- To verify the WF-500 appliance configuration, see "Verify the WF-500 WildFire Appliance Configuration" on page 14.
- To start forwarding files from a firewall, see "Forward Files to a WF-500 WildFire Appliance" on page 23.
- To update the WildFire appliance software, see "Update the WF-500 WildFire Appliance Software" on page 21.
- To configure the vm-interface that the appliance uses as part of its malware analysis, see "Set Up the Virtual Machine Interface" on page 16.

Verify the WF-500 WildFire Appliance Configuration

This section describes the steps required to verify the configuration of the WildFire appliance to ensure that it is ready to receive files from a Palo Alto Networks firewall. For more detailed information on the CLI commands referenced in this workflow, see "WildFire Appliance Software CLI Reference" on page 59.

VERIFY THE WILDFIRE APPLIANCE CONFIGURATION	

Step 1. Verify that the appliance is registered and that the subscription is activated.	1. Start an SSH session to the appliance's MGT interface.
	2. From the CLI, enter the following command:
	`admin@WF-500> request license info`
	
	Verify that the license is valid and that the value in the `Expired:` field displays `no`.
	For example:
	`Feature: Premium`
	`Description: 24x7 phone support; advanced replacement hardware service`
	`Serial: 009707000000`
	`Issued: February 11, 2013`
	`Expires: February 11, 2016`
	`Expired?: no`
	3. For appliances enabled for auto-submit, verify that the WildFire appliance can communicate with the Palo Alto Networks WildFire cloud by entering the following command:
	`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. If auto-submit is enabled, malware-infected files will be sent to this server.
	`Test wildfire`
	`wildfire registration: successful`
	`download server list: successful`
	`select the best server:`
	`cs-s1.wildfire.paloaltonetworks.com`
	
	Note The appliance will only forward files to the WildFire cloud if auto-submit is enabled. For information on enabling auto-submit, refer to the steps in "Perform the Initial Configuration" on page 10.

VERIFY THE WILDFIRE APPLIANCE CONFIGURATION (CONTINUED)

Step 2 Check WildFire server status on the appliance.

1. The following command displays the status of WildFire:

```
admin@WF-500> show wildfire status
```

The following displays an example output:

```
Connection info:
        Wildfire cloud:           wildfire-public-cloud
        Status:                   Idle
        Auto-Submit:              enabled
        VM internet connection:   disabled
        Best server:
        Device registered:        yes
        Service route IP address: 192.168.2.20
        Signature verification:   enable
        Server selection:         enable
        Through a proxy:          no
```

In this example, auto-submit is enabled, which means that files identified as malware will be forwarded to the Palo Alto Networks WildFire cloud. Signatures can be generated to protect against future exposure of the malware. Status `Idle` indicates that the appliance is ready to receive files. `Device registered` displays `yes`, which means the appliance is registered with the WildFire cloud system.

2. To verify that the appliance is receiving files from the firewalls and to verify if the appliance is sending files to the WildFire cloud for signature generation (if auto-submit is enabled), enter the following command:

```
admin@WF-500> show wildfire statistics
days 7
```

```
Last one hour statistics:
Total sessions submitted  :           0
Samples submitted         :           0
Samples analyzed          :           0
Samples pending           :           0
Samples (malicious)       :           0
Samples (benign)          :           0
Samples (error)           :           0
Malware sent to cloud     :           0

Last 7 days statistics:
Total sessions submitted  :          66
Samples submitted         :          34
Samples analyzed          :          34
Samples pending           :           0
Samples (malicious)       :           2
Samples (benign)          :          32
Samples (error)           :           0
Malware sent to cloud     :           0
```

3. To view more granular statistics, enter the following command:

```
admin@WF-500> show wildfire latest
[analysis |samples | sessions | uploads]
```

For example, to display details about the last 30 analysis results, enter the following command:

```
admin@WF-500> show wildfire latest
analysis
```

VERIFY THE WILDFIRE APPLIANCE CONFIGURATION (CONTINUED)		

Step 3	Verify that firewalls configured to forward files have successfully registered with the WildFire appliance.	1. Enter the following command to display a list of firewalls that have registered with the appliance:
		`admin@WF-500> show wildfire last-device-registration all`
		
		The output should the following information for each firewall that is registered to send files to the appliance: firewall serial number, date registered, IP address, software version, hardware model, and status. If no firewalls are listed, there may be network connectivity issues between the firewalls and the appliance. Check the network to confirm that the firewalls and WildFire appliance can communicate.
		
		Use ping tests from the appliance to the gateway address, or to one of the firewalls that is configured to forward to the appliance. For example, if one of the firewalls is at the IP address 10.0.5.254, replies will be displayed when running the following CLI command from the appliance:
		`admin@WF-500> ping host 10.0.5.254`

Set Up the Virtual Machine Interface

The virtual machine interface provides external network connectivity to the sandbox virtual machines in the WF-500 appliance. The following sections describe the virtual machine interface (vm-interface) and the steps required for configuring it. It also describes the steps required to connect the interface to a dedicated port on a Palo Alto Networks firewall to enable Internet connectivity.

- What is the Virtual Machine Interface?
- Configure the Virtual Machine Interface
- Configure the Firewall to Control Traffic for the Virtual Machine Interface

What is the Virtual Machine Interface?

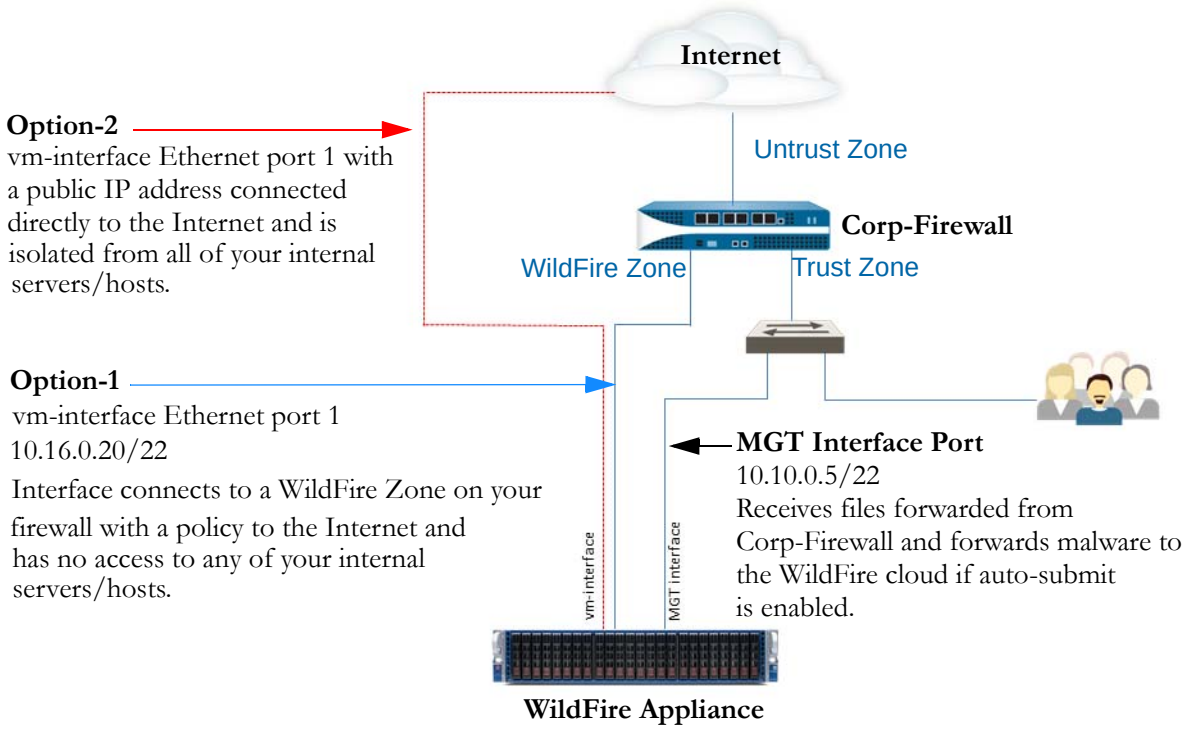
When configured and enabled, the vm-interface (labeled **1** on the back of the appliance) enables improved malware detection capabilities. This interface allows a file sample running on the WildFire virtual machines to communicate with the Internet and enables WildFire to better analyze the behavior of the sample file to determine if it exhibits characteristics of malware.

Caution

While we recommend that the vm-interface is enabled, it is very important that the interface is not connected 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):** The vm-interface is connected to an interface in a dedicated zone on a firewall that has a policy that only allows access to the Internet. 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 connection 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 vm-interface will not be logged unless a firewall or a traffic monitoring tool is placed between the WildFire appliance and the DSL connection.

Configure the Virtual Machine Interface

This section describes the steps required to configure the vm-interface on the WildFire appliance using the Option 1 configuration detailed in the preceding workflow. 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 will be routed as described in "Configure the Firewall to Control Traffic for the Virtual Machine Interface" on page 19.

By default, the vm-interface is configured using 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. Removing the configuration will cause commit failures.
.

CONFIGURE THE VIRTUAL MACHINE INTERFACE		

Step 1	Set the IP information for the vm-interface on the WildFire appliance. The following will be used for 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
	Note The vm-interface cannot be on the same network as the management interface (MGT).
		1. Enter configuration mode be entering the CLI command:
		`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`
		Note Only one DNS server can be assigned to the vm-interface. As a best practice, use your ISP's DNS server or an open DNS service.

Step 2	Enable the vm-interface.	1. To 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	Continue to the next section to configure the firewall interface to which the vm-interface will be connected.	See "Configure the Firewall to Control Traffic for the Virtual Machine Interface" on page 19.

Configure the Firewall to Control Traffic for the Virtual Machine 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, a new zone named wf-vm-zone is configured for connecting the appliance's vm-interface 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 INTERFACE FOR THE VIRTUAL MACHINE NETWORK		
Step 1	Configure the interface on the firewall that the vm-interface will connect to and set the virtual router. **Note** The wf-vm-zone that is configured in this step should only be used to connect the vm-interface from the appliance to the firewall. Do not add any other interfaces to the wf-vm-zone because intra-zone traffic will be enabled by default, which would enable traffic from the vm-interface to access a network other than the Internet.	1. From the web interface on the firewall, select **Network > Interfaces** and then select an interface, for example **Ethernet1/3**. 2. Select the **Interface Type 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 then 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 we 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 **Name** field enter **WildFire VM Interface**. 3. In the **Source** tab, set the **Source Zone** to **wf-vm-interface**. 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. **Note** If there are concerns that someone may 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 cause the implicit intra-zone allow rule that allows communications between interfaces in the same zone to be overridden and will deny/block all intra-zone communication.

CONFIGURE THE FIREWALL INTERFACE FOR THE VIRTUAL MACHINE NETWORK (CONTINUED)		
Step 3	Connect the cables.	Physically connect the vm-interface on the WildFire 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. From the WildFire appliance CLI operational mode run the following command:
		`admin@WF-500> show interface vm-interface`
		2. All of the interface counters will be displayed. Verify that received/transmitted counters have incremented. Run the following command to generate ping traffic:
		`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`

Update the WF-500 WildFire Appliance Software

This section describes the steps required to update the WildFire appliance software on a WF-500 WildFire appliance. The software updates contain the latest features and bug fixes for the software. The appliance can be upgraded using the Palo Alto Networks update server or by downloading and installing the updates manually (see "Manual Software Update" on page 22). For details about a specific software release, refer to the corresponding release note.

UPDATE THE WF-500 WILDFIRE APPLIANCE SOFTWARE		

Step 1	View the current version of the WildFire appliance software on the appliance and check to see if there is a new version available.	1. Enter the following command and check the `sw-version` field:
		`admin@WF-500> show system info`
		2. Enter the following command to view the latest release versions:
		`admin@WF-500> request system software check`
		Note If the appliance cannot contact the Palo Alto Networks update server, make sure it is licensed and that DNS is resolving properly. From the appliance, ping the Palo Alto Networks update server to make sure it is reachable by entering the following CLI command:
		`admin@WF-500> ping host updates.paloaltonetworks.com`

Step 2	Download and install a new version of the WildFire appliance software.	1. To install a new version of the software use the following command:
		`admin@WF-500> request system software download file filename`
		For example:
		`admin@WF-500> request system software download file WildFire_m-5.1.0`
		2. Verify that the file has finished downloading using the following command:
		`admin@WF-500> show jobs pending`
		or
		`admin@WF-500> show jobs all`
		3. After the file is downloaded, install it using the following command:
		`admin@WF-500> request system software install file filename`
		For example:
		`admin@WF-500> request system software install file WildFire_m-5.1.0`

UPDATE THE WF-500 WILDFIRE APPLIANCE SOFTWARE (CONTINUED)	

Step 3 After the new version is installed, reboot the appliance.	1. Monitor the upgrade status using the following command:
	`admin@WF-500> show jobs pending`
	2. After the upgrade is complete, reboot the appliance using the following command:
	`admin@WF-500> request restart system`
	3. After the reboot, verify that the new version is installed by running the following CLI command and then check the `sw-version` field:
	`admin@WF-500> show system info`

Manual Software Update

If the WildFire appliance does not have network connectivity to the Palo Alto Networks update servers, you can manually upgrade the software.	1. Navigate to https://support.paloaltonetworks.com/and in the **Manage Devices** section, click **Software Updates**.
	2. Download the WildFire appliance software image file to be installed to a computer running SCP server software.
	3. Import the software image from the SCP server:
	`scp import software from` *`username@ip_address/foldername imagefile`*
	For example:
	`admin@WF-500> scp import software from user1@10.0.3.4:/tmp/WildFire_m-5.1.0`
	4. Install the image file:
	`admin@WF-500> request system software install file` *`imagefilename`*
	5. After the upgrade is complete, reboot the appliance:
	`admin@WF-500> request restart system`
	6. After the reboot, verify that the new version is installed by entering the following CLI command and then check the `sw-version` field:
	`admin@WF-500> show system info`

Forward Files to a WF-500 WildFire Appliance

This section describes the steps required to set up a Palo Alto Networks firewall to start forwarding files to a WF-500 WildFire appliance and describes how to verify the appliance's configuration.

Although the firewall can forward to either a WildFire appliance (WildFire subscription required) or to the WildFire cloud, for better visibility make sure all of your firewalls point to the same WildFire system. For firewalls managed by Panorama, simplify WildFire administration by using Panorama Templates to push the WildFire server information, allowed file size, and the session information settings to the firewalls. Use Panorama device groups to configure and push file blocking profiles and security policy rules. Panorama can only point to one WildFire system (appliance or cloud).

If there is a firewall between the firewall that is forwarding files to WildFire and the WildFire cloud or WildFire appliance, make sure that the firewall in the middle has the necessary ports allowed.

- WildFire cloud: Uses port 443 for registration and file submissions.
- WildFire appliance: Uses port 443 for registration and 10443 for file submissions.

Perform the following steps on each firewall that will forward files to the WildFire appliance:

CONFIGURE FORWARDING TO THE WF-500 WILDFIRE APPLIANCE		
Step 1	Verify that the firewall has a WildFire subscription and that dynamic updates are scheduled and are up-to-date.	1. Navigate to **Device > Licenses** and confirm that the firewall has valid WildFire and Threat Prevention subscriptions installed. 2. Navigate to **Device > Dynamic Updates** and click **Check Now** to ensure that the firewall has the most recent Antivirus, Applications and Threats, and WildFire updates. 3. If the updates are not scheduled, schedule them now. Be sure to stagger the update schedules because only one update can be performed at a time. See "Dynamic Updates Best Practices" on page 25 for recommended settings.
Step 2	Define the WildFire server that the firewall will forward files to for analysis.	1. Navigate to **Device > Setup > WildFire**. 2. Click the **General Settings** edit icon. 3. In the **WildFire Server** field, enter the IP address or FQDN of the WF-500 WildFire appliance. **Note** The best way to set the **WildFire Server** field back to the default value is to clear the field and click **OK**. This will ensure that the correct value is added. When using a WildFire appliance, make sure that disable-server-select is not enabled, otherwise the appliance will not be able to receive files sent from the firewall. Check the following setting and make sure it is set to no: `admin@PA-200# set deviceconfig setting wildfire disable-server-select`

CONFIGURE FORWARDING TO THE WF-500 WILDFIRE APPLIANCE (CONTINUED)	
Step 3 Configure the file blocking profile to define which applications and file types will trigger forwarding to WildFire. **Note** If you choose **PE** in the objects profile File Types column to select a category of file types, do not also add an individual file type that is part of that category because this will result in redundant entries in the Data Filtering logs. For example, if you select PE do not also select **exe** because it is part of the PE category. This also applies to the **zip** file type, because supported file types that are zipped are automatically sent to WildFire. Choosing a category rather than an individual file type also ensures that as new file type support is added to a given category, they are automatically made part of the file blocking profile. If you select **Any**, all supported file types will be forwarded to WildFire.	1. Navigate to **Objects > Security Profiles > File Blocking**. 2. Click **Add** to add a new profile and enter a **Name** and **Description**. 3. Click **Add** in the **File Blocking Profile** window and then click **Add** again. Click in the **Names** field and enter a rule name. 4. Select the **Applications** that will match this profile. For example, selecting **web-browsing** as the application will cause the profile to match any application traffic identified as web-browsing. 5. In the **File Type** field, select the file types that will trigger the forwarding action. Choose **Any** to forward all file types supported by WildFire or select **PE** to only forward Portable Executable files. 6. In the **Direction** field select **upload**, **download**, or **both**. Selecting **both** will trigger forwarding whenever a user attempts to upload or download a file. 7. Define an **Action** as follows (choose **Forward** for this example): • **Forward**—The firewall will automatically forward any files matching this profile to WildFire for analysis in addition to delivering the file to the user. • **Continue-and-forward**—The user is prompted and must click **Continue** before the download occurs and the file is forwarded to WildFire. Because this action requires user interaction with a web browser, it is only supported for web-browsing applications. **Note** When using **continue-and-forward**, make sure that the ingress interface (the interface that first receives traffic for your users) has a management profile attached that allows response pages. To configure a management profile, select **Network > Network Profiles > Interface Mgmt** and select the **Response Pages** check box. Attach the management profile in the **Advanced** tab in the ingress interface configuration. 8. Click **OK** to save the changes.
Step 4 To forward files to WildFire from web sites using SSL encryption, enable forwarding of decrypted content. For information on configuring decryption, refer to the Palo Alto Networks Getting Started Guide. **Note** Only a superuser can enable this option.	1. Navigate to **Device > Setup > Content-ID**. 2. Click the edit icon for the **URL Filtering** options and enable **Allow Forwarding of Decrypted Content**. 3. Click **OK** to save the changes. **Note** If the firewall has multiple virtual systems, you must enable this option per VSYS. In this situation, navigate to **Device > Virtual Systems**, click the virtual system to be modified and select the **Allow Forwarding of Decrypted Content** check box.

CONFIGURE FORWARDING TO THE WF-500 WILDFIRE APPLIANCE (CONTINUED)		
Step 5	Attach the file blocking profile to a security policy.	1. Navigate to **Policies > Security**. 2. Click **Add** to create a new policy for the zones that you are applying WildFire forwarding to, or select an existing security policy. 3. On the **Actions** tab, select the **File Blocking** profile from the drop-down. **Note** If this security rule does not have any profiles attached to it, select **Profiles** from the **Profile Type** drop-down to enable selection of a file blocking profile.
Step 6	(Optional) Modify the maximum file size that the firewall can upload to WildFire.	1. Navigate to **Device > Setup > WildFire**. 2. Click the **General Settings** edit icon. 3. In the **Maximum File Size (MB)** field, enter the maximum file size for files are sent to WildFire for analysis (range 1-10 MB; default 2MB).
Step 7	(Optional) Modify session options that define what session information to record in WildFire analysis reports.	1. Click the **Session Information Settings** edit icon. 2. By default, all session information items will display in the reports. Clear the check boxes that correspond to any fields to remove from the WildFire analysis reports. 3. Click **OK** to save the changes.
Step 8	Commit the configuration.	Click **Commit** to apply the settings. During security policy evaluation, all files that meet the criteria defined in the file blocking policy will be forwarded to WildFire for analysis. For information on viewing reports for files that have been analyzed, see "Monitor, Track, and Prevent Malware on Your Network" on page 45. For information on verifying the configuration, see "Verify the WildFire Settings on the Firewall" on page 26.

Dynamic Updates Best Practices

The following bullet points list the best practice for dynamic updates on a typical firewall that is using WildFire and that has a WildFire and a Threat Prevention subscription. For a streamlined workflow, use Panorama to push dynamic update schedules to managed firewalls using Panorama templates. This ensures consistency across all firewalls and simplifies management of update schedules.

These guidelines provide two schedule options: the minimum recommended schedule and a more aggressive schedule. Choosing the more aggressive approach causes the device to perform updates much more frequently, some of which can be very large (over 100MB for antivirus updates). Also, in rare instances, there could be errors. Therefore, consider delaying new update installations until they have been released for a certain number of hours. Use the **Threshold (Hours)** field to specify how long after a release to wait before performing a content update.

- **Antivirus**—New antivirus content updates are released on a daily basis. To get the latest content, schedule these updates daily at minimum. For a more aggressive schedule, schedule them hourly.
- **Applications and Threats**—New App-ID, vulnerability protection, and anti-spyware signatures are released as weekly content updates (normally on Tuesdays). To receive the latest content, schedule the updates at least weekly. For a more aggressive schedule to ensure that the firewall receives the latest content soon after they are released (including occasional off-schedule emergency content releases), schedule them daily.
- **WildFire**—New WildFire antivirus signatures are published every 30 minutes. Depending on when new malware is discovered within the release cycle, coverage is provided in the form of a WildFire signature 30-60 minutes after it is first discovered by WildFire. To get the latest WildFire signatures, schedule these updates every hour or half-hour. For a more aggressive schedule, you may want to schedule the firewall to check for updates as often as every 15 minutes.

Although WildFire updates may conflict with an antivirus or threat signature update, it should update successfully because it is much smaller than typical antivirus/application and threat signature updates. Each WildFire update typically contains signatures generated over the last seven days at which point they are rolled into the antivirus signature updates every 24-48 hours.

Verify the WildFire Settings on the Firewall

This section describes the steps required to verify the WildFire configuration on the firewall.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL		
Step 1	Check the WildFire and Threat Prevention subscriptions and WildFire registration.	1. Navigate to **Device > Licenses** and confirm that a valid WildFire and Threat Prevention subscription is installed. If valid licenses are not installed, go to the **License Management** section and click **Retrieve license keys from the license server**.

Note	The firewall must have a WildFire subscription to forward files to a WildFire appliance.	2. To check that the firewall can communicate with a WildFire system, so files can be forwarded to it for analysis, run the following CLI command:
		`admin@PA-200> test wildfire registration`
		
		In the following output, the firewall is pointing to a WildFire appliance. If the firewall is pointing to the WildFire cloud, it will show the hostname of one of the WildFire systems in the WildFire cloud.
		`Test wildfire`
		`wildfire registration: successful`
		`download server list: successful`
		`select the best server: 192.168.2.20:10443`
		
		3. If problems persist with the licenses, contact your reseller or Palo Alto Networks System Engineer to confirm each license and to get a new authorization code if required.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)	
Step 2 Confirm that the firewall is sending files to the correct WildFire system.	1. To determine where the firewall is forwarding files (to the Palo Alto Networks WildFire cloud or to a WildFire appliance), navigate to **Device > Setup > WildFire**. 2. Click the **General Settings** edit button. 3. If the firewall is forwarding files to the WildFire cloud, this field should show **default-cloud**. If it is forwarding files to a WildFire appliance, the IP address or FQDN of the WildFire appliance will be displayed. In Panorama, the default cloud name is **wildfire-public-cloud**. **Note** If you modified the value in this field, but want to go back to the **default-cloud** setting, clear the **WildFire Server** field and click **OK**. This will reset the field back to the default. When using a WildFire appliance, make sure that disable-server-select is not enabled, otherwise the appliance will not be able to receive files sent from the firewall. Check the following setting and make sure it is set to no: `admin@PA-200# set deviceconfig setting wildfire disable-server-select`
Step 3 Check the logs.	1. Navigate to **Monitor > Logs > Data Filtering**. 2. Confirm that files are being forwarded to WildFire by viewing the **Action** column: • **Forward** is displayed if the file is successfully forwarded by the file blocking profile and security policy. • **Wildfire-upload-success** will be displayed if the file was sent to WildFire. This means the file is not signed by a trusted file signer and it has not been previously analyzed by WildFire. • **Wildfire-upload-skip** will be displayed for malware that has been seen before, so the sample does not need to be sent to the WildFire cloud. In this case, only session information (if enabled) will be sent in order to show a log entry in the WildFire web portal and in the Data Filtering log on the firewall. If benign file logging is enabled, **wildfire-upload-skip** will also be displayed for benign files that have been seen before. To enable this option run the following CLI command on the firewall: `admin@PA-200# set deviceconfig setting wildfire report-benign-file` 3. View the WildFire logs (subscription required) by selecting **Monitor > Logs > WildFire**. If WildFire logs are available, the firewall is successfully forwarding files to WildFire and WildFire is returning file analysis results. **Note** For more information on WildFire-related logs, refer to "About WildFire Logs" on page 46.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)		
Step 4	Check the file blocking policy.	1. Navigate to **Objects > Security Profiles > File Blocking** and click the file blocking profile to modify it. 2. Confirm that the action is set to **forward** or **continue-and-forward**. If set to **continue-and-forward**, only http/https traffic will be forwarded because this is the only type of traffic that allows for prompting the user to click continue.
Step 5	Check the security policy.	1. Navigate to **Policies > Security** and click the security policy rule that triggers file forwarding to WildFire. 2. Click the **Actions** tab and ensure that the file blocking policy is selected in the **File Blocking** drop-down.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)

Step 6 Check the WildFire status.

Run the following CLI commands to check the status of WildFire and verify that statistics are incrementing:

- Check the status of WildFire:

```
admin@PA-200> show wildfire status
```

When forwarding files to the WildFire cloud, the output should look as follows:

```
Connection info:
        Wildfire cloud:                 default cloud
        Status:                         Idle
        Best server:      ca-s1.wildfire.paloaltonetworks.com
        Device registered:              yes
        Valid wildfire license:         yes
        Service route IP address:       192.168.2.1
        Signature verification:         enable
        Server selection:               enable
        Through a proxy:                no

Forwarding info:
        file size limit (MB):           2
        file idle time out (second):    90
        total file forwarded:           0
        forwarding rate (per minute):   0
        concurrent files:               0
```

Note If the firewall is forwarding files to a WildFire appliance, the `Wildfire cloud:` field will display the IP address or hostname of the appliance and `Best server:` will not display a value.

- Use the following command to check statistics to determine if the values have incremented:

```
admin@PA-200> show wildfire statistics
```

The following displays the output of a working firewall. If no values display, the firewall is not forwarding files.

```
        Total msg rcvd:                          8819
        Total bytes rcvd:                     7064822
        Total msg read:                          8684
        Total bytes read:                     6756221
        Total msg lost by read:                   135
        DP receiver reset count:                    2
        Total file count:                          42
        CANCEL_FILE_DUP                            31
        CANCEL_FILESIZE_LIMIT                       2
        DROP_NO_MATCH_FILE                        135
        FWD_CNT_LOCAL_FILE                          9
        FWD_CNT_LOCAL_DUP                          30
        FWD_CNT_REMOTE_FILE                         9
        FWD_CNT_REMOTE_DUP_CLEAN                   24
        FWD_CNT_REMOTE_DUP_TBD                      3
        FWD_CNT_CACHE_SYNC                          1
        FWD_ERR_CONN_FAIL                       16776
        LOG_ERR_REPORT_CACHE_NOMATCH               47
        Service connection reset cnt:               1
        data_buf_meter                             0%
        msg_buf_meter                              0%
        ctrl_msg_buf_meter                         0%
        fbf_buf_meter                              0%
```

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)		
Step 7	Check dynamic updates status and schedules. To ensure that the firewall is automatically receiving signatures generated by WildFire.	1. Navigate to **Device > Dynamic Updates**. 2. Ensure that Antivirus, Applications and Threats, and WildFire have the most recent updates and that a schedule is set for each item. Stagger the update schedules because only one update can be performed at a time. 3. Click **Check Now** at the bottom of the windows to see if any new updates are available, which also confirms that the firewall can communicate with updates.paloaltonetworks.com. If the firewall does not have connectivity to the update server, download the updates directly from Palo Alto Networks. Log in to https://support.paloaltonetworks.com and in the **Manage Devices** section, click **Dynamic Updates** to see available updates. For more information on dynamic updates, refer to the Manage Content Updates section of the Palo Alto Networks Getting Started Guide.

3 Analyze Files Using the WildFire Cloud

This chapter describes the steps required to start uploading files to the Palo Alto Networks WildFire cloud for file analysis directly from the firewall, manually from the portal, or programmatically via the WildFire API. It includes the following sections:

Forward Files to the WildFire Cloud

To configure a firewall to automatically submit unknown files to WildFire, configure a file blocking profile with the forward or continue-and-forward action and then attach it to the security rule(s) that you want to inspect for zero-day malware. For example, you could configure a policy with a file blocking profile that triggers the firewall to forward any exe files users attempt to download during a web-browsing session. Forwarding of SSL-encrypted files is also supported provided that SSL decryption is configured on the firewall and the option to forward encrypted files is enabled.

If there is a firewall between the firewall that is forwarding files to WildFire and the WildFire cloud or WildFire appliance, make sure that the firewall in the middle has the necessary ports allowed.

- WildFire cloud: Uses port 443 for registration and file submissions.
- WildFire appliance: Uses port 443 for registration and 10443 for file submissions.

Perform the following steps on each firewall that will forward files to WildFire:

CONFIGURE A FILE BLOCKING PROFILE AND ADD IT TO A SECURITY PROFILE	
Step 1 Verify that the firewall has valid Threat Prevention and WildFire subscriptions and that dynamic updates are scheduled and up-to-date. **Note** Although the firewall can forward files to WildFire without a WildFire subscription, the WildFire logs will not be available on the firewall and the firewall will not receive sub-hourly WildFire malware signature updates. For more information on subscriptions, refer to "What are the Benefits of the WildFire Subscription?" on page 5.	1. Navigate to **Device > Licenses** and confirm that the firewall has valid WildFire and Threat Prevention subscriptions. 2. Navigate to **Device > Dynamic Updates** and click **Check Now** to ensure that the firewall has the most recent Antivirus, Applications and Threats, and WildFire updates. 3. If the updates are not scheduled, schedule them now. Be sure to stagger the update schedules because only one update can be performed at a time. See "Dynamic Updates Best Practices" on page 34 for recommended settings.

CONFIGURE A FILE BLOCKING PROFILE AND ADD IT TO A SECURITY PROFILE (CONTINUED)	
Step 2 Configure the file blocking profile to define which applications and file types will trigger forwarding to WildFire. **Note** If you choose **PE** in the objects profile File Types column to select a category of file types, do not also add an individual file type that is part of that category because this will result in redundant entries in the Data Filtering logs. For example, if you select PE do not select **exe** because it is part of the PE category. This also applies to the **zip** file type, because supported file types that are zipped are automatically sent to WildFire. Choosing a category rather than an individual file type also ensures that as new file type support is added to a given category, they are automatically made part of the file blocking profile. If you select **Any**, all supported file types will be forwarded to WildFire.	1. Navigate to **Objects > Security Profiles > File Blocking**. 2. Click **Add** to add a new profile and enter a **Name** and **Description**. 3. Click **Add** in the **File Blocking Profile** window and then click **Add** again. Click in the **Names** field and enter a rule name. 4. Select the **Applications** that will match this profile. For example, selecting **web-browsing** as the application will cause the profile to match any application traffic identified as web-browsing. 5. In the **File Type** field, select the file types that will trigger the forwarding action. Choose **Any** to forward all file types supported by WildFire or select **PE** to only forward Portable Executable files. 6. In the **Direction** field select **upload**, **download**, or **both**. The **both** option will trigger forwarding whenever a user attempts to upload or download a file. 7. Define an **Action** as follows: • **Forward**—The firewall will automatically forward any files matching this profile to WildFire for analysis in addition to delivering the file to the user. • **Continue-and-forward**—The user is prompted and must click continue before the download occurs and the file is forwarded to WildFire. Because this action requires user interaction with a web browser, it is only supported for web-browsing applications. **Note** When using **continue-and-forward**, make sure that the ingress interface (the interface that first receives traffic for your users) has a management profile attached that allows response pages. To configure a management profile, select **Network > Network Profiles > Interface Mgmt** and select the **Response Pages** check box. Attach the management profile in the **Advanced** tab in the ingress interface configuration. 8. Click **OK** to save the changes.
Step 3 To forward files to WildFire from web sites using SSL encryption, enable forwarding of decrypted content. For information on configuring decryption, refer to the Palo Alto Networks Getting Started Guide. **Note** Only a superuser can enable this option.	1. Navigate to **Device > Setup > Content-ID**. 2. Click the edit icon for the **URL Filtering** options and enable **Allow Forwarding of Decrypted Content**. 3. Click **OK** to save the changes. **Note** If the firewall has multiple virtual systems, you must enable this option per VSYS. In this situation, navigate to **Device > Virtual Systems**, click the virtual system to be modified and select the **Allow Forwarding of Decrypted Content** check box.

CONFIGURE A FILE BLOCKING PROFILE AND ADD IT TO A SECURITY PROFILE (CONTINUED)		
Step 4	Attach the file blocking profile to a security policy.	1. Navigate to **Policies > Security**. 2. Click **Add** to create a new policy for the zones to which to apply WildFire forwarding, or select an existing security policy. 3. On the **Actions** tab, select the **File Blocking** profile from the drop-down. **Note** If this security rule does not have any profiles attached to it, select **Profiles** from the **Profile Type** drop-down to enable selection of a file blocking profile.
Step 5	(Optional) Modify the maximum file size allowed for upload to WildFire.	1. Navigate to **Device > Setup > WildFire**. 2. Click the **General Settings** edit icon. 3. In the **Maximum File Size (MB)** field, enter the maximum file size for files that will be sent to WildFire for analysis (range 1-10 MB; default 2MB).
Step 6	(Optional) Modify session options that define what session information to record in WildFire analysis reports.	1. Click the **Session Information Settings** edit icon. 2. By default, all session information items will display in the reports. Clear the check boxes that correspond to any fields to remove from the WildFire analysis reports. 3. Click **OK** to save the changes.
Step 7	Commit the configuration.	Click **Commit** to apply the settings. During security policy evaluation, all files that meet the criteria defined in the file blocking policy will be forwarded to WildFire for analysis. For information on viewing reports for files that have been analyzed, see "Monitor, Track, and Prevent Malware on Your Network" on page 45. For information on verifying the configuration, see "Verify the WildFire Settings on the Firewall" on page 35.

Dynamic Updates Best Practices

The following bullet points list the best practice for dynamic updates on a typical firewall that is using WildFire and that has a WildFire and a Threat Prevention subscription. For a streamlined workflow, use Panorama to push dynamic update schedules to managed firewalls using Panorama templates. This ensures consistency across all firewalls and simplifies management of update schedules.

These guidelines provide two schedule options: the minimum recommended schedule and a more aggressive schedule. Choosing the more aggressive approach causes the device to perform updates much more frequently, some of which can be very large (over 100MB for antivirus updates). Also, in rare instances, there could be errors. Therefore, consider delaying new update installations until they have been released for a certain number of hours. Use the **Threshold (Hours)** field to specify how long after a release to wait before performing a content update.

- **Antivirus**—New antivirus content updates are released on a daily basis. To get the latest content, schedule these updates daily at minimum. For a more aggressive schedule, schedule them hourly.

- **Applications and Threats**—New App-ID, vulnerability protection, and anti-spyware signatures are released as weekly content updates (normally on Tuesdays). To receive the latest content, schedule the updates at least weekly. For a more aggressive schedule to ensure that the firewall receives the latest content soon after they are released (including occasional off-schedule emergency content releases), schedule them daily.
- **WildFire**—New WildFire antivirus signatures are published every 30 minutes. Depending on when new malware is discovered within the release cycle, coverage is provided in the form of a WildFire signature 30-60 minutes after it is first discovered by WildFire. To get the latest WildFire signatures, schedule these updates every hour or half-hour. For a more aggressive schedule, you may want to schedule the firewall to check for updates as often as every 15 minutes.

Verify the WildFire Settings on the Firewall

This section describes the steps required to verify the WildFire configuration on the firewall.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL		

Step 1	Check the WildFire and Threat Prevention subscription and WildFire registration.	1. Navigate to **Device > Licenses** and confirm that a valid WildFire and Threat Prevention subscription is installed. If valid licenses are not installed, go to the **License Management** section and click **Retrieve license keys from the license server**.
		2. To check that the firewall can communicate with a WildFire system, so files can be forwarded to it for analysis, run the following CLI command:
		`admin@PA-200> test wildfire registration`
		In the following output, the firewall is pointing to the WildFire cloud. If the firewall is pointing to a WildFire appliance, it will show the hostname or IP address of the appliance.
		`Test wildfire`
		`wildfire registration: successful`
		`download server list: successful`
		`select the best server: ca-s1.wildfire`
		3. If problems persist with the licenses, contact your reseller or Palo Alto Networks System Engineer to confirm each license and to get a new authorization code if required.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)	
Step 2 Confirm that the firewall is sending files to the correct WildFire system.	1. To determine where the firewall is forwarding files (to the Palo Alto Networks WildFire cloud or to a WildFire appliance), navigate to **Device > Setup > WildFire**. 2. Click the **General Settings** edit button. 3. If the firewall is forwarding files to the WildFire cloud, this field should show **default-cloud**. If it is forwarding files to a WildFire appliance, the IP address or FQDN of the WildFire appliance will be displayed. In Panorama, the default cloud name is **wildfire-public-cloud**. **Note** If you modified the value in this field, but want to go back to the **default-cloud** setting, clear the **WildFire Server** field and click **OK**. This will reset the field back to the default. If this field does not allow editing, check the following setting and make sure it is set to no: `admin@PA-200# set deviceconfig setting wildfire disable-server-select`
Step 3 Check the logs.	1. Navigate to **Monitor > Logs > Data Filtering**. 2. Confirm that files are being forwarded to WildFire by viewing the **Action** column: • **Forward** is displayed if the file is successfully forwarded by the file blocking profile and security policy. • **Wildfire-upload-success** will be displayed if the file was sent to WildFire. This means the file is not signed by a trusted file signer and it has not been previously analyzed by WildFire. • **Wildfire-upload-skip** will be displayed for malware that has been seen before, so the sample does not need to be sent to the WildFire cloud. In this case, only session information (if enabled) will be sent in order to show a log entry in the WildFire web portal and in the Data Filtering log on the firewall. If benign file logging is enabled, **wildfire-upload-skip** will also be displayed for benign files that have been seen before. To enable this option run the following CLI command on the firewall: `admin@PA-200# set deviceconfig setting wildfire report-benign-file` 3. View the WildFire logs (subscription required) by selecting **Monitor > Logs > WildFire**. If WildFire logs are available, the firewall is successfully forwarding files to WildFire and WildFire is returning file analysis results. **Note** For more information on WildFire-related logs, refer to "About WildFire Logs" on page 46.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)		
Step 4	Check the file blocking policy.	1. Navigate to **Objects > Security Profiles > File Blocking** and click the file blocking profile to modify it. 2. Confirm that the action is set to **forward** or **continue-and-forward**. If set to **continue-and-forward**, only http/https traffic will be forwarded because this is the only type of traffic that allows for prompting the user to click continue.
Step 5	Check the security policy.	1. Navigate to **Policies > Security** and click the security policy rule that triggers file forwarding to WildFire. 2. Click the **Actions** tab and ensure that the file blocking policy is selected in the **File Blocking** drop-down.

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)

Step 6 Check the WildFire status.

Run the following CLI commands to check the status of WildFire and verify that statistics are incrementing:

- Check the status of WildFire:

```
admin@PA-200> show wildfire status
```

When forwarding files to the WildFire cloud, the output should look as follows:

```
Connection info:
        Wildfire cloud:                 default cloud
        Status:                         Idle
        Best server:      ca-s1.wildfire.paloaltonetworks.com
        Device registered:              yes
        Valid wildfire license:         yes
        Service route IP address:       192.168.2.1
        Signature verification:         enable
        Server selection:               enable
        Through a proxy:                no

Forwarding info:
        file size limit (MB):           2
        file idle time out (second):    90
        total file forwarded:           0
        forwarding rate (per minute):   0
        concurrent files:               0
```

Note If the firewall is forwarding files to a WildFire appliance, the `Wildfire cloud:` field will display the IP address or hostname of the appliance and `Best server:` will not display a value.

- Use the following command to check statistics to determine if the values have incremented:

```
admin@PA-200> show wildfire statistics
```

The following displays the output of a working firewall. If no values display, the firewall is not forwarding files.

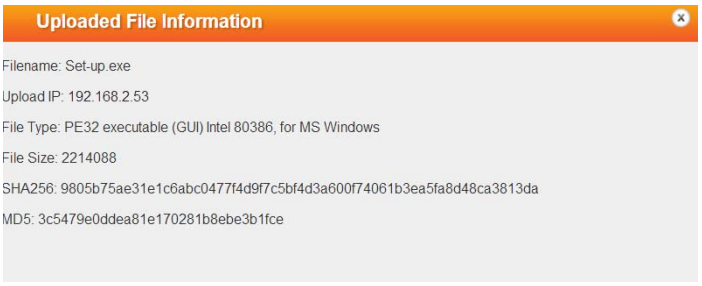
```
        Total msg rcvd:                          8819
        Total bytes rcvd:                     7064822
        Total msg read:                          8684
        Total bytes read:                     6756221
        Total msg lost by read:                  135
        DP receiver reset count:                   2
        Total file count:                         42
        CANCEL_FILE_DUP                           31
        CANCEL_FILESIZE_LIMIT                      2
        DROP_NO_MATCH_FILE                       135
        FWD_CNT_LOCAL_FILE                         9
        FWD_CNT_LOCAL_DUP                         30
        FWD_CNT_REMOTE_FILE                        9
        FWD_CNT_REMOTE_DUP_CLEAN                  24
        FWD_CNT_REMOTE_DUP_TBD                     3
        FWD_CNT_CACHE_SYNC                         1
        FWD_ERR_CONN_FAIL                      16776
        LOG_ERR_REPORT_CACHE_NOMATCH              47
        Service connection reset cnt:              1
        data_buf_meter                            0%
        msg_buf_meter                             0%
        ctrl_msg_buf_meter                        0%
        fbf_buf_meter                             0%
```

VERIFY THE WILDFIRE CONFIGURATION ON THE FIREWALL (CONTINUED)		
Step 7	Check dynamic updates status and schedules. To ensure that the firewall is automatically receiving signatures generated by WildFire.	1. Navigate to **Device > Dynamic Updates**. 2. Ensure that Antivirus, Applications and Threats, and WildFire have the most recent updates and that a schedule is set for each item. Stagger the update schedules because only one update can be performed at a time. 3. Click **Check Now** at the bottom of the windows to see if any new updates are available, which also confirms that the firewall can communicate with updates.paloaltonetworks.com. If the firewall does not have connectivity to the update server, download the updates directly from Palo Alto Networks. Log in to https://support.paloaltonetworks.com and in the **Manage Devices** section, click **Dynamic Updates** to see available updates. For more information on dynamic updates, refer to the Manage Content Updates section of the Palo Alto Networks Getting Started Guide.

Upload Files to the WildFire Cloud Portal

All Palo Alto Networks customers with a support account can manually upload files to the Palo Alto Networks WildFire portal for analysis. The WildFire portal supports manual upload of Win32 PE files that are a maximum of 10MB.

The following procedure describes the steps to upload files manually:

MANUAL UPLOAD TO WILDFIRE		
Step 1	Upload a file to be analyzed by WildFire.	1. Navigate to https://wildfire.paloaltonetworks.com/ and log in. 2. Click the **Upload File** button near the upper right side of the page and click **Choose File**. 3. Navigate to the file, highlight it, and then click **Open**. The file name will appear next to **Choose File**. 4. Click the **Upload** button to upload the file to WildFire. If the file uploads successfully, an **Uploaded File Information** pop-up similar to the following will display:  5. Close the **Uploaded File Information** pop-up.
Step 2	View the analysis results. It will take approximately five minutes for WildFire to complete a file analysis. **Note** Because a manual upload is not associated with a specific firewall, manual uploads will appear separately from your registered firewalls.	1. Refresh the portal page from your browser. 2. A **Manual** line item will be displayed in the **Device** list of your portal page and the analysis result **Malware** or **Benign** will also be displayed. Click the word **Manual**. 3. The report page will show a list of all files that have been uploaded to your account. Find the uploaded file and click the detail icon to the left of the date field. The portal displays a full report of the file analysis detailing the observed file behavior, including the user that was targeted, the application that delivered the malware, and all URLs involved in the delivery or phone-home activity of the sample. If WildFire identifies the file as malware, it generates a signature, which will be distributed to all Palo Alto Networks firewalls configured for Threat Prevention. Firewalls with a WildFire subscription can download these signatures on a sub-hourly basis.

Upload Files Using the WildFire API

Using the WildFire API, you can programmatically send file analysis jobs to the WildFire cloud and query the system for report data through a simple RESTful API interface.

This section contains the following topics:

About WildFire Subscriptions and API Keys

Access to the WildFire API key is provided if at least one Palo Alto Networks firewall has an active WildFire subscription registered to an account holder in your organization. You can share the same API key within your organization. The API key is displayed in the **My Account** section of the WildFire web portal, along with statistics, such as how many uploads and queries have been performed using the key. The key should be considered secret and should not be shared outside of authorized channels.

How to Use the WildFire API?

The WildFire API is a RESTful API that uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports RESTful services.

The API methods are hosted at https://wildfire.paloaltonetworks.com/ and the HTTPS protocol (not HTTP) is required in order to protect your API key and any other data exchanged with the service.

A WildFire API key allows up to 100 sample uploads per day and up to 1000 report queries per day.

WildFire API Submission Methods

Use the following methods to submit files to WildFire:

Submit a File to the WildFire Cloud Using the Submit File Method

The WildFire API supports Win32 executable files. The file along with your API key is required when submitting to have WildFire open the file in a sandbox environment and analyze the file for potentially malicious behaviors. The return code of the submit-file method indicates a success or error condition. If a 200 OK code was returned, the submission was successful and a result is normally available for query within five minutes.

URL	https://wildfire.paloaltonetworks.com/submit-file	
Method	POST	
Parameters	file	The sample file to be analyzed
	apikey	Your WildFire API key
Return	200 OK	Success; WildFire will process submission
	401 Unauthorized	API key invalid
	402 Payment Required	API key expired
	403 Forbidden	API key revoked
	405 Method Not Allowed	Method other than POST used
	406 Not Acceptable	API key error
	413 Request Entity Too Large	Sample file size over max limit of 10MB
	418 Unsupported File Type	Sample file type is not supported
	419 Max Request Reached	Max number of uploads per day exceeded

Submit a File to WildFire Using the Submit URL Method

Use the submit-url method to submit a file for analysis via a URL. This method is identical in interface and functionality to the submit-file method, except that the file parameter is replaced with a url parameter. The url parameter must point to an accessible supported file type (Win32 executable files). If a 200 OK code is returned, the submission is successful and a result is usually available for query within five minutes.

URL	https://wildfire.paloaltonetworks.com/submit-url	
Method	POST	
Parameters	url	The URL for the file to be analyzed
	apikey	Your WildFire API key

Return	200 OK	Success; WildFire will process submission
	401 Unauthorized	API key invalid
	402 Payment Required	API key expired
	403 Forbidden	API key revoked
	405 Method Not Allowed	Method other than POST used
	406 Not Acceptable	API key error
	413 Request Entity Too Large	Sample file size over max limit of 10MB
	418 Unsupported File Type	Sample file type is not supported
	419 Max Request Reached	Max number of uploads per day exceeded

Query for a WildFire XML Report

Use the get-report-xml method to query for an XML report of analysis results for a particular sample. Use either the MD5 or SHA-256 hash of the sample file as a search query.

URL	https://wildfire.paloaltonetworks.com/get-report-xml	
Method	POST	
Parameters	md5	The MD5 hash of the requested report or the sha256 hash as displayed in the next row.
	sha256	The SHA-256 hash of the requested report
	`apikey`	Your WildFire API key
Return	200 OK	Success; WildFire will process submission
	401 Unauthorized	API key invalid
	404 Not Found	The report was not found
	405 Method Not Allowed	Method other than POST used

Reports can also be retrieved from the WildFire cloud based on the serial number (device_ID) of the firewall that forwarded the file and the report ID (tid). The tid value can be located in the CSV, syslog, or API export of a threat log.

URL	https://wildfire.paloaltonetworks.com/publicapi/report
Method	POST

Parameters	device_id	The serial number of the firewall that forwarded the file to WildFire.
	report_id	The report ID (tid) is located in the CSV, syslog, or API export of a threat log.
	format	XML
Return	200 OK	Success; WildFire will process submission
	401 Unauthorized	API key invalid
	404 Not Found	The report was not found
	405 Method Not Allowed	Method other than POST used

Code Examples for Submit and Query

The following shell code example demonstrates a simple script to submit a file to the WildFire API for analysis. The API key is provided as the first parameter and the path to the file is the second parameter:

```
#manual upload sample to WildFire with APIKEY
#Parameter 1: APIKEY
#Parameter 2: location of the file

key=$1
file=$2

/usr/bin/curl -i -k -F apikey=$key -F file=@$file
https://wildfire.paloaltonetworks.com/submit-file
```

The following cURL command demonstrates a query for an XML report using the MD5 hash of the sample of interest:

```
curl -i -k -F md5=[MD5 HASH] -F apikey=[API KEY] -F
https://wildfire.paloaltonetworks.com/get-report-xml
```

The following cURL command demonstrates a query for an XML report using the device_ID and report_ID of the sample of interest:

```
curl -i -k -F device_id=[SERIAL NUMBER] -F report_id=[TID FROM LOG] -F format=xml
https://wildfire.paloaltonetworks.com/publicapi/report
```

4 Monitor, Track, and Prevent Malware on Your Network

This chapter describes the WildFire reporting and logging system and will show administrators how to use this information to track down threats and to identify users who have been targeted by malware.

About WildFire Logs

Each firewall that is configured to forward files to WildFire will log the forward action in the data filtering logs and after WildFire analyzes the file, the results will be sent back to the firewall and will appear in the WildFire logs (WildFire subscription required). The detailed analysis report for each file is available in the detailed WildFire log by clicking the **View WildFire Report** button. The report is then retrieved from the WildFire appliance or the WildFire cloud. If a WildFire subscription is not installed and the firewall is forwarding files to the WildFire cloud, the analysis report can be viewed from the WildFire portal at https://wildfire.paloaltonetworks.com.

If your firewalls are forwarding files to a WildFire appliance for analysis, log results can only be viewed from the firewall; there is no direct web portal access to the appliance.

- **Forwarding Action Logs**—The data filtering logs located in **Monitor > Logs > Data Filtering** will show the files that were blocked/forwarded based on the file blocking profile. To determine which files were forwarded to WildFire, look for the following values in the **Action** column of the log:

Log	Description
wildfire-upload-success	The file was sent to the cloud. This means the file is not signed by a trusted file signer, it has not been previously analyzed by WildFire.
wildfire-upload-skip	This will be displayed for malware that has been seen before, where the sample does not need to be sent to the WildFire cloud. In this case, only session information (if enabled) will be sent in order to show a log entry in the WildFire web portal. If benign file logging is enabled, **wildfire-upload-skip** will also be displayed for benign files that have been seen before where the file does not need to be sent to the cloud for analysis.

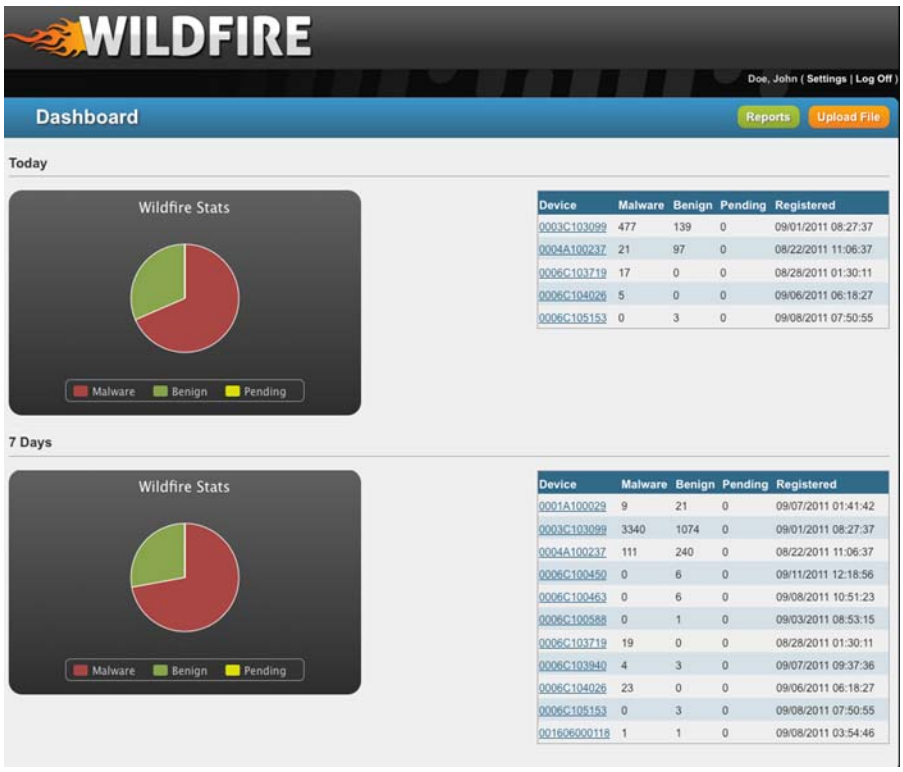
- **WildFire Logs**—The analysis results of the files scanned by WildFire are sent back to the firewall logs (WildFire subscription required) after the analysis completes. These logs are written to the firewall that forwarded the file in **Monitor > Logs > WildFire**. If logs are forwarded from the firewall to Panorama, the logs are written to the Panorama server in **Monitor > Logs > WildFire Submissions**. The **Category** column for the WildFire logs will either show **benign**, meaning that the file is safe, or **malicious**, indicating that WildFire determined that the file contains malicious code. If the file is determined to be malicious, a signature will be generated by the WildFire signature generator. If you are using a WildFire appliance, auto-submit must be enabled on the appliance so malware infected files will be sent to the WildFire cloud for signature generation.

  To view the detailed report for a file that has been analyzed by WildFire, locate the log entry in the WildFire log, click the icon to the left of the log entry to show the log details and then click the **View WildFire Report** button. A login prompt will appear to access the report and after entering the correct credentials the report is retrieved from the WildFire system and is displayed in your browser. For information on portal accounts to access the WildFire cloud, see "WildFire Portal User Accounts" on page 49. For information on the admin account that is used to retrieve reports from a WildFire appliance, see "Perform the Initial Configuration" on page 10 and the step that describes the portal-admin account.

Monitor Submissions Using the WildFire Cloud

Browse to the Palo Alto Networks WildFire cloud at https://wildfire.paloaltonetworks.com and log in 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 (as well as any files that have been uploaded manually). For each device, statistics will be displayed for the number of malware files that have been detected, benign files that have been analyzed, and the number of pending files that are waiting to be analyzed. Also displayed is the date and time that the firewall first registered with the portal to begin file forwarding to WildFire.

For information on configuring additional WildFire accounts that can be used to review report information, see "WildFire Portal User Accounts" on page 49.



Customize WildFire Portal Settings

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

WILDFIRE PORTAL SETTINGS	
Step 1 Configure the time zone for the portal account.	1. Navigate to the portal at https://wildfire.paloaltonetworks.com and log in using your Palo Alto Networks support login credentials or your WildFire user account. 2. Click the **Settings** link located at the upper right of the portal window. 3. Select the time zone from the drop-down and then click **Update Time Zone** to save the change. **Note** The time stamp that will appear on the WildFire detailed report will use the time zone set on your portal account. 4. Click the **Settings** link again to return to the settings page.
Step 2 Delete WildFire logs for specific firewalls. This will delete all logs and notifications for the selected firewall.	1. In the **Delete WildFire Logs** drop-down, select the firewall (by serial number). 2. Click the **Delete Logs** button. 3. Click **OK** to proceed with the deletion.
Step 3 Configure email notifications that will be generated based on the results of files submitted to WildFire.	1. From the portal settings page, locate the **Email Notifications** section. A table will be displayed with the column headings **Device**, **Malware**, and **Benign**. 2. The first row item will show **Manual**. Select **Malware** and/or **Benign** to receive a notification for files that are manually uploaded to the WildFire cloud, or that are submitted using the WildFire API. To receive notifications for firewalls that forward to the WildFire cloud, check the **Malware** and/or **Benign** check box next to each firewall. **Note** Select the check boxes directly below the column headings **Malware** and **Benign** to select all of the check boxes for the listed devices.

WildFire Portal User Accounts

WildFire portal accounts are created by a super user (or the registered owner of a Palo Alto Networks device) to give additional users the ability to log in to the WildFire web portal and view WildFire data for devices specifically granted by the super user or registered owner. A super user is the person who registered a Palo Alto Networks firewall and has the main support account for the device(s). The WildFire user can be an existing support site user that belongs to any account (including the sub-account, parent account, or any other account in the system), or they may not have a Palo Alto Networks support account at all and can be granted access to just the WildFire portal and a specific set of firewalls.

Add WildFire User Accounts

This section describes the steps required to add additional WildFire accounts to the WildFire cloud.

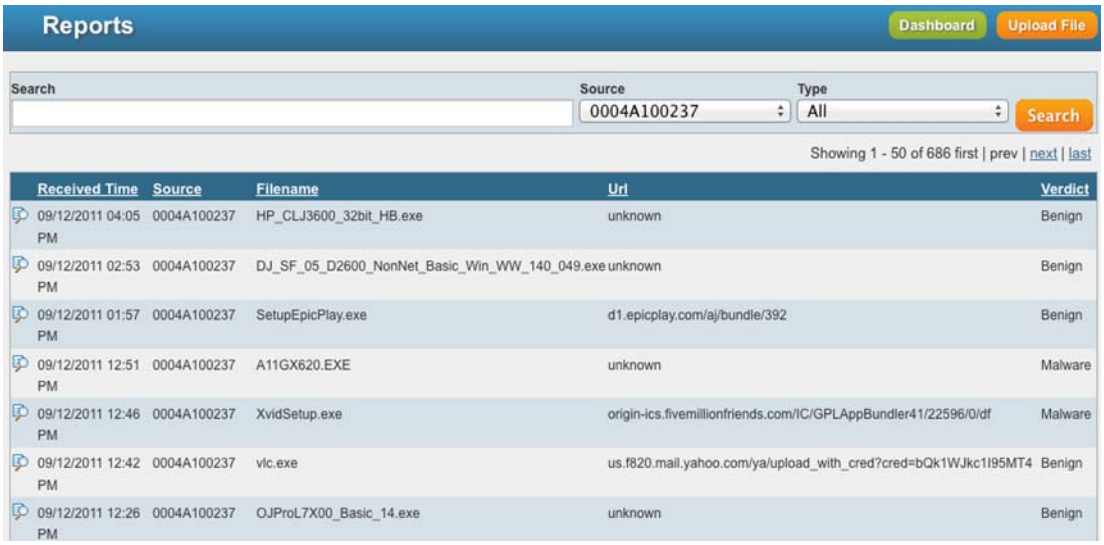
ADD WILDFIRE USER ACCOUNTS		
Step 1	Access the manage users and accounts section on the support site and select an account.	3. Log in to https://support.paloaltonetworks.com/. 4. Under **Manage Account** click on **Users and Accounts**. 5. Select an existing account or sub-account.
Step 2	Add a WildFire user.	1. Click the **Add WildFire User** button. 2. Enter the email address for the user recipient would like to add. **Note** The user can be an existing support site user that belongs to any account (including the sub-account, parent account, Palo Alto Networks, or any other account in the system), as well as any email address that does not have a support account at all. The only restriction is that the email address cannot be from a free web-based email account (Gmail, Hotmail, Yahoo, and so on). If an email address is entered for a domain that is not supported, a pop-up warning will be displayed.
Step 3	Assign firewalls to the new user account and access the WildFire portal.	1. Select the firewall(s) by S/N that you want to grant access to and fill out the optional account details. 2. An email will then be sent to the user. 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, an email will be sent with instructions on how to access the portal and how to set up a new password. 3. User can now log in to https://wildfire.paloaltonetworks.com and view WildFire reports for the firewalls to which they have been granted access. User 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 WildFire Reports

The primary method for viewing WildFire reports sent to the WildFire cloud or to a WildFire appliance is to access the firewall that forwarded the file to WildFire and then view the WildFire logs from the monitor tab. Click the log detail icon to the left of the WildFire log entry to view more details about the session and then click the **View WildFire Reports** icon to view the detailed WildFire analysis report. If the firewall is forwarding logs to Panorama, logs can be viewed from Panorama in the same area.

When submitting files to the WildFire portal (by firewall forwarding, manual upload, or the WildFire API), reports can be accessed from the firewall as well as from the WildFire portal. To access the reports from the portal, log in to https://wildfire.paloaltonetworks.com and click the **Reports** button at the top of the WildFire portal page. A list will be displayed showing the date the file was received, the firewall serial number that forwarded the file (or manual if the file was uploaded manually or using the WildFire API) and the filename or URL. Search options are also available at the top of the page and pagination controls are included.

To view an individual report from the portal, click the **Reports** icon to the left of the report name. To print a detailed report, use the browser print option. The following shows a sample report:



What is in the WildFire Reports?

The reports will show detailed behavioral information on the file that was run in the WildFire system, along with information on the user who was targeted, the application that delivered the file, and all URLs involved in the delivery or phone-home activity of the file. The following table describes each section that will be displayed in a typical WildFire analysis report. The organization of the report may differ depending on the version of the WildFire appliance software installed on the WildFire appliance, or if reports are viewed from the WildFire cloud. The report will contain some or all of the following information based on the session information defined on the firewall that forwarded the file and depending on the observed behavior.

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 it was not forwarded by a firewall. For example, the report would not show the Attacker/Source and Victim/Destination.

Report Heading	Description

File Information	• **SHA-256**—Displays the SHA information for the file. The SHA information is much like a fingerprint that uniquely identifies a file to ensure that the file has not been modified in any way. If the SHA information is compared with the original source file and they differ, then the file has been modified in some way.
	• **Antivirus Coverage**—Click this link to see if the file has been previously identified. This will bring up the https://www.virustotal.com/en/ website, which contains information about various antivirus vendors and will show whether or not the vendors have coverage for the infected file. If the file has never been seen by any of the listed vendors, **file not found** will be displayed.
	• **Verdict**—Displays the analysis verdict:
	  • **Benign**—The file is safe and does not exhibit malware behavior.
	  • **Malware**—WildFire identified the file as malware and will generate a signature to protect against future exposure. If a WildFire appliance analyzed the file and auto-submit is disabled, the file will not be forwarded to the WildFire cloud, so a signature will not be generated.

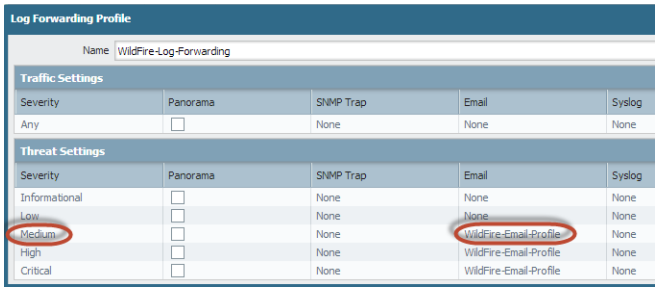
Session Information	Displays the session information that will appear in the WildFire reports. The settings for these options are defined on the firewall that sends the sample file to WildFire and is configured in **Device > Setup > WildFire** tab in the **Session Information Settings** section. The following lists the available options: • Source IP • Source Port • Destination IP • Destination Port • Virtual System (If multi-vsys is configured on the firewall) • Application • User (If User-ID is configured on the firewall) • URL • Filename
Behavioral Summary	Details the various behaviors that the file performed. Examples include whether it created or modified files, started a process, spawned new processes, modified the registry, or installed browser helper objects.
Network Activity	Shows network activity generated by the sample, such as accessing other hosts on the network and phone-home activity.
Host Activity	Lists any registry keys that were set, modified, or deleted.
Process	Lists files that started a parent process, the process name, and the action the process performed.
File	Lists files that started a child processes, the process name, and the action the process performed.

Set Up Alerts for Detected Malware

This section describes the steps required to configure a Palo Alto Networks firewall to send an alert each time WildFire returns a threat log to the firewall indicating malware was detected. This example describes how to configure an email alert. To configure syslogging, SNMP traps and/or log forwarding to Panorama, make sure the firewall is configured with SNMP server information and that the firewall is managed by Panorama. Panorama, syslog, or SNMP can then be selected along with Email as described in the following steps:

For more information on alerts and log forwarding, refer to the Palo Alto Networks Getting Started Guide section "Set Up Email Alerts", "Define Syslog Servers", and the "Set Up SNMP Trap Destinations" sections.

SET UP EMAIL ALERTS FOR MALWARE	
Step 1. Configure an email server profile if one is not configured.	1. Navigate to **Device > Server Profiles > Email**. 2. Click **Add** and then enter a **Name** for the profile. For example, **WildFire-Email-Profile**. 3. (Optional) Select the virtual system to which this profile applies from the **Location** drop-down. 4. Click **Add** 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): • **Server**—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. • **Display Name**—The name to show in the From field of the email. • **From**—The email address where notification emails will be sent from. • **To**—The email address to which notification emails will be sent. • **Additional Recipient(s)**—Enter an email address to send notifications to a second recipient. • **Gateway**—The IP address or host name of the SMTP gateway to use to send the emails. 5. Click **OK** to save the server profile. 6. Click **commit** to save the changes to the running configuration.
Step 2 Test the email server profile.	1. Navigate to **Monitor > PDF Reports > Email Scheduler**. 2. Click **Add** and select the new email profile from the **Email Profile** drop-down. 3. Click the **Send test** email button and a test email should be sent to the recipients defined in the email profile.

SET UP EMAIL ALERTS FOR MALWARE	(Continued)
Step 3 Configure a log forwarding profile. The log forwarding profile determines what traffic is monitored and what severity will trigger an alert notification.	1. Navigate to **Objects > Log Forwarding**. 2. Click **Add** and name the profile. For example, **WildFire-Log-Forwarding**. 3. In the **Threat Settings** section, choose the email profile from the **Email** column for **Medium** severity. The reason why medium is used here is because WildFire malware logs have a **Medium** severity. To alert on WildFire benign logs, select the severity **Informational**. 4. Click **OK** to save the changes.  **Note** If the firewall is managed by Panorama, click the **Panorama** check box to the right of **Medium** severity to enable log forwarding to Panorama. If an SNMP server is configured, select the server in the **SNMP Trap** drop-down to the right of **Medium** severity to forward traps to the SNMP server.
Step 4 Apply the log forwarding profile to the security profile that contains the file blocking profile.	1. Navigate to **Policies > Security** and click on the policy that is used for WildFire forwarding. 2. In the **Actions** tab **Log Setting** section, click the **Log Forwarding** drop-down and select the new log forwarding profile. In this example, the profile is named **WildFire-Log-Forwarding**. 3. Click **OK** to save the changes and then **commit** the configuration. Email alerts should now be received for Threat and Wildfire logs with medium severity.

WildFire in Action

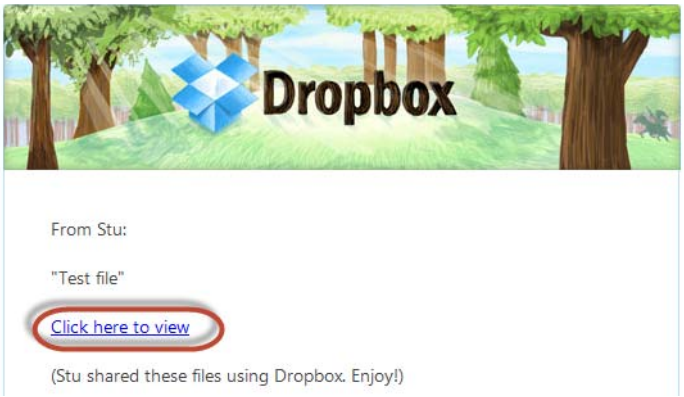
The following example scenario summarizes the full WildFire lifecycle. In this example, a sales representative from Palo Alto Networks downloads a new software sales tool that a sales partner uploaded to Dropbox. The sales partner unknowingly uploaded an infected version of the sales tool install file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

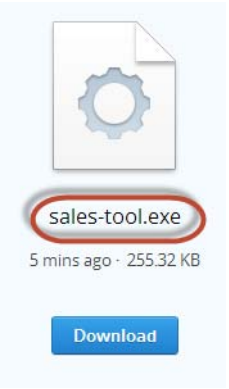
This example will demonstrate how the Palo Alto Networks firewall in conjunction with WildFire can discover zero-day malware downloaded by your users even when the traffic is SSL encrypted. After the malware is identified, the administrator is notified, the user who downloaded the file is contacted, and a new signature to protect against future exposure of the malware is automatically downloaded by the firewall. Although some file sharing web sites have an antivirus feature that checks files as they are uploaded, they can only protect against "known" malware.

For more information on configuring WildFire, see "Forward Files to the WildFire Cloud" on page 32 or "Forward Files to a WF-500 WildFire Appliance" on page 23.

This example uses a web site that uses SSL encryption, so decryption must be configured on the firewall and **Allow forwarding of decrypted content** must be enabled. For information on configuring decryption, refer to the *Palo Alto Networks Getting Started Guide*. For information on enabling forwarded of decrypted data, see "Forward Files to the WildFire Cloud" on page 32 or "Forward Files to a WF-500 WildFire Appliance" on page 23.

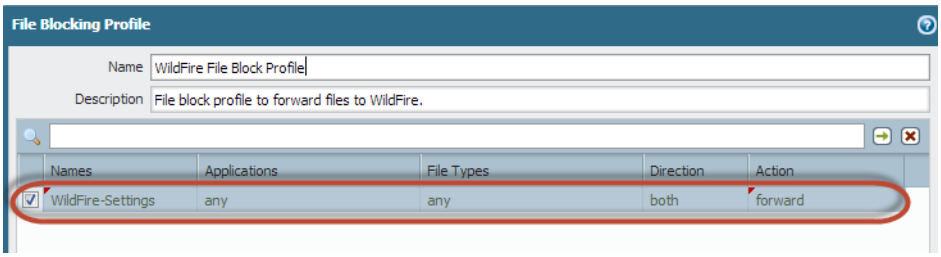
WILDFIRE EXAMPLE SCENARIO	
Step 1.	The sales rep from the partner company uploads a sales tool file named **sales-tool.exe** to his Dropbox account and then sends an email to the Palo Alto Networks sales representative with a link to the file.
Step 2	The Palo Alto sales rep receives the email from the sales partner and clicks the download link, which takes her to the Dropbox site. She then clicks **Download** and the file is saved to her desktop.

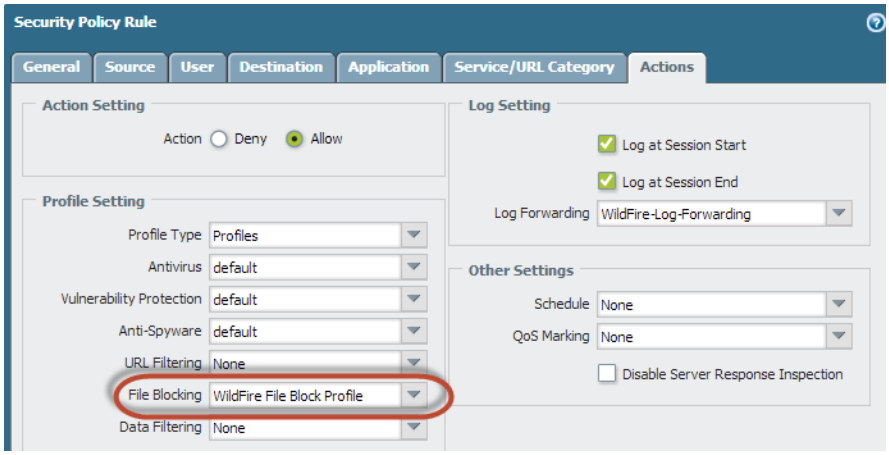


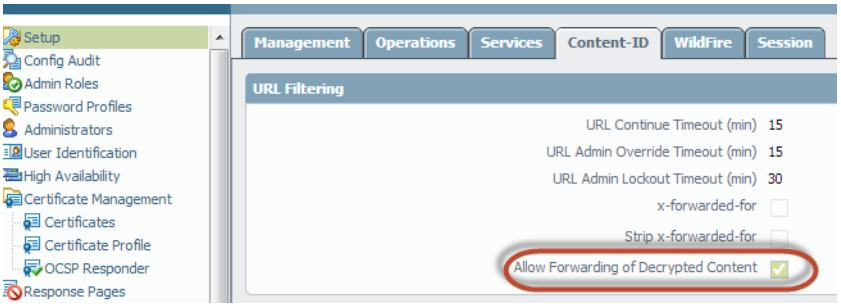


WILDFIRE EXAMPLE SCENARIO	(Continued)

Step 3 The firewall that is protecting the Palo Alto sales rep has a file blocking profile attached to a security policy that will look for files in any application that is used to download or upload any portable executable (PE) file type. As soon as the sales rep clicks download, the firewall policy also forwards the sales-toole.exe file to WildFire for analysis. Even though the sales rep is using Dropbox, which is SSL encrypted, the firewall is configured for decryption, so all traffic can be inspected and files can be forwarded to WildFire. The following screen shots show the File Blocking Profile, the Security Policy configured with the File Blocking profile, and the option to allow forwarding of decrypted content.

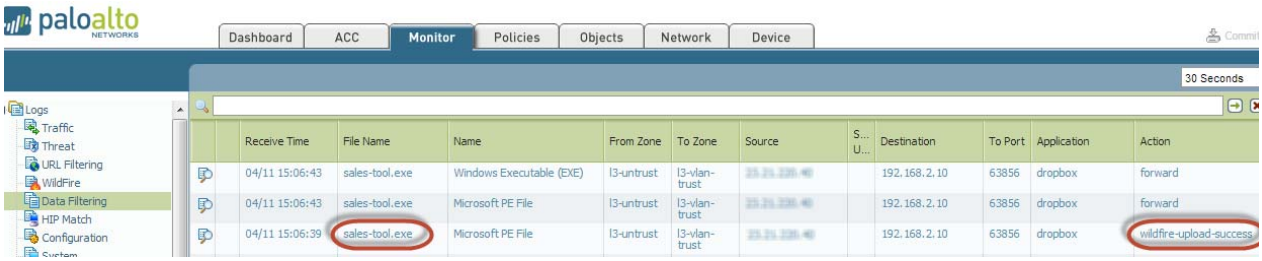






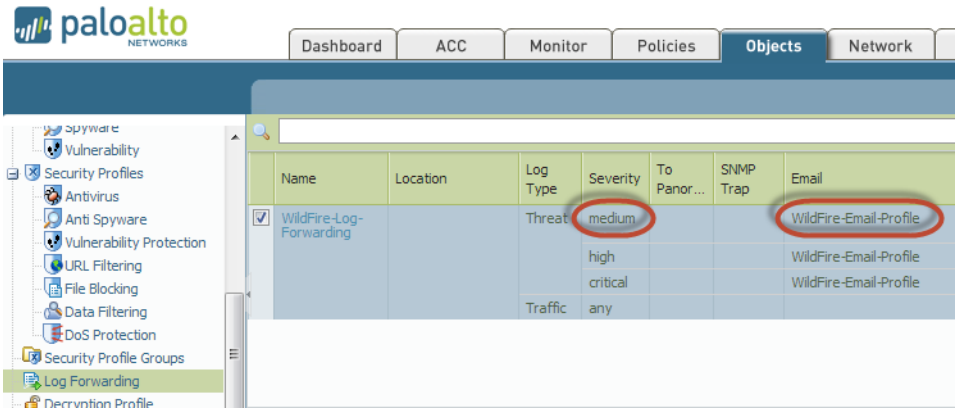
WILDFIRE EXAMPLE SCENARIO	(Continued)

Step 4 At this point, WildFire has received the file and is analyzing it for over 100 different malicious behaviors. To see that the file was forwarded successfully, view **Monitor > Logs > Data Filtering** on the firewall.



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 A log forwarding profile to email medium threat alerts is also configured, so the security administrator immediately receives an email about the malware downloaded by the sales rep.



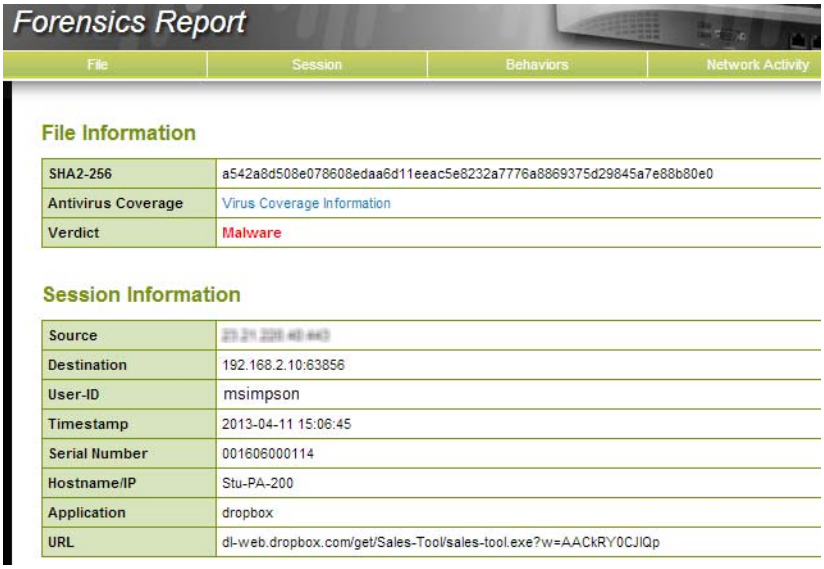
WILDFIRE EXAMPLE SCENARIO	(Continued)

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 shutdown the network or VPN connection that the sales rep 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 verify if the malware was run on the system by looking at the files, processes, and registry information detailed in the analysis report. If the malware was run, the support person can attempt to clean the system manually or re-image it.

For details on the WildFire report fields, see "What is in the WildFire Reports?" on page 50.

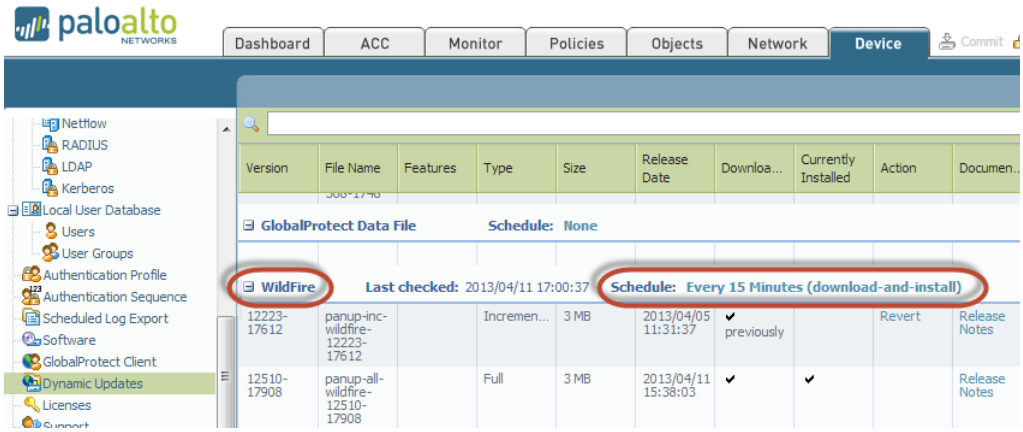
Partial view of the WildFire analysis report



WILDFIRE EXAMPLE SCENARIO	(Continued)

Step 8 Now that the malware has been identified and the user's 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 every 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 the new signature. This firewall and any other Palo Alto Networks firewall configured to download WildFire signatures is now protecting users against this newly discovered malware.



All of this happens well before most antivirus vendors are even aware of the zero-day malware. In this example, the malware is no longer considered zero-day because Palo Alto Networks knows about the malware and has already provided protection to its customers.

5 WildFire Appliance Software CLI Reference

This chapter describes the CLI commands that are specific to the WF-500 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 *Palo Alto Networks PAN-OS Command Line Interface Reference Guide*.

About the WildFire Appliance Software

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

- About the WildFire Appliance Software CLI Structure
- Access the CLI
- Use the WildFire Appliance Software CLI Commands

About the WildFire Appliance Software CLI Structure

The WildFire 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 WildFire appliance software CLI over SSH or by direct console access using the console port.

The WildFire appliance software CLI operates in two modes:

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

For more details on these modes, see "CLI Command Modes" on page 68.

Access the CLI

This section describes how to access and begin using the WildFire appliance software CLI:

- Establish a Direct Console Connection
- Establish an SSH Connection

Establish a Direct Console Connection

Refer to the *WF-500 WildFire Appliance Hardware Reference Guide* for hardware installation information and the Quick Start for information on initial device configuration.

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 WildFire appliance software CLI:

1. Open the console connection.
2. Enter the administrative user name. The default is admin.
3. Enter the administrative password. The default is admin.
4. The WildFire appliance software CLI opens in Operational mode, and the CLI prompt is displayed:
   `username@hostname>`

Use the WildFire Appliance Software CLI Commands

- WildFire Appliance Software CLI Command Conventions
- CLI Command Messages
- Access Operational and Configuration Modes
- Display WildFire Appliance Software CLI Command Options

WildFire Appliance Software CLI Command Conventions

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

```
username@hostname>
```

Example:

```
msimpson@wf-corp1>
```

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.

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 zone application 1.1.2.2
Unrecognized command
Invalid syntax.
[edit]
username@hostname#
```

Access Operational and Configuration Modes

When logging in, the WildFire 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 WildFire 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>
```

- 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
```

Command Option Symbols

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

Symbol	Description
*	This option is required.
>	There are additional nested options for this command.
+	There are additional command options for this command at this level.
|	There is an option to specify an “except value” or a “match value” to restrict the command.
“ “	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 “Test Group” 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 Group as the username and the following error wold be displayed: “test is not a valid name”. Note: A single quote would also be invalid in this example.

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
> profiles             profiles
```

```
  <Enter>              Finish input
[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
```

Restrict 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-corp1
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
time: Mon Apr 15 13:31:39 2013
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

username@hostname>
```

The following sample displays only the system model information:

```
username@hostname> show system info | match model
model: WF-500

username@hostname>
```

Privilege Levels

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

Level	Description
superreader	Has complete read-only access to the appliance.
superuser	Has complete read-write access to the appliance.

CLI Command Modes

This chapter describes the modes used to interact with the WildFire appliance software CLI:

About 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.

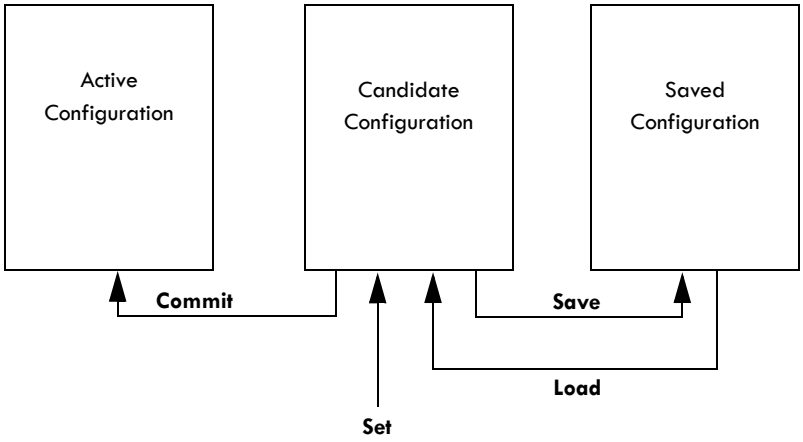
This section describes Configuration mode and the configuration hierarchy:

Configuration Mode Command Usage

Use the following commands to store and apply configuration changes:

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

When existing Configuration mode without issuing the save or commit command, the configuration changes could be lost if power is lost to the appliance.



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.

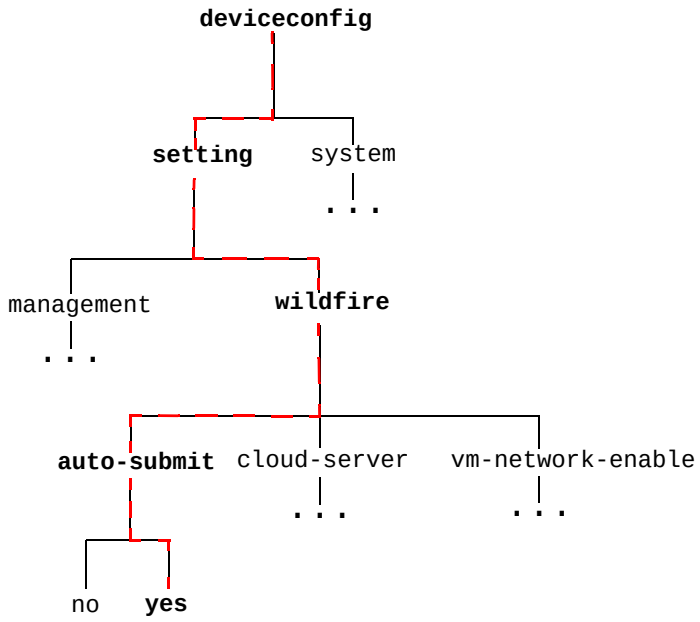
Because the candidate configuration is always unique, all the authorized changes to the candidate configuration will be consistent with each other.

About the 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 will be 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:

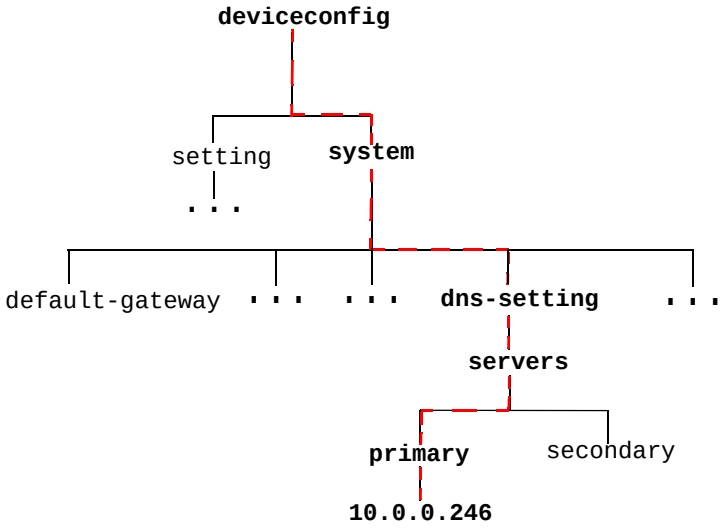


For example, the following command assigns the primary DNS server 10.0.0.246 for the appliance:

```
[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. For example, the banner

```
[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.

Level	Description
edit	Sets the context for configuration within the command hierarchy.
up	Changes the context to the next higher level in the hierarchy.
top	Changes the context to the highest level in the hierarchy.

The set command issued after using the up and top commands starts from the new context.

About Operational Mode

At the initial login to the device, the WildFire 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.
- **WildFire appliance software CLI navigation commands**—Enter Configure mode or exit the WildFire appliance software CLI. Includes **configure**, **exit**, and **quit** commands.
- **System commands**—Make system-level requests or restart. Includes **set** and **request** commands.

Set the Output Format for 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.

Configuration Mode Commands

This section contains command reference information for the following Configuration mode commands that are specific to the WildFire appliance software. All other commands that are part of the WildFire appliance software are identical to PAN-OS, refer to the *Palo Alto Networks PAN-OS Command Line Interface Reference Guide* for information on those commands.

All WildFire specific commands are in blue font in the following hierarchy output and are hyperlinked to the description.

```
deviceconfig {
  system {
    login-banner <value>;
    hostname <value>;
    domain <value>;
    speed-duplex
auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps-full-
duplex|
    1Gbps-full-duplex;
    ip-address <ip/netmask>;
    netmask <value>;
    default-gateway <ip/netmask>;
    vm-interface{
      ip-address <ip/netmask>;
      netmask <value>;
      default-gateway <ip/netmask>;
      mtu 576-1500;
      speed-duplex
      auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps
     -full-duplex|
      1Gbps-full-duplex;
      link-state up|down;
      dns-server <ip/netmask>;
    }
    geo-location {
      latitude <float>;
      longitude <float>;
    }
    timezone
    dns-setting {
        servers {
          primary <ip/netmask>;
          secondary <ip/netmask>;
        }
    }
    ntp-server-1 <value>;
    ntp-server-2 <value>;
    update-server <value>;
    secure-proxy-server <value>;
    secure-proxy-port 1-65535;
    secure-proxy-user <value>;
```

```
    secure-proxy-password <value>;
    service {
      disable-ssh yes|no;
      disable-icmp yes|no;
    }
  }
  setting {
    wildfire {
      cloud-server <value>;
      auto-submit yes|no;
      vm-network-enable yes|no;
    }
    management {
      admin-lockout {
        failed-attempts 0-10;
        lockout-time 0-60;
      }
      idle-timeout 1-1440;
    }
  }
}

mgt-config {
  users {
    REPEAT...
    <name> {
      phash <value>;
      permissions {
        role-based {
          superreader yes;
          OR...
          superuser yes;
        }
      }
    }
  }
}

predefined;

shared {
  log-settings {
    system {
      informational {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      low {
        send-syslog {
          using-syslog-setting <value>;
        }
```

```
      }
      medium {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      high {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      critical {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
    }
    config {
      any {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
    }
    syslog {
      REPEAT...
      <name> {
        server {
          REPEAT...
          <name> {
            server <value>;
            port 1-65535;
            facility
LOG_USER|LOG_LOCAL0|LOG_LOCAL1|LOG_LOCAL2|LOG_LOCAL3|LOG_LOCAL4|LOG_LOCAL5|LOG_LOCAL6|
LOG_LOCAL7;
          }
        }
      }
    }
  }
}
```

vm-interface

Description

The vm-interface is used to allow malware running on the WildFire virtual machines to access the Internet to enable more comprehensive file analysis. 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 is on an isolated network to the Internet. For more information about the vm-interface, refer to "Set Up the Virtual Machine Interface" on page 16.

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

Syntax

```
set vm-interface {
    ip-address <ip_address>;
    netmask <ip_address>;
    default-gateway <ip_address>;
    dns-server <ip_address>;
```

Options

```
admin@wf-corp1# set vm-interface
+ default-gateway   Default gateway
+ dns-server        dns server
+ ip-address        IP address for wildfire vm download interface
+ link-state        Link state up or down
+ mtu               Maximum Transmission Unit for the management interface
+ netmask           IP netmask for wildfire vm download interface
+ speed-duplex      Speed and duplex for wildfire vm download 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, superreader

wildfire

Description

Configure Wildfire settings to auto-submit malware to the Palo Alto Networks WildFire cloud to have signatures generated, define the cloud server that will receive malware infected files, and enable or disable the vm-interface. Please read the description of th vm-interface before enabling it.

Hierarchy Location

set deviceconfig settings

Syntax

```
wildfire {
      cloud-server <value>;
      auto-submit yes|no;
      vm-network-enable yes|no;
      }
```

Options

```
admin@wf-corp1# set wildfire
+ auto-submit automatically submit all malwares/incorrect verdict to public cloud
+ cloud-server Hostname for cloud server. Default is wildfire-public-cloud
+ vm-network-enable enable/disable
```

Sample Output

The following output shows that auto-submit is not enabled on the WildFire appliance, so malware infected files will not be sent to the WildFire cloud. If auto-submit was enabled, it would send files to the WildFire cloud because the cloud-server wildfire-public-cloud is defined. It also shows that the vm-interface is enabled, which will allow malware running on the WildFire virtual machines to access the Internet.

```
wildfire {
  auto-submit no;
  vm-network-enable yes;
  cloud-server wildfire-public-cloud;
}
```

Required Privilege Level

superuser, superreader

Operational Mode Commands

This section contains command reference information for the following Operational mode commands that are specific to the WildFire appliance software. All other commands that are part of the WildFire appliance software are identical to PAN-OS; refer to the *Palo Alto Networks PAN-OS Command Line Reference Guide* for information on those commands.

All WildFire-specific commands are in blue font in the following hierarchy output and are hyperlinked to the description.

```
test {
  wildfire {
    registration;
  }
}
set {
  wildfire {
     portal-admin {
       password <value>;
     }
  }
  OR...
  management-server {
    unlock {
      admin <value>;
    }
    OR...
    logging on|off|import-start|import-end;
  }
  OR...
  password;
  OR...
  ssh-authentication {
    public-key <value>;
  }
  OR...
  cli {
    config-output-format default|xml|set|json;
    OR...
    pager on|off;
    OR...
    confirmation-prompt on|off;
    OR...
    scripting-mode on|off;
    OR...
    timeout {
      idle 1-1440;
    }
    OR...
```

```
    hide-ip;
    OR...
    hide-user;
  }
  OR...
  clock {
    date <value>;
    time <value>;
  }
}

request {
  system {
    software {
      info;
      OR...
      check;
      OR...
      download {
        version <value>;
        OR...
        file <value>;
      }
      OR...
      install {
          version <value>;
          OR...
          file <value>;
        load-config <value>;
      }
    }
    OR...
    raid {
      remove <value>;
      OR...
      copy {
        from <value>;
        to <value>;
      }
      OR...
      add {
        REPEAT...
        <name> {
          force {
            no-format;
          }
        }
      }
    }
  }
  OR...
  password-hash {
```

```
    password <value>;
    username <value>;
  }
  OR...
  commit-lock {
    add {
      comment <value>;
    }
    OR...
    remove {
      admin <value>;
    }
  }
  OR...
  config-lock {
    add {
      comment <value>;
    }
    OR...
    remove;
  }
  OR...
  tech-support {
    dump;
  }
  OR...
  stats {
    dump;
  }
  OR...
  shutdown {
    system;
  }
  OR...
  system {
    software {
      info;
      OR...
      check;
      OR...
      download {
        version <value>;
        OR...
        file <value>;
      }
      OR...
      install {
          version <value>;
          OR...
          file <value>;
        load-config <value>;
      }
```

```
    }
  }
  OR...
  license {
    info;
    OR...
    fetch {
      auth-code <value>;
    }
    OR...
    install <value>;
  }
  OR...
  restart {
    system;
    OR...
    software;
  }
  OR...
  support {
    info;
    OR...
    check;
  }
}

check {
  pending-changes;
  OR...
  data-access-passwd {
    system;
  }
}

save {
  config {
    to <value>;
  }
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>1-1048576;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
```

```
        to-xpath <value>;
        mode merge|replace|append;
      }
  }
  OR...
  device-state;
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
        to-xpath <value>;
        mode merge|replace|append;
      }
      OR...
      repo {
        device <value>;
          file <value>;
          OR...
          version <value>;
      }
  }
}

delete {
  config {
    saved <value>;
    OR...
    repo {
      device <value>;
        file <value>;
        OR...
        running-config;
    }
  }
  OR...
  software {
    image <value>;
    OR...
    version <value>;
  }
}
```

```
clear {
  job {
    id 0-4294967295;
  }
  OR...
  log {
    config;
    OR...
    system;
  }
  OR...
  counter {
    device;
  }
}

show {
  arp management|ethernet1/1|ethernet1/2|all;
  OR...
  neighbor management|ethernet1/1|ethernet1/2|all;
  OR...
  web-server {
    log-level;
  }
  OR...
  config {
    diff;
    OR...
    running {
      xpath <value>;
    }
    OR...
    candidate;
  }
  OR...
  interface management|ethernet1/1;
  OR...
  management-clients;
  OR...
  counter {
    management-server;
    OR...
    interface management|ethernet1/1;
    OR...
    device;
  }
  OR...
  ntp;
  OR...
  clock;
  OR...
wildfire {
```

```
    sample-status {
      sha256 {
        equal <value>;
      }
    }
    OR...
    status;
    OR...
    statistics;
    OR...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|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...
      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...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    }
    OR...
    last-device-registration {
      all;
    }
  }
  OR...

  cli {
    info;
```

```
  OR...
  idle-timeout;
  OR...
  hide-ip;
  OR...
  hide-user;
  OR...
  permissions;
}
OR...
jobs {
  all;
  OR...
  pending;
  OR...
  processed;
  OR...
  id 1-4294967296;
}
OR...
location {
  ip <ip/netmask>;
}
OR...
system {
  software {
    status;
  }
  OR...
  masterkey-properties;
  OR...
  info;
  OR...
  resources {
    follow;
  }
  OR...
  raid {
      detail;
  }
  OR...
  disk-space;
  OR...
  disk-partition;
  OR...
  files;
  OR...
  state {
      filter <value>;
      OR...
      filter-pretty <value>;
      OR...
```

```
        browser;
    }
    OR...
    environmentals {
        fans;
        OR...
        thermal;
        OR...
        power;
    }
    OR...
    setting {
      multi-vsys;
    }
  }
  OR...
  high-availability {
    all;
    OR...
    state;
    OR...
    control-link {
      statistics;
    }
    OR...
    transitions;
    OR...
    path-monitoring;
    OR...
    local-state;
  }
  OR...
  log {
    config {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <value>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <value>;
      }
      end-time {
```

```
        equal <value>;
      }
      serial {
        equal <value>;
        OR...
        not-equal <value>;
      }
      client {
        equal web|cli;
        OR...
        not-equal web|cli;
      }
      cmd {
        equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
        OR...
        not-equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
      }
      result {
        equal succeeded|failed|unauthorized;
        OR...
        not-equal succeeded|failed|unauthorized;
      }
    }
    OR...
    system {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <value>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <value>;
      }
      end-time {
        equal <value>;
      }
      serial {
        equal <value>;
        OR...
        not-equal <value>;
      }
      opaque {
```

```
        contains <value>;
      }
      severity {
        equal critical|high|medium|low|informational;
        OR...
        not-equal critical|high|medium|low|informational;
        OR...
        greater-than-or-equal critical|high|medium|low|informational;
        OR...
        less-than-or-equal critical|high|medium|low|informational;
      }
      subtype {
        equal <value>;
        OR...
        not-equal <value>;
      }
      object {
        equal <value>;
        OR...
        not-equal <value>;
      }
      eventid {
        equal <value>;
        OR...
        not-equal <value>;
      }
      id {
        equal <value>;
        OR...
        not-equal <value>;
      }
    }
  }
}

debug {
  web-server {
    reset-cache;
    OR...
    log-level {
      info;
      OR...
      warn;
      OR...
      crit;
      OR...
      debug;
    }
  }
  OR...
  delete {
    sample {
```

```
    sha256 {
      equal <value>;
    }
  }
}
OR...
swm {
  list;
  OR...
  log;
  OR...
  history;
  OR...
  status;
  OR...
  unlock;
  OR...
  revert;
}
OR...
tac-login {
    permanently-disable;
    OR...
    challenge;
    OR...
    response;
}
OR...
software {
  restart {
    management-server;
    OR...
    web-server;
    OR...
    ntp;
  }
  OR...
  core {
    management-server;
    OR...
    web-server;
  }
  OR...
  trace {
    management-server;
    OR...
    web-server;
  }
}
OR...
cli on|off|detail|show;
OR...
```

```
system {
  maintenance-mode;
  OR...
  disk-sync;
  OR...
  ssh-key-reset {
    management;
    OR...
    all;
  }
}
OR...
device {
  set queue|all;
  OR...
  unset queue|all;
  OR...
  on error|warning|info|debug|dump;
  OR...
  off;
  OR...
  show;
  OR...
  clear;
  OR...
  dump {
    queues;
    OR...
    queue-stats;
    OR...
    queue <value>;
  }
  OR...
  flush {
    queue <value>;
  }
  OR...
  set-watermark {
    queue <value>;
    type high|low;
    value 0-4000;
  }
}
OR...
vardata-receiver {
  set {
    third-party libcurl|all;
    OR...
    all;
  }
  OR...
  unset {
```

```
    third-party libcurl|all;
    OR...
    all;
  }
  OR...
  on normal|debug|dump;
  OR...
  off;
  OR...
  show;
  OR...
  statistics;
}
OR...
wildfire {
  reset {
    forwarding;
  }
}
OR...
management-server {
  client {
    disable authd|useridd|ha_agent;
    OR...
    enable authd|useridd|ha_agent;
  }
  OR...
  conn;
  OR...
  on error|warn|info|debug|dump;
  OR...
  off;
  OR...
  clear;
  OR...
  show;
  OR...
  set {
    all;
    OR...
    comm basic|detail|all;
    OR...
    panorama basic|detail|all;
    OR...
    proxy basic|detail|all;
    OR...
    server basic|detail|all;
  }
  OR...
  unset {
    all;
    OR...
```

```
      comm basic|detail|all;
      OR...
      panorama basic|detail|all;
      OR...
      proxy basic|detail|all;
      OR...
      server basic|detail|all;
    }
  }
}

upload {
  generic_chunks {
    todir <value>;
    tofile <value>;
    offset 0-419430600;
    endoffile yes|no;
    content <value>;
  }
  OR...
  generic {
    name <value>;
    path <value>;
    content <value>;
    todir <value>;
    tofile <value>;
  }
  OR...
  config {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  software {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  license {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  certificate {
    name <value>;
    passphrase <value>;
    path <value>;
    content <value>;
    certificate-name <value>;
```

```
  format pkcs12|pem;
}
OR...
private-key {
  name <value>;
  passphrase <value>;
  path <value>;
  content <value>;
  certificate-name <value>;
  format pkcs12|pem;
}
OR...
keypair {
  name <value>;
  passphrase <value>;
  path <value>;
  content <value>;
  certificate-name <value>;
  format pkcs12|pem;
}
OR...
ssl-optout-text {
  name <value>;
  path <value>;
  content <value>;
}
OR...
ssl-cert-status-page {
  name <value>;
  path <value>;
  content <value>;
}
OR...
logo {
  name <value>;
  path <value>;
  content <value>;
}
OR...
custom-logo {
    login-screen {
      name <value>;
      path <value>;
    }
    OR...
    main-ui {
      name <value>;
      path <value>;
    }
    OR...
    pdf-report-header {
      name <value>;
```

```
        path <value>;
      }
      OR...
      pdf-report-footer {
        name <value>;
        path <value>;
      }
  }
}

download {
  certificate {
    certificate-name <value>;
    include-key yes|no;
    format pem|pkcs12;
    passphrase <value>;
  }
  OR...
  csv;
  OR...
  techsupport;
  OR...
  statsdump;
  OR...
  generic {
    file <value>;
  }
}

scp {
  import {
    configuration {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    license {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    software {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
  OR...
  export {
    mgmt-pcap {
```

```
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    configuration {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    tech-support {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
}

tftp {
  import {
    configuration {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    certificate {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
      certificate-name <value>;
      passphrase <value>;
      format pkcs12|pem;
    }
    OR...
    private-key {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
      passphrase <value>;
      certificate-name <value>;
      format pkcs12|pem;
    }
    OR...
    keypair {
      from <value>;
```

```
    file <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
    passphrase <value>;
    certificate-name <value>;
    format pkcs12|pem;
  }
  OR...
  license {
    from <value>;
    file <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
  }
  OR...
  software {
    from <value>;
    file <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
  }
}
OR...
export {
  config-bundle {
    to <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
  }
  OR...
  core-file {
    control-plane {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
  OR...
  device-state {
    to <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
  }
  OR...
  mgmt-pcap {
    from <value>;
    to <value>;
    remote-port 1-65535;
    source-ip <ip/netmask>;
  }
  OR...
```

```
    configuration {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    tech-support {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    log-file {
      management-plane {
        to <value>;
        remote-port 1-65535;
        source-ip <ip/netmask>;
      }
    }
  }
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>1-1048576;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
        to-xpath <value>;
        mode merge|replace|append;
      }
  }
  OR...
  device-state;
}

less {
    mp-log <value>;
    OR...
    mp-backtrace <value>;
}

grep {
  invert-match yes|no;
  line-number yes|no;
```

```
  ignore-case yes|no;
  no-filename yes|no;
  count yes|no;
  max-count 1-65535;
  context 1-65535;
  before-context 1-65535;
  after-context 1-65535;
  pattern <value>;
    mp-log <value>;
    OR...
    dp-log <value>;
}

tail {
  follow yes|no;
  lines 1-65535;
    mp-log <value>;
}

ssh {
  inet yes|no;
  port 0-65535;
  source <value>;
  v1 yes|no;
  v2 yes|no;
  host <value>;
}

telnet {
  8bit yes|no;
  port 0-65535;
  host <value>;
}

traceroute {
  ipv4 yes|no;
  first-ttl 1-255;
  max-ttl 1-255;
  port 1-65535;
  tos 1-255;
  wait 1-99999;
  pause 1-2000000000;
  do-not-fragment yes|no;
  debug-socket yes|no;
  gateway <ip/netmask>;
  no-resolve yes|no;
  bypass-routing yes|no;
  source <value>;
  host <value>;
}

netstat {
```

```
  route yes|no;
  interfaces yes|no;
  groups yes|no;
  statistics yes|no;
  verbose yes|no;
  numeric yes|no;
  numeric-hosts yes|no;
  numeric-ports yes|no;
  numeric-users yes|no;
  symbolic yes|no;
  extend yes|no;
  programs yes|no;
  continuous yes|no;
  listening yes|no;
  all yes|no;
  timers yes|no;
  fib yes|no;
  cache yes|no;
}

ping {
  bypass-routing yes|no;
  count 1-2000000000;
  do-not-fragment yes|no;
  interval 1-2000000000;
  source <value>;
  no-resolve yes|no;
  pattern <value>;
  size 0-65468;
  tos 1-255;
  ttl 1-255;
  verbose yes|no;
  host <value>;
}
```

test wildfire registration

Description

Runs a test to verify if a WildFire appliance or a firewall is properly registered with a WildFire server. If the test is successful, the IP address or server name of the WildFire server will be displayed, which indicates that the appliance/firewall will be able to send files to the WildFire server for analysis.

Hierarchy Location

Top level of operations mode.

Syntax

```
test {
  wildfire {
    registration;
  }
}
```

Options

```
No additional options.
```

Sample Output

The following shows a successful output on a firewall that is able to communicate with a WildFire appliance. If this is a WildFire 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

set wildfire portal-admin

Description

Sets the portal admin account password that will be used to view the WildFire reports from a firewall. The default username and password is admin/admin. After entering the command, press enter and a prompt will appear to change the password.

This account is used when viewing WildFire log details on the firewall or Panorama and clicking **View WildFire Report**. After authenticating, the WildFire detailed analysis report is retrieved and displayed in your browser.

The portal admin account is the only account for viewing reports from the logs; the password can be changed, but the account name cannot be changed and no additional accounts can be created.

Hierarchy Location

Top level of operations mode.

Syntax

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

Options

```
No additional options.
```

Sample Output

The following shows the ouput of this command.

```
admin@wf-corp1> set wildfire portal-admin password
Enter password   :
Confirm password :
```

Required Privilege Level

superuser, superreader

raid

Description

Use this option to manage the RAID pairs installed in the WildFire appliance. The WF-500 WildFire 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 WildFire WF-500 appliance with a correctly configured RAID.

```
admin@wf-corp1> show system raid

Disk Pair A                          Available
   Disk id A1                          Present
   Disk id A2                          Present
Disk Pair B                          Available
   Disk id B1                          Present
   Disk id B2                          Present
```

Required Privilege Level

superuser, superreader

show wildfire

Description

Show WildFire appliance registration information, activity, recent samples that have been analyzed, and virtual machine information.

Hierarchy Location

show wildfire

Syntax

```
sample-status {
      sha256 {
        equal <value>;
      }
    }
    OR...
    status;
    OR...
    statistics;
    OR...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|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...
      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...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    OR...
    last-device-registration {
      all;
    }
  }
```

Options

```
admin@wf-corp1> show wildfire
> 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
> statistics                 Show basic wildfire statistics
> status                     status
```

Sample Output

The following shows the output for this command.

```
admin@wf-corp1> show wildfire last-device-registration all

+--------------+---------------------+-------------+------------+----------+--
--
----+
| Device ID    | Last Registered     | Device IP   | SW Version | HW Model | Sta
tus |
+--------------+---------------------+-------------+------------+----------+--
--
----+
| 001606000114 | 2013-03-12 08:34:09 | 192.168.2.1 | 5.0.2      | PA-200   | OK
    |
+--------------+---------------------+-------------+------------+----------+--
--

admin@wf-corp1> show wildfire latest
> analysis   Show latest 30 analysis
> samples    Show latest 30 samples
> sessions   Show latest 30 sessions
> uploads    Show latest 30 uploads
```

```
show wildfire sample-status sha256 equal
c08ec3f922e26b92dac959f672ed7df2734ad7840cd40dd72db72d9c9827b6e8

Sample information:
+--------------------+------------------+----------+----------+----------+-------
------------+
| Create Time       | File Name       | File Type | File Size | Malicious | Status
|
+--------------------+------------------+----------+----------+----------+-------
------------+
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE        | 261420    | No        | analysis
complete |
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE        | 261420    | No        | analysis
complete |
+--------------------+------------------+----------+----------+----------+-------
------------+

Session information:
+--------------------+---------------+---------+-------------+---------+--------
---------+-------------+-------------+-----------+-----------+
| Create Time        | Src IP        | Src Port | Dst IP      | Dst Port | File
| Device ID    | App          | Malicious | Status    |
+--------------------+---------------+---------+-------------+---------+--------
---------+-------------+-------------+-----------+-----------+
| 2013-03-07 10:22:42 | 46.165.211.184 | 80       | 192.168.2.10 | 53620    |
5138e223a1069.exe | 001606000114 | web-browsing | No        | completed |
| 2013-03-07 10:22:02 | 46.165.211.184 | 80       | 192.168.2.10 | 53618    |
5138e1fb3e5fb.exe | 001606000114 | web-browsing | No        | completed |
| 2013-03-07 10:22:00 | 46.165.211.184 | 80       | 192.168.2.10 | 53617    |
5138e1fa13a66.exe | 001606000114 | web-browsing | No        | completed |
+--------------------+---------------+---------+-------------+---------+--------
---------+-------------+-------------+-----------+-----------+

Analysis information:
+--------------------+--------------------+--------------------+-----------+-------
----+
| Submit Time        | Start Time         | Finish Time        | Malicious | Status
|
+--------------------+--------------------+--------------------+-----------+-------
----+
| 2013-03-07 10:22:01 | 2013-03-07 10:22:01 | 2013-03-07 10:27:02 | No        |
completed |
+--------------------+--------------------+--------------------+-----------+-------
----+

admin@wf-corp1> show wildfire statistics days 7

Last one hour statistics:
Total sessions submitted  :           0
Samples submitted         :           0
Samples analyzed          :           0
Samples pending           :           0
Samples (malicious)       :           0
Samples (benign)          :           0
```

```
Samples (error)           :            0
Malware sent to cloud     :            0

Last 7 days statistics:
Total sessions submitted  :           23
Samples submitted         :            3
Samples analyzed          :            3
Samples pending           :            0
Samples (malicious)       :            0
Samples (benign)          :            3
Samples (error)           :            0
Malware sent to cloud     :            0

admin@wf-corp1> show wildfire status

Connection info:
        Wildfire cloud:                 wildfire-public-cloud
        Status:                         Idle
        Auto-Submit:                    disabled
        VM internet connection:         disabled
        Best server:
        Device registered:              no
        Service route IP address:       192.168.2.20
        Signature verification:         enable
        Server selection:               enable
        Through a proxy:                no
```

Required Privilege Level

superuser, superreader

show system raid

Description

Show the RAID configuration of the appliance. The WF-500 WildFire 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 WildFire WF-500 appliance.

```
admin@wf-corp1> show system raid detail

Disk Pair A                             Available
   Status                                   clean
   Disk id A1                             Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       partition_2  : active sync
   Disk id A2                             Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       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