WildFire™

WildFire automatically protects your networks from new and customized malware across a wide range of applications, including malware hidden within SSL-encrypted traffic. WildFire easily extends the threat prevention capabilities of the next-generation firewall to tackle some of the most challenging threats in the world today, and does so with full visibility and enforcement at up to 10Gbps.

- Proactively executes suspicious files in a safe environment to identify malware based on more than 100 malicious behaviors.
- Combines the visibility of the next-generation firewall with cloud-based analysis to ensure accurate, safe and scalable malware analysis.
- True in-line blocking of malware infecting files and command-and=control traffic at the firewall.

The modern threat landscape has fundamentally evolved, and cyber-security teams face threats on a daily basis that rely on stealth, persistence and the skilled avoidance of traditional security measures. Such a fundamental shift in one's adversary demands more than an incremental response, and modern security teams are re-evaluating some of their most basic security assumptions concerning how they look at network traffic, how threats are identified, and ultimately how they are blocked.

Palo Alto Networks® prepares cyber-security teams for this challenge by offering a new approach based on simple but powerful concepts:

- All network traffic must be fully inspected.
- Any unknowns must be actively and conclusively investigated at scale.
- Threats need to be blocked, not just detected.

These core principles are the foundation of Palo Alto Networks WildFire solution, in which full visibility, scalable analysis, and automated protection all work together to secure the network and its data. Only the next-generation firewall provides full-stack analysis and enforcement of all network traffic regardless of evasion and encryption, ensuring that hidden or anomalous threats are exposed. WildFire then proactively runs any unknown files in a safe, scalable sandbox environment where malware is conclusively identified and new protections are automatically developed. The result is a completely unique, closed loop approach to controlling cyberthreats based on next-generation visibility, cloud-based malware sandboxing, and reliable in-line blocking of threats.

WildFire Overview

At its core, WildFire detects and blocks targeted, polymorphic, or otherwise unknown malware. To do so, WildFire marries the unique visibility and control of the next-generation firewall with a cloud-based environment where malware is safely analyzed at scale. By proactively executing unknown files in a virtual environment, WildFire uncovers malware based on its real behavior, ensuring malware is detected even if it gets past traditional signatures.

This style of sandbox analysis is computationally intense by nature, and as a result, WildFire is designed on a cloud-based architecture that ensures seamless scalability. The WildFire public cloud enables any Palo Alto Networks customer to perform true malware sandboxing of unknown files without the need for any additional hardware. However, a hardware-enabled private cloud option is available to extend the WildFire architecture to customers who cannot use public cloud resources due to regulatory or privacy requirements.

paloalto NETWORKS
the network security company™

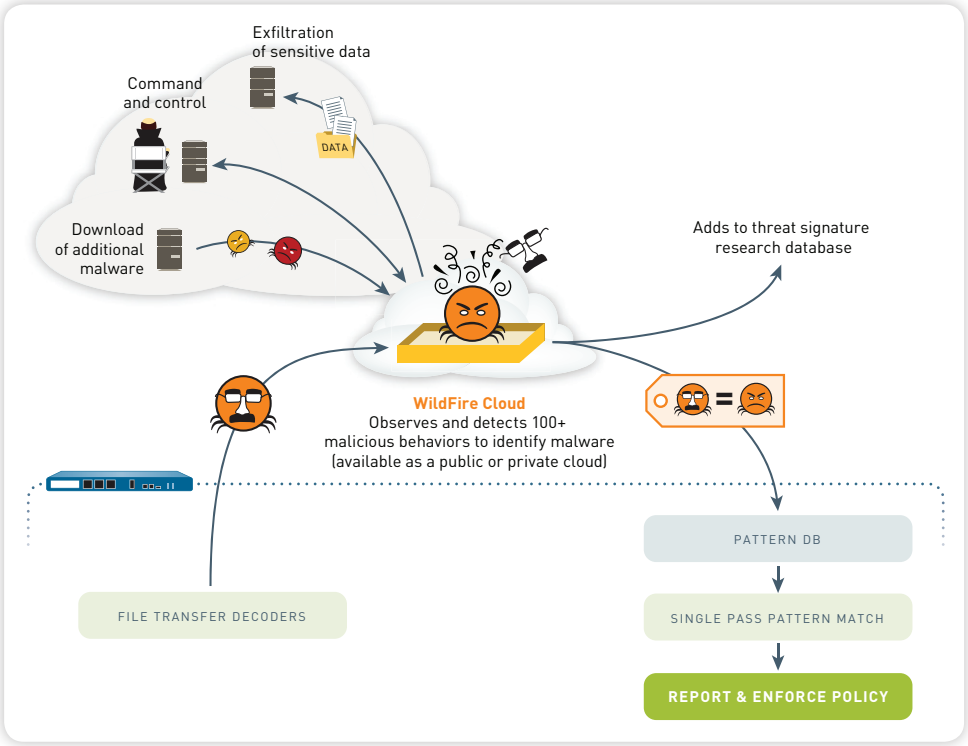
When a threat is detected, WildFire automatically feeds information and protections back to WildFire subscribers. Within in minutes, subscribers receive firewall logs with a verdict of the analysis including event context. More importantly, WildFire generates true malware protections for the newly discovered malware, and shares those protections with all WildFire subscribers world-wide within 30 to 60 minutes of the initial detection. These protections not only stop rapidly spreading malware, but also track unique identifiers in the malware body to proactively find and block malware variants. Additionally, WildFire analysis is used to update DNS-based malware signatures, update URL categories on the fly and to generate new command-and-control signatures, all of which can be used to identify and disrupt the all-important malware command-and-control traffic.

How WildFire Works

Visibility Into All Traffic

Advanced persistent threats (APTs) thrive on their ability to hide from security solutions. This is true not just of new malware, but of all traffic used in the attack. As a result, the quality of a cybersecurity solution is only as good as its ability to look into all traffic, and this is precisely why the next-generation firewall is a prerequisite for controlling these advanced attacks. As with all Palo Alto Networks analysis, WildFire benefits from the full-stack analysis of all traffic, across all ports and the ability to tightly control a variety of methods that attackers use to hide.

- **Abandoning Port-Based Assumptions:** For all of the advancements in IT security, virtually all security products fall back on outdated assumptions based on port. Traffic is allowed or blocked based on port, signatures are applied based on port, and additional decoders and analysis are applied based on the port. Palo Alto Networks forgoes these assumptions and performs a full-stack identification and decode of all traffic across all ports. This context is constantly monitored and updated to reflect any changes in the application or protocol. This process remains fundamentally unique in network security and ensures attackers can't hide by routing traffic in non-standard ways or tunneling within other approved traffic.
- **Visibility Into SSL Encrypted Traffic:** As more applications move to the web, SSL has become an increasingly common fact of life. And while SSL provides improved session security, it also has the effect of potentially creating an opaque vector where threats can flow without the prying eyes of security. Palo Alto Networks offers on-box SSL decryption that can be selectively applied based on policy. Decrypt only the traffic that interests you, and set policies to ensure traffic is never decrypted to sensitive sites such as health care or banking sites.
- **Visibility Into Unknown Traffic:** By positively classifying all traffic, Palo Alto Networks can further reveal the presence of any unknown or custom traffic. Such custom traffic is strongly correlated with malware and advanced threats, and simple next-generation firewall policies allow you to see this traffic and automatically enforce policy on it.



WildFire provides a logical combination of next-generation firewall hardware and scalable cloud-based malware analysis.

Conclusive Behavior-Based Analysis

When an unknown file is seen by the firewall, the file is transferred to the WildFire virtualized environment, where it is executed and all behaviors and communications are observed. WildFire monitors for more than 100 malicious behaviors to identify the true nature of malicious files based on their actions including:

- **Changes Made to the Host:** WildFire observes all process and hooking behaviors, changes made to registries, auto-run modifications, changes to security settings and any files that are created or modified. All changes are documented in WildFire reports.
- **Malicious Traffic and Hacking:** WildFire looks for suspicious or malicious network behaviors such as establishing backdoors, downloading additional executables, visiting dynamic DNS domains, scanning for vulnerabilities and much more.
- **Security Avoidance Behaviors:** WildFire also constantly looks for malware techniques used to avoid analysis such as attempting to avoid executing while being monitored, injecting into running or trusted processes and disabling host-based security features.

Using the Power of Cloud-Computing for Malware Analysis

Virtualized malware analysis requires massive amounts of computing resources, because the solution must provide a fully independent virtual environment to analyze every unknown or suspicious file. This means that computing requirements can swing wildly depending on the amount and type of traffic hitting the network. This has the potential to require a great deal of hardware for analysis, and even worse to create bottlenecks that limit the analysis of malware. To solve this problem, WildFire leverages a cloud-based architecture that allows computing resources to scale elastically based on need.

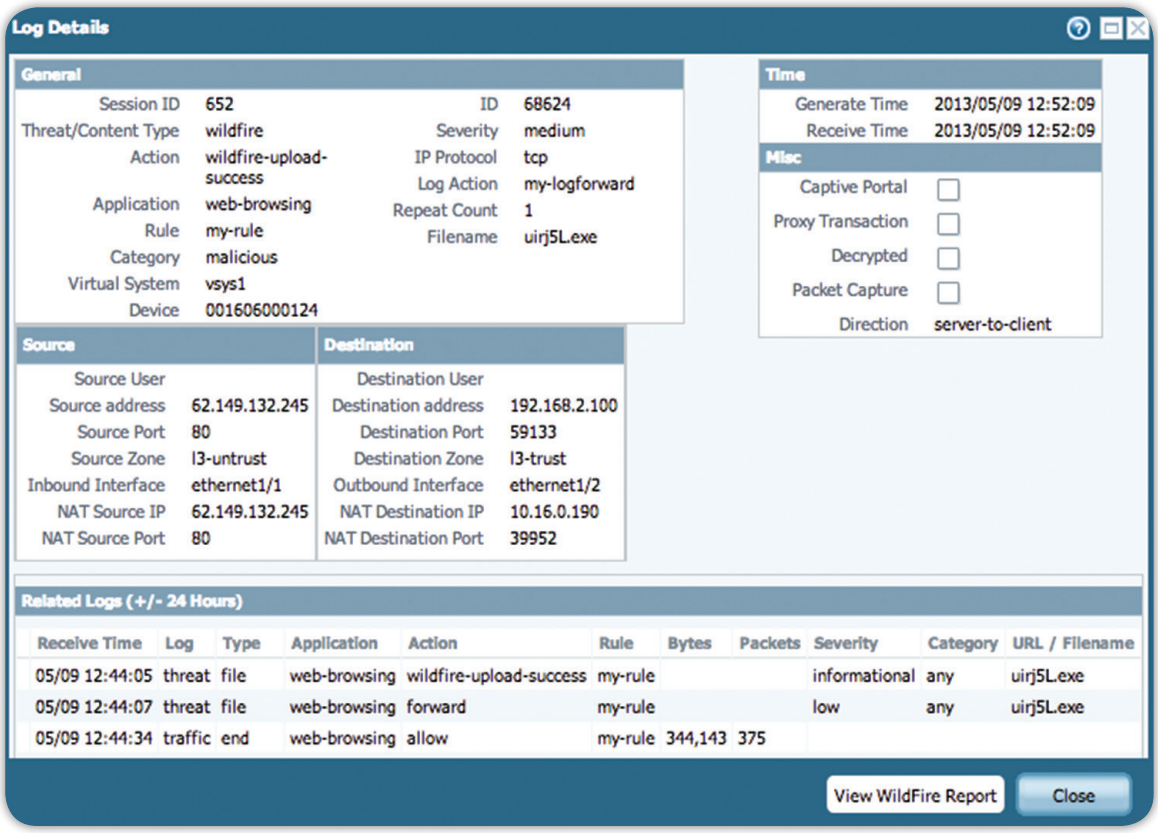
- **Shared Protections:** In addition to improved scalability, the WildFire cloud ensures that users can benefit from the analysis of all other WildFire users. Malware identified in one location, generates protections that apply to all users worldwide. This applies not only to malware samples, but also dangerous URLs, and DNS queries from malware as well.
- **Public Cloud:** By default, WildFire leverages a public cloud environment managed directly by Palo Alto Networks. All files are securely transferred between the firewall and the WildFire over encrypted connections, signed on both sides by Palo Alto Networks. Any files that are found to be benign are destroyed, while malware files are saved for further analysis.
- **Private Cloud:** For customers who do not use cloud-based solutions due to regulatory or privacy concerns, Palo Alto Networks offers a private cloud option for WildFire. This private cloud is enabled by the WF-500 WildFire Appliance, and allows customers to run a fully functioning version of the WildFire environment that remains within the customer's network.

Automated Prevention

Once a file is determined to be malicious, WildFire automatically develops protections for the new threat and generates integrated and correlated logs for security staff. Within minutes of submitting a file to WildFire, subscribers receive an integrated log with the verdict of the malware analysis, which is correlated with any other relevant logs in the Palo Alto Networks user interface. Additionally, all WildFire users can receive notifications via email based on policy.

The WildFire public cloud also develops a range of protections for all newly discovered malware (customers using a private cloud deployment have the option to submit confirmed malware to the public cloud in order to generate protections). WildFire automatically develops, tests and delivers new malware signatures within 30 to 60 minutes to all WildFire subscribers, worldwide. In addition to malware signatures, WildFire data is used to update DNS-based signatures, URL categories and command-and-control signatures as well.

- **Malware Signatures:** These signatures are based on unique identifiers in the malware payload that allow a single WildFire signature to block multiple polymorphic variants. These signatures are delivered to WildFire subscribers within 30 to 60 minutes of the initial submission of the file.
- **DNS Signatures:** WildFire records all DNS queries and maintains a database and signature list of DNS requests that are unique to botnets and malware operations.
- **Command-and-Control Signatures:** Palo Alto Networks researchers maintain full coverage for all command-and-control traffic observed in WildFire. These signatures provide a key method for identifying and controlling any malware infections already in the network.
- **URL Categories:** WildFire monitors any URLs and domains that malware communicates with. WildFire then provides updates on any newly discovered malicious domains to PAN-DB, Palo Alto Networks internally developed URL filtering database.



Integrated WildFire Logs

Malware Forensics and Event Analysis

Integrated Logging and Reporting

WildFire subscribers receive integrated WildFire logs on their firewalls, enabling teams to correlate WildFire events with other important events observed by the firewall. This ensures that staff can quickly and seamlessly tie applications, URLs, files, known threats and unknown threats into a coordinated approach to threat prevention. Additionally, Palo Alto Networks provides pre-built reports for WildFire events to provide ongoing documentation of emerging threats.

WildFire Portal

When dealing with new and emerging threats, it's important that security teams be able to quickly and easily investigate malware in order to correlate an infection with other security events or simply to aid in the cleanup in the case of an infection.

The WildFire Portal provides detailed analysis and forensics for every file analyzed by WildFire. Staff can track the overall rates of malware detected, and can drill down into detailed analysis on any given file. Staff can easily see the verdict of a file, the application, IP address and/or URL that delivered the file as well as the user that was targeted.

The analysis then provides granular details of the malware including all observed malicious behaviors, a list of any and all domains the malware visited, registry keys added or modified as well as any files created or modified. This analysis provides the context to know exactly how the malware attempted to enter the network, how it tries to communicate back out of the network and actions it performed on the target host. This information can provide teams with details to establish host-based indicators for infected machines, as well as providing the real-world data needed to adapt security policies to changing attack strategies. This data also helps security teams to teach and train network users by showing the names, locations and applications that have been used against them in phishing or social engineering attempts.

File Information

SHA-256	5d6bdab928f0be990e005dc7a9b2e815f42e9070bde4a85ec9f92c40dbfe8cb2
Antivirus Coverage	Virus Coverage Information
Verdict	Malware

Session Information

Source	109.86.104.76:80
Destination	192.168.2.100:59089
User-ID	unknown
Timestamp	2013-05-09 12:40:21
Serial Number	001606000124
Hostname/IP	taylor-200
Application	web-browsing
URL	yhbixpub.ru/newbos5.exe

Behavioral Summary

Behavior
Created a file in the Windows folder
Created or modified files in the Windows system folder
Created or modified files
Installed a driver
Listened on a specific port (backdoor behavior)
Created a hidden executable file
Started or stopped a system service
Registered a file as auto-start from a local directory
Modified registries or system configuration to enable auto start capablity
Modified Windows registries
Created an executable file in the Windows system folder
Attempted to sleep for a long period
Used direct IP instead of host name
Produced unknown traffic over the HTTP port

Analysis From the WildFire Portal

Maintaining the Privacy of Your Files

As with any use of the cloud, an enterprise must ensure that the cloud is used safely and without exposing enterprise data. WildFire is no exception, and provides customers with full control over what data is shared with WildFire and the additional protection of multiple layers of professionally managed security to ensure data is never exposed. Palo Alto Networks also offers the WF-500 appliance for customers who prefer to deploy WildFire as a private cloud.

Whether deployed as a private or public cloud, security teams always retain full control over exactly which files should be sent to the WildFire cloud. Teams may want to analyze all unknown files or simply those files coming from the Internet or other untrusted zones. In addition to control over which files are sent for analysis, policies can be set to control what relevant session information should be included with the sample for analysis. Session information refers to the context of the network session responsible for delivering the unknown file such as the application, target user, port number, source IP address, user and host name, as well as the attacking IP or URL. This data is often particularly useful for correlation purposes if a file is found to be malicious, but is not required for WildFire to determine the status of the file.

When a file is sent for analysis, the firewall establishes a secure connection between the local firewall and Palo Alto Networks WildFire cloud or local WF-500 appliance. This connection is secured on both ends by client certificates signed by Palo Alto Networks ensuring that data remains secure in transit and preventing the possibility of a man-in-the-middle attack. Once delivered to the WildFire cloud, the file is protected behind multiple layers of professionally managed security. Files are only allowed inbound to the WildFire cloud to ensure that benign files never leave the WildFire environment. Following analysis, benign files are destroyed and only the hash value retained in order to prevent future re-analysis.

WildFire Requirements:

PAN-OS version 5.0 or higher.

Licensing Information:

Basic WildFire functionality is available to all Palo Alto Networks customers at no charge. These users can automatically submit suspicious files to WildFire and protections are delivered with regular threat prevention content updates (threat prevention license is required). An additional WildFire license provides WildFire signatures every 30 minutes for all new malware detected anywhere in the world, integrated logging/reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day.

WF-500

The WF-500 is an optional hardware appliance to support customers who choose to deploy WildFire as a private cloud. The WF-500 is not required as WildFire deployments will use Palo Alto Networks secure public cloud by default.

PROCESSOR

- Dual 6-Core Intel Processor with Hyper-Threading

MEMORY

- 128 GB RAM

SYSTEM DISK

- 120GB SSD

STORAGE

- 2TB RAID1: 4 x 1TB RAID Certified HDD for 2 TB of RAID Storage

I/O

- 4x10/100/1000, DB9 Console serial port, USB

RACK MOUNTABLE

- 2U

POWER SUPPLY

- Dual 920W power supplies in hot swap, redundant configuration

MAXIMUM POWER CONSUMPTION

- 510 Watts

MAXIMUM BTU/HR

- 1740

INPUT VOLTAGE

- 100-240VAC

MAXIMUM CURRENT CONSUMPTION

- 11 Amps @ 100VAC

OPERATING TEMPERATURE

- 32 to 95 F, 0 to 35 C

NON-OPERATING TEMPERATURE

- -4 to 158 F, -20 to 70 C

SAFETY

- UL/CSA, CB

EMI

- FCC Class A, VCCI Class A, CE Class A

paloalto NETWORKS

the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com