WildFire® Service and Security Overview

This document provides an overview of the security practices put in place to help protect customer data that is sent to Palo Alto Networks' cloud-based WildFire® malware detection service. WildFire features security measures that are consistent with industry best practices to protect customer data within the WildFire cloud infrastructure.

Overview of WildFire

To meet the challenge of modern-day malware, Palo Alto Networks has developed WildFire, a service that integrates with our next-generation firewalls and provides detection and prevention of modern malware. WildFire identifies unknown or zero-day malware by directly executing files in a virtual environment and observing malicious behavior. This enables Palo Alto Networks to identify malware quickly and accurately, even if the malware has never been seen before. Signatures are automatically generated and distributed for identified malware and distributed to all Palo Alto Networks customers with a threat prevention license. WildFire makes use of an organization's on-premises firewalls for in-line high performance prevention in conjunction with a cloud-based service to provide fast protection for all enterprise locations.

There is a high likelihood that WildFire is not your organization's first experience with cloud-based technology. Cloud services have become a mainstay in today's corporate IT toolbox for delivering highly available, low cost services to customers. It is very likely that your organization already uses cloud-based services to perform any number of various business functions, such as applications for customer relationship management, human resources, finance, payroll, supply chain, etc., and possibly for managed data centers, compute infrastructure, or customer communications functions. If your organization is using any cloud-based services in these areas, you are already entrusting your confidential data to a third party provider and the security measures they have in place.

This document describes the advantages of combating modern malware in the cloud, explains why Palo Alto Networks has chosen to offer this technology as a cloud-based service, and describes the security measures in place to protect customer data.

Advantages of Combating Malware in the Cloud

Competing virtualized malware detection products have introduced substantial hardware, financial, and management burden by requiring dedicated hardware appliances at every ingress point of the network. WildFire, on the other hand, benefits from the reach and scalability of the cloud while remaining tightly integrated with the Palo Alto Networks next-generation firewalls for simple setup and enforcement. All that is required to help protect against zero-day malware is a few simple configuration steps on your Palo Alto Networks next-generation firewalls.

The WildFire cloud also provides access to vast hardware resources that would be impractical to deploy locally; enabling the best analysis possible. Additionally, WildFire can be easily updated by Palo Alto Networks researchers to quickly respond to evolving malware strategies, thus removing the need for IT teams to constantly update software or service packs on an in-house sandbox.

Offloading the complex infrastructure and compute resources required to host advanced virtualized based malware detection is not the only advantage. With WildFire in the cloud, Palo Alto Networks breaks the silos of information that have traditionally plagued other attempts at malware detection. In short, if a new or targeted threat is detected, that information and the ability to protect against the threat needs to be shared across the entire enterprise and not limited to the ingress point that detected the threat. WildFire centralizes the analysis of unknown files and provides a centralized source of protections for all Palo Alto Networks firewalls with a threat prevention license. Users of WildFire automatically receive signatures for never-before-seen malware that other users in the network have submitted to WildFire as part of their threat prevention subscription service.

Security Measures to Protect Customers

WildFire is tightly integrated with the Palo Alto Networks firewall and the user has total control over what is sent to the WildFire service using policy control. In a typical deployment, a policy is configured to send specific incoming file types to WildFire that originate from outside the network (the internet) and would ignore (not send) files that originate from inside the network. In this deployment, the only files that are uploaded to the WildFire service are files that had already entered the network from an outside, untrusted network. It is also important to note that all communications between the firewall and the cloud is encrypted and that the virtualized sandbox is protected behind multiple layers of security infrastructure.

Samples sent to WildFire are bundled with session data that helps the administrator determine what users and endpoints are implicated in a malware event and what application enabled the download. Session data can include file name, URL, user name, application, virtual system name, and source and destination IP and port. Device administrators have control over what session information is sent to the cloud, so users can maintain compliance with local laws and regulations (see Figure 1).

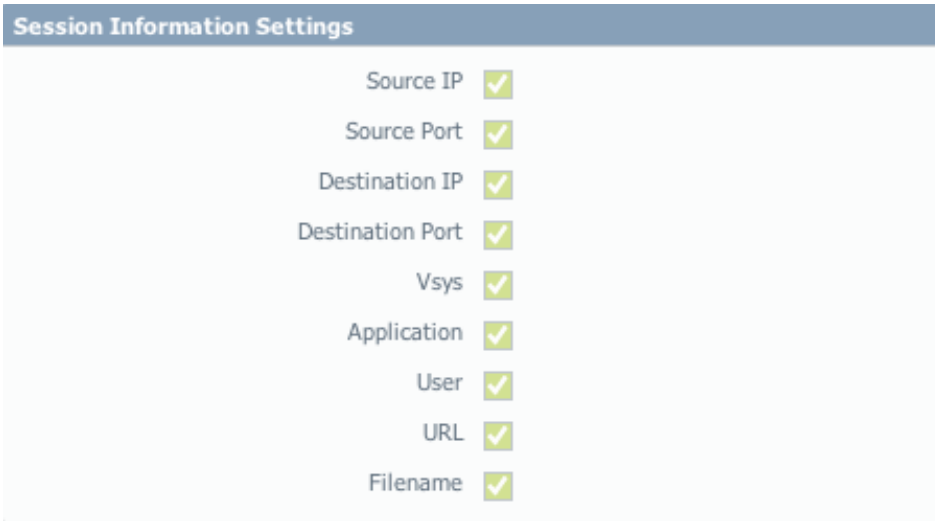

Figure 1. Configuration of WildFire session data settings. Session information can be useful to security staff in determining affected hosts and application vectors used by the malware. Customer's security staff and administrators determine the session information settings to maintain compliance with local laws and regulation.

Cloud Security: Behind the Scenes

WildFire features security measures that are consistent with industry best practices to help protect customer data within the WildFire cloud infrastructure. Data protection, high availability, and data privacy are of the utmost importance and Palo Alto Networks has put in place a cloud architecture designed to meet stringent cloud security requirements.

All communication between customer firewalls and the WildFire cloud occurs between the customer firewall and the WildFire cloud's nearest Amazon EC2 server. (See Figure 2.) There are currently five (5) Amazon EC2 servers distributed

across the globe in order to minimize the latency between the firewall and the WildFire service. The firewall automatically pings all known WildFire Amazon EC2 servers and chooses the fastest responding server.

Communication between customer firewalls and the Amazon EC2 server is encrypted using HTTPS/SSL encryption. Client-side and server-side certificates signed by Palo Alto Networks' Certificate Authority (CA) ensure that Palo Alto Networks firewalls will only connect to a valid WildFire cloud instance and vice-versa.

Session data and sample data is buffered on EC2 servers until the WildFire Analysis Center (located in California) is able to retrieve the data and perform the sample analysis. Typically, customer data is at rest on the EC2 server for a period of several seconds. Once data is retrieved from the EC2 server it is immediately deleted. Firewalls with IP-based ACLs in front of each of the EC2 instances, as well as in front of the WildFire Analysis Center, ensure that only connections between the EC2 servers and the WildFire Analysis Center are permitted. This communication is encrypted using HTTPS/SSL encryption.

Figure 2. Illustration of WildFire encrypted communication channels.

Customer data, including submitted files and associated session data, is retained by the WildFire Analysis Center for a period of up to 30 days in order to provide reports as well as for further analysis if it is determined to be needed. Additionally, samples (including application, source IP/port and source URL session data) that are determined to be malware are retrieved from the cloud and stored in the Palo Alto Networks malware library at company headquarters in California so that antivirus signatures can be generated and distributed to customers. Access to WildFire-related data is strictly controlled and is limited to members of the Palo Alto Networks Threat Research team.

Malware Information Sharing Practices

Palo Alto Networks strives to balance the importance of customer privacy with the benefits of timely sharing of emergent threat information among industry partners. Malware samples retained by Palo Alto Networks from customers via the WildFire service may be made available to industry partners in the malware research community as part of our approach to improve the overall quality of the anti-malware industry. However, session data associated with the malware is not shared with industry partners. Second-stage downloads performed by malware samples, as well as domains or IPs contacted by malware is also logged and may be made available to industry partners in the malware research community. Palo Alto Networks does not share WildFire data between customers or with other parties in a way that identifies who submitted the malware to the WildFire service.

For any security or privacy questions or concerns, please contact the Palo Alto Networks Threat Research team at ThreatResearch@paloaltonetworks.com for more information.

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 95054, USA
www.paloaltonetworks.com

Tel: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
Email: info@paloaltonetworks.com

This document is not a license to use the WildFire service or any other Palo Alto Networks products or services and does not grant any express or implied warranties. License terms, including any applicable warranties, can be found in the Palo Alto Networks End User License Agreement accompanying Palo Alto Networks products.

Revision History

Date	Revision	Comment
3/12/12	-	Document created