URL FILTERING PRIVACY

Palo Alto Networks® engaged TrustArc™, an independent data privacy risk management provider, to review and document the data flows and practices described in this datasheet. The purpose of this document is to provide customers of Palo Alto Networks with information needed to assess the impact of this service on their overall privacy posture by detailing how personal information may be captured, processed and stored by and within the service.

Product Summary

URL Filtering is a service that identifies and blocks access to malicious sites that may attempt to deliver malware or steal credentials and data. As part of this service, Palo Alto Networks maintains a cloud-based master database called PAN-DB. PAN-DB categorizes URLs based on their content at the domain, directory and page levels.

Palo Alto Networks next-generation firewalls use the information in PAN-DB to identify and filter URLs and prevent access to potentially risky sites. PAN-DB also receives updates from WildFire cloud-based threat analysis service to ensure the most current content categorizations for malicious websites. Through its integration with WildFire, PAN-DB receives previously uncategorized URLs from your firewall for analysis and categorization.

The URL Filtering service first conducts local lookups on a cache of known URLs stored on the device. If no decision can be reached based on these local cache results, the service queries PAN-DB in the cloud.

Information Processed by URL Filtering

URL Filtering operates on Palo Alto Networks® next-generation firewalls. As such, a range of data elements that may contain personal information – that is, data pertaining to or identifying a unique, identifiable individual – are collected and logged on the firewall, including:

- Source and destination IP addresses and ports, including NAT addresses
- Usernames associated with IP addresses or transactions, if enabled
- URLs being accessed and any referrer
- Categories of the URLs, if identified
- User agents (e.g., the name of the application-initiating session)
- Session-specific information – complete list available at https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/syslog-field-descriptions.

You can view a set of predefined or fully customized URL Filtering reports, giving your IT department visibility into URL Filtering and related web activity through the following:

- **User activity reports:** An individual user's activity report shows applications used, URL categories visited, websites visited and a detailed report of all URLs visited over a specified period of time.
- **URL activity reports**: A variety of "top 50" reports are available that display URL categories visited, URL users, websites visited, blocked categories, blocked users, blocked sites and more.
- **Real-time logging:** Logs can be filtered through an easy-to-use query tool that uses log fields and regular expressions to analyze traffic, threat or configuration incidents. Log filters can be saved and exported for more in-depth analysis and archival purposes. Logs can also be sent to a syslog server.

In the case of uncached URLs, the URL, destination IP address, and App-ID™ are transmitted to Palo Alto Networks WildFire® cloud-based threat analysis service.

Customer Privacy Options

You control the logging of usernames for the sessions on the firewall. The URL Filtering reporting functionality allows the creation of reports containing any data elements captured by the firewall, including usage reports for specific usernames. You have the option of activating administrative settings to block the display of certain usernames.

You also have the option of generating browse-time reports showing how much time a particular user spent on the internet, including specific domains.

Access and Disclosure

The information logged is stored on the firewall and can only be accessed by your system administrator and users authorized by the administrator. Palo Alto Networks customer support teams may also access report information, if allowed by the system administrator, for troubleshooting purposes.

In rare instances, the URL categorization process may uncover certain repeated illegal activity or access to illegal content, such as child pornography. In such cases, to the extent required or permitted by applicable law, Palo Alto Networks may notify law enforcement of the occurrence, along with the URL and contact information of the customer, for further investigation.

Retention

Retention times for data logged on the firewall are established by your system administrator. Requests for categorization of uncached URLs sent to PAN-DB are retained for six months.

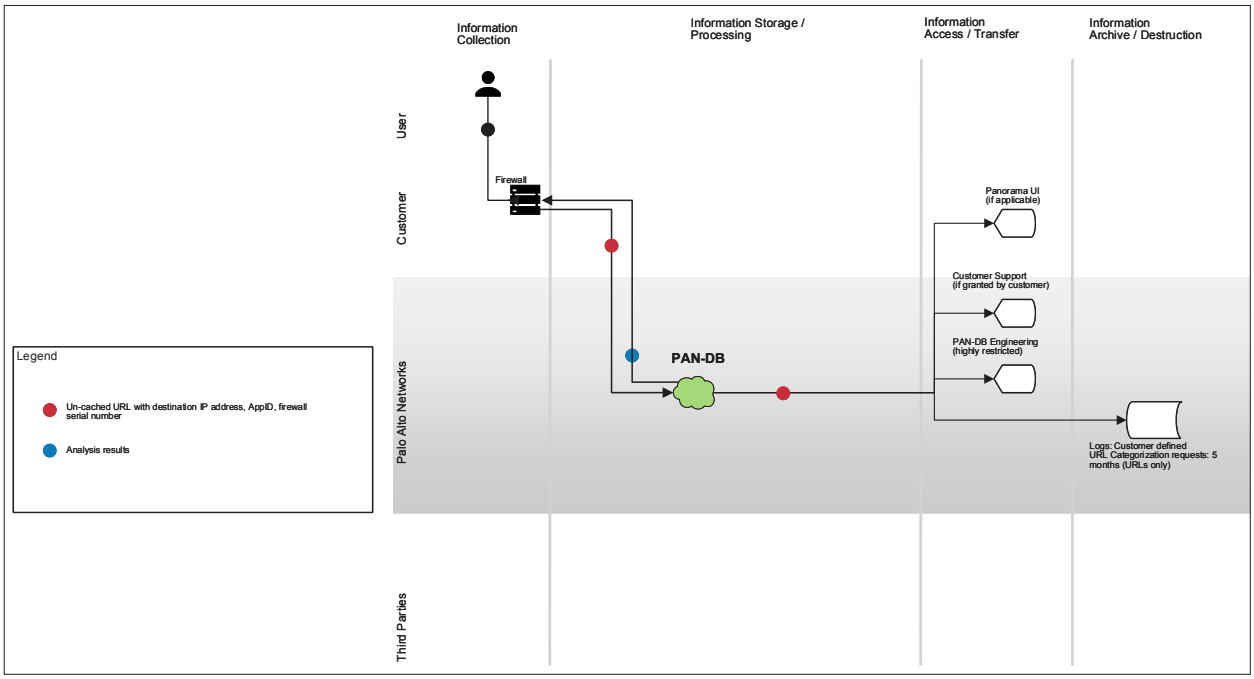
Security of Data in PAN-DB

All log data is stored locally on the firewall and can only be accessed by your system administrator and by authorized users designated the administrator. Information transferred to PAN-DB in the Palo Alto Networks cloud, such as uncached URLs, occurs over SSL connections.

Resources

- **Datasheet:** https://www.paloaltonetworks.com/resources/datasheets/integrated-url-filtering-datasheet
- **"At a Glance" Document:** https://www.paloaltonetworks.com/resources/faq/PAN_AAG_UF_031015
- **Lightboard on Phishing can be accessed at**: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb

Dataflow



About This Datasheet

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

url-filtering-privacy-ds-041818