LOGZILLA DOCUMENTATION

Palo Alto

LogZilla App Store application: Palo Alto

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/palo-alto

Overview

Palo Alto Networks next-generation firewalls running **PAN-OS** classify applications, users, and threats to secure network traffic. PAN-OS devices generate syslog messages for traffic flows, security threats, URL filtering, WildFire analysis, configuration changes, and system events.

The Palo Alto app parses these logs, extracts metadata into user tags, and reformats messages into readable key-value pairs for searching and alerting.

App Function

- Detects and auto-classifies all PAN-OS log types: **TRAFFIC**, **THREAT**, **SYSTEM**, **CONFIG**, **URL**, **WILDFIRE**, **TUNNEL**, **USERID**, **HIPMATCH**, and **DATA**.
- Parses key/value pairs from each event and stores them as user tags for fast filtering.
- Extracts high-value threat fields: severity, threat name, direction, and application for SOC threat hunting.
- Automatically converts numeric ports to friendly service names (e.g., `443` → `https`).
- Normalizes geographic locations (RFC1918 ranges → "Internal").
- Re-formats CSV messages into readable key/value pairs.
- Ships with Security and Traffic dashboards plus high-priority triggers for critical threats, C2, malware, and data exfiltration.

Vendor Documentation

- PAN-OS Administrator's Guide (https://docs.paloaltonetworks.com/pan-os)
- Configure Syslog Monitoring (https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-syslog-monitoring)
- Syslog Field Descriptions (https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/syslog-field-descriptions)
- Traffic Log Fields (https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/traffic-log-fields)

LogZilla Configuration

The Palo Alto app requires a dedicated syslog port for Palo Alto events.

Navigate to **Settings > System > Application Ports**
Set **Palo Alto syslog port** to a dedicated port (e.g., `5518`)
Click **Save**
The syslog and parser services will reload automatically. Both TCP and UDP listeners are enabled on the configured port.

Device Configuration

Configure Syslog Server Profile

Navigate to **Device > Server Profiles > Syslog** and click **Add**
Enter a **Name** for the profile
If the firewall has multiple virtual systems, select the **Location** (vsys or Shared)
In the **Servers** tab, click **Add** and configure:

- **Name**: Unique name for the server entry
- **Syslog Server**: LogZilla server IP address or FQDN
- **Transport**: TCP (recommended), UDP, or SSL
- **Port**: `5518` (dedicated Palo Alto port)
- **Format**: BSD (default) or IETF
- **Facility**: LOG_USER (default)

Click **OK** to save the server profile

Configure Syslog Hostname Format (Optional)

Navigate to **Device > Setup > Management**
Click the Edit icon in the **Logging and Reporting Settings** section
Select the **Log Export and Reporting** tab
Set **Syslog HOSTNAME Format** to one of:

- `FQDN` (default) - hostname and domain name
- `hostname` - hostname only
- `ipv4-address` - IPv4 address of sending interface
- `ipv6-address` - IPv6 address of sending interface

Click **OK** to save

Configure Custom Log Formats

Threat Log Format
Select `Custom Log Format` tab, choose `Threat`, and paste:

```
PaloAlto_Threat type="$type" src="$src" dst="$dst" rule="$rule" srcuser="$srcuser"
sessionid="$sessionid" action="$action" misc="$misc" dstloc="$dstloc" referer="$referer"
http_method="$http_method" http_headers="$http_headers"
```

Traffic Log Format

Select `Custom Log Format` tab, choose `Traffic`, and paste:

```
PaloAlto_Traffic type="$type" src="$src" dst="$dst" natsrc="$natsrc" natdst="$natdst" rule="$rule"
srcuser="$srcuser" from="$from" to="$to" sessionid="$sessionid" sport="$sport" dport="$dport"
natsport="$natsport" natdport="$natdport" proto="$proto" action="$action" bytes="$bytes"
packets="$packets" dstloc="$dstloc" action_source="$action_source"
```

Save and commit all configuration changes

Log Source Details

Item	Value
Vendor	Palo Alto Networks
Device Type	Next-Generation Firewall
Collection Method	Syslog (TCP/UDP)
Configurable Log Output?	Yes
Log Source Type	CSV or Key-Value pairs

Incoming Log Formats

PAN-OS can output logs in two different ASCII formats, both of which are handled by the Palo Alto app:

CSV syslog - the default format where each log is a comma-separated list of fields. The first few fields indicate the log *type* (e.g. `TRAFFIC`, `THREAT`).
Custom key/value syslog - when a *Custom Log Format* is configured on the firewall the message is emitted as white-space separated key/value pairs (e.g. `type="TRAFFIC" src="10.1.1.1" ...`).
Regardless of the on-device format, the app rewrites the event so the final stored message is an easy-to-read set of key/value pairs.

Parsed Metadata Fields

The following user tags are extracted from PAN-OS log messages.

Common Fields (All Log Types)

Tag Name	Example	Description
PA Type	TRAFFIC	Log type identifier
SrcIP	192.168.1.100	Source IP address
DstIP	10.0.1.50	Destination IP address
Action	allow	Action taken
PA Rule	Allow-Web	Security rule name
User	domain\user	Source username
Application	web-browsing	App-ID identified application
PA Src Location	Internal	Source geographic location
PA Dst Location	United States	Destination geographic location
PA Device Name	PA-440	Device hostname

Traffic Log Fields

Tag Name	Example	Description
SrcNAT	203.0.113.1	NAT source IP
DstNAT	203.0.113.2	NAT destination IP
DstPort	https	Destination port (service name)
Protocol	tcp	Protocol
PA Action Source	from-policy	Action source
PA Session End Reason	tcp-fin	Session termination reason

Threat Log Fields

Tag Name	Example	Description
PA Subtype	vulnerability	Threat subtype
PA Threat Name	Eicar File Detected(39040)	Threat signature name and ID
PA Severity	critical	Threat severity level
PA Category	malware	Threat category
Direction	client-to-server	Traffic direction

URL Log Fields

Tag Name	Example	Description
PA URL	malware-site.net/download	Accessed URL
PA Category	phishing	URL category

WildFire Log Fields

Tag Name	Example	Description
PA Filename	malware.exe	Analyzed filename
PA Category	malware	WildFire verdict

HIP Match Log Fields

Tag Name	Example	Description
PA Machine Name	DESKTOP-ABC123	Endpoint machine name
PA OS	Windows	Endpoint operating system

Tag Name	Example	Description
PA HIP Profile	Compliant	HIP profile match

Config Log Fields

Tag Name	Example	Description
PA Admin	admin	Administrator username
PA Client IP	192.168.50.76	Admin client IP
PA Result	Succeeded	Configuration result

System Log Fields

Tag Name	Example	Description
PA Content Type	general	Content type
PA Event ID	general	Event identifier

Log Examples

Traffic Log (CSV Format)

```
1,2025/07/03 10:15:30,021201157768,TRAFFIC,end,2817,2025/07/03 10:15:30,
192.168.50.100,8.8.8.8,0.0.0.0,0.0.0.0,Allow-DNS,,,dns,vsys1,trust,untrust,
ethernet1/1,ethernet1/2,,2025/07/03 10:15:30,12345,1,53,53,0,0,0x0,udp,allow,
150,150,0,1,2025/07/03 10:15:28,2,any,0,1234567890,0x0,US,US,0,1,0,aged-out,0,
0,0,0,,PA-440,from-policy
```

Threat Log (CSV Format)

```
1,2025/07/03 11:22:45,021201157768,THREAT,url,2817,2025/07/03 11:22:45,
192.168.50.50,203.0.113.100,0.0.0.0,0.0.0.0,Block-Malware,domain\jsmith,,
web-browsing,vsys1,trust,untrust,ethernet1/1,ethernet1/2,,2025/07/03 11:22:45,
54321,1,54321,80,0,0,0x0,tcp,block-url,"malware.example.com/payload",
```

```
malware(12345),informational,client-to-server,1234567891,0x0,US,RU,0,
text/html,,,,,0x0,,,,,,,,,PA-440
```

System Log (CSV Format)

```
1,2025/07/03 09:29:05,021201157768,SYSTEM,general,2817,2025/07/03 09:29:05,,
general,,0,0,general,informational,"Connection to Update server:
updates.paloaltonetworks.com completed successfully, initiated by
192.168.50.2",7520354041554025364,0x8000000000000000,0,0,0,0,,PA-440,0,0,
2025-07-03T09:29:47.040-06:00
```

Config Log (CSV Format)

```
1,2025/07/03 09:29:36,021201157768,CONFIG,0,2817,2025/07/03 09:29:37,
192.168.50.76,,edit,admin,Web,Succeeded,network interface ethernet
ethernet1/3,7520354041554010118,0x8000000000000000,0,0,0,0,,PA-440,0,,0,
2025-07-03T09:29:37.609-06:00
```

Custom Key-Value Format (Traffic)

```
PaloAlto_Traffic type="TRAFFIC" src="192.168.1.100" dst="203.0.113.50"
natsrc="203.0.113.1" natdst="203.0.113.50" rule="Allow-Web"
srcuser="domain\jdoe" from="trust" to="untrust" sessionid="54321"
sport="54321" dport="443" proto="tcp" action="allow" bytes="2048"
packets="15" dstloc="US" action_source="from-policy"
```

Custom Key-Value Format (Threat)

```
PaloAlto_Threat type="THREAT" src="192.168.1.100" dst="203.0.113.50"
rule="Allow-Web" srcuser="domain\jdoe" sessionid="54321" action="alert"
misc="" dstloc="US" referer="https://example.com" http_method="GET"
http_headers="User-Agent: Mozilla/5.0"
```

Triggers

Trigger	Description
`Palo Alto: Critical/High Severity Threat`	Critical or high severity threat detected
`Palo Alto: Command and Control Detected`	C2 traffic detected (immediate investigation)
`Palo Alto: Malware/Spyware Detected`	Virus, spyware, or WildFire malware
`Palo Alto: Phishing Detected`	Phishing category URL or threat
`Palo Alto: Threat Detected`	General threat with block/drop/reset action
`Palo Alto: Traffic Denied`	Traffic denied or dropped
`Palo Alto: Configuration Change Failed`	Failed configuration change
`Palo Alto: Configuration Change`	Configuration change with admin context
`Palo Alto: Data Exfiltration Attempt`	DATA filtering/DLP event
`Palo Alto: WildFire Malware Detected`	WildFire malware verdict
`Palo Alto: Endpoint HIP Check`	GlobalProtect HIP profile match
`Palo Alto: System Event`	System events with content type
`Palo Alto: System Error`	System errors or critical events