

LOGZILLA DOCUMENTATION

Palo Alto PAN-OS Configuration

Configure Palo Alto PAN-OS syslog server profiles, custom log formats for traffic and threat logs, and log forwarding to LogZilla

Receiving Data in LogZilla · Generated June 11, 2026 · logzilla.ai/docs/receiving-data/paloalto-pan-os-configuration

Configure PAN-OS Syslog

Prerequisites

- Include the device IPv4 address in the syslog header: Panorama/Device > Setup > Management → Logging and Reporting Settings → Log Export and Reporting → set Syslog HOSTNAME Format to ipv4-address.
- Confirm syslog listener ports in LogZilla (see [Syslog Settings](https://www.logzilla.ai/docs/administration/syslog-settings) (<https://www.logzilla.ai/docs/administration/syslog-settings>)).

Create a syslog server profile

Opens `Server Profiles > Syslog` and select `Add`.

A profile Name and Location is specified (Location refers to the virtual system when VSYS is enabled).

On the `Servers` tab, an entry is added with:

- Syslog Server (LogZilla IP or hostname)
- Transport (UDP/TCP as required)
- Port (default 514 for UDP)
- Facility (for example, LOG_USER)

Custom log formats

Threat logs

```
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 logs

```
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"
```

Attach log forwarding

A `Log Forwarding` profile is created or updated to reference the syslog server profile (`Objects → Log Forwarding`).

The forwarding profile is applied to the required security policies: `Policies → Security → select a rule → Actions → set Log Forwarding` to the created profile. `Log at Session End` can be enabled as required.

Commit changes

Commit the configuration (Changes → Commit).

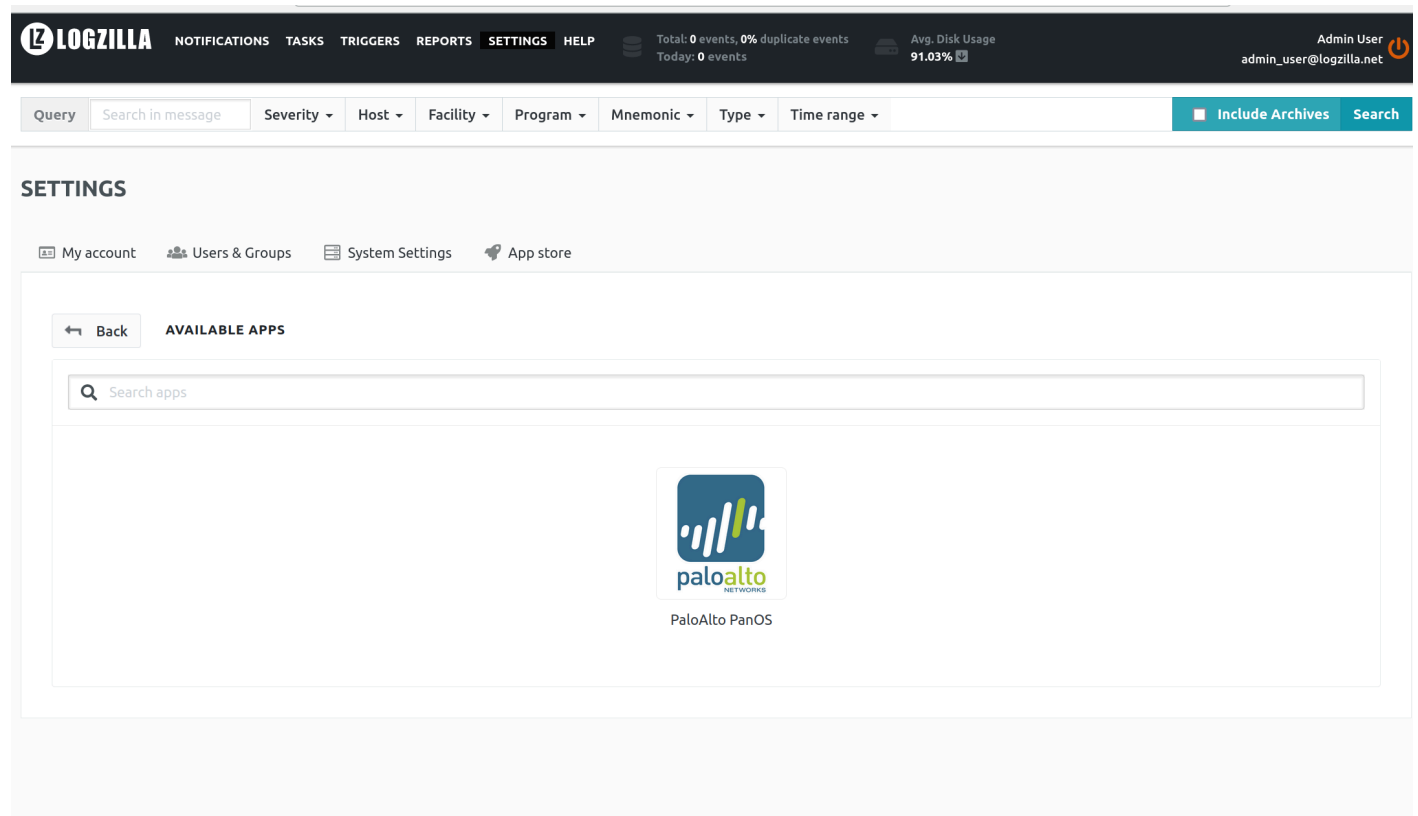
Verify in LogZilla

- Reception can be confirmed by searching for the device host or expected text in LogZilla.
- For packet-level checks, use [Syslog Troubleshooting](https://www.logzilla.ai/docs/administration/syslog- troubleshooting) (<https://www.logzilla.ai/docs/administration/syslog- troubleshooting>).

LogZilla Rules and Dashboards

Rules and dashboards for Palo Alto are available in the LogZilla appstore (Settings → App store).

Install the Palo Alto app to enable the rule.



The screenshot displays the LogZilla web interface. At the top, a navigation bar includes the LogZilla logo and menu items: NOTIFICATIONS, TASKS, TRIGGERS, REPORTS, SETTINGS (highlighted), and HELP. On the right of the navigation bar, there are status indicators: 'Total: 0 events, 0% duplicate events' and 'Today: 0 events', along with 'Avg. Disk Usage 91.03%'. The user is identified as 'Admin User' with the email 'admin_user@logzilla.net'. Below the navigation bar is a search bar with a 'Query' field and a 'Search' button. The main content area is titled 'SETTINGS' and contains a sub-menu with 'My account', 'Users & Groups', 'System Settings', and 'App store' (selected). The 'App store' section is titled 'AVAILABLE APPS' and features a search bar labeled 'Search apps'. A single app, 'Palo Alto PanOS', is displayed with its logo and name.

Related topics

- [Syslog Settings](https://www.logzilla.ai/docs/administration/syslog-settings) (<https://www.logzilla.ai/docs/administration/syslog-settings>)
- [Syslog Troubleshooting](https://www.logzilla.ai/docs/administration/syslog- troubleshooting) (<https://www.logzilla.ai/docs/administration/syslog- troubleshooting>)

Example dashboards

After installation, the dashboards will look similar to these examples.

Threat dashboard

The screenshot displays the LogZilla Threat dashboard for Palo Alto. At the top, there's a navigation bar with 'LOGZILLA' logo, 'NOTIFICATIONS 19', 'TASKS', 'TRIGGERS', 'REPORTS', 'SETTINGS', and 'HELP'. It also shows system stats: 'Total: 14.4m events, 34% duplicate events', 'Avg. Disk Usage: 23.66%', and 'New version available!'. The user is identified as 'Admin User' with email 'support@logzilla.net'.

The dashboard features several widgets:

- Threat Events Per Second:** A gauge showing 'Average' at 23 and 'Max' at 56, alongside a bar chart of events per second over time.
- Threat Events Minute:** A gauge showing 'Average' at 1.1k and 'Max' at 1.4k, with a bar chart of events per minute.
- Top Blocked Users:** A table listing users like k2arn (22), 0a2h (21), kyng (21), nbwek (18), v72ew (18), and v102y (9).
- Threat vs. Threat Distribution:** A bar chart comparing 'TRAFFIC' (red) and 'THREAT' (green) over time.
- Top Destination Locations:** A table showing event counts for locations: United States (7,151), Brazil (1,270), Ireland (150), Canada (107), France (34), Poland (34), Germany (15), Japan (15), and Singapore (15).
- Threat Rules:** A table showing event counts for rules: Web Default (8,421), Web Collaborators (100), Web Personnel (50), Web Privileged Access (49), and Web Streaming (32).
- Top 5 Users:** A table listing top users: 0a2h (22), k2arn (22), kyng (21), idpp (19), and nbwek (18).
- Threat Actions:** A line chart showing 'block/ut' (green) and 'alert' (red) actions over time.
- Live Stream: Threat Events:** A table of recent events with columns for SEVERITY, HOST, FACILITY, PROGRAM, MESSAGE, FIRST SEEN, and LAST SEEN.

At the bottom, there's a footer with 'English', 'EULA', 'Copyright © 2014-2020 LogZilla - All Rights Reserved', and 'v6.6.15'.

Traffic dashboard

LOGZILLA NOTIFICATIONS TASKS TRIGGERS REPORTS SETTINGS HELP Total: 14.4m events 34% duplicate events Avg. Disk Usage Today: 2.5m events 21.55% Admin User support@logzilla.net

Query Search in message Severity Host Facility Program Mnemonic Time range Type Search

PaloAlto: Traffic

Traffic Events Per Second

Average: 49
Max: 84

Traffic Events Per Day

Average: 0
Max: 15.3k

Top Source Users

Top NAT Sources

Top Destination Locations

EVENT_SRC_PALALTO_TRAFFIC_DESTINATION_LOCATIONS	EVENTS
United States	13,019
Brazil	894
Ireland	347
Russian Federation	133
158.230.210.126-217.87.113.18	83
66.199.81.188-48.161.8.719	72
Portugal	61
Argentina	52
Australia	49
China	49
Germany	48
Ukraine	48
Canada	39
Poland	39
Moldova Republic Of	37
5.175.199.207-107.224.10.194	33
789.74.20-204.58.234.122	33
Japan	25
United Kingdom	24
Netherlands	23
Singapore	22
Cyprus	13
Estonia	13
France	13
Indonesia	13

Traffic Action Sources

Top Traffic Sources

Top Hosts

Traffic Rules

Traffic Actions

Live Stream: Traffic Events

SEVERITY	HOST	FACILITY	PROGRAM	MESSAGE	FIRST SEEN	LAST SEEN
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="122.39.81.232" d="dst" 194.2.38.7 - "natsrc=" 47.9.197.170 - "natdst=" 194.2.38.7 - "rule="Web Default" srcuser="user_cianb" from="LAN" to="WAN" sessionid="132269" repeatrt="1" sport="55819" dport="443" nat sport="39662" natdport="443" proto="tcp" action="allow" bytes="8367" packets="98" dstloc="Brazil" action_source="from-policy"	2020-01-15 12:08:52.0890	2020-01-15 12:08:52.0890
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="16.231.509.149" d="dst" 52.2.34.171 - "natsrc=" 86.212.222.189 - "natdst=" 52.2.34.171 - "rule="Rule 300" srcuser="user_2brs" from="DMZ" to="WAN" sessionid="12184" repeatrt="1" sport="52483" dport="5061" nat sport="52483" natdport="5061" proto="tcp" action="allow" bytes="62" packets="1" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:28.0740	2020-01-15 12:08:52.0730
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="181.196.1.147" d="dst" 61.217.245.19 - "natsrc=" 47.9.197.170 - "natdst=" 61.217.245.19 - "rule="Internet Services" srcuser="user_ajysc" from="LAN" to="WAN" sessionid="21361" repeatrt="1" sport="63761" dport="443" nat sport="60235" natdport="443" proto="tcp" action="allow" bytes="62" packets="1" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:28.0560	2020-01-15 12:08:52.0570
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="123.4.106.7" d="dst" 132.82.161.81 - "natsrc=" 47.9.197.170 - "natdst=" 132.82.161.81 - "rule="Internet Services" srcuser="user_2brs" from="LAN" to="WAN" sessionid="190126" repeatrt="1" sport="57434" dport="53" nat sport="28392" natdport="53" proto="udp" action="allow" bytes="292" packets="2" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:28.0380	2020-01-15 12:08:52.0410
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="121.197.15.228" d="dst" 160.36.87.35 - "natsrc=" 47.9.197.170 - "natdst=" 160.36.87.35 - "rule="RULE-WFPI" srcuser="user_2brs" from="LAN" to="WAN" sessionid="104940" repeatrt="1" sport="48170" dport="443" nat sport="17965" natdport="443" proto="tcp" action="allow" bytes="15670" packets="63" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:28.0200	2020-01-15 12:08:52.0240
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="115.203.236.176" d="dst" 39.189.136.245 - "natsrc=" 47.9.197.170 - "natdst=" 39.189.136.245 - "rule="Web Collaborators" srcuser="user_vj2z" from="LAN" to="WAN" sessionid="129914" repeatrt="1" sport="60745" dport="443" nat sport="65468" natdport="443" proto="tcp" action="allow" bytes="7042" packets="29" dstloc="Brazil" action_source="from-policy"	2020-01-15 12:08:28.0030	2020-01-15 12:08:52.0080
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="192.244.183.55" d="dst" 137.146.178.179 - "natsrc=" 47.9.197.170 - "natdst=" 137.146.178.179 - "rule="RULE-DUMMY" srcuser="user_kewp" from="LAN" to="WAN" sessionid="74072" repeatrt="1" sport="53514" dport="443" nat sport="11083" natdport="443" proto="tcp" action="allow" bytes="418" packets="0" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:27.9850	2020-01-15 12:08:51.9910
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="192.244.183.55" d="dst" 113.252.1.167 - "natsrc=" 47.9.197.170 - "natdst=" 113.252.1.167 - "rule="Web Default" srcuser="user_kewp" from="LAN" to="WAN" sessionid="25196" repeatrt="1" sport="53513" dport="80" nat sport="21972" natdport="80" proto="tcp" action="allow" bytes="568" packets="6" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:27.9670	2020-01-15 12:08:51.9750
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="192.244.183.55" d="dst" 113.252.1.167 - "natsrc=" 47.9.197.170 - "natdst=" 113.252.1.167 - "rule="Web Default" srcuser="user_kewp" from="LAN" to="WAN" sessionid="138387" repeatrt="1" sport="53518" dport="80" nat sport="35996" natdport="80" proto="tcp" action="allow" bytes="562" packets="6" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:27.8490	2020-01-15 12:08:51.9580
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="122.227.4.147" d="dst" 61.217.245.19 - "natsrc=" 47.9.197.170 - "natdst=" 61.217.245.19 - "rule="Internet Services" srcuser="user_jm0" from="LAN" to="WAN" sessionid="52295" repeatrt="1" sport="55497" dport="443" nat sport="63815" natdport="443" proto="tcp" action="allow" bytes="62" packets="1" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:27.7930	2020-01-15 12:08:51.9420
info	181.223.138.241	USER	PaloAlto_Traffic	type="TRAFFIC" src="157.221.169.171" d="dst" 61.217.245.19 - "natsrc=" 47.9.197.170 - "natdst=" 61.217.245.19 - "rule="Internet Services" srcuser="user_ogp2h" from="LAN" to="WAN" sessionid="29569" repeatrt="1" sport="60213" dport="443" nat sport="41258" natdport="443" proto="tcp" action="allow" bytes="62" packets="1" dstloc="United States" action_source="from-policy"	2020-01-15 12:08:27.7130	2020-01-15 12:08:51.9250

English EULA Copyright © 2014-2020 LogZilla - All Rights Reserved v6.6.15