LOGZILLA DOCUMENTATION

Checkpoint

LogZilla App Store application: Checkpoint

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/checkpoint

Overview

Check Point Software Technologies provides enterprise network security solutions including next-generation firewalls, VPN gateways, and threat prevention systems. The VPN-1 & FireWall-1 product family delivers deep packet inspection, application control, and identity awareness capabilities.

App Function

The Check Point app performs the following functions:

- Parse Check Point syslog messages containing key-value pairs
- Extract network, identity, and security metadata into user tags
- Translate numeric values (confidence level, app risk) to human-readable names
- Convert port numbers to service names
- Classify events for cross-vendor filtering (network, security, auth)

LogZilla Configuration

Check Point requires a dedicated syslog port in LogZilla because Check Point's syslog format does not include a standard program name field.

Step 1: Configure Dedicated Port

Navigate to **Settings > System > Application Ports**
Set **Check Point syslog port** to a dedicated port (e.g., `5514`)
Click **Save**
The syslog and parser services will reload automatically. Both TCP and UDP listeners are enabled on the configured port.

Step 2: Configure Check Point Device

Navigate to **Logs & Monitoring** → **External Log Servers**
Click **Configure** under Syslog Servers
Add a new syslog server with:

- **Protocol**: UDP or TCP
- **IP address**: LogZilla server IP
- **Port**: The dedicated port configured above (e.g., `5514`)

Enable **System logs** and/or **Security logs**

Click **Apply**

Vendor Documentation

- Check Point Log Reference (https://support.checkpoint.com/results/sk/sk144192)
- Check Point Community (https://community.checkpoint.com)
- Check Point Support Center (https://support.checkpoint.com)

Log Source Details

Item	Value
Vendor	Check Point Software Technologies
Device Type	Next-Generation Firewall, VPN Gateway
Collection Method	Syslog (RAW port)
Configurable Log Output?	Yes
Log Source Type	Key-value pairs

Incoming Log Format

Check Point logs use key-value pair format with values enclosed in double quotes.

```
<85>Aug 8 15:55:39 GATEWAY01 Action="accept" inzone="Internal"
outzone="External" src="172.16.0.4" dst="8.8.8.8" proto="17"
protocol="DNS-UDP" user="" ProductName="VPN-1 & FireWall-1"
```

Parsed Metadata Fields

The app extracts a curated whitelist of fields using human-friendly tag names.

Global Tags

Tag Name	Example	Description
Vendor	Check Point	Vendor name
Product	Firewall	Product name
Event Class	network	Event classification (network, security, auth)

Standardized Tags

Tag Name	Example	Description
Action	accept	Firewall action
SrcIP	172.16.0.4	Source IP address
DstIP	8.8.8.8	Destination IP address
User	jsmith	Username
Protocol	DNS-UDP	Protocol name
DstPort	https	Destination port
SrcNAT	203.0.113.1	NAT translated source IP
DstNAT	203.0.113.2	NAT translated destination IP

Check Point Product Tags

Tag Name	Example	Description
CP Product	VPN-1 & FireWall-1	Check Point product name
CP Product Family	Network	Product family
CP Source Zone	Internal	Source security zone

Tag Name	Example	Description
CP Destination Zone	External	Destination security zone
CP Rule	Allow-Web	Matched rule name
CP Policy	Standard	Security policy name

Identity Tags

Tag Name	Example	Description
CP Source User	jsmith	Source username
CP Source Machine	WORKSTATION01	Source machine name
CP VPN User	vpn_user1	VPN username

Security Tags

Tag Name	Example	Description
CP Attack	SQL Injection	Detected attack name
CP Malware Family	Trojan	Malware family name
CP Verdict	Malicious	Threat verdict
CP Severity	High	Event severity
CP Confidence	High	Threat confidence

Application Control Tags

Tag Name	Example	Description
CP Application	Facebook	Application name
CP App Risk	Medium	Application risk level

Tag Name	Example	Description
`CP Category`	`Social Networking`	URL/application category

Value Translations

The app translates numeric values to human-readable names:

Confidence Level

Raw	Translated
0	N/A
1	Low
2	Medium-Low
3	Medium
4	Medium-High
5	High

Application Risk

Raw	Translated
0	Unknown
1	Very Low
2	Low
3	Medium
4	High
5	Critical

Event Classification

The `Event Class` tag enables cross-vendor dashboard filtering:

Value	Trigger Fields
`security`	attack, malware_family, malware_action, protection_id
`auth`	auth_status, auth_method
`network`	Default for firewall logs

MITRE ATT&CK Mapping

The app maps security events to MITRE ATT&CK techniques:

Event Type	MITRE Technique	Tactic
SQL Injection	T1190	Initial Access
XSS Attack	T1189	Initial Access
Command Injection	T1059	Execution
Brute Force	T1110	Credential Access
DoS/DDoS	T1499	Impact
Malware/Trojan	T1204	Execution
Ransomware	T1486	Impact

Triggers

Trigger	Condition
Check Point: MITRE ATT&CK Threat Detected	Any MITRE-mapped threat
Check Point: Malware Detected	CP Malware Family exists

Trigger	Condition
Check Point: Attack Detected	CP Attack exists
Check Point: High Risk Application	CP App Risk = Critical/High
Check Point: VPN Connection Failed	VPN product + deny action
Check Point: Traffic Denied	Action = deny/drop/reject/block
Check Point: Traffic Accepted	Action = accept/allow

Log Examples

Firewall Accept

```
<85>Aug 8 15:55:39 GATEWAY01 Action="accept" inzone="Internal"
outzone="External" src="172.16.0.4" dst="8.8.8.8" proto="17"
xlatesrc="70.163.95.60" protocol="DNS-UDP" user=""
ProductName="VPN-1 & FireWall-1" svc="53" rule_name="Outgoing"
```

Firewall Drop

```
<85>Aug 8 16:22:15 GATEWAY01 Action="drop" src="203.0.113.50"
dst="192.168.1.100" proto="6" attack="SQL_Injection"
malware_action="block" verdict="malicious" severity="high"
ProductName="IPS Blade"
```

VPN Connection

```
<85>Aug 8 17:45:30 VPNGW01 Action="accept" src="198.51.100.45"
dst="192.168.1.100" proto="6" vpn_user="jsmith@company.com"
identity_type="vpn" client_type_os="Windows_10"
ProductName="VPN-1 & FireWall-1"
```