LOGZILLA DOCUMENTATION

Fortiweb

LogZilla App Store application: Fortiweb

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/fortiweb

Overview

FortiWeb is a standalone Web Application Firewall (WAF) appliance produced by Fortinet. FortiWeb protects web applications and APIs against OWASP Top 10 threats, DDoS attacks, malicious bots, and other web-based attacks.

FortiWeb is a **separate product** from FortiGate. While FortiGate firewalls include a built-in WAF module (`type="utm" subtype="waf"`), FortiWeb is a dedicated WAF appliance with its own distinct log format.

App Function

- Parse FortiWeb key/value pair log format
- Extract high-value tags for analysis and alerting
- Provide triggers for WAF attack detection and admin events
- MITRE ATT&CK mapping for attack events (T1190) and admin access (T1078)

Vendor Documentation

- FortiWeb Product Page (https://www.fortinet.com/products/web-application-firewall/fortiweb)
- FortiWeb 7.0 Log Reference (https://docs.fortinet.com/document/fortiweb/7.0.0/log-message-reference)

Device Configuration

Configure the FortiWeb appliance to send syslog to LogZilla:

Log into the FortiWeb web interface
Navigate to **Log & Report > Log Policy > Syslog Policy**
Click **Create New**
Configure the syslog server:

- Enter the LogZilla server IP address
- Set port to 514 (or match the LogZilla configuration)
- Set facility to `local0`

Navigate to **Log & Report > Log Policy > Log Settings**
Enable the log types to forward:

- **Attack Log** (recommended)
- **Traffic Log** (optional, high volume)
- **Event Log** (recommended)

Click **OK** to save

Verification

Generate web traffic through the FortiWeb, then verify events appear in LogZilla with the program name `FortiWeb`.

Incoming Log Format

FortiWeb uses a different KV format from FortiGate:

```
date=YYYY-MM-DD time=HH:MM:SS log_id=NNNNN msg_id=NNNNNN
device_id=FVVM... vd="value" type=attack pri=alert key=value ...
```

Key differences from FortiGate:

Field	FortiGate	FortiWeb
Log ID	`logid="0000000013"`	`log_id=20000042`
Severity	`level="warning"`	`pri=alert`
Type	`type="utm" subtype="waf"`	`type=attack`
Device ID	*(none)*	`device_id=FVVM...`
Message ID	*(none)*	`msg_id=000000001500`
Quoting	All values quoted	Mixed

Parsed Metadata Fields

Global Tags

Tag	Example	Description
`Vendor`	`Fortinet`	Vendor name
`Product`	`FortiWeb`	Product name

Tag	Example	Description
Event Class	Security	Cross-vendor classification
Event Type	Threat	Specific event type
MitreId	T1190	MITRE ATT&CK technique ID
MITRE Tactic	Initial Access	MITRE ATT&CK tactic

Standardized Tags

Tag	Example	Description
SrcIP	198.51.100.23	Source IP address
DstIP	10.1.1.50	Destination IP address
DstPort	https	Destination port (service name)
User	admin	Username (admin events)
Action	Deny	Action taken

FortiWeb-Specific Tags

Tag	Example	Description
FortiWeb Type	attack	Log type
FortiWeb Subtype	system	Event subtype
FortiWeb Status	success	Event status
FortiWeb Service	https	Service protocol
FortiWeb VDOM	root	Virtual domain
FortiWeb Device ID	FVVM020000012345	Appliance serial

Tag	Example	Description
FortiWeb Threat Level	Critical	Attack severity
FortiWeb Signature	SQL Injection	OWASP signature
FortiWeb Policy	owasp-top10	WAF policy name
FortiWeb HTTP Method	POST	HTTP method
FortiWeb HTTP Status	200	Response code
FortiWeb Server Pool	api-servers	Backend pool
FortiWeb Content Switch	api-server	Content route
FortiWeb Country	Russia	Source country

High-Cardinality (HC) Tags

The following tags are declared as high-cardinality and excluded from indexing:

- SrcIP
- DstIP
- User
- FortiWeb Signature

Log Examples

Attack - SQL Injection Blocked

```
date=2026-03-01 time=14:22:15 log_id=20000042 msg_id=000000001500
device_id=FVVM020000012345 vd="root" timezone="(GMT-5:00)New_York"
type=attack pri=alert proto=tcp service=https
src=198.51.100.23 src_port=44100 dst=10.1.1.50 dst_port=443
http_method=POST http_url=/api/v1/users http_host=api.example.com
msg="SQL Injection detected" action=Deny policy="owasp-top10"
signature_subclass="SQL Injection" signature_id=060010001
threat_level=Critical signature_cve="CVE-2021-44228"
```

Traffic - Normal Web Request

```
date=2026-03-01 time=16:05:00 log_id=30000010 msg_id=000000001700
device_id=FVVM020000012347 vd="PROD" timezone="(GMT+9:00)Tokyo"
type=traffic pri=info proto=tcp service=https
src=192.0.2.88 src_port=61234 dst=10.3.3.50 dst_port=443
http_method=GET http_url=/dashboard/main http_host=app.corp.local
http_response_code=200 policy="web-protection-1"
```

Admin Login

```
date=2026-03-01 time=18:00:00 log_id=10000150 msg_id=000000001900
device_id=FVVM020000098765 vd="vdom1"
timezone="(GMT-8:00)Los_Angeles"
type=event subtype=admin pri=information
user="admin" ui="GUI(192.168.1.100)" action=login status=success
src=10.1.1.25 msg="Admin login successful"
```

MITRE ATT&CK Mapping

Event Type	Technique	Tactic
WAF Attack	T1190	Initial Access
Admin Login	T1078	Defense Evasion

Triggers

Trigger	Description
`FortiWeb: MITRE ATT&CK Threat Detected`	MITRE-mapped events
`FortiWeb: Attack Blocked`	Blocked attack events
`FortiWeb: Attack Alert (Not Blocked)`	Alert-only attacks
`FortiWeb: Critical Threat`	Critical threat level
`FortiWeb: SQL Injection`	SQL injection attempts

Trigger	Description
`FortiWeb: Cross-site Scripting`	XSS attempts
`FortiWeb: Command Injection`	Command injection
`FortiWeb: Admin Login`	Admin access events
`FortiWeb: System Configuration Change`	Config changes