LOGZILLA DOCUMENTATION

Watchguard

Rules, dashboards, and triggers for Watchguard Firewall and Proxy

LogZilla App Store · Generated June 12, 2026 · logzilla.ai/docs/logzilla-appstore/watchguard

© LogZilla Corporation · logzilla.ai

Overview

WatchGuard Technologies produces network security appliances including the Firebox firewall series. WatchGuard devices provide unified threat management (UTM), intrusion prevention, VPN, and proxy services. Devices generate syslog messages for traffic events, attacks, VPN connections, and system health.

App Function

- Parse WatchGuard logs in both BSD syslog and IBM LEEF formats
- Extract network metadata (IPs, ports, protocols, interfaces)
- Categorize events by area (Firewall, Proxy, VPN, System)
- Provide dashboards for traffic monitoring and threat detection
- Alert on attacks, IPS detections, and policy violations

Vendor Documentation

- WatchGuard Syslog Server Settings (https://www.watchguard.com/help/docs/help-center/en-us/Content/en-US/Fireware/logging/send_logs_to_syslog_c.html)
- Types of Log Messages (https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/logging/log_message_types_c.html)

Device Configuration

Configure the WatchGuard Firebox to send syslog to LogZilla. The Firebox supports up to three syslog servers and two log formats: Syslog (BSD) and IBM LEEF.

Log Format Selection

Format	Use Case	Notes
Syslog	Standard syslog servers	BSD format with msg_id field
IBM LEEF	QRadar integration	LEEF 1.0 format, no Performance logs

Log Message Types

Type	Description
Traffic	Packet filter and proxy rule events
Alarm	Triggered events (IPS, AV, DoS, Policy)
Event	User activity, authentication, VPN
Debug	Diagnostic information
Statistic	Performance metrics

Syslog Facilities

Facility	Log Type
Local0	Alarm (highest priority)
Local1	Traffic
Local2	Event
Local3	Diagnostic
Local4	Performance

Fireware Web UI (v12.4+)

Log in to the Fireware Web UI
Navigate to **System** > **Logging**
Click the **Syslog Server** tab
Select **Send log messages to these syslog servers**
Click **Add**
Enter the LogZilla server IP address and port (default: 514)
Select **Log Format**: Syslog or IBM LEEF
Configure syslog facility for each log type (Local0 for alarms, Local1-4 for others)
Click **Save**

Policy Manager

Open Policy Manager and connect to the Firebox
Select **Setup** > **Logging**
Select **Send log messages to these syslog servers**
Click **Add**
Enter the LogZilla server IP address and port (default: 514)
Select **Log Format**: Syslog or IBM LEEF
Configure syslog facility for each log type
Click **OK**, then save the configuration to the Firebox

Verification

Generate test traffic or trigger a policy, then verify events appear in LogZilla with program name `firewall`.

Incoming Log Format

WatchGuard supports two log formats:

BSD Syslog Format

```
msg_id="3000-0148" Deny 0-External Firebox 32 udp 20 64 192.168.100.1 255.255.255.255 52346 10001
(Unhandled External Packet-00)
```

IBM LEEF Format

```
LEEF:1.0|WatchGuard|XTM|12.5.3.B616762|30000148|policy=Any From Firebox-00  disp=Allow  in_if=Firebox
out_if=0-External proto=udp src=192.168.100.2 srcPort=38963 dst=4.2.2.1 dstPort=53
```

Parsed Metadata Fields

Global Tags

Tag Name	Example	Description
`Vendor`	`WatchGuard`	Vendor name

Tag Name	Example	Description
Product	Firebox	Product name
Event Class	security	Cross-vendor event classification

Standardized Tags

Tag Name	Example	Description
SrcIP	192.168.1.100	Source IP address (HC)
DstIP	10.0.0.1	Destination IP address (HC)
DstPort	https	Destination port (named service)
Protocol	TCP	Network protocol
Action	Allow	Firewall action
User	admin	Username (HC)
SrcInt	1-Trusted	Source interface
DstInt	0-External	Destination interface

Security Tags

Tag Name	Example	Description
MitreId	T1498	MITRE ATT&CK technique ID (enables UI lookup)
MITRE Tactic	Impact	MITRE ATT&CK tactic
WG Signature ID	1112464	IPS signature ID (HC)
WG Signature Name	EXPLOIT buffer overflow	IPS signature name
WG Virus	EICAR-Test-File	Detected malware name

Tag Name	Example	Description
`WG Event Type`	`VPN Auth Failure`	WatchGuard-specific event type

MITRE ATT&CK Coverage

Security events are mapped to MITRE ATT&CK techniques:

Technique	Tactic	Event Types
T1498	Impact	DoS/DDoS flood attacks
T1046	Discovery	Port and IP scans
T1557	Credential Access	ARP spoofing attacks
T1090	Command and Control	IP spoofing, source routing
T1071	Command and Control	Blocked sites/ports
T1190	Initial Access	IPS exploit detections
T1204	Execution	APT threats, malware
T1566	Initial Access	Spam/phishing emails

Log Examples

IP Already On Blocked List

```
msg_id="3000-002A" IP address 192.168.111.10 will not be added to the
blocked sites list because it already exists.
```

Quota Usage for User

```
msg_id="3000-0065" User James@Firebox-DB used 21 MB of the bandwidth
quota (100 MB) and used 1 minute of the time quota (3 minutes).
```

DNS Parse Error

```
msg_id="1DFF-0003" Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143
56704 53 msg="ProxyDeny: DNS parse error" (DNS-proxy-00)
```

APT Threat Notification

```
msg_id="0F01-0015" APT threat notified. Details=''Policy Name:
HTTPS-proxy-00 Reason: high APT threat detected Task_UUID:
d09445005c3f4a9a9bb78c8cb34edc2a Source IP: 10.0.1.2 Source Port:
43130 Destination IP: 67.228.175.200 Destination Port: 443 Proxy
Type: HTTP Proxy Host: analysis.lastline.com Path:
/docs/lastline-demo-sample.exe
```

Dashboards

Dashboard	Focus	Key Widgets
`WatchGuard: Security`	Threat detection and MITRE analysis	Threats, MITRE tactics, malware, IPS
`WatchGuard: Network`	Traffic analysis and visibility	Sources, destinations, interfaces, protocols

Triggers

Trigger	Description
`WatchGuard: MITRE ATT&CK Threat Detected`	Catch-all for any MITRE-mapped threat
`WatchGuard: DDoS Attack Detected`	DDoS flood attacks (MITRE T1498)
`WatchGuard: Port or IP Scan Detected`	Network reconnaissance (MITRE T1046)
`WatchGuard: ARP Spoofing Attack`	Layer 2 credential theft (MITRE T1557)
`WatchGuard: Malware Detected`	Virus or malware found by proxy
`WatchGuard: IPS Intrusion Blocked`	IPS signature triggered

© LogZilla Corporation · logzilla.ai

Trigger	Description
`WatchGuard: Potential C2 Communication`	Blocked C2 traffic (MITRE T1071)
`WatchGuard: Traffic Routing Anomaly`	IP spoofing or source routing (MITRE T1090)
`WatchGuard: Spam or Phishing Detected`	Email threats (MITRE T1566)
`WatchGuard: Malicious User Execution`	APT or malware execution (MITRE T1204)
`WatchGuard: Credential Access Attempt`	Credential theft attempts
`WatchGuard: VPN Authentication Failure`	Failed VPN login attempts

© LogZilla Corporation · logzilla.ai