LOGZILLA DOCUMENTATION

Sonicwall

LogZilla App Store application: Sonicwall

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

Overview

SonicWall SonicOS is the operating system for SonicWall NSa, NSsp, NSv and TZ firewall appliances. SonicOS 6.x and 7.x emit syslog events for traffic flows, SSL VPN authentication, application control, content filtering, geo-IP blocking, and IPv6 anomalies. The parser handles the Default (key=value) syslog format and normalizes events into LogZilla tags for cross-vendor dashboards and triggers.

App Function

- Parse SonicWall Default-format syslog from SonicOS 6.x and 7.x
- Detect SonicWall traffic by message content, so a customized "Syslog ID" on the firewall does not break parsing
- Extract source/destination IPs, MACs, ports, zones, NAT, applications, rules, and content-filter categories
- Classify events by message ID into Auth / Network / Security / Web Event Classes and apply compliance framework tags
- Strip vendor-embedded timestamp and per-event sequence counter to enable deduplication of repeated events

Vendor Documentation

- SonicOS 7.0 Device Log - Syslog (https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7.0.1-device_log/Content/Logs_Syslog/logs-syslog.htm)
- SonicOS/X 7.0.1 Log Events Reference Guide (PDF) (https://www.sonicwall.com/techdocs/pdf/SonicOS-X_7.0.1_LogEvents_ReferenceGuide.pdf)
- SonicWall technical documentation portal (https://www.sonicwall.com/support/technical-documentation)

Device Configuration

Configure the SonicWall to send syslog to LogZilla:

Log into the SonicWall management interface
Navigate to **Device > Log > Syslog** (SonicOS 7.x) or **Log > Syslog** (SonicOS 6.x)
Under **Syslog Servers**, click **Add**
Configure:

- **Name or IP Address**: LogZilla server IP
- **Port**: 514 (default) or any port LogZilla is listening on
- **Server Type**: Syslog Server

Under **Syslog Settings**, set:

- **Syslog Format**: Default

- **Syslog Facility**: Local Use 0 (or any local facility)
- **Syslog ID**: leave as `firewall` (the default), or set it to a custom value. The parser detects SonicWall events by message content, so any value works.

Click **Accept** / **Save** to apply

Verification

After saving, verify events appear in LogZilla under the program name `SonicWall` with the `Vendor: SonicWall` user tag.

Incoming Log Format

SonicWall Default-format messages are space-separated key=value pairs. The program field carries the configured Syslog ID (`id=<value>`) and the message body begins at `sn=`:

```
sn=<serial> time="<ts>" fw=<fw_ip> pri=<n> c=<category_id> gcat=<group>
m=<msg_id> msg="<text>" src=<ip>:<port>:<intf> srcZone=<zone>
natSrc=<ip>:<port> dst=<ip>:<port>:<intf> dstZone=<zone>
natDst=<ip>:<port> usr="<user>" proto=<proto>/<svc>
rule="<rule_name>" app=<id> appName='<app>' n=<seq>
fw_action="<action>"
```

Common fields:

Field	Description
`sn`	Device serial number
`time`	Vendor timestamp (stripped from the message during parsing)
`fw`	Firewall public/management IP
`pri`	SonicWall internal priority (0=emergency .. 7=debug)
`c`	Numeric category code
`gcat`	Group category (2=network access, 3=geo-ip, 4=ssl-vpn, 6=traffic, 10=app-rules, 13=ssl-vpn-client)
`m`	Message ID (drives Event Class / Type classification)
`src` / `dst`	IP:port:interface tuples

Field	Description
`srcZone` / `dstZone`	SonicWall security zone (LAN, WAN, SSLVPN, DMZ)
`natSrc` / `natDst`	Post-NAT addresses
`usr`	Authenticated user (`Unknown` if unauthenticated)
`proto`	Protocol family and service (`tcp/https`, `udp/dns`)
`fw_action`	Firewall verdict (`forward`, `drop`, `deny`, `NA`)
`n`	Per-event sequence counter (stripped to enable deduplication)

Parsed Metadata Fields

Cross-Vendor Tags

Tag	Source	Example
`Vendor`	constant	`SonicWall`
`Product`	constant	`Firewall`
`Event Class`	derived from `m=`	`Network`, `Security`, `Auth`, `Web`
`Event Type`	derived from `m=` + `fw_action`	`Access Control`, `Session`, `Policy Violation`, `Threat`
`Action`	`fw_action=`	`forward`, `drop`, `NA`
`SrcIP` / `DstIP`	`src=` / `dst=`	`192.168.1.10`
`DstPort`	translated by name	`https`, `domain`, `dynamic`
`SrcInt` / `DstInt`	interface portion of `src=` / `dst=`	`X0`, `X4`
`SrcMAC` / `DstMAC`	`srcMac=` / `dstMac=`	`00:00:5e:00:53:01`

Tag	Source	Example
Protocol	proto=	TCP, UDP, ICMP
User	usr= (skipped when "Unknown")	user1
Domain	dstname=	www.example.com
MitreId / MITRE Tactic	derived from m=	T1071 / Command and Control
Compliance – <framework>	derived from Event Type	1

Vendor-Specific Tags

Tag	Source	Example
SrcZone / DstZone	srcZone= / dstZone=	LAN, WAN, SSLVPN
SonicWall App Name	appName=	General HTTPS
SonicWall App Category	appcat=	BUSINESS-APPS Microsoft Office 365
SonicWall Category	Category=	Information Technology/Computers
SonicWall Rule	rule=	Default Access Rule

High-Cardinality Tags

The following tags can grow to thousands of unique values across a large deployment and are stored on disk:

- SrcIP, DstIP
- SrcMAC, DstMAC
- User
- Domain

Event Class / Type Mapping

m=	Description	Event Class	Event Type
98	Connection Opened	Network (Security if blocked)	- / Access Control
537	Connection Closed	Network (Security if blocked)	- / Access Control
97	Web site hit	Web	-
263	SSL VPN logout	Auth	Session
580	TCP SYN/FIN dropped	Security	Access Control
793	App Rules Alert	Security	Policy Violation
1080	SSL VPN remote login	Auth	Session
1153	SSL VPN session activity	Auth	Session
1154	App Control Detection Alert	Security	Policy Violation
1199	Geo-IP responder blocked	Security	Access Control
1430	IPv6 extension header	Network	-
14	IPS Detection Alert	Security	Threat
608	Possible scan/flood	Security	Threat

Log Examples

All examples use synthetic IPs (RFC 5737), MACs (RFC 7042), and a placeholder serial.

Connection Opened (m=98) - SonicOS 7 with custom Syslog ID

```
id=tz470 sn=0040104B0001 time="2026-01-15 10:34:10" fw=203.0.113.1 pri=6
c=262144 gcat=6 m=98 msg="Connection Opened"
src=192.168.1.10:59112:X0 srcZone=LAN natSrc=203.0.113.1:49147
dstMac=00:00:5e:00:53:01 dst=198.51.100.20:53:X4 dstZone=WAN
natDst=198.51.100.20:53 usr="Unknown" proto=udp/dns sent=82
```

```
rule="Default Access Rule" app=49169 appName='General DNS'
n=109246078 fw_action="forward" dpi=1
```

Connection Closed (m=537) - SonicOS 6 with default Syslog ID

```
id=firewall sn=0040104B0001 time="2026-01-15 10:34:10" fw=203.0.113.1
pri=6 c=1024 m=537 msg="Connection Closed"
srcMac=00:00:5e:00:53:02 src=192.168.1.55:57897:X0
dstMac=00:00:5e:00:53:01 dst=198.51.100.21:443:X4 usr="Unknown"
proto=tcp/https sent=14063 rcvd=8283 rule="Default Access Rule"
app=49177 appName='General HTTPS' n=112742081 fw_action="NA" dpi=1
```

Web Site Hit with Content Filter Category (m=97)

```
id=tz470 sn=0040104B0001 time="2026-01-15 10:34:10" fw=203.0.113.1 pri=6
c=1024 gcat=2 m=97 msg="Web site hit"
src=192.168.1.40:53525:X0 srcZone=LAN dst=198.51.100.40:80:X4
dstZone=WAN proto=tcp/http rule="Default Access Rule"
dstname=www.example.com Category="Information Technology/Computers"
n=13446700 fw_action="forward"
```

SSL VPN Login (m=1080)

```
id=tz470 sn=0040104B0001 time="2026-01-15 12:36:59" fw=203.0.113.1 pri=6
c=0 gcat=4 m=1080 msg="SSL VPN zone remote user login allowed"
src=198.51.100.60::X4 dst=203.0.113.1::X4 usr="user1" sess="GMS" dur=0
note="user1 via Client from 198.51.100.60" n=153 fw_action="NA"
```

Geo-IP Responder Block (m=1199)

```
id=tz470 sn=0040104B0001 time="2026-01-15 10:35:23" fw=203.0.113.1 pri=1
c=0 gcat=3 m=1199 src=192.168.1.77:50479:X0 srcZone=LAN
dst=198.51.100.70:443:X4 dstZone=WAN proto=tcp/https
rule="Block Inbound" app=49177 appName='General HTTPS'
msg="Responder from country blocked: Responder IP:198.51.100.70 Country Name:Reserved"
n=514722 fw_action="drop"
```

App Rules Alert (m=793)

```
id=tz470 sn=0040104B0001 time="2026-01-15 10:38:08" fw=203.0.113.1 pri=1
c=16 gcat=10 m=793 src=192.168.1.42:16327:X0 srcZone=LAN
dst=198.51.100.80:80:X4 dstZone=WAN proto=tcp/http
rule="Default Access Rule" app=49175 appName='General HTTP'
msg="App Rules Alert" af_polid=1 af_policy="Block TLD"
af_type="HTTP Client Request" af_service="HTTP" af_action="Reset/Drop"
n=46694 fw_action="NA"
```

Dashboards

A single dashboard, **SonicWall**, ships with the app and shows:

- Today's blocked / security / SSL VPN counts
- Events per second and event-class breakdown over time
- Source / destination zones and protocols
- Top source / destination IPs and ports
- Top web hosts, applications, content filter categories
- Top access rules, SSL VPN users, MITRE tactics
- Recent events search widget

Triggers

Trigger	Fires on
`SonicWall: Outbound Security Block`	LAN-sourced traffic blocked by security policy (geo-IP, ACL deny)
`SonicWall: App Rules Block`	Application firewall block (m=793, m=1154)
`SonicWall: SSL VPN Login`	SSL VPN authentication / session events
`SonicWall: Inbound Connection Blocked`	WAN-sourced traffic dropped/denied/rejected
`SonicWall: High Severity Event`	Syslog severity 0-3