LOGZILLA DOCUMENTATION

Juniper Srx

LogZilla App Store application: Juniper Srx

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

Overview

Juniper SRX is a line of network security devices that combines firewall, intrusion prevention, and unified threat management capabilities. The SRX series runs JunOS and provides session flow logging for network traffic analysis and security monitoring.

App Function

- Parse JunOS structured and unstructured syslog messages
- Extract network flow metadata (IPs, ports, zones, policies)
- Categorize events by message type and action
- Map security events to MITRE ATT&CK framework
- Provide dashboards for traffic analysis and security monitoring

Structured Messages

Recognizes JunOS message types via MSGID field in RFC 5424 structured data. Sets appropriate user tags for fields contained in each message type.

Unstructured Messages

Parses session-related events (`RT_FLOW_SESSION_CREATE`, `RT_FLOW_SESSION_CLOSE`, `RT_FLOW_SESSION_DENY`) from BSD-style syslog. Reformats messages into key/value pairs for readability.

Vendor Documentation

- System Logging Overview (https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/system-logging.html)

Device Configuration

Configure the SRX to send syslog messages to LogZilla:

Log into the SRX via CLI or J-Web

Configure a syslog host:

```
set system syslog host <logzilla-ip> any any
set system syslog host <logzilla-ip> port 514
```

For structured syslog (recommended):

```
set system syslog host <logzilla-ip> structured-data
```

Commit the configuration:

```
commit
```

Verification

Generate traffic or trigger a policy match, then verify events appear in LogZilla with `Vendor: Juniper` and `Product: SRX` tags.

Log Source Details

Item	Value
Vendor	Juniper Networks
Device Type	Routers, switches, and security devices running JunOS
Supported Software Version(s)	JunOS 11.x and newer (tested on SRX-series firewalls)
Collection Method	Syslog
Configurable Log Output?	Partially - JunOS supports both structured and unstructured syslog formats
Log Source Type	JunOS syslog
Exceptions	N/A

Incoming Log Format

Juniper JunOS devices generate syslog messages in two distinct formats:

Structured Format: Uses structured data elements with key-value pairs enclosed in brackets, following RFC 5424 structured data format.

Unstructured Format: Uses space-separated fields in a fixed order, primarily for session flow events.

Both formats are processed by the Juniper app to extract relevant security and network flow information.

Supported Log Types

Supported Structured Message Types

The app recognizes the following JunOS message types (MSGID):

- `SECINTEL_SERVICE_MANAGEMENT`
- `AAMWD_NETWORK_CONNECT_FAILED`
- `APPTRACK_SESSION_CREATE`
- `APPTRACK_SESSION_CLOSE`
- `LIBJSNMP_NS_LOG_WARNING`
- `RTLOG_CONN_ERROR`
- `LICENSE_EXPIRED_KEY_DELETED`
- `UI_NETCONF_CMD`
- `UI_CHILD_START`
- `UI_CHILD_STATUS`
- `RT_FLOW_SESSION_CREATE`
- `RT_FLOW_SESSION_CLOSE`
- `RT_FLOW_SESSION_DENY`

Supported Unstructured Message Types

Session-related events (`RT_FLOW_SESSION_CREATE`, `RT_FLOW_SESSION_CLOSE`, `RT_FLOW_SESSION_DENY`) output as space-separated fields (see log examples below).

Parsed Metadata Fields

The following user tags are extracted from structured messages:

Tag Name	Example	Description
Event Class	network	Cross-vendor event classification
SrcIP	11.22.33.44	Source IP address
DstIP	55.66.77.88	Destination IP address
DstPort	HTTPS	Destination port with service name
Policy	PolicyEnforcer-Rule1-1	Security policy name
Reason	ICMP error	Session close or deny reason
Action	CLOSE	Session action type
Message Type	RT_FLOW_SESSION_CLOSE	JunOS message type identifier
Service	junos-http	JunOS service name
Protocol	TCP	Network protocol name
Source Zone	trust	Source security zone
Destination Zone	untrust	Destination security zone
User	admin	Username associated with session
MitreId	T1071	MITRE ATT&CK technique ID (DENY events)
MITRE Tactic	Command and Control	MITRE ATT&CK tactic

Unstructured Message Tags

Unstructured messages are reformatted into key/value pairs. The following user tags are extracted:

Tag Name	Example	Description
Event Class	network	Cross-vendor event classification
Message Type	RT_FLOW_SESSION_CLOSE	JunOS message type identifier

Tag Name	Example	Description
Action	CLOSE	Session action type
SrcIP	11.22.33.44	Source IP address
DstIP	55.66.77.88	Destination IP address
DstPort	dynamic	Destination port with service name
Policy	13101705	Security policy name
Protocol	TCP	Network protocol name
Source Zone	DMZ_One	Source security zone
Destination Zone	DMZ_Two	Destination security zone
Service	junos-telnet	JunOS service name (DENY events)
Reason	TCP SERVER RST	Session close reason

Log Examples

Structured Message - Session Close

```
2018-07-13T09:49:21.734Z TESTER RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.49 reason="ICMP error" source-address="11.22.33.44"
source-port="1298" destination-address="55.66.77.88"
destination-port="53" service-name="None"
nat-source-address="11.22.33.44" nat-source-port="8325"
nat-destination-address="55.66.77.88" nat-destination-port="53"
src-nat-rule-type="source rule" src-nat-rule-name="source-nat-rule"
dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="6"
policy-name="PolicyEnforcer-Rule1-1" source-zone-name="trust"
destination-zone-name="untrust" session-id-32="20267666"
packets-from-client="1" bytes-from-client="64" packets-from-server="0"
bytes-from-server="0" elapsed-time="1" application="INCONCLUSIVE"
nested-application="INCONCLUSIVE" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/1.0" encrypted="UNKNOWN"]
```

Structured Message - Network Connect Failed

```
2024-06-01T12:34:56.789Z TESTER AAMWD - AAMWD_NETWORK_CONNECT_FAILED
[junos@2636.1.1.1.2.136 severity="2" proxy-port="None" proxy-address="None"
ip-address="11.22.33.44" hostname="host1.us-west-1.company.net"
error-message="Unauthorized" destination-port="443"] <2> Access host
srxapi.eu-west-1.sky.junipersecurity.net on ip 52.210.70.159 port 443 proxy
None port None Unauthorized.
```

Unstructured Message - Session Close

```
RT_FLOW_SESSION_CLOSE: session closed TCP SERVER
RST: 11.22.33.44/50488->55.66.77.88/48001 None
11.22.33.44/50488->55.66.77.88/48001 N/A N/A N/A N/A 6
13101705 DMZ_One DMZ_Two 120095417 16(8769) 15(1262) 2
UNKNOWN UNKNOWN N/A(N/A) reth8.1122 UNKNOWN
```

Unstructured Message - Session Denied

```
RT_FLOW_SESSION_DENY: session denied
11.22.33.44/36619->55.66.77.88/23 junos-telnet 6(0)
default-deny-log untrust DMZ_TESTONE UNKNOWN UNKNOWN N/A(N/A)
reth8.88 UNKNOWN policy deny
```

MITRE ATT&CK Mapping

Session deny events are mapped to MITRE ATT&CK techniques:

Event Type	MITRE ID	Tactic	Description
RT_FLOW_SESSION_DENY	T1071	Command and Control	Blocked network traffic

Dashboards

One dashboard is included:

- **Juniper SRX: Firewall Overview** - Security events, MITRE tactics, session counts, top sources/destinations, policies, and denied sessions

Triggers

Trigger	Description
`Juniper SRX: MITRE ATT&CK Threat Detected`	Catch-all for blocked traffic
`Juniper SRX: Session Denied`	Firewall blocked traffic
`Juniper SRX: User Authentication`	User authentication events