LOGZILLA DOCUMENTATION

Linux iptables

Adds rules, dashboards, and triggers for the Linux iptables firewall

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

Overview

Linux iptables is the standard firewall functionality built into Linux systems. It provides packet filter rules for the Linux kernel firewall. The filters are organized in different tables containing chains of rules for network traffic packet handling.

App Function

The Linux IPTables app provides security-focused analysis of firewall logs:

- Parse iptables/netfilter log messages in `key=value` format
- Extract network metadata tags for filtering and analysis
- Map blocked traffic to MITRE ATT&CK techniques for threat classification
- Exclude internal-to-internal traffic from MITRE tagging to reduce alert fatigue
- Assign Criticality levels based on source context (High for external, Medium for internal)
- Categorize all firewall events as `security` class
- Provide Security Dashboard for SOC analysts
- Alert on MITRE-mapped threats and high-value port access attempts

Vendor Documentation

- Netfilter Project (https://www.netfilter.org/) - Official iptables/nftables project
- iptables Manual (https://linux.die.net/man/8/iptables) - Command reference
- MITRE ATT&CK (https://attack.mitre.org/) - Threat technique framework
- MITRE T1021 Remote Services (https://attack.mitre.org/techniques/T1021/)
- MITRE T1190 Exploit Public-Facing Application (https://attack.mitre.org/techniques/T1190/)

Device Configuration

Configure Linux iptables to send firewall logs to syslog:

Enable logging for dropped packets in iptables rules:

```
iptables -A INPUT -j LOG --log-prefix "[IPTables-Dropped] " --log-level 4
iptables -A FORWARD -j LOG --log-prefix "[IPTables-Dropped] " --log-level 4
```

Forward kernel logs to LogZilla using one of the following methods. Replace `LOGZILLA_IP` with the LogZilla server IP address or DNS name.

Option A: syslog-ng

Add the following to `/etc/syslog-ng/syslog-ng.conf`:

```
destination d_logzilla { udp("LOGZILLA_IP" port(514)); };
filter f_kern { facility(kern); };
log { source(s_sys); filter(f_kern); destination(d_logzilla); };
```

Restart syslog-ng: `systemctl restart syslog-ng`

Option B: rsyslog

Create a configuration file to forward kernel facility logs:

```
cat > /etc/rsyslog.d/50-logzilla.conf << 'EOF'
# Forward iptables/kernel logs to LogZilla
kern.* @LOGZILLA_IP:514
EOF
systemctl restart rsyslog
```

Verification

Generate test traffic by attempting to connect to a blocked port, then verify events appear in LogZilla with `program: iptables`.

Incoming Log Format

Iptables logs use space-separated `key=value` format:

```
IN=eth0 OUT= MAC=aa:bb:cc:dd:ee:ff SRC=192.168.1.100 DST=10.0.0.1
LEN=40 PROTO=TCP SPT=12345 DPT=443
```

Parsed Metadata Fields

Tag	Example	Description
Vendor	Linux	Vendor name for cross-vendor filtering
Product	iptables	Product name for cross-vendor filtering
Event Class	security	Cross-vendor event classification
Event Type	access_denied	Specific event type (access_denied for blocked traffic)
SrcInt	eth0	Source/input interface
DstInt	eth1	Destination/output interface
MAC	4a:2a:b8:8e:09:87	Interface MAC address
SrcIP	185.153.196.126	Source IP address
DstIP	134.122.74.164	Destination IP address
Protocol	TCP	Network protocol
DstPort	https	Destination port (service name)
SrcIP to DstIP	192.168.1.100->8.8.8.8	Source to destination flow
SrcIP to Port	192.168.1.100->https	Source IP to port flow
MitreId	T1021	MITRE ATT&CK technique ID
MITRE Tactic	Lateral Movement	MITRE ATT&CK tactic category
IPTables Threat	SSH Access Attempt	Detected threat type
Criticality	High	Threat severity (High=external source, Medium=internal source)

Log Examples

Packet Blocked by Firewall

```
[IPTables-Dropped] IN=eth0 OUT= MAC=4a:2a:b8:8e:09:87:fe:00:00:00:01:01:08:00
SRC=11.22.33.44 DST=55.66.77.88 LEN=40 TOS=0x00 PREC=0x00 TTL=246 ID=57949
PROTO=TCP SPT=50369 DPT=110 WINDOW=1024 RES=0x00 SYN URGP=0
```

UDP Scan Attempt

```
IN=ens18 OUT= MAC=4a:51:b8:89:03:43:f4:92:bf:72:e4:fe:08:00
SRC=98.180.5.104 DST=192.168.10.110 LEN=182 TOS=0x00 PREC=0x00 TTL=110
ID=23459 DF PROTO=UDP SPT=47818 DPT=34092 LEN=162
```

Triggers

Triggers are aligned with MITRE ATT&CK techniques for threat classification.

MITRE ATT&CK Catch-All

Trigger	Description
`IPTables: MITRE ATT&CK Blocked Access Attempt`	Any blocked traffic mapped to MITRE (excludes internal-to-internal)

Specific MITRE Techniques

Trigger	MITRE ID	Description
`IPTables: Remote Service Access (T1021)`	T1021	SSH, RDP, VNC, Telnet attempts
`IPTables: Database/Application Access (T1190)`	T1190	MySQL, PostgreSQL, MongoDB, Redis
`IPTables: LDAP Reconnaissance (T1087)`	T1087	LDAP/LDAPS directory queries

Trigger	MITRE ID	Description
`IPTables: Kerberos Attack (T1558)`	T1558	Kerberos ticket attacks
`IPTables: Container API Access (T1609)`	T1609	Docker, Kubernetes API access
`IPTables: TOR/Proxy Traffic (T1090)`	T1090	TOR anonymization traffic
`IPTables: Crypto Mining (T1496)`	T1496	Bitcoin, Ethereum mining traffic

Port-Based Triggers

Trigger	Description
`IPTables: SSH Access Attempt`	Blocked SSH connection attempts