VOIP AND SIP FIREWALL

Rosa SIP Firewall

A security layer in front of your PBX that detects and blocks SIP attacks

Rosa SIP Firewall sits between the IP PBX and the internet and carries all SIP traffic through itself. It detects SIP scanning tools, password guessing and username enumeration, floods and malformed messages, and bans attackers automatically and progressively based on a threat score. Toll fraud attempts towards risky numbers, country-based restriction, threat intelligence feeds, optional Suricata IDS, an L3/L4 firewall and SIEM integration are managed from a Turkish web interface.

HIGHLIGHTS

01

SIP-specific attack detection

Scanning tools such as SIPVicious, REGISTER and INVITE password guessing, extension enumeration, floods, malformed messages and SQL injection in SIP headers are checked on every request.

02

Automatic, progressive banning

A decaying threat score is kept for every source IP; once a threshold is crossed the IP is banned, and repeat offenders get longer bans. Trunks, offices and allow-listed addresses are never banned.

03

Toll fraud and geo restriction

Sources that dial premium or IRSF number prefixes, or place many international calls in a short time, are banned; SIP traffic is restricted by source country with an allow or deny list.

04

Single entry point in front of the PBX

Phones and carrier trunks reach the PBX only through the firewall; per-domain PBX routing, health checks and failover to a backup PBX, NAT traversal and media relay come built in.

WHO IT'S FOR

- Organisations that must expose their PBX to the internet for remote staff and branch phones
- IT teams that want to protect their PBX from SIP scanning and password guessing
- Businesses that want to reduce the risk of costly international calls through compromised extensions
- Service providers hosting several customer PBXs under different SIP domains
- Security teams that want VoIP security events in their existing SIEM

Features 67 FEATURES

The list below shows, module by module, what the current version of the product does.

SIP attack detection 10

- Scanning tools such as SIPVicious, sipcli and sipsak recognised by User-Agent and banned on the first message
- REGISTER and INVITE password guessing (brute force) detection
- Detection of attempts with many different usernames from one IP
- Extension and number enumeration detected from 404/604 replies of the PBX
- Flood protection with a per-IP request density limit
- Rejection of malformed, non-RFC-compliant and over-8 KB messages
- Blocking of SQL injection patterns in SIP headers
- Rejection of requests for domains that are not served
- Detection of in-dialog injection attempts such as out-of-dialog BYE/CANCEL
- Rejection of disallowed SIP methods

Threat scoring and banning 7

- Decaying threat score per source IP; automatic ban at the threshold
- Longer bans for repeat offenders (5 minutes, 1 hour, 24 hours)
- Permanent ban at a very high threat score
- Bans kept across restarts and resynchronised regularly
- Allow-listed, trunk and office sources are never banned
- Manual blocking or allowing of an IP address, timed or permanent
- IP detail page: threat score, matching feeds, recent events, one-click block/unblock

Toll fraud and geo restriction 6

- Risky destination prefix table: premium, IRSF, high risk, international
- Sample risky prefixes included; add, edit and disable
- Immediate ban of a source that dials a premium or IRSF number
- Ban of a source placing international calls above a per-minute threshold
- Allow or deny list by source country
- Events enriched with country and ASN

Threat intelligence 5

- Spamhaus DROP/EDROP, FireHOL Level 1, blocklist.de and VoIPBL feeds included
- Feed addresses dropped at the network layer (nftables)
- Management networks, private IP ranges and the allow list are protected from feeds
- Automatic refresh every 6 hours, manual refresh and per-feed on/off
- IP reputation score learned from attack history (country, ASN, offence count)

Intrusion detection (IDS) 5

- Optional Suricata traffic monitoring on the WAN interface
- ET Open rules and Rosa VoIP signatures
- Custom rules with live reload
- Automatic ban of the source on alerts at a chosen severity
- IDS alert list and contribution to the reputation score

SIP proxy and PBX protection 9

- Phones and carrier trunks reach the PBX only through the firewall
- Multiple SIP domains and aliases, each domain routed to its own PBX
- Multiple PBXs per domain with priority order and failover to the next PBX
- PBX health checks with OPTIONS every 10 seconds
- Trusted source definitions and a separate PBX port for carrier trunks
- NAT traversal for remote phones; the PBX remains the registrar
- Media relay with rtpengine; in-kernel forwarding where supported
- PBX identity hiding: Server/User-Agent masked, internal headers not accepted from outside
- SIP keeps flowing with the last known security state even if the security service or database stops

Network and firewall 8

- Interface roles: WAN, LAN, DMZ, management
- VLAN (802.1Q) and PPPoE; static or DHCP addressing, static routes and DNS
- Live interface status: link, speed, MAC address, traffic
- Ordered L3/L4 rules: accept, drop, reject; interface, protocol, port and logging
- Object groups: host, network, port, port range
- NAT: port forwarding (DNAT), SNAT, masquerade
- Confirm-or-rollback for network and rule changes; unconfirmed changes revert automatically
- SSH and management interface reachable only from defined management networks

Monitoring, anomalies and reporting 5

- Dashboard: attacks blocked in the last 24 hours, active bans, event count and attack type breakdown
- Security events filtered by attack type and source IP
- Event volume anomalies against an hour-of-week baseline, overall and per domain
- Acknowledge anomalies, mark them resolved or false positive
- CSV export of events, IDS alerts and the block list (24 hours, 7 days, 30 days)

Notifications and SIEM integration 4

- Forwarding to SIEM as syslog (RFC 5424) or CEF over UDP/TCP
- Email (SMTP), Telegram and webhook notification channels
- Minimum severity per target and channel
- Test message and channel status indicator

Administration and deployment 8

- Turkish web interface over HTTPS
- Administrator, operator and viewer roles
- Password storage with argon2id; 15-minute account lockout after 5 failed logins; session timeout
- Optional Let's Encrypt certificate
- Installer script for Debian 12/13
- Automatic database backup on update; reverts to the previous version if unhealthy
- Configuration and database backup/restore script
- Administrator password reset command

Technical specifications

Placement	SIP proxy between the PBX and the internet; one-arm (single interface) or two-arm (separate PBX interface) deployment; public IP setting behind 1:1 NAT
SIP transport	SIP over UDP and TCP (default 5060)
PBX compatibility	Standard SIP PBXs; FreeSWITCH, Asterisk, Yeastar, Cisco CUCM and generic types selectable in the interface. The PBX remains the registrar; trunk traffic can be sent to a separate PBX port
Media	RTP relayed through rtpengine on every call; default port range 20000–39999; in-kernel forwarding where the kernel supports it
Threat intelligence	Spamhaus DROP/EDROP, FireHOL Level 1, blocklist.de, VoIPBL; refreshed every 6 hours; DB-IP Lite country and ASN database
Intrusion detection	Optional Suricata (monitoring mode, WAN interface); ET Open rules, Rosa VoIP signatures and custom rules; automatic ban at a chosen severity
Integrations	SIEM: syslog RFC 5424 or CEF over UDP/TCP; notifications: email (SMTP), Telegram, webhook; CSV reports
Authentication and authorisation	Username/password (argon2id), 15-minute lockout after 5 failed logins, session timeout; administrator, operator and viewer roles
Requirements	Debian 12 or 13 (amd64/arm64); physical, virtual or cloud server; minimum 2 vCPU / 4 GB RAM, 4 vCPU / 8 GB recommended for production
Interface	Turkish web interface over HTTPS; access only from defined management networks; optional Let's Encrypt certificate

DEPLOYMENT Installed on a Debian 12 or 13 server (physical, virtual machine or cloud server) with an installer script; the SIP proxy, media relay, security engine and web interface run on the same server. Phones and carrier trunks are pointed at the firewall, and the PBX is restricted to accept SIP and RTP only from the firewall. The update script backs up the database first and reverts to the previous version if the new one does not come up healthy.

Book a demo or request a quote

Contact us to see the product in your own environment and discuss scope and pricing.

PHONE +90 850 441 3 441
+90 324 350 03 50
EMAIL bilgi@martateknoloji.com.tr
WEB martateknoloji.com.tr
ADDRESS Mersin Teknopark 35C/B5, Çiftlikköy, 33343 Yenişehir / Mersin, Türkiye
Mersin · İzmir · London

© 2026 Marta Teknoloji A.Ş. — Information in this brochure is for guidance; feature scope may vary by version and deployment.