

The edge of your voice network.

SipPulse SBC sits between your voice network and everything that connects to it: carriers, customer PBXs, Microsoft Teams, Zoom, WhatsApp and the browser. It does for voice what a firewall does for data: it protects, adapts and shows every call.

Proxy + B2BUA

every SIP packet regenerated

Approved SIP-I

ITU-T-97 and ISUP-BR

STIR/SHAKEN

authentication built in

Teams · Zoom · WhatsApp

and WebRTC on the same edge

THE CHALLENGE

Every connected network is an open door

• Many doors

Carriers, customer PBXs, unified communications platforms and browsers all reach your network through the same place.

• Attacks and abuse

Extension scanning, password guessing, call bursts above the contracted rate and equipment that does not follow the SIP standard.

• Regulation and quality

Authenticated calls, short-call control required by a Brazilian provisional measure and quality the customer notices.

THE SOLUTION

How SipPulse SBC solves it

An edge that regenerates SIP

In B2BUA mode every SIP packet is regenerated: what arrives off-standard leaves right, and the internal topology stays hidden. Proxy mode serves high performance.

Protection in layers

TFPS drops, in the kernel and before the Proxy, IPs that scan or brute-force SIP. Each endpoint has its own calls-per-second limit (the excess gets a 503), there is a blocklist, and the firewall applies rules in safe mode: if not confirmed within 120 s, the rule rolls itself back.

Interconnection on the same edge

SIP-I with carriers, Microsoft Teams, Zoom Phone, WhatsApp and WebRTC (WSS), STIR/SHAKEN built in, encrypted media (TLS, DTLS-SRTP) and codec transcoding.

Visibility of the operation

Analytics with ASR, NER, ACD, PDD and failure causes by route, endpoint and area code; an audio quality score (MOS) measured by AI; CDRs, packet capture (PCAP) and export to Homer (HEP).

DIFFERENTIATORS

Why SipPulse SBC

1 Built for Brazilian telephony

SIP-I approved with the leading carriers in Brazil, caller ID matched to the dialed area and short-call control, as the provisional measure requires.

3 Ready for AI agents

MCP server: an AI assistant queries and configures the SBC with the same permissions, safe mode and audit trail as the interface.

2 Many SBCs, one management

Gateway servers in the same interface and active/passive high availability: the standby server takes over in about 4 seconds.

4 Changes without surprises

Test route shows which route and which number a call would use, before it happens.

MODELS

An SBC for each operation

SBC-UNI

Contact center

Optimized for high volumes of simultaneous calls, random CLI and integration with CPA.

SBC-NNI

Fixed-line and wholesale carriers

SIP-I interconnection with carriers, ISUP approvals and transcoding.

SBC-NNI-CC

Contact center with interconnection

Combines UNI and NNI features for those who both serve customers and interconnect.

FEATURES

What comes with the SBC

Signaling and routing

- Proxy and B2BUA modes
- Topology hiding
- Routes by priority and regex
- Weighted load balancing or overflow
- SIP and number manipulation
- Test route
- Source-based routing

Caller ID and regulation

- Caller ID profiles with several lists
- Number from the dialed area
- Short calls per number and list
- Minimum duration (held BYE)
- CPA: call classification

Security

- TFPS: blocking in the kernel
- Firewall with safe mode
- CPS limit per endpoint
- Blocklist, with a voicemail rule
- STIR/SHAKEN
- TLS and DTLS-SRTP
- MFA and audit trail

Media

- Codec transcoding
- Call recording and SIPREC
- RTP forwarding in the kernel
- AI audio quality score (MOS)

Interconnection and UC

- SIP-I (ITU-T-97, ISUP-BR)
- Microsoft Teams
- Zoom Phone
- WhatsApp in the SBC itself
- WebRTC (WSS)
- Authentication via API

Operations and integrations

- Real-time dashboard
- Analytics by route, endpoint and area code
- CDR, PCAP and Homer (HEP)
- Zabbix and Prometheus
- Configuration backup
- REST API and MCP server

TECHNICAL

Specifications

Operating modes	Proxy (high performance) and B2BUA (SIP regeneration)
Protocols	SIP over UDP, TCP, TLS and WSS; WebRTC
Interconnection	SIP-I (ITU-T-97, ISUP-BR)
Security	STIR/SHAKEN, TLS, DTLS-SRTP, TFPS, firewall with safe mode, MFA
High availability	Active/passive (VRRP), replication between gateway servers, anycast (BGP)
Monitoring	Analytics, Zabbix, Prometheus, Homer (HEP)
Management	Web interface (HTTPS), REST API, MCP server
Operating systems	Rocky Linux 8, 9 and 10; Oracle Linux 9 and 10
Capacity	Sized with SipPulse engineering, according to the hardware and the features enabled
Licensing	On-premise, per concurrent channel; Cloud, monthly subscription with management included. Analytics and MCP are license modules.

More than 200 carriers trust SipPulse.

Watch the overview and the technical demo on the product page, or request your demo.

sippulse.com/en/products/sbc
info@sippulse.com

SipPulse SBC 8.5 · Datasheet v5 · October 2026