FRAFOS SBC

Strong security for VoIP networks and critical infrastructure

The long-term strategy at FRAFOS has always been to provide reliable, high-quality voice communications as one of the pillars of successful Air Traffic Management (ATM) as well as Public Safety, Public Transport, and other CRITIS environments.

With the FRAFOS session border controller (SBC) our customers deploy a reliable and secure session border controller that was designed to meet the needs of a wide range of deployment scenarios.

The FRAFOS SBC not only secures the signaling and media communication, offers call routing and signaling adaptation, but also builds the basis for the only EAL4+ BSI certified SBC in Germany. This makes the FRAFOS SBC the perfect tool for addressing the rapidly changing business and network requirements of private, governmental and Public Safety providers.

The FRAFOS SBC acts as a VoIP firewall that protects internal services from the outside world and hides the internal topology from possible attackers. Using header filtering, number screening, white- and blacklisting and protocol syntax checking, the FRAFOS SBC can filter-out malicious content before entering the customer's network protect against potential cyber-attacks, stop denial-of-service attacks (DoS), and prevent fraud attempts.

FRAFOS SBC at a Glance

- Advanced Denial of Service (DoS) and overload protection
- Fraud prevention
- SIP Protocol normalization
- High Availability
- SIPREC support
- MS-Teams Direct Routing
- Load balancing
- Central management
- Logging and CDR generation
- WebRTC
- SIPREC
- ED-137 compliance

Key features

High Availability and Reliability

To address the needs of our customers in the ATM services, Public Safety and CRITIS sectors, the FRAFOS SBC was designed with the highest reliability standards in mind. In order to ensure the continuity of active calls even under hardware or software failures, the FRAFOS SBC implements active-standby as well as active-active high availability concepts.

To accommodate for the failure of network or voice communication servers, the FRAFOS SBC monitors neighboring nodes, detects failures, and routes traffic only to available nodes.

Finally, the FRAFOS SBC increases the reliability of a communication system by load balancing incoming calls among a cluster of voice servers based on round-robin, weights, or availability.

Scalable Design

To accommodate the various needs and performance requirements of customers of all sizes and sectors, the FRAFOS SBC was developed to be deployed over different hardware and software platforms. It is implemented in the container technology to run on different cloud, virtualization, and native server operating system environments.

Flexible Routing Framework

The FRAFOS SBC offers flexible routing capabilities. Signaling traffic can be routed according to pre-defined static routing rules with optional SIP Redirect mode; integrated routing tables can be provisioned remotely using the REST API, or the routing decision can be fully controlled by triggering a query to a remote 3rd party server that implements the routing logic itself. All these mechanisms support load-balancing among multiple destinations and provide routing to a backup server when the initial destination fails or is not responding.
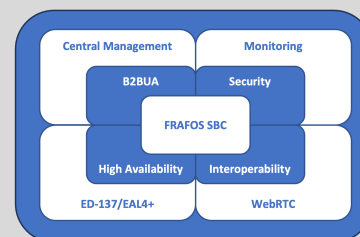
Central Management

Larger networks often deploy numerous SBCs to cover multiple branches, usage scenarios or load requirements. Therefore, a flexible and configurable management environment is a vital element in running a stable and reliable network. The FRAFOS Cluster Configuration Management (CCM) provides the administrator with an intuitive interface for:

- **Administration:** The CCM enables the administrator to define the configuration of the administered SBCs, define templates for configuring clusters of SBCs and conduct manual interactions such as halting or restarting an SBC.

- **Life-cycle Management:** Manage the life cycle of the configuration of a FRAFOS SBC. Define, load, and modify the configuration of separate SBCs.

- **Central management:** Manage multiple SBCs or clusters of SBCs from a central location.

- **Backup and restore:** Enable the versioning and easy backup and restore of the configuration of each SBC.

Assured Interoperability

SBCs are deployed as the intersection between different vendors and peering points. The FRAFOS SBC configuration framework ensures the interoperability on different layers:

- **SIP header manipulation:** The FRAFOS SBC can remove certain headers, add others, and manipulate the content of headers and message bodies.

- **Stateful message handling:** To support the differences between different specifications the FRAFOS SBC is capable of overcoming differences in the call flows and generating appropriate responses and requests.

- **Transport layer mediation:** SIP can be transported over UDP, TCP and TLS. Further, it can work over IPv4 and IPv6. The FRAFOS SBC can enable two elements using different transport protocols and encryption methods to communicate seamlessly with each other.

- **Application layer mediation:** Support DTMF interworking, and the interoperability between RTP and secure RTP (SRTP).

- **Media transcoding:** The SBC supports software-based transcoding of various audio codecs.

Customizable Policies

Different peering partners will have different requirements in terms of used transport protocols, media codecs, Service Level Agreements (SLAs), SIP signaling and session control. The SBC enables our customers to customize the peering behavior of the SBC in accordance with their own policies as well as those of the peering partners and use different policies per interface and partner.

Access Control and Fraud Prevention

The FRAFOS SBC controls which users and what messages can cross the borders of a VoIP infrastructure and use the offered VoIP services. This is achieved by several features:

- **Media access control:** The FRAFOS SBC allows media traffic from a subscriber only after the successful signaling of a call. Further, The FRAFOS SBC blocks traffic with unwanted codecs and limits the amount of traffic that can be sent by a subscriber.

- **Fraud prevention:** Operators often face the case that a user subscribes for a flat rate telephony residential service but then starts reselling telephony minutes. This kind of behavior causes substantial financial losses to the service provider and overloads the network. To suppress this fraud possibility, the SBC can limit the number of parallel calls generated by a user as well as the duration and frequency of calls.

Rule-based Configuration

To manipulate a header, decide on how to route or police an incoming or outgoing message, the FRAFOS SBC provides a rule-based configuration framework that uses rules designed as

If Condition then Action

Conditions can apply to matching any of the following:

- Source Realm, Call Agent, Source IP, port, SBC interface
- Any part of the SIP message itself
- SIP Method, RURI, From, To, headers
- Media type, codec
- Whether the caller is already registered

If a condition is met, then any of the following Actions can be executed:

- Change some part of the SIP message (RURI, From, To, headers, body content...)
- Activate or deactivate SIP Extensions
- Activate filtering, limiting, recording

- Activate media processing, NAT handling, DTMF interworking, SRTP, transcoding
- Drop the message or route to some destination

WebRTC Support

The FRAFOS SBC can act as a WebRTC gateway and connect web-clients to SIP telephony in a transparent manner. The FRAFOS WebRTC anchors signaling and media and translates between different standards for WebRTC and SIP, particularly security, codecs and signaling protocols.

The WebRTC standards group have left the specification of the signaling protocol to be used to the vendors. Thereby, it is not possible to implement a WebRTC Gateway that works with all vendors' WebRTC applications. The FRAFOS WebRTC Gateway was designed to support WebRTC applications that use SIP as the signaling protocol.

The FRAFOS WebRTC gateway is a software-based solution that requires an additional license and can be either deployed as part of the FRAFOS SBC or as a standalone solution.

Detailed System Monitoring

FRAFOS' unique Monitor solution enables the detailed monitoring of all deployed SBCs. The FRAFOS Monitor provides administrators with an aggregated view of user activity based on usage reporting data collected from the FRAFOS SBC. This highly interactive, near real-time view can be used for trend analysis of both short-term and long-term use patterns, troubleshooting, auditing server policies, and identifying user misconduct.

The FRAFOS Monitor collects data close-to-real-time and hence enables our customers to have an elaborate overview of the performance of their communication infrastructure and be alerted to failures.

Compliance with ATM standards

The FRAFOS SBC implements the ED-137 SIP standards enhancement and follows the EUROCONTROL SBC in ATM VoIP implementation guidelines.

These include:

- Compliance with true multi-level redundancy
- Interoperability between the SIP/RTP and the ED-137 standards and systems
- A full set of security functionality features
- Compatibility management
- Resiliency improvement
- Reporting, logging, and troubleshooting
- Performance requirements
- Testing, certification, and support

Microsoft-Teams Direct Routing

Microsoft Teams Direct Routing enables MS-Teams customers to connect to local PSTN or SIP trunk providers using a certified SBC.

The FRAFOS SBC is certified to support Direct Routing for MS-Teams enterprise clients as well as different scenarios of multi-tenancy (hosted service provider model). In both cases, FRAFOS SBCs can be deployed as on-premise applications or a virtualized instance

Deployment Experience

The FRAFOS SBC software platform has been in deployment since more than a decade by VoIP service providers, call centers, public safety organs and governmental institutions. The adherence of the FRAFOS SBC to the Emergency Call standards in Germany (1TR119 DTAG-Standard) has enabled the FRAFOS SBC to fulfill the needs of more than 50 emergency call handling institutions and police agencies. The software basis is used by call center and VoIP service providers requiring manner.

Finally, the software platform constitutes the core of the only EAL4$+$ BSI certified SBC in Germany which is used by various governmental institutions with the highest security requirements in Germany.

Technical specifications

Signaling Features

- SIP RFC compliant
- B2BUA
- Per source / destination configurable SIP header / message body manipulation
- Local registration information

Media Services

- WebRTC
- SW based transcoding (G711u/a, G726, GSM, iLBC, L16, G722, Speex; on request: G729a, G729a/b, AMR)
- DTMF interworking (in-band / RFC2833/4733 / SIP INFO)
- NAT/NAPT on media
- Audio codec relay
- Video codec relay
- RTP inactivity monitoring
- Codec filtering

Protocol support

- SIP
- RTP, RTCP
- UDP, TCP, TLS including TLS v1.3, and Mutual TLS
- Translation between transport protocols
- IPv4, IPv6, and IPv4/IPv6 Interworking
- SNMP, NTP, SSH
- DNS
- SRTP (SDES, DTLS), STUN, ICE

QoS Control

- Bandwidth limitation and management
- Call admission control per peering partner/trunk
- Bandwidth limitation and management

Security

- Signaling and media topology hiding
- Signaling and media encryption
- DoS protection
- Call rejection under DoS
- Call rate limitation
- Call admission control per peering partner/trunk

Advanced Applications

- WebRTC Gateway
- Audio Conferencing
- Announcement services
- SIPREC and RTSP-based recording

Management Capabilities

- Centralized GUI based configuration and monitoring
- SSH access
- SNMP v2/v3 status and logs
- Prometheus interface
- Local logging of alarms, events, and statistics
- LDAP access control

High Availability

- Active/Hot Standby redundancy model
- Load balancing and load sharing

Supported Platforms

- Software is provided as a Container
- COTS Server (appliance), virtualization, cloud

Call Routing

- Call blocking and filtering
- Embedded routing engine
- Least cost routing
- API-based Table based routing