ABC SBC: Secure Peering

FRAFOS GmbH

Introduction

While an increasing number of operators have already replaced their SS7 based telecommunication core network with a SIP based solution, the interconnection to neighboring partners is still often realized over an SS7 peering point. This means that a call that is carried over a VoIP network is translated to an SS7 call and then possibly back to VoIP again. The translation requires specialized components and resources, which increases the network operation costs and introduces unnecessary processing delay. To avoid these costs and delays operators have started introducing SIP based interconnection and peering points.

The ABC SBC enables operators to establish secure borders to their neighbors by offering topology hiding, denial of service protection and mediation in a scalable manner

Topology Hiding

As the result of a SIP session establishment the involved end parties will have exchanged the IP addresses of where to send and receive media traffic. This means that a user using VoIP for calling a PSTN number will know the IP address of the PSTN gateway that is responsible for bridging the VoIP service with PSTN. Further, during the session establishment all the involved proxies will include their addresses in the Via headers.

A malicious user could use this information to either attack an operator's proxy or even get access to the PSTN gateways directly. By having the ability to contact the PSTN gateways directly, an attacker might be able to misuse any security holes that might exist at the PSTN gateway. This would allow the attacker to initiate calls to the PSTN with the costs being incurred on the operator.

When deploying the ABC SBC as the interconnection element to other operators, the ABC SBC hides all information about the internal components of the operator before forwarding them to a neighbor. The ABC SBC replaces the addresses of internal

components with its own. Hence, headers such as contact, Via, Record-Route, Route and so on would include the ABC SBC's address only.

Depending on the level of trust established with a certain neighbor, the ABC SBC can be configured to also route the media traffic and hence hide the internal addressing information of the media handling components.

Denial of Service and Overload Protection

Like any other Internet-based service VoIP servers can be the target of denial of service attacks. Attacks can be disguised as legitimate VoIP traffic so distinguishing between a denial of service attack or a sudden surge in traffic due to some event is not always possible. Hence, VoIP operators need to incorporate mechanisms that monitor the load and the incoming traffic, identify the overloaded resources and the cause of the overload and react in a manner that will prevent a complete service interruption.

In order to keep the malicious traffic and overload away from the core servers, e.g. applications servers, proxies and PSTN gateways, the ABC SBC supports the following protection mechanisms:

- **Traffic limitation:** Service providers can limit the rate of incoming calls and registrations. Once these limits are exceeded, the ABC SBC starts rejecting messages arriving in excess of these limits. These limits can apply to single sources, e.g., accept no more than X REGISTER requests from source Y, or a range of senders or to all incoming traffic.
- **Content filtering:** An attacker could try to get access to some protected resources by launching an SQL injection attack or try to bring a server down by sending SIP messages with malformatted content. By analyzing the content of incoming SIP messages and rejecting messages that seem to include malicious content, the ABC SBCs can protect the core components of the network.

Lawful Interception

As the border control node, the ABC SBC will very likely be one of the few network elements in the operator's network, which can route both the signaling and media packets of the user. Hence, ABC SBC can be the ideal place for supporting regulatory features such as lawful interception.

The ABC SBC integrates media processing capabilities that can enable the service provider to record active sessions as well as route signaling and media information for certain calls to an appropriate location.

Access Control and Fraud Prevention

In order to accept calls only from trusted neighbors the ABC SBC provides white and black lists. These lists are used to indicate which traffic to accept and which to reject.

Further, the ABC SBC supports the use of TLS towards neighboring operators. Traffic that is received over untrusted links can then be discarded.

In terms of fraud prevention, the ABC SBC will monitors the sum of exchanged traffic between two peering partners. In case the service level agreement was violated, the ABC SBC will reject new calls and drop excess traffic.

Interoperability Mediation

With different standardization groups working on SIP and the different interpretation of developers to the same specifications, interoperability between SIP components of different manufacturers and for different network architectures is unfortunately not always guaranteed.

The ABC SBC offers a powerful GUI based mediation functionality that enables an operator to adapt incoming and outgoing traffic. Using the ABC SBC mediation GUI, a service provider can configure the following actions:

- Stateless SIP header manipulation: The ABC SBC can be configured to remove certain headers and add others.

- Statefull message handling: To support the differences between the IMS and IETF specifications the ABC SBC is capable of overcoming differences in the call flows and generating appropriate responses and requests.
- Message blocking: The ABC SBC drops/rejects requests and messages not supported by an operator.
- Header manipulation: The ABC SBC can be configured to change the content of a certain header.
- Transport mediation: SIP can be transported over UDP, TCP and SCTP. Further, it can work over IPv4 and IPv6. The ABC SBC can enable two elements using different transport protocols to communicate seamlessly with each other.
- Media transcoding: The ABC SBC supports software based transcoding of media.

Capacity

The ABC SBC supports up to 7000 simultaneous calls running with G.711 codec on the standard hardware offered by FRAFOS. To scale an interconnection point more nodes with each node getting its own IP address can be added. In case an entire interconnection point is to be reached by a single address then FRAFOS also offers a SIP-load balancing solution that enables the operator to cluster a number of ABC SBCs behind a single entry point.

Technical Specifications

Supported Platforms Linux	**High Availability** Active/Hot Standby redundancy model
WebRTC Features Javascript SIP over WebSocket NAT traversal using ICE, TURN, STUN JsSIP support	**QoS Control** Bandwidth limitation and management Call admission control per peering partner/trunk
Media Services Routing audio codec including G.711 and OPUS. Routing of video codec including VP8 Dynamic jitter control NAT/NAPT on media RTP inactivity monitoring Codec filtering	**Call Routing** Call blocking and filtering Embedded routing engine Load balancing Peer monitoring and availability detection Alternative routing on failure Table based routing for LCA
Media Applications Call recording Announcement services Software based transcoding (G711u/a, G726, OPUS, iLBC, L16, G722, Speex; on request: G729a, G729a/b, AMR)	**SIP** Registration pass-through Registration caching and offload SIP header manipulation SIP Back2Back UA
Management Capabilities GUI based configuration and monitoring Secure embedded web-based GUI SSH access SNMP V2 status and logs Local logging of alarms, events and statistics REST and XML RPC based open interfaces	**Protocol Support** UDP, TCP WebSocket Translation between transport protocols Per source/destination transport layer mediation SNMP, NTP, SSHDNS RTP, RTCP, SRTP TLS, DTLS, SDES
Virtualization	**Hardware**

Amazon cloud Virtualization software OVM, KVM ..	Hardware independent

About FRAFOS

FRAFOS GmbH is a manufacturer of VoIP solutions with offices in Berlin and Prague. FRAFOS was incorporated as privately held company in May 2010, in Berlin, Germany.

The history of FRAFOS team and technology goes back to the late nineties. As researchers at the prestigious German public R&D institute Fraunhofer FOKUS, the FRAFOS founders were the among the first to work the SIP and RTP standards and to develop open source solutions that paved the way for the VoIP revolution.

FRAFOS offers SIP session management and security solutions of the latest generation that come either as a standalone solution or as a cloud ready implementation. The flagship product of FRAFOS, the ABC SBC, offers open interfaces and built in multimedia applications such as recording and announcements. The ABC SBC enables the service providers and enterprises to simplify their service infrastructure and prepares them for future challenges.