SC.SS7 Firewall

Empowering standard switching equipment

Vulnerability in the SS7 protocol stack could lead to disclosure of subscriber's personal data and key communication services malfunctions. Since changes in the existing MNO's infrastructure are a very complex and labor-intensive process, and protocol revision is not envisaged in the nearest future, SS7 Firewall is used to protect the network.

The **SC.SS7 Firewall** platform expands capabilities of standard switching equipment and prevents intervention into mobile communication network operation. Due to various rules for SS7 traffic analysis and filtration, this platform ensures protection from security threats from outside (from other networks). Unwanted or fraud traffic is detected automatically. About threats on a network it is reported in real time.

SC.SS7 Firewall collects detailed statistics about system loading and the structure of analyzed data.

Besides protection of MNO's equipment and subscribers, platform performance capabilities allow to facilitate balancing and traffic transfer between mobile network components, as well as significantly speed up new services deployment.

It is possible to install the platform only with SMS traffic control functions. Such version is called **SC.SMS Firewall.**

Key features

- Flexible logic of MAP, CAP queries analysis
- External ISUP traffic control (information collection, call modification and blocking with indication of any possible dropping causes)
- Fulfilment of active network queries to other blocks of the MNO's signaling network. Typically, these requests are sent towards HLR to identify MSC/VLR that provides the service to the subscriber and the current subscriber state
- Identification and blocking of clone SIM cards in roaming
- Collection of detailed statistics about SS7 traffic:
  - On ISUP calls
  - On SMS traffic
  - On CAP traffic
- Implementation of some HLR functions:
  - Protection against a SIM card activity monitoring by other operators
  - SRI queries processing
- Easy-to-use interfaces for SS7 traffic processing, which allow to individually solve MNO's needs in analysis, monitoring and modification of SS7 traffic
- Constant recording of transit SS7 traffic for its further analysis
- Simultaneous work with many STPs (Signal Transfer Point)
- Capability to connect simultaneously 2G/3G networks and IMT-MC networks (CDMA2000)
- Flexible routing conditions for SS7 traffic (for example, to organize simultaneous operation of several SMSCs and smooth traffic transfer between them). When choosing a route, it could be necessary to consider the following parameters, such as Global Title, Point Code, SSN, MAP operation code, sender and receiver numbers in the message body
- (Optional) Use of an internal programming language to customize the logic:

- Message routing
- Modification, deletion or addition of message parameters
- Message billing

- Functions for the **SC.SMS Firewall** installation variant:
  - External SMS traffic control (information collection, identifying spam mailing sessions and blocking them on the fly)
  - Identifying and blocking of malicious SMS traffic of various types (SMS-Flooding, SMS-Spoofing, SMS-Smishing)
  - Modification of the SMS TP-Reply-Path flag on the fly. Flag is issued by a telephone, which sends SMS and tells that is it necessary to answer for received SMS through SMSC of the message sender
  - Other processing as per MNO's wish

Benefits & advantages

- Flexible configuration of filtering parameters. Capability to process only SMS traffic (including outcoming)
- Transparent performance and ease of implementation leaving the internal structure of the operator mostly unchanged
- System fault tolerance and high performance
- Capability to work both in 2G/3G networks, and in CDMA
- The **SC.SS7 Firewall** platform ensures easy integration of several SMS centers and transfer to a new solution
- The platform can operate in a virtual environment

Integration scheme

The solution presupposes two techniques for integration into the MNO’s network:

1. Routing of SS7 traffic at the MTP3 (PC) levels
2. Integration into the communications channel (SIGTRAN, G.703 E1 SL, G.703 E1 HSL)