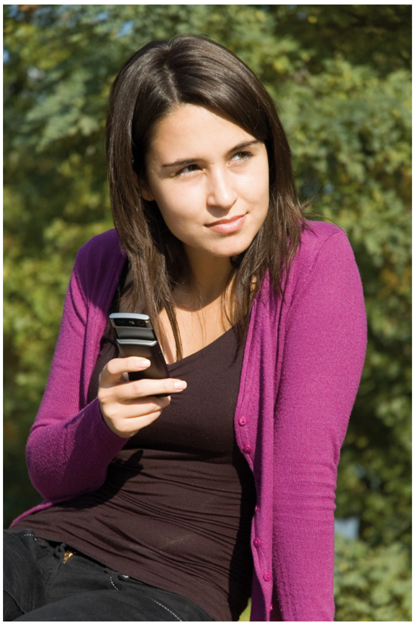
SGA-MAPFW
A powerful MAP screening and filtering tool

Features & Capabilities



AITIA's SGA-MAPFW is a MAP Firewall solution capable of screening, filtering, forwarding, or answering MAP messages within the operator's core network. With our solution you can filter out unwanted MAP MSUs reaching your equipment, thus protecting both your subscribers and your network at the same time.

Complex filtering rules can be set up based on the SCCP and MAP parameters combined with the origin of the particular message. Screening rules can include transparent forwarding, logging to PCAP or SGA format, emitting SNMP traps, creating CDRs, or rejecting undesired MAP MSUs with TCAP END or ABORT messages with configurable result codes.

Routing is accompanied with optional SCCP/ClgPA/TT replacement in the forward and backward directions.

The telecom interface for AITIA's MAP Firewall can be either SS7 or SIGTRAN, based on the actual network requirements.

Configuration

To achieve the expected results, messages with MAP contents should flow through the SGA-MAPFW software. Proper network routing can simply be carried out by SCCP/TT replacement.

Definition files (for screening rules, actions, etc.) and output files (logs, CDRs) are in text based human-readable format.

Hardware

The minimal hardware configuration consists of an industrial grade PC with an SGA interface card for the SS7 version or with standard Ethernet interfaces for the SIGTRAN version (virtualisation is also applicable). The operating software is well optimized, hence little computational capacity is required, which allows the operators to run various other SGA applications on the same machine. Application availability can be increased by system duplication, which is highly cost-effective due to the minimal hardware requirements.

SGA-MAPFW
A powerful MAP screening and filtering tool

Technical details

Features:

- Thousands of rules can be set with appropriate relations
- Practically all MAP versions are supported
- Several vendor specific extensions are supported
- Rules can be assigned to 10 different profiles based on the required actions
- SNMP traps are generated for alarming
- IMSI and operator name prefix lists are available for name-based filtering
- "SGA Message Viewer", our sophisticated telecom protocol analyzer, is also included in the package

Simple filtering criteria include:

- SCCP / Calling Party Address
  - by GT number or prefix
  - by country name
  - by operator's name
- MAP / Operation Code
- MAP / HLR, SMSC, etc.
  - by GT number or prefix
  - by country name
  - by operator's name
- IMSI
  - by number or prefix
  - by country name
  - by operator's name

Possible actions for the screened messages:

- Forward as is
- Log into message file (PCAP / SGA)
- Create CDR
- Send SNMP trap
- Answer with TCAP/END message (configurable error cause value)
- Answer with TCAP/ABORT message
- Any combinations of these above

The minimum requirements for hardware virtualisation include 2GB RAM, 20GB free disk space, and 2GHz CPU. The SIGTRAN version requires two Ethernet interfaces for multihomed SCTP association to provide full georedundancy.

AITIA Telecommunications References

T-Mobile · telenor · vodafone

invitel · NOKIA · ERICSSON