Overview

Highlight

- ITU International Standard: ISUP, MAP, CAMEL, SIP…
- Support HTTP/API.
- Callflow Definition.
- High Avaibility 1+1
- Routing Table.
- Whitelist/Blacklist
- Call Filtering Criteria with User Define.
- Whitelist/Blacklist.
- Number Manipulation
- ISUP/TDM and SIP processing.
- Support SIP tag.
- Variant Report on demand.

IA-SPOOF Solution

(Intelligent Anti-Spoofing SECaaS)

The IA-SPOOF solution has been successfully tested in a number of Vietnamese carriers to meet the requirements of the Ministry of Information and Communications on preventing forgery of caller phone numbers, causing confusion for customers using the IA-SPOOF solution. using telecommunications services of Vietnamese carriers.

The solution is ready to integrate with telecommunications networks, meeting standard interfaces and protocols of ITU-T and IETF such as ITU standards sets Q.764 – Q.767, SCCP, TCAP, ISUP, MAP, SIP RFC 3261.

Capable of distinguishing phone numbers/subscribers using MNP services and classifying in-network or out-of-network subscribers to provide appropriate handling rules for each type of subscribers.

Provide a connection interface and be able to customize with IT business systems according to customer requirements.

The system provides connectivity with different components in the telecommunications core network such as: SS7 STP signaling system, HLR system, MNP system, NGN switchboard system, national IP voice gateway system VoIP SBC economy, GMSC/MSS gateway system, centralized monitoring system, centralized reporting system, centralized CDR charge storage system...

The solution can be deployed on many types of server hardware of different brands such as HP, Dell, IBM ... In addition, it supports deployment on existing virtualization platforms of customers such as VMware, KVM ...

Intuitive graphical management interface makes it easy to operate and exploit with system administrators.

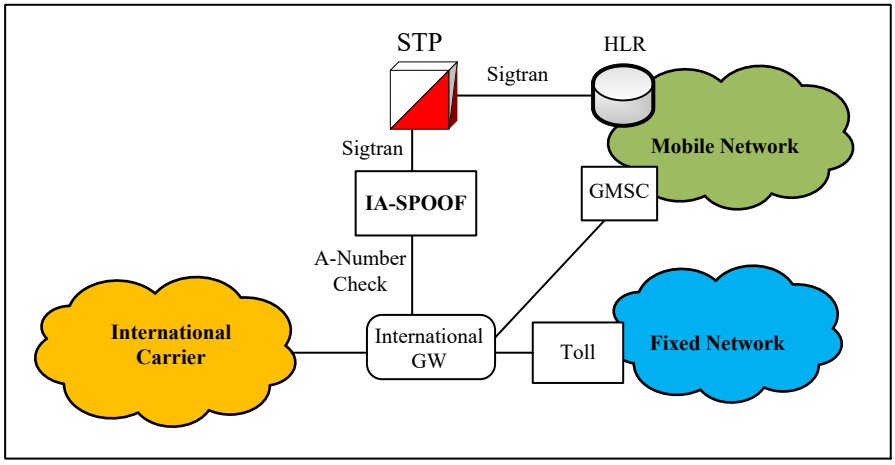
Ready to integrate with data sources from other systems to enhance analysis, statistics and reporting capabilities, providing intuitive tools for administrators to operate and monitor the system.

Overview

The IA-SPOOF solution to prevent incoming international calls from spoofing the caller's phone number (the source of the call) is deployed to connect to the international gateway - the main source of incoming calls. fake call. The system monitors, detects and prevents/cancels fake calls:

- Calls from international to the telecommunications network receiving calls with caller numbers belonging to the enterprise's telecommunications network.
- International calls to telecommunications networks receiving calls with caller numbers belonging to other enterprises' telecommunications networks.

The system is located at the international connection port, which is the point of receiving call traffic in international directions before entering the domestic network. The main function of the system is to monitor and block/cancel calls before connecting to the mobile network.



he system is designed to independently handle signal processing and voice traffic, allowing customization when integrating the network to perform either or both functions.

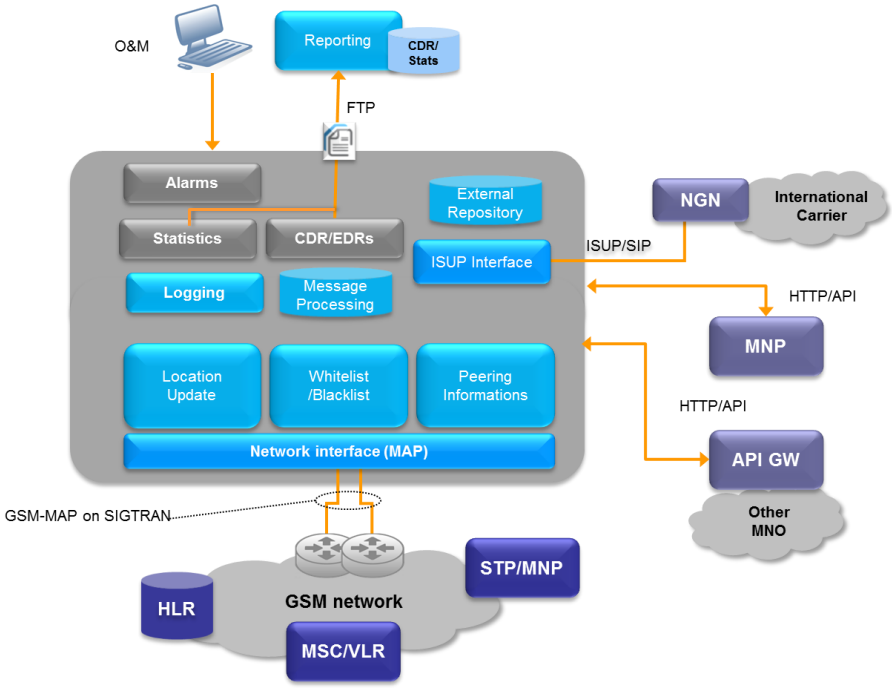
The system fully supports signaling protocols such as SS7 over Sigtran, SIP over IP network, receiving and processing messages over TDM or VoIP connections.

The system sets up blocking, filtering, and forwarding mechanisms that do not change the parameters in the signaling message (SIP or ISUP).

Overview

IA-SPOOF system connected to components:

- Connect to STP to connect to SS7 signaling network.
- Connect to SBC or NGN to receive signaling messages.
- Connect to GW API to get query information from other databases.
- Connect with MNP to classify subscribers on the network or outside the network.
- Connecting to a centralized storage system.

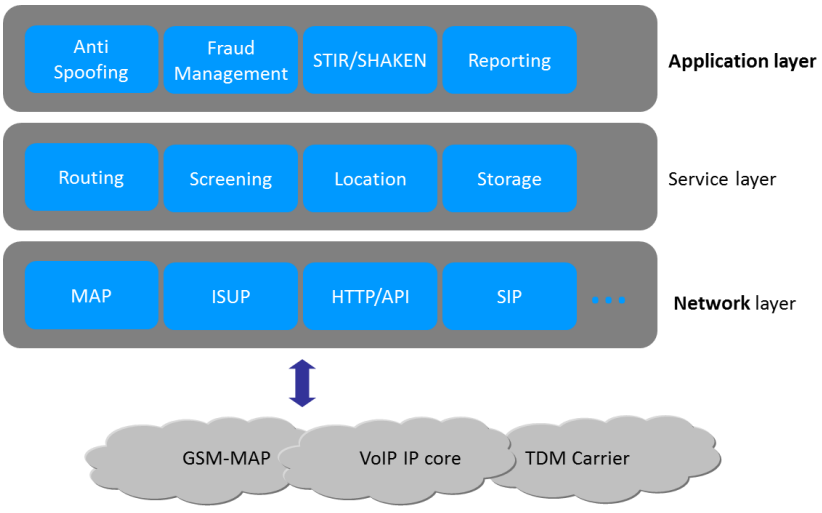


- Indirect connection with NGN and GMSC to receive and process intercept/destroy signaling messages.

Architecture

IA-SPOOF software is designed with modules that are easy to upgrade, modify or replace each Module.

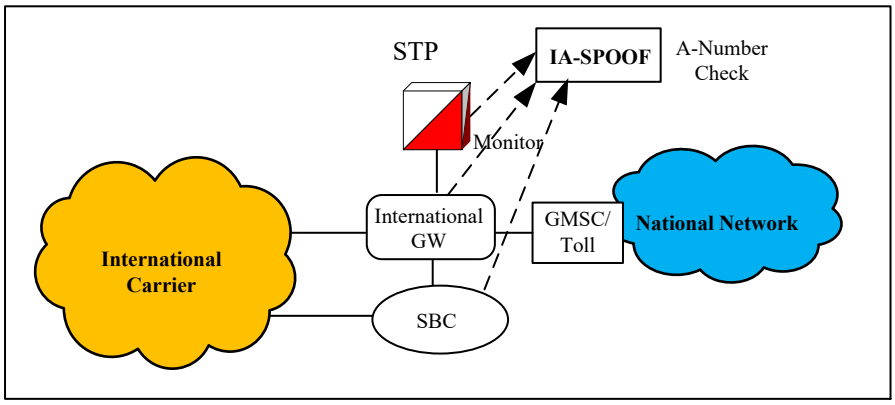
- Network Layer provides communication with telecommunications networks such as ISUP, MAP, SIP, HTTP/API.
- Service Layer provides service features such as routing (Routing), message monitoring analysis (Screening), updating roaming subscriber location (Location Update) ...
- Application layer provides features for system administrators such as implementing fake call blocking/cancelling conditions, checking and monitoring fraudulent calls, providing STIR/SHAKEN prevention mechanism, functions Synthesize report statistics, provide Troubleshooting tools such as searching and checking events, call information on the system.



The software supports the ability to deploy on multiple partitions simultaneously and centrally administer, monitor and report in a central partition.

Call spoof handling feature:

- Call spoofing application detects, and checks calls with the correct domestic phone number roaming abroad from a valid subscriber or not.
- The system provides the function of searching and querying forgery detection information from many sources.
- Customize call spoof checking in different methods.

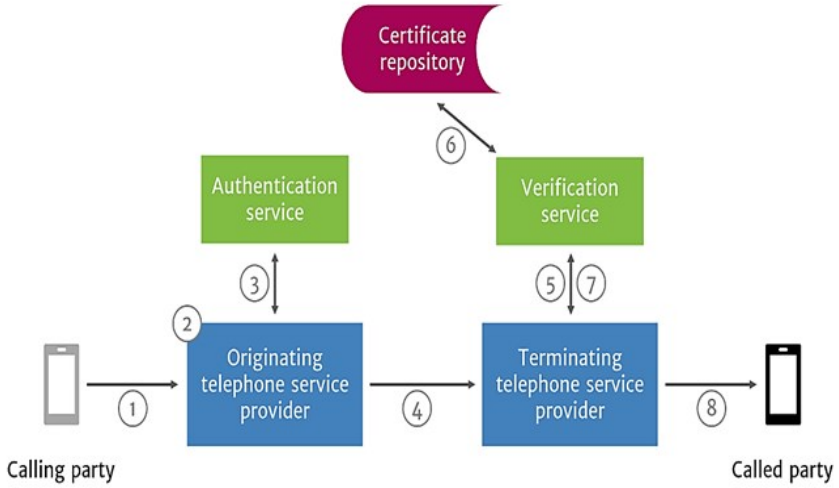


- Statistics and monitoring of priority phone numbers to check for spoofs.
- Spoofing monitoring.

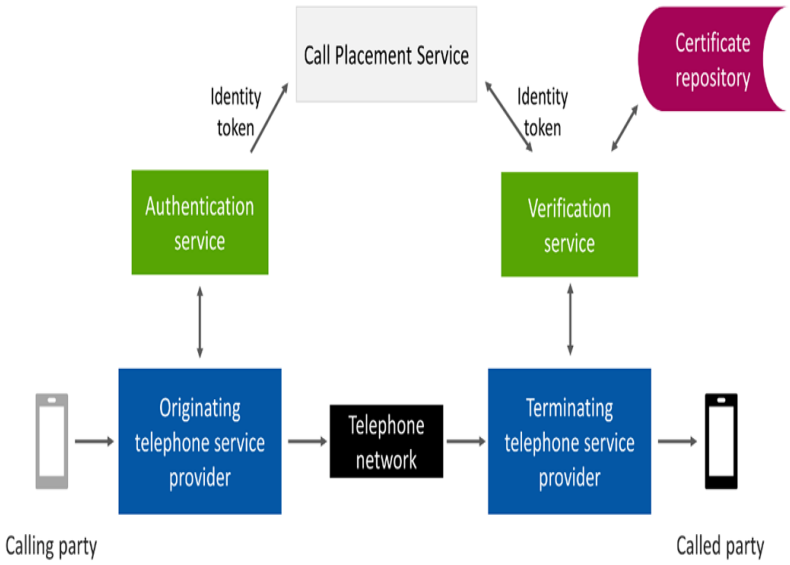
STIR and SHAKEN call authentication feature:

Call authentication solution (Authentication) using STIR/SHAKEN procedures (through existing research the US and Canada have deployed, UK and Norway are researching to deploy):

- STIR (Secure Telephony Identity Revisited) is the IETF standard for caller ID authentication. STIR works by adding a private key to the Session Initiation Protocol information used to initiate and route calls in VOIP systems. The originating network (network A) then attaches its own encrypted network private key to the SIP header with the identity of the caller (caller ID). The terminating network (network B) checks the correctness of the call by using network A's public key (retrieved from the public key database) in combination with network A's private key (STIR decryption).



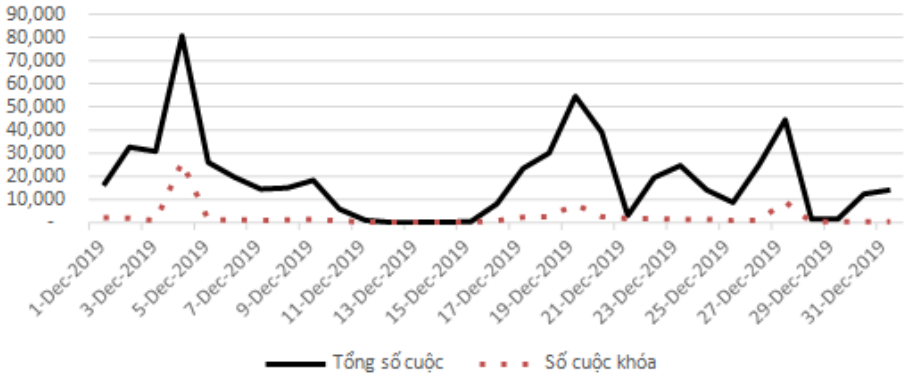
- For non-VOIP systems, such as mobile phones and landlines, call routing information is by signaling number 7 (SS#7). In this case, the STIR standard cannot be used, but the SHAKEN (Signature-based Handling of Asserted information using toKENs) procedure must be used. SHAKEN works according to the following principle: The calling network (Network A) encrypts (PASSporT) the SIP Identity header with the public key of the called network and sends this header over the Internet privately (out-of-the-box). -band) to the CPS call location service of the called network; Calls are routed over the phone network as usual (Calls routed over a SIP or TDM or hybrid network will work); When the called network receives the call, it will send information to the VS verification service, the VS service uses the private key of network A to check and compare the SIP Identity header obtained from the CPS of network A with the caller number. ; If the caller number in the SIP Identity header matches the number received by the caller, connect to the called number.



Call spam prevention feature:

The system analyzes signaling messages and CDR calls to analyze and detect the following behaviors:

- Detecting spikes in traffic to high rates (IRSF International Revenue Share Fraud).
- Detect call spam behavior.
- Detecting bait calling behavior (Wangiri).
- etecting PBX hacking (PBX hacking).
- Detecting fraud using manipulated B-numbers programming vulnerabilities.
- Sends alerts on fraudulent calls when thresholds are reached and allows the option to temporarily block these calls.
- An AI system in identifying and adjusting alarm thresholds based on actual traffic sources

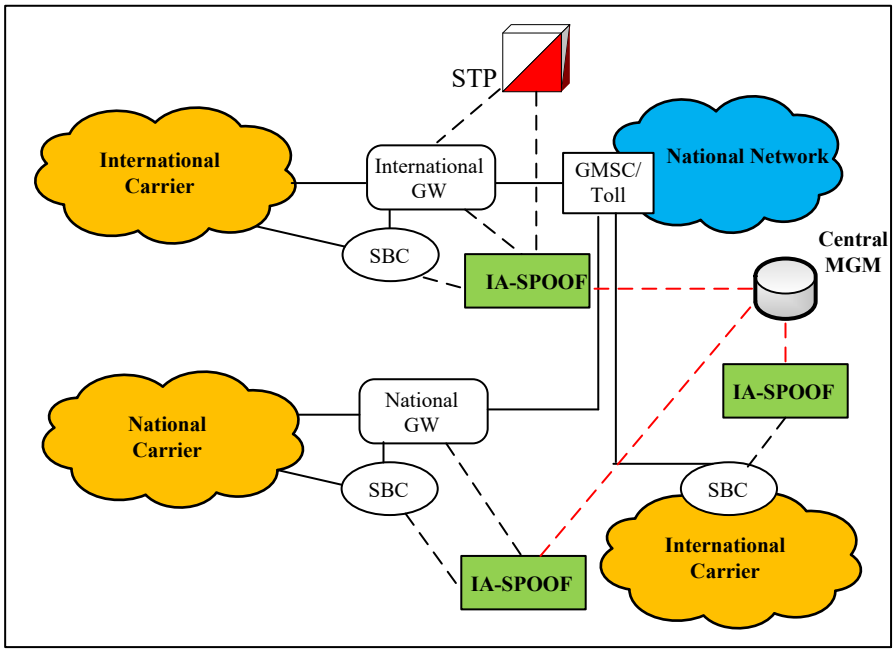


- Detect forms of fraud and spam in addition to using simbox.

Distributed on many Sites:

A distributed system capable of handling signaling messages or voice traffic on multiple sites simultaneously and synchronizing data.:

- Distributed message (or traffic) processors.
- he filtering/blocking rules sync with each other on the Sites.
- Centralized unified configuration.

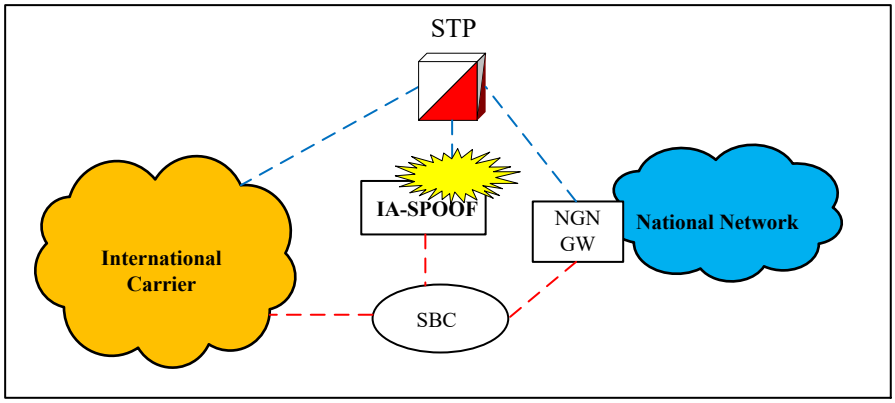


- Sites that support on-site redundant configuration.

Failed Over mechanism:

The system is able to integrate with core network components to ensure uninterrupted service redundancy:

- The system integrated into the network acts as a network Node ensuring that the mechanisms know the state of the Node.
- When the IA-SPOOF system fails, the messages will continue to be routed to the destination system and skip the IA-SPOOF network node.

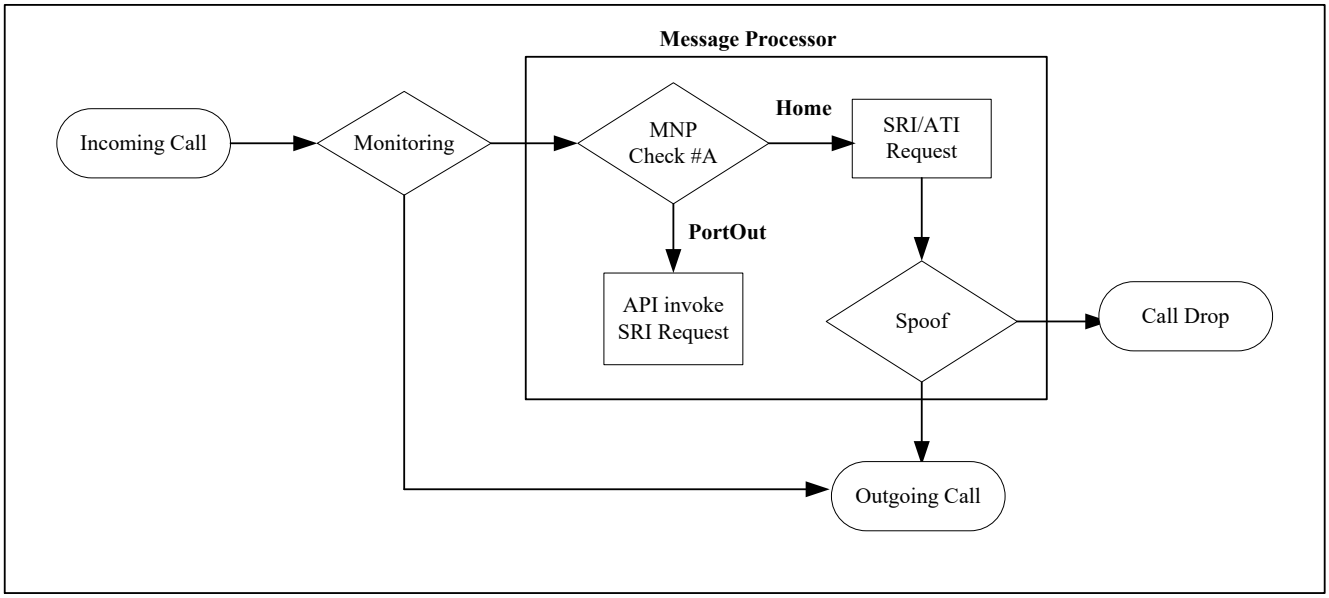


- Service is maintained and automatically routed when the IA-SPOOF system fails.
- The system provides a monitoring mechanism when there is no traffic or the failure rate (KPI) declines.

Features

The IA-SPOOF system supports customization of call handling flowcharts and features to check subscriber number information in the call.

Process Flow:



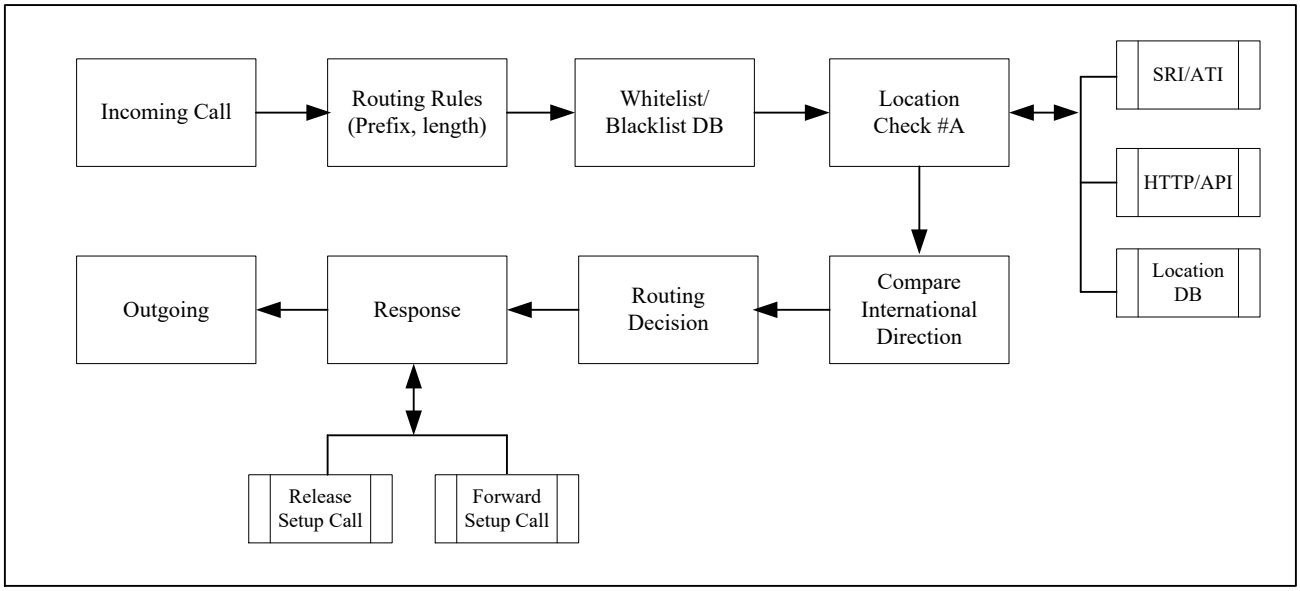
The Messages Processor call processing block supports many different call handling scenarios at the same time, allowing customizations to be set up.

The system provides a call monitoring bypass function that allows to open/unblock/cancel all incoming calls (the system is in monitoring mode).

Features

The IA-SPOOF system supports customization of call handling flowcharts and features to check subscriber number information in the call.

Sample diagram depicting call flow:



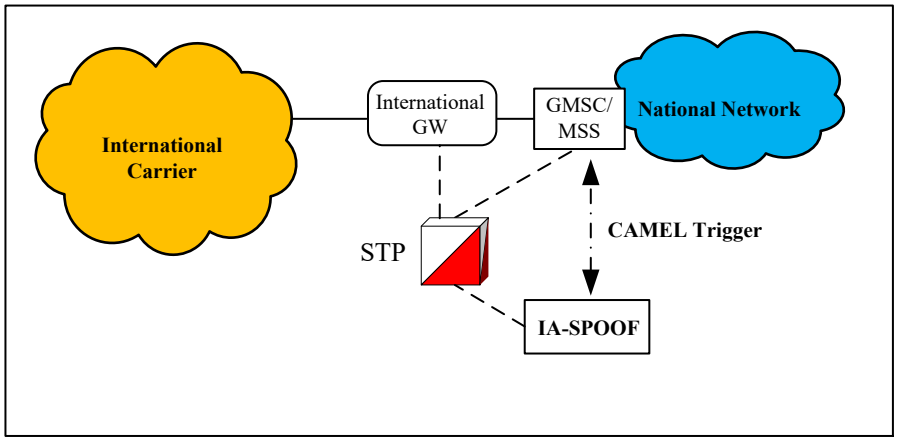
Basic call handling features:

- Routing handling function: stipulating and standardizing the format of caller and dialed phone numbers according to Vietnam's standards (with specified prefix and number length).
- Function to process according to the allowed/restricted list (Whitelist/Blacklist) that regulates subscribers to be banned or prioritized.
- Function to check the subscriber's address corresponding to the caller's number (applicable to mobile calls). This function supports many different mechanisms simultaneously:
  - Mechanism for using HLR query SRI/ATI messages (or MNP on STP systems).
  - Mechanism for using HTTP/API (or Rest API) queries to other Enterprise (or other business) systems.
  - Mechanism of using a database to store temporary information about Outbound Roaming subscribers.
- all routing decision function: perform call blocking/cancellation based on response/reply indication of call release signaling message or forwarding received call initiation message.

Features

IA-SPOOF system supports receiving call trigger from GMSC/MSS systems via CAMEL.

Diagram depicting call flow:



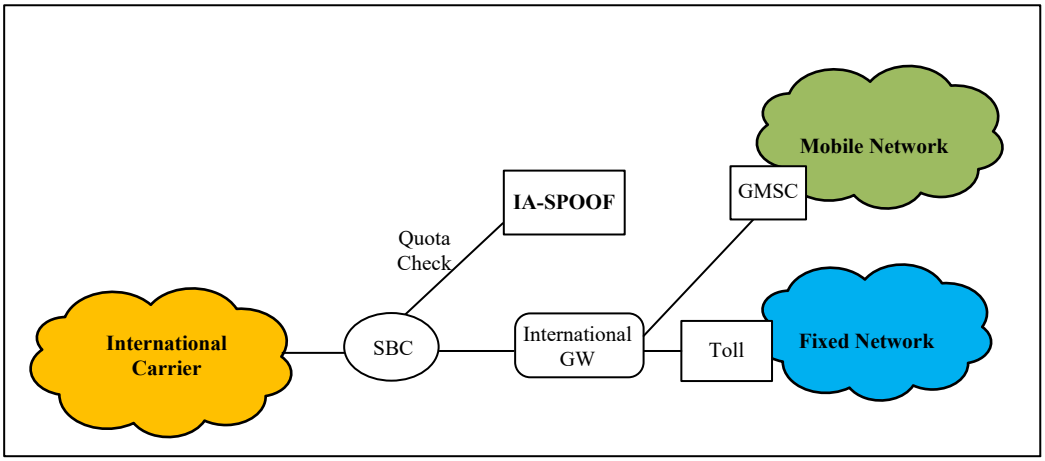
Basic trigger handling features:

- Provide blocking rules defined by parameters: IMSI, MSISDN, VLR...
- Receive, process and analyze CAMEL IDP messages.
- Allows defining, declaring any service flags on the HLR.
- Check and authenticate roaming subscribers when making calls.
- Handling MT calls.

Billing and Rating

IA-SPOOF system supports VoIP prepaid billing.

Connect to an international VoIP network:

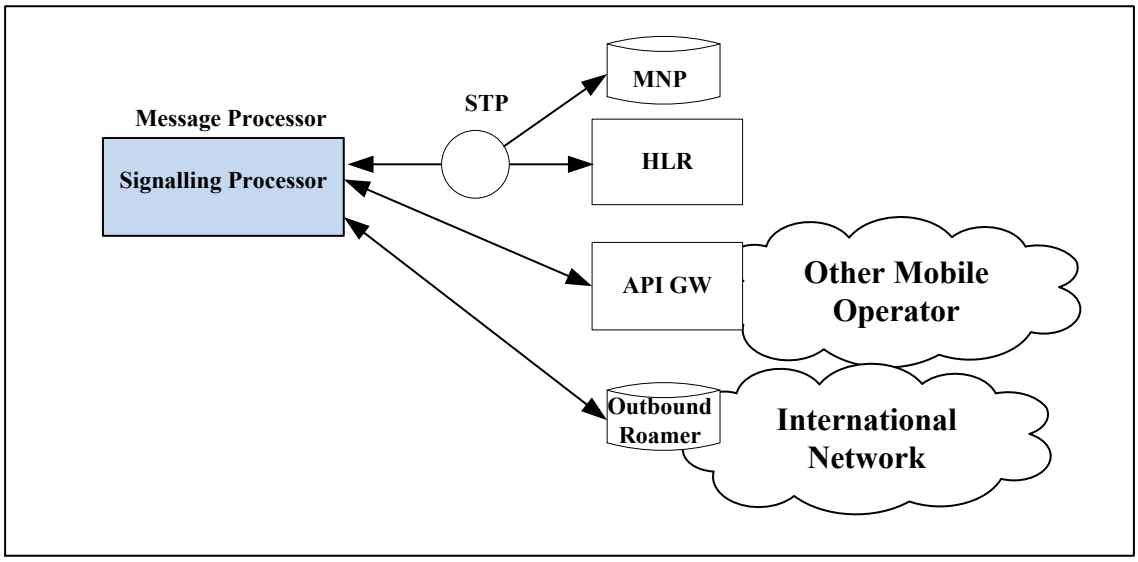


Prepaid billing and statistical processing features:

- Provides rules for monitoring internationally connected VoIP trunks.
- Receive and process SIP tag messages.
- Definition of international connectivity partners.
- Read and analyze CDR from SBC system.
- Handling international MT calls (prepaid for trunks).
- Define tariff rates for each number.

Query Processing

The IA-SPOOF system provides various query mechanisms through multiple interfaces that connect to the components of the telecommunication network.



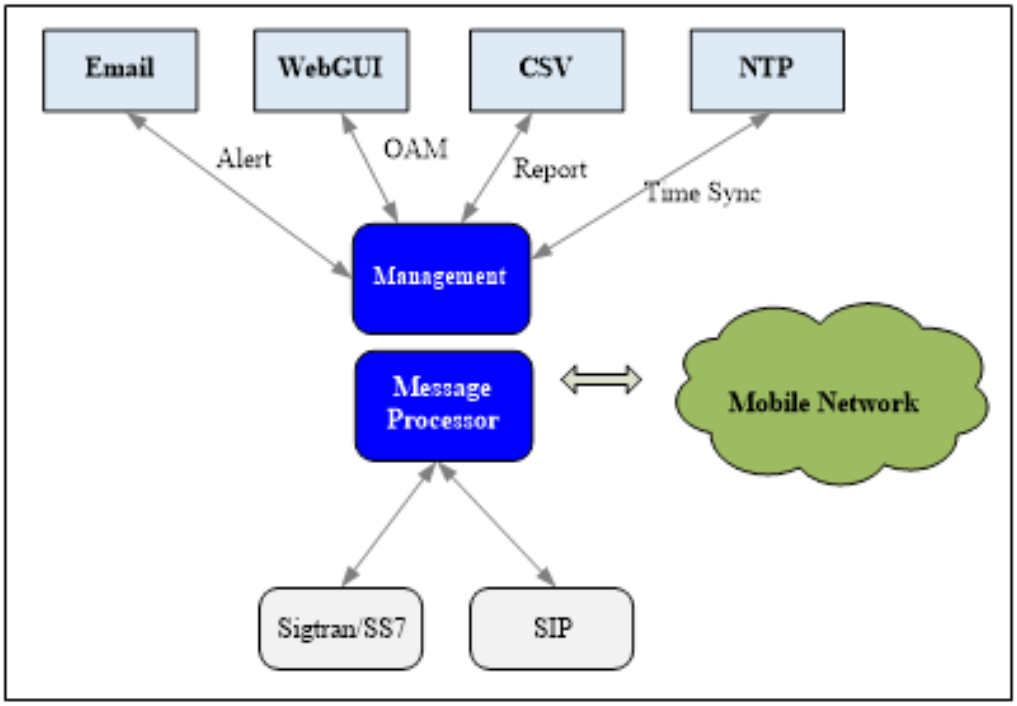
Query processing mechanisms can be configured to selectively or combine multiple different query mechanisms for different types of traffic.:

- Query to HLR database (information on network subscribers).
- Query to MNP database (information about subscribers using MNP services):
  - Non-Port subscribers
  - Port-In subscribers
  - Port-Out subscribers
- Query to the Outbound Roamer DB subscriber database. The system is capable of updating the status of Outbound Roaming subscribers.
- Query to GW API gateway to collect information of off-net subscribers.

The IA-SPOOF system provides management of response delay parameters on different types of queries to ensure call processing delay.

Reporting

Centralized management and reporting system IA-SPOOF ensures the configuration of blocking/filtering processors in sync with each other on the entire system.

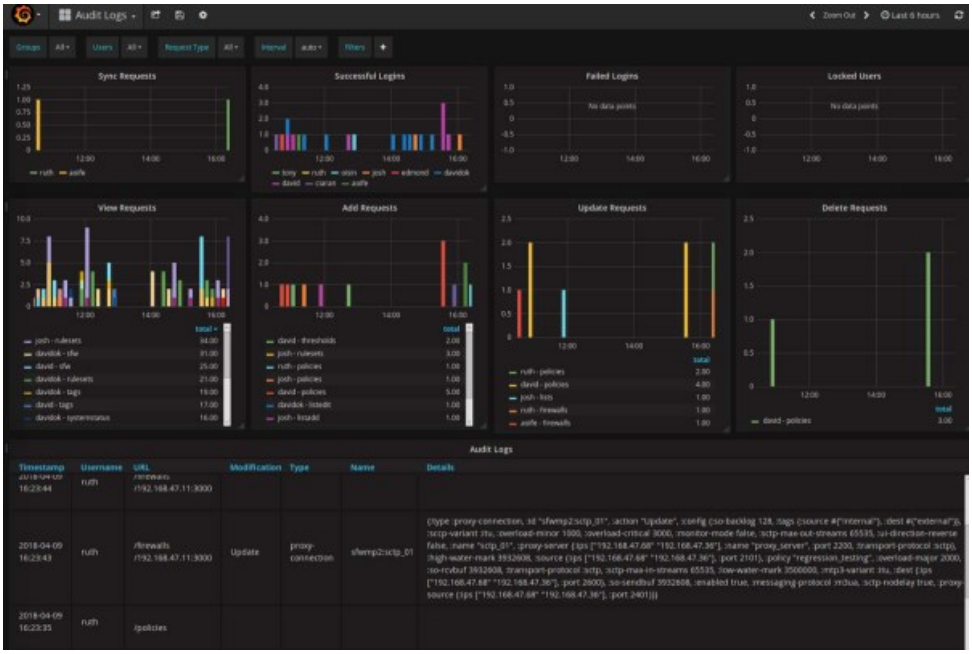


The administration system provides an interface to the administrative functions and communicates with the functions of the administrator:

- Send email alerts to administrators.
- Web GUI interface for administrators to configure, manage and monitor services.
- Communicate with centralized reporting system, upload and download CSV report KPI files.
- Synchronization with NTP clock system.

Reporting

Reporting interface based on Grafana technology allows querying, displaying, alerting and helping users understand data metrics.



The solution provides a number of standard reports, in addition, users can define more reports according to actual use:

- Report form in accordance with general regulations such as: blocking results of calls with incorrect caller numbers, results of blocking calls with international service codes that do not agree to cooperate with network operators, blocking results fake call carrier mobile number.
- Report on average call handling delay.
- International VoIP and TDM output reports on.
- Report filter blocking rate on each type of VoIP and TDM traffic
- Report filter blocking rate on each international VoIP partner.
- Report filter blocking rate on each international partner TDM
- Report Top most violating partners in international connection partners
- Report the trend chart of violations of partners
- The system has the ability to set thresholds to monitor the following criteria: average delay, filter blocking rate.

Specification and Features

Compliance:

- SIP protocol support with RFC 3261.
- upports protocol SS7 ITU-T standard Q.764 – Q.767, SCCP, TCAP, ISUP, MAP
- Support MNP.
- HTTP/API protocol support.

Security:

- Administration interface via HTTPS security protocol.
- System Privilege.
- Audit log.
- Warning User wrong access many times.
- Statistics of IP access to the system.

Administrator:

- Monitor the operating status of the system: CPU, memory, HDD usage...
- Monitor service operation status: processes, modules, connection interfaces.
- Monitor the processing traffic on the system.
- Monitor connections: SS7 signaling, HTTP API (including Rest API).
- System configuration management: numerical processing tables, time parameters, error code tables...
- Manage connections to other external data enrichment systems.
- Manage configuration backup and restore.
- Manage log, trace log on API ports connecting national carriers.

Features:

- Provide Whitelist/Blacklist filter block list (first number or subscriber number).
- Provide VIP subscriber list.
- Provide address list of international TDM or VoIP partners.
- Provide a set of rules to handle destination phone numbers (used for routing).
- Call Flow customization.
- Customizable adjustment of time thresholds: waiting for query reply, waiting time (bypass)…
- Customizable adjustment of time thresholds: waiting for query reply, waiting time (bypass)….
- Distinguish network node addresses.
- Provides SIP, ISUP signaling processing function.
- Set error codes for signaling message return.
- Provide the function of querying subscriber location information: MAP SRI, MAP ATI, HTTP API (including Rest API)...
- Provide function to query MNP subscriber information: MAP SRI, HTTP API (including Rest API)…
- Capable of handling voice traffic.
- Handle SIP tags.
- Integrated centralized signaling monitoring system.

Specification and Features

Reporting:

- The system provides different report templates: The solution must support daily, weekly, monthly reports and reports according to the time frame configurable by the administrator.
- Information about the average latency of each hop and process, on-net and off-network: receive and reply to network messages, receive and respond to information query messages.
- Call information about caller number, called number, processing status (Allow/Block), Whitelist/Blacklist list, length of caller number, error code returned to network device...
- Provides a graphical user interface for displaying charts and data and for all reports: Graph types: Graph, Bar, Gauge, Histogram pie (Pie), heatmap (heatmap) ... allows to render csv . reports.
- Filter blocking rate on each connection direction (integrated with VNPT's partner information collection system). Filter blocking rate for each number of callers, called, by carriers.
- Top violated partners.
- Graph of violations of partners (integrated with VNPT's partner information collection system).
- Customize the configuration of report templates in JSON format, which is easy to copy (duplicate), modify (edit) to customize the available report templates.
- Import/Export report templates at the request of the user.
- Supports connection and integration of many different types of databases: MySQL, Microsoft SQL, PostgreSQL, InfluxDB, Elasticsearch...
- Customize different types of reports: frequency of spam calls, fraudulent calls, blocking rate filtering each SS7/TDM connection direction...

Troubleshooting

- Provide a tool to look up call information: caller number, called number, time, or connection partner information (if any).
- Dump query results, lookup call information to data files (json format)..

Traffic Monitoring

- Set monitoring threshold for indicators: average latency, filter blocking rate.
- Monitoring alerts via Dashboard (or email if available) statistical reports.
- System error alerts via email.
- Monitoring signaling, processing load according to preset thresholds.