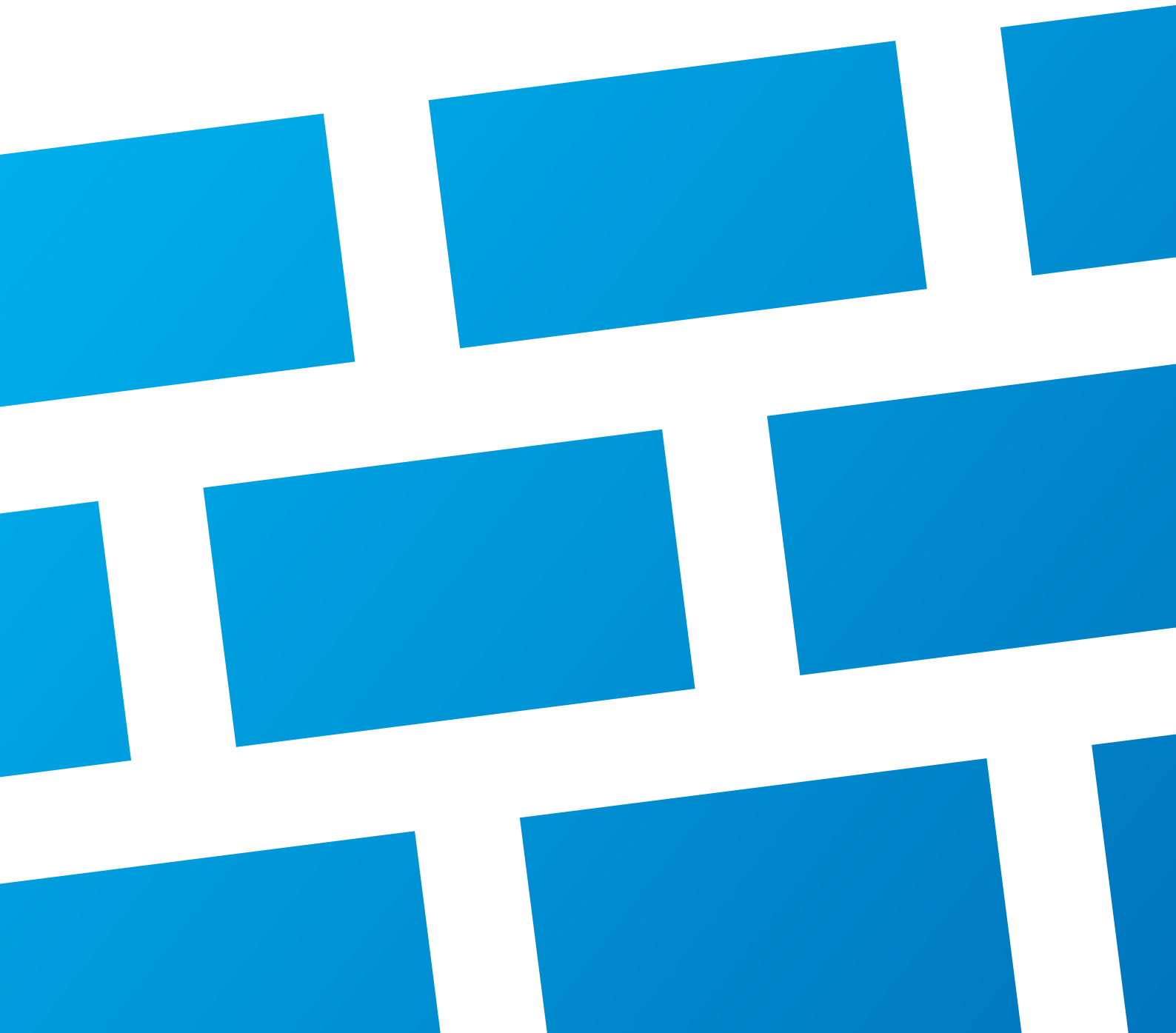
PROTEI Signaling Firewall

Universal solution for signaling networks protection



Why the need?

SS7 protocol was initially designed to be used within fixed-line operators, with no built-in security. In the design of 2G/3G networks, which rely on SS7 signaling, security wasn't a high priority concern, and there was no foresight about how mobile would penetrate the world and what type of security challenges interconnect would bring (as soon as the signaling network was considered as the closed ecosystem).

Within the past 10...15 years, more unconventional service providers such as MVNO's, mini-operators, VAS and roaming service hubs and content providers are entering the telecom market on both national and international levels. These players normally interconnect with existing operators and carriers via standard signaling networks and may address any network node worldwide having the connection to the global signaling network via the backdoor of some small player. Thus, such interconnections open an access to the global telco signaling networks for hackers and spammers.

Attackers are increasingly taking advantage of the vulnerabilities of signaling protocols. They may listen to calls, locate individual users, pass un-authorized data traffic, read messages which may expose some personal information e.g., passwords, 2FA, etc.

As soon as today's signaling networks are not isolated anymore, intruder may exploit network flaws and intercept calls/SMSs, bypass billing, steal money from mobile accounts, or affect mobile network operability:

- Compromising of subscriber's location
- Illegitimate redirection of terminating or originating calls (e.g., Terminating call redirection, Control of unconditional forwarding, Originating call redirection, etc.)
- USSD request manipulation (e.g., USSD spoofing, Money transfer)
- SMS message manipulation
- Subscriber profile changing (e.g., delete or update the subscriber's O-CSI subscription)
- Subscriber information disclosure (e.g., Balance and Location disclosure, IMSI disclosure, etc.)
- Network information disclosure (e.g., SendRoutingInfo, SendRoutingInfoForLCS, etc.)
- Subscriber traffic interception (e.g., SMS interception, Call interception and forwarding)
- Denial of Service (DoS) attacks

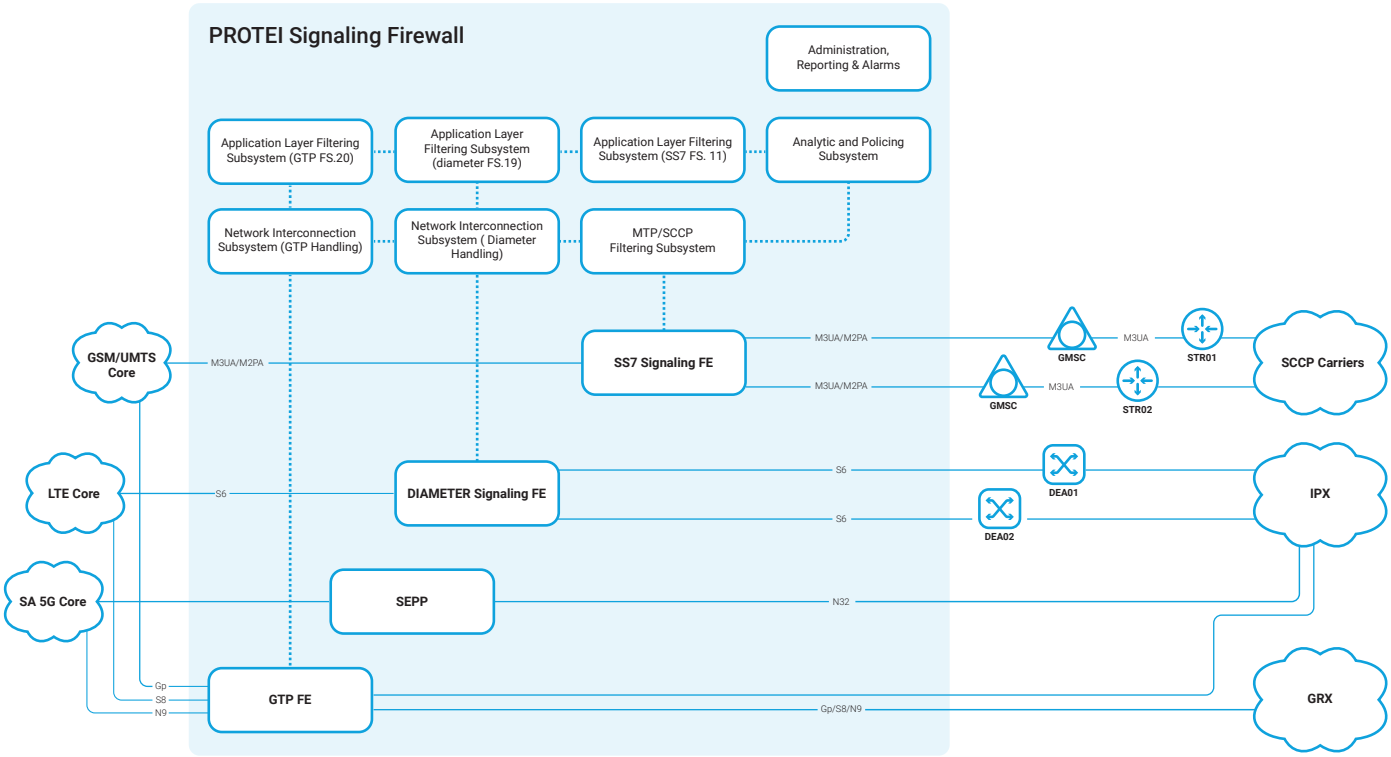
Such cases highlighted the vulnerabilities in SS7 and DIAMETER standards and network elements, thus created the need of introducing dedicated systems with advanced signaling network protection capabilities.

Solving the Issues

Being experts in the field, PROTEI introduced an advanced Signaling Firewall intending to help operators in monitoring, controlling and managing SS7, DIAMETER and GTP traffic addressed to and sourced from the mobile network.

PROTEI Signaling Firewall is designed to detect and handle the wide variety of attacks related to above mentioned signaling protocols. PROTEI Signaling Firewall implemented in the strict compliance with GSMA security specifications (FS.11, FS.19, FS.20 etc). Besides that, system supports flexible customization capabilities to ensure easy adoption to the real environment and protection from unconventional attacks.

The system is an effective tool for preventing network and subscriber oriented attacks such as spamming, flooding, fraud generation, tracking, Identity theft, DoS (Denial of service) or Illegal interception. The system provides a flexible routing management and policy management individually for each SS7, GTP and DIAMETER peer or connection based on a wide range of filtering criteria.

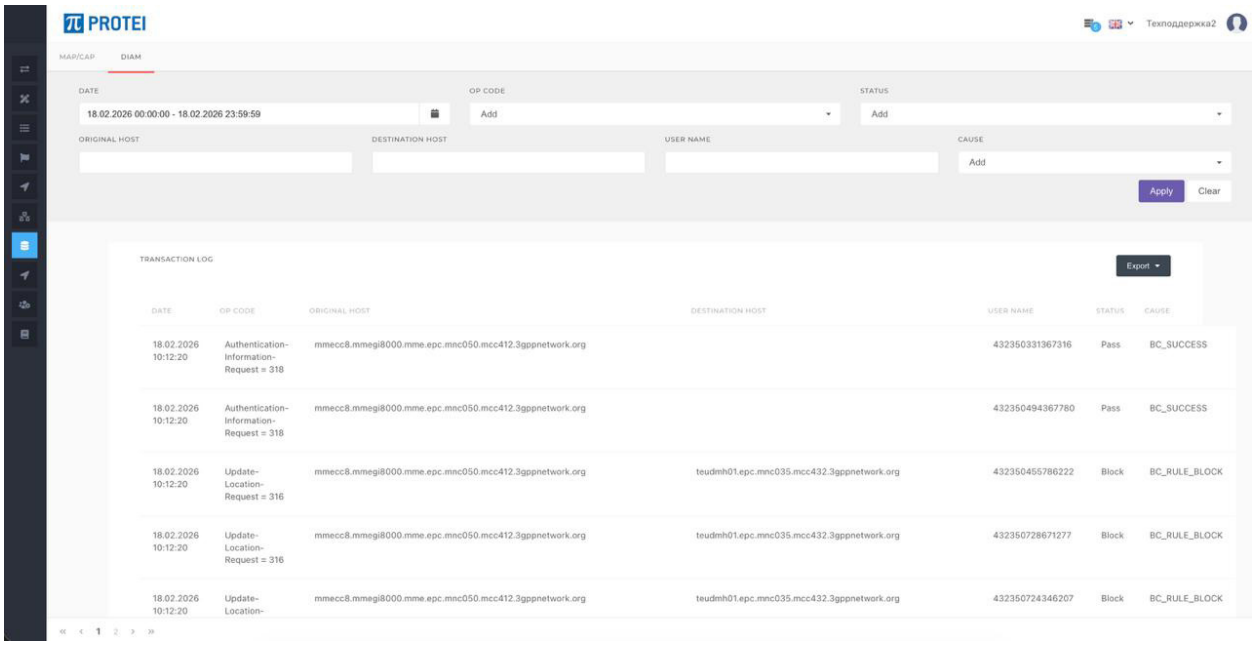


Features

- Compliance to GSMA Fraud and Security Group specifications (FS.11, FS.19, FS.20)
- Universal solution for all kind of protocols with the common information database and ability to perform information correlation between different protocols and events coming from different signaling domains
- Flexible routing and policy management configurable individually for each signaling connection and/or signaling partner/peer basing on:
  - Address information (GT, Host ID/Realm etc)
  - Subscriber information – location, velocity, previous transactions
  - Particular protocol (MAP, CAP, Diameter, GTP)
  - Diameter Application-ID and/or Command code
  - Information elements/AVPs presence and values
  - Block messages that are for intra-PLMN only
- Variety of connectivity schemes:
  - Transit mode
  - Passive mode
  - Overlay proxy mode
- Support all protocols and versions operator may use:
  - Wide range of DIAMETER-based protocols and applications (S6, Swx, Cx, Sh etc)
  - MAP v1…3 support
  - CAMEL v1…4 support
  - GTP v0…v2 handling
- Scalable according to network growth (horizontal scaling) with load-sharing or 1+1 redundancy
- Powerful logging system (CDR generation and detailed statistic collecting)
- Convenient WEB UI including Rule Builder for customized transaction handling logic creation
- Detailed CDRs/EDRs generation
- Advanced KPI dashboards as well as Grafana-based monitoring subsystem
- Carrier-class throughput – thousands transactions per second per one VNFC
- VNF-based or bare-metal deployment

Protection measures and approaches

- Message encoding validation (mandatory fields control, duplicated fields detection and so on)
- Message categorization as per GSMA methodology for SS7, Diameter and GTP trafficSupport
- Transaction awareness and per subscriber stateful transaction handling
- Velocity Check
- Traffic threshold management/limitation per message type, peer etc
- Variety of message blocking capabilities



Professional Telecommunications Incorporation (Protei)

Headquarter

Wasfi Al-Tal Street, Al Otoum Business Center No. 98, Suite 205 P.O. Box 961741
Amman 11196, Jordan

Tel.: +962 6 560 78 33

E-mail: sales@protei.me

Website: www.protei.me

GCC Branch

Business Village Deira,
Al Maktoum Road 4th Floor, Block-B
P.O. Box 183, Dubai U.A.E

Tel.: +971 (0) 4 230 6029

E-mail: sales@protei.me

Website: www.protei.me