

■ NETWORK SECURITY

Signaling Firewall

One platform to protect your SS7, Diameter, GTP and 5G signalling against fraud, intrusion and revenue loss.



FS.11

GSMA SS7 security compliant

FS.19

GSMA Diameter security compliant

FS.20

GSMA GTP security compliant

1+1

Redundancy or horizontal scaling

■ WHY IT MATTERS

Your signalling network is no longer a closed club

SS7 was designed for a small, trusted community of fixed-line operators — security was never part of the plan. Today, that same signalling network connects thousands of players worldwide, and attackers know it.

Over the past 10–15 years, new players — MVNOs, mini-operators, VAS and roaming hubs, content providers — have joined the market at national and international level. They interconnect through standard signalling networks and can reach any node in the world. Each new connection is also a potential back door for **hackers and spammers**.

Attackers exploit these weaknesses to listen to calls, track subscribers, read messages containing passwords and two-factor codes, bypass billing, steal money from mobile accounts or disrupt the network itself.

■ Typical signalling attacks

- ✓ Exposure of a subscriber's location
- ✓ USSD manipulation — spoofing and fraudulent money transfers
- ✓ Subscriber profile changes, such as deleting or altering O-CSI subscriptions
- ✓ Disclosure of network data, e.g. SendRoutingInfo and SendRoutingInfoForLCS
- ✓ Denial of Service (DoS)
- ✓ Illegitimate redirection of terminating or originating calls, including unconditional forwarding
- ✓ SMS manipulation and interception
- ✓ Disclosure of subscriber data: balance, location, IMSI
- ✓ Interception of subscriber traffic — calls and SMS

The result: a clear need for dedicated protection

These threats expose vulnerabilities in the SS7 and Diameter standards and the network elements that use them. Operators need a purpose-built system with advanced signalling protection capabilities.

■ THE SOLUTION

PROTEI Signaling Firewall: complete protection, one platform

Built on deep signalling expertise, PROTEI Signaling Firewall helps operators **monitor, control and manage SS7, Diameter and GTP traffic** to and from their mobile network — with 5G SA interconnect protected through the SEPP.

It is implemented in strict compliance with GSMA security specifications **FS.11, FS.19 and FS.20**, while flexible customisation lets you adapt it to your real

network and stop unconventional attacks that standards alone do not cover.

It stops spamming, flooding, fraud, tracking, identity theft, DoS and illegal interception, with routing and policy managed individually for every SS7, GTP and Diameter peer.



- PROTEI Signaling Firewall architecture: one platform protecting SS7, Diameter, GTP and 5G interconnect

CAPABILITIES

Features

Standards-based

Compliant with GSMA FS.11, FS.19 and FS.20 security specifications.

Cross-protocol intelligence

A common database correlates events across SS7, Diameter and GTP.

Every protocol you run

Diameter (S6, SWx, Cx, Sh...), MAP v1-3, CAMEL v1-4, GTP v0-v2.

Flexible deployment

Transit, passive or overlay-proxy mode; VNF or bare metal.

Carrier-class scale

Thousands of TPS per VNFC; load-sharing or 1+1 redundancy.

Easy to operate

Web UI with Rule Builder, CDRs/EDRs, KPI and Grafana dashboards.

Granular routing and policy

Rules can be configured individually for each signalling connection or partner, based on:

- ✓ Address information — Global Title, Host ID, Realm
- ✓ Subscriber information — location, velocity and previous transactions
- ✓ Protocol — MAP, CAP, Diameter or GTP
- ✓ Diameter Application-ID and command code
- ✓ Presence and values of information elements and AVPs
- ✓ Messages that must remain intra-PLMN only

Protection measures and approaches

- ✓ Message encoding validation
- ✓ GSMA message categorisation for SS7, Diameter and GTP
- ✓ Stateful, per-subscriber transaction handling
- ✓ Velocity checks against impossible movement
- ✓ Thresholds per message type and peer
- ✓ Flexible message-blocking actions



■ ABOUT PROTEI

Carrier-grade telecom solutions since 2009

Founded in 2009 and headquartered in Amman, Jordan, Professional Telecommunication Incorporation (PROTEI) designs and delivers carrier-grade software for mobile and fixed network operators, MVNOs, enterprises and governments. Our portfolio of 50+ systems and solutions spans core network, roaming, messaging, value-added services, data management, public safety and customer care.

With development centres in Jordan, Europe and the CIS, live deployments across the Middle East, Europe, Africa, Latin America, Central Asia and the CIS, and regional offices in the UAE and Central Asia, PROTEI serves more than 400 clients. Every platform is designed in-house under ISO 9001:2015 and ISO 14001:2015 certified quality management.

17

Years in telecom

400+

Clients worldwide

45

Countries

50+

Systems & solutions

Turn your network into your next growth engine.

Talk to our experts about signalling security for your 2G to 5G network — and see how PROTEI can help you grow revenue, cut costs and protect every subscriber.

Professional Telecommunication Incorporation (PROTEI)

Headquarters · Amman

Wasfi Al-Tal Street, Al Otoum Business Center 98, Suite 205
P.O. Box 961741, Amman 11196, Jordan

T +962 6 560 78 33

E sales@protei.me

GCC Branch · Dubai

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

T +971 (0) 4 230 6029

E sales@protei.me



www.protei.me