# PROTEI SS7 Firewall

Being experts in the field, PROTEI introduced their SS7 Firewall which intended to help operators in monitoring, controlling and managing SS7 traffic with other national and/or international operators, carriers and other telecom services providers. PROTEI SS7 Firewall is designed to detect and handle unexpected or unconventional SS7 messages through applying appropriate MTP, SCCP, TCAP and MAP policing rules.

Furthermore, and in order to assure full SS7 protection capabilities, PROTEI SS7 Firewall adopts the GSMA definition of SS7 attacks specified in GSMA IR.82 and in updates to specifications from the GSMA Fraud and Security Group (FS.11, FS.07, IR.70, and IR.71).

## Why the need?

Within the past few 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, and as such players will normally interconnect with existing operators and carriers, hackers and spammers found more ways to log onto the expanding SS7 network.

As a result of such mandatory growth, the telecom industry experienced a lot of cases where hackers used one party's network to pass fraudulent SS7 traffic towards other networks and abusing standard SS7 messages to track subscribers, remove/add service, deny access and even intercept calls and SMS's.

And while some operators were able to prevent some basic attaches using standard STP's or GMSC's policing features, most of the serious SS7 attaches we robust to such basic features, leading some operators to adopt total blocking of SS7 relations with "infected" operators in order to maintain networks' safety as well as subscribers privacy and even prevent revenue loses.

Such cases highlighted the vulnerabilities in SS7 standards and network elements, thus created the need of introducing dedicated systems with advanced SS7 traffic monitoring and control capabilities.

## Benefits

- Preventing Network oriented SS7 attacks:
  - Spamming and flooding
  - Fraud generation
- Preventing Subscriber oriented SS7 attacks:
  - Tracking
  - Identity theft
  - DoS (Denial of service)
  - Illegal interception
- Easley upgradable to serve SMS-FW functionalities
- Built on standard and proven technology through live implementations
- Flexible pricing model to meet budget expectations
- Dedicated Technical Architecture and Installation team
- 24x7x365 Support

## Features

- Compliance to GSMA Fraud and Security Group specifications (IR.82, FS.11, FS.07, IR.70, and IR.71) .
- Flexible routing management and policy management individually for each SS7 connection (PC or GT)
- Wide range of filtering criteria for SS7 messages:
  - MTP3 and SCCP layer filtering
  - Application layer filtering (Filter TCAP and MAP layers content)
  - Application layer management (Block/Modify MAP layer content)
- SS7 time window to control MSU's flow from a certain SS7 connection (PC or GT)
- SS7 Anti-SPAM functionality protecting the network from mass MSU sending with similar operation code or similar originator (PC or GT)
- Network Addresses Masking functionality
- Personalized Black and White Lists
- Supports GSM MAP phase I, II, III
- Fully compatible with ETSI GSM 03.40 and 03.38
- Support HSL (2 Mbps SS7 links, G.703 Annex A)
- Supports SIGTRAN (M3UA and M2PA links)
- gateway in case of E1 connectivity;
- Scalable according to network growth (horizontal scaling);
- Powerful logging system (CDR generation and detailed statistic collecting);
- Supports load-sharing or 1+1 redundancy
- Comprehensive CLI for all Operation Administration & Maintenance activities
- Fully featured SNMP based network monitoring
- Detailed system performance and recording with CDRs

## Supported Network Protection Approaches

- Monitoring and Alerting: where the SS7 firewall generates detailed reports on the SS7 traffic and generates alerts on suspect SS7 attacks based on preset thresholds on operation codes per GT or PC.
- Basic Policing Rules: Filtering rules set independently for each layer of the SS7 stack; MTP, SCCP, TCAP or MAP. The rules may be set through the system GUI for the specific parameters of each layer.
- Advanced Policing Rules: when a complex SS7 attack scenario is identified, a combination of filtering rules might be needed, where the user combines the required SS7 parameters of the different layers (PC, SCCP addresses, NI, OP-Code, Application layer addresses… etc.) to create the required rule that matches the detected attack.

## Scalability and SS7 Dimensions

- Highly scalable; up to 1000 TPS over a single server
- Up to 32 SS7 links per one SS7 card
- Unlimited number of M3UA and M2PA links

## Supported Protocols

- SCCP Layer
  - ITUT Q711-Q714
  - ETSI ETS 300 589
- TCAP Layer
  - ITUT Q.771-Q.775
  - ETSI ETS 300 287-1
- MAP v1…3
  - 3GPP 29.002

## SIGTRAN

- SCTP RFC 2960 and RFC 4960
- M3UA RFC 3332
- M2PA RFC 4165

## OA&M

- SS7 or SIGTRAN connectivity management;
- SCCP routing rules configuration;
- Policy management (white and black lists' definition);
- Configuration of connectivity parameters for integration with other NE's;
- Alarm indication subsystem mana gement (trap generation criteria, MIB settings);
- CDR and statistical information viewing.

## System Logging

- Real time configurable logging levels
- Detailed protocol debug
- System and exception logs
- User and Admin history

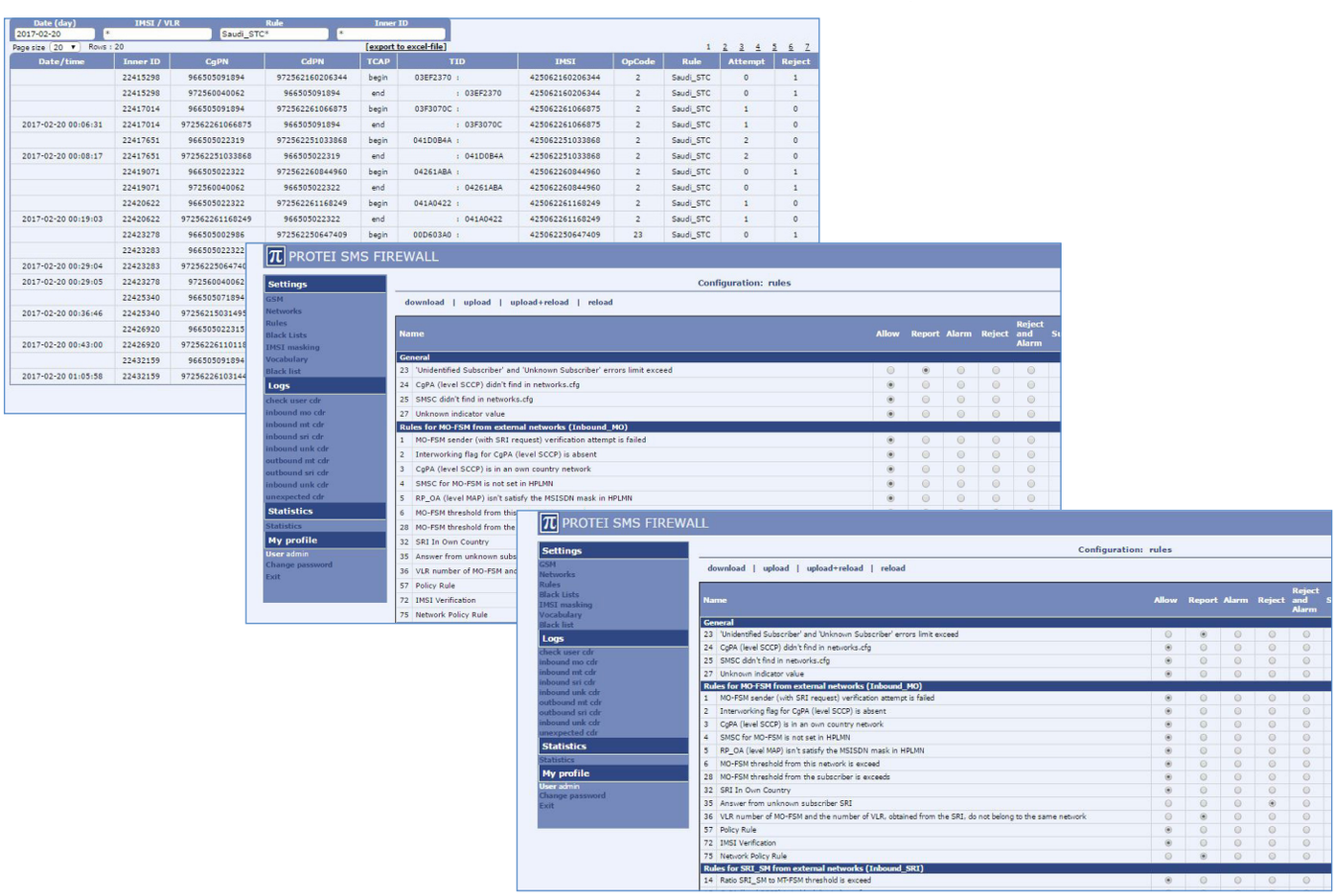
## SNMP

SNMP Version 1,2 and 3 with the following traps are supported:

- Not enough free space for storage
- Server reboot
- Restarts of SW components
- SS7 link establishment/loss or SIGTRAN associations activation/deactivation
- Traffic statistical traps
- Enter/Exit congestion protection mode for the entire system and for particular service logic types
- Trigger is activated (i.e. traffic processing rule is applied and some packet rejected or forwarded…etc.)

## Support

PROTEI provides a range of post-sales support packages to meet client requirements and budget. These range from basic best-effort support up to dedicated golden web, email and telephone support provided 24x7x365. Furthermore, customers get up to 1 year free of charge support all purchased products.




PROTEI
60A B.Sampsonievsky, St.Petersburg,
194044, Russia , Business Center "Telecom"
Tel.: +7 812 449 47 27 Fax: +7 812 449 47 29
E-mail: sales@protei.com Web: www.protei.com

PROTEI MENA Branch
Al-Otoum Business Center - Suite No. 205, Was Al-Tal St. No. 98, P.O. Box 961741 Amman 11196 Jordan
Tel.: +962 (6) 560 7822 /33 Fax: +962 (6) 562 0807
E-mail: sales@protei.me Web: www.protei.me