PROTEI Signaling Firewall

Universal solution for signaling networks protection

PROTEI

Why the need?

Within the past few years, more unconventional service providers such as MVNO's, Private LTE networks, mini-operators, VAS and roaming service hubs and content providers are entering the telecom market on both national and international levels. Such players will normally inter connect with existing operators and carriers, hackers and spammers found more ways to log onto the expanding SS7 and DIAMETER networks.

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 and DIAMETER traffic towards other networks and abusing standard SS7 and DIAMETER messages to track subscribers, remove/add service, deny access and even intercept calls and SMS's. Such cases highlighted the vulnerabilities in SS7 and DIAMETER standards and network elements, thus created the need of introducing dedicated systems with advanced SS7 and DIAMETER traffic monitoring and control capabilities.

Solving the Issues

Being experts in the field, PROTEI introduced an advanced Signaling Firewall. It is intended to help operators in monitoring, controlling and managing SS7 messages and DIAMETER traffic within mobile network.

PROTEI Signaling Firewall is designed to detect and handle both unexpected or unconventional SS7 messages and possible DAMETER-related attacks. Furthermore, and in order to assure full protection capabilities, PROTEI Signaling Firewall adopts the GSMA specifications (FS.11, FS.07, IR.70, IR.71, FS.19). Such functionality combination can guarantees the network protection from any fraud or attacks and prevents revenue loses.

PROTEI Signaling Firewall supports several network protection approaches: Monitoring and Alerting, Basic Policing Rules, Advanced Policing Rules.

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 or DIAMETER connection based on a wide range of filtering criteria.

Benefits

- Preventing Network oriented SS7 and DIAMETER attacks
- Preventing SS7 and DIAMETER attacks: Tracking, Identity theft, DoS (Denial of service)
- Built on standard and proven technology through live implementations
- Spamming and flooding
- Fraud generation
- Easley upgradable functionalities
- Installation over a virtual environment as VNF
- Flexible pricing model to meet budget expectations
- Dedicated Technical Architecture and Installation team
- 24x7x365 Support

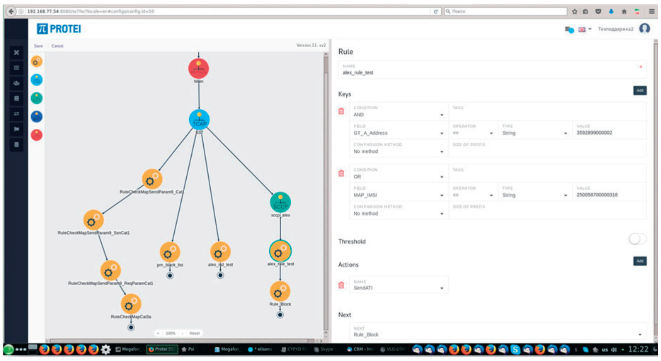
Protection levels

The system should be able to work on two levels:

- Connection level (limiting hosts and peers, connections may be established from);
- Application level (analyzing transactions and transaction parameters).

Features

- Compliance to GSMA Fraud and Security Group specifications (FS.11, FS.07, IR.70, IR.71, FS.19);
- Flexible routing management and policy management individually for each SS7 connection (PC or GT) or basing on the packet parameters for DIAMETER traffic (address information, packet type, application code, AVP values, location information etc);
- 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);
  - DIAMETER messages (Low-layer filtering, application layer filtering).
- SS7 anti-SPAM and Diameter anti-flooding functionality protecting the network from mass MSU sending with similar operation code or similar originator;
- Basic and advanced policy rules supporting;
- Network Addresses Masking functionality;
- Personalized Black and White Lists;
- Support GSM MAP phase I, II, III;
- Support HSL (2 Mbps SS7 links, G.703 Annex A);
- Supports SIGTRAN (M3UA and M2PA links);
- Fully compatible with ETSI GSM 03.40 and 03.38;
- 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 CDRs/EDRs as well as traffic handling KPIs as well as Grafana-based monitoring subsystem.



Rule

NAME: alex_rule_test

Keys

CONDITION: AND
FIELD: GT_A_Address | OPERATOR: == | TYPE: String | VALUE: 3592899000002
COMPARISON METHOD: No method

CONDITION: OR
FIELD: MAP_IMSI | OPERATOR: == | TYPE: String | VALUE: 250058700000316
COMPARISON METHOD: No method

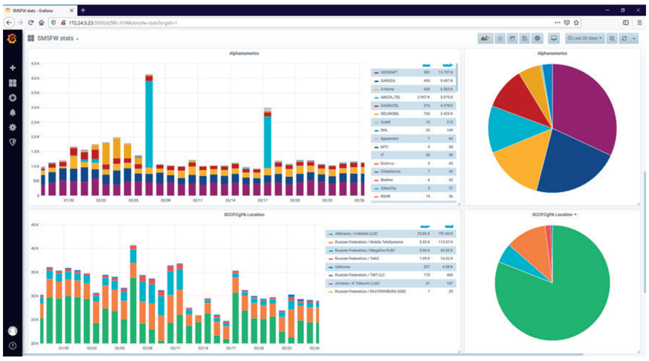
Threshold

Actions

NAME: SendATI

Next

NEXT: Rule_Block



	max	total
GOODNET	583	13.707 K
GARUDA	495	9.497 K
A-Home	428	6.363 K
ABAZA_TEL	2.957 K	5.075 K
GAGRATEL	316	4.578 K
DELIMOBIL	726	2.425 K
Gultel	15	213
DHL	25	169
bgoperator	7	64
MTC	9	58
IT	40	50
Drom.ru	5	45
ChitaiGorod	7	43
Beeline	6	42
ZdravCity	5	37
RSHB	15	36

	max	total
Abkhazia / A-Mobile LLSC	33.85 K	797.60 K
Russian Federation / Mobile TeleSystems	5.92 K	113.07 K
Russian Federation / MegaFon PJSC	5.04 K	54.02 K
Russian Federation / Tele2	1.09 K	16.02 K
Unknown	537	4.08 K
Russian Federation / TMT LLC	170	460
Armenia / K Telecom CJSC	51	107
Russian Federation / EKATERINBURG-2000	7	29

System Scalability

PROTEI Signaling Firewall is a carrier-class solution that can be scaled horizontally. Modulus structure of the platform allows flexible development and modernization by using identical connecting units for different configurations. Automatic configuration synchronization between modules is supported. Network based architecture additionally increases system reliability.

Throughput of the Interface subsystem – up to 1000 TPS

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.

PROTEI HQ

60A B.Sampsonievsky, Business Center «Telecom»
Saint-Petersburg, 194044, Russia Federation
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, Wasfi Al-Tal
St. No. 98, P.O. Box 961741 Amman 11196 Jordan
Tel.: +962 (6) 560 78 22/33 Fax: +962 (6) 562 08 07
E-mail: sales@protei.me Web: www.protei.me