



MOBILEUM

FIREWALL AND SECURITY SOLUTIONS



Why is security important?



52%

Of consumers would leave or consider leaving their operator because of a security breach



3rd

Most likely reason to churn.
After price and coverage



62%

Of consumers would want to use 2FA less, stop using or have an alternative

58%

Of enterprises would leave or consider leaving their operator because of a security breach

2nd

Most likely reason to churn.
After price

73%

Of enterprises would want to use 2FA less, stop using or have an alternative

Source 2017 and 2018 consumer and Enterprise survey by Mobile Squared (sponsored by Mobileum/EI)



What is the business case?

- Brand protection
- Regulation (or threat of)
- Churn
- Fraud
- Fines
- Revenue from legitimate access

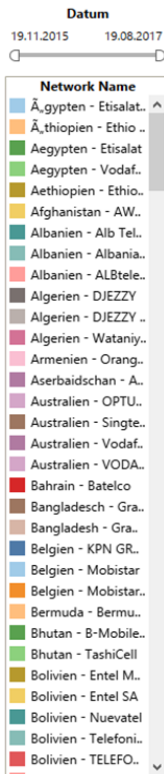
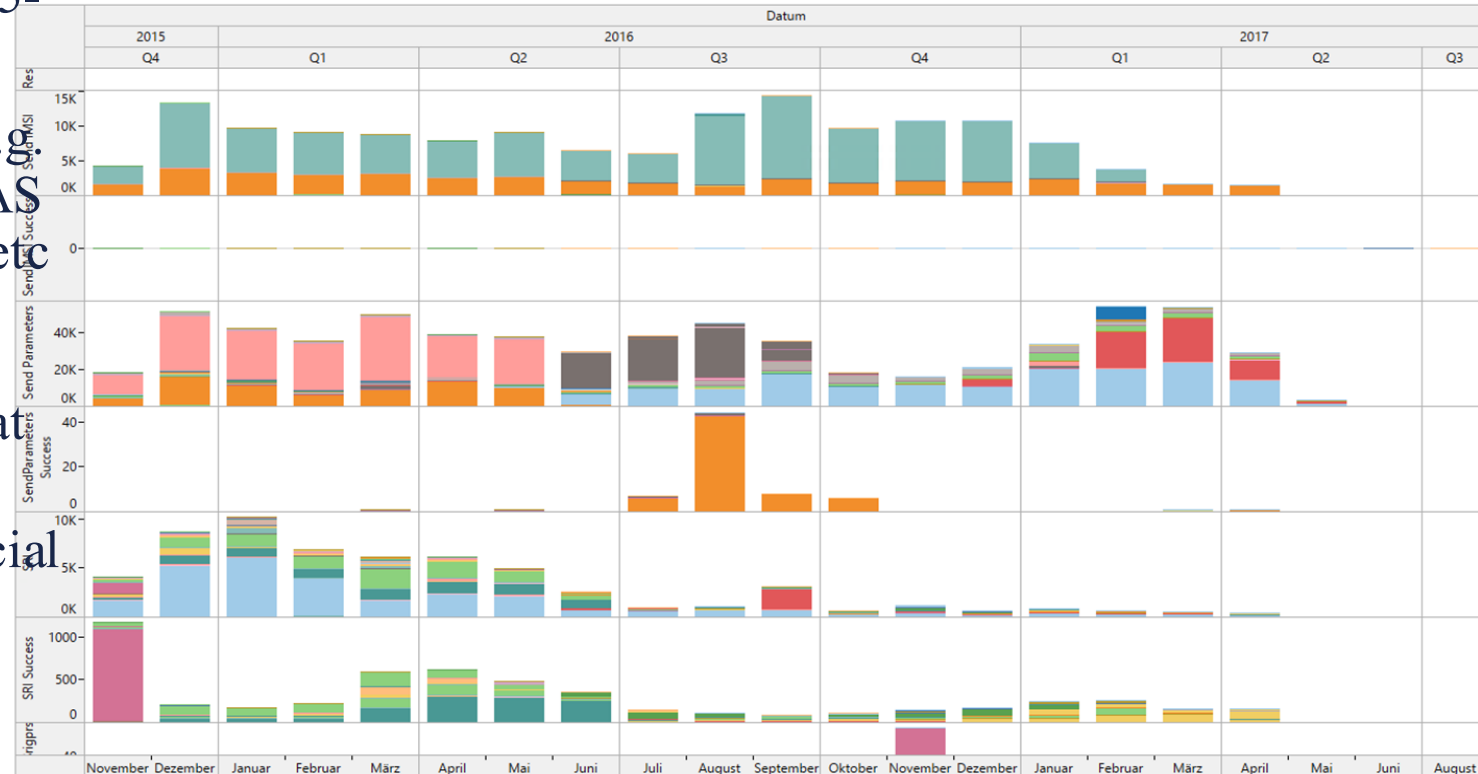


The threat is real and can be blocked

(DT before and after. Presented at FASG in 2017 in conjunction with DT)

SFW live

- Typical reported attacks 0.5-0.05%
- Many are false positives e.g. Hubs, shared networks, VAS mis-config, Anti-steering etc
- DT blocking ~0.02%
- Vast majority of attacks Can 1
 - ATI – Many commercial services
- Low volume of serious frauds
 - E.g. Fake LU



- Note – initially protected only home subscribers then added inbound roamers (see few attacks in Q2) (Risk of false positives until number plan of all roaming partners well understood)



Recent recognition



November 2017

Evolved Intelligence Signalling Firewall Wins Security Solution of the year

SS7 and Diameter Signalling Firewall received industry-wide recognition at the 2017 Global Telecoms Awards in London, picking up the award for Security Solution of the Year.



December 2017

New report names company as leading Signalling Firewall supplier.

Independent research by Telecom specialists Rocco Market leader for mobile network signalling security firewalls based on feedback from mobile operators worldwide.



**Winner 2018
Security Solution**

February 2018

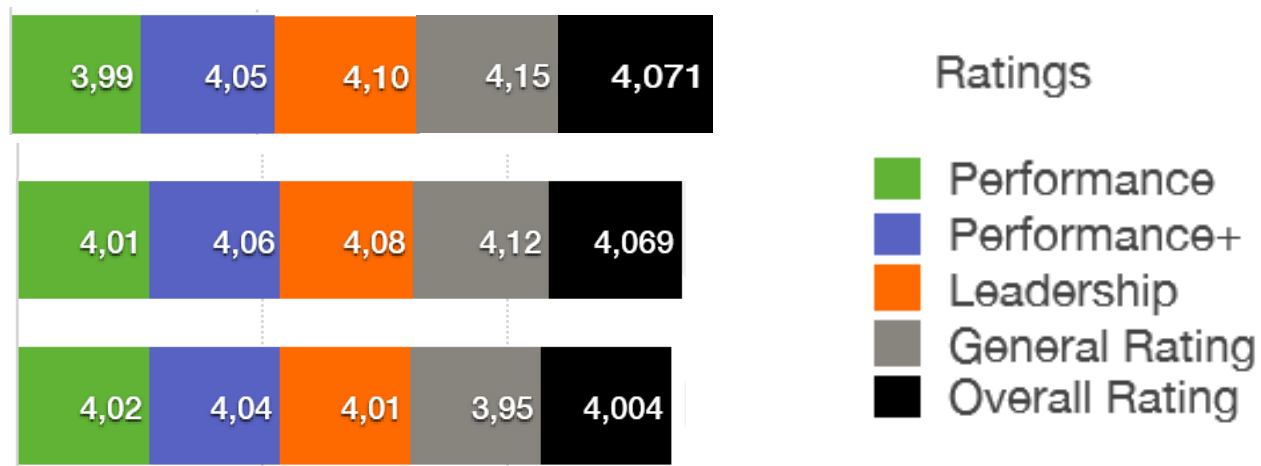
GSMA Mobile World Congress award

Firewall won Best Mobile Authentication & Security Solution award at 2018 Mobile World Congress in Barcelona



Snapshot from Rocco Report

Tier 1 Leader Board



MNO Feedback

“Excellent leader in Firewalls”

“The Number one vendor of SS7 Firewall”

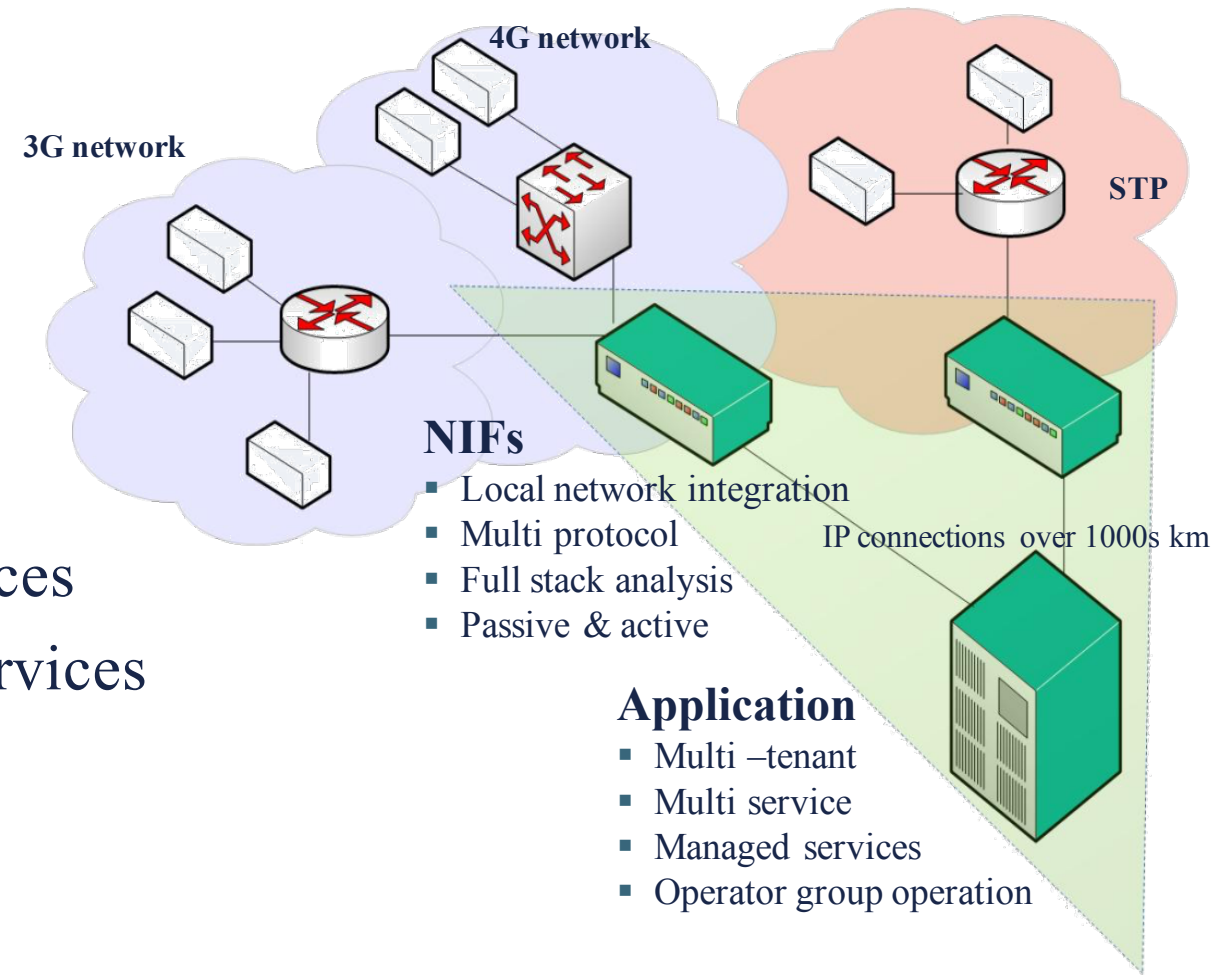
“Strong leadership in Signalling and Firewalls”

“They have a great reputation and we are always inspired with how much intelligence information they have”



Architecture

- Hybrid cloud architecture
 - › No need to choose between central/local
 - › Local integration. Central operation.
- Same architecture for roaming & security
- Inherently multi-tenant
- Same platform active/passive, 3G/4G, all services
- Ideal for groups, channel partners, managed services
- Hosting centres in UK
- Enables quick/remote deployment





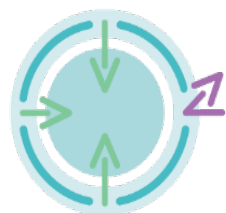
Firewall modules

Firewall Security Features



Insight

- Historic analysis of unusual signalling (e.g. scanning)
- Drill down to find new threats
- Tracking changes in behavior
- Reporting and searching
- Full signalling trace



Signalling Firewall

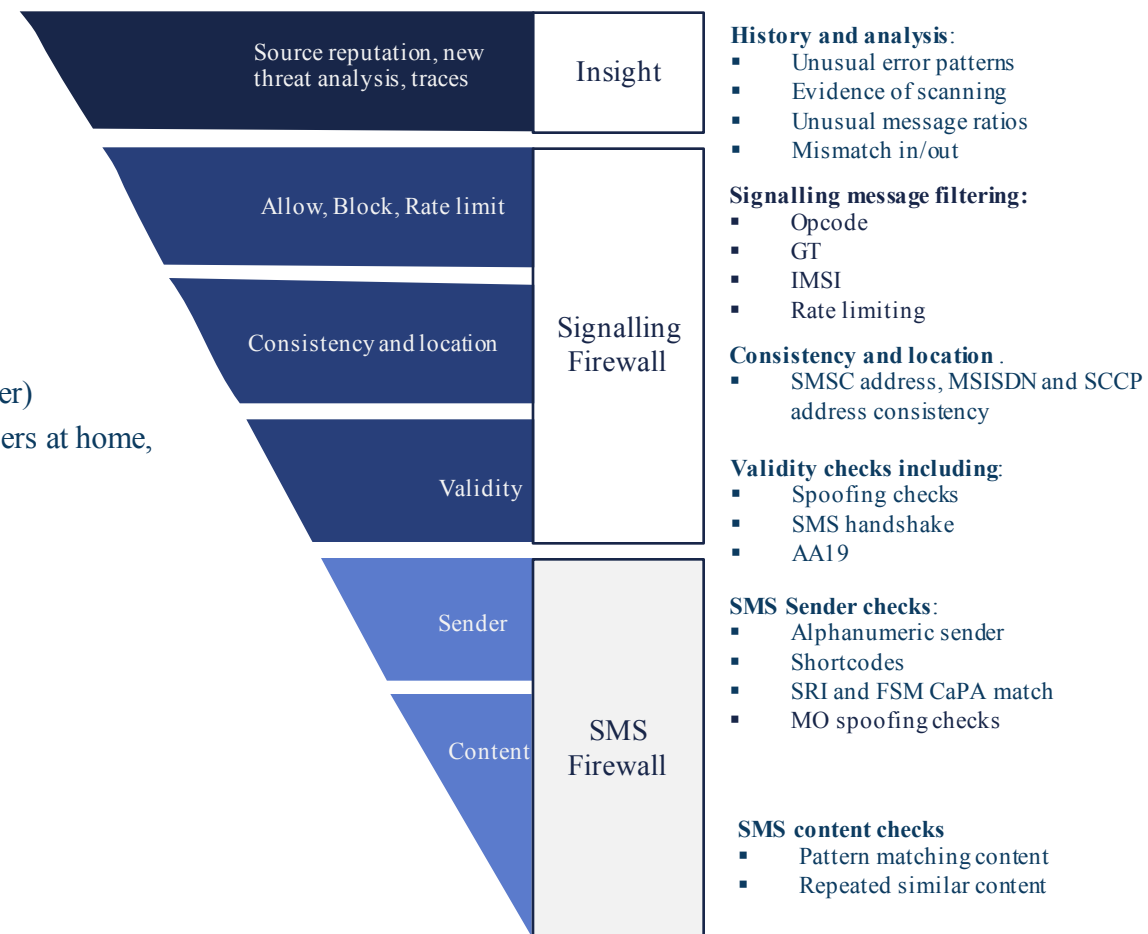
- Blocking suspicious opcodes/command codes, parameters and GTs
- Covers all threats identified by GSMA in FS11 (SS7) and FS19 (Diameter)
- Blocks category 1,2,3 threats (plus rate limiting, anti-spoofing, subscribers at home, configurable actions)
- Flexible blacklist, and whitelisting for real-world signalling
- Powerful UI with underlying rules engine



SMS Firewall

- Blocking suspicious SMS (content, senders)
- Detect and protect the bypass of the correct routes for A2P messaging and SMS spam

Signalling Firewall Screening Layers





Firewall rules (Full support for FS11/19)

Quarterly updates for GSMA identified threats and from customer sharing (reciprocity)

Expert and advanced rules

Cross protocol checks (e.g. CAP/MAP keys, SS7/Diameter location/attachement)
Validity checks. Expert rules – for regexp matching in UI

State, validity and history (Category 3)

Inter message and protocol consistency: location, velocity checks, AA19. Limit GT & opcode volumes.
E.g: UL velocity check, Purge from right location, Limit SRI_SM rate.

Consistency – Category 2 (Category 2)

Intra layer consistency and sender validation (for no reply messages). Validate if message from home network
E.g. ISD, IDR

Address rules (allow/block) (Category 0/1)

Default deny. Allow/block based on source, destination network/realm, opcode/command code ..
E.g.: SRI-SM from interconnect partner. ATI not allowed. ULR only from roaming partner.

INCREASING COMPLEXITY



Rich, powerful and easy to use functionality

- Extensive protocol support
 - › MTP, SCCP, TCAP, MAP, CAP, Diameter
- Powerful configurable rules:
 - › Configurable data items for rules
 - › Whitelists and blacklist message, source, destination and parameters/AVP
 - › Consistency checks – across signalling layers and against subscriber HPLMN
 - › Validity checks – against e.g. AA19, active IMSI
 - › History and state checks: Last location, velocity check
 - › Message rate limits per opcode/command code, source, subscriber
 - › Block on SMS source/text (SMS firewall rules)
 - › Watch, whitelist, blacklist on subscriber/VIPs
- Rich set of parameters for rules
 - › Opcode/command code
 - › Parameters/AVPs – e.g. SSN/node, application context
 - › Subscriber/IMSI/hostname
 - › Source/destination – i.e. GT or host/realm
- Configurable actions on rule

ID	Source	Destination	Traffic Type	Tags
0	roaming_partners Custom E.164	tenant Any E.164	MAP_locationCancellation MAP_cancelLocation	+
1	roaming_partners HPLM E.164	tenant SSN E.164	MAP_locationCancellation MAP_cancelLocation	+
2	roaming_partners HPLM E.164	tenant VLR E.164	MAP roamingNumberQuery MAP provideRoamingNumber	+
3	roaming_partners VLR E.164	tenant VLR E.164	MAP roamingNumberQuery MAP provideRoamingNumber	+
4	roaming_partners HPLM E.164	tenant VLR E.164	MAP_subscribeDeletion MAP resetSubscriberData	+
5	roaming_partners HPLM E.164	tenant SSN E.164	MAP_subscribeDeletion MAP resetSubscriberData	+
6	roaming_partners HPLM E.164	tenant VLR E.164	MAP_resetSubscriberData MAP resetSubscriberData	+
7	roaming_partners HPLM E.164	tenant SSN E.164	MAP_resetSubscriberData MAP resetSubscriberData	+
8	roaming_partners HPLM E.164	tenant VLR E.164	MAP_subscribeDeletion MAP resetSubscriberData	+
9	roaming_partners HPLM E.164	tenant SSN E.164	MAP_subscribeDeletion MAP resetSubscriberData	+
10	roaming_partners HPLM E.164	tenant VLR E.164	MAP_subscribeDeletion MAP resetSubscriberData	+
11	roaming_partners VLR E.164	tenant HPLM E.164	MAP_subscribeDeletion MAP sendParameters	+
12	roaming_partners VLR E.164	tenant HPLM E.164	MAP_subscribeDeletion MAP sendParameters	+
13	roaming_partners VLR E.164	tenant HPLM E.164	MAP_subscribeDeletion MAP sendParameters	+
14	roaming_partners VLR E.164	tenant HPLM E.164	MAP_subscribeDeletion MAP sendParameters	+

Allow Rule 2

ID: 2

Traffic Type: MAP

Source: RoamingPartners

Destination: Tenant

Number Plan: E.164

Number Plan: E.164

Source SSN: Custom

Destination SSN: Any

Application Context: MAP_locationCancellation

Application Context/Version: Any Version

Operation Code: MAP_cancelLocation

Comment: Allow Rule 2: From source HPLM to destination VLR with context MAP_locationCancellation for upgrade MAP_cancelLocation

Tags: + Create tag

Dependent Rules: consistency rule 1 validity rule 15

Buttons: Save, Cancel, Create

Check ServiceCentreAddress is the same as the calling party address

Enabled: ☒

Opcoodes: ☒ MAP sendRoutingInfoForShortMessage ☒ MAP reportSMDeliveryStatus

Rule Action: Drop

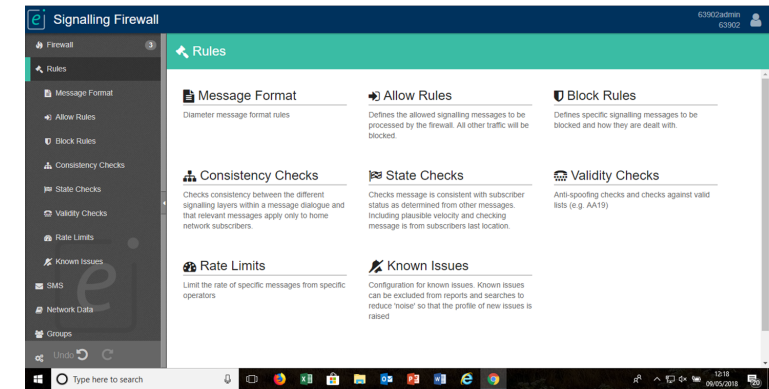
Applicability Criteria: None

Buttons: + Create tag



Managing firewalls in real life

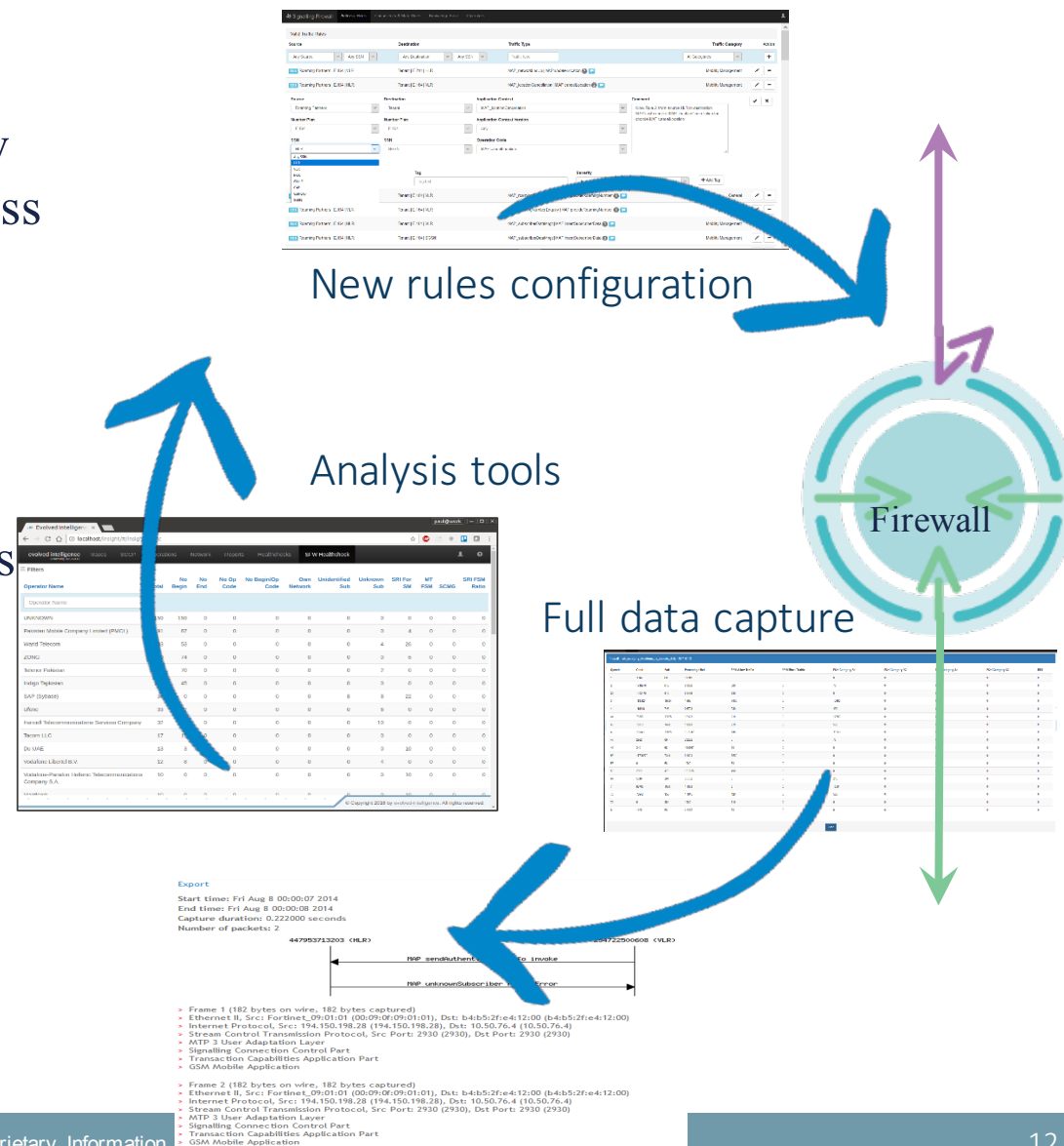
- Configured (and tagged) for FS11 and FS19 standard rules
 - › Reciprocity agreement – share real threats across customers and from our threat intelligence
- Experience of “wild” signalling.
 - › Maintaining accurate number analysis
 - › Roaming hubs, Late ISD, Pooled VLR, shared HLR
 - › Configured “out of the box” to avoid issues – but easy to edit with exceptions
- Screens to configure standard rules, data easily via UI
 - › Eg: Simple to add roaming partner
 - › E.g: Simple to add/block new routes
 - › E.g. Block, allow, monitor specific IMSI or GT
- Controlled rule introduction. No downtime (for rules or software upgrades)
 - › Eg: warn initially
 - › E.g. Rule versioning – save / revert / export
 - › E.g. Set of rules to implement together
 - › Eg: Rule dependencies displayed automatically, conflicts flagged etc
- Known issues can be filtered to find new sources
- Privacy / GDPR support
- Alerts (inbox/SIEM) on active attack source or IMSI attacked from multiple sources





Threat management methodology & requirements

- High functionality firewall delivered to protect against know threats (FS11,19 including protection at home, spoofing, cross protocol attacks etc – co-author of specs)
- Real world exceptions to avoid false positives (e.g. shared networks, hubs)
- Analytics to track, find new and drill down to details
- Operational tools to easily manage firewall (e.g. testing rules versioning)
- Easy to configure rules (direct from analysis)
- Threat intelligence from supplier and other operators (reciprocity – largest footprint)

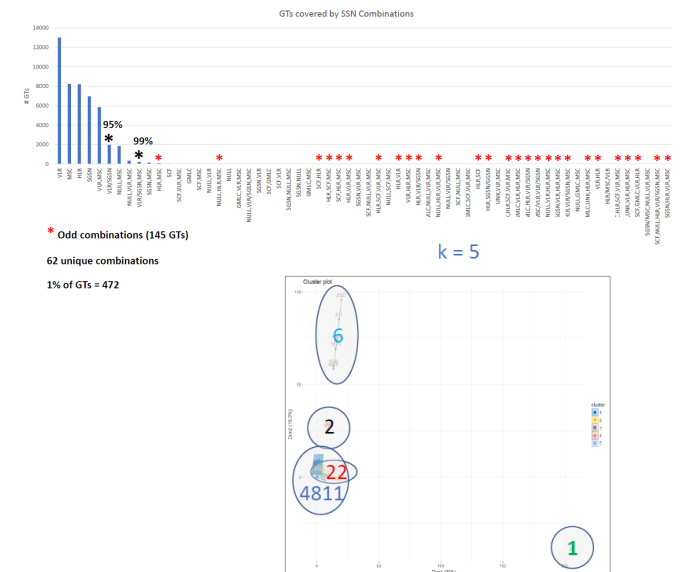
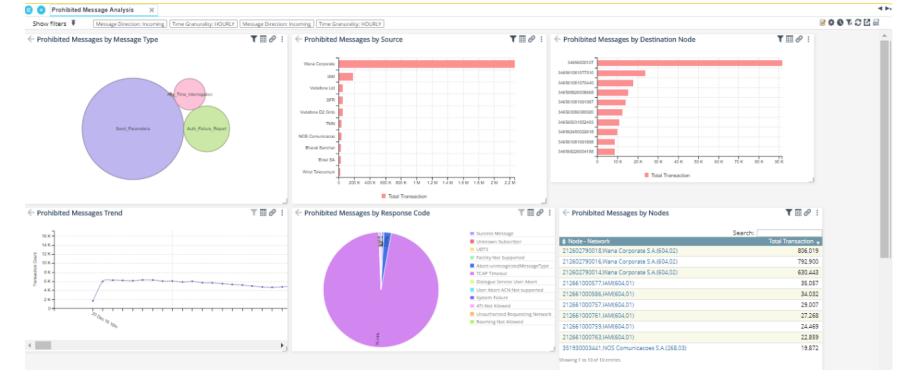




Threat analysis

- Reports on each attack / rule violation
 - › Trends, sources etc
 - › Link to signalling from each attack / rule
 - › Customisable visualisation
- Forensic analysis
 - › Reports and trends on sources, IMSIs
 - › Drill down to signalling (both directions)
- Scanning analysis
 - › Reports on unusual activity (e.g. many unknown sub)
- Suspicious GT analysis (e.g. cluster, SSN analysis)
 - › Wisdom as optional add-on. Will be integrated.

(Goal – add MNS graphics)





Summary

- Leading functionality, SS7 and diameter firewall
- Proven over last 2 years in tier 1 operators
- Full CAP/MAP/Diameter (GTP soon) cross protocol Cat 1,2,3 and more
- Practical and easy to manage for real world environment
- Analytics to track trends, sources and identify new threats



 **MOBILEUM**

Thank You