Cellusys®

GTP Signalling Firewall

Real-time Prevention and Detection of Attacks on Mobile Signalling Networks

Cellusys®

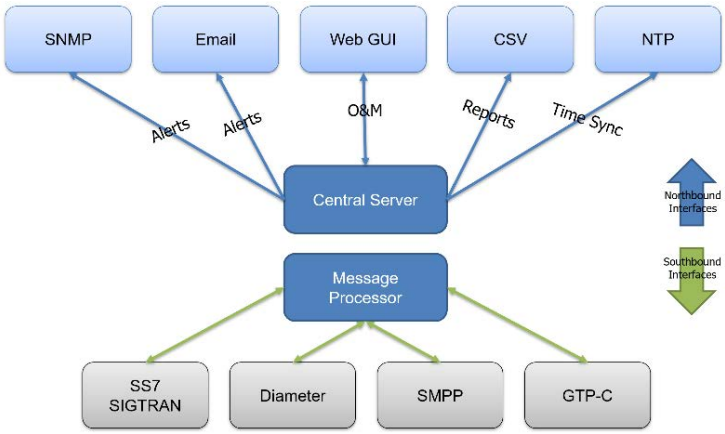
GTP Signalling Firewall

Overview

The unified Cellusys Signalling Firewall(1) system protects a mobile operator's network by sitting on its external links to other networks and filtering messages from reaching the network, ensuring threats from individual messages, flooding or other issues are prevented from reaching the network and causing issues. The unified firewall supports all relevant signalling protocols: SS7/SIGTRAN, Diameter, SMPP, GTP.

Benefits of the unified firewall:

- Consistent processing of rules over all protocols
- CAT1/2/3 checks in one firewall for all protocols
- Cross-protocol checks for complex threat scenarios
- MAP queries for location checks for all protocols (e.g. GTP Session Create).
- Common reporting over all incidents

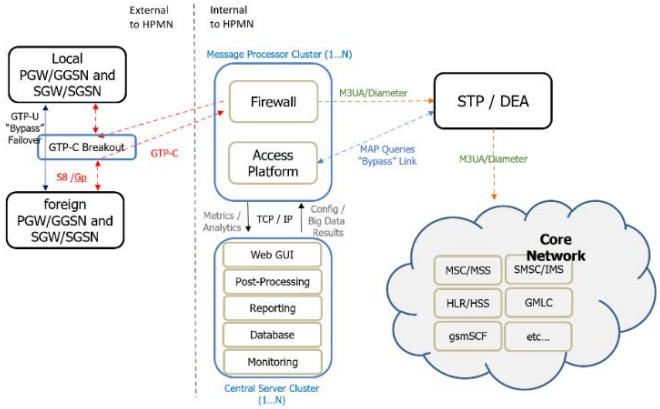


Features

GTP Firewall provides full control over the signalling stack from IP to GTP. Base for the GTP integration into the Cellusys Signalling Firewall is the GSMA FS.20 standard – with focus on roaming traffic. The Signalling Firewall will apply pre-defined (GSMA FS.20) and user-defined policies to this GTP-C traffic. As for all rules, they can be customized by the user using the same rule definitions known from SS7, Diameter etc. Every GTP-C parameter is exposed and available for query and policy enforcement. Due to internal correlation, each rule has access to relevant fields of the GTP-C messages even if the field is not present in the original message (such as IMSI in PDP-Context-Delete Messages).

As for all protocols, Cellusys Signalling Firewall can drop GTP-C packets, modify message attributes or generate error messages and return these to the message source. Also, it can rate limit messages from a given source / range of sources or on any message attribute. In order to apply additional checks, the firewall can send external queries to determine real subscriber location based on a source of GTP-C packet (CAT3).

In-line Architecture GTP-C



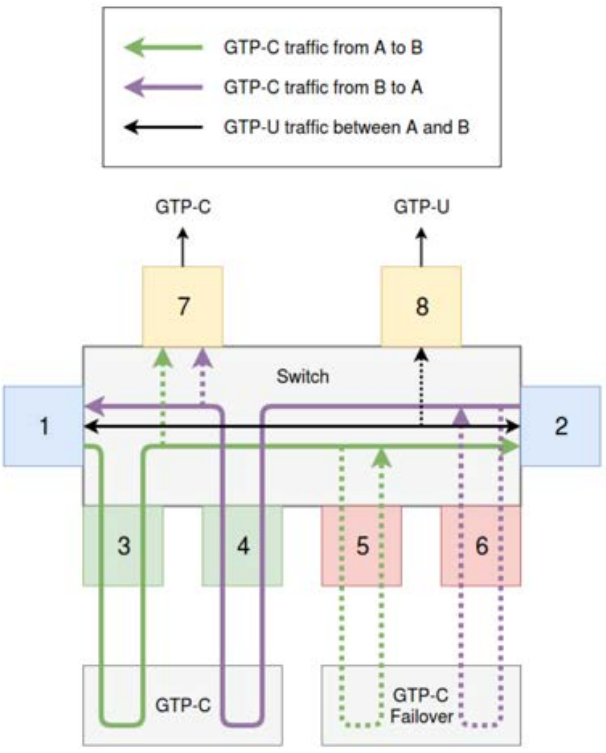
(1) https://www.cellusys.com/security-solutions/signalling-firewall/

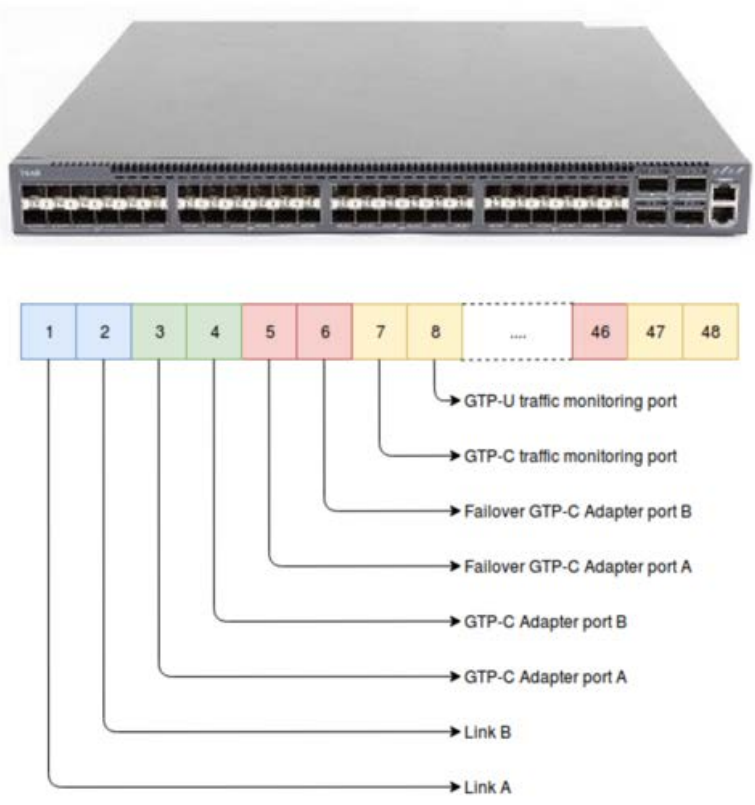
GTP Signalling Firewall

Network integration

Integration of GTP is done inline: physical links carrying roaming GTP traffic will be connected to the GTP firewall switch. Using BISDN-OS(2) as platform this switch extracts relevant GTP-C messages bidirectional and forwards them to the firewall message processor, while all other traffic is transparently bypassed. The integration supports all current physical interfaces using SFPs (100MBps – 100Gbps). Up to 8 links can be connected using one GTP firewall switch. Also mirror ports are available to connect other Cellusys products such as Mobile Broadband Monitoring. Permanent port monitoring of the GTP firewall switch supports switching to other firewall instances or completely bypass all traffic (transparent mode).

Specifically, due to the inline mode, no network configuration on PS nodes is required. This simplifies the integration dramatically.





(1) BISDN Linux Distribution, basebox.org

Cellusys®

Roaming | Security | Analytics

www.cellusys.com