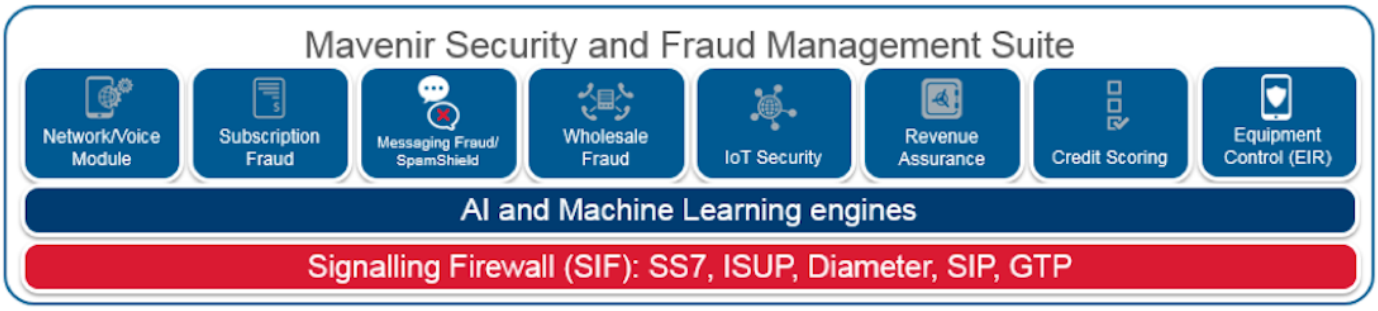
Signaling Firewall



SIGNALING FIREWALL: SS7, ISUP, DIAMETER, SIP, GTP

The mobile communication world has experienced a wide range of changes over the last decade. Innovations in handsets, applications and services required shifts in how the mobile operator runs the business. While attention was focused on moving to IP, addressing new business models, services, data monetization etc., the underlying industry technology was unknowingly vulnerable to security and privacy attacks.

Gaining access to mobile networks has always been a target for various attackers, but due to equipment complexity and specialization of the physical layer connectivity, mobile network infrastructure was essentially a closed environment. However, with the evolution towards an IP-based architecture, networks have become much more accessible and hackers' interest has surged.

Motivation behind attacks

Hackers are continuously developing new exploits for computers and mobile devices. They are looking for ways to get into the secure networks and gain access to information.

Mobile networks are no exception. While mobile handsets are generally secure when used carefully, the network itself can be an obvious target for exploitation. Information may be gained on subscriber's identity or location, voice calls or texts may be blocked, intercepted or eavesdropped, funds can be transferred between accounts, billing systems bypassed or even network level denial of service (DOS) attacks launched.

With DOS attacks, in the network signaling world, the intended result may very well be temporarily eliminating communications in a specific geographical area which would severely impact law enforcement, public services or key high value targets in the area.

Another aspect of Denial of Service attacks is related to end-users. In these cases, targeted mobile subscribers can become unknowing victims not realizing that certain services on their handsets are not functioning.

The Mavenir Signaling Firewall (SIF) offers mobile operators several capabilities to protect their subscribers by controlling Mobile Network Operators' SS7, Diameter, SIP and GTP signaling streams:

- Integrates as a dedicated entity to centralize all security activity
- Provides insight monitoring of Signaling flow, focusing on the interconnection networks
- Allows proactive prevention of attacks, detection of the sources
- Facilitates partnerships with other GSMA members
- Supports MNO's roadmap, including protection to LTE network through Diameter interface

The Signaling Firewall layer enables integration of various machine learning, anti-fraud modules into the network of mobile operator ensuring for real-time detection and blocking of fraud attempts and security issues.

Mavenir's Signaling Firewall implements the GSMA mitigation recommendations (FS.11 and FS.19) to detect and prevent the signaling-based attacks. In addition, it includes key, unique features specifically resulting from assessment results/insights of numerous mobile operator networks world-wide. These assessments have been performed either through passive traffic monitoring or intrusive attacks executed on request from mobile operators to understand issues in the networks, clearly indicating that almost all networks are vulnerable. Constant audits and managed services provide Mavenir customers with continuous improvements of the Firewall products ensuring protection from current and future threats.