TITANIUMPLATFORM.COM

TITAN.IUM

SIGNALING, ROUTING
AND SECURITY

Product Data Sheet

Signaling Firewall (SFW)

Business Benefits

- Multi-protocol protection in one product: SS7, Diameter and SIP.
- Message screening, barring, rate limiting, and SLA enforcement.
- Stateful protection against known and emerging threats.
- Protects against GSMA Fraud and Security Group defined attacks.
- Protects against Wangiri, IRSF, robocalling and other fraud types.
- Deployed on carrier-grade Titan.ium Titan platform and within Titan.ium ecosystem.

TITAN.IUM

Product Data Sheet

Signaling Firewall (SFW)

The Challenge

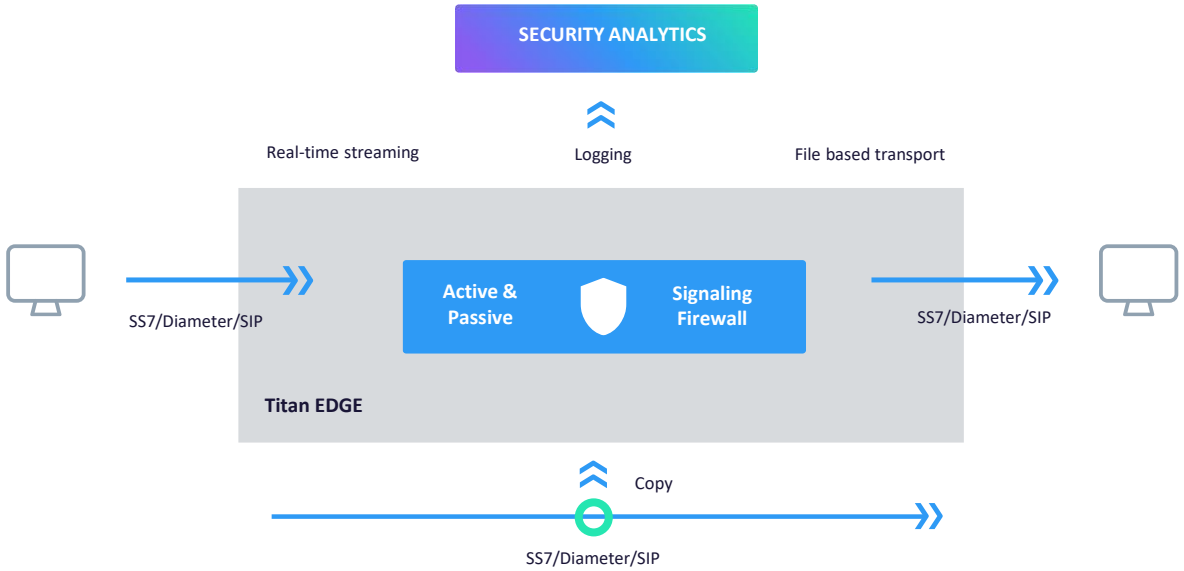
Experts have been warning for many years about SS7 security concerns and how SS7 can be abused to redirect calls, track locations, and capture text messages. SS7 is very slowly being replaced by newer signaling protocols like Diameter, but during this extended period of gradual migration, these security concerns remain.

The widespread adoption of Diameter and SIP does not mitigate against these concerns. Instead, they are amplified by the all-IP nature of these protocols, which has been shown to make them even more vulnerable to security exploits than SS7.

Add to this the growth of various forms of signaling derived revenue fraud and it becomes clear that operators need to deploy a highly secure signaling architecture that addresses not just these concerns, but also protects the network against new security threats that will inevitably emerge again and again

The Titan.ium Solution

Titan.ium's Signaling Firewall (SFW) provides a highly scalable, multi-protocol (SS7, Diameter and SIP) signaling firewall network element that can be used to protect operator network from a wide array of security threats.



Signaling Firewall can statefully monitor both individual protocol dialogs and cross protocol parameter congruency, allowing it to incorporate all available information when evaluating messages for plausibility, possible fraud and many other use cases.

Signaling Firewall is both deep and wide. Despite covering all SS7, Diameter and SIP, SFW can dive down and examine and operate upon any parameter of any message, even parameters in nested Diameter AVPs. Operations can include message screening, message modification and message rate limiting. These can be applied to all messages or to just specified messages. SFW can be configured to silently discard messages that are found to be outside of its provisioned rules, or to respond with a configurable error message. Taken together, these capabilities allow SFW to protect downstream network elements from overload, enforce SLA limits and protect against fraud.

Product Data Sheet
Signaling Firewall (SFW)

The Titan.ium Solution (continued)

Using information gleaned from its visibility across multi-protocol network signaling, Signaling Firewall can detect and protect against attack scenarios defined by the GSMA Fraud and Security Group (FASG). SFW can also be configured to detect and protect against Wangiri fraud and robocalling fraud.

With three highly flexible deployment models, Signaling Firewall can be deployed into almost any network topology, often without disruption to existing routing plans. SFW can be overlaid onto existing signaling elements, deployed in front of or behind existing nodes or can be integrated with other Titan.ium-supplied elements.

This is in fact a key advantage of Signaling Firewall. It can collocate its SS7, Diameter and SIP capabilities with other Titan.ium STP, DSC and SIP products on a common Titan platform and within a Titan.ium ecosystem, employing Titan.ium's dynamic service chaining mechanisms to provide truly integrated services. The resulting solution radically simplifies signaling, security, and routing in the network.

Titan.ium's Signaling Firewall allows operators to protect their networks from a wide variety of security and fraud threats, protecting both the network and its subscribers. This protection has the additional benefit of being future proof vs. static. SFW employs an incredibly flexible and highly configurable method for allowing operators to define the functions they want it to perform in the network. This flexibility provides operators with the tools they need to react quickly to any newly emerging threat, ensuring that their networks always remain protected and secure. Titan.ium's SFW protects networks now and into the future.

Key Capabilities

Multi-protocol Firewall
Signaling Firewall supports the following protocols:

- SS7
  - ✓ Variants: ITU-T, ANSI, Chinese, TTC (Japanese)
  - ✓ Transport: SCTP over IPv4 and IPv6 (SIGTRAN), E1/T1 LSL, E1/T1 HSL, ATM
  - ✓ Layer 2: M2PA, M2UA, MTP2
  - ✓ Layer 3: M3UA, MTP3
  - ✓ Higher Layers: SCCP, TCAP, MAP, CAP, INAP, ISUP
- SIP
  - ✓ RFC 3261 et al
  - ✓ Transport: SCTP, TCP and UDP over IPv4 and IPv6
- Diameter
  - ✓ RFC 6733 and RFC 6737
  - ✓ Transport: SCTP and TCP over IPv4 and IPv6

Fraud Detection and Protection
Using its dynamic message rate measurement capabilities, Signaling Firewall can detect and protect against various fraud types such as Wangiri and Robocalling.

Carrier Grade Platform
Signaling Firewall is a real-time security element built on Titan.ium's carrier grade, field-hardened Titan platform and the cloud-native Titan.ium ecosystem.

TITAN.IUM

Product Data Sheet
Signaling Firewall (SFW)

Key Capabilities (continued)

Message Screening
The Titan.ium Signaling Firewall allows operators to monitor, validate, and access-control SS7, Diameter and SIP messages in a comprehensive fashion (every message, every parameter). This allows SFW to be configured to detect and prevent fraudulent or malicious use of an operator's network.

Message Rate Limiting
Signaling Firewall can apply message rate limits in a highly configurable fashion to all SS7, Diameter and SIP messages, allowing it to enforce Service Level Agreements and protect upstream network elements. It can silently discard messages exceeding the defined rate or reply with an error message.

DESS Phase 1 Support
Signaling Firewall supports Diameter End-to-End Security (DESS) Phase 1, which verifies that essential parts of a Diameter request have not been modified on their transmission path.

Stateful Firewall
Signaling Firewall can inspect SS7 TCAP and Diameter dialogs in a stateful manner. This allows it to do such things as cross-protocol message parameter plausibility checking, subscriber velocity checking, and verifying that SS7 TCAP dialogs follow the standardized flow. Many other use cases are possible

GSMA Fraud and Security Group (FASG) Attack Protection
Signaling Firewall can protect in accordance with:
- GSMA FS.07 – "SS7 and SIGTRAN Network Security"
- GSMA FS.11 – "SS7 Interconnect Security Monitoring and Firewall Guidelines"
- GSMA FS.19 - "Diameter Interconnect Security"
- GSMA FS.21 - "Interconnect Signaling Security Recommendations"
- GSMA FS.38 – "SIP Network Security"

Flexible Deployment Models
Signaling Firewall can be deployed in several ways:
- Overlay Firewall – Signaling Firewall receives and controls network-selected messages.
- Front-end / Back-end In-line Firewall – Network messaging flows through Signaling Firewall.
- Integrated Firewall – Signaling Firewall is integrated with other Titan.ium signaling products like STP or DSC.

Contact Titan.ium Today
Please visit www.titaniumplatform.com for product or solution information. For configuration and pricing details, please contact your local account representative via sales@titaniumplatform.com

About Titan.ium
Titan.ium Platform is a leader in signaling, routing, subscriber data management, and security software and services.
Our solutions are deployed in more than 80 countries by over 180 companies, including eight of the world's top ten communications service providers and all of the top five. Titan.ium supports any network, domain, signaling protocol, and infrastructure with advanced routing capabilities and a unified end-user experience.

DISCOVER THE POSSIBILITIES.
INNOVATION AT YOUR FINGERTIPS