TITANIUMPLATFORM.COM

TITAN.IUM

SIGNALING, ROUTING
AND SECURITY

Product Data Sheet

SS7 Signaling Firewall (SS7-SFW)

Business Benefits

- Message screening, barring, rate limiting, and SLA enforcement.
- Protects against GSMA Fraud and Security Group defined attacks.
- Protects against IRSF, Wangiri, robocalling and other fraud types.
- Powerful and flexible rules engine allows operators to respond in real time to emerging threats.
- Deployed on Titan.ium's carrier grade Titan™ platform and/or Titan.ium™ framework.
- Same SFW product can also protect Diameter and SIP.

TITAN.IUM

Product Data Sheet

SS7 Signaling Firewall (SS7-SFW)

The Challenge

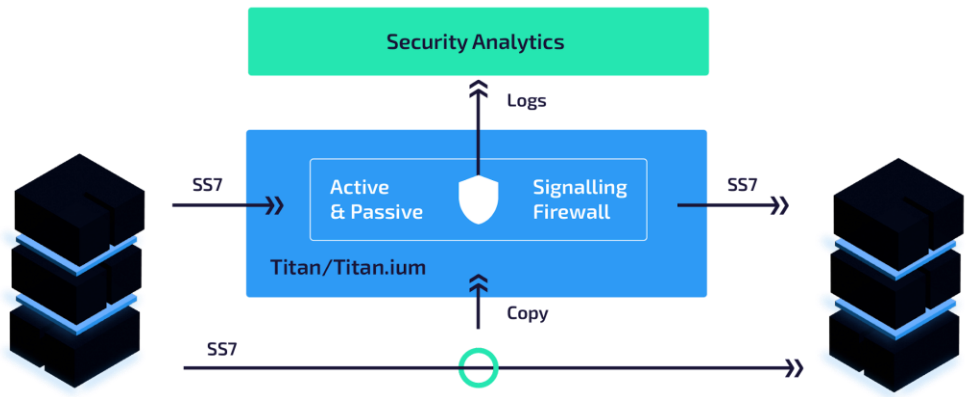
Industry experts have been warning for many years about SS7 security concerns and how SS7 can be abused to redirect calls, track locations, and capture text messages. SS7 is very slowly being replaced by newer signaling protocols like Diameter, but during this extended period of gradual migration, these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

These vulnerabilities are being exploited with vigor and determination by fraudsters worldwide, targeting both networks and their subscribers. This has driven the sustained growth of an ever-expanding set of signaling based fraud, saddling operators with enormous financial losses, lowered customer satisfaction (CSAT) and subscriber churn.

It is clear that operators need to secure their SS7 signaling architecture in a way that addresses not just these already well-known concerns, but also allows them to protect their networks in real time against newly emerging threats without having to wait for a vendor-provided solution.

The Titan.ium Solution

Titan.ium's SS7 Signaling Firewall (SS7-SFW) provides a highly scalable SS7 signaling firewall network element that can be used to protect operator networks and their subscribers from today's security threats as well as those that will inevitably emerge tomorrow. The same firewall can also protect Diameter and SIP. For more information, see the separate Diameter and SIP Firewall datasheets.



The SS7-SFW is more than just a rules engine that can implement the findings of a post processing Fraud Management System. Such systems can take hours or days to deliver meaningful findings. Operators cannot wait that long. During those hours and days, losses are mounting, damaging ROI, CSAT and customer retention. Operators need a security solution that can react intelligently in real time. SFW is that solution.

SS7-SFW's powerful rules engine, coupled with its innovative Dynamic Gauges and powerful message dissectors, allow it to dig deeply into the network signaling and detect fraudulent activity in real time. Once detected, the SS7-SFW can take immediate and assertive action such as blocking the fraudulent traffic or can take a more measured approach and log the findings for post analysis. The choice is up to the operator. Blocking the traffic stops losses before they mount. Logging the traffic allows for considered human oversight. A combination of the two may provide the best of both worlds and is fully supported.

TITAN.IUM

Product Data Sheet

SS7 Signaling Firewall (SS7-SFW)

The Titan.ium Solution (continued)

Despite covering all SS7, the SS7-SFW can dive deep, both examining and operating upon any parameter of any message, even parameters at the deepest levels of the protocol stack. Operations can be applied to all messages or just to messages meeting operator-specified criteria. The SS7-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 the SS7-SFW to defend against fraud, protect downstream network elements from DDOS attacks and/or simple overload, enforce SLA limits and more.

Using information gleaned from the monitored SS7 signaling, as well as the Diameter and SIP signaling that may be present on the same platform, the SS7-SFW can detect and protect against GSMA Fraud and Security Group (FASG) attack scenarios and can also be configured to detect and protect against a wide variety of other fraud types, including IRSF, various forms of bypass fraud, Wangiri, fraudulent robocalling and more.

With three highly flexible deployment models, the SS7-SFW 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.

Business Benefits

Titan.ium's SS7-SFW allows operators to protect their networks and subscribers from a wide variety of security and fraud threats. This protection comes with the additional benefit of being future proof vs. static. SS7- SFW's powerful and flexible rules engine allows operators to rapidly update the functions it is performing in the network. This provides operators with the ability to react quickly to any newly emerging threat, ensuring that their network remains protected and secure at all times. The SS7-SFW protects networks now and into the future.

Key Capabilities

Multi-protocol SS7 Firewall

SS7-SFW supports the following protocols:

- 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

Message Screening

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

Message Rate Limiting

SS7-SFW can apply message rate limits in a highly configurable fashion, allowing it to enforce Service Level Agreements, protect downstream network elements from DDOS attacks and from simple overload. Messages beyond the max rate can be logged and then discarded or responded to.

TITAN.IUM

Product Data Sheet

SS7 Signaling Firewall (SS7-SFW)

Key Capabilities (continued)

GSMA Fraud and Security Group (FASG) Attack Protection

The SS7-SFW 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.21 – "Interconnect Signaling Security Recommendations"

Real Time Fraud Detection

Using its dynamic rate gauges, message dissectors, location and number portability checks, all orchestrated by its powerful rules engine, the SS7-SFW can detect frauds such as IRSF, Bypass Fraud, Wangiri, Robocalling and more in real time.

Real Time Fraud Response

Under the control of its powerful rules engine, the SS7-SFW can react intelligently to detected fraud in real-time, before operator losses become significant. Operators can also deploy new rules in real time, allowing them to combat any emerging threat before it causes real damage.

Stateful Firewall

The SS7-SFW can inspect SS7 TCAP dialogs in a stateful manner. This capability extends to the Diameter and SIP signaling that may also be present on the same platform. This enables such things as cross protocol stack message parameter checking, plausibility checking, subscriber velocity checking, and verification that SS7 TCAP dialogs follow the standardized flow. Many other use cases are supported.

Network Function Concentration

The SS7-SFW can be collocated with other Titan.ium products on a common platform (Titan or Titan.ium), employing Titan.ium's dynamic service chaining mechanisms to provide truly integrated services. This solution can radically simplify signaling, security, and routing in the network.

Flexible Deployment Models

The SS7-SFW 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