TITANIUMPLATFORM.COM

TITAN.IUM

SIGNALING, ROUTING
AND SECURITY

Product Data Sheet

Diameter Signaling Firewall (DIA-SFW)

Business Benefits

- Message screening, barring, rate limiting, and SLA enforcement.
- Protects against GSMA Fraud and Security Group defined attacks.
- 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 SS7 and SIP.

TITAN.IUM

Product Data Sheet

Diameter Signaling Firewall (DIA-SFW)

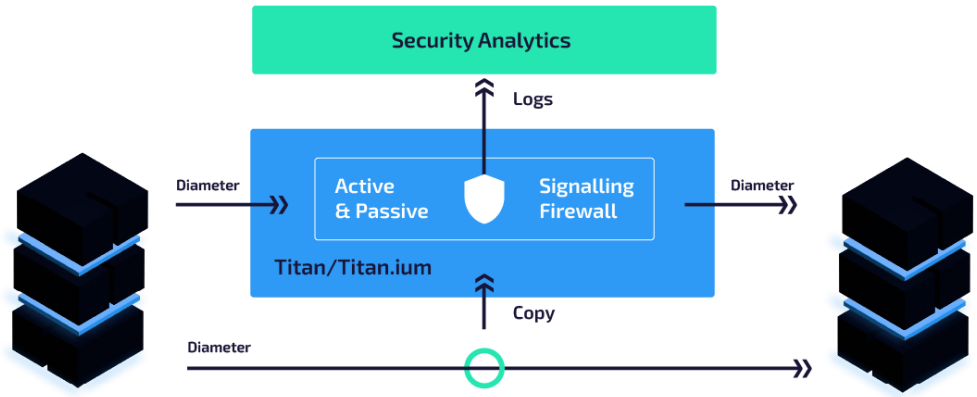
The Challenge

Industry experts have been sounding the alarm for some time about the security vulnerabilities of the SS7 protocol widely used as the signaling basis for fixed and mobile (2G/3G) networks. The emergence of 4G has not reduced the level of alarm. It is true that 4G has driven widespread adoption of Diameter and SIP as the new primary signaling mechanisms for mobile networks. However, rather than resolving signaling security concerns, this has amplified those concerns, driven by the all-IP nature of Diameter (and SIP). This has been shown to make Diameter even more vulnerable to security exploits than SS7. Fraudsters worldwide are creatively and vigorously exploiting this fact.

In response, operators need to secure their Diameter signaling architecture in a way that addresses not just already known concerns, but also protects their networks in real time against newly emerging threats in a manner that allows them to react in real time without waiting for a vendor-provided solution.

The Titan.ium Solution

Titan.ium's Diameter Signaling Firewall (DIA-SFW) provides a highly scalable Diameter 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 SS7 and SIP. For more information on this, see the separate SS7 Firewall and SIP Firewall datasheets.



Many networks deal with security issues by fielding a CDR and event-based post processing Fraud Management System (FMS) which then relies on a rules engine to implement its findings. However, Titan.ium's DIA-SFW is more than just a rules engine to implement FMS decisions. Such systems can take hours or days to deliver meaningful findings. Operators cannot afford to wait that long. During those hours and days, losses are mounting and ROI, CSAT and customer retention are being damaged. Operators need a security solution that can react intelligently in real time, not just implement history-based FMS decisions. DIA-SFW is that solution.

DIA-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, DIA-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.

TITAN.IUM

Product Data Sheet

Diameter Signaling Firewall (DIA-SFW)

The Titan.ium Solution (continued)

Despite covering all of Diameter, the DIA-SFW can dive deep, examining and operating upon any parameter of any message, even parameters in deeply nested Diameter AVPs. Operations can include message screening, message modification, message rate limiting and more. These can be applied to all messages or just to messages meeting operator-specified criteria. The DIA-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 DIA-SFW to defend against fraud, protect downstream network elements from TDOS/DDOS attacks and/or simple overload, enforce SLA limits and more.

Using information gleaned from its visibility across all of Diameter, as well as across SS7 and SIP signaling that may also be present on the same platform, DIA-SFW can detect and protect against attack scenarios defined by the GSMA Fraud and Security Group (FASG), along with specific protections tuned to local network conditions.

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

Business Benefits

Titan.ium's DIA-SFW 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 versus static. SFW employs an incredibly flexible and highly configurable way of 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 remain protected and secure at all times. Titan.ium's DIA-SFW protects networks now and into the future.

Key Capabilities

Multi-protocol Diameter Firewall

- RFC 6733 and RFC 6737
- Transport: SCTP and TCP over IPv4 and IPv6

DESS Phase 1 Support

DIA-SFW supports Diameter End-to-End Security (DESS) Phase 1, critical technology that verifies that essential parts of Diameter messages have not been modified on their transmission path.

Message Screening

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

Message Screening

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

TITAN.IUM

Product Data Sheet

Diameter Signaling Firewall (DIA-SFW)

Key Capabilities (continued)

Message Rate Limiting

DIA-SFW can apply message rate limits in a highly configurable fashion to all Diameter 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.

GSMA Fraud and Security Group (FASG) Attack Protection

Signaling Firewall can protect in accordance with

- GSMA FS.19 - "Diameter Interconnect Security", Category 1, 2 and 3
- GSMA FS.21 - "Interconnect Signaling Security Recommendations"

Real Time Fraud Detection

Using its dynamic rate gauges, message dissectors and location and number portability checks, all orchestrated by its powerful rules engine, DIA-SFW can detect security and fraud issues in real time.

Real Time Fraud Response

Under the control of its powerful rules engine, DIA-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 emerging threats before they can cause real damage.

Stateful Firewall

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

Network Function Concentration

DIA-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

DIA-SFW can be deployed in several ways:

- Front-end / Back-end In-line Firewall – Network messaging flows through Signaling Firewall.
- Integrated Firewall – SFW is integrated with other Titan.ium signaling products like the 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