

Oracle Communications EAGLE Network Security

During all times network security will remain as the key business concern for any communication service provider. As they look to interconnect and provide multiple services to their customers, newer security use cases can be identified. With interconnects, more fragile points can be leveraged by the network hackers to seek entry into the network. A greater variety of telephony providers offering service and convergence of SS7 with next generation architectures have created the need for Operators to be more vigilant in their efforts to secure networks and services. The industry is moving rapidly to secure the network boundaries from rogue interconnect partners, as researchers expose service providers publicly. Traditionally SS7 networks have been trust based networks working on trust between different service providers. Recently this trust has been compromised by hackers getting access to the SS7 networks and breaching the trust by fraudulent calls, robo calling, messaging fraud. This has caused service providers to rethink their network security and begin implementing access control at their network boundaries. Oracle Communications Network Security solution is an immaculate way to mitigate all those risks arising from both known and unknown factors.

Key Business Benefits

- Integrated with signaling platform, lowers maintenance costs, higher reliability
- Ability to mitigate security risks from external and internal sources
- Competitive advantage
- Customer privacy and loyalty
- Robust business and operations environment
- Real time monitoring and observability into the network nodes functionalities.

BEST PRACTISE USE CASES

- **Target all layers**

Develop security policies targeting all layers; IP transport, network routing and management (MTP), non-circuit related (SCCP), circuit related (ISUP), and Mobile Applications Part (MAP).

- **Create white lists**

Create policies that are highly restrictive to allow authorized traffic based on origination, destination, message type and operation. White lists only allow traffic that is listed, all other traffic is blocked. Blacklists may be used to apply policies to messages that were allowed using ranged white lists.

- **Gateway STP's**

Deploy Gateway STP's as the point of interconnect to screen and filter all incoming network traffic. Restrict access allowed for all interconnected networks, do not give unlimited access.

- **Monitor for threats**

Service providers need to continuously evaluate, monitor and mitigate security risks, as they roll out newer technologies. The ability of monitoring incoming network traffic and proactively detect abnormal behaviors that could affect network performance, service QoS or high value subscribers is essentially an overall security strategy.

Key Features

- Advanced filter and screening integrated with signaling platform
- Flexible "chaining" of filters to create very precise security policies
- Security policies at all protocol layers: MTP, SCCP, TCAP and MAP
- Filter and screen on all SCCP calling party and called party parameters
- Integrated monitoring

EAGLE NETWORK SECURITY

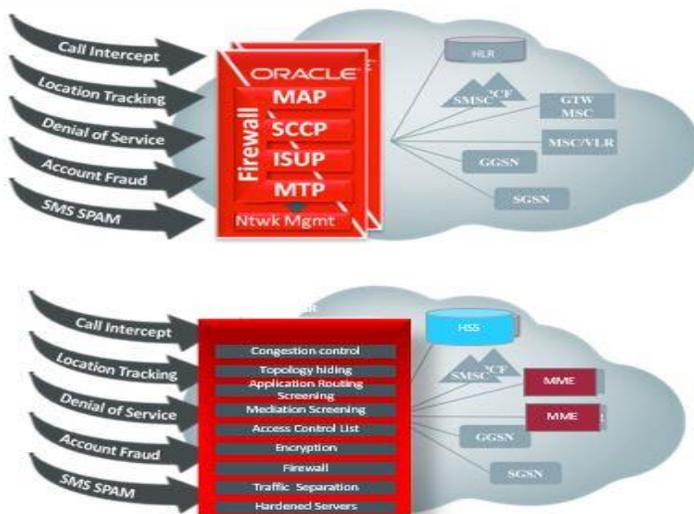


Figure 2. Oracle Communications Network Security

EAGLE ideal for Service providers requiring gateway STP's with sophisticated routing and screening capabilities. Powerful and flexible multi-layer security policies target messages at MTP, SCCP, ISUP and MAP protocol layers.

EAGLE/s security solution allow service providers to create filters within Gateway Screening and SCCP/GTT modules. The ability to connect or "chain" filters together results in very specific policies, filtering traffic based on origination, destination, services accessed and even the operations requested from a service.

Oracle Communications Solutions

- Oracle Communications Policy Management.
- Oracle Communications DSR
- Oracle Communications Policy Control Function (PCF)
- Oracle Communications Common Signaling, Security and Edge Protection Proxy (SEPP).
- Oracle Communications Common Signaling, Network Repository Function (NRF).
- Oracle Communications Common Signaling, Unified Data Repository/ Unstructured

Gateway Screening functions as the primary firewall application, applying security policies on all messages before being distributed internally for further processing or routed externally.

The System Connection Control Part (SCCP) is an internal module that translates parameters within received messages to determine and insert a destination address for a network service (e.g. HLR, Free Phone, VLR). SCCP procedures allow a single network address to be published enabling access to multiple network services, effectively hiding the topology of the internal network, applying filters and screening rules enhances the ability to manage access to network services, giving greater control over who has access and what operations are allowed.

Data Storage Function (UDR /UDSF).

- Oracle Communications Common Signaling, Service Communication Proxy (SCP).
- Oracle Communications Common Signaling, Binding Support Function (BSF).
- Oracle Communications Common Signaling, Interworking and Mediation Function (IWF).
- Oracle Communications Common Signaling, Network Exposure Function (NEF).

MONITORING FOR SECURITY THREATS

EAGLE with Oracle Communication's Next Gen Performance Intelligent Center (PIC) delivers the unique advantage of network monitoring that is tightly integrated with the EAGLE signaling platform. The latest GUI provides unmatched ease of controlling and taking corrective measures accordingly. Administration systems takes advantage of this relationship, allowing sharing of much of the network setup data (e.g.linksets, link set names, etc.) easing the burden of administering the monitoring system.

PIC delivers real-time traffic alarms, usage statistics and performs detailed key performance indicator (KPI) metrics to detect new security issues so that the appropriate EAGLE screening rules may be applied.

EAGLE SIGNALING SOLUTIONS

Networks world-wide rely on EAGLE as the platform of choice for providing robust and reliable signaling solutions. With an impressive share of the global STP market EAGLE has become the most widely deployed platform in the industry. Strong R&D efforts backed by Oracle's industry expertise and stability ensures EAGLE's continued success, delivering features and functionality assuring service providers their investments will be viable for years to come.

SUMMARY

Oracle Communications solutions enable service providers to both manage and monetize the explosive growth in mobile data traffic and multimedia applications. They help service providers analyze subscribers' quality of service, set policies to improve customer experience and optimize network performance.

Oracle Communications helps billions of people, devices and machines intelligently connect and engage over any network. With proven capabilities, scalable solutions, network security, common intelligent signaling platform, Oracle Communications solutions guarantees high availability and continued support.

CONNECT WITH US

Call +1.800.ORACLE1 or visit [oracle.com](https://www.oracle.com).

Outside North America, find your local office at [oracle.com/contact](https://www.oracle.com/contact).

 blogs.oracle.com/oracle

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 1119

 | Oracle is committed to developing practices and products that help protect the environment

ORACLE®

