ORACLE DATA SHEET

EAGLE

Network Security

ORACLE COMMUNICATIONS

Network security is a key concern for service providers as they interconnect networks and provide universal services to their subscribers. 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 wide range of end-user devices that can now connect to the telecom networks adds to the complexity. The industry is moving rapidly to secure the network boundaries from rogue interconnect partners, as researchers expose service providers publicly. Service providers may do little vetting of their interconnect partners, resulting in “open" networks accessible to nefarious actors. This has caused service providers to rethink their network security, and begin implementing access control at their network boundaries.

SECURITY BEST PRACTICES

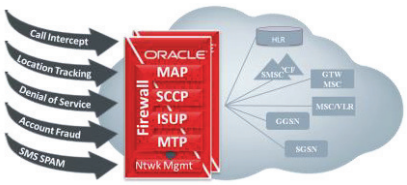
- Deploy Gateway STP/s at all points of interconnect.

  Restrict access for all interconnected networks.
- Security policies targeting all layers of the protocol.
- Utilize white lists, be very restricted in allowing traffic.
- Continuously monitor for security threats.

Best Practices

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.



Gateway STP - central point of entry into network

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 Application 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 particular messages that were allowed using ranged white lists.

Monitor for threats

Service providers need to continuously evaluate, monitor and mitigate security risks, especially as they roll out new technologies. The ability to monitor incoming network traffic and proactively detect abnormal behaviors that could affect network performance,

ORACLE

service QoS or high-value subscribers is essential an overall security strategy

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
- Customer loyalty
- Robust business and operations environment

KEY FEATURES

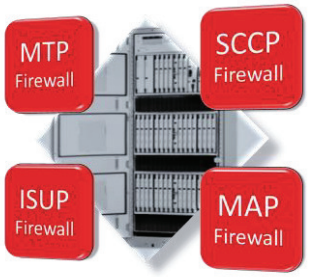
- Advanced filter and screening integrated with signaling platform.
- Flexible "chaining" of filters to create very precise security policies.
- Security policies at all protocol layers; MTP, SCCP, TCAP and MAP.
- Filter and screen on all SCCP calling party and called party parameters.
- Integrated monitoring

RELATED SERVICES

The following services support Oracle Main Product:

- Product Support Services
- Professional Services

EAGLE Network Security



Securing at all layers

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 particular service.

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.

The parameters utilized for filtering within both the Gateway Screening module and the SCCP module are depicted within the following tables.

GATEWAY SCREENING

MTP	SCCP
Allowed Origination Point Code	Allowed Calling Party Address
Blocked Origination Point Code	Allowed Translation Type
Allowed Calling Party Address	*Allowed Called Party Address*
Allowed Signaling Information Octet	*Allowed Affected Point Code (SCCP Management)*
Allowed Destination Point Code	
Allowed Affected Destination Field (Network Management)	
Allowed ISUP Message Type	

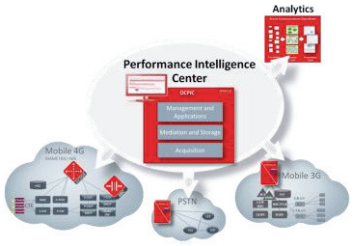
SCCP/TCAP/MAP FILTER PARAMETERS

SCCP Originating Parameters	SCCP Destination Parameters	TCAP/MAP
Linkset Name	Global Title Indicator	Operation Code
[Global Title Indicator	Translation Type	IMSI

Translation Type	*Numbering Plan*	*MSISDN*
Numbering Plan	*Nature of Address*	*VLRNb*
Nature of Address	*Calling Party Addr Digits*	*SMRPOA*
Called Party Addr Digits	*Calling Party Addr SSN*	*SMRPDA*
Called Party Addr SSN	*Calling Party Address Point Code*	
OPC	*DPC*	

Monitoring for Security Threats

EAGLE with Oracle Communication's Performance Intelligent Center (PIC) delivers the unique advantage of network monitoring that is tightly integrated with the EAGLE signaling platform. Administration systems takes advantage of this relationship, allowing the sharing of much of the network setup data (e.g. linksets, linkset names, etc) easing the burden of administering the monitoring system.



Network monitoring and analytics

PIC delivers real-time traffic alarms 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 52% 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.

EAGLE worldwide deployment

CONTACT US

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services