

Signaling Defense®

THE CHALLENGE

To ensure your network is sufficiently protected during this era of significant change

In this era of widespread interconnection and SS7-IP convergence, a carrier's signaling network—one of their most critical assets—is increasingly at risk of experiencing incidents that can disrupt customer service or compromise customer data.

The table below highlights several incidents that have occurred on different networks despite Gateway Screening, typically a carrier's first line of signaling defense, being deployed on the carrier's SS7 network. The names of the carriers who experienced the incidents have been omitted to maintain their anonymity.

Description of Actual SS7 Network Incidents	
Carrier A	A partner unintentionally sent excessive test messages into Carrier A's network causing an MSC to fail which resulted in disruption to thousands of customers.
Carrier B	Had a database mined in order to obtain sensitive customer information.
Carrier C	Received malformed messages that could not be processed by multiple network elements causing the nodes to stop providing service to customers.
Carrier D	An interconnect partner, in violation of their interconnect agreement, sent an excessive number of database queries into Carrier D's network causing congestion that impaired the ability of Carrier D's subscribers to complete calls.

Whether unintentionally or maliciously caused, each of the incidents had a negative effect on the carrier's customers, operations and/or financial performance, and each could have been prevented had the carrier had more comprehensive packet inspection and message control capabilities actively protecting their SS7 network, capabilities that Gateway Screening does not provide.

Instead, Gateway Screening provides only Partial Packet Inspection and Basic Message Control, an approach to network security that does not provide sufficient protection and risk mitigation against today's ever-increasing risks.

The table below summarizes Gateway Screening's core functionality and key weaknesses.

Gateway Screening's Core Functionality and Weaknesses	
Partial Packet Inspection	Only the "lower layer" elements of each SS7 message are inspected (MTP3, parts of SCCP), allowing the content and function-rich "upper layer" elements (TCAP, MAP, ISUP, etc.) to enter a carrier's network without being examined.
Basic Message Control	Messages can either be allowed or blocked; there are no advanced control capabilities such as message thresholding, re-routing, modification and response.

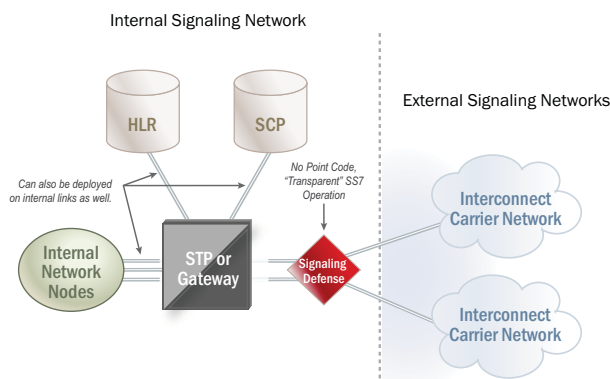
THE SOLUTION

Ensure you have Comprehensive Perimeter Control with Signaling Defense

In contrast to Gateway Screening, Sevis' **Signaling Defense** provides *Comprehensive Perimeter Control* over every message that enters or leaves your signaling network. Signaling Defense accomplishes this through the use of Deep Packet Inspection and Advanced Message Control (see table), with policy creation aided by decision support (visibility) tools and a centralized management system.

Signaling Defense resides atop Sevis' *Signaling ASE® Platform*, a "transparent" SS7 element that does not require an SS7 point code or any SS7 network re-engineering to install. While often situated on SS7 carrier-to-carrier interconnect links to ensure the integrity of a carrier's network perimeter, Signaling Defense can be positioned on any internal signaling link as well (for example SCP, HLR, Switch or BSC links). This flexibility enables a carrier to enhance their message control capabilities at any point in their network, including the "Access Edge."

Signaling Defense's Core Functionality and Strengths	
Deep Packet Inspection	Ensures that both the lower and upper layer elements of every signaling message are examined and evaluated according to user-customized network access and control policies that are centrally managed.
Advanced Message Control	Enables carriers to allow or stop questionable messages as well as perform advanced signaling message control functions to include message thresholding, syntax checking, re-routing, modification, offloading and response.



Comparison of Gateway Screening and Signaling Defense Capabilities		
Capability	Gateway Screening	Signaling Defense
MTP 3 header inspection	✓	✓
SCCP header inspection	Partial	✓
Message type inspection	Varies	✓
SCCP content inspection		✓
TCAP content inspection		✓
MAP content inspection		✓
ISUP content inspection		✓
Protocol conformance/syntax		✓
Decision support tools		✓
Reside on any signaling link		✓
Advanced message control		✓

The Architecture:

One platform, no point code, many solutions

Each Sevis solution utilizes Sevis' patented **Signaling ASE® System**, a proven, carrier-grade system that enables both Sevis and partner-developed applications to be deployed without an SS7 point code, thus eliminating the need for operators to re-engineer their signaling network upon installation and allowing any ASE-enabled solution to operate independent of a carrier's existing vendor infrastructure.

The ASE System is comprised of the ASE Platform (the "transparent" SS7 network element) and the ASE Manager. The ASE System is the cornerstone of all of Sevis solutions, and once deployed it can be the foundation to help you address other needs in addition to network security and risk mitigation to include controlling SMS spam (*SMS Defense*), enhancing fraud control (*Active Fraud Eliminator*) and resolving network interoperability issues (*Network Mediator*).



The ASE platform and ASE architecture

Technical Specifications: Carrier-grade, high availability, flexible

Protocols

ANSI

- T1.111 MTP
- T1.113 ISUP
- T1.112 SCCP
- T1.114 TCAP
- AIN 0.1/0.2
- IN
- ANSI-41 D
- WIN

ITU/ETSI/3GPP

- Q.701 – Q.705, Q.707 MTP
- Q.761 – Q.764 ISUP
- Q.711 – Q.714 SCCP

- Q.771 – Q.774 TCAP
- Q.721 – Q.724 TUP
- INAP CS-1/CS-2
- GSM MAP
- CAMEL

Sigtran

- M3UA
- M2PA

Application

- SMPP
- SS7oIP

Platform Specifications

Chassis

- 2 U high, rack-mountable chassis
- 19" (482.6 mm) or 23" (584.2 mm) rack mount
- Packet switching backplane
- 3 trunk interface module slots
- Up to 12 T1/E1s per platform
- Up to 48 transparent low speed SS7 links per chassis
- Up to 3 transparent ATM high speed links per chassis
- Chassis clustering
- Alarm status display module
- Telco alarm interface (dry/wet contact relay)

- 5 10/100 Base-T Ethernet ports
- Hardware/software status reporting

Power Supplies and Fans

- N+1 redundancy
- Hot swappable
- DC (-48V)
- A and B DC power feed

Trunk Interface Module

- Up to four T1/E1s
- Up to 16 transparent low speed SS7 links
- Up to 1 transparent ATM high speed link
- A, B, C, D, E, F links
- Channel associated signaling
- T1/E1, RJ-48C
- Hot swappable
- 3 10/100 Base-T Ethernet ports
- Drop and insert grooming
- Automatic link protection
- LED status indicators
- Rear transition module

Regulatory Compliance

- NEBS Level III certified
- ETSI 300 019 2-1 to 2-4
- CE
- FCC Part 15, Class A (CSA)

Temperature Range

- Operating: -5°C to +55°C (23°F to 131°F)
- Storage: -40°C to +70°C (-40°F to +158°F)

Management Server

Architecture

- Centralized client/server
- Dual processor
- RAID 5
- Hot-plug hard drives
- Hot-plug redundant power supplies
- Java-based GUI client

Event Management

- Event filtering with audible event notification
- Hardware/software status reporting

Performance Management

- CPU and memory utilization monitoring
- Link status monitoring
- Detailed platform/server statistics

Security Management

- User-configurable multi-level security access
- User authentication and activity timeout
- Encrypted management interfaces

The Company: Helping carriers protect their revenue, subscribers and network

Sevis Systems helps communications service providers protect their revenue, subscribers and network through innovative signaling solutions. Founded in 1999, Sevis is an employee owned and operated company that is headquartered in Plano, Texas. Sevis' solutions have been purchased by some of the largest service providers in the world and are resold by globally-recognized equipment suppliers including Alcatel-Lucent. To find out more about Sevis and our unique solutions, please call us at **877.517.3847** or visit our website at **www.sevis.com**. We look forward to working with you.