SECURITY TARGET

FOR

SONUS TRUNKING SUITE (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS)

RELEASE V09.00

Evaluated Assurance Level: 2+

Document No. 1744-000-D010

Version: 1.0, 20 July 2012

Prepared for:

Sonus Networks, Inc.

4 Technology Park Drive

Westford, Massachusetts

USA, 01886

Prepared by:

Electronic Warfare Associates-Canada, Ltd.

1223 Michael St., Suite 200

Ottawa, Ontario

K1J 7T2

AMENDMENT RECORD SHEET

Rev.	Issue Date	Description	Author	Reviewer
0.1	12 September 2011	Initial draft for Sonus review	R. Starman	M. Gauvreau
0.2	2 October 2011	Updated draft – submitted for registration	R. Starman	T. MacArthur
0.3	28 November 2011	Incorporated CSEC comments	R. Starman	----
0.4	29 November 2011	Incorporated CSEC and Sonus comments	R. Starman	----
0.5	19 December 2011	Address outstanding items	R. Starman	----
0.6	12 March 2012	Changes to incorporate Evaluator observations and align ST with ADV document	R. Starman	----
0.7	22 March 2012	Minor edits for improved internal consistency, including corrected document number.	R. Starman	----
0.8	18 June 2012	Incorporated Sonus feedback, revised TOE version, and improved alignment with ADV document	R. Starman	----
0.9	26 June 2012	Incorporated additional Sonus feedback of 21 June 2012.	R. Starman	----
0.91	28 June 2012	Updated Section 1.7 to reflect latest documents	R. Starman	----
1.0	20 July 2012	Added FIPS certificate numbers, removed extraneous application notes and references, and added tested software versions of the TOE.	R. Starman	----

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Target of Evaluation (TOE) specified in this Security Target (ST) is the **Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS)**, **Release V09.00**.

The TOE is a packet telephony trunking suite that provides full integration between a packet infrastructure and a Public Switched Telephone Network (PSTN). The TOE is comprised of the following network elements:

- Insight Element Management System (EMS);
- GSX/NBS 9000 High-density Media Gateway Open Services Switch (GSX);
- Policy and Routing Server (PSX);
- SGX4000 SS7 Signaling Gateway (SGX); and
- DataStream Integrator Call Data Record Translation Engine (DSI).

1.1 DOCUMENT ORGANIZATION

This document is structured as follows:

- **Section 1 - Introduction** provides the ST reference, the TOE reference, the TOE overview and the TOE description.
- **Section 2 - Conformance Claims** describes how the ST conforms to the Common Criteria and Packages. This ST does not conform to a Protection Profile.
- **Section 3 - Security Problem Definition** describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.
- **Section 4 - Security Objectives** defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition
- **Section 5 - Extended Components Definition** defines the extended components which are then detailed in Section 6.
- **Section 6 - Security Requirements** specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.
- **Section 7 - TOE Summary Specification** describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.
- **Section 8 - Other References** identifies reference documents beyond the TOE guidance documentation listed in Section 1.7 (p. 27) that are either referred to directly in this Security Target or aid in better understanding the TOE and the application of its technology.

1.2 SECURITY TARGET REFERENCE

This document, version 1.0, dated 20 July 2012, is the ***Security Target for the Sonus Trunking Suite (GSX/NBS 9000, SGX 4000, PSX, DSI, EMS), Release*** **V09.00**.

1.3 TARGET OF EVALUATION REFERENCE

The Target of Evaluation for this Security Target is software-only, comprised of the software components identified in Table 1.

Table 1: TOE Identification Details

Application / Network Element	Software Version	Hardware ID[1]
Sonus Trunking Suite comprised of the following:	Release V09.00	N/A
• Insight Element Management System (EMS)	Release V09.00.00A201	N/A
• GSX/NBS 9000 High-density Media Gateway Open Services Switch (GSX)	Release V09.00.00A203	N/A
• DataStream Integrator Call Data Record Translation Engine (DSI)	Release V09.00.00A201	N/A
• Policy and Routing Server (PSX)	Release V09.00.00A200	N/A
• SGX4000 SS7 Signaling Gateway (SGX)	Release V07.03.06R008	N/A

1.4 TERMINOLOGY AND ACRONYMS

1.4.1 Terminology and Acronyms

1.4.1.1 Terminology

Where practicable, this document uses telecommunication terms consistent with the standardized vocabulary for 3GPP specifications defined in **[3GPP TR 21.905]** (see p. 100 for details). For ease of reference, important terms (e.g., "*subscriber*", etc.) have been extracted from **[3GPP TR 21.905]** and included here.

The following terminology is used in this ST:

Attack Potential	The Attack Potential of an attacker to the TOE or latent vulnerability in the TOE is a function of the attacker's expertise, resources and motivation. Sections B.3 through B.5 of the Common Criteria's *Common Methodology for Information Technology Security Evaluation* (CEM) (version 3.1, revision 3 final dated July 2009) provide guidance to developers and evaluators on how to assess Attack Potential.
Call Data Record	CDR - See Charging Data Record
Charging Data Record	A Charging Data Record (CDR) is a formatted collection of information about a chargeable event (e.g. time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and

[1] The TOE is intended to run on specific hardware that is part of the IT operational environment. Hardware specifics are described at Section 1.5.5 on page 15.

	accounting. For each party to be charged for parts of or all charges of a chargeable event a separate CDR shall be generated, i.e. more than one CDR may be generated for a single chargeable event, e.g. because of its long duration, or because more than one charged party is to be charged. Source: **[3GPP TR 21.905]**
Darkgray POLICER	Darkgray POLICER on the GSX Ethernet Network Interface (NIF) provides protection against Denial of Service (DoS) and Distributed Denial of Service (DDos) attacks. Darkgray (or default peer) policing applies to packets that are not white-listed (received from a known peer), not black-listed (received from a known attacker), and not evaluated under a lightgray policer. Source: p. 3-143 **[GSX Ops Guide]**
DataStream Integrator Call Data Record Translation Engine	DataStream Integrator Call Data Record Translation Engine (DSI) provides a full range of services to efficiently manage network usage data for all of a carrier's needs. The DSI is an advanced data translation engine that is used to collect, correlate, and produce a standards compliant billing stream according to customer specific services and billing usage criteria, founded on the raw call accounting records produced by Sonus network elements. DSI also provides a standards-based service for delivery of the billing stream to 3rd party billing systems specified by Sonus' customers. DSI supports generation of Automatic Message Accounting (AMA) standard billing streams from the GSX network element. Sources: **[DSI Admin Guide]**, p. 1-1, **[GSX Ops Guide]**, p. 1-6
Discard Rate	Within the Sonus Trunking Suite, an attack is recognized by an excessive packet discard rate (of various packet types). Once recognized, these attacks are announced through major or minor alarms. Packet discard rate thresholds and durations are defined by the TOE for recognizing an attack and as well for recognizing a cessation of the attack, which is also announced via the alarms.
Discard Rate Profile	The act of discarding a packet triggers the threshold and duration monitoring actions that are configured in a Discard Rate Profile. A Discard Rate Profile is assigned to each major or minor alarm. The alarm may be associated with a particular server module, or with the entire system. When a (Discard Rate Profile) threshold is met and a discard rate (or higher) is maintained for a prescribed duration, an associated alarm triggered. That alarm is cleared when a lesser threshold is met and that discard rate (or lower) is maintained for a prescribed duration.
DSI	DataStream Integrator Call Data Record Translation Engine
EMS	Insight Element Management System
GSX	See GSX/NBS 9000 High-density Media Gateway Open Services Switch
GSX/NBS 9000 High-density Media Gateway Open Services Switch	High density Packet Telephony Gateway (switch) that provides SONET (synchronous optical networking) and Ethernet interfaces to the packet environment. Source: **[GSX Ops Guide]**

M3UA	MTP3 User Adaptation Layer - M3UA provides an interface to MTP3 (Message Transfer Part Level 3, the signaling network layer of SS7), allowing ISUP (ISDN[2] User Part) information to be carried over IP links. M3UA runs over Stream Control Transmission Protocol (SCTP). Source: **[SGX Ops Guide]**, p.1 -5
M3UA – ASP Link	The SGX4000 supports M3UA links to Signal Transfer Points (STPs) that provide the signaling gateway function in addition to the STP signaling transfer function. For an SGX local node, one M3UA– Application Service Provider (ASP) link exists from each CE to each STP SGP (Signaling Gate Process). Each M3UA– ASP link needs a corresponding signaling transport (SIGTRAN) SCTP association, and the link is assigned to the association. There is a one-to-one relationship between each link and an association. Source: **[SGX Ops Guide]**, p.1 -5
M3UA – ASP Linkset	The SGX4000 SS7 Signaling Gateway supports M3UA links to STPs that provide the signaling gateway function in addition to the STP signaling transfer function. The M3UA – ASP links from an SGX local node to an STP SGP will belong to an M3UA – ASP Linkset. The linkset must be created before the signaling link can be created. Source: **[SGX Ops Guide]**, p.1 -6
M3UA – SGP Link	The SGX4000 SS7 Signaling Gateway communicates with GSXs over SIGTRAN M3UA. The links from the SGX to the GSX are called M3UA – SGP links. Each M3UA – SGP link needs a corresponding SIGTRAN SCTP association, and the link is assigned to the association. There is a one-to-one relationship between each link and an association. Source: **[SGX Ops Guide]**, p.1 -6
Management Network Adapter	The Management Network Adapter (MNA) is an Ethernet network interface (NIF) used by the TOE GSX network element for management traffic.
Media Gateway Control Part	Media Gateway Control Part (MGCP) Source: **[3GPP TR 21.905]**
MGCP Softswitch	A Media Gateway Control Protocol (MGCP) soft switch may replace the Policy and Routing Server (PSX) and SGX4000 SS7 Signaling Gateway (SGX) elements of a GSX network. Source: **[GSX Ops Guide]**, p. 1-6
Netconf	Network Configuration Protocol (Netconf) is defined by an Internet Engineering Task Force (IETF) request for comments (RFC) **[RFC 4741]** that provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages.
Packet Telephony Gateway	The device that interconnects the PSTN and PBXs across a packet infrastructure. These switches provide connectivity between circuit-switched and packet environments for voice, data and fax transmission.

[2] ISDN – Integrated Digital Services Network

	Source: **[GSX Ops Guide]**
Parameter Interchange Format	The TOE GSX network element utilizes a binary parameter interchange format (PIF) file to provide persistent storage of all administrative values. The PIF file captures a snapshot of the current configuration and is used to restore a GSX's configuration during reboot. There is one binary PIF file for each GSX, and a backup of that file. The binary parameter file and the backup is written to the mass storage device for that GSX and stored in the GSX System Tree. This constitutes, in effect, the "archive" of a GSX's configuration. Source: Adapted from p. 2-9 of **[GSX Ops Guide]**
Point Code(s)	Signaling points are identified uniquely using their point codes. At each signaling point in the SS7 network, signaling messages are identified, processed and routed for distribution using the routing label of a message. This label consists of the following: • Destination Point Code (DPC) field: Point code of the destination switch in SS7 Signaling messages. • Originating Point Code (OPC) field: Point code of the originating switch in SS7 Signaling messages. • Signaling Link Selection (SLS) field: Used to select a signaling link for routing (see page 5 for additional detail). **[SGX Ops Guide]**, p.1 -5
PSX	Sonus Policy and Routing Server
Policy and Routing Server	The Sonus Policy and Routing Server (PSX) provides a central database of service, routing, and call treatment for one or more GSXs.
Service Provider	A Service Provider is either a Network Operator or another entity that provides services to a Subscriber Source: **[3GPP TR 21.905]**
SGX	See SGX4000 SS7 Signaling Gateway
SGX4000 SS7 Signaling Gateway	The SGX4000 SS7 Signaling Gateway (SGX) provides connectivity between one or more GSXs and the Signaling System 7 (SS7) network for circuit switched call routing and services. Integrated SS7 link termination allows the GSX to serve as the physical interface point connecting the GSX directly to the SS7 signaling network Source: **[GSX Ops Guide]**
Signal Transfer Point	A Signal Transfer Point (STP) is where a message received on one signaling link is transferred to another link.
Signaling Connection Control Part	The Signaling Connection Control Part (SCCP) provides additional functions to the message transfer part (MTP) for both connectionless and connection-oriented network services to transfer circuit-related and non-circuit-related signaling information between switches in the SS7 network.
SS7 Signaling Link Selection	The signaling link used to route the call is determined by the value of the *Signaling Link Selection* (SLS) field. The SGX software uses the SLS field to select the particular link from a linkset and to control load sharing. The MTP layer of the software dynamically assigns the SLS to the active link in the linkset. Source: **[SGX Ops Guide]**, p.1 -7
Stream Control	Stream Control Transmission Protocol (SCTP). SCTP is a connection-

Transmission Protocol	oriented protocol that runs on IP. SCTP guarantees in-sequence delivery within each stream. Source: **[SGX Ops Guide]**, p.1 -6
SUA	SUA is a SIGTRAN term that stands for *SCCP (Signaling Connection Control Part) User Adaptation Layer*. SUA provides an interface to SCCP, allowing user part signaling messages (e.g., TCAP[3] and RANAP[4]) over IP links. SUA runs over SCTP. Source: **[SGX Ops Guide]**, p.1 -6
Subscriber	A Subscriber is an entity that is engaged in a Subscription with a service provider. The Subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorized to enjoy these services, and also to set the limits relative to the use that associated users make of these services. Source: **[3GPP TR 21.905]** Note that Subscribers are not users of the TOE. The TOE transports subscriber's telephony and media packets from interconnected telecommunications peers to other connected peers across the TOE, but Subscribers do not have access to the TOE Security Functions (TSF).
Subscription	Subscription describes the commercial relationship between the Subscriber and the Service Provider. Source: **[3GPP TR 21.905]**
TCAP	TCAP (Transaction Capabilities Part) is specified in the ITU-T Q.771 to Q.775 series of specifications to define a standardized mechanism for telephony services to exchange information across a network.
Telecommunications Service Provider	A Telecommunications Service Provider (TSP) is the owner/operator of the TOE. The TSP deploys the TOE in its telecommunications infrastructure to provide packetized voice and multimedia services to its Subscribers.
Terminal	A device into which a universal integrated circuit card (UICC) can be inserted and which is capable of providing access to 3GPP System services to users, either alone or in conjunction with a UICC. Source: **[3GPP TR 21.905]**
Terminal Equipment	Terminal Equipment (TE) is equipment that provides the functions necessary for the operation of the access protocols by the user. Source: **[3GPP TR 21.905]**

1.4.1.2 Acronyms

The following acronyms are used in this ST:

3GPP	3rd Generation Partnership Project
AC	Alternating Current
ADS	Active Directory Services (Server)
AES	Advanced Encryption Standard
ALOM	Advanced Lights-out Management
AMA	Automatic Message Accounting
ANSI	American National Standards Institute

[3] TCAP - Transaction Capabilities Part

[4] RANAP - Radio Access Network Application Part

API	Application Programming Interface
ASMONIA	Attack analysis and Security concepts for MObile Network infrastructures, supported by collaborative Information exchange (see http://www.asmonia.de)
ASP	Application Service Provider
ASX	Sonus Access Server
ATM	Asynchronous Transfer Mode
CA	Certificate (Certification) Authority
CAN	Circuit Network Adapter
CAS	Channel Associated Signaling
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCS	Common Channel Signaling
CDC	Call Data Channel
CDR	Call Data Record
CE	Computing Element
CIC	Circuit Identification Code
CLI	Command Line Interface
CNS	Circuit Network Server
CPC	Calling Party's Category
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
DC	Direct Current
DDoS	Distributed Denial of Service
DER	Distinguished Encoding Rules
DLP	Data Leak Prevention
DoS	Denial of Service
DPC	Destination Point Code
DSI	Sonus DataStream Integrator Call Data Record Translation Engine
DSL	Digital Subscriber Line
DVD	Digital Video Disk Digital Versatile Disk
EAL	Evaluation Assurance Level
EMS	Sonus Insight Element Management System
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GB	Gigabyte
GETS	Government Emergency Telecommunications Service
GHz	Gigahertz
GNA	Gateway Network Adapter
GSX	Sonus GSX/NBS9000 High-density Media Gateway Open Services Switch
GUI	Graphical User Interface
H.323	ITU-T Recommendation H.323 (Packet-based multimedia communications systems)
HA	High Availability
HMAC	Hash Message Authentication Code
HPC	High Probability of Completion
HTTPS	Hypertext Transfer Protocol Secure

IAM	Initial Address Message
ID	Identification
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
ILOM	Integrated Lights-out Management
IMX	Sonus Multimedia Platform
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Digital Services Network
ISUP	ISDN User part
IT	Information Technology
LAN	Local Area Network
LATA	Local Access and Transport Area
LI	Lawful Intercept
LOM	Lights-out Management
M3UA	MTP3 User Adaption Layer (see page 4)
MB	Megabyte
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MNA	Management Network Adapter
MNS	Management Network Server
MTP	Message Transfer Part
MTP3	Message Transfer Part Level 3
N/A	Not Applicable
NAT	Network Address Translation
NBC	Network Border Controller
NBS	Network Border Switch
NEBS	Network Equipment Building System
Netconf	Network Configuration Protocol
NFS	Network File System
NIF	Network Interface
NIST	United States National Institute of Standards and Technology
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OPC	Originating Point Code
PBX	Private Branch Exchange
PIF	Parameter Interchange Format
PIPE	Policy Information Provisioning Engine protocol (Sonus proprietary)
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PNA	Packet Network Adapter
PNS	Packet Network Server
PP	Protection Profile
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PSX	Sonus Policy and Routing Server
QGE	Quad Gigabit Ethernet
RADIUS	Remote Authentication Dial In User Service

RAID	Redundant Array of Inexpensive Disks
RANAP	Radio Access Network Application Part
RAS	Remote Access Server
RFC	Request for Comments
ROM	Read Only Memory
RSA	Rivest, Shamir and Adleman
RTCP	Real-time Control Protocol (See **[RFC 3550]**)
RTP	Real-time Protocol (See **[RFC 3550]**)
SA	Security Association
SBC	Session Border Controller
SCCP	Signaling Connection Control Part (see page 5)
SCP	Secure Copy (part of SSH)
SCSI	Small Computer System Interface Small Computer Standard Interface
SCTP	Stream Control Transmission Protocol (see page 5)
SFP	Security Functional Policy
SFR	Security Functional Requirement
SFTP	Secure FTP (part of SSH)
SG	Signaling Gateway
SGP	Signaling Gate Process
SGX	Sonus SGX4000 SS7 Signaling Gateway
SHA	Secure Hash Algorithm
SIF	Subinterface
SIGTRAN	Signaling Transport
SIP	Session Initiated Protocol
SIP-I	Session Initiation Protocol with encapsulated ISUP
SIPS	Secure SIP
SLS	Signaling Link Selection
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SPS	Specialty Server
SRTCP	Secure RTCP (See **[RFC 3711]**)
SRTP	Secure RTP (See **[RFC 3711]**)
SRX	Sonus Call Session Server
SS7	Signaling System 7
SSH	Secure Shell protocol
ST	Security Target
STP	Signal Transfer Point
SUA	SCCP User Adapter (layer). (See page 6)
TAC	Sonus' Technical Assistance Center
TCAP	Transaction Capabilities Part
TCL	Tool Command Language
TCP	Transmission Control Protocol
TE	Terminal Equipment
TLS	Transport Layer Security protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	Telecommunications Service Provider
TSP	TOE Security Policy
UDP	User Datagram Protocol

UICC	Universal Integrated Circuit Card
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
WPS	Wireless Priority Service
xDSL	Digital Subscriber Line Technologies
XML	Extensible Markup Language

1.5 TOE OVERVIEW

1.5.1 TOE Type

The TOE is a telephony trunking suite.

1.5.2 Usage

As adoption of packet voice technologies continues to increase, telecommunications carriers are now interconnecting with third parties using Internet Protocol (IP) connections rather than traditional circuit networks. Because most telephones, faxes, and other devices are connected to the existing Public Switched Telephone Network (PSTN) and to Private Branch Exchanges (PBXs), converged network carriers must have some means of interconnecting them across a packet infrastructure (such as the Internet). Systems that provide this interconnection are called a Packet Telephony Gateways. These systems support packet peering such that real-time communication traffic is passed from one packet network to another all the while respecting and enforcing separation between the networks' administrative and security domains.

Examples of packet peering include a telecommunications carrier peering with:

- another carrier,
- an application service provider (ASP),
- an enterprise, or
- the public Internet.

The Target of Evaluation (TOE) specified by this Security Target is a distributed software TOE that is a telephony trunking solution providing full integration between a packet infrastructure and a PSTN. The Sonus Trunking Suite is comprised of the following network elements:

- Insight Element Management System (EMS);
- GSX/NBS 9000 High-density Media Gateway Open Services Switch (GSX);
- Policy and Routing Server (PSX);
- SGX4000 SS7 Signaling Gateway (SGX); and
- DataStream Integrator Call Data Record Translation Engine (DSI).

1.5.2.1 Insight Element Management System (EMS)

Sonus Insight, is a web-based Element Management System (EMS) that provides a graphical user interface (GUI) for managing all aspects of the Sonus Trunking Suite. The EMS provides the

Administrator and Operator with granular control over every connected Sonus network element, from provisioning to near real-time performance monitoring.

The EMS is intended to be used by network operators to quickly configure new media gateways, session border controllers (SBCs) / network border controllers (NBCs), trunk groups, call routes and subscriber services. The EMS also supports flow-through provisioning and broad integration through application programmable interfaces (APIs). Through the EMS user interfaces, Administrators and Operators are able to set customizable alarm thresholds and monitor alarms and events in near real time.

In addition to the network elements identified above (i.e., GSX, PSX, SGX, and DSI), the EMS can manage the following network elements that have not been included within the scope of this evaluation:

- Sonus Access Server (ASX);
- Active Directory Services (ADS) server;
- Sonus multimedia platform (IMX);
- Sonus call session server (SRX); and
- Sonus NBS5200 Network Border Switch.

The EMS software allows fault monitoring for all the above-listed Sonus devices as well as numerous Riverstone and Solaris devices.

The Sonus EMS:

- implements operations, administration, maintenance, and configuration functions for Sonus system elements;
- runs on a Sun (Oracle) Netra platform;
- is accessed by the network operator over a trusted path via a standard Web browser; and
- is the primary interface for interfacing with service-provider network management systems.

1.5.2.2 GSX/NBS 9000 High-density Media Gateway Open Services Switch

The GSX/NBS9000 High-density Media Gateway Open Services Switch ("*GSX*") is a carrier-class packet telephony gateway that provides all of the capabilities required to provide telephony service on a packet backbone for voice, data, and fax transmission.

The GSX:

- provides Synchronous Optical Networking (SONET) and Ethernet interfaces to the packet environment;
- can terminate and interconnect up to 22,176 simultaneous Voice Over IP (VoIP) calls;
- supports toll-quality voice in a packet network environment (IP or Asynchronous Transfer Mode (ATM));
- performs limited PSTN user interaction (announcements, tones, and digit collection) under the control of the Policy and Routing Server (PSX);
- handles higher level SS7 (for example, ISUP), ISDN, and CAS[5] signaling and uses the Sonus SGX SS7 Signaling Gateway for lower level PSTN signaling (such as SS7 MTP);

[5] CAS - Channel Associated Signaling

- supports Session Initiated Protocol (SIP), SIP with encapsulated ISUP (SIP-I), and H.323 protocols for signaling to IP telephony devices; and
- can support peering relationships between packet carriers by also functioning as a network border switch.

The GSX can be configured to support the following types of connections:

PSTN-to-PSTN	PSTN devices (like telephones and fax machines) can interconnect through a packet network. In these connections, the GSX provides intra-LATA[6] (tandem) or inter-LATA (toll or long-distance) service.
PBX-to-PSTN/PBX	A Private Branch Exchange (PBX) can connect to the GSX through a direct Primary Rate Interface (PRI) or CAS connection, bypassing the PSTN. Devices attached to these PBXs can interconnect with any other compatible device in the network.
Packet-to-PSTN/PBX	There are a growing number of telephones and other devices that connect directly to the packet network without using the PSTN: premises packet gateways, cable telephony devices, xDSL[7], packet PBXs, etc. The GSX allows these devices to interconnect with devices on the PSTN or on PBXs.
Services Mediation	The GSX can identify Internet modem calls and immediately switch them to a Remote Access Server (RAS) for packet conversion.
Packet-to-Packet	There are a number of different scenarios in which the GSX may be used to transport traffic packet to packet. Often signaling protocols need to be translated so traffic may be sent through the GSX to perform this function. The GSX may also be used to provide security at the edge of a carrier's network when that carrier is exchanging VoIP traffic with some other company over an IP network.

1.5.2.3 Policy and Routing Server

The Policy and Routing Server ("*PSX*") is responsible for the main call processing functions in a packet network, including call screening and blocking, support for number translation services such as local number portability, calling name delivery, and toll-free services, call routing, and billing. The PSX provides a central database of service, routing, and call treatment information for one or more GSXs.

The Sonus Policy and Routing Server (PSX) is a highly scalable soft switch that controls the interworking of circuit-based and IP-based media streams at the media gateway. The PSX provides both policy and routing services. Scalability is achieved using both multiprocessor configurations and load sharing across multiple PSX systems. The PSX includes a database of signaling addresses for routing calls. It receives signaling information from a GSX, H.323 gateway or gatekeeper, or SIP application server, and instructs the requesting system on how to establish calls. The PSX also interacts with PSTN databases via TCAP or, for authorization code validation, via transactional SIP, and may route calls to application servers to enable a range of enhanced services. PSX does the following call processing:

- Input Call Processing;
- Services;

[6] LATA – Local Access and Transport Area
[7] xDSL – Digital Subscriber Line Technologies

- Number (Pre-Routing) Translation;
- Standard Routing; and
- Output Call Processing.

1.5.2.4 SGX4000 SS7 Signaling Gateway

The SGX4000 SS7 Signaling Gateway ("*SGX*") provides connectivity between one or more GSXs and the Signaling System 7 (SS7) network for circuit switched call routing and services. Its integrated SS7 link termination allows the GSX to serve as the physical interface point connecting the GSX directly to the SS7 signaling network.

Features:

- The gateway provides SS7 and SIGTRAN signaling functionality and represents the ISUP and TCAP application servers on the IP network to the SS7 network.
- The ISUP and TCAP application servers run on the GSX and PSX respectively.
- The SGX contains two Computing Elements (CEs), where each CE is a separate Oracle Netra 4250 loaded with the SGX software.
- An SGX can hold a maximum of 8 local nodes. Each local node spans both CEs. The SGX communicates with GSXs over SIGTRAN M3UA, and communicates with PSXs over SIGTRAN SUA.
- An SGX local node can communicate with STPs over standard SS7 TDM links or over SIGTRAN links. This release supports M3UA links to STPs that provide the signaling gateway function in addition to the STP signaling transfer function.

1.5.2.5 DataStream Integrator Call Data Record Translation Engine (DSI)

DataStream Integrator Call Data Record Translation Enginer ("*DSI*") is an advanced data translation engine that is used to collect, correlate, and produce a standards compliant billing stream according to customer-specific services and billing usage criteria, founded on the raw call accounting records produced by the Sonus Trunking Suite's network elements. The DSI also provides a standards-based service for delivery of the billing stream to 3rd party billing systems specified by Sonus' customers.

DSI supports generation of AMA[8] standard billing streams from the GSX network element.

The DSI can be deployed in three different configurations:

- *DSI-L0* provides essential services to capture raw network usage data. DSI-L0 is offered as a redundant pair of servers associated with a group of GSX platforms. Aside from its role to capture raw network usage data from GSX clients, the DSI-L0 redundant server pair also provides unique services to each GSX that is "homed" to the pair with storage for the GSX software boot image, configuration files, announcement files, and event logs.
- *DSI-L1* provides workflow capabilities for management and distribution of raw network usage data. DSI-L1 is similarly offered as a redundant pair of servers normally associated with a group of GSX platforms. DSI-L1 may also be deployed as a centralized "island" for management of network usage data from a number of feeder DSI-L0 systems. The DSI-L1 server pair may also receive network usage data from PSX, ASX, IMX, and/or third-party network elements. Distribution of network usage data in either raw or mediated form requires either DSI-L1 or DSI- L2.

[8] AMA - Automatic Message Accounting

- *DSI-L2* provides advanced mediation capabilities for standards-compliant billing streams/ interfaces, custom billing streams/interfaces, reporting services for Call Logs, and tools for system and application integration with a variety of third-party and legacy applications. DSI-L2 is offered as a scalable cluster of servers numbering from a minimum of one (1) to a maximum of 16 servers in the cluster. Though a single node server configuration is offered, the developer strongly recommended that any DSI-L2 deployment have a minimum of two (2) servers to enable High Availability protection and thus ensure business continuity in the event of any single server failure.

Call Data Record (CDR) streaming allows CDRs to be sent directly to accounting applications bypassing GSX event-based logging. This provides an alternative to an NFS/DSI-based logging server for accounting records.

1.5.3 Security Features

With the everyday threat of security breaches to the network, the Sonus Trunking Suite provides advanced security measures at multiple levels. It uses Transport Layer Security (TLS) to secure its web-based operations, management and administrative interface. Furthermore, communication links between the EMS and the Sonus Trunking Suite's network elements are secured through the use of the Secure Shell (SSH) protocol. The user security manager interface in the EMS allows system administrators to define security roles and access restrictions based on the end-user's organizational structure. By supporting RADIUS, powerful features such as RSA SecurID® can be enabled by end-users. The EMS interface also enables administrators to generate user activity reports for tracking the details of each user's activities, assuring the administrator's accountability.

The GSX network element is not only a high-capacity media gateway, but it also functions as a network border switch (NBS) within a Sonus Trunking Suite deployment. This enables the Sonus Trunking Suite to provide IP-to-IP border control and PSTN media gateway capabilities; integrating security, session control and media control. The Sonus Trunking Suite has extensive signaling and multimedia manipulation capabilities which permit it to function as a multimedia firewall. It also delivers full Network Address Translation (NAT) and topology hiding, simplifying the interaction between the service provider and external networks, and securing the private network from would-be intruders. Commercial relationships governing the amount of traffic to be exchanged between service providers or customers are fulfilled by the Sonus Trunking Suite's GSX, which monitors and polices the amount of traffic flowing between a carrier's network and an external entity. The Sonus Trunking Suite also includes dynamic and administrator-configurable policers that protect the core network that it is deployed in from denial of service (DoS) types of attacks.

Working with the other elements in the Sonus Trunking Suite, the DSI ensures that network usage data is formatted properly and distributed to back-office applications such as billing, fraud, settlement, performance traffic management and signaling analysis and reporting systems. The Sonus Trunking Suite provides the reliability carriers demand for their mission-critical, revenue-generating data. Communications between the Sonus Trunking Suite and back-office applications are also carried over SSH.

The PSX element is the heart of the Sonus Trunking Suite. It acts as the call routing engine on the IP network and it also acts as a SIP proxy, SIP redirector, and an H.323 Gatekeeper for the GSX. Through the PSX, the Sonus Trunking Suite provides local element level congestion control and network-wide traffic management controls, which allow end-user carriers to deal with network overload conditions in a graceful manner.

1.5.4 TOE Environment

Each component of the TOE is designed to be installed and used in an environment that is:

- configured and controlled in accordance with Administrator guidance that is supplied with the product;
- managed by Administrators working under a consistent security policy; and
- physically secured with access control measures and physical protection mechanisms.

1.5.5 Hardware and Software Supplied by the IT Environment

This section identifies any non-TOE hardware, software, and firmware that is required by the TOE to operate correctly as specified herein.

1.5.5.1 Non-TOE Hardware

As the TOE is software only, the hardware identified in Table 2 is required in the IT environment for the TOE to run on. Where more than one hardware item is listed against a TOE network element, the evaluated configuration of the TOE supports the identified hardware.

Table 2: Non-TOE Hardware

Network Element	Hardware	Comment(s)
EMS	Oracle (Sun) Netra 240	Minimum requirements: • 2 x 1.5 GHz CPUs, • 4 GB memory • 2 x 146 GB hard drives, • QGE Card, • DVD ROM, • Alarm card firmware (see Table 3), • at least 4GB swap space Optional equipment includes: • SANnet II SCSI RAID System
	Oracle (Sun) Netra 440	Minimum requirements: • 4 x 1.6 GHz CPU, • 8 GB memory, • 4 x 146 GB hard drives, • QGE Card, • 2 x 10/100/1000 Ethernet Ports, • DVD ROM, • Alarm card firmware (see Table 3), and • at least 8 GB swap space Optional equipment includes: • SANnet II SCSI RAID System
	Oracle (Sun) Netra T5220	Four drive configuration meeting at least the following minimum requirements: • 4 x 1.2 GHz CPU, • 16 GB memory, • 4 x 146 GB hard drives, and • 4 x 10/100/1000 Ethernet Ports Optional equipment includes: • StorageTek 2540 array RAID system

Table 2: Non-TOE Hardware

Network Element	Hardware	Comment(s)
		• IBM 3524 FC RAID
	Oracle (Sun) Netra T5220HA	Four drive configuration meeting at least the following minimum requirements: • 4 x 1.2 GHz CPU, • 16 GB memory, • 4 x 146 GB hard drives, • Quad GigENET Card, • 4 x 10/100/1000 Ethernet Ports, and • Fiber Channel Card
	UPS	The EMS platform should be protected by an uninterrupted power supply (UPS) to prevent the ungraceful shutdown of its fault management capability.

GSX	Bespoke hardware custom built by Sonus	High-level description of the hardware:
		• Chassis
		  ○ Mid-plane
		  ○ Dual redundant power feeds
		  ○ Cooling system
		• Hot-swappable modules (can be removed or replaced while the GSX is powered up)
		  ○ Management network servers and adapters (MNS and MNA)
		  ○ Packet network servers and adapters (PNS and PNA)
		  ○ Circuit network servers and adapters (CNS and CNA)
		  ○ Specialty servers to support different audio codecs (SPS)
		
		In the Evaluated Configuration, the GSX is configured with the following:
		• two (2) MNS21 / MNA21 pairs;
		• 11 CNS86 / CNA81 pairs;
		• one (1) CNS86-R / CNA81 pair; and
		• two (2) PNS41 / PNA40 pairs.

DSI	Oracle (Sun) Netra T2000	Standard Platform for DSISW-L0 and/or DSISW-L1 configurations Minimum requirements: • 4 X 1 GHz CPU, • 8 GB RAM, • 2 X 146 GB hard drives, • 4 X 10/100/1000 Ethernet ports, and • DVD ROM drive
	Oracle (Sun) Netra 240	Optional Platform for DSISW-L0 and/or DSISW-L1 configurations only; not certified for production DSISW-L2 operations

Table 2: Non-TOE Hardware

Network Element	Hardware	Comment(s)
		Minimum requirements: • 1 X 1.5 GHz USIIIi CPU/1MB cache, • 2 GB ECC Memory (4x512MB DIMM), • 2 Ultra 160 SCSI 146 GB HDDs, • 4 X 10/100 Ethernet ports, • DVD ROM, and • Alarm card firmware (see Table 3)
	Oracle (Sun) Netra 240	Optional Platform for DSISW-L2 configuration Minimum requirements: • 2 X 1.5 GHz USIIIi CPU/1MB cache, • 4 GB ECC Memory (8x512MB DIMM), • 2 Ultra 160 SCSI 146 GB HDDs, • 4 X 10/100 Ethernet ports, • DVD ROM, and • Alarm card firmware (see Table 3)
	Oracle (Sun) Netra 440	Optional Platform for DSISW-L2 configuration Minimum requirements: • 4 X 1.6 GHz CPUs, • 8 GB memory, • 4 X 146 GB hard drives, • QGE card, • 2 x 10/100/1000 Ethernet ports, • DVD ROM drive, and • Alarm card firmware (see Table 3)
	Oracle (Sun) Netra T5220	Optional Platform for DSISW-L0 and/or DSISW-L1 configurations Standard Platform for DSISW-L2 configuration • Minimum requirements: • 1 X Quad-Core UltraSPARC T2, 1.2 GHz, 32 thread CPU, • 16 GB memory, • 4 X 146 GB hard drives, • Quad GigENET Card, • 4 x 10/100/1000 Ethernet ports, • Fiber Channel Card, and • dual AC or DC power supplies
	Oracle (Sun) Netra X4270	DSIW-L1 configuration consisting of the following minimum requirements: • Intel Xeon L5518 CPU, • 16 GB memory, • 4 x 146 GB hard drives, • 4 x 10/100/1000 Ethernet ports, • 1 dedicated 10/100 Ethernet management

Table 2: Non-TOE Hardware

Network Element	Hardware	Comment(s)
		port • 1 RJ45 serial management port • Alarm card firmware (see Table 3) Optional equipment includes: • IBM 3524 FC RAID system

PSX	Oracle (Sun) Netra 240	Minimum requirements:
		• two CPUs,
		• 4 GB memory,
		• two 146 GB drives,
		• Alarm card firmware (see Table 3), and
		• RAID for High Availability (HA) configuration:
		  ○ DotHill SANnet II SCSI RAID
		  ○ five 73 GB 10K RPM drives
		  ○ two DC power supplies
		  ○ two controllers

	Oracle (Sun) Netra 440	Minimum requirements: • four CPUs, • 8 GB memory, • four 146 GB drives, • Alarm card firmware (see Table 3), and • Same RAID for HA configurations as the Netra 240 above.
	Oracle (Sun) Netra T5220	Four drive configuration meeting at least the following minimum requirements: • 4 x 1.2 GHz CPU, • 16 GB memory, • 4 x 146 GB hard drives, and • 4 x 10/100/1000 Ethernet Ports Optional equipment includes: • StorageTek 2540 array RAID system • IBM 3524 FC RAID
SGX	Oracle (Sun) Netra X4250	Minimum requirements: • Dual Quad Core, 3.0GHz or 2.13 GHz Xeon® L5408 CPU, • 16 GB RAM, • 2 x 146 GB SAS disk drives • Dual NEBS Level 3-certified DC or AC power supplies, • 2U form factor, • two 2.0 USB ports (rear), and • Alarm card firmware (see Table 3).

In addition to the hardware required specifically for the TOE above, the IT environment requires the following general purpose hardware:

- Servers to provide:
  - RADIUS authentication,
  - NTP server, and
  - DNS server.
- A MS-Windows™ compatible workstation for remotely administering the TOE.

Optional hardware not included in the evaluated configuration includes:

- An external timing source, either a Building Integrated Timing Source (BITS) timer for IP-based connections, or a Synchronous Equipment Timing Source (SETS) timer for providing timing synchronization for SONET connections.
- General purpose servers for:
  - back office / billing systems and call accounting server(s) (for processing call accounting records), and
  - disaster recovery servers or services to store replicated database data from the TOE.

1.5.5.2 Non-TOE Software

Table 3 identifies software that is required to be installed on the identified TOE network element hardware as part of the IT environment to assure the correct operation of the TOE in delivering its claimed security functionality (i.e., TSF).

Table 3: Non-TOE Software

Network Element	Software	Comment(s)
EMS	Solaris v10[9]	Host operating system
	Oracle 11g[9]	Data repository for the TOE
	Sun Lights-out Management (LOM) software: • Advanced Lights-out Management (ALOM) v1.6.2 for Netra N240, or N440 • Integrated Lights-out Management (ILOM) 2.0.4.28a for Netra T5220	Alarm card firmware referred to for this network element in Table 2.

[9] This software is part of Sonus' Common Services Platform (CSP) used by the EMS, PSX, DSI TOE subsystems.

Table 3: Non-TOE Software

Network Element	Software	Comment(s)
GSX	N/A	There are no non-TOE software components installed on the GSX. Its "*Marlin*" operating system provides this element's contribution to the TSF.
DSI	Either: • Common Services Platform per footnote 9 (Solaris v10 and Oracle 11g) • Red Hat Enterprise Linux 6.1 and Oracle 11g	The DSI is designed for use in a telecommunications environment using either host operating system, depending on the end-user's needs.
	Sun LOM software: • ALOM v1.6.2 for Netra T2000, N240, or N440 • ILOM 2.0.4.28a for Netra T5220	Alarm card firmware referred to for this network element in Table 2
	Sun Netra SNMP Management Agent 1.6 or higher	
	Sun Cluster and Sun Cluster Agent for Oracle 3.2U2 or higher	
	Third-party add-ons for Solaris: • sudo 1.6.8 p12 • lsof 4.8 • top 3.8.1	
PSX	Common Services Platform per footnote 9 on page 19: • Solaris v10 • Oracle 11g	See comments for EMS
	Sun LOM software: • ALOM v1.6.2 for Netra T2000, N240, or N440 • ILOM 2.0.4.28a for Netra T5220	Alarm card firmware referred to for this network element in Table 2
SGX	Red Hat Linux 5.3	Host operating system
	ILOM 3.0.3.30 r44534 for Netra X4250	Alarm card firmware referred to for this network element in Table 2

In addition to the software required specifically for the TOE hardware above, the IT environment requires the following general purpose software:

- Browser to support secure hypertext transfer protocol (HTTPS) connections from the EMS Operator Workstation to the EMS server. Sonus recommends Internet Explorer 6.0 or newer.
- Java Plugin 1.6.0_12 or newer for the EMS Operator Workstation.
- Sonus recommends that the EMS Operator Workstation be equipped with Microsoft Windows XP Service Pack 3 or newer.

- Server configured to perform RADIUS authentication.
- At least one server configured to provide NTP v3 time synchronization services[10] to each TOE element[11].

1.6 TOE DESCRIPTION

1.6.1 Physical Sonus Trunking Suite Boundary

Figure 1 (page 21) shows the TOE in its deployment configuration. The TOE's network elements are located within a physically secured area, residing on a secured and isolated network. Local TOE network element console access is available to authorized TOE administrators for the following subsystems:

- GSX,
- SGX,
- DSI,
- PSX, and
- EMS.

The EMS provides the primary TOE administrative interface to TOE Administrators and Operators via a browser-based interface on a remote computer over a secured and trusted channel.

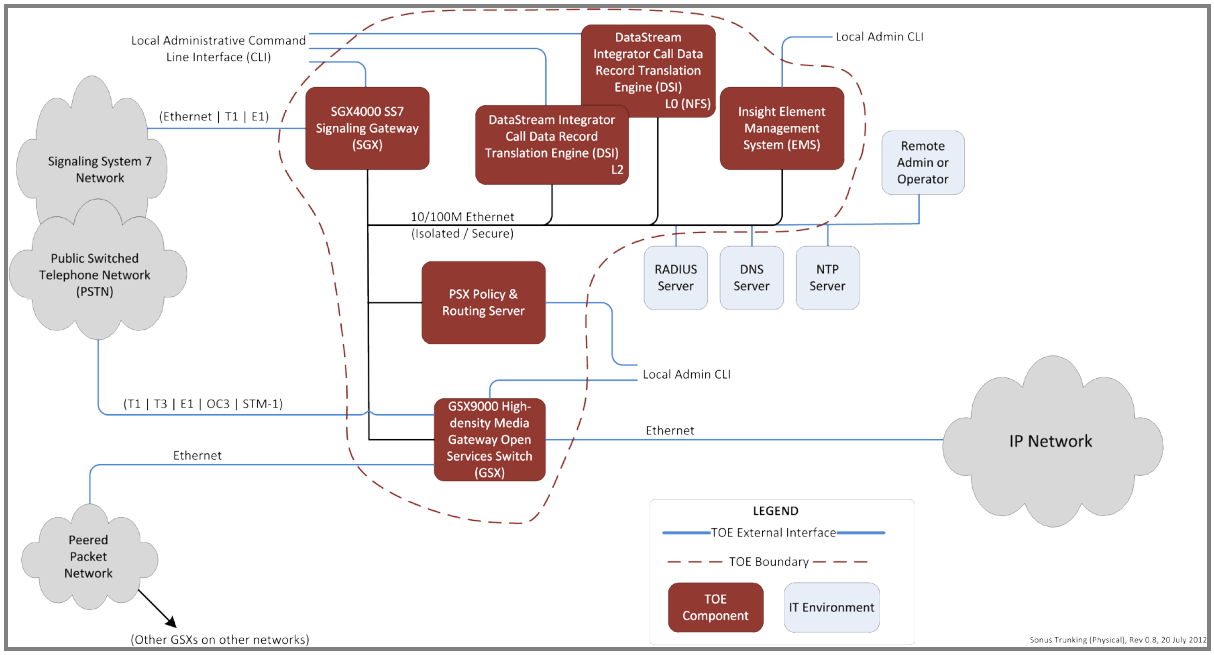

Figure 1: Distributed TOE – Physical Installation

[10] The TOE can synchronize using NTP versions 1, 2, & 3, but v3 is the default and preferred version.

[11] The TOE subsystems can synchronize with more than one NTP server, but in doing so, the operator must ensure that these NTP servers are synchronized. Conflicting time information from multiple, not synchronized NTP servers may cause errors in the TOE subsystems.

The evaluated configuration of the TOE is software only consisting of the software identified in Table 1, installed and configured on the following platforms supplied by the IT environment as depicted at Figure 3:

- two (2) EMS network elements running on Netra T5220 servers as described in Table 2 including the optional IBM 3524 FC RAID;
- three (3) PSX network elements running on Netra T5220 servers, also as described in Table 2. Two (2) of the PSX network elements will be configured in a master/replica operating mode, each of which will be equipped with the optional IBM 3524 FC RAID. The third PSX will be configured as a master standby, but without the optional IBM 3524 FC RAID;
- one (1) DSI network element running on a Netra X4270 server as described in Table 2, including the optional IBM 3524 FC RAID;
- one (1) SGX network element running on a Netra X4250 as described in Table 2; and
- one (1) GSX network element equipped as described in Table 2, i.e.:
  - one (1) MNS21 / MNA21 pair;
  - 11 CNS86 / CNA81 pairs;
  - one (1) CNS86-R / CNA81 pair; and
  - two (2) PNS41 / PNA40 pairs.

Each server above will also have the non-TOE software identified in Table 3 for its respective network element installed on it.

1.6.2 Logical Sonus Trunking Suite Boundary

Figure 2 on the next page presents a high-level logical view of the TOE boundary, while Figure 3 on 24 presents a more detailed diagram that identifies key internal and external TOE interfaces.

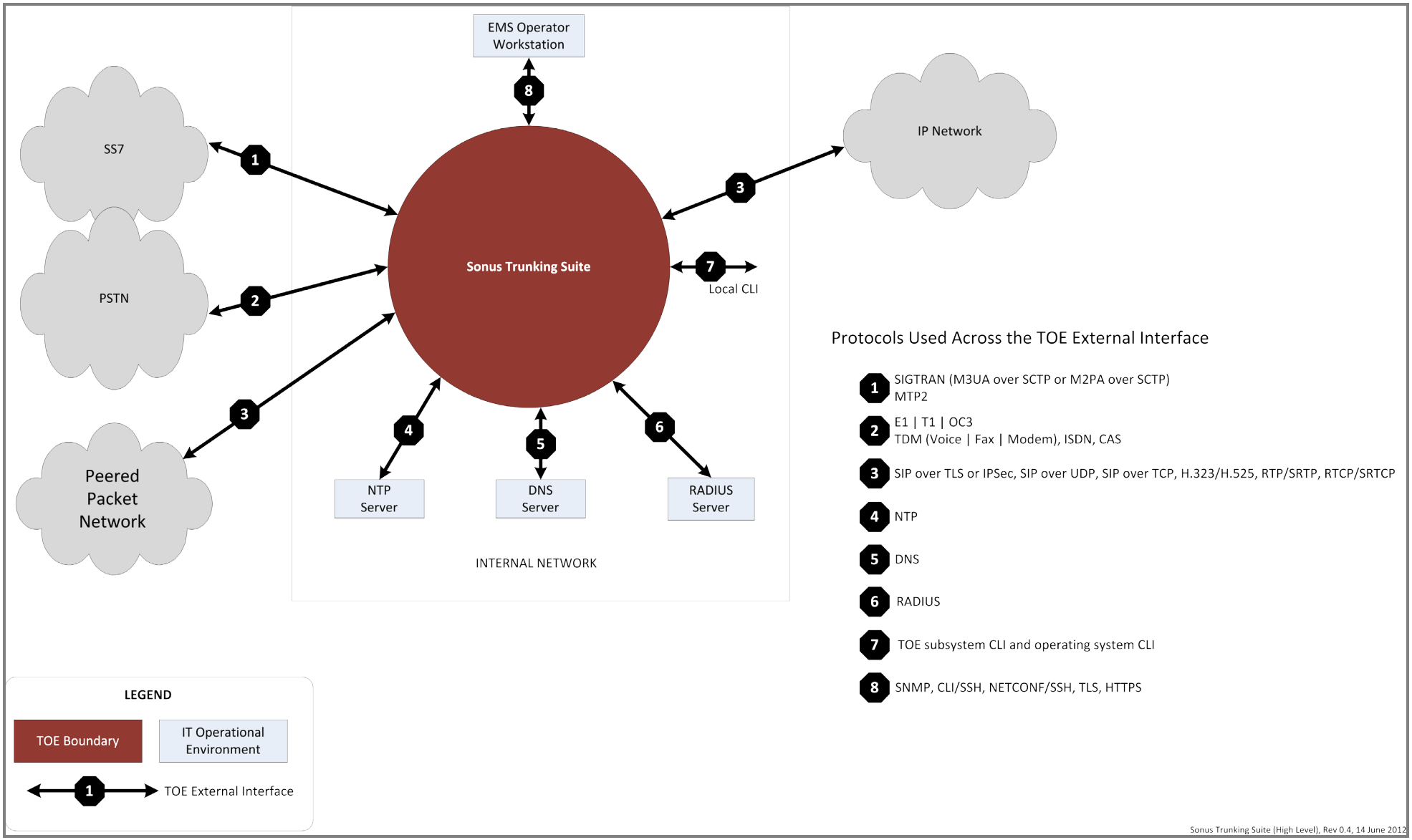

Figure 2: High-level Logical TOE Boundary

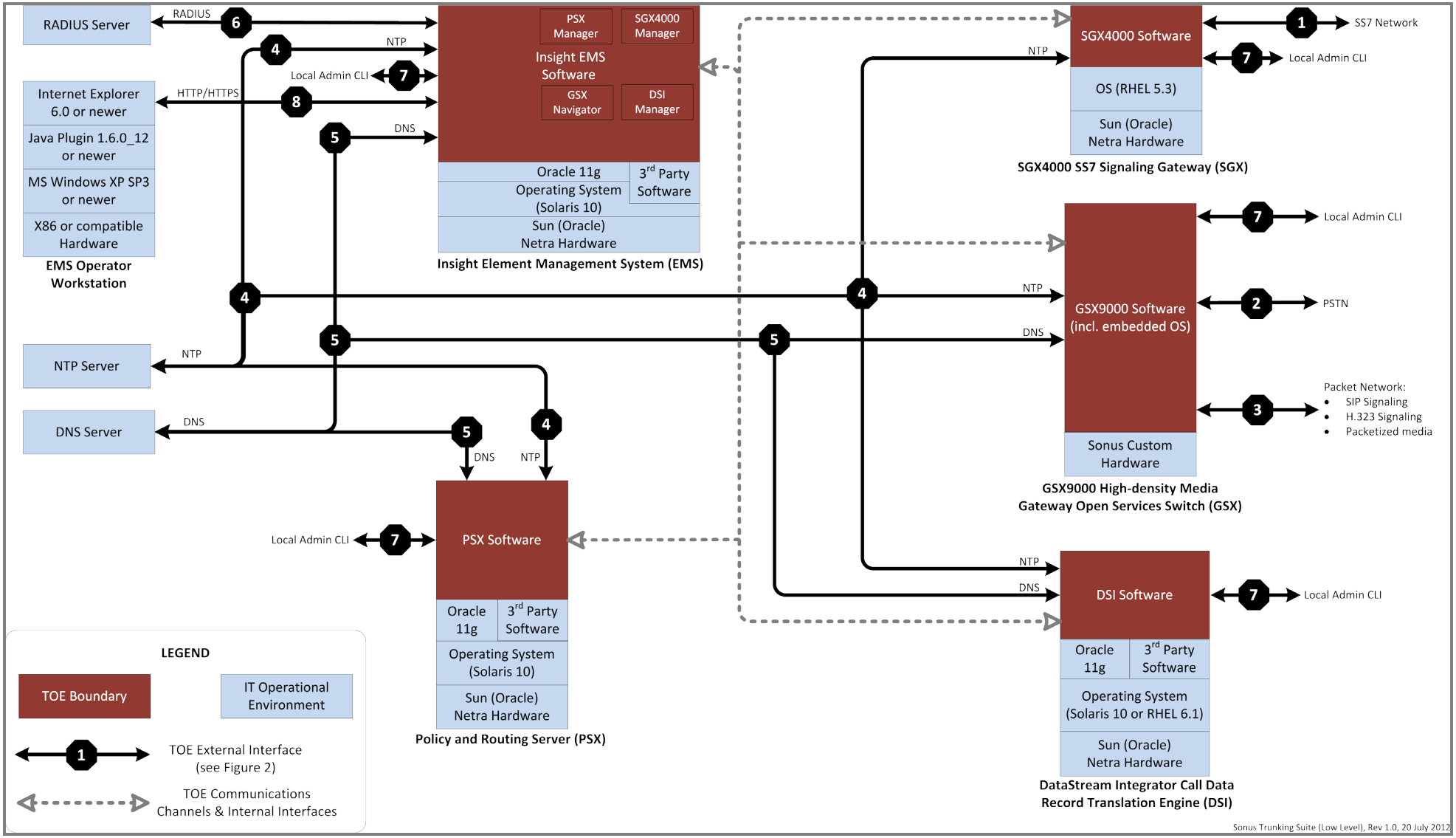

Figure 3: Low-level Logical TOE Diagram

1.6.3 Security Functions Provided by the TOE

The primary security functions of the TOE are:

- Security Audit
- Cryptographic Support for Trusted Path / Channels and Secured Communications
- User Data Protection (Information Flow Control)
- Identification and Authentication
- Security Management
- Resource Utilization
- Access to the TOE

1.6.3.1 Security Audit

The Sonus Trunking Suite records security relevant events related to the security functions it provides. Authorized administrators can select which events are audited and the level of audit detail to be recorded. Audit reporting functionality is also available to search the audit log.

The Sonus Trunking Suite detects when the capacity of the audit trail is approaching configurable thresholds, and the system administrator can define actions to be taken when the threshold is exceeded. The system protects audit records against modification and only authorized administrators are able to delete records. Sonus Trunking Suite also provides reliable time information to record in its audit records.

1.6.3.2 Cryptographic Support for Trusted Path / Channels and Secured Communications

The Sonus Trunking Suite supports secure communication both within its own scope of control (between TOE network elements (i.e., they are TOE subsystems)) as well as with other systems and trusted IT entities via the Secure Shell (SSHv2.0, including Secure FTP and Secure Copy), HTTPS, Internet Protocol Security (IPSec), and Transport Layer Security (TLSv1) protocols. Communication via these protocols provides protection against unauthorized disclosure and modification via cryptographic mechanisms. The protocols are used as follows:

- SSH: is used to establish a secure channel for remote Administrative access to TOE subsystems from the EMS server.
- HTTPS: is used to secure the communication channel between the EMS Operator Workstation (outside the TOE) and the EMS management server.
- Secure FTP (SFTP) and Secure Copy (SCP): are used to securely copy Call Data Records (CDRs) up to the EMS from the DSI when queried by an authorized Operator.
- TLS: used to secure signaling information carried by the SIP protocol for interfacing with peered telecommunication service providers.
- IPSec: also used to secure signaling information over the SIP protocol for interfacing with peered telecommunications service providers.

1.6.3.3 User Data Protection (Information Flow Control)

The Sonus Trunking Suite enforces three information flow policies:

- The TOE security function (TSF) enforces a PEERED information flow control policy for the transfer of IP traffic and multimedia packets across the TOE from connected IT entities for onward transmission to other connected IT entities.
- The TSF enforces an AUTHENTICATED information flow control policy for EMS-initiated traffic to TOE subsystems for operational administration. This policy also enforces local operational and administrative CLI commands at each of the TOE subsystems.
- The TSF enforces an ENCRYPTED information flow control policy for intra-TOE channel security for operating and administering TOE subsystems via the EMS management interfaces over HTTPS, TLS, and SSH. This policy also enforces channel security for secure signaling for the GSX subsystem with peered telecommunications services providers by transporting signaling protocols over either TLS or IPSec.

1.6.3.4 Identification and Authentication

The Sonus Trunking Suite authenticates the claimed identity of each operational and administrative user before allowing the user to perform any further actions. The TOE internally maintains a set of identifiers associated with processes which are derived from the unique identifier upon login by Administrator or Operator users.

The TSF enforces restrictions when establishing user sessions to ensure that the set of active roles available to that user is limited to those roles for which the user is authorized.

The TOE only permits authorized Administrators to manage user accounts (e.g. define role(s), add/delete users). The TOE allows for the configuration of password criteria to enforce strong passwords where required by organizational policy. The TOE can be configured to lock user accounts when the number of failed authentication attempts reaches an administrator defined limit.

1.6.3.5 Security Management

The Sonus Trunking Suite provides the security management roles of Administrator and Operators. Operators are users assigned to roles that authorize them to perform specific actions within the TOE. Users in the Administrator role can perform all management functions within the TOE Scope of Control.

1.6.3.6 Resource Utilization

The Sonus Trunking Suite includes a number of features to assure effective use of TOE resources. It supports the Government Emergency Telecommunications Service (GETS) to provide authorized government and emergency services personnel with prioritized and high probability of completion (HPC) calling during periods when the network is overloaded (i.e., emergencies, etc.).

Additionally, the TOE includes a number of protection mechanisms to protect the system from high volume network-based attacks and permit the TOE to continue to provide its primary services.

The Sonus Trunking Suite also includes quota services for its own internal storage quotas to permit automated switchover to standby devices if disk storage approaches preset limits.

1.6.3.7 Access to the TOE

The Sonus Trunking Suite incorporates protection mechanisms for Administrator and Operator user sessions. The TOE will lock out these types of users for a definable period of time following a prescribed number of login failures. Additionally, the TOE will automatically logout inactive sessions after a defined period of inactivity. The Sonus Trunking Suite includes a feature that enables Administrators to define account age-out periods so that user accounts that have been unused for a prescribed period are automatically deactivated.

The TOE also enables an authorized Administrator to configure the system to display a logon banner before the logon dialog.

1.7 TOE GUIDANCE DOCUMENTATION

The guidance documentation that accompanies the TOE includes the following:

[DSI Admin Guide]	*DataStream Integrator DSI Administration and Maintenance Guide (Solaris & Linux)*, Sonus Part Number: 550-05398, Document Version: 1, Software Version: V08.04.01
[DSI Alarms Guide]	*DSI DataStream Integrator Alarm Troubleshooting Guide*, Sonus Part Number: 550-05399, Document Version: 1, Software Version: V08.04.01
[DSI Install Guide - Linux]	*DataStream Integrator Installation and Upgrade Guide (Linux)*, Sonus Part Number: 550-05397, Document Version: 1, Software Version: V08.04.01
[DSI Install Guide - Solaris]	*DataStream Integrator DSI Installation and Upgrade Guide (Solaris)*, Sonus Part Number: 550-05396, Document Version: 1, Software Version: V08.04.01
[DSI Install Guide – Solaris]	*DataStream Integrator DSI Installation and Upgrade Guide (Solaris)*, Sonus Part Number: 550-05396, Document Version: 1, Software Version: V08.04.01
[DSI Release Notes – Linux]	*DataStream Integrator (Linux) Version 8.4.1 Patch 1 Release Notes*, Software Version: DSI 08.04.01R000, Document Number: 550-05534, Document Version: 1
[EMS Alarms Guide]	*Insight Element Management System Alarm Troubleshooting Guide*, Sonus Part Number: 550-05404 Document Version: 1 Software Version: V08.04.01
[EMS Install Guide]	*Insight Element Management System Software Installation and Upgrade*, Guide Sonus Part Number: 550-05413, Document Version: 1, Software Version: V08.04.01
[EMS Release Notes]	*Insight Version 08.04.01 Release Notes*, Software Version: EMS 08.04.01R000, Document Number: 550-05414, Document Version: 2
[EMS Traffic Manager Guide]	*Insight Element Management System Traffic Manager User Guide*, Sonus Part Number: 550-05411, Document Version: 1, Software Version: V08.04.01
[EMS User Guide]	*Insight Element Management System User Guide*, Sonus Part Number: 550-05403, Document Version: 1, Software Version: V08.04.01
[GSX Alarms Guide]	*GSX9000 and GSX4000 Series Open Services Switch Alarm Troubleshooting Guide*, Sonus Part Number: 550-05376 Document Version: 2 Software Version: V08.04.01
[GSX Install Guide]	*GSX9000 Open Services Switch Installation and Upgrade Guide*, Sonus Part Number: 550-05374, Document Version: 1, Software Version: V08.04.01
[GSX Ops Guide]	*GSX9000 and GSX4000 Series Open Services Switch Operations Guide*, Sonus Part Number: 550-05375, Document Version: 1 Software Version: V08.04.01
[GSX Release Notes]	*GSX9000™ and GSX4000™ Open Services Switch Version 08.04.01F001 Release Notes*, Software Version: GSX 08.04.01F001,

	Document Number: 550-05530, Document Version: 1
[Lawful Intercept Guide]	*Sonus Networks Lawful Intercept Solution Guide*, Sonus Part Number: 550-05410, Document Version: 1, Software Version: V08.04.01
[PSX Alarms Guide]	*PSX Policy Server Alarm Troubleshooting Guide Sonus*, Part Number: 550-05392, Document Version: 1, Software Version: V08.04.01
[PSX CLI Guide]	*Sonus Insight CLI User Guide For PSX*, Sonus Part Number: 550-05405, Document Version: 1, Software Version: V08.04.01
[PSX CLI Guide]	*Sonus Insight CLI User Guide For PSX*, Part Number 550-05405, Document Version 1, Software Version V08.04.01
[PSX Install Guide]	*PSX Policy Server Installation and Upgrade Guide*, Sonus Part Number: 550-05389, Document Version: 1, Software Version: V08.04.01
[PSX Product Guide]	*PSX Policy Server Product Description Guide*, Sonus Part Number: 550-05390, Document Version: 1, Software Version: V08.04.01
[PSX Provisioning Guide]	*PSX Policy Server Provisioning Guide*, Sonus Part Number: 550-05391, Document Version: 1, Software Version: V08.04.01
[PSX Release Notes]	*PSX Policy Server Version 08.04.01F001 Release Notes*, Software Version: PSX 08.04.01F001, Document Number: 550-05582, Document Version: 1
[PSX Tools Guide]	*Sonus Policy Server Tools Guide*, Sonus Part Number: 550-05393 Document Version: 1 Software Version: V08.04.01
[SGX Alarms Guide]	*SGX4000 Signaling Gateway Alarm Troubleshooting Guide*, Sonus Part Number: 550-05208, Document Version: 1, Software Version: V07.03.06
[SGX CLI Guide]	*SGX4000 SS7 Gateway CLI User Guide*, Sonus Part Number: 550-05207, Document Version: 1.0, Software Version: V07.03.06
[SGX Install Guide]	*SGX4000 Software Installation Guide*, Sonus Part Number: 550-05269, Document: 1, Software: V07.03.06
[SGX Ops Guide]	*SGX4000 SS7 Gateway Operations Guide*, Sonus Part Number: 550-05206, Document Version: 1, Software Version: V07.03.06
[SGX Release Notes]	*SGX4000 SS7 Gateway Version 7.3.6 Release Notes*, Software Version: SGX4000 07.03.06R000, Document Number: 550-02656, Document Version: 2.0, February 28, 2011
[X-Platform Alarm Guide]	*Cross-Platform Alarm Troubleshooting Guide (Agent Framework Host Monitoring Linux Platform Monitoring RAID Sun Netra Agent System Management Veritas Management)*, Sonus Part Number: 550-05412, Document Version: 1, Software Version: V08.04.01

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST has been prepared in accordance with the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1, Revision 3 Final (July 2009):

- Part 1: Introduction and General Model, CCMB-2009-07-001;
- Part 2: Security Functional Components, CCMB-2009-07-002;
- Part 3: Security Assurance Components, CCMB-2009-07-003; and
- Evaluation Methodology, CCMB-2009-07-004.

The Target of Evaluation (TOE) for this ST is conformant with the:

- functional requirements specified in CC Part 2; and
- CC Part 3 assurance requirements for EAL 2, augmented with:
    - ALC_FLR.2 (Flaw Reporting Procedures), and
    - ALC_DVS.1 (Identification of Security Measures).

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE described by this ST does not claim conformance with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

Threat agents consist of unauthorized persons or external IT entities that are not authorized to use the TOE as well as authorized administrators and operators of the TOE who make errors in configuring the TOE.

Threat agents are divided into two categories:

- Attackers who are not TOE administrators or operators: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE administrators and operators: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. However, TOE administrators and operators are assumed to not be willfully hostile to the TOE.

Threat agents are assumed to have a maximum Attack Potential of Basic[12].

The IT assets requiring protection are:

- Subscriber data transitioning across the TOE;
- TOE operational integrity including its configuration data; and
- TOE operational performance including TOE security functionality.

Table 4: Threats

Identifier	Description
T.ADMIN_ERROR	An Administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An authorized Administrator's or Operator's intentions may become malicious, resulting in TSF data being compromised.
T.AUDIT_COMPROMISE	A malicious external entity (Subscriber or attacker) or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded.
T.DATA_REUSE	A malicious entity attempts to reuse TSF data in order to bypass the TOE Security Policy.
T.RESOURCE_EXHAUSTION	A malicious process or entity (Subscriber or attacker) may block others from system resources via a resource exhaustion denial of service attack. Examples include, but are not limited to: distributed denial

[12] Attack Potential is a function of expertise, resources and motivation. Refer to Section B.4 of the "*Common Methodology for Information Technology Security Evaluation - Evaluation Methodology*", Document ID: CCMB-2009-07-004 for a detailed discussion of Attack Potential and how it is estimated.

Table 4: Threats

Identifier	Description
	of service (DDoS) attack, user call flooding, faked or replayed call control messages, etc.
T.THEFT_OF_SERVICES	A malicious entity (Subscriber or attacker) exploits a flaw in the TOE or the IT operational environment to use telecommunications services without being charged by the Telecommunications Service Provider.
T.TSF_COMPROMISE	A malicious external entity (Subscriber or an attacker) or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified or deleted).
T.UNATTENDED_SESSION	An entity other than an Administrator or Operator may gain unauthorized access to an unattended TOE control or management session.
T.UNAUTHORIZED_ACCESS	An entity other than an Administrator or Operator may gain unauthorized access (view, modify, delete) to TOE data. A malicious entity (Subscriber or attacker), process, or external IT entity may: • masquerade as an Administrator or Operator to gain unauthorized access to TOE data or resources; or • misrepresent itself as the TOE to obtain Administrator or Operator identification and authentication credentials.
T.UNIDENTIFIED_ACTIONS	Malicious external entities (Subscribers or attackers) or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain unidentified by TOE Administrators or Operators leading to ineffective mitigation of their effects.

3.2 ORGANIZATIONAL SECURITY POLICIES

Table 5 defines the Organizational Security Policies (OSPs) that are to be enforced by the TOE, its operational environment, or a combination of the two.

Application Notes: *1. OSPs are security rules, procedures, or guidelines imposed (or presumed to be imposed) by the end-user Telecommunications Service Provider in its operational environment.*

2. Organizational security policies may be defined by the end-user of the TOE. Sonus Networks Inc., as the TOE developer, provides procedural security recommendations to the purchaser of the TOE in its operational user guidance documentation.

Table 5: Organizational Security Policies

Identifier	Description
P.ACCESS_BANNER	The TOE will display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators or Operators consent by accessing the TOE.

Table 5: Organizational Security Policies

	TOE Administrators will be able to prescribe the access banner contents consistent with the policies of the Telecommunications Service Provider.
P.ACCOUNTABILITY	The authorized Administrators and Operators of the TOE will be held accountable for their actions administering and operating the TOE.
P.AUTHORIZATION	The TOE will limit the extent of each user's abilities in accordance with the TOE security policy.
P.AUTHORIZED_USERS	The TOE will be operated and administered by Telecommunications Service Provider personnel who have been granted specific rights to administer the TOE. Such personnel will be "vetted" to help ensure their trustworthiness. Operator and Administrator connectivity to the TOE will be restricted. Non-administrative entities (i.e., Subscribers) will have their media packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.
P.DEPLOYED_CONFIG	The deployed configuration of the TOE in its intended environment will be: • at least as restrictive as the baseline evaluated configuration defined herein; and • configured in accordance with guidance documentation.
P.I&A	All Administrators and Operators will be identified and authenticated prior to accessing any controlled resources.
P.INTEGRITY	Security-relevant data collected and produced by the TOE will be protected from modification.
P.NEED_TO_KNOW	The TOE will limit access to data in protected resources to those authorized Administrators and Operators who have a need to know.
P.ROLES	The TOE will provide multiple administrative roles for secure administration of the TOE. These roles will be separate and distinct from each other.
P.TRACE	The TOE will provide the ability to review the actions of individual Administrators and Operators.

3.3 SECURITY ASSUMPTIONS

This section identifies the assumptions that are made about the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of the security functionality prescribed herein.

The personnel, physical, and network connectivity measures identified in the three following subsections are the minimum required to be provided by the operational environment to maintain the security of the TOE.

3.3.1 Personnel

Table 6 identifies the assumptions made regarding the personnel who will manage and operate the TOE in its intended operating environment.

Table 6: TOE Operational Environment – Personnel Assumptions

Identifier	Description
A.ACCESS	It is assumed that rights for TOE Administrators and Operators to gain access and perform operations on TOE subjects and objects are based on their membership in one or more roles (and the profiles that accompany these roles). These roles: • are granted by one of the primary TOE Administrators; and • accurately reflect the individuals' job function, responsibilities, qualifications, and/or competencies within the Telecommunications Service Provider's organization that is operating the TOE.
A.MANAGE	It is assumed that there will be one or more competent and trustworthy individuals assigned to manage TOE security. These individuals will have responsibility for the following functions: • create and maintain roles; • establish and maintain relationships among roles; and • assign users to, and revoke users from, roles.

3.3.2 Physical Environment

Table 7: TOE Operational Environment – Physical Environment Assumptions

Identifier	Description
A.PHYSICAL	It is assumed that physical security, commensurate with the value of the TOE and the data it contains and processes is provided by the operational environment.

3.3.3 Network Connectivity

The specific conditions identified in Table 8 are assumed to exist in the TOE's networked operational environment.

Table 8: TOE Operational Environment – Network Connectivity Assumptions

Identifier	Description
A.CONNECTIVITY	It is assumed that the TOE: • is connected on the Telecommunication Service Provider's core (trusted) network, and • is connected to the PSTN and the SS7 network via Telecommunication Service Provider peering relationships that are managed through procedural mechanisms that are outside the scope of this Security Target.

Table 8: TOE Operational Environment – Network Connectivity Assumptions

Identifier	Description
A.EXT_AUTHORIZATION	It is assumed that external authentication services will be available on the Telecommunication Service Provider's core network outside the TOE boundary for TOE Administrators and Operators via RADIUS. It is further assumed that the authentication services provided above are compliant with their respective definitive Internet Engineering Task Force (IETF) standards or Request for Comments (RFCs).
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the correct operation, administration and support of the TOE.
A.TIMESOURCES	It is assumed that a Network Time Protocol (NTP) server will be available in the environment for the TOE to synchronize its local subsystem clocks with for its own use in providing reliable timestamps.

4 SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means). Mappings of security objectives to assumptions, threats and organizational security policies, along with supporting rationale, are found in Section 4.3.

4.1 SECURITY OBJECTIVES FOR THE TOE

This section defines the security objectives that are to be addressed by the TOE.

Table 9: TOE Security Objectives

Identifier	Description
O.ADMIN_ROLE	The TOE will provide roles to isolate administrative and operational management actions.
O.AUDIT	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
O.DISPLAY_BANNER	The TOE will display, where appropriate, an advisory warning regarding use of the TOE that is configurable by authorized Administrators.
O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.
O.MANAGE	The TOE will provide the functions and facilities necessary to support TOE Administrators and Operators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.PROTECT	The TOE will provide mechanisms to protect TSF data and resources.
O.PROTECTED _CHANNELS	The TOE will provide cryptographic confidentiality and integrity mechanisms for TSF data while in transit to remote parts of the TOE.
O.RESOURCE_EXHAUSTION	The TOE will provide mechanisms that mitigate external entities' (Subscribers, attackers) attempts to exhaust TSF resources (e.g., Denial of Service, occupying all SSH listeners, etc.).
O.SESSION_PROTECT	The TOE will provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate alarms and send them to an Operator Workstation or to an external IT entity.

Table 9: TOE Security Objectives

Identifier	Description

O.TOE_ACCESS	The TOE will provide access control mechanisms that:
	• provide authorized users (Administrators and Operators) with logical access to the TOE; and
	• explicitly deny access to:
	  • all unauthorized users, and
	  • specific Administrators or Operators when appropriate.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means.

Table 10: Security Objectives for the Operational Environment

Identifier	Description
OE.CONNECTIVITY	The operational environment will provide: • a connection for the TOE on the Telecommunication Service Provider's core (trusted) network, and • the TOE with connections to the PSTN and the SS7 network via peering relationships established by the Telecommunications Service Provider that are managed through procedural mechanisms.
OE.CRYPTO	The operational environment will provide cryptographic mechanisms to protect select Subscriber data.
OE.DOMAIN_ISOLATION	Each TOE subsystem's operating system will maintain a domain for the TOE's own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.
OE.EXT_AUTH_SVCS	The operational environment will provide RADIUS authentication services to the TOE.
OE.EXT_TIMESOURCES	The IT operational environment will provide at least one NTP server for use by the TOE to synchronize its subsystems' internal clocks.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.

Table 10: Security Objectives for the Operational Environment

Identifier	Description
OE.SESSION_PROTECT	The operating systems upon which the TOE is installed will provide mechanisms that mitigate the risk of unattended sessions being hijacked.
OE.TRUSTED_ADMIN	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and • trusted to follow and apply all administrative guidance.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Security Objectives Rationale Related to Threats

Each of the identified threats to security identified in Section 3.1 is addressed by one or more security objectives. Table 11 below provides a mapping from the TOE and Operational Environment Security Objectives defined in Sections 4.1 and 4.2 to the identified Threats. Following this table is rationale that discusses how each threat is addressed by one or more Security Objectives.

Table 11: Mapping Between Security Objectives and Threats

	THREAT									
	T.ADMIN_ERROR	T.ADMIN_ROGUE	T.AUDIT_COMPROMISE	T.DATA_REUSE	T.RESOURCE_EXHAUSTION	T.THEFT_OF_SERVICES	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNIDENTIFIED_ACTIONS
O.ADMIN_ROLE		X								
O.AUDIT		X	X			X				X
O.I&A						X			X	
O.MANAGE	X									
O.PROTECT									X	
O.PROTECTED _CHANNELS				X						
O.RESOURCE_EXHAUSTION					X					
O.SESSION_PROTECT								X		
O.SYSTEM_MONITORING										X
O.TOE_ACCESS						X			X	
OE.CRYPTO				X						
OE.DOMAIN_ISOLATION			X		X		X			
OE.SESSION_PROTECT								X		
OE.PHYSICAL			X				X	X	X	
OE.TRUSTED_ADMIN	X	X								

4.3.1.1 T.ADMIN_ERROR

Threat:	**T.ADMIN_ERROR** An Administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.	
Objective(s):	**O.MANAGE**	The TOE will provide the functions and facilities necessary to support TOE Administrators and Operators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	OE.TRUSTED_ADMIN	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and • trusted to follow and apply all administrative guidance.
Rationale:	T.ADMIN_ERROR is countered by these security objectives as rationalized below. O.MANAGE contributes to mitigating this threat by providing the security mechanisms (e.g., tools for reviewing audit data) for administrators to perform TOE administration effectively, and to quickly alert the administrator of ineffective security policies on the TOE. OE.TRUSTED_ADMIN provides for Administrators who have been carefully screened for competence and have been provided adequate training in all aspects of installing, configuring, and operating the TOE in a secure manner, thereby also contributing to the mitigation of this threat.	

4.3.1.2 T.ADMIN_ROGUE

Threat:	**T.ADMIN_ROGUE** An authorized Administrator's or Operator's intentions may become malicious, resulting in TSF data being compromised.	
Objective(s):	**O.ADMIN_ROLE**	The TOE will provide roles to isolate administrative and operational management actions.
	O.AUDIT	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
	OE.TRUSTED_ADMIN	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and

		• trusted to follow and apply all administrative guidance.
Rationale:	T.ADMIN_ROGUE is countered by the three security objectives as rationalized below. O.ADMIN_ROLE: It is important to limit the functionality of administrative roles. If the intentions of an individual in an administrative role become malicious, O.ADMIN_ROLE mitigates this threat by isolating the administrative actions within that role and limiting the functions available to that individual. This objective presumes that separate individuals will be assigned separate distinct roles with no overlap of allowed operations between the roles. O.AUDIT: While an audit capability doesn't necessarily stop an Administrator or Operator from carrying out malicious activities, it contributes to the mitigation of this threat by providing Administrators with the ability to review security-relevant events and determine cause, including what user account or role caused an audit event to be recorded. OE.TRUSTED_ADMIN also contributes to mitigating this threat by requiring that Administrators and Operators are carefully screened for trustworthiness by the organization.	

4.3.1.3 T.AUDIT_COMPROMISE

Threat:	**T.AUDIT_COMPROMISE** A malicious external entity (Subscriber or attacker) or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded.	
Objective(s):	**OE.PHYSICAL**	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.
	O.AUDIT	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
	OE.DOMAIN_ISOLATION	Each TOE subsystem's operating system will maintain a domain for the TOE's own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.
Rationale:	T.AUDIT_COMPROMISE is countered by these security objects as rationalized below. Tampering with, or destruction of, audit data by physical means is addressed by OE.PHYSICAL, which provides physical security controls to the TOE environment, thereby contributing the mitigation of this threat. O.AUDIT provides the capability to detect and create records of security relevant events. Audit records identify the user responsible for the event and	

	are an important form of evidence that can be used to track an attacker's actions. O.AUDIT also provides the capability to specifically protect audit information from external interference, tampering, or unauthorized disclosure, thereby mitigating the threat. OE.DOMAIN_ISOLATION protects the TOE and its resources (including audit data) by ensuring that the security policies implemented by the TOE to protect the audit information are always invoked by the TOE's subsystems' underlying operating systems and thus mitigating the threat.

4.3.1.4 T.DATA_REUSE

Threat:	**T.DATA_REUSE** A malicious entity attempts to reuse TSF data in order to bypass the TOE Security Policy.	
Objective(s):	**O.PROTECTED _CHANNELS**	The TOE will provide cryptographic confidentiality and integrity mechanisms for TSF data while in transit to remote parts of the TOE.
	OE.CRYPTO	The operational environment will provide cryptographic mechanisms to protect select Subscriber data.
Rationale:	T.DATA_REUSE is countered by these security objects as rationalized below. O.PROTECTED _CHANNELS mitigates this threat by enforcing cryptographic integrity checks that include measures designed to detect and thwart attempts to replay TSF data. Similarly, application of OE.CRYPTO by the IT environment uses cryptographic integrity mechanisms that include measures that are designed to detect and thwart attempts to replay select Subscriber data as it transverses the TOE thereby mitigating this threat.	

4.3.1.5 T.RESOURCE_EXHAUSTION

Threat:	**T.RESOURCE_EXHAUSTION** A malicious process or entity (Subscriber or attacker) may block others from system resources via a resource exhaustion denial of service attack.	
Objective(s):	**O.RESOURCE_EXHAUSTION**	The TOE will provide mechanisms that mitigate external entities' (Subscribers, attackers) attempts to exhaust TSF resources (e.g., Denial of Service, occupying all SSH listeners, etc.).
	OE.DOMAIN_ISOLATION	Each TOE subsystem's operating system will maintain a domain for the TOE's own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

Rationale:	T.RESOURCE_EXHAUSTION is significantly diminished by these security objectives as discussed below. O.RESOURCE_EXHAUSTION helps mitigate this threat by ensuring that the TOE includes mechanisms to mitigate attempts by external entities to capture and exhaust TSF resources. The TOE provides wire-speed mechanisms to protect itself against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks originating outside the core (trusted) network that include the following: • IP packet validation, discarding non-conforming packets without further processing; • Media packet validation, discarding non-conforming packets without further processing; • Source-based filtering including black, white, and light and dark gray listing; and • Dynamically setting discard rate profiles to ensure that the rate of incoming packets stay below a threshold value, otherwise they are discarded as non-conforming. OE.DOMAIN_ISOLATION contributes to mitigation of this threat by ensuring that the TOE's underlying operating systems ensure that resources remain committed and allocated to core TOE security functionality when faced with competing resource allocation requirements.

4.3.1.6 T.THEFT_OF_SERVICES

Threat:	**T.THEFT_OF_SERVICES** A malicious entity (Subscriber or attacker) exploits a flaw in the TOE or the IT operational environment to use telecommunications services without being charged by the Telecommunications Service Provider.	
Objective(s):	**O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.

	O.TOE_ACCESS	The TOE will provide access control mechanisms that:
		• provide authorized users (Administrators and Operators) with logical access to the TOE; and
		• explicitly deny access to:
		  • all unauthorized users, and
		  • specific Administrators or Operators when appropriate.

	O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and

		Operators) before granting access to controlled resources.
Rationale:	T.THEFT_OF_SERVICES is countered by these security objectives as discussed below. O.TOE_ACCESS contributes to mitigating this threat by ensuring that only authorized users have access to TOE services. O.I&A contributes to mitigating this threat by uniquely identifying and authenticating the claimed identities of administrative and operations personnel prior to granting them access to the TOE and its services. O.AUDIT contributes to the mitigation of this threat by ensuring that security events relative to Subscriber attempts to steal TOE services are recorded for follow-up action by the Telecommunications Service Provider.	

4.3.1.7 T.TSF_COMPROMISE

Threat:	**T.TSF_COMPROMISE** A malicious external entity (Subscriber or an attacker) or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified or deleted).	
Objective(s):	**OE.DOMAIN_ISOLATION**	Each TOE subsystem's operating system will maintain a domain for the TOE's own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.
	OE.PHYSICAL	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.
Rationale:	T.TSF_COMPROMISE is countered by these security objectives as discussed below. The tampering with or destruction of TSF hardware, software, or configuration data via physical means by a malicious external entity is mitigated by the physical security controls present in the TOE environment (OE.PHYSICAL). OE.DOMAIN_ISOLATION diminishes the threat of tampering with or destruction of TSF hardware, software, or configuration data by other (non-physical) means. It ensures that the TOE subsystems' host operating systems each maintain a security domain for execution of the TSF that protects it from interference and tampering by untrusted subjects and enforces the separation between the security domains of subjects within the TOE scope of control.	

4.3.1.8 T.UNATTENDED_SESSION

Threat:	**T.UNATTENDED_SESSION** An entity other than an Administrator or Operator may gain unauthorized access to an unattended TOE control or management session.

Objective(s):	**O.SESSION_PROTECT**	The TOE will provide mechanisms that mitigate the risk of unattended sessions being hijacked.
	OE.SESSION_PROTECT	The operating systems upon which the TOE is installed will provide mechanisms that mitigate the risk of unattended sessions being hijacked.
	OE.PHYSICAL	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.
Rationale:	T.UNATTENDED_SESSION is countered by these security objectives as discussed below. When an authorized Administrator or Operator leaves an active session unattended, an unauthorized person may gain access to the unattended session. O.SESSION_PROTECT mitigates this threat by providing mechanisms to protect Operator and Administrator data and resources from unauthorized access by ensuring that the TSF will lock an interactive session and make the visible contents unreadable after a specified time interval of session inactivity. Similarly, for those TOE subsystems that do not provide this capability, OE.SESSION_PROTECT ensures that the subsystem's underlying operating system is configured to either lock or automatically terminate an interactive session after a specified time interval of session inactivity thereby mitigating the threat. OE.PHYSICAL contributes to mitigating this threat by ensuring that only authorized Administrators and Operators have physical access to the TOE subsystem consoles and the TOE management system (EMS).	

4.3.1.9 T.UNAUTHORIZED_ACCESS

Threat:	**T.UNAUTHORIZED_ACCESS** An entity other than an Administrator or Operator may gain unauthorized access (view, modify, delete) to TOE data. A malicious entity (Subscriber or attacker), process, or external IT entity may: • masquerade as an Administrator or Operator to gain unauthorized access to TOE data or resources; or • misrepresent itself as the TOE to obtain Administrator or Operator identification and authentication credentials.	

Objective(s):	**O.TOE_ACCESS**	The TOE will provide access control mechanisms that:
		• provide authorized users (Administrators and Operators) with logical access to the TOE; and
		• explicitly deny access to:
		  • all unauthorized users, and
		  • specific Administrators or Operators when appropriate.

	O.PROTECT	The TOE will provide mechanisms to protect TSF data and resources.
	OE.PHYSICAL	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.
	O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.
Rationale:	T.UNAUTHORIZED_ACCESS is countered by these security objectives as discussed below. Unauthorized users may physically access TOE resources. To mitigate this threat, OE.PHYSICAL restricts the physical access only to authorized personnel. O.TOE_ACCESS and O.I&A mitigate this threat by restricting all access controls to authorized users based on their user identity. At the same time, O.PROTECT enforces access rules by providing mechanisms to prevent the TSF data from unauthorized disclosure and modification, thereby mitigating this threat.	

4.3.1.10 T.UNIDENTIFIED_ACTIONS

Threat:	**T.UNIDENTIFIED_ACTIONS** Malicious external entities (Subscribers or attackers) or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain unidentified by TOE Administrators or Operators leading to ineffective mitigation of their effects.	
Objective(s):	**O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
	O.SYSTEM_MONITORING	The TOE will provide the capability to generate alarms and send them to an Operator Workstation or to an external IT entity.
Rationale:	T.UNIDENTIFIED_ACTIONS is countered by these security objectives as discussed below. The threat of an Administrator or Operator failing to know about audit events may occur. To mitigate this threat, O.AUDIT provides the capability to selectively view audit information, and alert the Administrator or Operator of identified potential security violations. O.SYSTEM_MONITORING results in the generation of prioritized aural and visual alerts on the operator management station so that timely action can be taken by Administrators or Operators, thereby mitigating this threat.	

4.3.2 Environment Security Objectives Rationale Related to Assumptions

Table 12 maps the security objectives for the Operational Environment to the Security Assumptions. Following this table is rationale that discusses how each Assumption is addressed by one or more Operational Environment Security Objectives.

Table 12: Mapping Between Security Objectives and Assumptions

	SECURITY ASSUMPTION						
	A.ACCESS	A.CONNECTIVITY	A.EXT_AUTHORIZATION	A.MANAGE	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TIMESOURCES
OE.CONNECTIVITY		X					
OE.EXT_AUTH_SVCS			X				
OE.EXT_TIMESOURCES							X
OE.NO_GENERAL_PURPOSE					X		
OE.PHYSICAL						X	
OE.TRUSTED_ADMIN	X			X			

4.3.2.1 A.ACCESS

Assumption:	**A.ACCESS** It is assumed that rights for TOE Administrators and Operators to gain access and perform operations on TOE subjects and objects are based on their membership in one or more roles (and the profiles that accompany these roles). These roles: • are granted by one of the primary TOE Administrators; and • accurately reflect the individuals' job function, responsibilities, qualifications, and/or competencies within the Telecommunications Service Provider's organization that is operating the TOE.	
Objective(s):	**OE.TRUSTED_ADMIN**	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and • trusted to follow and apply all administrative guidance.
Rationale:	OE.TRUSTED_ADMIN meets this assumption in that the TOE Administrators and Operators charged with running the TOE have been selected by their employer to fulfill the roles assumed in A.ACCESS.	

4.3.2.2 A.CONNECTIVITY

Assumption:	**A.CONNECTIVITY** It is assumed that the TOE: • is connected on the Telecommunication Service Provider's core (trusted) network, and • is connected to the PSTN and the SS7 network via Telecommunication Service Provider peering relationships that are managed through procedural mechanisms that are outside the scope of this Security Target.	
Objective(s):	**OE.CONNECTIVITY**	The operational environment will provide: • a connection for the TOE on the Telecommunication Service Provider's core (trusted) network, and • the TOE with connections to the PSTN and the SS7 network via peering relationships established by the Telecommunications Service Provider that are managed through procedural mechanisms.
Rationale:	OE.CONNECTIVITY ensures that the TOE is placed within a networked environment that is both suitable for the TOE security functionality it is providing, and protected from threats originating from the external, untrusted IP-based network(s). Furthermore, this objective ensures that the TOE end user (e.g., a Telecommunications Service Provider) establishes formal (e.g. contractual) peering relationships with other telecommunications providers prior to establishing connections to the PSTN and SS7 networks by the TOE.	

4.3.2.3 A.EXT_AUTHORIZATION

Assumption:	**A.EXT_AUTHORIZATION** It is assumed that external authentication services will be available on the Telecommunication Service Provider's core network outside the TOE boundary for TOE Administrators and Operators via RADIUS. It is further assumed that the authentication services provided above are compliant with their respective definitive Internet Engineering Task Force (IETF) standards or Request for Comments (RFCs).	
Objective(s):	**OE.EXT_AUTH_SVCS**	The operational environment will provide RADIUS authentication services to the TOE.
Rationale:	OE.EXT_AUTH_SVCS meets the assumption by providing the external authentication services needed by the TSF.	

4.3.2.4 A.MANAGE

Assumption:	**A.MANAGE** It is assumed that there will be one or more competent and trustworthy

	individuals assigned to manage TOE security. These individuals will have responsibility for the following functions: • create and maintain roles; • establish and maintain relationships among roles; and • assign users to, and revoke users from, roles.	
Objective(s):	**OE.TRUSTED_ADMIN**	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and • trusted to follow and apply all administrative guidance.
Rationale:	OE.TRUSTED_ADMIN meets this assumption by ensuring that the organization deploying the TOE selects and trains competent personnel to administer and operate the TOE.	

4.3.2.5 A.NO_GENERAL_PURPOSE

Assumption:	**A.NO_GENERAL_PURPOSE** It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the correct operation, administration and support of the TOE.	
Objective(s):	**OE.NO_GENERAL_PURPOSE**	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
Rationale:	OE.NO_GENERAL_PURPOSE meets the assumption by ensuring that the computer systems upon which the TOE software is deployed are dedicated solely to the TOE for its delivery of the TOE Security Functionality.	

4.3.2.6 A.PHYSICAL

Assumption:	**A.PHYSICAL** It is assumed that physical security, commensurate with the value of the TOE and the data it contains and processes is provided by the operational environment.	
Objective(s):	**OE.PHYSICAL**	Physical security will be provided for the TOE by the IT environment, commensurate with the value of the IT assets protected by the TOE.
Rationale:	Physical security must be provided for the TOE by the IT environment to ensure that the TOE is capable of addressing the threats to TOE assets (OE.PHYSICAL).	

4.3.2.7 A.TIMESOURCES

Assumption:	**A.TIMESOURCES** It is assumed that a Network Time Protocol (NTP) server will be available in the environment for the TOE to synchronize its local subsystem clocks with for its own use in providing reliable timestamps.	
Objective(s):	**OE.EXT_TIMESOURCES**	The IT operational environment will provide at least one NTP server for use by the TOE to synchronize its subsystems' internal clocks.
Rationale:	OE.EXT_TIMESOURCES ensures that the IT environment provides the required external time sources needed by the TOE so that it can both: (a) interoperate correctly with the other IT entities that it interfaces with, and (b) provide reliable timestamps for its audit records that are correctly synchronized across the distributed parts of the TOE.	

4.3.3 Security Objectives Rationale Related to Organizational Security Policies

Table 13 maps the security objectives for the TOE and the Operational Environment to the Organizational Security Policies. Following this table is rationale that discusses how each Organizational Security Policy is addressed by one or more Security Objectives.

Table 13: Mapping Between Security Objectives and Organizational Security Policies

	ORGANIZATIONAL SECURITY POLICIES									
	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.AUTHORIZATION	P.AUTHORIZED_USERS	P.DEPLOYED_CONFIG	P.I&A	P.INTEGRITY	P.NEED_TO_KNOW	P.ROLES	P.TRACE
O.ADMIN_ROLE									X	
O.AUDIT		X					X			X
O.DISPLAY_BANNER	X									
O.I&A		X	X			X				
O.PROTECT			X				X	X		
O.TOE_ACCESS			X	X				X		
OE.NO_GENERAL_PURPOSE					X					
OE.TRUSTED_ADMIN					X					

4.3.3.1 P.ACCESS_BANNER

Policy:	**P.ACCESS_BANNER** The TOE will display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators or Operators consent by accessing the TOE.

	TOE Administrators will be able to prescribe the access banner contents consistent with the policies of the Telecommunications Service Provider.	
Objective(s):	**O.DISPLAY_BANNER**	The TOE will display, where appropriate, an advisory warning regarding use of the TOE that is configurable by authorized Administrators.
Rationale:	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays a banner that provides authorized Administrators and Operators with an advisory warning about the unauthorized use of the TOE.	

4.3.3.2 P.ACCOUNTABILITY

Policy:	**P.ACCOUNTABILITY** The authorized Administrators and Operators of the TOE will be held accountable for their actions administering and operating the TOE.	
Objective(s):	**O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
	O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.
Rationale:	Enforcement of this policy requires that users be uniquely identified (O.I&A) and that their security relevant actions be monitored and recorded (O.AUDIT). The recorded audit information can be selectively reviewed in search of any potential security violations (O.AUDIT).	

4.3.3.3 P.AUTHORIZATION

Policy:	**P.AUTHORIZATION** The TOE will limit the extent of each user's abilities in accordance with the TOE security policy.	

Objective(s):	**O.TOE_ACCESS**	The TOE will provide access control mechanisms that:
		• provide authorized users (Administrators and Operators) with logical access to the TOE; and
		• explicitly deny access to:
		  • all unauthorized users, and
		  • specific Administrators or Operators when appropriate.

	O.PROTECT	The TOE will provide mechanisms to protect TSF data and resources.

	O.I&A	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.
Rationale:	O.TOE_ACCESS and O.I&A support this policy by requiring the TOE to uniquely identify authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users. Within the TOE, O.PROTECT provides mechanisms to prevent TSF data from unauthorized disclosure and modification.	

4.3.3.4 P.AUTHORIZED_USERS

Policy:	**P.AUTHORIZED_USERS** The TOE will be operated and administered by Telecommunications Service Provider personnel who have been granted specific rights to administer the TOE. Such personnel will be "vetted" to help ensure their trustworthiness. Operator and Administrator connectivity to the TOE will be restricted. Non-administrative entities (i.e., Subscribers) will have their media packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.	
Objective(s):	**O.TOE_ACCESS**	The TOE will provide access control mechanisms that: • provide authorized users (Administrators and Operators) with logical access to the TOE; and • explicitly deny access to: o all unauthorized users, and o specific Administrators or Operators when appropriate.
Rationale:	Within the set of all the users (Administrators and Operators) that may interact with the TOE, authorized users are those with access to the information within the TOE after being successfully identified and authenticated by the TOE. Access control policies are used by the TOE to define the access permitted to the system and its resources. These policies are supported by the implementation of authorized user attributes that identify the user-allowed accesses to TOE information. O.TOE_ACCESS supports this policy by ensuring that users only gain authorized access to TOE information and its resources by checking user attributes before system use.	

4.3.3.5 P.DEPLOYED_CONFIG

Policy:	**P.DEPLOYED_CONFIG** The deployed configuration of the TOE in its intended environment will be:

	• at least as restrictive as the baseline evaluated configuration defined herein; and • configured in accordance with guidance documentation.	
Objective(s):	**OE.TRUSTED_ADMIN**	Personnel working as authorized TOE Administrators and Operators are: • carefully selected and trained for proper operation of the TOE; and • trusted to follow and apply all administrative guidance.
	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
Rationale:	OE.TRUSTED_ADMIN contributes to meeting this policy in that the TOE Administrators are trusted to follow and apply all security-related guidance provided by the Developer, included the application of the latest security patches when released. The TOE will not have extraneous software or applications installed on it (OE.NO_GENERAL_PURPOSE) which helps to reduce the attack surface of the TOE, thereby also contributing to satisfaction of this policy.	

4.3.3.6 P.I&A

Policy:	**P.I&A** All Administrators and Operators will be identified and authenticated prior to accessing any controlled resources.	
Objective(s):	**O.I&A**	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.
Rationale:	In support of the policy to identify and authenticate a user (Administrator or Operator) before access is granted to any controlled resources, O.I&A will uniquely identify and authenticate the claimed authorized users.	

4.3.3.7 P.INTEGRITY

Policy:	**P.INTEGRITY** Security-relevant data collected and produced by the TOE will be protected from modification.	
Objective(s):	**O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized

		Administrators for review.
	O.PROTECT	The TOE will provide mechanisms to protect TSF data and resources.
Rationale:	O.PROTECT provides mechanisms to prevent TSF data from unauthorized disclosure and modification. O.AUDIT will record information about security-relevant events and store than in a protected log file that is viewable by authorized administrative and operational personnel (Administrators or Operators).	

4.3.3.8 P.NEED_TO_KNOW

Policy:	**P.NEED_TO_KNOW** The TOE will limit access to data in protected resources to those authorized Administrators and Operators who have a need to know.	
Objective(s):	**O.TOE_ACCESS**	The TOE will provide access control mechanisms that: • provide authorized users (Administrators and Operators) with logical access to the TOE; and • explicitly deny access to: • all unauthorized users, and • specific Administrators or Operators when appropriate.
	O.PROTECT	The TOE will provide mechanisms to protect TSF data and resources.
Rationale:	O.TOE_ACCESS ensures that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE scope of control is allowed to proceed. O.PROTECT enforces this policy by providing the mechanisms to protect the TSF data from disclosure and modification.	

4.3.3.9 P.ROLES

Policy:	**P.ROLES** The TOE will provide multiple administrative roles for secure administration of the TOE. These roles will be separate and distinct from each other.	
Objective(s):	**O.ADMIN_ROLE**	The TOE will provide roles to isolate administrative and operational management actions.
Rationale:	To appropriately administer the system, O.ADMIN_ROLE requires the system to provide multiple administrator and operator roles to isolate actions performed by these different roles.	

4.3.3.10 P.TRACE

Policy:	**P.TRACE** The TOE will provide the ability to review the actions of individual Administrators and Operators.	
Objective(s):	**O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.
Rationale:	A common organizational security policy is to maintain records allowing for individuals to be held responsible for the actions that they take with respect to organizational assets. Information can be one of the most valuable assets that an organization possesses. To satisfy this policy, O.AUDIT provides suitable mechanisms to accurately and selectively review those records by authorized personnel to provide accountability at the individual user level to determine any potential security violation	

4.3.4 Security Objectives Summary Mapping

This section provides a consolidated summary of the three previous sections demonstrating that each organizational security policy, threat and assumption maps to no less than one security objective.

Table 14: Security Objectives Summary Map

	TOE Security Objectives											Environment Security Objectives								
Organizational Security Policies	**O.ADMIN_ROLE**	**O.AUDIT**	**O.DISPLAY_BANNER**	**O.I&A**	**O.MANAGE**	**O.PROTECT**	**O.PROTECTED_CHANNELS**	**O.RESOURCE_EXHAUSTION**	**O.SESSION_PROTECT**	**O.SYSTEM_MONITORING**	**O.TOE_ACCESS**	**OE.CONNECTIVITY**	**OE.CRYPTO**	**OE.DOMAIN_ISOLATION**	**OE.EXT_AUTH_SVCS**	**OE.EXT_TIMESOURCES**	**OE.NO_GENERAL_PURPOSE**	**OE.SESSION_PROTECT**	**OE.PHYSICAL**	**OE.TRUSTED_ADMIN**
P.ACCESS_BANNER			X																	
P.ACCOUNTABILITY		X		X																
P.AUTHORIZATION				X		X					X									
P.AUTHORIZED_USERS											X									
P.DEPLOYED_CONFIG																	X			X
P.I&A				X																
P.INTEGRITY		X				X														
P.NEED_TO_KNOW						X					X									
P.ROLES	X																			
P.TRACE		X																		

Table 14: Security Objectives Summary Map

	TOE Security Objectives											Environment Security Objectives								
	O.ADMIN_ROLE	O.AUDIT	O.DISPLAY_BANNER	O.I&A	O.MANAGE	O.PROTECT	O.PROTECTED_CHANNELS	O.RESOURCE_EXHAUSTION	O.SESSION_PROTECT	O.SYSTEM_MONITORING	O.TOE_ACCESS	OE.CONNECTIVITY	OE.CRYPTO	OE.DOMAIN_ISOLATION	OE.EXT_AUTH_SVCS	OE.EXT_TIMESOURCES	OE.NO_GENERAL_PURPOSE	OE.SESSION_PROTECT	OE.PHYSICAL	OE.TRUSTED_ADMIN
Threats																				
T.ADMIN_ERROR					X															X
T.ADMIN_ROGUE	X	X																		X
T.AUDIT_COMPROMISE		X												X					X	
T.DATA_REUSE							X						X							
T.RESOURCE_EXHAUSTION								X						X						
T.THEFT_OF_SERVICES		X		X							X									
T.TSF_COMPROMISE														X					X	
T.UNATTENDED_SESSION									X									X	X	
T.UNAUTHORIZED_ACCESS				X		X					X								X	
T.UNIDENTIFIED_ACTIONS		X								X										
Assumptions																				
A.ACCESS																				X
A.CONNECTIVITY												X								
A.EXT_AUTHORIZATION															X					
A.MANAGE																				X
A.NO_GENERAL_PURPOSE																	X			
A.PHYSICAL																			X	
A.TIMESOURCES																X				

5 EXTENDED COMPONENTS DEFINITION

This Security Target does not define any extended components for the TOE.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 SECURITY REQUIREMENTS PRESENTATION CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets and bolded, e.g., [**selected item**]. To improve readability selections of [**none**] are generally not shown.
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*]. To improve readability assignments of [*none*] are not shown unless doing so aids in the readability and understandability of the specified requirement.
- Refinement: Refined components are identified by using underlining additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_IFC.1(1), Subset Information Flow Control (Peered Policy)' and 'FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC.

Table 15: Summary of Security Functional Requirements

Class	Identifier	Name
Security Audit (FAU)	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential Violation Analysis
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in Case of Possible Audit Data Loss
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic Operation
User Data Protection (FDP)	FDP_IFC.1(1)	Subset Information Flow Control (Peered Policy)
	FDP_IFC.1(2)	Subset Information Flow Control (Authenticated Policy)
	FDP_IFC.1(3)	Subset Information Flow Control (Encrypted

Table 15: Summary of Security Functional Requirements

Class	Identifier	Name
		Channel Policy)
	FDP_IFF.1(1)	Simple Security Attributes (Peered Policy)
	FDP_IFF.1(2)	Simple Security Attributes (Authenticated Policy)
	FDP_IFF.1(3)	Simple Security Attributes (Encrypted Channel Policy)
	FDP_UCT.1	Basic Data Exchange Confidentiality
Identification and Authentication (FIA)	FIA_AFL.1(1)	Authentication Failure Handling (EMS GUI)
	FIA_AFL.1(2)	Authentication Failure Handling (CLI Access)
	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.5	Multiple Authentication Mechanisms
	FIA_UID.2	User Identification Before Any Action
Security Management (FMT)	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MSA.1(1)	Management of Security Attributes (Peered Policy)
	FMT_MSA.1(2)	Management of Security Attributes (Authenticated Policy)
	FMT_MSA.1(3)	Management of Security Attributes (Encrypted Channel Policy)
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SAE.1	Time-limited Authorization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_STM.1	Reliable Time Stamps
	FPT_TDC.1	Inter-TSF Basic TSF Data Consistency
Resource Utilization (FRU)	FRU_PRS.1	Limited Priority of Service
	FRU_RSA.1	Maximum Quotas
TOE Access (FTA)	FTA_SSL.3	TSF-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
Trusted path/channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ARP.1 Security Alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential Violation Analysis

FAU_ARP.1.1 The TSF shall take [*the following action(s):*

a) *record the security-relevant event into the log, including:*

i. Timestamp - displays the date and time the alarm occurred,

ii. Description - short textual description on the cause of the alarm,

iii. Reporter – identification of the component that reported the alarm, and

iv. Severity - criticality of the alarm;

b) *utilize SNMP traps to report events to the EMS subsystem; and*

c) *provide a visual and/or audible alarm on the EMS management terminal*]

upon detection of a potential security violation.

6.2.1.2 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) start-up and shutdown of the audit functions;

b) all auditable events for the [**not specified**] level of audit; and

c) [*the auditable events identified in column 2 of Table 16*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) date and time of the event, type of event, subject identity (if applicable), and the outcome (success, ~~or~~ failure, or detail of the action that generated the audit event) of the event; and

b) for each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*any additional audit information identified in column 3 of Table 16*].

Table 16: Audit Data Generation (FAU_GEN.1)

Functional Component	Auditable Event	Additional Audit Information
FDP_UCT.1	The identity of each subject using SIP over TLS signaling.	None
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken.	None
FIA_UAU.2	Unsuccessful use of the authentication mechanism	None
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FMT_MOF.1	All modifications to the behaviour of functions in the TSF	None
FMT_MTD.1	Modifications to the values of TSF data	None
FMT_SMF.1	Use of the management function	None
FMT_SMR.1	Modification to the group of users that are part of a role	None
FRU_RSA.1	Rejection of allocation operation due to resource limits	None
FRU_PRS.1	Failure to complete a high priority call	None
FTP_ITC.1	Failure of the trusted channel function(s)	None

6.2.1.3 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FIA_UID.1 Timing of Identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.4 FAU_SAA.1 Potential Violation Analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*Administrator-defined packet discard rates and durations for the following event types:*

i. white list discards (packets from known friendly peers);

ii. black list discards (packets from known attacking peers);

iii. darkgray discards (packets from unknown peers);

iv. lightgray discards (packets from registered peers);

v. per VLAN discards (packets destined for particular logical interfaces that have otherwise been validated by white list, lightgray, and darkgray policers);

vi. media discards (rtp packets);

vii. "rogue media with bad source" discards (media packets containing an unexpected source address);

viii. "rogue media with unallocated port" discards (media packets containing an unexpected destination port number); or

ix. SERVER PROTECT discards (signaling and control packets that exceed the system overall IP bandwidth limits)

] known to indicate a potential security violation; and

b) [*For each of these events, an events per second threshold value prescribed by the Administrator (or higher) must be maintained for an Administrator-specified duration (in seconds) to trigger the associated alarm. To clear the alarm a lesser Administrator-defined threshold must be maintained for an Administrator-specified duration (in seconds).*]

6.2.1.5 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1 The TSF shall provide [*Administrators and authorized Operators*] with the capability to read [*all audit information listed in Table 16*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.6 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.7 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to ~~apply~~ [*filter and sort*] ~~of~~ audit data based on [:

a) *Event Name;*

b) *Severity;*

c) *Owner;*

d) *Type;*

e) *Device;*

f) *Time;*

g) *Count; and*

h) *Summary (textual description of event)*].

Application Note: The default sort order for the above is descending chronological, by last event. Times are normalized to the time-zone setting of the EMS server.

6.2.1.8 FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [**object identity, event type**]

b) *[where object identity may be:*

i. GSX subsystem,

ii. SGX subsystem,

iii. PSX subsystem,

iv. DSI subsystem, or

v. EMS subsystem; and

c) *where event type may be:*

i. SNMP traps, set to either:

(1) "enabled", or

(2) "disabled"; or

ii. Administrator-defined alarm threshold values:

(1) CPU usage,

(2) memory usage;

(3) swap space usage,

(4) file system usage, or

(5) application CPU usage; or

iii. associated with any of the following for the GSX subsystem:

(1) software subsystem,

(2) severity, or

(3) *GSX module.*]

6.2.1.9 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorized modifications to the stored audit records in the audit trail.

Application Note: *None of the user roles specified by FMT_SMR.1 at Section 6.2.5.9 have "modify" or "delete" access to the audit records. Should the administrator need to delete audit records outside the normal course of day-to-day operations, access to the underlying operating system (IT operational environment) administrator / root account via its CLI is required, which is outside the control of the TSF.*

6.2.1.10 FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected Audit Trail Storage

FAU_STG.3.1 The TSF shall [*rotate log files and delete the oldest*] ~~if~~ when the audit trail exceeds [

a) 10 MB for individual SNMP trap logs up to a maximum limit configured by the Administrator; and

b) *an Administrator-specified maximum file size for all remaining audit log files*].

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations identified in column 2 of Table 17*] in accordance with a specified cryptographic algorithm [*multiple algorithms as identified in column 3 of Table 17*] and cryptographic key sizes [*multiple key sizes or output size as applicable for the cryptographic operation as identified in column 4 of Table 17*] that meet the following: [*the applicable referenced standard in column 5 of Table 17*].

Table 17: TSF Cryptographic Operations

ID	Operation	Algorithm (Mode)	Key Size or Digest Size (bits)	Standard	CAVP Cert No.
FCS_COP.1.1(1)	Symmetric encryption / decryption	AES (CBC)	128, 192, 256	**[FIPS PUB 197]**	2117
FCS_COP.1.1(2)	Asymmetric encryption / decryption	RSA	1024	PKCS #1, v1.5 **[RFC 2313]**	1098
FCS_COP.1.1(3)	Message Digest	SHS (SHA-1)	160	**[FIPS PUB 180-4]**	1841
FCS_COP.1.1(4)	HMAC	HMAC-SHA-1	Key: 160 Digest: 160	**[FIPS PUB 198-1]**	1289

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1(1) Subset Information Flow Control (Peered Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(1) Simple security attributes

FDP_IFC.1(1).1 The TSF shall enforce the [*PEERED INFORMATION FLOW CONTROL SFP*] on [

a) *Subjects: each IT entity that sends and receives information through the TOE;*

b) *Information: traffic sent through the TOE from one subject to another; and*

c) *Operations: receive or drop information*].

6.2.3.2 FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(2) Simple security attributes

FDP_IFC.1(2).1 The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW CONTROL SFP*] on [

a) *Subjects: TOE identifiers representing either authenticated system Administrators or system Operators;*

b) *Information: EMS subsystem initiated traffic and CLI commands; and*

c) *Operations: administration and operations management commands*].

6.2.3.3 FDP_IFC.1(3) Subset Information Flow Control (Encrypted Channel Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1(3) Simple security attributes

FDP_IFC.1(3).1 The TSF shall enforce the [*ENCRYPTED INFORMATION FLOW CONTROL SFP*] on [

a) *Subjects – TOE interfaces;*

b) *Information – network packets; and*

c) *Operations – SSH (including SFTP and SCP), TLS, IPSec, and HTTPS*].

Application Note: The ENCRYPTED INFORMATION FLOW CONTROL SFP is used to enforce intra-TOE channel security in support of operating and administering TOE subsystems via the EMS management interfaces over HTTPS, TLS, and SSH. It also enforces channel security for secure signaling for the GSX TOE subsystem by transporting signaling protocols over TLS or IPSec.

6.2.3.4 FDP_IFF.1(1) Simple Security Attributes (Peered Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(1) Subset Information Flow Control

FMT_MSA.3 Static Attribute Initialization

FDP_IFF.1(1).1 The TSF shall enforce the [*PEERED INFORMATION FLOW CONTROL SFP*] based on the following types of subject and information security attributes: [

a) *subject security attributes:*

i. presumed IP address; and

b) *information security attributes:*

i. protocol,

ii. interface (NIF or subinterface (SIF[13])) range,

iii. presumed IP address of source subject,

iv. presumed IP address of destination subject,

v. source port number or range,

vi. destination port number or range,

vii. packet type:

[13] Each SIF is assigned to a NIF, and given a unique name and IEEE 802.1q compliant-number (i.e., VLAN tag).

(1) Media,

(2) Signaling, and

(3) Management,

viii. packet rate, and

ix. *registered or registering peers (i.e., SIP endpoints)*].

Application Note: *The GSX subsystem provides the Administrator or authorized Operator with a number of configurable media Policers through which packets must be accepted, or they are dropped.*

FDP_IFF.1(1).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) *subjects on the internal network can cause information to flow to the TOE if the presumed IP address of the source subject translates to an internal network IP address.*

b) *subjects on an external packet-based connected network can cause information to flow through the GSX subsystem to TOE subsystems and other IT entities connected on the internal network if:*

i. all the information security attribute values are unambiguously permitted by the information flow security policy rules defined in the GSX subsystem, where such rules:

(1) may be composed from all possible combinations of the values of the information flow security attributes, and

(2) are created by an authorized System Administrator or Operator;

ii. the presumed address of the source subject, in the information, translates to a network address on the other connected network; and

iii. *the address of the destination subject, in the information, translates to an address on the trusted network.*].

FDP_IFF.1(1).3 The TSF shall enforce ~~the~~ [*no additional rules*].

FDP_IFF.1(1).4 The TSF shall explicitly authorize an information flow based on the following rules: [*an authorized Operator or System Administrator shall have the capability to view all information flows allowed by the information flow policy rule set before the rule set is applied*].

FDP_IFF.1(1).5 The TSF shall explicitly deny an information flow based on the following rules: [

a) *The TOE shall reject requests for access or services where the information arrives on an external GSX subsystem interface, and the presumed address of the source subject is an internal IT entity on the internal network;*

b) *The TOE shall reject requests for access or services where the information arrives on the internal GSX subsystem interface, and the presumed address of the source subject is an external IT entity on the external network; and*

c) *The GSX subsystem shall drop media packets that meet its rogue media quarantine function tests*].

Application Note: *The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Thus, a "presumed address" is used to identify source and destination addresses.*

6.2.3.5 FDP_IFF.1(2) Simple Security Attributes (Authenticated Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(2) Subset Information Flow Control

FMT_MSA.3 Static Attribute Initialization

FDP_IFF.1(2).1 The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW CONTROL SFP*] based on the following types of subject and information security attributes: [

a) *Subject security attributes:*

i. source and destination port and IP address,

ii. protocol,

iii. username/password or account/password,

iv. user profile, and

v. user session idle timeout; and

b) *Information security attributes:*

i. authenticated identity of source subject,

ii. identity of destination subject and,

iii. *administrative or operations mechanism and the transport layer protocol carrying it*].

Application Note: *The administrative or operations mechanism identified at (b)(iii) above refers to the management protocol or administrative commands being transported between TOE subsystems over the TOE communications channels and internal interfaces as depicted on Figure 3 (p. 24). Examples include:*

- *Sonus' proprietary Policy Information Provisioning Engine (PIPE) protocol over SSH between the EMS and PSX subsystems,*
- *Netconf over SSH between the EMS and SGX subsystems, and*
- *CLI commands executed at the GSX subsystem over an SSH connection from the EMS.*

FDP_IFF.1(2).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) *Subjects on the internal network can cause information to flow from a TOE subsystem to another TOE subsystem if:*

i. the human user initiating the information flow has authenticated according to FIA_UAU.5;

ii. the presumed address of the source subject translates to an internal network address; and

iii. the address of the destination subject translates to the corresponding TOE subsystem on the internal network.

b) *Human users on a local console TOE subsystem can cause information to flow from a TOE subsystem to another TOE subsystem if:*

i. the human user-initiating the information flow has authenticated locally according to FIA_UAU.2; and

ii. *the address of the destination subject translates to the corresponding TOE subsystem on the internal network*].

Application Note: *The reference to FIA_UAU.5 in sub-paragraph (a) above is for RADIUS-based authentication to the EMS TOE subsystem. See section 6.2.4.6 (p. 69) for details re: FIA_UAU.5.*

FDP_IFF.1(2).3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1(2).4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*]

FDP_IFF.1(2).5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.2.3.6 FDP_IFF.1(3) Simple Security Attributes (Encrypted Channel Policy)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1(3) Subset Information Flow Control

FMT_MSA.3 Static Attribute Initialization

FDP_IFF.1(3).1 The TSF shall enforce the [*ENCRYPTED INFORMATION FLOW CONTROL SFP*] based on the following types of subject and information security attributes: [

a) *Subjects: TOE subsystem interfaces;*

b) *Subject Security attributes:*

i. set of source subject identifiers, and

ii. set of destination subject identifiers;

c) *Information: network packets; and*

d) *Information Security attributes:*

i. presumed identity of source subject, and

ii. *presumed identity of destination subject*].

FDP_IFF.1(3).2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) *the presumed identity of the source subject is in the set of source subject identifiers;*

b) *the identity of the destination subject is in the set of source destination identifiers;*

c) *the information security attributes match the attributes in an information flow policy rule defined by the System Administrator or an authorized Operator; and*

d) *the selected information flow policy rule specifies:*

i. that the information flow is to be permitted, and

ii. the cryptographic operations are to be applied to that information flow to assure confidentiality and integrity of the flow].

FDP_IFF.1(3).3 The TSF shall enforce ~~the~~ [*no additional rules*].

FDP_IFF.1(3).4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1(3).5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.2.3.7 FDP_UCT.1 Basic Data Exchange Confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [*ENCRYPTED INFORMATION FLOW CONROL SFP*] to [**transmit, receive**] ~~user~~ signaling data in a manner protected from unauthorized disclosure.

Application Note: This requirement enables the use of secure signaling between the TOE and trusted external IT entities using SIP over IPSec or TLS.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1(1) Authentication Failure Handling (EMS GUI)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_AFL.1(1).1 The TSF shall detect when [**an administrator configurable positive integer within [*the range from 1 to 9*]**] unsuccessful authentication attempts occur ~~related to~~ [*since the last successful login to the EMS TOE subsystem by a valid user identity*].

FIA_AFL.1(1).2 When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [*take one or both of the following actions as configured by the Administrator:*

a) lock the account for the configured period of time, or

b) *lockout (i.e., block) the user's presumed IP address from connecting to the EMS TOE subsystem for the configured period of time*].

6.2.4.2 FIA_AFL.1(2) Authentication Failure Handling (CLI Access)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_AFL.1(2).1 The TSF shall detect when [**an administrator configurable positive integer within [*the range shown in column 2 of Table 18*]**] unsuccessful authentication attempts occur related to [*local console access for the claimed user identity*].

FIA_AFL.1(2).2 When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [*take the action(s) shown in column 3 of Table 18*].

Table 18: FIA_AFL.1(2) Authentication Failure Handling (CLI Access) By TOE Subsystem

Subsystem	Range of Failed Attempts	Action(s) Taken
EMS	Any integer value, including 0	When configured by the Administrator (i.e., an integer value greater than 0), the TOE subsystem will record the user ID and each failed login attempt exceeding the set value to the audit log.
GSX	Any integer value from 0 to 15	Lock-out the user account for an Administrator-configurable period of time ranging from 1 to 360 minutes, after which the invalid login attempt counter is reset and the user can re-authenticate.

6.2.4.3 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) *identity (i.e., userID);*

b) *association of a userID with one or more roles; and*

c) *password*].

6.2.4.4 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*a minimum number of characters as prescribed by the Administrator for the EMS and GSX subsystems*].

6.2.4.5 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.6 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*remote EMS TOE subsystem users with the option to use RADIUS mechanisms subject to the rules defined in FIA_UAU.5.2*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*following options, as configured by the Administrator:*

a) *local authentication only – only local authentication will be performed for EMS TOE subsystem users;*

b) *remote with fallback to local authentication – RADIUS authentication to the EMS TOE subsystem will be performed first, with a fallback to local authentication; and*

c) *remote authentication only – Only RADIUS authentication will be performed to the EMS TOE subsystem, and local authentication will be disabled*].

6.2.4.7 FIA_UID.2 User Identification Before Any Action

Hierarchical to: FIA_UID.1 Timing of Identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [**determine the behaviour of, disable, enable, modify the behaviour of**] the functions [*identified below*] to [*Administrators and authorized Operators:*

a) *administer and use the EMS to manage all TOE subsystems, including:*

i. start/stop EMS services;

ii. register each of the following TOE subsystem nodes with EMS for remote management:

(1) GSX,

(2) SGX,

(3) PSX, and

(4) DSI;

iii. remotely manage the operational configuration of each inter-connected TOE subsystem via the EMS GUI;

iv. remotely start/stop services on all connected TOE subsystems;

v. remotely manage and report on the network topology of the inter-connected TOE subsystems;

vi. *remotely monitor, report on, and modify configuration settings based on the operational status of TOE subsystems on the network;*

vii. *conduct maintenance actions on the EMS and remotely conduct maintenance actions on all inter-connected TOE subsystems;*

viii. *remotely issue administrative and operations management CLI commands to all connected TOE subsystems over a secured communications channel; and*

ix. *remotely configure Call Data Channel (CDC) for Lawful Intercept;*

b) *locally administer the GSX via its CLI;*

c) *locally administer the SGX via its CLI;*

d) *locally administer the PSX via its CLI; and*

e) *locally administer the DSI via its CLI*].

6.2.5.2 FMT_MSA.1(1) Management of Security Attributes (Peered Policy)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control, or
FDP_IFC.1(1) Subset Information Flow Control]
FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(1).1 The TSF shall enforce the [*PEERED INFORMATION FLOW CONTROL SFP*] to restrict the ability to [**change_default, query, modify, delete**] the security attributes: [

a) *presumed source and destination IP address;*

b) *protocol;*

c) *interface;*

d) *source and destination port number or range;*

e) *packet type (media, signaling or management);*

f) *packet rate; and*

g) *SIP endpoint (registering or registered)*]

to [*Administrators and authorized Operators*].

6.2.5.3 FMT_MSA.1(2) Management of Security Attributes (Authenticated Policy)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control, or
FDP_IFC.1(2) Subset Information Flow Control]
FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(2).1 The TSF shall enforce the [*AUTHENTICATED INFORMATION FLOW CONTROL SFP*] to restrict the ability to [**change_default, query, modify, delete**] the security attributes: [

a) *presumed source and destination IP address;*

b) *protocol;*

c) *source and destination port number or range;*

d) *username or account name and its associated password;*

e) *user profile; and*

f) *user session idle timeout*]

to [*Administrators and authorized Operators*].

6.2.5.4 FMT_MSA.1(3) Management of Security Attributes (Encrypted Channel Policy)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control, or
FDP_IFC.1(3) Subset Information Flow Control]
FMT_SMR.1 Security Roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(3).1 The TSF shall enforce the [*ENCRYPTED INFORMATION FLOW CONTROL SFP*] to restrict the ability to [**change_default, query, modify, delete**] the security attributes: [

a) *TOE subsystem interface communication connections;*

b) *secure signaling definitions:*

i. SIP over TLS, and

ii. SIP over IPSec; and

c) *HTTPS connection configuration between the EMS Operator Workstation and the EMS TOE subsystem server*]

to [*Administrators and authorized Operators*].

6.2.5.5 FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes
FMT_SMR.1 Security Roles

FMT_MSA.3.1 The TSF shall enforce the [*PEERED, AUTHENTICATED, and ENCRYPTED INFORMATION FLOW CONTROL SFPs*] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Administrators and authorized Operators*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.6 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [**change_default, query, modify, delete, clear**] ~~the~~ [*all TSF data*] to [*Administrator-defined operational and management roles within each TOE subsystem*].

6.2.5.7 FMT_SAE.1 Time-limited Authorization

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FPT_STM.1 Reliable time stamps

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [*user accounts and passwords for the GSX subsystem*] to [*the Administrator*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [*disable the user account until its associated account or password aging threshold value is reset by an Administrator*] after the expiration time for the indicated security attribute has passed.

6.2.5.8 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) *the security management functions identified at FMT_MOF.1.1 (section 6.2.5.1), broadly stated as:*

i. start-up and shutdown of each TOE subsystem;

ii. create, modify, and delete TOE subsystem configuration items for:

(1) network topology management,

(2) TOE fault management,

(3) TOE performance management,

(4) TOE maintenance management (including back-up and recovery), and

(5) TOE security management;

iii. create, report on (view), and delete or roll the audit trail; and

iv. *user profile and password management*].

6.2.5.9 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator, Provisioner, and Operator*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: *The Provisioner role is an enhanced Operator role with limited additional privileges delegated to it by the Administrator. For the purposes of this ST, the Provisioner role is included within the Operator role, unless specifically identified where relevant.*

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [**disclosure, modification**] when it is transmitted between separate parts of the TOE.

6.2.6.2 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.2.6.3 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*the following data types*] when shared between the TSF and another trusted IT product: [

a) *X.509 certificates;*

b) *GSX configuration files; and*

c) *SNMP traps*].

FPT_TDC.1.2 The TSF shall use [*the interpretation rules identified below*] when interpreting the TSF data from another trusted IT product: [

a) *X.509 certificates shall be readable for import into the TSF when they are correctly formatted in accordance with either of the following formats:*

   i. PKCS#12[14] *(i.e., file type *.p12), or*

   *ii. Distinguished Encoding Rules (DER) (i.e., file type *.der).*

b) *GSX configuration files shall be imported into a target GSX TOE subsystem when they are correctly formatted in accordance with Sonus' PIF binary standard, and a configuration import command has been executed by the Administrator.*

[14] Public Key Cryptography Standard (PKCS) 12 entitled "*Personal Information Exchange Syntax*" is a standard prepared by RSA Security that defines a file format which is used to store private keys with accompanying public key certificates that are protected with a password-based symmetric key.

c) *The EMS TOE subsystem shall read and report on IT devices that are included in its Management Information Base (MIB) that send fault or alarm information correctly formatted with any of SNMP versions: 1, and 2*].

6.2.7 Resource Utilization (FRU)

6.2.7.1 FRU_PRS.1 Limited Priority of Service

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to [*the following*] shall be mediated on the basis of the subject's assigned priority [:

a) *element routing;*

b) *switch trunk group routing; and*

c) *carrier selection*].

Application Note: *While not explicitly identified in the above, the Sonus Trunking Suite supports the High Probability of Completion (HPC) network capability intended to provide enhanced probability of call completion to authorized Government Emergency Telecommunication Service (GETS) and Wireless Priority Service (WPS) users during times of network stress and/or congestion. HPC features include: GETS Call Routing, Office-Wide Call Queuing, and SIP Resource Priority Header.*

6.2.7.2 FRU_RSA.1 Maximum Quotas

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*CPU usage, memory usage, swap space usage, and file system usages*] that [**subjects**] can use [**simultaneously**].

6.2.8 TOE Access (FTA)

6.2.8.1 FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*an Administrator-defined idle session logout period for user accounts for the following TOE subsystems:*

a) *GSX – disabled by default, but is configurable in terms of an Administrator-defined number of minutes of inactivity from 0 (never logout) to 720; and*

b) *SGX – 30 minutes, configurable over a range from 0 to 120 minutes*].

6.2.8.2 FTA_TAB.1 Default TOE Access Banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE for the following TOE subsystems once configured by the Administrator:

a) EMS for remote web-based GUI; and

b) GSX for local CLI logon.

6.2.9 Trusted path/channels (FTP)

6.2.9.1 FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the TSF, another trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*secure signaling with external SIP peers*].

6.2.9.2 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification, disclosure**].

FTP_TRP.1.2 The TSF shall permit [**remote users**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**initial user authentication**, [*and all remote administrative actions carried out by a remote operator connected to the EMS TOE subsystem via its web-based GUI*]].

6.3 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw Reporting Procedures (ALC_FLR.2) and Identification of Security Measures (ALC_DVS.1). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 and ALC_DVS.1 augmentation since there are a number of areas where current Sonus practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 19: EAL 2 Assurance Requirements.

Table 19: EAL 2 Assurance Requirements

Assurance Class	Assurance Components	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
	ALC_DVS.1	Identification of security measures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.4 CC COMPONENT HIERARCHIES AND DEPENDENCIES

Table 20 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

Table 20: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
FAU_ARP.1	FAU_SAA.1	Yes
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes Yes - Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FAU_SAA.1	FAU_GEN.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes

Table 20: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes Yes
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.3	FAU_STG.1	Yes
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[No No Yes - CCS Instruction #4, Annex A, Response to FAQ 3] Yes - CCS Instruction #4, Annex A, Response to FAQ 3
FDP_IFC.1(1)	FDP_IFF.1(1)	Yes
FDP_IFC.1(2)	FDP_IFF.1(2)	Yes
FDP_IFC.1(3)	FDP_IFF.1(3)	Yes
FDP_IFF.1(1)	FDP_IFC.1(1) FMT_MSA.3	Yes Yes
FDP_IFF.1(2)	FDP_IFC.1(2) FMT_MSA.3	Yes Yes
FDP_IFF.1(3)	FDP_IFC.1(3) FMT_MSA.3	Yes Yes
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	[Yes Yes] [No Yes]
FIA_AFL.1(1)	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_AFL.1(2)	FIA_UAU.1	Yes - Satisfied by FIA_UAU.2 which is hierarchical to FIA_UAU.1
FIA_ATD.1	None	Yes
FIA_SOS.1	None	Yes
FIA_UAU.2	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FIA_UAU.5	None	Yes
FIA_UID.2	None	Yes
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1(1)] FMT_SMR.1 FMT_SMF.1	[No Yes] Yes Yes
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1(2)] FMT_SMR.1 FMT_SMF.1	[No Yes] Yes Yes
FMT_MSA.1(3)	[FDP_ACC.1 or FDP_IFC.1(3)]	[No Yes]

Table 20: Functional Requirements Dependencies

SFR	Dependencies	Dependency Satisfied?
	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	Yes Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes – Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FPT_ITT.1	None	Yes
FPT_STM.1	None	Yes
FPT_TDC.1	None	Yes
FRU_PRS.1	None	Yes
FRU_RSA.1	None	Yes
FTA_SSL.3	None	Yes
FTA_TAB.1	None	Yes
FTP_ITC.1	None	Yes
FTP_TRP.1	None	Yes

6.5 SECURITY REQUIREMENTS RATIONALE

Table 21 provides a mapping between the SFRs and the TOE's Security Objectives.

Table 21: Mapping of SFRs to Security Objectives

SFR	O.ADMIN_ROLE	O.AUDIT	O.DISPLAY_BANNER	O.RESOURCE_EXHAUSTION	O.I&A	O.MANAGE	O.PROTECT	O.PROTECTED_CHANNELS	O.SESSION_PROTECT	O.SYSTEM_MONITORING	O.TOE_ACCESS
FAU_ARP.1 Security Alarms		X								X	
FAU_GEN.1 Audit Data Generation		X									
FAU_GEN.2 User Identity Association		X									
FAU_SAA.1 Potential Violation Analysis										X	
FAU_SAR.1 Audit Review		X									
FAU_SAR.2 Restricted Audit Review		X									
FAU_SAR.3 Selectable Audit Review		X									
FAU_SEL.1 Selective Audit		X									
FAU_STG.1 Protected Audit Trail Storage		X									
FAU_STG.3 Action in Case of Possible Audit Data Loss		X									
FCS_COP.1 Cryptographic Operation							X	X			
FDP_IFC.1(1) Subset Information Flow Control (Peered Policy)				X			X				X
FDP_IFC.1(2) Subset Information Flow Control (Authenticated Policy)							X				X
FDP_IFC.1(3) Subset Information Flow Control (Encrypted Channel Policy)							X	X			X
FDP_IFF.1(1) Simple Security Attributes (Peered Policy)				X			X				X
FDP_IFF.1(2) Simple Security Attributes (Authenticated Policy)							X				X
FDP_IFF.1(3) Simple Security Attributes (Encrypted Channel Policy)							X	X			X

Table 21: Mapping of SFRs to Security Objectives

SFR	O.ADMIN_ROLE	O.AUDIT	O.DISPLAY_BANNER	O.RESOURCE_EXHAUSTION	O.I&A	O.MANAGE	O.PROTECT	O.PROTECTED_CHANNELS	O.SESSION_PROTECT	O.SYSTEM_MONITORING	O.TOE_ACCESS
FDP_UCT.1 Basic Data Exchange Confidentiality							X	X			
FIA_AFL.1(1) Authentication Failure Handling (EMS GUI)					X						X
FIA_AFL.1(2) Authentication Failure Handling (CLI Access)					X						X
FIA_ATD.1 User Attribute Definition	X				X						X
FIA_SOS.1 Verification of Secrets					X						
FIA_UAU.2 User Authentication Before Any Action					X						X
FIA_UAU.5 Multiple Authentication Mechanisms					X						X
FIA_UID.2 User Identification Before Any Action		X			X						X
FMT_MOF.1 Management of Security Functions Behaviour	X					X					
FMT_MSA.1(1) Management of Security Attributes (Peered Policy)				X		X					
FMT_MSA.1(2) Management of Security Attributes (Authenticated Policy)						X					
FMT_MSA.1(3) Management of Security Attributes (Encrypted Channel Policy)						X					
FMT_MSA.3 Static Attribute Initialization				X			X				
FMT_MTD.1 Management of TSF Data	X					X					
FMT_SAE.1 Time-limited Authorization						X					X
FMT_SMF.1 Specification of Management Functions						X					
FMT_SMR.1 Security Roles	X				X	X					
FPT_ITT.1 Basic Internal TSF Data Transfer Protection							X	X			
FPT_STM.1 Reliable Time Stamps		X								X	
FPT_TDC.1 Inter-TSF Basic TSF Data Consistency						X					
FRU_PRS.1 Limited Priority of Service				X							

Table 21: Mapping of SFRs to Security Objectives

SFR	O.ADMIN_ROLE	O.AUDIT	O.DISPLAY_BANNER	O.RESOURCE_EXHAUSTION	O.I&A	O.MANAGE	O.PROTECT	O.PROTECTED_CHANNELS	O.SESSION_PROTECT	O.SYSTEM_MONITORING	O.TOE_ACCESS
FRU_RSA.1 Maximum Quotas				X							
FTA_SSL.3 TSF-initiated Termination									X		X
FTA_TAB.1 Default TOE Access Banners			X								
FTP_ITC.1 Inter-TSF Trusted Channel						X	X	X			
FTP_TRP.1 Trusted Path					X	X		X			

6.5.1 Security Functional Requirements Rationale Related to Security Objectives

This section rationalizes how the Security Functional Requirements contribute to satisfying the stated Security Objectives for the TOE.

6.5.1.1 O.ADMIN_ROLE

Objective: **O.ADMIN_ROLE**	The TOE will provide roles to isolate administrative and operational management actions.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FIA_ATD.1	User Attribute Definition
	FMT_MTD.1	Management of TSF Data
	FMT_SMR.1	Security Roles
	FMT_MOF.1	Management of Security Functions Behaviour
Rationale:	FMT_SMR.1 establishes the administrative and operational roles for the TOE that are to be isolated from each other by the TSF. FMT_MTD.1 isolates administrative and operational actions by restricting the ability for specified roles to complete operations on TSF data. FMT_MOF.1 contributes to the roles isolation by restricting the ability to effect TSF functionality to Administrators and authorized Operators FIA_ATD.1 maintains an association of a user identity to a role that isolates administrators from operations management (operator roles).	

6.5.1.2 O.AUDIT

Objective: **O.AUDIT**	For security-relevant events, the TOE will generate, record and store, protect, and make audit records available to authorized Administrators for review.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FAU_ARP.1	Security Alarms
	FAU_GEN.1	Audit Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.3	Action in Case of Possible Audit Data Loss
	FIA_UID.2	User Identification Before Any Action
	FPT_STM.1	Reliable Time Stamps
Rationale:	FAU_ARP.1 records security-relevant information into an audit log when potential security violations are detected. FAU_GEN.1 and FAU_GEN.2 create audit records and record them into an audit log, and for audit events resulting from actions of users, the audit event is associated with the identity of that user. FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 restrict review of audit records to Administrators and authorized Operators who can review all audit records, as well as filter and sort audit data based on selectable criteria. FAU_SEL.1 enables the Administrator or Operator to down select and audit events that may only be of interest for a particular situation such as system account data, system debugging data, security events, system events or	

	system traces. FAU_STG.1 protects audit records from deletion to provide assurance that the records are available when required by the Administrator. FAU_STG.3 rolls over old log files when they approach an Administrator-configured maximum size in order to assure the availability of audit records when required. FIA_UID.2 ensures that Administrators and authorized Operators have been successfully identified before they are granted access to the audit log. FPT_STM.1 provides reliable time stamps for all audit records.

6.5.1.3 O.DISPLAY_BANNER

Objective: **O.DISPLAY_BANNER**	The TOE will display, where appropriate, an advisory warning regarding use of the TOE that is configurable by authorized Administrators.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FTA_TAB.1	Default TOE Access Banners
Rationale:	FTA_TAB.1 provides the Administrator with the capability to configure advisory warning messages to users logging into the EMS and GSX TOE subsystems.	

6.5.1.4 O.RESOURCE_EXHAUSTION

Objective: **O.RESOURCE_EXHAUSTION**	The TOE will provide mechanisms that mitigate external entities' (Subscribers, attackers) attempts to exhaust TSF resources (e.g., Denial of Service, occupying all SSH listeners, etc.).	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FDP_IFC.1(1)	Subset Information Flow Control (Peered Policy)
	FDP_IFF.1(1)	Simple Security Attributes (Peered Policy)
	FMT_MSA.1(1)	Management of Security Attributes (Peered Policy)
	FMT_MSA.3	Static Attribute Initialization
	FRU_PRS.1	Limited Priority of Service
	FRU_RSA.1	Maximum Quotas
Rationale:	FDP_IFC.1(1) and FDP_IFF.1(1) provide Policers used by the TSF to reject packets at wire-rates if they fail to conform with criteria including packet type and packet rate. This mechanism serves to enable the TSF to protect and allocate its resources without exhausting them. FMT_MSA.3 and FMT_MSA.1(1) together provide the Administrator with the means to specify default ACLs and IP Policer rules based on packet type and packet rate that restrict in-bound packets to protect against resource exhaustion. FRU_PRS.1 ensures that in the event of adverse network conditions such as overload, High Probability of Completion labeled calls will be prioritized and afforded a high assurance that the call will be successfully routed and connected. FRU_RSA.1 establishes maximum quotas for key system parameters (CPU usage, memory usage, swap space usage, and file system usage) used by TOE subjects in order to protect the TSF from resource exhaustion.	

6.5.1.5 O.I&A

Objective: **O.I&A**	The TOE will uniquely identify and authenticate the claimed identity of all administrative and operational personnel (Administrators and Operators) before granting access to controlled resources.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FIA_AFL.1(1)	Authentication Failure Handling (EMS GUI)
	FIA_AFL.1(2)	Authentication Failure Handling (CLI Access)
	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.5	Multiple Authentication Mechanisms
	FIA_UID.2	User Identification Before Any Action
	FMT_SMR.1	Security Roles
	FTP_TRP.1	Trusted Path
Rationale:	FIA_UAU.2, FIA_UAU.5 and FIA_UID.2 satisfy this objective by ensuring that the claimed identity of all TOE users are verified before management or operational access to the TOE is granted by the TSF. FIA_SOS.1 supports this objective by providing a means for Administrator to specify secrets to be verified by claims of Operator or Administrator identities. FIA_AFL.1(1) and (2) support this objective by ensuring that the TSF can take prescribed actions in response to unsuccessful authentication attempts. FMT_SMR.1 and FIA_ATD.1 support this objective by ensuring that users and user attributes are tied to administrative or operational management roles. FTP_TRP.1 supports this objective as a necessary requirement for remote administrative and operational management users to authenticate to the TOE via FIA_UAU.5.	

6.5.1.6 O.MANAGE

Objective: **O.MANAGE**	The TOE will provide the functions and facilities necessary to support TOE Administrators and Operators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MSA.1(1)	Management of Security Attributes (Peered Policy)
	FMT_MSA.1(2)	Management of Security Attributes (Authenticated Policy)
	FMT_MSA.1(3)	Management of Security Attributes (Encrypted Channel Policy)
	FMT_MTD.1	Management of TSF Data
	FMT_SAE.1	Time Limited Authorization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
	FPT_TDC.1	Inter-TSF Basic TSF Data Consistency
	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path
Rationale:	In general, the TOE supports Administrators and authorized Operators in the	

	management of security functions, security attributes and data while also restricting these from unauthorized use. FMT_MOF.1 and FMT_SMF.1 satisfy the objective by restricting the ability to exercise and make changes to all facets of TSF functionality to Administrators and authorized Operators. FMT_MTD.1 complements FMT_MOF.1 in satisfying the objective by restricting operations to TSF data and configuration settings to Administrators and authorized Operators. FMT_SMR.1 supports the objective by establishing and enforcing role-based security by the TSF. FMT_MSA.1(1), FMT_MSA.1(2), and FMT_MSA.1(3) support the objective by enforcing the three defined Security Function Policies to restrict changes to TSF security attributes to Administrators and authorized Operators. FMT_SAE.1 supports the objective by enforcing Administrator-configured limits on accounts and passwords. FPT_TDC.1 supports the objective by enabling the TOE to import and use data from external trusted IT products, such as enabling an Administrator to import GSX configuration files from other systems into these TOE subsystems for quick instantiation into known configurations. FTP_ITC.1 and FTP_TRP.1 support the objective by provide Administrators and authorized Operators with the means to exercise administrative and operational management commands over secured channels between TOE subsystems and also from the remote Operator Workstation when required.

6.5.1.7 O.PROTECT

Objective: **O.PROTECT**	The TOE will provide mechanisms to protect TSF data and resources.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FCS_COP.1	Cryptographic Operation
	FDP_IFC.1(1)	Subset Information Flow Control (Peered Policy)
	FDP_IFC.1(2)	Subset Information Flow Control (Authenticated Policy)
	FDP_IFC.1(3)	Subset Information Flow Control (Encrypted Channel Policy)
	FDP_IFF.1(1)	Simple Security Attributes (Peered Policy)
	FDP_IFF.1(2)	Simple Security Attributes (Authenticated Policy)
	FDP_IFF.1(3)	Simple Security Attributes (Encrypted Channel Policy)
	FDP_UCT.1	Basic Data Exchange Confidentiality
	FMT_MSA.3	Static Attribute Initialization
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FTP_ITC.1	Inter-TSF Trusted Channel
Rationale:	FCS_COP.1 satisfies this objective by providing cryptographic algorithms that have been validated under the Cryptographic Algorithm Validation Program (CAVP) for the TSF to use to protect TSF data. FDP_UCT.1 satisfies this objective by ensuring that TOE administrative and operational management data is protected from unauthorized disclosure. FPT_ITT.1 satisfies this objective by protecting TSF data from disclosure and modification when it is transmitted between TOE subsystems. FTP_ITC.1 satisfies this objective by providing communications channels for securely communicating TSF data (SIP signaling information) with	

	external trusted peers. FDP_IFC.1(3) and FDP_IFF.1(3) support this objective through enforcement of the ENCRYPTED information flow control SFP on transmitted TOE administrative and operational management data by FDP_UCT.1. FDP_IFC.1(1) and FDP_IFF.1(1) support this objective by providing the TSF with the capability to pass or drop in-bound packets or signaling information based on Administrator-configured criteria. FDP_IFC.1(2) and FDP_IFF.1(2) support this objective by ensuring that only authenticated Administrators and Operators can execute administrative or operational management commands via either a local console CLI or via the EMS web-based GUI. FMT_MSA.3 supports this objective by providing the Administrator and authorized Operators with the means to define restrictive default values for security attributes.

6.5.1.8 O.PROTECTED _CHANNELS

Objective: **O.PROTECTED _CHANNELS**	The TOE will provide cryptographic confidentiality and integrity mechanisms for TSF data while in transit to remote parts of the TOE.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FCS_COP.1	Cryptographic Operation
	FDP_IFC.1(3)	Subset Information Flow Control (Encrypted Channel Policy)
	FDP_IFF.1(3)	Simple Security Attributes (Encrypted Channel Policy)
	FDP_UCT.1	Basic Data Exchange Confidentiality
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path
Rationale:	FCS_COP.1 satisfies this objective by providing cryptographic algorithms that have been validated under the Cryptographic Algorithm Validation Program (CAVP) for the TSF to use to protect TSF data. FDP_IFC.1(3) and FDP_IFF.1(3) support this objective through enforcement of the ENCRYPTED information flow control SFP on transmitted TOE administrative and operational management data to remote parts of the TOE. FDP_UCT.1 satisfies this objective by ensuring that TOE administrative and operational management data is protected from unauthorized disclosure. FPT_ITT.1 satisfies this objective by protecting TSF data from disclosure and modification when it is transmitted between TOE subsystems. FTP_ITC.1 satisfies this objective by providing secure communications channels to protect TSF data (SIP signaling information) from modification and disclosure when transmitted to trusted external IT entities (signaling peers). FTP_TRP.1 satisfies this objective by providing a trusted path between the TSF and remote users conducting administrative or operational management actions on the TOE.	

6.5.1.9 O.SESSION_PROTECT

Objective: **O.SESSION_PROTECT**	The TOE will provide mechanisms that mitigate the risk of unattended sessions being hijacked.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FTA_SSL.3	TSF-initiated Termination
Rationale:	FTA_SSL.3 satisfies the objective by providing the TSF with the capability to terminate inactive user sessions after an Administrator-prescribed period of time.	

6.5.1.10 O.SYSTEM_MONITORING

Objective: **O.SYSTEM_MONITORING**	The TOE will provide the capability to generate alarms and send them to an Operator Workstation or to an external IT entity.	
Security Functional Requirements:	**SFR Name**	**SFR Title**
	FAU_ARP.1	Security Alarms
	FAU_SAA.1	Potential Violation Analysis
	FPT_STM.1	Reliable Time Stamps
Rationale:	FAU_ARP.1 satisfies this objective by providing the TSF with the means to provide visual and audible alarms on the EMS management terminal upon detection of a potential security violation. FAU_SAA.1 supports this objective by the GSX TOE subsystem being able to trigger an alarm based on a potential security violation. FPT_STM.1 supports this objective by providing reliable time stamps for alarms.	

6.5.1.11 O.TOE_ACCESS

Objective: **O.TOE_ACCESS**	The TOE will provide access control mechanisms that:
	• provide authorized users (Administrators and Operators) with logical access to the TOE; and
	• explicitly deny access to:
	  • all unauthorized users, and
	  • specific Administrators or Operators when appropriate.	

Security Functional Requirements:	**SFR Name**	**SFR Title**
	FDP_IFC.1(1)	Subset Information Flow Control (Peered Policy)
	FDP_IFC.1(2)	Subset Information Flow Control (Authenticated Policy)
	FDP_IFC.1(3)	Subset Information Flow Control (Encrypted Channel Policy)
	FDP_IFF.1(1)	Simple Security Attributes (Peered Policy)
	FDP_IFF.1(2)	Simple Security Attributes (Authenticated Policy)
	FDP_IFF.1(3)	Simple Security Attributes (Encrypted Channel Policy)
	FIA_AFL.1(1)	Authentication Failure Handling (EMS GUI)
	FIA_AFL.1(2)	Authentication Failure Handling (CLI Access)
	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.5	Multiple Authentication Mechanisms

	FIA_UID.2	User Identification Before Any Action
	FMT_SAE.1	Time-limited Authorization
	FTA_SSL.3	TSF-initiated Termination
Rationale:	FDP_IFC.1(1) and FDP_IFF.1(1) collectively satisfy this objective by enforcing the PEERED information flow SFP on IT entities and dropping unauthorized traffic (from non-peered entities). FDP_IFC.1(2) and FDP_IFF.1(2) collectively satisfy this objective by enforcing the AUTHENTICATED information flow control SFP on commands arising from authenticated system Administrators or Operators. FDP_IFC.1(3) and FDP_IFF.1(3) collectively satisfy this objective by enforcing the ENCRYPTED information flow control SFP on network packets prior to them transiting the TOE interfaces. FIA_AFL.1(1) and FIA_AFL.1(2) satisfy this objective by providing a means to detect unsuccessful authentication attempts. This enables a configurable threshold that prevents unauthorized users from gaining access to the TOE by guessing authentication data. It also provides the means to lockout or block a remote user's IP address from connecting to the EMS TOE subsystem for an administrator-configured period of time. FIA_ATD.1 satisfies this objective by defining user security attributes that are used by the TSF to enforce the type of access provided to the user. FIA_UAU.2, FIA_UAU.5, and FIA_UID.2 support this objective by ensuring that users are identified and authenticated before gaining access to the TSF. FTA_SSL.3 supports this objective by ensuring that user sessions that are idle for an Administrator-configured period of time are terminated by the TSF. FMT_SAE.1 supports this objective by enabling the Administrator to specify an expiration time (i.e., a validity period) for TOE user accounts and passwords. Expired accounts are unable to access the TOE until re-enabled by the Administrator.	

6.5.2 Security Assurance Requirements Rationale

Sonus has decided that the TOE will be evaluated at EAL2, augmented with Flaw Reporting Procedures (ALC_FLR.2) and Identification of Security Measures (ALC_DVS.1). This combination is termed EAL2+. This level of assurance meets clients' requirements, and it provides a level of independently assured security that is consistent with the postulated threat environment. Specification of EAL2+ also includes the vulnerability assessment component.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

The TOE generates audit records for security-relevant events and alarms. Alarms are prioritized according to a five-point severity scale ranging from indeterminate to critical as described in Table 22 below. There is also a sixth alarm rating (cleared) that is used by the TOE to correlate events in the fault management database.

Table 22: TOE Events Severity Ratings

Severity	Description	Typical Recommended Action(s) to Take
Critical	Call impairment is either already occurring or is imminent.	Requires immediate operator action. Contact Sonus Technical Assistance Center (TAC); may require reconnecting cables, replacing components, or rebuilding a drive.
Major	Future call impairment is a significant concern.	Take action as soon as possible. Contact Sonus TAC; may require reconnecting cables, replacing components, or rebuilding a drive.
Minor	Low-impacting situations or conditions.	Normally, calls/revenue are not impacted by these low-severity events. Determine if error is routine (minor), or indicative of a significant problem.
Informational	Intended to help the user identify potential future problems.	Usually requires no immediate operator action.
Indeterminate	If the TOE's EMS subsystem cannot determine the severity level from trap information or rules data, the severity level is set to "Indeterminate".	This situation normally only occurs from traps received from third-party devices, and may be attributed to outdated mapping rules or lack of current trap details
Cleared	The "Cleared" severity is set according to the prescribed rule logic and automation logic that correlate events existing in the fault database.	N/A

Upon detection of potential security violations, the TOE records each event into the log. It provides a short textual description of the alarm cause, it identifies the criticality of the alarm and it identifies the TOE component that reported the alarm. All logs are time stamped with the local time of the EMS TOE subsystem. To ensure consistency of timestamps throughout the TOE, a Network Time Protocol (NTP) server is situated in the IT operational environment to provide reliable, synchronized time to each TOE subsystem.

When caused by a TOE user, audit events are associated with that user in the audit log. The list of audit events is identified in Table 16, starting on page 59.

The GSX TOE subsystem monitors its packet discard rate in 11 different dimensions, and when the rate exceeds a threshold level that is either built-in to the system or configured by the Administrator, the GSX will trigger an alarm.

The TOE provides administrators and authorized operators with the means to read and review the audit logs. The log data can be filtered and sorted using any of 8 different categories (name, severity, owner, type, device, time, count, and text-based summary of the event).

The primary mechanism for capturing TOE subsystem audit data to the EMS subsystem is via SNMP traps. However, the EMS subsystem also interconnects with the PSX and DSI subsystems via EMS agents installed on them. The EMS agents enable the remote operational management of the subsystems via the EMS. Additionally, each installed agent generates a set of localized subsystem log and audit files to provide Operators and Administrators with enhanced visibility into the operations, health, and security of the TOE.

The TOE provides administrators and authorized operators with the capability to audit any subset of the full range of auditable events. The user can configure the selectable audit by TOE subsystem, by event type, and by threshold values.

Audit logs are protected from unauthorized modification and deletion as only the Administrator can delete the audit logs. The TOE limits the size of individual log files to an Administrator-defined default maximum size, after which a new log file is started. The TOE will maintain an Administrator-specified number of log files before it will roll (i.e., delete the oldest) log files over to continue recording. Only the Administrator can configure the maximum size of each log.

TOE Security Functional Requirements addressed: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FAU_STG.3, and FPT_STM.1.

7.1.2 Cryptographic Support for Trusted Path / Channels and Secured Communications

The TOE supports secure communication both within its own scope of control (between TOE subsystems) as well as with other systems via the SSHv2.0, HTTPS, IPSec, and TLSv1 protocols. Communication via these protocols is protected against unauthorized disclosure and modification via cryptographic mechanisms. These protocols are used as follows:

- SSH: is used to establish a secure channel for remote Administrative access to PSX, GSX, and SGX subsystems via the EMS management GUI.

  As part of the SSH implementation, the TOE also supports SFTP and SCP for securely copying CDRs from the TOE to an externally-connected Call Accounting server (outside the TOE).

- HTTPS: is used to secure the communication channel between the EMS Operator Workstation (outside the TOE) and the EMS management server. HTTPS is also invoked for client/server communications between the EMS and PSX. It is also used to secure the communications channel between the EMS and the PSX and DSI subsystems when the EMS agents on those two systems are being configured by the Administrator or authorized Operator.

- TLS: used to secure signaling information carried by the SIP protocol for interfacing with peered telecommunication service providers. Administrators are able to configure TLS to use the following cipher suites:

  - *nosuite* (i.e., do not use any cipher suites),

- *rsa-with-null-sha*,
- *rsa-with-aes-128-cbc-sha* (default), and
- *rsa-with-3des-ede-cbc-sha*.

Only the the default cipher suite (rsa-with-aes-128-cbc-sha) is supported in the CC Evaluated Configuration.

- IPSec: also used to secure signaling information over the SIP protocol for interfacing with peered telecommunications service providers. Administrators can configure IPSec to use the following ciphers:
  - *three-des-cbc* as defined in **[RFC 2451]**,
  - *aes-cbc-128* (default) as defined in **[RFC 3602]**, and
  - null (i.e., no encryption). This is not a valid option for the IPSec IKE[15] Profile, nor is it supported in the CC Evaluated Configuration of the TOE. This option is available for use during testing only.

  Furthermore, the TOE's IPSec IKE profile uses *HMAC-SHA1-96* by default for integrity.

The TOE provides Administrators with the means to create and configure local or remote (Certificate Authority (CA) or trusted entity) certificates. The TOE's in-built Public Key Infrastructure (PKI) support provides for a common set of infrastructure features supporting public key and certificate-based authentication based on RSA public/private key pairs and X.509 digital certificates. The TOE is capable of importing and exporting PKCS#12-formatted certificates, as well as importing DER formatted certificates issued by third-party Certification Authorities.

The TOE's cryptographic algorithms have been validated under the Cryptographic Algorithm Validation Program (CAVP)[16]. Refer to Table 17 on page 63 for a list of the validated algorithms and their corresponding CAVP certificate numbers.

The TOE is able to read and use self-signed PKI (i.e., X.509) public key certificates for establishment of secured communication channels. The GSX subsystem is able to import configuration files, exported from trusted systems in a known configuration to support rapid deployment of subsystems by the end-user's organization.

TOE Security Functional Requirements addressed: FCS_COP.1, FTP_ITC.1, FTP_TRP.1, FPT_ITT.1, and FPT_TDC.1

7.1.3 User Data Protection (Information Flow Control)

The TOE enforces three information flow control policies:

- PEERED – this policy regulates the general flow of data through the TOE from external IT entities in addition to information that is shared with TOE subsystems that are not subject to the other two information flow control policies. This policy will make traffic flow decisions based on subject and information security attributes. The primary focus of this policy is the transfer of IP traffic and multimedia packets across the TOE from connected IT entities for onward transmission to other connected IT entities on a peered packet network or a PSTN.

[15] IKE refers to the Internet Key Exchange protocol. IKE is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations (SAs).

[16] The Cryptographic Algorithm Validation Program (CAVP) encompasses validation testing for FIPS approved and NIST recommended cryptographic algorithms and components of algorithms. The CAVP was established by NIST and the Communications Security Establishment Canada (CSEC) in July 1995.

- AUTHENTICATED – this policy regulates the flow of administrative and operational management commands from the EMS Operator Workstation to TOE subsystems. The policy also enforces local operational and administrative management commands to the TOE via each subsystem's local CLI.
- ENCRYPTED – this policy is used to enforce intra-TOE channel security in support of operating and administering TOE subsystems via the EMS management interfaces. HTTPS protects the connection between the EMS Operator Workstation and the EMS TOE subsystem server.

  Intra-TOE management (operations and administration) actions are protected using the encrypted channel mechanisms for the TOE subsystems identified in Table 23 below.

  The policy enforces channel security for secure signaling between the GSX TOE subsystem and any peered external IT entities it is signaling with using SIP over TLS or IPSec (see Table 24).

  Use of the ENCRYPTED information flow control policy ensures that TOE administrative and operational management data is protected from unauthorized disclosure. Additionally, enforcement of this policy ensures that this data is protected from modification, deletion, insertion and replay errors while en route between TOE subsystems. In the event that one of these errors occurs, the TSF is able to detect it.

Table 23: ENCRYPTED Information Flow Control SFP - Internal TOE Subsystems

Intra-TOE Communications	Encrypted Channel	Description
EMS ↔ PSX	HTTPS	Agent configuration
	PIPE over SSH	User and role integration between the two subsystems, administrative and operations management commands (CLI and via API)
EMS ↔ DSI	HTTPS	Subsystem and agent configuration Transfer of CDRs to the EMS from the DSI based on authorized Operator search criteria Transfer of Call Trace Data from the DSI to the EMS based on authorized Operator search criteria.
	TLS	Collection of GSX Parameter Interchange Format (PIF) files.
EMS ↔ GSX	SSH	Subsystem configuration (API and CLI commands)
EMS ↔ SGX	Netconf over SSH	Subsystem configuration and management. Set trap destinations and set SNMP read/write community strings, call control client creation

Table 24: ENCRYPTED Information Flow Control SFP – External IT Entities

TOE Subsystem	Encrypted Channel	Description
GSX ↔ Peered telecommunications services providers[17] 3	SIP over TLS	SIP Signaling
	SIP over IPSec	
EMS ↔ EMS Operator Workstation 8	HTTPS	Remote Administrator or Operator management GUI to EMS

TOE Security Functional Requirements addressed: FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFF.1(1), FDP_IFF.1(2), FDP_IFF.1(3), and FDP_UCT.1

7.1.4 Identification and Authentication

The TOE authenticates the claimed identity of each user before allowing the user to perform any further actions. The TOE internally maintains a set of identifiers associated with processes which are derived from the unique identifier upon login by Administrator or Operator users. The TOE supports remote authentication and use by Administrators and authorized Operators working from an EMS Operator Workstation that is part of the IT operational environment when connecting to the EMS TOE subsystem. Administrators can configure the EMS subsystem to require either username/password authentication or RADIUS-based authentication.

The TOE tracks unsuccessful logon attempts, and will take actions that have been configured by the Administrator. These actions can range from temporarily locking out the user for a period of time to blocking the IP address of the user if he is attempting to connect to the EMS from the EMS Operator Workstation.

Each TOE subsystem also supports local console CLI access for authorized users. The Administrator can define a maximum number of authentication failure attempts that are permitted before the TSF enforces a defined action or actions. Refer to Table 18 on page 69 for additional information.

The TSF enforces restrictions that can be specified by an Administrator when establishing user sessions to ensure that the set of active roles available to that user is limited to those roles for which the user is authorized (refer to Table 26 on page 96 for additional information).

The TOE maintains a userID and password for individual users. Each userID is assigned to one or more roles by the Administrator in order to carry out his or her day-to-day operational management functions of the TOE. The list of TSF-maintained roles and their associated permitted actions or privileges are described in Table 26 on page 96.

The TOE is capable of enforcing password quality metrics on a subsystem-by-subsystem basis as identified in Table 25 on the next page.

[17] Refer to the interfaces identified on Figure 2 at page 23.

Table 25: Password Quality Metrics by TOE Subsystem

TOE Subsystem	Password Quality Metrics
EMS	• minimum number of characters in the password: 10; • minimum number of alphabetic characters in the password: 4; • minimum number of special characters in the password: 2; • maximum number of repeated characters in the password: 2; and • unless configured otherwise by the Administrator, the four (4) most recent password values may not be used when resetting the password.
GSX	• password string length shall be not less than 4 and not greater than 16 characters.
PSX DSI SGX	Password quality metrics are not enforced for these subsystems.

Application Note: The Administrator can optionally require additional password complexity enforcement for the EMS subsystem in lieu of the above by running the "configureJumpstart.sh" script. Doing so will enforce the following rules for the EMS subsystem:

- *The password cannot be the same as the username.*
- *The password must be at least 8 characters long.*
- *The password must contain characters from at least two of the following categories:*
  - *lowercase letters,*
  - *uppercase letters,*
  - *numbers, and*
  - *special characters.*

The TOE allows for the configuration of password criteria to enforce strong passwords where required by organizational policy. The TOE can be configured to lock user accounts when the number of failed authentication attempts reaches an administrator defined limit.

TOE Security Functional Requirements addressed: FIA_AFL.1(1), FIA_AFL.1(2), FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, and FIA_UID.2

7.1.5 Security Management

The TOE includes the security management roles of Administrator, Provisioners, and Operators. Provisioners and Operators are operational day-to-day users assigned to roles that authorize them to perform specific operational management actions within the TOE. Users in the Administrator role can perform all management functions within the TOE Scope of Control.

The EMS subsystem is the primary tool for managing the distributed TOE. At the highest level, Administrators and authorized Operators (including Provisioners) are able to carry out the following management functions of the TOE from the EMS:

- register each of the four other subsystem nodes with EMS for remote management:
  - GSX,
  - SGX,
  - PSX, and
  - DSI;

- remotely manage the operational configuration of each inter-connected TOE subsystem via the EMS GUI;
- remotely start/stop services on all connected TOE subsystems;
- remotely manage and report on the network topology that the inter-connected TOE subsystems reside on;
- remotely monitor, report on, and modify configuration settings as required based on, the operational status of all TOE subsystems on the network;
- conduct maintenance actions on the EMS and remotely conduct maintenance actions on all inter-connected TOE subsystems;
- remotely issue administrative and operations management CLI commands to all connected TOE subsystems over a secured communications channel;
- create, report on (view), and delete or roll that audit logs;
- conduct user profile and password management; and
- remotely configure Call Data Channel (CDC) for Lawful Intercept.

In managing the TSF, Administrators and authorized operators (i.e. Provisioners and / or Operators) have the abilities identified in Table 26.

Table 26: Roles & Privileges Maintained by TOE

Admin / Management Action	Role		
	Operator	**Provisioner**	**Administrator**[18]
CLI access to subsystems	The User can login and access targets, but has no TCL[19] access.	The User has read/ write access to a subset of TCL commands.	The User has read/ write access to all TCL commands and can execute scripts.
Manage DSI (via DSI Manager in EMS)	N/A	N/A	Full access to DSI Manager
Fault Management	The User can only monitor assigned views.	The User can create, modify, and delete views used by Operators. The User can also monitor any alarm and delegate alarms to Operators.	The User can create, modify, and delete views used by Operators. The User can monitor any alarm, delegate alarms to Provisioners or Operators, and create, modify, and delete real time filters. The User also has access to the Fault Forwarding, Customize Alarm Management, and Event Purge and Administration

[18] Within Sonus' operational guidance documentation, this role is also presented as "Super User". For consistency with CC terminology and the Security Target, the term "Administrator" has been used throughout this document.

[19] TCL – Tool Command Language – is Sonus' CLI scripting language.

Table 26: Roles & Privileges Maintained by TOE

Admin / Management Action	Role		
	Operator	Provisioner	Administrator[18]
			sections of Fault Manager.
GSX Management (via GSX Navigator in EMS)	The User can access GSX Navigator. The User can issue show commands to view current configuration but cannot execute Create, Configure or Delete commands on these objects. The User does not have access to the Task Configurator. Operators also gain access to the various reports in the Tools section.	This User has the capabilities of Operator plus the ability to execute Create, Configure or Delete commands in the GSX Navigator except those commands pertaining to user management and SNMP management. In addition, Provisioners have access to the Task Configurator and can run task lists, but cannot modify them. The User also has access to the Trunk Group Wizard.	This User has all the capabilities of Provisioner plus the ability to edit, save and manage task lists in the Task Configurator. This includes the ability to Create, Configure, and Delete USER and Create, Configure, and Delete the SNMP management client.
Manage EMS (via Insight GUI)	N/A	Allows access only to the Node Registration tab in the Insight Administration section.	This User has access to the Insight GUI for managing the EMS subsystem.
Sonus Trunking Suite Health Reports	The User can view the output of scheduled reports.	In addition to viewing scheduled reports, the User can create, run and save On Demand reports, but cannot schedule reports.	User has all the capabilities of Provisioner plus the ability to schedule reports.
Manage SGX (via SGX4000 Manager in the EMS)	Allows read-only access to the SGX4000 Manager objects.	Allows read / write access to the Managed Objects , but does not allow administrative commands such as software backup, restore, upgrade, switchover , etc.	Allows full access to the SGX4000 Manager
Performance Management	The User has access to Reports but does not have access to Data Collection or Thresholding.	N/A	User has full access to Performance Management.
Manage PSX (via PSX Manager in the EMS)	N/A	N/A	The “Super User” has Entity Level Control, which allows the specification of access privileges to each PSX entity as either Read/ Write, Read Only, or

Table 26: Roles & Privileges Maintained by TOE

Admin / Management Action	Role		
	Operator	Provisioner	Administrator[18]
			None
Tools	N/A	N/A	User has access to the Tools section within EMS (call trace reports, call history reports, inventory reports, report scheduler, trunk group wizard and trunk group reporting, and task initiation of GSX commands via the CLI).
Users and roles management	N/A	N/A	User has access to the Users and Roles section within the EMS

The TOE provides Administrators with the capability to define time-limited authorizations for user accounts and passwords on the GSX subsystem as described in Table 27

Table 27: Time-limited Authorization

Limited Authorization Parameter	Period of Authorization	Notes
Password validity period	Range from 0 to 999 days. A value of 0 disables password or user account aging.	The default setting is '0'. The CC Evaluated Configuration Guidance document identifies to the Administrator the requirement to change the default setting in order to comply with FMT_SAE.1.
User account validity period		

The TOE also enables Administrators to terminate user sessions if and when required.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.3, FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, and FMT_SMR.1

7.1.6 Resource Utilization

The TOE includes a number of features to assure effective use of TOE resources. It supports the Government Emergency Telecommunications Service (GETS) to provide authorized government and emergency personnel with prioritized and high probability of completion (HPC) calling during periods when the network is overloaded (i.e., emergencies, etc.). The TSF's High Probability of Completion (HPC) features comprise a set of network capabilities applied during call setup that provide authorized GETS users with enhanced call completion during times of network stress and/or congestion. An HPC call is recognized based on the code point in the Calling Party's Category (CPC) parameter of the incoming Initial Address Message (IAM). An HPC call can also be recognized by the analysis of the dialed or signaled digits from the Called Party Number parameter. The GSX subsystem enables HPC-identified calls to receive additional network treatment to further increase the probability of call completion by assigning routing and carrier selection priorities to the call.

Additionally, the TOE includes a number of denial of service protection mechanisms to protect the system from high volume network-based attacks and permit the TOE to continue to provide its primary services.

The TOE includes quota services for its own internal storage quotas to permit automated switchover to standby devices if disk storage approaches preset limits. It also monitors CPU, memory, swap space, and file system usage on each subsystem to ensure that the TSF is able to function correctly under adverse conditions. In its default configuration, the TSF will monitor and alarm on the resource usage quotas identified in Figure 4.

Threshold Type	DSI	INSIGHT	SGX	PSX
CPU Usage Thresholds: sonusHostCpuAvgUsageRisingThresholdNotification sonusHostCpuAvgUsageFallingThresholdNotification	Minor: 50% - 45% Major: 70% - 65% Critical: 90% - 85%	Minor: 50% - 45% Major: 70% - 65% Critical: 90% - 85%	Minor: 70%-60% Major: 80%-75% Critical: 90%-85%	Minor: 70%-65% Major: 80%-75% Critical: 90%-85%
Memory Usage Thresholds: sonusHostMemUsageRisingThrshldNotification sonusHostMemUsageFallingThrshldNotification	Minor: 85%-80% Major: 95%-90%	Minor: 85%-80% Major: 95%-90%	Major 90%-85%	Critical 90%-85%
Swap Space Usage: sonusHostSwapUsageRisingThresholdNotification sonusHostSwapUsageFallingThresholdNotification	Minor: 85%-80% Critical: 95%-90%	Minor: 85%-80% Critical: 95%-90%	Major: 95%-90%	Critical: 95%-90%
File System Usage: sonusHostFsUsageRisingThresholdNotification sonusHostFsUsageFallingThresholdNotification sonusHostFsUsageThresholdNotification	Minor: 70% -65% Major: 80% - 75% Critical: 90% - 85%	Minor: 70% -65% Major: 80% - 75% Critical: 90% - 85%	Minor: 70% -65% Major: 80% - 75% Critical: 90% - 85%	Minor: 70% -65% Major: 80% - 75% Critical: 90% - 85%

Figure 4: Default Resource Usage Threshold Matrix

TOE Security Functional Requirements addressed: FRU_PRS.1, FRU_RSA.1

7.1.7 Access to the TOE

The TOE incorporates protection mechanisms for Administrator and Operator user sessions. The TOE will lock out users for a definable period of time following a prescribed number of login failures. Additionally, the TOE will automatically logout inactive sessions after an Administrator-configurable period of inactivity. The TOE includes a feature that enables Administrators to define account age-out periods so that user accounts that have been unused for a prescribed period are automatically deactivated.

Finally, the TOE enables an authorized Administrator to configure the system to display a logon banner before the logon dialog to EMS and GSX users.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_TAB.1

8 OTHER REFERENCES

This section lists references other than the TOE guidance documentation presented in Section 1.7 on page 27 that either aid in better understanding the TOE or are referred to directly in this Security Target.

[3GPP TR 21.905] Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 10), Specification ID: 3GPP TR 21.905, Version 10.3.0 (2011-03)

[3GPP TS 25.413] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface Radio Access Network Application Part (RANAP) signaling (Release 10), V10.2.0 (2011-06), retrieved from http://www.3gpp.org/ftp/Specs/html-info/25413.htm on 10 August 2011

[ASMONIA TRA] Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals D5.1(I)-1.2, prepared by the ASMONIA[20] Project, retrieved from http://www.asmonia.de/deliverables/D5.1_I_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf on 29 August 2011.

[FIPS PUB 180-4] *Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4*, March 2012, Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL)

[FIPS PUB 197] *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001, Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL)

[FIPS PUB 198-1] *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198-1, July 2008, Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL)

[GR-1083-CORE] Generic Requirements for Exchange Access Automatic Message Accounting (AMA), GR-1083-CORE, Issue 2, Revision 1 Telcordia Technologies, December, 1997

[GR-1100-CORE] Billing Automatic Message Accounting Format (BAF) Generic Requirements, GR-1100-CORE, Issue 4, Telcordia Technologies, December, 1999

[GR-1343-CORE] Generic Requirements for the Automatic Message Accounting Data Networking System (AMADNS), GR-1343-CORE, Issue 2, Telcordia Technologies, September, 1996

[GR-508-CORE] Automatic Message Accounting (AMA) Section 8, GR-508-CORE, Issue 2, Revision 1, Telcordia, December, 1998

[ITU-T Q.771 – Q.775] ITU-T Recommendations Q.771 to Q.775 "Signaling System No. 7

[20] *ASMONIA* - Attack analysis and Security concepts for MObile Network infrastructures, supported by collaborative Information exchAnge; a research effort funded by the German government.

(SS7) - Transaction Capabilities (TCAP)"

[Lucent Billdats] Billdats Data Manager AMADNS Interface Specification (Data Server to DPMS), Document No. 02DM-SE-0024, Issue 1.0, Lucent Technologies, December 11, 1998

[RADIUS RFCs] *Remote Authentication Dial In User Service (RADIUS)* definitive Requests for Comments (RFCs) including the following and their respective updates:

- RFC 2865 (June 2000): Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 (June 2000): RADIUS Accounting

[RFC 2313] *PKCS #1: RSA Encryption Version 1.5*, RFC 2313, March 1998, Internet Engineering Task Force

[RFC 2404] *The Use of HMAC-SHA-1-96 within ESP and AH*, RFC 2404, November 1998, Internet Engineering Task Force

[RFC 2407] *The Internet IP Security Domain of Interpretation for ISAKMP, RFC 2407*, November 1998, Internet Engineering Task Force

[RFC 2408] *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998, Internet Engineering Task Force

[RFC 2409] *The Internet Key Exchange (IKE)*, RFC 2409, November 1998, Internet Engineering Task Force

[RFC 2451] *The ESP CBC-Mode Cipher Algorithms*, RFC 2451, November 1998, Internet Engineering Task Force

[RFC 2833] *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, RFC 2833, March 2000, Internet Engineering Task Force

[RFC 3261] *SIP: Session Initiation Protocol*, RFC 3261, June 2002, Internet Engineering Task Force

[RFC 3329] *Security Mechanism Agreement for the Session Initiation Protocol (SIP)*, RFC 3329, January 2003, Internet Engineering Task Force

[RFC 3550] *RTP: A Transport Protocol for Real-Time Applications*, RFC 3550, July 2003, Internet Engineering Task Force

[RFC 3588] *Diameter Base Protocol*, RFC 3588, September 2003, Internet Engineering Task Force

[RFC 3602] *The AES-CBC Cipher Algorithm and Its Use with IPsec*, RFC 3602, September 2003, Internet Engineering Task Force

[RFC 3711] *The Secure Real-time Transport Protocol (SRTP)*, RFC 3711, March 2004, Internet Engineering Task Force

[RFC 4109] *Algorithms for Internet Key Exchange version 1 (IKEv1)*, RFC 4109, November 1998, Internet Engineering Task Force

[RFC 4251] *The Secure Shell (SSH) Protocol Architecture*, RFC 4251, January 2006, Internet Engineering Task Force

[RFC 4252] *The Secure Shell (SSH) Authentication Protocol*, RFC 4252, January

2006, Internet Engineering Task Force

[RFC 4253] *The Secure Shell (SSH) Transport Layer Protocol*, RFC 4253, January 2006, Internet Engineering Task Force

[RFC 4254] *The Secure Shell (SSH) Connection Protocol*, RFC 4254, January 2006, Internet Engineering Task Force

[RFC 4303] *IP Encapsulating Security Payload (ESP)*, RFC 4303, December 2005, Internet Engineering Task Force

[RFC 4733] *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals*, RFC 4733, December 2006, Internet Engineering Task Force (Obsoletes [RFC 2833])

[RFC 4741] *NETCONF Configuration Protocol*, RFC 4741, December 2006, Internet Engineering Task Force

[RFC 5246] *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, August 2008, Internet Engineering Task Force

[RFC 5905] *Network Time Protocol Version 4: Protocol and Algorithms Specification*, RFC 5905, June 2010, Internet Engineering Task Force