CA GigaStor 14.1
Security Target

Version v1.3
August 4, 2011

Prepared for:

CA Technologies

One CA Plaza

Islandia, NY 11749 USA

Prepared by:

Booz Allen Hamilton

Common Criteria Testing Laboratory

900 Elkridge Landing Road, Suite 100

Linthicum, MD 21090-2950

Table of Contents

List of Figures

List of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1.

1.1.1 ST Identification

ST Title: CA GigaStor 14.1 Security Target

ST Version: v1.3

ST Publication Date: August 4, 2011

ST Author: Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for the TOE. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

Chapter 2 describes the TOE Description, which includes the physical and logical boundaries, and describes the components and/or applications that are excluded from the evaluated configuration.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the Security Problem Definition as it relates to threats, Operational Security Policies, and Assumptions met by the TOE.

Chapter 5 identifies the Security Objectives of the TOE and of the Operational Environment.

Chapter 6 describes the Extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 7 describes the Security Functional Requirements.

Chapter 8 describes the Security Assurance Requirements.

Chapter 9 is the TOE Summary Specification (TSS), a description of the functions provided by the TOE to satisfy the SFRs and SARs.

Chapter 10 is the Security Problem Definition Rationale and provides a rationale or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims for the chosen EAL, any deviations from CC Part 2 concerning SFR dependencies, and a mapping of threats to assumptions, objectives, and SFRs. It also identifies the items used to satisfy the Security Assurance Requirements for the evaluation.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1, Table 1-2, and Table 1-3. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Terminology	Definition
GigaStor Administrator	A GigaStor user that has been given administrative privileges to access and configure the GigaStor probe in all instances.
GigaStor User	A defined GigaStor user defined whose role is to be able to view and interact with captured network traffic as permitted by the GigaStor Administrator. A GigaStor user cannot set configurations.
Instance	A preconfigured data buffer that is populated with traffic data.
Windows Administrator	The local Administrator account on the GigaStor appliance. This user can interact with the software installed directly on the appliance and is considered to have the same privileges as a GigaStor Administrator.

Table 1-1: GigaStor Specific Terminology

Terminology	Definition
CRC	Cyclic Redundancy Check. A CRC is a type of check value designed to catch transmission errors. A decoder calculates the CRC for the received data and compares it to the CRC appended by the encoder. A mismatch indicates that the data was corrupted in transit.
DAC	Discretionary Access Control (DAC) is a type of access control defined by the Trusted Computer System Evaluation Criteria "as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong."
DCE	Terminal adapter for X.21A data circuit-terminating equipment (DCE) is a device that sits between the data terminal equipment (DTE) and a data transmission circuit. It is also called data communications equipment and data carrier equipment. In the context of GigaStor, DCE is used to represent one interface to the capture card while DTE is used to represent the other. This can be used with certain network TAPs to determine the direction of traffic.
DS3	Framing specification used in transmitting digital signals at 44.736-Mbps on a T3 facility.
DTE	DTE is used primarily for those devices that display user information. It also includes any devices that store or generate data for the user. The system units, terminals, and printers all fall into the DTE category.

	In the context of GigaStor, DTE is used to represent one interface to the capture card while DCE is used to represent the other. This can be used with certain network TAPs to determine the direction of traffic.
IPX	Internetwork Packet Exchange (IPX) is a legacy network protocol used by the Novell NetWare operating systems to route packets through an internetwork. IPX is a datagram protocol used for connectionless communications - similar to IP (Internet Protocol) in the TCP/IP suite.
ISL	A method of encapsulating tagged LAN frames and transporting them over a full-duplex, point-to-point Ethernet link. The encapsulated frames may be token-ring or Fast Ethernet, and are carried unchanged from transmitter to receiver.
MPLS	Mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.
OCx	Optical Carrier specification used in ATM/SONET the 'x' represents a multiple of 51.84Mbps transmission (OC3 = 3 x 51.84 Mbps, OC24 = 24 x 511.84 Mbps).
T1	Data transfer system that transfers digital signals at 1.544 megabits per second.
T3	Communications line which can transmit data at 44.746 Megabits per second (Mbps).

Table 1-2: Industry Specific Terminology

Terminology	Definition
Authorized user	A user who, in accordance with proper authentication/authorization, is allowed to perform an operation.
External IT entity	Any IT product or system, trusted or not, outside of the TOE that interacts with the TOE.
Object	A resource or entity; examples include: dataset, volume, or command issued by a user
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 1-3: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CC	Common Criteria

CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria for Information Technology Security Evaluation
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DAC	Discretionary Access Control
DCE	Data Circuit-terminating Equipment
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
DTE	Data Terminal Equipment
EAL	Evaluation Assurance Level
FIFO	First-in First-out
FTP	File Transfer Protocol
Gb	Gigabit
GB	Gigabyte
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISL	Inter-Switch Link
IT	Information Technology
KVM	Keyboard, Video or Visual display unit, Mouse
LAN	Local Area Network
MAC	Media Access Control (address)
MPLS	Multiprotocol Label Switching
NetBIOS	Network Basic Input/Output System
NI	Network Instruments
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
OS	Operating System
PP	Protection Profile

QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SPAN	Switch Port Analyzer
SQL	Subject Query Language
ST	Security Target
TAP	Test Access Point
TB	Terabyte
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TOS	Type of Service
TSF	TOE Security Function
TTL	Time to live
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Table 1-4: Acronym Definitions

1.1.5 References

[1] Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-004, Version 3.1 Revision 3, July 2009

[2] CA GigaStor User Guide rev. 2

[3] CA Observer User Guide rev. 2

1.1.6 CC Concepts

The following are CC concepts as used in this document. A Subject is any user of the TOE (GigaStor user or GigaStor Administrator). An Object (i.e., captured traffic) can be a dataset, volume, command issued by a user, etc. An Operation is any action on a resource (e.g. read, write, create, fetch, update, control, alter, or scratch). A Security Attribute is information such as username, passwords, permissions, etc. that is kept in the Windows registry for users. An External Entity is anything outside of the TOE that affects the TOE.

1.2 TOE Reference

CA GigaStor 14.1.0043.0000

1.3 TOE Overview

CA GigaStor 14.1 is an enterprise network probe appliance. It is connected to a network tap or a switch port mirror and captures all visible traffic which is immediately written to a high-capacity RAID array for analysis. Traffic can then be analyzed locally or remotely using the NI Observer software package. GigaStor allows for in-depth statistical analysis of network trends, traffic patterns, or error conditions. It also allows for packet analysis into specific network events stored in the traffic window on the RAID.

The TOE:

- Collects network traffic data over dedicated capture interfaces
- Stores the collected traffic into a customized disk array
- Allows users to view specific packet data as well as aggregate statistics on the collected traffic

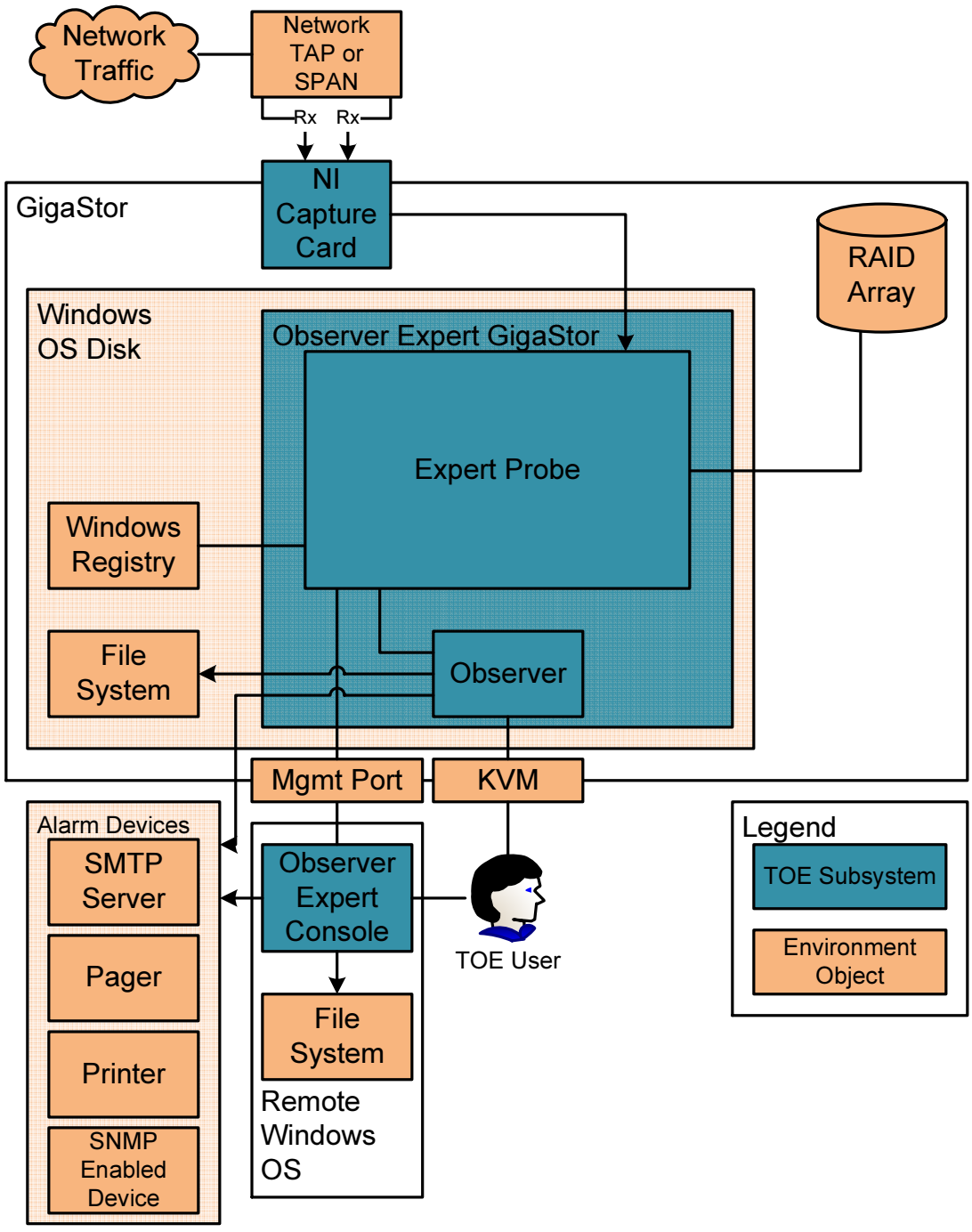

Figure 1-1: GigaStor TOE Boundary

As illustrated in Figure 1-1, the TOE boundary contains 3 components: Observer Expert Console, Observer Expert GigaStor, and the NI Capture Card.

The Observer Expert GigaStor is accessed by a local user interacting with the GigaStor appliance via a KVM. This user must log in as a Windows Administrator and then run the Observer software to access the interface. The Observer Expert GigaStor is divided further into the Observer component that controls the user interface, and the Expert Probe component that contains the packet capture and control mechanisms for network traffic. The user interface allows for analysis and dissection at the packet level as well as the calculation of general statistics and information at the network level. The TOE stores its entire user information and system configuration in the Windows Registry on the GigaStor appliance.

The Observer Expert Console is installed software on a remote Windows OS and is accessed by running the software on the remote system. This software acts as a thick client connecting to the GigaStor appliance over the management interface. It provides the same user functions as the Observer Expert GigaStor, except that it is run remotely.

The NI Capture Card is connected to a network tap or a network switch port that is configured to operate as a mirror or SPAN interface. It receives and captures the traffic to be monitored. The TOE stores all of the captured traffic into a large RAID-0 array and operates a sliding window of network traffic whenever the disk becomes full.

The TOE also provides the ability to trigger alarms on various network conditions. When an alarm is triggered, the user can be alerted through the Observer consoles, interacting with the Windows file system (local or remote), sending an email, dialing a pager, printing to a printer, or sending an SNMP trap.

1.4 TOE Type

The TOE type for GigaStor is Network Management. Network Management is defined by CCEVS as follows: “Technology that helps to protect networks against malicious attacks that might deny access or use of the network. For example, the technology used to control access to network management centers and to protect network management transactions from various kinds of attacks.”

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

Component	Definition
Observer Expert GigaStor	This represents the version of Observer that is installed by default on the GigaStor Appliance. It contains two subcomponents: *Expert Probe*: This component handles the actual capture of network traffic data and the writing of it to disk. It also handles the user access to that network traffic data and the configuration of the TOE system. *Observer*: This is the user front-end that allows interaction with the captured traffic data. This interface and functionality is identical to that described for the Observer Expert Console below.
Observer Expert Console	The Observer Expert will allow a user to view packet/decode information that is forwarded from the expert probe. It connects to a dedicated instance and allows interaction with the packet buffer that is associated with that interface. It takes actions on alarm notifications that are forwarded from the expert probe. The Observer Expert Console will also calculate many different statistics related to the collected data on the fly and present them to the user.
NI Capture Card	Capture card that receives and forwards all visible network traffic. This interface is receive only and does not register an IP address on the monitored network.

Table 2-1: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
KVM	This is the monitor, keyboard, and mouse that are used by the local Windows Administrator to interact with the GigaStor appliance directly.
Management Port	A dedicated NIC that is used by the remote Observer Expert Console to connect to the GigaStor Expert Probe.
Network Tap, Mirror, or SPAN	This is an environmental component that is responsible for forwarding network traffic to the TOE. • A Network Tap is a networking device that is connected in-line between two devices on a network and forwards all traffic between those devices to a third interface that is connected to the TOE.

	• A Mirror is a port configured on a managed switch that will forward all traffic seen on all interfaces of the switch to that single port that will be connected to the TOE. • SPAN is a Cisco proprietary technology that can forward all traffic from a Cisco switch to another device on the network (i.e. the TOE).
Pager	The TOE has the ability to dial a pager upon the detection of a configured network alarm condition.
Printer	The TOE has the ability to print a notice to the default Windows printer upon the detection of a configured network alarm condition.
RAID Array	A set of hard drives configured in a RAID-0 array to which all network traffic data is immediately written.
SMTP Server	The TOE has the ability to send an email using a configured SMTP server upon the detection of a configured network alarm condition.
SNMP Enabled Device	The TOE has the ability to send an SNMP trap message to a configured SNMP enabled device upon the detection of a configured network alarm condition.
Windows File System	The TOE has the ability to write details of events to the Windows file system upon the detection of a configured network alarm condition. It can also perform other interactions with the windows file system such as Run a program, or write to the Windows event log.
Windows Registry	The TOE pulls information from the Windows registry in order to authenticate users and check user permissions. The TOE also reads and writes information into the Windows registry to determine filters, alarms, and TOE configuration.

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications are related to GigaStor but are not included in the evaluated configuration. They provide no added security related functionality. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

- Observer Standard [Software] – Observer Standard is a separately licensed software product in the Observer family of software. It allows for local packet capture from the client machine only and does not allow for connections to the GigaStor appliance. All of its analysis functionality is incorporated into Observer Expert. This software is excluded because, in the evaluated configuration, traffic is captured by the GigaStor appliance only. Observer Standard is discussed in guidance documentation but is excluded from the evaluation.
- Observer Expert (non-console) [Software] – Observer Expert (non-console) is a separately licensed software product in the Observer family of software. It allows for local packet capture from the client machine in addition to connecting to the

GigaStor appliance. All of its analysis functionality is included with Observer Expert (console). This software is excluded because, in the evaluated configuration, traffic is captured by the GigaStor appliance only. Observer Expert (non-console) is discussed in guidance documentation but is excluded from the evaluation.

- Observer Suite [Software] – Observer Suite is a separately licensed software product in the Observer family of software. It allows for local packet capture from the client machine in addition to connecting to the GigaStor appliance. In addition to the analysis functionality of Observer Expert, it contains an SNMP management console for monitoring and managing SNMP enabled devices. It also includes additional functionality for HTML reporting. This software is excluded because, in the evaluated configuration, traffic is captured by the GigaStor appliance only. Observer Suite is discussed in guidance documentation but is excluded from the evaluation.

- GigaStor SAN [Hardware] – GigaStor SAN is a separate hardware appliance that requires a connection to a SAN (Storage Area Network) for the storage of captured traffic instead of storing it in a locally attached raid array. This hardware option is excluded because of its dependency on environmental storage for proper operation. GigaStor SAN is discussed in guidance documentation but is excluded from the evaluation.

- GigaStor WAN [Hardware] – GigaStor WAN represents different hardware configurations for the GigaStor appliance. It includes additional hardware interfaces to capture traffic from Wide Area Circuits (T1, T3, DS3, OCx, etc). This option is excluded because of its dependency on additional hardware connected to the GigaStor appliance. GigaStor WAN is discussed in guidance documentation but is excluded from the evaluation.

2.3.2 Installed but Requires a Separate License

No components are installed but require a separate license.

2.3.3 Installed But Not Part of the TSF

These capabilities exist within GigaStor, but are not included in the TSF.

- Netflow/sFlow – Netflow and sFlow are specifications for collecting additional IP traffic information from enabled network equipment. This functionality is not part of the TSF because it requires specific environmental components (routers/switches) that are present and configured to forward flow information to the TOE. It is excluded also because the flow information must be sent to the management port of the GigaStor appliance. In the evaluated configuration, the management port is considered to be separate from the capture interface.

- Snort Rules – The Snort IDS defines a standard language for triggering on network events. Observer defines a method for importing externally defined

Snort rules. This functionality, however, is outside of the TSF because GigaStor does not provide or control the rules that are used. These rules are expected to come from a third party source.

2.4 Physical Boundary

2.4.1 Hardware

The GigaStor system contains a hardware appliance as well as remote software. Therefore, it is a combination hardware/software TOE.

2.4.1.1 GigaStor Appliance

The following GigaStor appliance models are included in this evaluation:

Appliance	Description
GigaStor	This is the base GigaStor appliance that contains a capture card and a RAID array for traffic storage.
GigaStor Expandable	This model contains the base GigaStor hardware along with disk expansion units that can allow for the connection of additional hard-drives for traffic storage.
GigaStor Portable	This model contains the base GigaStor hardware along with a built-in keyboard, monitor, and trackpad.

Table 2-3: GigaStor Appliance Models

Note: The different GigaStor models are identical in security functionality and only differ in scalability.

Each GigaStor comes with the following hardware:

	Included Hardware
CPU	AMD Opteron Processor 254 2.8 GHz
Memory	8-32 GB RAM
Disk	2-16 TB : GigaStor 32 - 96 TB : GigaStor Expandable 2- 4 TB : GigaStor Portable
Capture	1GbE NI Capture Card

Table 2-4: GigaStor Hardware Specifications

2.4.1.2 Observer Expert Console

The system requirements for the remote Observer Expert Console are as follows:

	Recommended Hardware	Minimum Hardware
CPU	Quad Core Pentium Class Processor	Dual Core Pentium Class Processor

Memory	8GB RAM	2 GB RAM

Table 2-5: Observer Expert Requirements

2.4.2 Software

2.4.2.1 GigaStor Appliance

The software installed on the evaluated GigaStor appliances is identical. They contain only minor hardware differences. The following software is pre-installed on GigaStor appliances.

	Included Software
Operating System	Microsoft Windows XP Professional x64 Edition SP2
TOE	Observer Expert GigaStor 14.1

Table 2-6: GigaStor Appliance Installed Software

2.4.2.2 Observer Expert Console

The following software is required for proper installation of Observer Expert Console

	Recommended Software	Minimum Software
Operating System	Microsoft Windows XP x64	Microsoft Windows XP
TOE	Observer Expert Console 14.1	Observer Expert Console 14.1

Table 2-7: Observer Expert Console Required Software

2.5 Logical Boundary

The logical boundary of the TOE is described in the terms of the security functionalities that the TOE provides to the systems that utilize this product for network management.

The logical boundary of the TOE will be broken down into the following security classes: Traffic Capture and Analysis, User Data Protection, Identification and Authentication, and Security Management. Listed below are the security functions with a listing of the capabilities associated with them:

2.5.1 Traffic Capture and Analysis

The TOE is able to capture network traffic on the capture interface. Each packet that is captured contains the following information: Source, Destination, Size, Date, Daytime, Diff Time, Relative Time, Summary, and Packet Data. The traffic data is stored in the GigaStor RAID array where it is protected from unauthorized modification and deletion. When the disks are full, the oldest traffic is overwritten and the most recent traffic is maintained. A GigaStor Administrator has the ability to filter the traffic that is written to disk. Once the data has been written, the TOE provides users with the ability to view and interpret the captured traffic. During traffic review, a GigaStor user has the ability to

filter the traffic during analysis. The TOE also provides the ability to define network conditions that can trigger an alarm. Once an alarm has been triggered, the TOE can take one or more of the following actions as configured by the user: Append to an event log, Append to Windows System log, Pop-up a message, Sound a signal, Print to the default Windows printer, Write to a file, Execute a program, Send an e-mail, Dial a pager, Send SNMP trap, Execute Observer Statistics or Packet Capture, or no action.

2.5.2 User Data Protection

The TOE utilizes a DAC policy for enforcing permissions on user actions. The TOE defines the following permissions that can be applied to a user: access to the probe, configure, redirect, select adapters, capture packets, network trending, internet patrol, modify partial packet capture size, modify shared filters, reconstruct data, replay VoIP (Audio/Video), and transfer capture files covered. In addition, a user can be granted Administrator Rights to perform the following operations: create, edit, delete GigaStor instances; configure GigaStor probe; create, edit, delete users, and assign permissions.

If a user does not have the permission to perform a certain action, that action is grayed out in the user interface. The permissions are applied to all users with the exception of GigaStor Administrators, which have full access to the TSF.

2.5.3 Identification and Authentication

The TOE provides user accounts that have the following attributes: username, password, instance(s) allowed, permissions, or Administrator rights. All users must successfully identify and authenticate themselves utilizing their username and password combination before they can make any TSF-related actions.

2.5.4 Security Management

The security management of the TOE is controlled by user actions that are authorized by the TOE's DAC policy. The security attributes are edited and assigned using this same DAC policy. The TOE will provide permissive default values for these security attributes. There are two roles within the TOE: GigaStor users and GigaStor Administrators. All TOE users are one of these roles. GigaStor Administrators will be able to specify alternative default values based upon the needs of the TOE deployment. Using the functions within the TOE, GigaStor Administrators can revoke security attributes for users. A user's username, instance(s) allowed, and permissions can all be revoked by a GigaStor Administrator. Once an attribute has been revoked, the denial of access occurs on the next authentication attempt. Best practice would dictate that the GigaStor Administrator immediately manually disconnect the user to force re-authentication and the enforcement of the attribute change.

3 Conformance Claims

3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2009-07-004, Version 3.1 Revision 3 July 2009.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended for EAL2 to include all applicable NIAP and International interpretations through 06 January 2011.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant plus flaw remediation for EAL2 to include all applicable NIAP and International interpretations through 06 January 2011.

3.4 PP Claims

This ST does not claim conformance to any Protection Profile.

3.5 Package Claims

This TOE has a package claim of EAL2.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE is conformant to EAL2 package claims augmented with ALC_FLR.1.

3.7 Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

4 Security Problem Definition

4.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

4.2 TOE Threats

T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted, via user error, system error, or other actions.

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.MASK Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.

T.MISUSE Users of the IT system the TOE monitors may perform undesirable actions upon the IT system in question, whether by utilizing functions within the IT system that adversely affects the system or by altering the configuration to be insecure.

T.STEALTH A malicious user or process could perform suspicious activities against the TOE or objects in the Operational Environment monitored by the TOE without a TOE authorized user becoming aware of this behavior.

T.UNAUTH Users could gain unauthorized access to the TOE or its data stores by bypassing identification and authentication requirements.

4.3 Organizational Security Policies

There are no Organizational Security Policies that apply to the TOE.

4.4 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

4.4.1 Personnel Assumptions

A.ADMIN One or more authorized administrators are assigned to install, configure and manage the TOE and the security of the information it contains.

A.NOEVIL **Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.**

A.PATCHES System administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.

A.PASSWORD Users select strong passwords according to the policy described in the administrative guidance and will protect their own authentication data.

4.4.2 Connectivity Assumptions

A.AUDIT The Operational Environment will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE, the information it collects, and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.

A.FILESYS The security features offered by the Operational Environment protect the files used by the TOE.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE, and administrators will not install any general-purpose computing functionality to the Operational Environment upon which the TOE resides.

4.4.3 Physical Assumptions

A.LOCATE **The TOE will be located within controlled access facilities that will prevent unauthorized physical or logical access.**

5 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

5.1 TOE Security Objectives

The following are the TOE security objectives:

O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.

O.ALERT The TOE will provide measures for determining security alerts when audit data or IT records that represent any of these alerts is recorded.

O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.

O.CAPTURE The TOE will provide measures for collecting security relevant data from the IT system upon which it is installed. These events that will assist the authorized users in detecting misuse of the IT system, the information contained within, and/or its security features that would compromise the integrity of the IT system and violate the security objectives of the IT system.

O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.

O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.

5.2 Security Objectives for the operational environment of the TOE

The TOE's operating environment must satisfy the following objectives.

OE.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.

OE.AUDIT The Operational Environment will provide generation and storage of the audit event records using the machine upon which the TOE is installed.

OE.FILESYS	The security features offered by the Operational Environment will protect the files used by the TOE.
OE.GENPUR	No general-purpose computing capabilities will exist upon the TOE or the Operational Environment upon which the TOE resides.
OE.LOCATE	The TOE will be located within controlled access facilities that will prevent unauthorized physical access and will be logically isolated to the intranet of the IT system that it monitors.
OE.NOEVIL	All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.
OE.PASSWORD	All users of the TOE will select appropriately strong passwords and will protect their own authentication data.
OE.SYSTIME	The Operational Environment will provide reliable system time.

6 Extended Security Functional and Assurance Requirements

6.1 Extended Security Functional Requirements for the TOE

The following table provides a summary of the Extended Security Functional Requirements that are implemented by the TOE.

Security Function	Extended Security Functional Components
Traffic Capture and Analysis (FAU_EXT)	FAU_ARP_EXT.1 Traffic Alarms
	FAU_GEN_EXT.1 Traffic Capture
	FAU_SAA_EXT.1 Potential Traffic Alarm Analysis
	FAU_SAR_EXT.1 Captured Traffic Review
	FAU_SAR_EXT.3 Selectable Captured Traffic Review
	FAU_SEL_EXT.1 Selective Traffic Capture
	FAU_STG_EXT.2 Guarantees of captured traffic availability
	FAU_STG_EXT.3 Action in case of possible captured traffic loss

Table 6-1: Extended Security Functional Requirements for the TOE

6.1.1 Class FAU_EXT: Traffic Capture and Analysis

6.1.1.1 FAU_ARP_EXT.1 Component Definition

The purpose of creating additional requirements for traffic alarms is to highlight the primary functionality of the TOE. There are no current SFRs that refer to creating alarms with respect to the review of captured traffic or even the review of generic data. The closest requirements available were the Security Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_ARP_EXT.1.1 The TSF shall take [***assignment: list of actions***] upon detection of a specified condition or range of conditions.

Dependencies: FAU_SAA_EXT.1 Potential Traffic Alarm Analysis

6.1.1.2 FAU_ARP_EXT.1 Traffic Alarms

Hierarchical to: No other components.

FAU_ARP_EXT.1.1 The TSF shall take [***one or more of the following actions: Append to an event log, Append to Windows System log, Pop-up a message, Sound a signal, Print to the default Windows printer, Write to a file, Execute a program, Send an e-mail, Dial a pager, Send SNMP trap, Execute Observer Statistics or Packet Capture, or no action***] upon detection of a specified condition or range of conditions.

Dependencies: FAU_SAA_EXT.1 Potential Traffic Alarm Analysis

6.1.1.3 FAU_GEN_EXT.1 Component Definition

The purpose of creating additional requirements for traffic capture is to highlight the primary functionality of the TOE. There are no current SFRs that refer to traffic capture or generic data collection. The closest requirements available were the Security Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 The TSF shall be able to capture traffic of the following types:

a) All traffic relating to [***assignment: types of traffic***]; and

b) [***assignment: any additional types of traffic***].

FAU_GEN_EXT.1.2 The TSF shall record at least the following information for captured traffic:

a) Source, Destination, Size, Date, Daytime, Diff Time, Relative Time, Summary, Packet Data; and

b) For each collected packet, based on the auditable event definitions of the functional components included in the PP/ST, [***assignment: other traffic relevant information***].

Dependencies: FPT_STM.1 Reliable time stamps

6.1.1.4 FAU_GEN_EXT.1 Traffic Capture

Hierarchical to: No other components.

FAU_GEN_EXT.1.1 The TSF shall be able to capture traffic of the following types:

a) All traffic relating to [***Ethernet traffic on the capture interface***]; and

b) [***no additional types***].

FAU_GEN_EXT.1.2 The TSF shall record at least the following information for captured traffic:

a) Source, Destination, Size, Date, Daytime, Diff Time, Relative Time, Summary, Packet Data; and

b) For each collected packet, based on the auditable event definitions of the functional components included in the PP/ST, [***no additional information***].

Dependencies: FPT_STM.1 Reliable time stamps

6.1.1.5 FAU_SAA_EXT.1 Component Definition

The purpose of creating additional requirements for defined traffic alarm conditions is to highlight the primary functionality of the TOE. There are no current SFRs that refer to creating alarm conditions for traffic capture or generic data collection. The closest requirements available were the Security Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_SAA_EXT.1.1 The TSF shall be able to apply a set of rules in monitoring the captured traffic and based upon these rules indicate a potential alarm for the enforcement of the SFRs.

FAU_SAA_EXT.1.2 The TSF shall enforce the following rules for monitoring captured traffic:

a) Based upon [***assignment: subset of defined auditable events***] as configured in the TSF; and

b) [***assignment: any other rules***].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.6 FAU_SAA_EXT.1 Potential Traffic Alarm Analysis

Hierarchical to: No other components.

FAU_SAA_EXT.1.1 The TSF shall be able to apply a set of rules in monitoring the captured traffic and based upon these rules indicate a potential alarm for the enforcement of the SFRs.

FAU_SAA_EXT.1.2 The TSF shall enforce the following rules for monitoring captured traffic:

a) Based upon [***pre-defined alarms, NI analyzer card alarms, VoIP alarms, Application transaction analysis alarms, and filter-based alarms***] as configured in the TSF; and

b) [***meeting configured threshold values exclusive to each alarm type***].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.7 FAU_SAR_EXT.1 Component Definition

The purpose of creating additional requirements for data review is to highlight the primary functionality of the TOE. There are no current SFRs that refer to captured traffic review or generic data review. The closest requirements available were the Security

Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_SAR_EXT.1.1 The TSF shall provide [***assignment: authorized users***] with the capability to read [***assignment: list of captured traffic information***] from the captured traffic.

FAU_SAR_EXT.1.2 The TSF shall provide the captured traffic in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.8 FAU_SAR_EXT.1 Captured Traffic Review

Hierarchical to: No other components.

FAU_SAR_EXT.1.1 The TSF shall provide [***authorized users***] with the capability to read [***captured traffic information within their scope***] from the IT data records.

FAU_SAR_EXT.1.2 The TSF shall provide the IT data records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.9 FAU_SAR_EXT.3 Component Definition

Hierarchical to: No other components.

FAU_SAR_EXT.3.1 The TSF shall provide the ability to perform filtering of captured traffic based on [***assignment: list of filterable fields***].

Dependencies: FAU_SAR_EXT.1 Captured Traffic Review

6.1.1.10 FAU_SAR_EXT.3 Selectable Captured Traffic Review

Hierarchical to: No other components.

FAU_SAR_EXT.3.1 The TSF shall provide the ability to perform filtering of captured traffic based on [***Zero or more of the following: Source, Destination, Pair, Pair with ports, Address, Comments, Error, Expert Packets, Ethernet Physical Port, IP Header, Fragment Bits, Fragment Offset, IP options, TOS/Precedence, Extension Headers, Flow Label, Traffic Class, TTL/Hop Limit, Length, MPLS, Numeric Value, Partial Packet Payload, Pattern, Port, Protocol, VLAN tag, and VLAN ISL***].

Application Note: *Pair refers to the communication between a specific Source and Destination.*

Dependencies: FAU_SAR_EXT.1 Captured Traffic review

6.1.1.11 FAU_SEL_EXT.1 Component Definition

The purpose of creating additional requirements for selective traffic capture is to highlight the primary functionality of the TOE. There are no current SFRs that refer to selective traffic capture or selective generic data capture. The closest requirements available were the Security Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of traffic to be captured from the set of all captured traffic based on [***assignment: list of filterable fields***].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

FMT_MTD.1 Management of TSF data

6.1.1.12 FAU_SEL_EXT.1 Selective Traffic Capture

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of traffic to be captured from the set of all captured traffic based on [***Zero or more of the following: Source, Destination, Pair, Pair with ports, Address, Comments, Error, Expert Packets, Ethernet Physical Port, IP Header, Fragment Bits, Fragment Offset, IP options, TOS/Prescedence, Extension Headers, Flow Label, Traffic Class, TTL/Hop Limit, Length, MPLS, Numeric Value, Partial Packet Payload, Pattern, Port, Protocol, VLAN tag, and VLAN ISL***].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

FMT_MTD.1 Management of TSF data

6.1.1.13 FAU_STG_EXT.2 Component Definition

The purpose of creating additional requirements for captured traffic data storage is to highlight the primary functionality of the TOE. There are no current SFRs that refer to captured traffic data storage or generic data storage. The closest requirements available were the Security Audit class of requirements. These are slightly altered to pertain to captured traffic rather than audit records.

Hierarchical to: No other components.

FAU_STG_EXT.2.1 The TSF shall protect the stored captured traffic from unauthorized deletion.

FAU_STG_EXT.2.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorized modifications to the stored captured traffic.

FAU_STG_EXT.2.3 The TSF shall ensure that [***assignment: metric for saving captured traffic***] stored captured traffic will be maintained when the following conditions occur: [selection: captured traffic storage exhaustion, failure, attack].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.14 FAU_STG_EXT.2 Guarantees of IT Data Availability

Hierarchical to: No other components.

FAU_STG_EXT.2.1 The TSF shall protect the stored captured traffic from unauthorized deletion.

FAU_STG_EXT.2.2 The TSF shall be able to [prevent] unauthorized modifications to the stored captured traffic.

FAU_STG_EXT.2.3 The TSF shall ensure that [***all but the oldest***] stored captured traffic will be maintained when the following conditions occur: [captured traffic storage exhaustion].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.15 FAU_STG_EXT.3 Component Definition

Hierarchical to: No other components.

FAU_STG_EXT.3.1 The TSF shall [***assignment: actions to be taken in case of possible IT data storage failure***] when the storage exceeds [***assignment: pre-defined limit***].

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.1.1.16 FAU_STG_EXT.3 Action in Case of IT Data Loss

Hierarchical to: No other components.

FAU_STG_EXT.3.1 The TSF shall [***overwrite the oldest captured traffic***] when the storage exceeds [***maximum capacity***].

Application Note: *This SFR represents the sliding window of traffic data that is available to the user.*

Dependencies: FAU_GEN_EXT.1 Traffic Capture

6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

7.1 Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

Security Function	Security Functional Components
User Data Protection (FDP)	FDP_ACC.1 Subset Access Control
	FDP_ACF.1 Security Attribute Based Access Control
Identification and Authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_REV.1 Revocation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles

Table 7-1: Security Functional Requirements for the TOE

7.1.1 Class FDP: User Data Protection

7.1.1.1 FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [***DAC Policy***] on [

S***ubject: TOE users***

Object: capture probe

Operations: access to the probe, configure, redirect, select adapters, capture packets, network trending, internet patrol, modify partial packet capture size, modify shared filters, reconstruct data, replay VoIP (Audio/Video), transfer capture files covered by the SFP, Administrator Rights (create, edit, delete GigaStor instances; configure GigaStor probe; create, edit, delete users, and assign permissions)].

Dependencies: FDP_ACF.1 Security attribute based access control

7.1.1.2 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [***DAC Policy***] to objects based on the following: [***a set of allowed operations on a capture probe to be performed by a TOE user***].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***based on the DAC policy, a TOE user can perform operations on the capture probe and all unauthorized operations are inaccessible***].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***the initial GigaStor Administrator has full access to the TSF***].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

7.1.2 Class FIA: Identification and Authentication

7.1.2.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***username, password, instance(s) allowed, permissions, or Administrator Rights***].

Dependencies: No dependencies.

7.1.2.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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.

Dependencies: FIA_UID.1 Timing of identification

7.1.2.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies.

7.1.3 Class FMT: Security Management

7.1.3.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [***see Actions and Object column in Table 9-10***] to [***users with the appropriate permissions or Administrator Rights as listed in Table 9-10]***.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

7.1.3.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [***DAC Policy***] to restrict the ability to [***See Actions column in Table 9-10***] the security attributes [***See Object column in Table 9-10***] to [***users with the defined permissions or Administrator Rights listed in Table 9-10***].

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

7.1.3.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [***DAC Policy***] to provide [permissive] default values for security attributes that are used to enforce the SFP.

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

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

7.1.3.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [***see the Actions column in Table 9-10]*** the [***see the Objects column in Table 9-10***] to [***see the Permission column in Table 9-10***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

7.1.3.5 FMT_REV.1 Revocation

Hierarchical to: No other components.

FMT_REV.1.1 The TSF shall restrict the ability to revoke [***username, instance(s) allowed, permissions, and Administrator Rights***] associated with the [users] under the control of the TSF to [***GigaStor Administrators***].

FMT_REV.1.2 The TSF shall enforce the rules [***Denial of access, permissions, or Administrator Rights upon the next attempt to authenticate to the TOE***].

Dependencies: FMT_SMR.1 Security roles

7.1.3.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***list of management functions provided in Table 9-10 and Table 9-10***].

Dependencies: No dependencies.

7.1.3.7 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***GigaStor user, GigaStor Administrator***].

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

Dependencies: FIA_UID.1 Timing of identification

7.2 Operations Defined

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were modified from existing Security

Audit (FAU) requirements, are designed to address the requirements for the TOE's primary function, which is collection and indexing of IT data and the ability to search said data.

The CC permits four functional component operations – assignment, refinement, selection, and iteration – to be performed on functional requirements. This ST will highlight the four operations in the following manner:

- Assignment: allows the specification of an identified parameter. Indicated with ***bold text and italics*** if further operations are necessary by the Security Target author.
- Refinement: allows the addition of details. Indicated with ***underlined bold text and italics*** if further operations are necessary by the Security Target author.
- Selection: allows the specification of one or more elements from a list. Indicated with underlined text.
- Iteration: allows a component to be used more than once with varying operations. Indicated with the iteration number within parentheses after the short family name, e.g. FAU_GEN.1 (1), FAU_GEN.1 (2).

8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2 augmented with ALC_FLR.1.

Assurance Family	Security Assurance Requirement	
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
Lifecycle 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.1	Flaw reporting procedures
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

9 TOE Summary Specification

9.1 TOE Security Functions

The following sections identify the security functions of the TOE. They include Traffic Capture and Analysis, User Data Protection, Identification and Authentication, Security Management, Security Architecture.

9.1.1 Traffic Capture and Analysis

The primary functionality of the TOE is to collect and analyze network traffic data.

9.1.1.1 Capture

GigaStor contains an NI (Network Instruments) capture card that is meant to be connected to a device on the monitored network that will forward traffic for the GigaStor to receive. This could be an environmental network tap or a network switch port that is configured to operate as a mirror or SPAN interface. There are two interfaces on the capture card. These interfaces are labeled as DTE and DCE respectively. When connected to a supported network tap, they can indicate the direction of traffic based on which interface it is received on. The capture interfaces can receive data only. They do not register an IP on the monitored network or have the ability to transmit data in any way.

For each packet of the captured network traffic, the TOE will record the following information:

Data Field	Description
Source:	Contains the source information for the currently selected packet. Includes the Ethernet interface and the MAC address, IP address, or the domain name of the source of the packet.
Destination:	Contains the destination information for the currently selected packet. Includes the Ethernet interface and the MAC address, IP address, or the domain name of the destination of the packet.
Size:	Contains the number of bytes contained within the selected packet
Date:	Contains the date the packet was received
Day Time:	Contains the time the packet was received.
Diff Time:	Contains the time since the last packet.
Relative Time:	Contains the time in seconds (and minutes), since the start of the capture session.
Summary:	Details the type of the packet (i.e. DHCP, ARP, etc.); can include TCP/UDP packet type, source/destination IP address, port numbers, and number of errors.
Packet Data:	Contains the raw packet content stored in hexadecimal.

Table 9-1: Captured Data Fields

Although the TOE is designed to allow for the capture of all traffic, it does provide GigaStor Administrators with the ability to filter the data before it is written to disk. The different filtering options are listed in Table 9-6. All filtering options are available except for those labeled with "post-filter only."

9.1.1.2 Traffic Storage

After potentially being filtered, all captured traffic is written to a disk array on the appliance pre-configured with RAID 0 (data striping). The RAID configuration is employed in order to provide the disk throughput to handle significant network load conditions. Access to the raw data on disk is restricted to the local Windows Administrator only. No other TOE users (i.e. GigaStor Administrators or users) have the ability to modify or delete the data once it has been written. Data is written to disk in a circular buffer fashion. Once the RAID storage is full, the oldest traffic data is overwritten. This provides a sliding window of the most recent network traffic data that is available for analysis. This window will be of constant size (i.e. the size of the RAID), but will vary in time based on the network load.

9.1.1.3 Review

TOE users (GigaStor users and GigaStor Administrators) interact with the TOE in one of two ways:

- *Observer Expert GigaStor* – this represents the Observer software that comes preinstalled on the GigaStor. To interact with this software, a user must be communicating to the appliance locally via a KVM.
- *Observer Expert Console* – this represents the Observer thick client software that can be installed on a remote Windows OS. This software connects to the Probe over the management NIC using a proprietary protocol over TCP.

From a user perspective, the Observer software that is used with these two interfaces is identical. The Observer portion of Observer Expert GigaStor presents the same graphical interface as Observer Expert Console. The only difference is that the Observer Expert GigaStor contains the Expert Probe that contains the packet capture and control mechanisms that run in the background.

When using the Observer interface, each user is given access to a read-only data buffer that is populated with requested traffic data read from the RAID array. The GigaStor Administrator must pre-configure these data buffers (or instances). One instance is defined for each simultaneous user interaction with the captured data and only one user can be interacting with an instance at one time. A user is able to interact with this instance in multiple ways.

Using decode analysis, a GigaStor user is able to view the exact content of each packet that makes up the network traffic. The user can view all of the packets that arrived in a given window of time, or packets can be viewed in real-time as they arrive in the RAID. The TOE presents a chart that contains a list of packets and for each packet, all of the

data fields listed in Table 9-1. Upon selection of a packet, the user can then view the raw packet content in hexadecimal and ASCII, as well as a decoded representation of the packet data. This representation shows and identifies all recognizable fields in the packet headers and payload. A user can then expand or collapse fields and subfields as necessary. For example, a generic TCP packet would be decoded to show the Ethernet header, the IP header, the TCP header, and the payload. Upon expansion of the TCP header, a user could identify all of the different TCP fields such as source port, destination port, sequence number, acknowledgement number, etc. Upon selection of any field or subfield, the corresponding packet portion is highlighted in the raw packet content window.

In addition to deep packet inspection, the TOE is also able to calculate various types of statistical information about the captured traffic and present it to the user using a combination of charts and graphs.

Statistical Analysis

Statistical Type	Description
Bandwidth Utilization	Shows bandwidth usage statistics for the captured traffic.
Bandwidth Utilization – with Filter	Shows bandwidth usage statistics for traffic that matches a given filter (see Table 9-6)
Internet Observer Mode	Shows internet usage by users (Internet Patrol tab), by connection pairs (Pairs Matrix tab), or by sub-protocols (IP Sub-protocols tab).
Activity Display	Shows critical network utilization and broadcast information graphed against a traffic reference line.
Errors by Station	Displays error packets broken down by the source (station) of the error and the type of error packet.
Vital Signs	Shows the current network activity mapped with current error conditions on your network.
Pair Statistics (Matrix)	Tracks all conversation pairs on your network and allows a user to examine the details of a specific conversation for analysis.
Protocol Distribution	Displays network protocol usage statistics, both by protocol and by Quality of Service (QoS) precedence.
Router Observer	Shows router utilization rates to help determine if the router is acting as a bottleneck for network traffic.
Size Distribution Statistics	Shows statistics about the sizes of packets on the network.
Top Talkers Statistics	Shows most active stations on the network, along with broadcast/multicast statistics.
Utilization History	Displays long-term bandwidth utilization data and allows that data to be exported.
Utilization Thermometer	Displays the current network bandwidth utilization as a percentage of

	the total theoretical network speed.
Web Observer	Shows a Web server from the standpoint of the traffic flow into and out of the device.
VLAN Statistics	Shows the Virtual Local Area Networks (VLANs) operating on the Ethernet network.
Network Summary	Shows a summary of current network activity in a browsable tree.

Table 9-2: Statistical Types

Trending Analysis

Trending/Analysis Type	Description
Application Transaction Analysis	The Application Transaction Analysis window shows the following about applications and servers: Application response time, Application errors, Total application requests, Network delay
Network Trending	GigaStor's Network Trending allows a user to collect, store, view, and analyze the network traffic statistics over long periods of time. This will provide a baseline for comparison data.
MultiHop Analysis	MultiHop Analysis graphically conversations that traverse multiple network hops.
Application Analysis	Application Analysis allows for the viewing of detailed information about how a server is performing. It gives information such as response time and failed requests. It can determine what applications are using a specific URL and can determine what Financial Information eXchange (FIX) statistics have passed through the network.
End-to-End Analysis	End-to-End Analysis can determine the exact time conversations between two network points occurred.

Table 9-3: Trending/Analysis Types

Expert Analysis

Expert Analysis Type	Description
Expert Summary problem analysis	Shows all error events in a single display.
TCP/UDP/ICMP Events	Displays protocol-based and application-based problems as well as slow response/no response and slow connect/no connect issues.
IPX Events	Displays all communication errors being transferred via Novell.
NetBIOS Events	Displays the number of NetBIOS conditions and events that are being transferred over the network.
VoIP Events	Tracks network conditions between VoIP phones and call managers and logs a number of VoIP-related events and status flags. Also provides the ability to replay VOIP audio and video from

	specific calls.
Time Interval Analysis of any conversation	Time Interval Analysis shows network errors organized by time periods to identify whether a problem is sporadic or consistent.
Connection Dynamics	Provide a graphical view of system conversations. Packet-to-packet delay times are shown, allowing identification of long latency and response times. Retransmissions and lost packets are flagged for identification.
Reconstruct Streams	Show TCP or higher level stream data that is combined from separate packets belonging to the same data set.
Server Analysis	Displays a server/device's characteristics and response times charted against the number of simultaneous requests asked of that device. Response times are charted for recorded request sets and plotted for predicted response times as request loads increase.
What If Modeling analysis	Starts with measurements based on actual client/server conversations or peer-to-peer conversations, and plots possible response time, utilization, and packet flow scenarios.

Table 9-4: Expert Analysis Types

GigaStor Control Panel

GigaStor Control Panel Information	Description
Summary	Shows high level information about the other information sections below.
MAC Stations	List the MAC stations that are seen communicating in the defined window of captured traffic.
IP Stations	List the IP stations that are seen communicating in the defined window of captured traffic.
IP Pairs	List the set of IP addresses that are seen communicating with each other in the defined window of captured traffic
MPLS	List all Multi-Protocol Label Switching protocol communications seen in the defined window of captured traffic.
TCP Applications	List all TCP Applications identified from the traffic in the defined capture window.
UDP Applications	List all UDP Applications identified from the traffic in the defined capture window.
VLAN	Show the Virtual Local Area Network (VLAN) tags observed in the defined capture window.
Physical Ports	Show the Physical Ports that traffic is being captured on.
FIX Analysis	Show any Financial Information eXchange (FIX) that have passed during the defined capture window.

Table 9-5: GigaStor Control Panel Information

The TOE also provides the ability for GigaStor users to filter the traffic that is under review inside of that user's data buffer. When a filter is applied, only traffic that matches the filter specification is shown in the decode analysis and the specified traffic is used exclusively during the calculation of traffic statistics. The different filtering options are listed in Table 9-6. All filters in this table can be applied during traffic review. User defined filters can also be saved and shared between different users.

Filter Type	Description
Address	Specify a hardware or IP address or range of addresses to be included in the filter. This can be applied for the following fields: • Source • Destination • Pair (Source + Destination) • Pair with ports (Source/Destination pair with specific port numbers)
Comment	Filter for packets that have been commented by an Observer user and saved with a capture file (post-filter only).
Error	Filter for various categories of network errors: CRC, Alignment, packet too small, packet too large, etc.
Expert Packets	This rule allows for filtering of Observer-generated Expert packets (post-filter only).
Ethernet Physical Port	Allows for filtering of direction (DCE or DTE) on a full-duplex Ethernet port.

IP Header	This option allows for filtering based on IPv4 or IPv6 header options including:
	• Fragment Bits
	• Fragment Offset
	• IPv4
	  o IP Options
	  o TOS/Precedence
	• IPv6
	  o Extension Header
	  o Flow Label
	  o Traffic Class
	• TTL/Hop Limit

Packet Length	Filter on packet length in Bytes based on values that are 1) less than, equal to, or greater than a specified length or 2) fall within a range of length values.
MPLS	The MPLS filter allows a user to filter on any level of the Multi-Protocol Label Switching protocol.
Numeric Value	Filter for a numeric value (or range of values) that is embedded within a byte, word, or double word at a known offset, either from the beginning of the packet, or from a specified protocol header.
Pattern / Partial Packet	Filter for particular ASCII, Regular Expression, hexadecimal, or binary strings starting at specified offset (either from the beginning of the packet, or from the

Payload	beginning of a particular protocol header) or within a specified range.
Port	Specify a port or range of ports for inclusion or exclusion.
Protocol	Select a protocol and field to filter on. For example, a user can filter for ICMP Destination unreachable messages, or the presence of a VLAN tag.
VLAN tag	Filter for packets that contain a VLAN tag and/or match specific tag values (VLAN ID, priority, etc).
VLAN ISL	Filter for packets that are part of VLAN ISL (Cisco proprietary VLAN).

Table 9-6: Filter Types

9.1.1.4 Alarms

The TOE has the ability to take one or more actions upon the detection of certain network conditions. A user defines the network condition that triggers an alarm based on the captured network traffic and then assigns one or more pre-defined actions that can be taken as a result. The different condition types that can be defined are as follows:

Condition Type	Description
Pre-defined Alarms	Triggers for error and bandwidth usage conditions sensed on the network.
NI Analyzer Card Alarms	Trigger on various conditions related to the state of the NI Capture Card
VOIP Alarms	Trigger when VOIP usage or quality metrics pass a certain threshold.
Application Transaction Analysis Alarms	Trigger on any server-related statistics collected via application analysis.
Filter-based Alarms	Allows a user to define an Observer filter as a triggered alarm. See Table 9-6

Table 9-7: Alarm Conditions

Each condition contains pre-defined options that allow for the setting of threshold values and condition configuration.

Once the alarm conditions have been defined, a separate action can be defined for each alarm or a single action can be set for all alarms. An action is independent of the actual trigger or alarm (i.e., any action can be configured for any trigger or alarm). The different actions that can be taken are as follows:

Action	Description
Append to an event log	When selected, the trigger condition is written to the event log. The event log is displayed in the Triggers and Alarms dialog.
Append to Windows System log	When selected, the trigger condition is written to the Windows System Log, in the Applications section.
Pop-up a message	When selected, opens a pop up message window on the Observer station that displays the trigger condition.

Sound a signal	When selected, sounds an audible signal on the Observer station when the trigger condition is reached.
Print to the default Windows printer	When selected, prints a trouble ticket to the default Windows printer. The trigger condition will be printed on the trouble ticket.
Write to a file	When selected, writes the current trigger condition to a user specified file.
Execute a program	When selected, executes a program on the Windows command line.
Send an e-mail	When selected, sends an e-mail message to a user defined SMTP server.
Dial a pager	When selected, sends the trigger information to a pager as the action.
Send SNMP trap	When selected, sends an SNMP trap to a designated IP address
Execute Observer Statistics or Packet Capture	When selected, automatically Starts/Stops any one of statistical displays or packet capture options when the trigger condition is reached

Table 9-8: Alarm Actions

9.1.2 User Data Protection

The TOE utilizes a DAC Policy, which means that each user within GigaStor is explicitly granted or denied access to a set of operations on a probe instance. When a user intends to access an operation to which that user has not been authorized, the operation is grayed out in the Observer interface. All set permissions are stored in the Windows registry on the local GigaStor appliance. Therefore, although the Observer presents the user with the display, access to the operation is enforced on the server side by the GigaStor Expert Probe. The permissions that belong to the DAC policy are as follows:

Permission	Description
Access to probe instance	User is allowed to interact with the instance. Denied access to this permission restricts all of the following permissions.
Configure	User is allowed to change the probe's configuration options (such as memory usage, etc.).
Redirect	User is allowed to change the destination analyzer for probe analysis data.
Select adapters	User is allowed to change the adapter setting for the probe
Capture packets	User is allowed to view captured packets from the probe's network
Network trending	User is allowed to view Network Trending data from the probe's network
Internet patrol	User is allowed to run Internet Patrol on the probe's network
Modify partial packet capture size	User is allowed to change the partial packet capture setting in the Packet Capture Settings dialog for this probe.
Modify shared filters	User is allowed to modify shared filters.
Reconstruct data	User is allowed to reconstruct and view content streams from the probe's

	network (such as images over HTTP, files over FTP, etc.).
Replay VoIP (Audio/Video)	User is allowed to replay the audio and video (if applicable) of VOIP streams from the probe's network.
Transfer Capture Files	Transfer packet capture buffers to the remote Observer system and view the traffic data locally.

Table 9-9: User Permissions

In addition to the permissions above, a user can be granted Administrator rights and become a GigaStor Administrator. This user can create and edit instances, configure the GigaStor probe, and configure users and permissions. Having Administrator rights gives the user full access to the TSF.

9.1.3 Identification and Authentication

In the evaluated configuration, GigaStor enforces identification and authentication for all users accessing the network traffic, enforced through Observer. Access to the local Observer Expert Probe is restricted to users who are local Windows Administrators on the GigaStor appliance. Before allowing access to the appliance, these users must first authenticate using the standard Windows authentication mechanism. The local Windows Administrators are assumed to also be GigaStor Administrators because they have unrestricted access to TOE functions.

Users connecting via the remote Observer Expert Console are required (in the evaluated configuration) to log in using a username and password before they can attempt to connect to any instance on the probe. In addition to username and password, the TOE maintains a list for all users of instances that they are allowed to access. Therefore a user could be authenticated but denied access to a particular instance. Once the user is allowed access to an instance, the TOE checks the Administrator flag associated with each user to determine if that user is a GigaStor Administrator or a GigaStor user. GigaStor Administrators have been given admin rights and have unrestricted access to the TSF. GigaStor users have access to a subset of the TOE as defined by the permissions in the DAC policy above (except Administrator Rights). All of the user security attributes (username, password, instance(s) allowed, permissions, and Administrator rights) are stored in the Windows registry on the GigaStor appliance and are verified before allowing any interaction with network traffic.

9.1.4 Security Management

The security management of the TOE is controlled by user actions that are performed under the DAC policy as described in Section 9.1.3. There are two roles defined within the TOE: GigaStor users and GigaStor Administrators. All user accounts are considered one of those two roles. GigaStor users are defined as any user that can have any subset of permissions, but does not have Administrator Rights. GigaStor Administrators have Administrator Rights, which allow them to manage GigaStor instances, GigaStor probes, and user accounts.

The TOE defines the following objects and actions upon those objects that are available to users with the appropriate permissions.

Objects	Actions	Permissions
GigaStor Instance	Create, Edit, Delete	Administrator Rights
	Redirect	Redirect
	Configure allocated Memory	Configure
	Configure network adapter	Select adapters
	Configure packet capture settings	Modify partial packet capture size
GigaStor Probe	Configure probe reserved Memory	Administrator Rights
	Configure system clock synchronization	Administrator Rights
Captured Traffic	View, Filter (See Table 9-6), Decode	Access to probe instance, Capture packets
	View GigaStor Control Panel Information from Table 9-5	Access to probe instance, Capture packets
	View Statistical Types from Table 9-2 (excluding Internet Observer Statistics)	Access to probe instance
	View Internet Observer statistics	Access to probe instance, Internet Patrol
	View Trending/Analysis Data specified in Table 9-3 (excluding Network Trending)	Access to probe instance
	View Network Trending Information	Access to probe instance, Network trending
	View Expert Analysis Data specified in Table 9-4 (excluding VOIP replaying and Stream Reconstruction)	Access to probe instance, Capture packets
	Reconstruct Streams	Access to probe instance, Capture packets, Reconstruct data
	Replay VOIP calls	Access to probe instance, Capture packets, Replay VoIP (Audio/Video)
	Transfer	Access to probe instance, Capture packets, Transfer capture files
Shared Filters	Create, Edit, Delete	Modify shared filters
Observer Alarms/Triggers	Create, Edit, Delete, Configure	Access to probe instance
Users	Create, Edit, Delete, Assign Permissions	Administrator Rights

Table 9-10: GigaStor Management Functions

The TOE will provide permissive default values for security attributes. When a user is initially created, that user has access to all of the permissions defined in Table 9-9. Therefore, new users can perform any action within system by default, except for actions restricted to GigaStor Administrators. GigaStor Administrators have the ability to specify alternative default values based upon the needs of the TOE deployment.

GigaStor Administrators possess the ability to edit the security attributes for users in the system. This is governed by the same DAC policy described above. The following table describes the modification of attributes:

Attributes	Actions	Permissions
Username	Create	Administrator Rights
Password	Reset	None (Users can reset their own passwords)
Instance(s) Allowed	Grant/Deny Access	Administrator Rights
Permissions (See Table 9-9)	Assign	Administrator Rights
Administrator Rights	Assign	Administrator Rights

Table 9-11: User Attributes

The GigaStor Administrator can add or revoke access to the permissions defined in Table 9-9 at any time. The GigaStor Administrator can add or revoke access to instances in general as well as delete a user completely, thereby revoking that username. These changes can be applied to all users except for the initial original GigaStor Administrator account. This account cannot be modified.

Any change to a users attributes does not take effect until the next time that user attempts to log into the system. Therefore, in order to enforce any revocation of privileges, a GigaStor Administrator must use the TOE functions to manually disconnect the effected user. The user will then be forced to re-authenticate and the changes will be enforced.

9.1.5 Security Architecture

GigaStor has multiple architecture features that enhance the security functions of the TOE.

The local Windows Administrator on the GigaStor appliance is the only user that has the ability to access or modify the raw files stored on the RAID array. GigaStor Administrators do not necessarily have local Windows Administrator access. Therefore, even though they can interact with the traffic data written to disk using the TOE functions (i.e. filtering), they cannot interact with it in any out-of-band fashion. Similar, but more restrictive logic applies to standard GigaStor users. GigaStor users can only interact with read-only copies of the network traffic and have no ability, even using TOE functions, to modify the data on the RAID array. GigaStor users have no local access to the Windows installation on GigaStor, and therefore cannot use any logical means to alter the RAID array or its data. All user and TOE configuration is stored within the Windows registry on the GigaStor appliance on a drive separate from the RAID array. This means that the

GigaStor configuration data space has no overlap with the GigaStor captured traffic data space.

The local Windows Administrator account is the only account that is defined on the GigaStor appliance Windows environment. Therefore, local access to the GigaStor appliance implies full access to TOE data and there is no possibility for privilege escalation from any other Windows accounts. Because of this, it is assumed that only GigaStor Administrators have access to the local Windows Administrator account. Furthermore, Windows is a trusted 3rd party component that is expected to provide a reasonably secure local authentication mechanism for the local Windows Administrator account.

Remote GigaStor users cannot get access to GigaStor data (i.e. connect to an instance and interact with network traffic) until after Windows has booted completely and the identification, authentication, and authorization functionality of GigaStor has been started.

The capture interfaces are located on completely separate hardware from the management NIC and have independent network connections. As long as the capture and management interfaces are connected to separate networks, no traffic from the capture interfaces can interfere with the management NIC. Also, because the capture interfaces are receive only and have no network address, no device on the capture network has the ability to communicate directly with the GigaStor appliance.

The physical RAM that is used by the GigaStor software on the appliance to store packet buffers is completely reserved by the software. The Windows operating system will only recognize and use a portion of the actual physical RAM attached to the device. The packet buffer RAM is completely dedicated and is not under the control of Windows. Therefore, it will never be swapped out to disk or be re-used by other Windows software/services.

Furthermore, a block of memory within the GigaStor dedicated storage will be reserved and allocated for each specific instance defined in the system. This means that each user packet buffer is separately allocated and controlled by GigaStor. Packet buffers are separate in physical RAM and there is no overlap between them.

Every user interaction with an instance (as well as modes within that instance) is controlled by a different software execution thread that also controls the RAM associated with that instance. It is therefore difficult for one thread to directly affect another or access the RAM allocated to another instance.

9.2 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following tables.

Security Function	Security Functional Components
Traffic Capture and Analysis (FAU_EXT)	FAU_ARP_EXT.1 Traffic Alarms
	FAU_GEN_EXT.1 Traffic Capture
	FAU_SAA_EXT.1 Potential Traffic Alarm Analysis
	FAU_SAR_EXT.1 Captured Traffic Review
	FAU_SAR_EXT.3 Selectable Captured Traffic Review
	FAU_SEL_EXT.1 Selective Traffic Capture
	FAU_STG_EXT.2 Guarantees of captured traffic availability
	FAU_STG_EXT.3 Action in case of possible captured traffic loss

Figure 9-1: Extended Security Functional Components for the TOE

Security Function	Security Functional Components
User Data Protection (FDP)	FDP_ACC.1 Access control policy
	FDP_ACF.1 Access control functions
Identification and Authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_REV.1 Revocation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles

Figure 9-2: Security Functional Components for the TOE

9.2.1 Traffic Capture and Analysis

This section maps directly to the information found in Section 9.1.1. This security classification addresses the following requirements:

FAU_ARP_EXT.1, FAU_GEN_EXT.1, FAU_SAA_EXT.1, FAU_SAR_EXT.1, FAU_SAR_EXT.3, FAU_SEL_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3

The referred section specifically addresses FAU_ARP_EXT.1 and FAU_SAA_EXT.1 by providing a list of what kind of network conditions trigger alarms as well as the actions taken upon a triggered alarm. FAU_GEN_EXT.1 is satisfied by providing a list and

description of each field that is populated within captured Ethernet traffic. FAU_SAR_EXT.1 is satisfied by providing information on how users are given access to the captured traffic, and the various ways traffic can be presented. FAU_SAR_EXT.3 and FAU_SEL_EXT.1 are satisfied by listing and describing all the fields that can have filters applied to them, either on incoming traffic to be written, or on traffic that is read from the RAID array. FAU_STG_EXT.2 and FAU_STG_EXT.3 are satisfied by describing how data is captured by supplying information about the NI Capture Card and RAID Array. It also explains that the raid array is a sliding window of the most recent data, and that no functionality exists for users to modify or delete the data through TOE functionality.

9.2.2 User Data Protection

This section maps directly to the information found in Section 9.1.2. This security classification addresses the following requirements:

FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 are addressed by explaining how users and their allowed permissions scope what a user can perform using TOE functionality. This explanation describes the DAC policy utilized by the TOE.

9.2.3 Identification and Authentication

This section maps directly to the information found in Section 9.1.3. This security classification addresses the following requirements:

FIA_ATD.1, FIA_UAU.2, FIA_UID.2

FIA_ATD.1 is addressed by showing the attributes a user has: username, password, instance(s) allowed, permissions, or Administrator rights. FIA_UAU.2 and FIA_UID.2 are detailed by explaining the user interfaces in the TOE and how nothing can be done until they successfully log in to the TOE.

9.2.4 Security Management

This section maps directly to the information found in Section 9.1.4. This security classification addresses the following requirements:

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1

FMT_MOF.1, FMT_MTD.1, and FMT_SMF.1 are addressed by referring to Table 9-10, which details all of the functions available within the system based upon permissions. FMT_MSA.1 is explained by referring to Table 9-11, which details all of the security attributes involved in the DAC policy. FMT_MSA.3 is shown by stating that users created have access to all of the permissions defined in Table 9-9. FMT_REV.1 is addressed by stating that users can have their user account or permissions revoked at any time by a GigaStor Administrator. FMT_SMR.1 is addressed by enumerating the roles within the TOE and specifying the key differentiators of those roles.

10 Security Problem Definition Rationale

10.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

Assumption	Objective	Rationale
A.ADMIN One or more users authorized by the Operational Environment will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. ADMIN in order to ensure that only the users authorized by the TOE will install and configure the TOE to bring it into the evaluated configuration. During operation only the users authorized by the TOE will be able to manage the TOE in a manner that maintains its ADMIN objectives.
A.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
A.PATCHES Users exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.	OE.ADMIN One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. PATCHES in order to ensure that the users authorized by the TOE will properly patch the TOE and the Operational Environment in a manner that maintains their security objectives.
A.PASSWORD Users select strong passwords according to the policy described in the administrative guidance and will protect their own authentication data.	OE.PASSWORD All users of the TOE will select appropriately strong passwords and will protect their own authentication data.	OE.PASSWORD maps to A.PASSWORD in order to ensure that user authentication data is sufficiently secure and therefore that the authentication mechanism itself is more secure.
A.AUDIT The Operational Environment will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE, the information it collects, and/or its security features that would compromise the integrity of the	OE.AUDIT The Operational Environment will provide generation and storage of the audit event records using the machine upon which the TOE is installed.	OE.AUDIT maps to A.AUDIT to ensure that there is audit event data captured by the Operational Environment of the TOE that enhances the security functionality of the product with respect to the data that authorized users may utilize to make security decisions.

TOE and violate the security objectives of the TOE.		
A.FILESYS The security features offered by the Operational Environment protect the files used by the TOE.	OE.FILESYS The security features offered by the Operational Environment will protect the files used by the TOE.	OE.FILESYS maps to A.FILESYS in order to ensure that the Operational Environment's native security features are utilized when securing data relevant to the TOE outside of its boundary.
A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE, and administrators will not install any general-purpose computing functionality to the Operational Environment upon which the TOE resides.	OE.GENPUR No general-purpose computing capabilities will exist upon the TOE or the Operational Environment upon which the TOE resides.	OE.GENPUR maps to A.GENPUR in order to ensure that the TOE will not be used for any purposes other than those prescribed by the vendor. Specifically, the addition of non-TOE software or firmware that would add non-TSF functionality or present additional threat vectors is prohibited.
A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical or logical access.	OE.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access and will be logically isolated to the intranet of the IT system that it monitors.	OE.LOCATE maps to A.LOCATE in order to ensure that physical security is provided in the environment where the TOE operates.

Table 10-1: Assumption to Objective Mapping

Threat	Objective	Rationale
T.ACCESS Authorized users could gain electronic access to protected TOE resources by attempting to establish a connection that they are not permitted to perform.	O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	O.ACCESS addresses T.ACCESS by providing the authorized administrators of the TOE with the capability to specify access restrictions on the protected TOE resources to authenticated TOE users.
	O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	O.MANAGE addresses T.ACCESS by ensuring only users authorized by the TOE can use the TOE provided resources to manage and monitor the TOE's capabilities.
T.ADMIN_ERROR A user may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	O.ROBUST_ADMIN_GUIDANCE The TOE will provide the TOE's users with the necessary information for secure delivery, installation, management, and operation of the TOE.	O.ROBUST_ADMIN_GUIDANCE helps to mitigate T.ADMIN_ERROR by ensuring the TOE users have guidance that instructs them how to administer the TOE in a secure manner and to provide the TOE users with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that a user might make that could cause the TOE to be configured in a way that is unsecure.
	O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	O.MANAGE addresses T.ADMIN_ERROR by ensuring only users authorized by the TOE can use the TOE provided resources to manage and monitor the TOE's auditing capabilities.
T.MASK Users whether they be malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.	O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	O.AUTH addresses T.MASK by ensuring that all users that try and access the TOE become identified and authenticated before access is granted.
T.MISUSE	O.CAPTURE	O.CAPTURE addresses

Threat	Objective	Rationale
Users of the IT system the TOE monitors may perform undesirable actions upon the IT system in question, whether by utilizing functions within the IT system that adversely affects the system or by altering the configuration to be insecure.	The TOE will provide measures for collecting security relevant data from the IT system upon which it is installed. These events that will assist the authorized users in detecting misuse of the IT system, the information contained within, and/or its security features that would compromise the integrity of the IT system and violate the security objectives of the IT system.	T.MISUSE by providing the users authorized to utilize the TOE with the capability to perform monitoring functions by utilizing the data that the TOE collects. This data is potentially able to allow these users to find undesirable actions performed upon the IT system the TOE monitors.
	O.ALERT The TOE will provide measures for determining security violations and will create alarms when audit data that represents any of these violations is processed.	O.ALERT helps mitigate T.MISUSE by allowing the TOE to send alerts to configured users upon a potential security issue within the operational environment.
T.STEALTH A malicious user or process could perform suspicious activities against the TOE or objects in the Operational Environment monitored by the TOE without a TOE user authorized by the Operational Environment becoming aware of this behavior.	O.ALERT The TOE will provide measures for determining security violations and will create alarms when audit data that represents any of these violations is processed.	O.ALERT addresses T.STEALTH by providing the users with the ability of receiving alert notifications from the TOE when events are considered to be a security violation based on defined policy.
	O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	O.AUTH addresses T.STEALTH by ensuring that all users that try and access the TOE become identified and authenticated before access is granted.
	O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	O.ACCESS helps to mitigate T.STEALTH by providing the TOE with access control functions, which restricts access to the TOE and its objects to users which have been authorized access by an administrator.
	O.CAPTURE The TOE will provide measures for collecting security relevant data from the IT system upon which it is installed. These events that will assist the authorized users in	O.CAPTURE helps to mitigate T.STEALTH by providing the TOE with captured traffic data that allows authorized users to determine the origin of security-relevant network traffic transferred over the IT

Threat	Objective	Rationale
	detecting misuse of the IT system, the information contained within, and/or its security features that would compromise the integrity of the IT system and violate the security objectives of the IT system.	system the TOE monitors.
	OE.AUDIT The Operational Environment will provide local access control, and storage of the event audit records which are stored on the machine where the TOE is installed.	OE.AUDIT helps to mitigate T.STEALTH by providing the TOE with Operational Environment's ability to store the audit data and protect the event audit records from local access.
	OE.SYSTIME The Operational Environment will provide reliable system time.	OE.SYSTIME helps to mitigate T.STEALTH by ensuring the accuracy of the tools necessary to monitor network activity as provided via O.CAPTURE.
T.UNAUTH Users could gain unauthorized access to the TOE or its data stores by bypassing identification and authentication requirements.	O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	O.ACCESS helps to mitigate T.UNAUTH by providing the TOE with access control functions, which restricts access to the TOE and its objects to users which have been authorized access by an administrator.
	O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	O.AUTH helps to mitigate T.UNAUTH by ensuring that all users that try and access the TOE become identified and authenticated before access is granted.
	O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	O.MANAGE helps to mitigate T.UNAUTH by ensuring only users authorized by the TOE can use the TOE provided resources to manage and monitor the TOE's auditing capabilities.
	OE.ADMIN One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the	OE.ADMIN helps to mitigate T.UNAUTH by ensuring that only administrators authorized by the TOE can configure and manage the TOE.

Threat	Objective	Rationale
	information it contains.	

Table 10-2: Threat to Objective Mapping

10.2 Operational Security Policy Rationale

There are no Organizational Security Policies that apply to the TOE.

10.3 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE objectives.

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	FDP_ACC.1 Access control policy	FDP_ACC.1 details that the policy defined by FDP_ACF.1 is enforced on all users looking to perform any action on the TOE.
	FDP_ACF.1 Access control functions	FDP_ACF.1 details all of the access control factors. It also shows some use cases for specific scenarios of the DAC policy.
	FIA_ATD.1 User attribute definition	FIA_ATD.1 shows all of the user attributes that are utilized to authorize users, including permissions and allowed instances.
	FMT_REV.1 Revocation	FMT_REV.1 details how a user loses his or her session object based upon administrative changes.
	FMT_SMR.1 Security Roles	FMT_SMR.1 requires users to only perform actions within the users' role.
O.ALERT The TOE will provide measures for determining security alerts when audit data or IT records that represent any of these alerts is recorded.	FAU_ARP_EXT.1 Traffic Alarms	FAU_ARP_EXT.1 sends alerts to various configured destinations based upon the security alarm conditions defined within FAU_SAA_EXT.1
	FAU_SAA_EXT.1 Potential Traffic Alarm Analysis	FAU_SAA_EXT.1 defines security alarm conditions created by authorized users.
O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the security-relevant attributes of all users. This includes attributes related to authentication and access control.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires users to authenticate to the TOE before any TSF-mediated actions are allowed.

Objective	Security Functional Components	Rationale
	FIA_UID.2 User identification before any action	FIA_UID.2 requires users to identify themselves to the TOE before any TSF-mediated actions are allowed.
O.CAPTURE The TOE will provide measures for collecting security relevant data from the IT system upon which it is installed. These events that will assist the authorized users in detecting misuse of the IT system, the information contained within, and/or its security features that would compromise the integrity of the IT system and violate the security objectives of the IT system.	FAU_GEN_EXT.1 Traffic Capture	FAU_GEN_EXT.1 details the types of captured packet data that the TOE collects, the types of data sources, and the minimum contents of the data that is collected. This provides assurance that sufficient data is available to TOE users for analysis.
	FAU_SAR_EXT.1 Captured Traffic Review	FAU_SAR_EXT.1 states that authorized users are only allowed to read the captured packet information over which said user has scope.
	FAU_SAR_EXT.3 Selectable Captured Traffic Review	FAU_SAR_EXT.3 describes the filtering method to determine which stored data is presented to authorized users via their passive instance.
	FAU_SEL_EXT.1 Selective Traffic Capture	FAU_SEL_EXT.1 describes the filtering method to determine which collected data is actually written to the local storage.
	FAU_STG_EXT.2 Guarantees of captured traffic availability	FAU_STG_EXT.2 states that no TOE user can delete or modify data, and that all data is preserved indefinitely within the TOE functionality. This provides assurance that the indexed data is complete and accurate.
	FAU_STG_EXT.3 Action in case of possible captured traffic loss	FAU_STG_EXT.3 states that the TOE will roll over the oldest data with the newest collected data, assuring that the newest data is always available.
O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 defines the capabilities that can be enabled or disabled on specific users by authorized users.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 defines the management actions and which permissions allow users to perform specific functions. Authorized users are able to perform these access control policy changes.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 requires all security-relevant attributes have permissive default values, and that an authorized user has the ability to override default

Objective	Security Functional Components	Rationale
		values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 defines the conditions which permissions allow users to perform specific actions on TSF data. Authorized users are able to perform these access control policy changes.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 defines the functions that can be performed by specific types of users of the TOE.
	FMT_SMR.1 Security Roles	FMT_SMR.1 defines the roles associated with each user of the TOE.
O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.	AGD_OPE.1 Operational User Guidance	AGD_OPE.1 describes the proper delivery, usage, and management of the TOE.

Table 10-3: Security Functional Requirements Rationale

10.4 EAL2 Justification

The threats that were chosen are consistent with attacker of basic attack potential, therefore EAL2 augmented with ALC_FLR.1 was chosen for this ST. ALC_FLR.1 is not required, but provides additional quality assurance to the product.

10.5 Requirement Dependency Rationale

The table below lists each requirement from claimed Security Functional Requirements with a dependency and indicates whether the dependent requirement was included. If a dependency has not been met, a short rationale is provided to show why the dependency was not included.

Functional Component	Dependency	Included
FAU_ARP_EXT.1	FAU_SAA_EXT.1	YES
FAU_GEN_EXT.1	FPT_STM.1	NO, the environment fulfills this dependency (OE.SYSTIME).
FAU_SAA_EXT.1	FAU_GEN_EXT.1	YES
FAU_SAR_EXT.1	FAU_GEN_EXT.1	YES
FAU_SAR_EXT.3	FAU_SAR_EXT.1	YES

FAU_STG_EXT.2	FAU_GEN_EXT.1	YES
FAU_SEL_EXT.1	FAU_GEN_EXT.1	YES
	FMT_MTD.1	YES
FAU_STG_EXT.3	FAU_GEN_EXT.1	YES
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1	YES
	FMT_MSA.3	YES
FIA_UAU.2	FIA_UID.1	YES (Hierarchy: FIA_UID.2)
FMT_MOF.1	FMT_SMR.1	YES
FMT_MSA.1	FDP_ACC.1 or FDD_ICF.1	YES (FDP_ACC.1)
	FMT_SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_REV.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES (Hierarchy: FIA_UID.2)

Table 10-4: Requirement Dependencies