LogLogic v4.6.1
Open Log Management Platform
Security Target

Release Date: 30 June 2009
Version: 2.0

Prepared for: **LogLogic Inc.**
110 Rose Orchard Way, Suite 200
San Jose, CA 95134

Prepared by: **Savvis Federal Systems**
45901 Nokes Boulevard
Sterling, VA 20166

Table of Contents

List of Figures

List of Tables

Introduction

This document presents the Security Target (ST) for the LogLogic v4.6.1 Open Log Management Platform at Evaluation Assurance Level 2+.

An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). An ST principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats which that product is intended to counter, and any known rules with which the product must comply.
- A set of security objectives and a set of security requirements to address that problem.

The ST for a TOE is a basis for agreement between developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. Because the audience for an ST may include not only evaluators but also developers and, "those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE" this ST minimizes terms of art from the *Common Criteria for Information Technology Security Evaluations* (CC).

1.1 ST Reference

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title	LogLogic v4.6.1 Open Log Management Platform Security Target
Version:	2.0
Publication Date:	30 June 2009
ST Author	Savvis Federal Systems (SFS)
Assurance Level:	EAL2 augmented with ALC_FLR.2
Protection Profile Conformance	U.S. Government Protection Profile: Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, 25 July 2007.

1.2 TOE Reference

The TOE claiming conformance to this ST is identified as: LogLogic v4.6.1 Open Log Management Platform with one or more LX Appliance (Model numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model numbers ST2010 and ST 3010). Throughout the remainder of the ST, the TOE is referred to as LogLogic v4.6.1.

1.3 Document Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement, and selection are defined in Section C.4 the CC version 3.1 Part 1.

a) The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)]

b) The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold** for additions and ~~strike-through~~ for deletions.

c) The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

d) The iteration operation is used to repeat or reuse a CC requirement multiple times in the same document with different operations used to complete the requirement for each occurrence. Iterations are denoted by an increasing number inside parenthesis following the requirements short name. Example: FCS_COP.1 (1).

e) Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.4 Document Terminology

This section describes terms that are used throughout the IDSSPP and Section 4 of Part 1 of the Common Criteria. The following terms are a subset of those definitions. In addition to these general definitions, this Security Target also references specialized definitions. They are listed in table 1 below to aid the user of the Security Target.

Term	Definition
Analyzer data	Data collected by the Analyzer functions
Analyzer functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Anomaly	Activity determined by the TOE as deviating or inconsistent from the norm.
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Trail	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various

	activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authentication data	Information used to verify the claimed identity of a user.
Authorized Administrator	A subset of authorized users that manage an IDS component
Authorized User	A user that is allowed to perform IDS functions and access data
Availability	Assuring information and communications services will be ready for use when expected.
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
Class	A grouping of CC families that share a common focus.
Data Source	Networked third-party devices or applications such as firewalls, VPN concentrators, servers, routers, switches, storage devices, and applications
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
IDS component	A Sensor, Scanner, or Analyzer.
Information Technology (IT) System	May range from a computer system to a computer network
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System (IDS)	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.

IDS Analyzer (Analyzer)	The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
IDS Scanner (Scanner)	The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
IDS Sensor (Sensor)	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Java	An object-oriented programming language based loosely on C++ language and developed by Sun Microsystems, Inc.
MySQL	A multithreaded, multi-user SQL database management system (DBMS) owned by a subsidiary of Sun Microsystems, Inc.
Network	Two or more machines interconnected for communications
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Operational environment	The environment in which the TOE is operated.
Package	A named set of either functional or assurance requirements
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Scanner data	Data collected by the Scanner functions
Scanner functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner

	data)
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Sensor data	Data collected by the Sensor functions
Sensor functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data)
Security Attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security
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.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
Trojan Horse	An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE

	and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user, that does not affect the operation of the TSF.
Virus	A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Table 1: Document Terminology

1.5 Document Acronyms

CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HA	High Availability
IDS	Intrusion Detection System
IDSAPP	Intrusion Detection System Analyzer Protection Profile
IT	Information Technology
NTP	Network Time Protocol
OSP	Organizational Security Policy
PP	Protection Profile

RAID	Redundant Arrays of Inexpensive Disks
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function

Table 2: Document Acronyms

1.6 TOE Overview

The TOE is LogLogic v4.6.1 Open Log Management platform, an Intrusion Detection system (IDS) that analyzes event logs for network anomalies or security policy breaches. The TOE provides administrative alerts, flexible reporting, and searching on the analyzed data and long term storage of unaltered event logs.

Log data is collected from networked third-party sources such as firewalls, VPN concentrators, servers, routers and switches, storage devices, and applications (both commercial and custom developed).

1.7 TOE Description

The LogLogic v4.6.1 TOE is composed of two families of physically distinct components. The LX series of appliances normalizes event log data, stores it in a database, and provides analysis, alerting, and reporting through metalog creation.

The LX appliance supports a number of methods to capture event logs from log sources:

1. The LX appliance can be configured to receive streamed event logs using the SYSLOG, HTTP, or HTTPS protocols.
2. The LX appliance can receive event logs from sources configured to use a collector agent.
3. Event log files can be transferred to the LX appliance using a file transfer method with one of the following protocols: SFTP, SCP, HTTP, HTTPS, FTP, FTPS, CIFS.
4. The following source specific methods:
    a. Outbound log file retrieval to Checkpoint LEA /CPMI log sources
    b. Outbound MS SQL queries via JDBC

The LX appliance provides searching and flexible reporting via provided templates and up to 15,000 custom reports.

The TOE computes a MD5 hash for each event log file it collects and stores the hash value in the database separately from the log itself. It will check for that MD5 hash value in the database and if it already exists then it is considered to be a duplicate and does not replace the file.

The ST series of appliances archives unaltered logs for long-term retention. The LX and ST appliances communicate over an encrypted TCP tunnel providing for the secure transfer of logs or archiving. Adding additional appliances scales the solution as the monitored network and log data volume grow.

The LX and ST have their own independent data stores and log retention periods. The LX appliance has the capability of archiving raw log data and metadata for up to 90 days. The ST appliance provides for long-term archival of raw log data.

Log data older than 90 days on the ST appliance can be searched. Alternatively, administrators can use the Replay function. The replay function will stream archived logs stored on the ST device back to the LX device for re-analysis, alerting, and reporting.

The following conditions must be met for the TOE to be deployed in the evaluated configuration:

1. At least one LogLogic LX Appliance (There can be more than one LX deployed in the evaluated configuration) and at least one LogLogic ST Appliance (There can be more than one ST deployed in the evaluated configuration.) When configured to support HA, the TOE consists of a minimum of three network appliances such that at least one ST or LX is part of a HA pair.

2. To utilize all of the evaluated security functionality of the TOE, the TOE environment would include commercially available RADIUS, TACACS, or Active Directory authentication servers.

Figure 1 represents the minimal set of the TOE components required to provide the full set of functionality described in this ST. Figure 2 shows how additional LX Appliances can be added to the deployment. Figure 3 shows the LX and ST appliances deployed in an optional HA failover configuration.

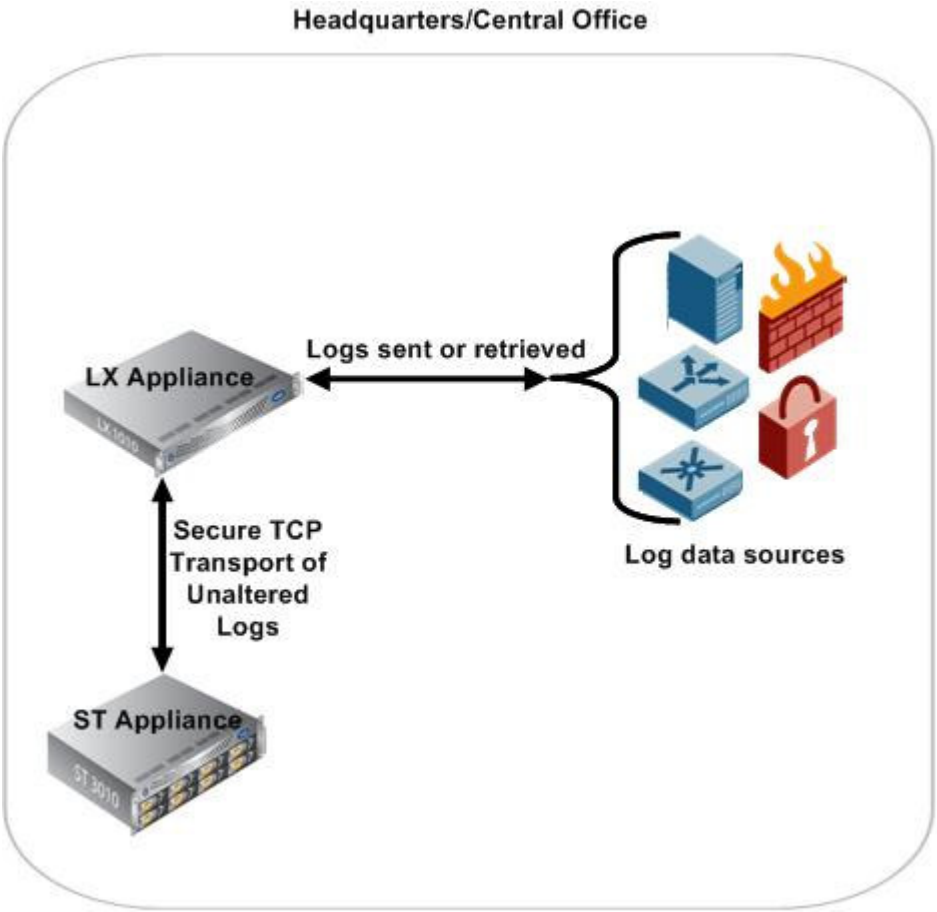

Figure 1: TOE Deployment Configuration #1

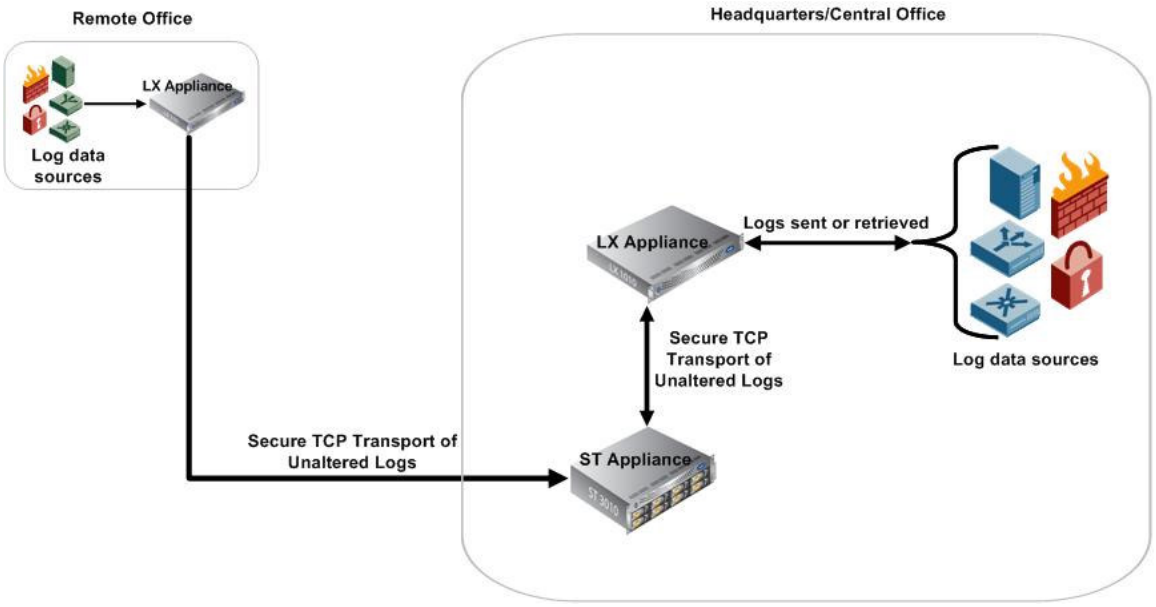

Figure 2: TOE Deployment Configuration #2

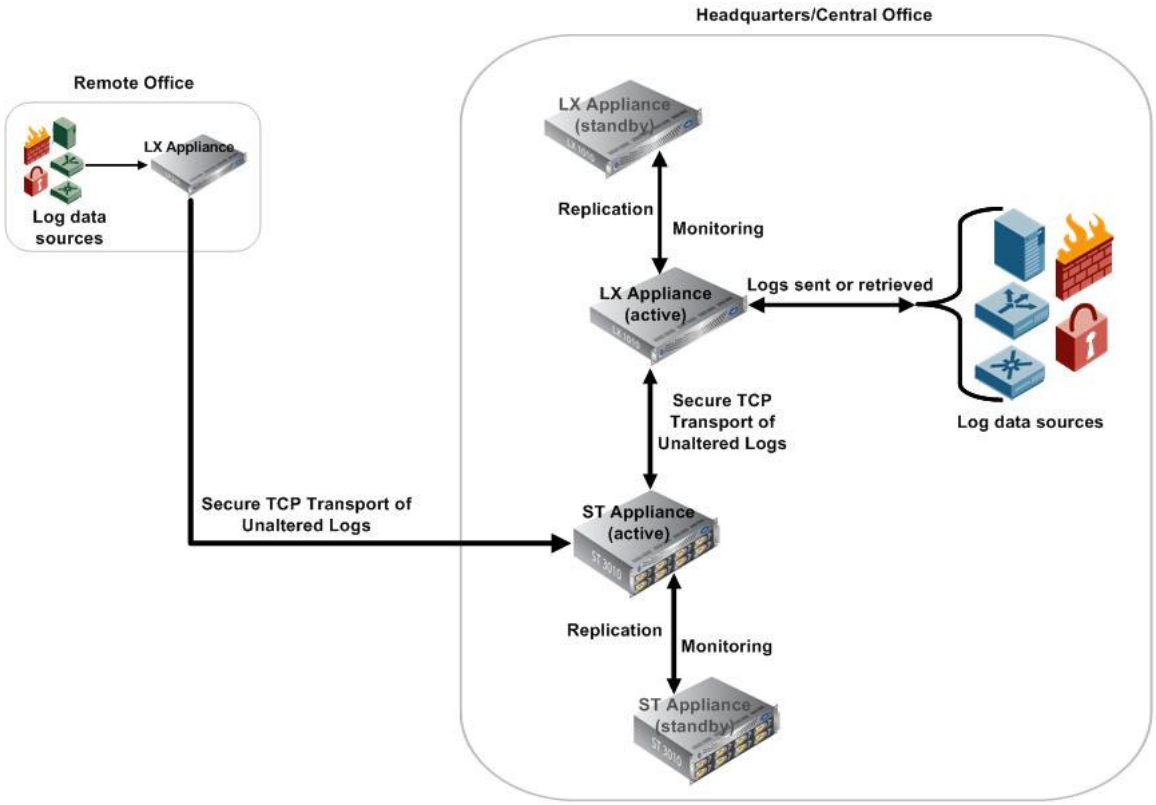

Figure 3: LX and ST appliances deployed in an optional failover configuration

1.7.1 Physical Boundaries

This section lists the specific hardware and software components of the product and denotes which are in the TOE and which are in the environment. Figure 4 shows a depiction of the TOE and its environment.

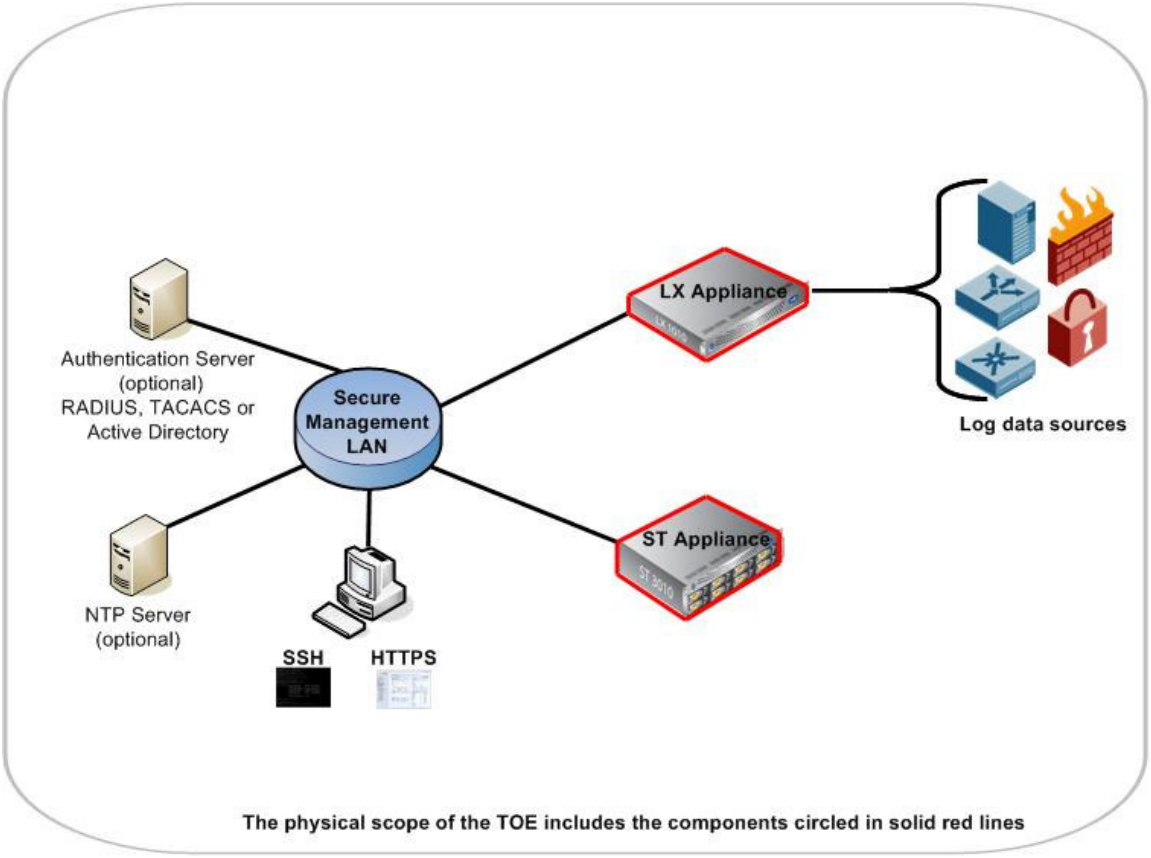

Figure 4: TOE Physical Boundaries

1.7.1.1 Hardware Components

Table 3 identifies the LogLogic v4.6.1 appliance models that comprise the TOE's hardware components and provides detailed specifications of the LX and ST models.

TOE Model	CPU	Memory	Hard Drive Capacity	Ethernet ports	Sustained message/sec
LX510	Single	512 MB	250 GB	1 x 10/100 (Eth0) 1 x 10/100/1000	500 MPS
LX1010	Single	1 GB	250 GB	1 x 10/100 (Eth0) 1 x 10/100/1000	1500 MPS
LX2010	Dual	4 GB	8*250 GB	1 x 10/100 (Eth0) 2 x 10/100/1000	4000 MPS
ST2010	Dual	2 GB	2*250 GB	1 x 10/100 (Eth0) 4 x 10/100/1000	75000 MPS
ST3010	Dual	2 GB	8*500 GB	1 x 10/100 (Eth0) 4 x 10/100/1000	75000 MPS

Table 3: LogLogic v4.6.1 Hardware

Each TOE hardware model is pre-installed with the software components identified in table 4 below.

TOE Software Component	Description
LogLogic v.4.6.1	The LogLogic software
Linux OS	A hardened Linux kernel Operating System
MySQL	A relational database management system
Tomcat	A Java HTTP web server environment for Java code to execute
Java SDK	A set of programming tools and data structures for Java code to execute

Table 4: LogLogic v4.6.1 Software components

1.7.2 Logical Boundaries

The TOE consists of a minimum of two network appliances (one LX and one ST appliance) each executing the software described in table 2. When configured to support HA, the TOE consists of a minimum of three network appliances such that at least one ST or LX is part of a HA pair.

The TOE captures event log data from a variety of network sources in the operating environment and analyzes them for anomalies. An anomaly is activity determined by the TOE as deviating or inconsistent from the norm. The TOE provides administrative alerts when an anomaly is detected. The Analyzer data is stored in a database and made available for viewing, searching, and reporting. Long-term storage of raw, unaltered logs is also provided.

The TOE includes security management capabilities through a web server interface and a CLI. The web server interface provides management functionality, and an implementation of SSLv.3/TLS protocol to support that functionality. The CLI provides a limited management interface available through a physical serial console connection. Access by serial port is restricted to authorized administrators allowed physical access. The CLI is also accessible through SSHv2. The TOE requires administrators to be successfully identified and authenticated before access to the web server interface or CLI is granted. The TOE includes an optional facility to interact with an external RADIUS, TACACS, or Active Directory identification and authentication server that is located in the operating environment. For Active Directory, only the roles provided by the TOE are permitted in the evaluated configuration.

The web server interface divides Administrator tasks from User tasks through a navigation menu. All management functions are allowed only if the user has the appropriate authorization. Administrators can also perform User functions on the Appliance as needed. Once a function is selected, the user or administrator is presented with a tab-based, hyperlinked web pages providing access control specific management functions.

The TOE maintains its own logical security domain for code execution and does not contain a general-purpose operating system or the ability to run user applications. Further, the TOE ensures external IT entities cannot directly affect secure operation of the TOE by providing network traffic filtering. The TOE provides secure transfer of event logs when transferred between LX and ST devices through a LogLogic proprietary encrypted tunnel.

To support generation of accurate timestamps in audit records and reports, the TOE provides NTP client and server functions for accurate sources of time and clock synchronization. Appliances within the TOE can synchronize with other TOE appliances, or alternatively, can interface to an external NTP server located in the operating environment. When the TOE provides NTP server functionality for synchronization among TOE appliances, LX Appliances must use an ST Appliance as the source NTP server.

1.7.3 Operational Environment

This section describes TOE dependencies on the environment in which the TOE is operated. The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only authorized administrators are to have access to connect to the serial console, or gain physical access to the hardware storing log data. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its install environment.

- The Operational Environment must include one or more log data device sources on one or more monitored networks including any peripheral devices and/or cabling.
- Log Sources in the Operational Environment that utilize Collector Agents for the TOE to be capable of capturing log data must be configured with the appropriate collector for that source.
- The Operational Environment must protect data transmitted from sources that use non-secure protocols.
- The Operational Environment must include Web browser (Microsoft Internet Explorer 6.0 or higher, or Mozilla Firefox 2.0 or higher) to be used by administrators of the TOE to communicate with the TOEs web GUI interface.
- The Operational Environment must include java virtual machine (JVM) v1.5 or higher (for Real-Time Viewer).
- The Operational Environment must include a SSHv2 client
- The Operational Environment must include a SSLv3 or TLS client

- Alerts notify the administrator of any unusual network traffic or Appliance system anomalies.
    - If the alert feature is configured to use Simple Network Management Protocol (SNMP) Trap actions to notify the administrator when an alert is generated, the TOE is dependent upon a network management station running an SNMP server in the TOE operational environment.
    - If the alert feature is configured to send e-mail messages when an alert is triggered, the TOE is dependent upon an SMTP server in the TOE operational environment. The SNMP server can be any entity capable of receiving SNMP traps V1 or V2c.
    - If the alert feature is configured to send SYSLOG messages when an alert is triggered, the TOE is dependent upon an SYSLOG server in the TOE operational environment.
- If the LogLogic v4.6.1 TOE is configured to use RADIUS, TACACS, or Active Directory authentication, the TOE is dependent upon a RADIUS or TACACS or Active Directory authentication server in the TOE operational environment.
- If the LogLogic v4.6.1 TOE is configured to use an external source to provide an accurate source of time and clock synchronization, the TOE is dependent upon a NTP server in the TOE operational environment.

A monitor and keyboard locally connected to the appliance must at a minimum be available for installation and initial configuration. For installation, identification and authentication to the TOE is required. The monitor and keyboard are optional once the installation and configuration is completed.

1.7.4 TSF Data

The TSF data consists of the following:

- Information flow policy rules
- Audit trail
- Analytical result data related to IDS_ANL.1.2
- Unaltered duplicate copies of the event log
- Configuration settings
- Alerts and alert rules
- Report templates
- Cryptographic keys

1.7.5 Security Attributes

- Information flow policy rules
- Source Device IP address
- Authentication key
- Transport layer port
- TCP, UDP protocol
- User account attributes as defined in FIA_ATD.1

1.7.6 User Data

- Event data in transit to the TOE

Once event logs from external sources have been stored within the TOE, that data is no longer considered user data.

1.7.7 Features Outside Evaluated Scope

This section identifies the features that the LogLogic v4.6.1 TOE provides which are **not** in the scope of current Common Criteria evaluation. These features are not required to meet any of the security claims for the TOE.

The following features interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

a) An SNMP agent running on the Appliance, responding to SNMP queries. (Note this is separate and distinct from the TOEs capability to send SNMP trap alerts.)

b) The LogLogic Web Services API. The LogLogic Web Services API allows for the development of 3rd party programs for use as an alternative tool to interface and manage a LogLogic Appliance.

c) Updating Appliance Software feature. (Updating the appliance software would remove the TOE from the evaluated configuration.)

d) Using NAS, SAN, and/or WORM storage connectivity and optional raw log data encryption with a LogLogic ST Appliance.

e) The LogLogic LG 400 and MX models are not part of the TOE. Those model offer only a subset of the evaluated security functionality.

f) Use of the restore function in non-HA failover pair. (Backup and restore functionality are allowed only if they're used as part of an HA failover pair using SCP.)

g) Use of Parsed data alerts. Parsed data alerts meets certain conditions specified using an exact phrase based on a Pre-defined Search Filter.

1.7.8 Guidance Documentation

The TOE includes the following administrative guidance:

- *LogLogic Administration Guide, Release 4.6, September 2008*
- *LogLogic Users Guide, Release 4.6, September 2008*
- *LogLogic Quick Start Guide, Release 4.5, June 2008*
- *Supplemental Installation and Administrative Guidance for the Common Criteria Evaluated Configuration, version 1.0, June 30, 2009*

1.7.9 LogLogic Collectors

The evaluated configuration allows use of LogLogic developed collectors. A collector is installed on specific log sources to enable the TOE to capture log data from those sources. A LogLogic developed collector is required for the following log sources:

- IBM i5/OS
- IBM z/OS (OS/390)
- ISS Site Protector
- Novell eDirectory

- Symantec AntiVirus
- HP NonStop

2 Conformance Claims

2.1 CC Conformance Claims

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation Part 1 – September 2006 Version 3.1, Revision 1 and CC for Information Technology Security Evaluation Parts 2 & 3 – September 2007 Version 3.1 Revision 2.

The ST is:

CC Version 3.1 Part 2 extended.

CC Version 3.1 Part 3 conformant.

2.2 PP and Package Claims

This ST is Evaluation Assurance Level 2 augmented with ALC_FLR.2.

The ST is conformant with the U.S. Government Protection Profile: Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, 25 July 2007. [IDSAPP]

2.3 Conformance Rationale

This section provides rationale for *demonstrable* conformance on why the ST is considered to be "equivalent or more restrictive" than the [IDSAPP] The rationale below demonstrates the ST levies more restrictions on the TOE and less restrictions on the operational environment.

Security problem definition: Equivalent. Assumptions, threats, and OSPs as defined in the PP are unmodified in the ST.

Security objectives: More restrictive. O.EXPORT exists in the PP but not in the ST as the TOE does not make analyzer data available to other IDS components. In addition, OE.AUDIT_SORT and OE.AUDIT_PROTECTION are objectives met by the TOE and not the operating environment. Therefore it levies less restriction on the operational environment.

SFRs: More Restrictive. FPT_ITA.1, FPT_ITC.1, FPT_ITI.1 and FIA_AFL.1 from [IDSAPP] are removed in the ST as the TOE does export data to other trusted IT entities, per PD-0127. FIA_UAU.1 and FIA_UID.1 were modified to include an option for user authentication by an external authentication server.

SARs: Equivalent. The Security Assurance Requirements for EAL2 are drawn from [IDSAPP] and are unmodified.

3 Security Problem Definition

The TOE described in this PP is intended to operate in environments having a basic level of robustness. Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimal. Authorized users of the TOE are cleared for all information managed by the IDS component, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low.

Entities in the Operating environment on which the TOE depends for security functions must be of at least the same level of robustness as the TOE. It is necessary for such an environment that the underlying operating system on which the IDS component is installed be evaluated against a basic robustness protection profile for operating systems.

The TOE in and of itself is not of sufficient robustness to store and protect information of such criticality that the integrity or secrecy is critical to the survival of the enterprise.

3.1 Assumptions

The assumptions are ordered into three categories: personnel assumptions, physical environment assumptions, and operational assumptions.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.

A. REM_OPER The authorized administrators will only be able to remotely access the TOE using secure protocols, strong authentication, and from trusted platforms.

3.1.2 Physical Environment Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.DIRECT Only authorized administrators within the physically secure boundary protecting the TOE have access to the TOE from direct (not logically controlled) connection (for example, serial console or an associated switch console port).

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST	The TOE can only be accessed by authorized users.
A.INTEGR	The authorized administrator will ensure that measures are taken in the Operating environment to protect event logs in transit.

3.2 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.

3.2.1 TOE Threats

T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOE's analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.UNATHDVCE	An unauthorized device may attempt to interact with the TOE causing an influx of data that the TOE cannot handle.
T.DATACOMP	A user or process may cause through an unsophisticated data-targeting attack or error, TSF data to be inappropriately accessed (viewed, modified, or deleted). This includes TSF data transmitted between the TOE.
T.INSECUSE	An authorized user or administrator may use or administer the TOE in an insecure manner that allows disclosure of, corruption to, or disruption of access to sensitive log data.

T.INTEGR An unauthorized user may attempt to modify event log data in transit from IT devices in the Operating Environment to the TOE.

3.2.2 Analytical Threats

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the IDSAPP.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

4 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.

4.1 Information Technology (IT) Security Objectives

The following are the TOE security objectives:

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDACTS	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.EVENTS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and Analyzer data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the Analyzer functions.
O.INTEGR	The TOE must ensure the integrity of all audit and Analyzer data.
O.SECRMT	The TOE must ensure secure communication in support of remote administration.
O.TMSTMP	The TOE will provide a time stamp for its own use.
O.TRAFFIC	The TOE must filter the flow of all network traffic from IT entities attempting to interact with the TOE.
O.LOGCON	When the TOE transfers event log data to another TOE component, it will ensure the confidentiality and integrity of the data.

4.2 Security Objectives for the Operating Environment

This section defines the non-IT security objectives for the environment and the IT security objectives for the environment.

4.2.1 Non-IT Security Objectives For The Operating Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures and will not require the implementation of functions in the TOE hardware and/or software.

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.

OE.INTROP The TOE is interoperable with the IT System it monitors and other IDS components within its IDS.

OE.INTEGR The authorized administrator for the TOE must ensure that appropriate measures have been taken in the TOE operating environment to protect event log data in transit to the TOE from modification or disclosure by use of physical isolation or cryptographic means.

4.2.2 IT Security Objectives For The Operating Environment

The following IT security objectives for the environment are to be addressed by the operating environment by technical means.

OE.I&A If the TOE is configured to use external authentication, the TOE operating environment shall provide the ability to uniquely identify and authenticate users.

OE.TMSTMP If the TOE is configured to use an external time source, the TOE operating environment shall be able to generate reliable timestamps for the TOE's use.

4.3 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement. Table 3 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

	O.PROTCT	O.IDACTS	O.EVENTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECRMT	O.TMSTMP	O.TRAFFIC	O.LOGCON	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.INTEGR	OE.I&A	OE.TMSTMP
A.ACCESS																			**X**			
A.PROTCT																**X**						
A.LOCATE																**X**						
A.MANAGE																		**X**				

	O.PROTCT	O.IDACTS	O.EVENTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECRMT	O.TMSTMP	O.TRAFFIC	O.LOGCON	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.INTEGR	OE.I&A	OE.TMSTMP
A.NOEVIL															X	X	X					
A.NOTRUST																X	X					
A.INTEGR																				X		
T.COMINT	X					X	X			X											X	
T.COMDIS	X					X	X														X	
T.LOSSOF	X					X	X			X											X	
T.NOHALT		X				X	X														X	
T.UNITSYS			X																			
T.PRIVIL	X					X	X														X	
T.IMPCON					X	X	X								X						X	
T.INFLUX								X														
T.FALACT				X																		
T.FALREC				X																		
T.FALASC				X																		
T.INTEGR																				X		
T.INSECUSE											X				X			X				
T.DATACOMP											X	X		X	X							
T.UNATHDVCE													X									
P.ANALYZ		X																		X		
P.DETECT				X					X			X										X
P.MANAGE	X				X	X	X								X		X	X				
P.ACCESS	X						X	X														
P.ACCACT							X		X			X										X
P.INTEGR										X												
P.PROTCT					X											X						

Table 5: Tracings between Threats and Security Objectives

A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.

The OE.INTROP objective ensures the TOE has the needed access.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.

The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.INTEGR The authorized administrator will ensure that measures are taken in the Operating environment to protect event logs in transit.

The OE.INTEGR environment objective counters this threat by requiring an authorized administrator to ensure that appropriate measures have been taken in the operating environment to protect event log data from modification while in transit to the TOE.

T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.I&A objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.COMDIS An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and

OE.I&A objectives by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.

The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.I&A objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.I&A objectives by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.

T.UNITSYS Unauthorized attempts to access IT systems may go undetected which causes modification of the IT System protected data or undermines the IT System security functions.

The O.EVENTS objective counters this threat by requiring the TOE collect and store event logs that might be indicative of inappropriate activity.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.I&A objectives by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH and OE.I&A objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.I&A objectives by only permitting authorized users to access TOE functions.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.INTEGR An unauthorized user may attempt to modify event log data in transit from IT devices in the Operating Environment to the TOE.

The OE.INTEGR environment objective counters this threat by requiring an authorized administrator to ensure that appropriate measures have been taken in the operating environment to protect event log data from modification while in transit to the TOE.

T.INSECUSE An authorized user or administrator may use or administer the TOE in an insecure manner that allows disclosure of, corruption to, or disruption of access to sensitive log data.

The O.SECRMT objective counters this threat by ensuring that administrators use secure communication when performing remote administration of the TOE that will not be disclosed or modified.
The OE.PERSON objective mitigates this threat by ensuring that users are made aware of their responsibilities for using the TOE's functions in a secure manner.
The OE.INSTAL objective mandates that the TOE be installed in a secure manner.

T.DATACOMP A user or process may cause through an unsophisticated data-targeting attack or error, TSF data to be inappropriately accessed (viewed, modified, or deleted). This includes TSF data transmitted between the TOE.

The O.LOGCON objective counters this threat by ensuring when the TOE forwards event log data to another TOE component, data will not be disclosed or modified.
The O.SECRMT objective counters this threat by ensuring that administrators use secure communication when performing remote administration of the TOE that will not be disclosed or modified.
The O.TMSTMP and OE.TSMTMP objectives help mitigate this threat by assisting time-based analysis of activities associated with data access.
The OE.INSTAL objective mandates that the TOE be installed in a secure manner.

T.UNATHDVCE An unauthorized device may attempt to interact with the TOE causing an influx of data that the TOE cannot handle.

The O.TRAFFIC objective counters this threat by filtering the flow of TCP/IP network traffic from IT entities attempting to interact with the TOE.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.

The O.AUDITS and O.IDACTS objectives address this policy by requiring collection of audit and Scanner data.

P.MANAGE The TOE shall only be managed by authorized users.

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection.

P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The O.TMSTMP and OE.TMSTMP objectives will provided a time stamp for each audit.

P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

The O.OFLOWS objective requires the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST. The extended components defined in this section are members of existing CC Part 2 families and are based on the existing CC Part 2 SFRs.

5.1.1 FIA Identification and Authentication

The FIA class is extended to include 2 additional components.

The FIA class addresses the requirements to verify a claimed user identity. The extended components defined in this section require the TOE to ensure that either the Operating environment or the TOE verifies claimed user identities.

5.1.1.1 FIA_UAU_TRD.1 Timing of authentication with a third party

FIA_UAU_TRD.1 is an extension to the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be performed by the TOE or Operating environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_TRD.1

The following actions could be considered for the management functions in FMT:

- If authentication is by the TOE, management of the authentication data by an administrator
- If authentication is by the TOE, management of the authentication data by the associated user
- Managing the list of actions that can be taken before the user is authenticated.

Audit: FIA_UAU_TRD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism;
- Basic: All use of the authentication mechanism;
- Detailed: All TSF mediated actions performed before authentication of the user.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or
FIA_UID_TRD.1 Time of identification with a third party.

FIA_UAU_TRD.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*].

FIA_UAU_TRD.1.2 The TSF shall require each user to be successfully authenticated by [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.2 FIA_UID_TRD.1 Timing of identification with a third party

FIA_UID_TRD.1 is an extension to the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be performed by the TOE

or Operating environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_TRD.1

The following actions could be considered for the management functions in FMT:

- If identification is by the TOE, management of the user identities;
- If an authorized administrator can change the actions allowed before identification, the managing of the action lists.

Audit: FIA_UID_TRD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;
- Basic: All use of the user identification mechanism, including the user identity provided.

Hierarchical to: No other components.

Dependencies: None

FIA_UID_TRD.1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is identified by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*].

FIA_UID_TRD.1.2 The TSF shall require each user to be successfully identified by the [selection: *Operating environment, TOE or the Operating environment as configured by the administrator*] before allowing any other TSF-mediated actions on behalf of that user.

5.1.2 IDS IDS Component Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions. The IDS family includes these classes, components, and elements below:

5.1.2.1 IDS_ANL.1 - Analyzer analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) [selection: statistical, signature, integrity]; and

b) [assignment: other analytical functions].

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: other security relevant information about the result].

5.1.2.2 IDS_RCT.1 - Analyzer react

IDS_RCT.1.1 The TSF shall send an alarm to [assignment: alarm destination] and take [assignment: appropriate actions] when an intrusion is detected.

5.1.2.3 IDS_RDR.1 - Restricted data review

IDS_RDR.1.1 The Analyzer shall provide [assignment: authorized users] with the capability to read [assignment: list of Analyzer data] from the Analyzer data.

IDS_RDR.1.2 The Analyzer shall provide the Analyzer data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The Analyzer shall prohibit all users read access to the Analyzer data, except those users that have been granted explicit read-access.

5.1.2.4 IDS_STG.1 - Guarantee of analyzer data availability

IDS_STG.1.1 The Analyzer shall protect the stored Analyzer data from unauthorized deletion.

IDS_STG.1.2 The Analyzer shall protect the stored Analyzer data from modification.

IDS_STG.1.3 The Analyzer shall ensure that [assignment: metric for saving Analyzer data] Analyzer data will be maintained when the following conditions occur: [selection: Analyzer data storage exhaustion, failure, attack].

5.1.2.5 IDS_STG.2 - Prevention of Analyzer data loss

IDS_STG.2.1 The Analyzer shall [selection: 'ignore Analyzer data', 'prevent Analyzer data, except those taken by the authorized user with special rights', 'overwrite the oldest stored Analyzer data '] and send an alarm if the storage capacity has been reached.

6 Security Requirements

This section defines the security requirements for the TOE and the operational environment (that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends).

The CC divides security requirements into two categories:

- Security functional requirements (SFRs), that is, requirements for security functions such as information flow control, audit, I&A.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

The security requirements that are levied on the TOE are specified in this section of the ST.

6.1 Security Functional Requirements

This section defines the TOE SFRs that are directly taken from the CC Version 3.1 or from the extended components defined in Section 5. The TOE shall satisfy the SFRs stated in the table below which lists the names of the SFR components. Following the table, the individual functional requirements are restated with any necessary operations completed.

Functional Component	Functional Component Name	PP Conformance[1]
FAU_GEN.1 (1)	Audit Data Generation	Drawn directly
FAU_GEN.1 (2)	Audit Data Generation	Added
FAU_SAR.1	Audit Data Review	Drawn directly
FAU_SAR.2	Restricted audit review	Drawn directly
FAU_SAR.3	Selectable Audit Data Review	Drawn directly
FAU_SEL.1	Selective audit	Drawn directly
FAU_STG.2	Guarantees of audit data availability	Drawn directly
FAU_STG.4	Prevention of audit data loss	Drawn directly
FCS_CKM.1 (1)	Cryptographic Key Generation	Added
FCS_CKM.1 (2)	Cryptographic Key Generation	Added
FCS_CKM.1 (3)	Cryptographic Key Generation	Added
FCS_CKM.2	Cryptographic Key Distribution	Added
FCS_CKM.4	Cryptographic Key Destruction	Added
FCS_COP.1 (1)	Cryptographic Operation	Added
FCS_COP.1 (2)	Cryptographic Operation	Added
FCS_COP.1 (3)	Cryptographic Operation	Added
FCS_COP.1 (4)	Cryptographic Operation	Added

[1] This column indicates whether the SFR was drawn directly from the PP, modified from the PP, or added beyond what's defined in the PP.

FCS_COP.1 (5)	Cryptographic Operation	Added
FCS_COP.1 (6)	Cryptographic Operation	Added
FDP_IFC.1 (1)	Subset information flow control	Added
FDP_IFF.1 (1)	Simple security attributes	Added
FDP_IFC.1 (2)	Subset information flow control	Added
FDP_IFF.1 (2)	Simple security attributes	Added
FDP_IFC.1 (3)	Subset information flow control	Added
FDP_IFF.1 (3)	Simple security attributes	Added
FDP_IFC.1 (4)	Subset information flow control	Added
FDP_IFF.1 (4)	Simple security attributes	Added
FDP_IFC.1 (5)	Subset information flow control	Added
FDP_IFF.1 (5)	Simple security attributes	Added
FIA_AFL.1	Authentication failure handling	Added
FIA_ATD.1	User Attribute Definition	Drawn directly
FIA_UID_TRD.1	Third-party Identification Sequence	Modified
FIA_UAU_TRD.1	Third-party Authentication Sequence	Modified
FMT_MOF.1 (1)	Management of the TOE	Modified
FMT_MOF.1 (2)	Management of the TOE	Added
FMT_MSA.1	Management of security attributes	Added
FMT_MSA.3	Static attribute initialization	Added
FMT_MTD.1	Management of TSF data	Drawn directly
FMT_SMF.1	Specification of Management Functions	Added
FMT_SMR.1	Specification of Roles	Modified
FPT_ITT.1	Internal Data Transfer Protection	Added
FPT_FLS.1	Failure with preservation of secure state	Added
FPT_STM.1	Reliable Time stamps	Drawn directly
FTP_ITC.1 (1)	Inter-TSF trusted channel	Added
FRU_FLT.1	Degraded fault tolerance	Added
IDS_ANL.1	Analyzer Analysis	Drawn directly
IDS_RCT.1	Analyzer React	Drawn directly
IDS_RDR.1	Restricted Data Review	Drawn directly
IDS_STG.1	Guarantee of Analyzer Data Availability	Drawn directly
IDS_STG.2	Prevention of Analyzer data loss	Drawn directly

Table 6: Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 (1) Audit Data Generation

FAU_GEN.1.1 (1) The TSF shall be able to generate an audit record of the following auditable events**:**

a) Start-up and shutdown of the audit functions

b) All auditable events for the *basic* level of audit;

c) [Access to the Analyzer and access to the TOE and Analyzer data].

Application Note: The auditable events for the basic level of auditing are included in Table 5 Auditable Events.

FAU_GEN.1.2 (1) The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in the Details column of Table 5 – Auditable Events.

Functional Component	Auditable Events	Details
FAU_GEN.1	Start- up and shutdown of audit functions	
FAU_GEN.1	Access to TOE	
FAU_GEN.1	Access to the TOE Analyzer data	**Object ID, Requested access**
FAU_SAR.1	Reading of audit records and report generation.	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	
FIA_UAU_TRD.1	All use of the authentication mechanism	**User identity, location**
FIA_UID_TRD.1	All use of the identification mechanism	**User identity, location**
FMT_MOF.1 (1)	All modifications in the behavior of the functions of the TSF	
FMT_MOF.1 (2)	All modifications in the behavior of the functions of the TSF	

Functional Component	Auditable Events	Details
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**

Table 7: Auditable Events – FAU_GEN.1 (1)

6.1.1.2 FAU_GEN.1 (2) Audit Data Generation

FAU_GEN.1.1 (2) The TSF shall be able to generate an audit record of the following auditable events**:**

a) Start-up and shutdown of the audit functions

b) All auditable events for the *not specified* level of audit;

c) [The Auditable Events column in table 8].

FAU_GEN.1.2 (2) The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in the Details column of Table 8.

Functional Component	Auditable Events	Details
FMT_MSA.1	Modifications of the values of security attributes	
FMT_MSA.3	Modifications of the default setting of restrictive rules. All modifications of the initial values of security attributes.	
FMT_MTD.1	All modifications to the values of TSF data	
FCS_COP.1	Success of operation	
FCS_CKM.1 (1) – (4)	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM.2	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	

Functional Component	Auditable Events	Details
FCS_CKM.4	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_COP.1 (1) – (7)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FDP_IFF.1 (1) - (5)	All decisions on requests for information flow.	The presumed address of the source subject
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts.	The identity of the administrator making the authentication attempts.

Table 8: Auditable Events – FAU_GEN.1 (2)

6.1.1.3 FAU_SAR.1 Audit Data Review

FAU_SAR.1.1 The TSF shall provide [authorized Administrators, Configuration Administrators, User Administrators, Report Administrators] with the capability to read [all audit data] from the audit records.

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

6.1.1.4 FAU_SAR.2 Restricted Audit Review

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

6.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform [sorting] of audit data based on [date and time, subject identity, type of event, and success or failure of related event].

6.1.1.6 FAU_SEL.1 Selective Audit

FAU_SEL1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *event type*;

b) [no additional attributes].

6.1.1.7 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to *detect* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [90 percent] stored audit records will be

maintained when the following conditions occur: *audit storage exhaustion*

6.1.1.8 FAU_STG. 4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [send an alarm] if the audit trail is full.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1(1) Cryptographic Key Generation (SSH)

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [RSA Encryption Standard (PKCS#1)]

Application Note: This SFR supports FTP_ITC.1 (1).

6.1.2.2 FCS_CKM.1(2) Cryptographic Key Generation (HTTPS/SSL/TLS)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [PKCS #1 RSA Cryptography Standard].

Application Note: This SFR supports FTP_ITC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (2).

6.1.2.3 FCS_CKM.1(3) Cryptographic Key Generation (Blowfish)

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Blowfish] and specified cryptographic key sizes [256 bits] that meet the following: [none].

Application Note: This SFR supports FDP_IFC.1 (1), FDP_IFF.1 (1), and FPT_ITT.1.

6.1.2.4 FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [diffie-hellman-group1-sha1] that meets the following: [RFC 4253]

Application Note: This SFR supports FTP_ITC.1 (1).

6.1.2.5 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite method] that meets the following: [no standard].

Application Note: No formal key destruction method is followed for SSHv2 and SSLv3 or TLS. Keys are overwritten as new keys are loaded. This SFR supports FTP_ITC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (2), FDP_IFC.1 (1), FDP_IFF.1 (1) and FPT_ITT.1.

6.1.2.6 FCS_COP.1(1) Cryptographic Operation (SSH Confidentiality)

FCS_COP.1.1(1) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES, TDES, and blowfish] and cryptographic key sizes [168 bits (TDES), 128 bits (Blowfish), 128 bits, 192 bits, 256 bits (AES)] that meet the following: [FIPS 46-3 (TDES), FIPS 197(AES), RFC 2451 (Blowfish)].

Application Note: This SFR supports FTP_ITC.1 (1).

6.1.2.7 FCS_COP.1(2) Cryptographic Operation (SSH Integrity)

FCS_COP.1.1(2) The TSF shall perform [secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [HMAC-SHA1 and HMAC-MD5] and cryptographic key sizes [160 bits (HMAC-SHA1), and 128 bits (HMAC-MD5)] that meet the following: [FIPS 198 and RFC 2104 HMAC-SHA1, RFC 1321 (HMAC-MD5)].

Application Note: This SFR supports FTP_ITC.1 (1).

6.1.2.8 FCS_ COP.1(3) Cryptographic Operation (HTTPS/SSL/TLS)

FCS_COP.1.1(3) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bits] that meet the following: [FIPS PUB 197 - Advanced Encryption Standard].

Application Note: This SFR supports FTP_ITC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (2).

6.1.2.9 FCS_ COP.1(4) Cryptographic Operation (Blowfish)

FCS_COP.1.1(4) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [Blowfish] and cryptographic key sizes [256 bits] that meet the following: [None].

Application Note: The TOE implements Blowfish encryption when transferring logs between TOE components. Blowfish encryption is also used to encrypt passwords when users are authenticated by an external authentication server. This SFR supports FDP_IFC.1 (1) and FDP_IFF.1 (1).

6.1.2.10 FCS_ COP.1(5) Cryptographic Operation (SHA-1)

FCS_COP.1.1(5) The TSF shall perform [shared secret password hashing] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [160 bits] that meet the following: [FIPS PUB 180-1- Secure Hash Standard]

Application Note: The TOE performs SHA-1 hashing of a shared secret between each TOE component. Before logs are transferred, each TOE component must authenticate one another via an authentication string.

6.1.2.11 FCS_ COP.1(6) Cryptographic Operation (MD5)

FCS_COP.1.1(6) The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [128 bits] that meet the following: [RFC 1321]

Application Note: The TOE calculates a MD5 hash for each event log file it collects and stores the hash value in the database separately from the log itself. It will check for that MD5 hash value in the database and if it already exists then it is considered to be a duplicate and does not replace the file.

Application Note: The TOE hashes users password using MD5 before sending to a Radius or TACACS+ external authentication server

6.1.3 User Data Protection (FDP)

6.1.3.1 FDP_IFC. (1) Subset Information Flow Control –log transfer (LL Secure Tunnel)

FDP_IFC.1.1 (1) The TSF shall enforce the [log transfer SFP] on [

Subjects: Another instance of the TOE (LX or ST device)

Information: unaltered logs

Operation: accept information flow, deny information flow]

6.1.3.2 FDP_IFF.1(1) Simple Security Attributes- log transfer (LL Secure Tunnel)

FDP_IFF.1.1 (1) The TSF shall enforce the [log transfer SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Source Device IP address, authentication key

Information Security Attributes: destination IP address, TCP protocol, destination port]

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:[

- destination ip matches localhost
- destination port equals 11965
- protocol equals LogLogic TCP protocol
- source ip matches ip of a valid source device in the enabled message routing rule
- authenticated key of source is valid]

FDP_IFF.1.3 (1) The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 (1) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 (1) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.3 FDP_IFC.1 (2) Subset Information Flow Control – event log encrypted (SFTP, SCP, HTTPS, FTPS, Checkpoint log sources)

FDP_IFC.1.1(2) The TSF shall enforce the [event log encrypted SFP] on [

Subjects: IT Device

Information: event logs

Operation: receive information]

6.1.3.4 FDP_IFF.1(2) Simple Security Attributes - event log encrypted (SFTP, SCP, HTTPS, FTPS, Checkpoint log sources)

FDP_IFF.1.1 (2) The TSF shall enforce the [event log encrypted SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Source device IP address, protocol

Information Security Attributes: source IP address, TCP protocol, destination port, MD5/SHA-1 integrity hash]

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a ~~controlled~~ **source** subject and **a destination subject** ~~controlled information~~ via a controlled operation if the following rules hold: [

- destination ip matches localhost
- protocol matches that of a valid protocol as defined in the rule (SFTP, SCP, HTTPS, FTPS, Checkpoint LEA/CPMI)
- source ip matches that of a valid source device as enabled in the rule
- integrity enforced by the encryption protocol]

FDP_IFF.1.3 (2) The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 (2) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 (2) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.5 FDP_IFC.1 (3) Subset Information Flow Control –event log outbound initiated (HTTP, FTP, CIFS, MSSQL)

FDP_IFC.1.1 (3) The TSF shall enforce the [event log outbound initiated SFP] on [

Subjects: IT Device

Information: network packets containing event logs

Operation: receive information

6.1.3.6 FDP_IFF.1(3) Simple Security Attributes- event log outbound initiated (HTTP, FTP, CIFS, MS SQL)

FDP_IFF.1.1 (3) The TSF shall enforce the [event log outbound initiated SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Source device IP address, protocol

Information Security Attributes: source IP address, TCP protocol, destination port]

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a ~~controlled~~ **source** subject and **a destination subject** ~~controlled information~~ via a controlled operation if the following rules hold: [

- destination ip matches localhost
- protocol matches that of a valid protocol as defined in the rule (HTTP, FTP, CIFS, MSSQL)
- source ip matches that of a valid source device as enabled in the rule]

FDP_IFF.1.3 (3) The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 (3) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 (3) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.7 FDP_IFC.1 (4) Subset Information Flow Control – event log inbound initiated (SYSLOG)

FDP_IFC.1.1(4) The TSF shall enforce the [event log inbound initiated SFP] on [

Subjects: IT Device

Information: network packets containing event logs

Operation: receive information]

6.1.3.8 FDP_IFF.1(4) Simple Security Attributes- event log inbound initiated (SYSLOG)

FDP_IFF.1.1 (4) The TSF shall enforce the [event log inbound initiated SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Source device IP address

Information Security Attributes: destination port, protocol]

FDP_IFF.1.2 (4) The TSF shall permit an information flow between a ~~controlled~~ **source** subject and **a destination subject** ~~controlled information~~ via a controlled operation if the following rules hold: [

- destination ip matches localhost
- destination port = 514
- protocol= UDP, TCP protocol
- source ip matches ip of a valid source device as enabled in the rule]

FDP_IFF.1.3 (4) The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 (4) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 (4) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.9 FDP_IFC.1(5) Subset Information Flow Control – network traffic control

FDP_IFC.1.1 (5) The TSF shall enforce the [network traffic control SFP] on [

Subjects: Any IT device

Information: TCP/IP network traffic

Operation: accept information flow, deny information flow]

6.1.3.10 FDP_IFF.1(5) Simple Security Attributes- network traffic control

FDP_IFF.1.1 (5) The TSF shall enforce the [network traffic control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Source device IP address

Information Security Attributes: source IP address, TCP protocol, UDP protocol, destination port]

FDP_IFF.1.2 (5) The TSF shall permit an information flow between a ~~controlled~~ **source** subject and **a destination subject** ~~controlled information~~ via a controlled operation if the following rules hold: [

- source ip matches that ip of a valid source device as enabled in the rule
- protocol equals UDP, or TCP protocol
- destination ip matches localhost
- destination port equals one of the following:
  - Http Collector: 4433 (TCP)
  - HTTP: 80 (TCP)
  - HTTPS: 443 (TCP)
  - Inbound LX Traffic: 5514 (ST Appliances only, TCP)
  - Loglogic Tunnel: 11965 (TCP)
  - NTP: 123 (UDP)
  - RealTime Viewer: 4514 (TCP)
  - SSH: 22 (TCP)
  - SSL: 4443 (TCP)
  - SNMP: 161 (UDP)
  - SNMP-Trap: 162 (UDP)
  - SYSLOG: 514 (UDP)]

FDP_IFF.1.3 (5) The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 (5) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5 (5) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer*

within [the range 0 – 25][2] unsuccessful authentication attempts occur related to [authentication attempts by an administrator to an LX or ST appliance].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [lock the account for a time duration of 1-9999 minutes as specified by the administrator].

Application Note: Authentication Failure Handling applies only to Web user roles. The single CLI role cannot be locked out.

6.1.4.2 FIA_ATD.1 User Attribute Definition

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

a) User identity;

b) Authentication data;

c) Authorizations; and

d) [no other security attributes]

6.1.4.3 FIA_UID_TRD.1 Timing of Identification with a third party

FIA_UID_TRD.1.1 The TSF shall allow [the presentation of the TOE login screen and the presentation of the CLI login prompt] on behalf of the user to be performed before the user is identified by the *TOE or the Operating environment as configured by the administrator*.

FIA_UID_TRD.1.2 The TSF shall require each user to be successfully identified by the *TOE or the Operating environment as configured by the administrator* before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.4 FIA_UAU_TRD.1 Timing of Authentication with a third party

FIA_UAU_TRD.1.1 The TSF shall allow the presentation of the TOE login screen and the presentation of the CLI login prompt on behalf of the user to be performed before the user is authenticated by the *TOE or the Operating environment as configured by the administrator.*

FIA_UAU_TRD.1.2 The TSF shall require each user to be successfully authenticated by *TOE or the Operating environment as configured by the administrator* before allowing any other TSF-mediated actions on behalf of that user.

Application Note: "As configured by the administrator" refers to the authorized administrator configuring the TOE to authenticate users using the authentication parameters stored locally within the TOE or to defer authentication to a remote authentication server in the operational environment (RADIUS, TACACS, or Active Directory).

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MOF.1 (1) Management of security functions behavior - IDS

FMT_MOF.1.1 (1) The TSF shall restrict the ability to *modify the behavior of* the functions **of analysis and reaction** to ~~authorized Analyzer administrators~~

[2] A value of 0 means that the TSF will never disable the administrator account due to failed login attempts.

Configuration Administrators.

6.1.5.2 FMT_MOF.1 (2) Management of security functions behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to determine the behavior of, disable, enable, modify the behavior of the functions [as defined in table 9]

	Administrator	Configuration Administrator	User Administrator	Report Administrator	Console Administrator
Manage Devices	X	X			
Backup/Restore	X	X			
Access Control	X	X			
Port Configuration	X	X			
Message Routing Configuration	X	X			
Access Management Station	X	X			
Manage Alerts	X	X			
Manage File Transfer Rules	X	X			
Manage Check Point Devices	X	X			
Manage PIX/ASA Msg Codes	X	X			
Manage Packages	X	X			
System Configuration	X	X			
Manage SSL Certificate	X	X			
Manage Users	X		X		
Manage Administrators	X				
Summary Reports	X			X	
Real-Time Reports	X			X	
Custom Reports	X			X	
Search Archived Data	X			X	
Replay	X			X	
Real-Time Viewer	X			X	

	Administrator	Configuration Administrator	User Administrator	Report Administrator	Console Administrator
Manage Network Interfaces					**X**
Manage RAID Configuration					**X**
Manage System Configuration Settings					**X**
Display Appliance and System Interface Status					**X**
Perform a Data Migration					**X**

Table 9: FMT_MOF role to function restriction

6.1.5.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1 The TSF shall enforce the [log transfer, event log encrypted, event log outbound initiated, event log inbound initiated, and network traffic control SFP(s)] to restrict the ability to *change_default, query, modify, delete* the security attributes [source IP address, destination IP address, TCP protocol, UDP protocol, destination port] to [Administrator, Configuration Administrator].

6.1.5.4 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [log transfer, event log encrypted, event log outbound initiated, event log inbound initiated, and network traffic control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

6.1.5.5 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *query* **and add Analyzer and audit data, and shall restrict the ability to query and modify all other TOE data** to [Administrator, Configuration Administrator, User Administrator, Report Administrator].

6.1.5.6 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [as defined in table 10]

Function	Description
Manage Devices	Add, modify, and remove devices and

	device groups.
Backup/Restore Database	Define the backup configuration for the Appliance.
Manage Access Control	Define access rules for TCP or UDP packets accessing the Appliance.
Port Configuration	Add, modify, and remove the port definitions on the Appliance
Message Routing Configuration	Manage the Appliance message routing configuration. Users can add, modify, and remove upstream devices and routing filters as well as generating/regenerating the Authentication String.
Access Management Station	Manage remote Appliances. If enabled, the privileges defined for the user apply to all remote Appliances in the Management Station relationship.
Manage Alerts	Add, modify, and remove alerts.
Manage File Transfer Rules	Add, modify, and remove file transfer rules for devices.
Manage Check Point Devices	Add, modify, and remove Check Point devices.
Import/Export	Import and export configuration components in bulk such as alerts, reports, search filters, and packages.
Manage PIX/ASA Msg Codes	Manage the categorization of incoming messages based on the PIX/ASA severity and message.
Manage Packages	Add, modify, remove packages on the Appliance to allow an administrator to import and export all the components together between Appliances in a single package and access all package components from a single location in the user interface.
System Configuration	Manage system settings for the Appliance. Users have full access to

	configure general settings, remote servers, data retention values, Appliance network settings, and time settings.
Manage SSL Certificate	Manage LogLogic signed certificates, import certificates, and import private keys.
Manage Users	Create, modify, and remove Configuration, User, and Report Administrators on the Appliance.
Manage Administrators	Create, modify, remove Administrators
Custom Reports	Create, modify, remove, and run custom reports.
Summary Reports	Create, modify, remove, and run Summary reports.
Real-Time Reports	Create, modify, remove, and run Real-Time reports.
Search Archived Data	Search log data captured by the Appliance.
Replay	Replay archived data from an ST Appliance on an LX Appliance.
Manage Network Interfaces	Activate, deactivate, or restart all network interface(s)
Manage RAID Configuration	Display information and perform maintenance operations on controller(s), unit(s) and port(s).
Manage System Configuration Settings	Sets up the system IP address, DNS server IP address, Ethernet type, system clock and time zone, NTP server IP address, Management Appliance IP address, and failover. Change CLI password, reboot, halt, copy public key (used for file authentication when transferring files using the secure protocols SCP or SFTP).

Display Appliance and System Interface Status	Displays the current state of the Appliance in real-time. Display the status of the current system interface information that is stored on the disk, history of changes made during this session, pending changes not yet saved, current system date and time.
Data Migration	Migrate data and configuration settings from one LogLogic Appliance to another.

Table 10: Specification of Management Functions

6.1.5.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles: **authorized administrator,** ~~authorised Analyzer administrators~~**, authorized Configuration Administrator and** [User Administrator, Report Administrator, and Console Administrator].

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

Application Note: In the IDS Analyzer Protection Profile, the FMT_SMR.1 requirement specifies the security role of "authorized Analyzer administrator". For this ST, this role has been replaced by the role of "Configuration Administrator". This modified requirement is applicable to this TOE claiming compliance against the IDS Analyzer PP as the TSF that is maintaining the "Configuration Administrator" security role maps directly to the "authorized Analyzer administrator" role defined in the IDS Analyzer PP.

6.1.6 Protection of TSF (FPT)

6.1.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

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

6.1.6.2 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF **when configured to support HA** shall preserve a secure state when the following types of failures occur: [LX or ST appliances are installed and configured in an active/standby failover pair and connectivity is interrupted between the pair.]

6.1.6.3 FPT_STM.1 Time Stamps

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

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_ITC.1 (1) Inter-TSF trusted channel

FTP_ITC.1.1 (1) The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 (1) The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 (1) The TSF shall use a trusted channel for the following functions: [remote administration of the TOE via SSH or SSL/TLS][3]

6.1.8 Resource Utilization (FRU)

6.1.8.1 FRU_FLT.1 Degraded fault tolerance

FRU_FLT.1.1 The TSF **when configured to support HA** shall ensure the operation of [all the management and event log collection capabilities, except possible loss of audit records and changes made to the security configuration that occur within the 3 seconds of the connection being lost] when the following failures occur: [LX or ST appliances are installed and configured in an active/standby failover pair and connectivity is interrupted between the pair.]

6.1.9 IDS Component Requirements (IDS)

6.1.9.1 IDS_ANL.1 Analyzer Analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) *statistical*; and

b) [Analysis as defined in the alert type column in table 11 below].

Alert Type	Triggered when...
Cisco PIX/ASA Messages Alert	The messages/second rate for a specific PIX/ASA message code is above or below specified rates.
Message Volume Alert	The messages/second rate is above or below specified rates.
Network Policy Alert	A network policy message is received with an Accept or Deny Policy Action.
Pre-defined Search Filter Alert	A text search filter matches message fields.
Ratio Based Alert	The specified message count is above or below a specified percentage of total

[3] This SFR applies PD0108

	messages.
System Alert	An Appliance system criteria is exceeded.
VPN Connections Alert	A VPN connection is denied access and/or disconnected.
VPN Messages Alert	Combinations of specific VPN message area, severity, and code. This alert is applicable to Cisco VPN and Nortel Contivity devices.
VPN Statistics Alert	Recorded statistics on VPN or Radius messages match relative or absolute criteria.

Table 11: Additional Analytical Functions

Application Note: The Adaptive Baseline Alert described in administrative guidance is considered an IDS statistical analysis function and therefore not listed in table 11.

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) [no other security relevant information about the result].

6.1.9.2 IDS_RCT.1 Analyzer React

IDS_RCT.1.1 The TSF shall send an alarm to [any one or more of the following as defined by the Administrator: web console, SNMP server, SYSLOG server, email server] and take [no other actions] when an intrusion is detected.

6.1.9.3 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The Analyzer shall provide [Administrator, Report Administrator] with the capability to read [log messages, reports (that includes the analytical results)] from the Analyzer data.

IDS_RDR.1.2 The Analyzer shall provide the Analyzer data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The Analyzer shall prohibit all users read access to the Analyzer data, except those users that have been granted explicit read-access.

6.1.9.4 IDS_STG.1 Guarantee of Analyzer Data Availability

IDS_STG.1.1	The Analyzer shall protect the stored Analyzer data from unauthorized deletion.
IDS_ STG.1.2	The Analyzer shall protect the stored Analyzer data from modification.
IDS_ STG.1.3	The Analyzer shall ensure that [90 percent] Analyzer data will be maintained when the following conditions occur: *Analyzer data storage exhaustion*.

6.1.9.5 IDS_STG.2 Prevention of Analyzer data loss

IDS_STG.2.1	The Analyzer shall *overwrite the oldest stored Analyzer data* and send an alarm if the storage capacity has been reached.

6.2 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment). Table 9 identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements.

Assurance Class	Assurance Component ID	Assurance Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ASE: 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

ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 12: Security Assurance Requirements

6.3 Security Functional Requirements for the Operational Environment

This section presents the SFRs for the operational environment that are taken from the CC Version 3.1 or from the extended components defined in Section 5. The operational environment shall satisfy the SFRs stated in the table below which lists the names of the SFR components. These requirements do not levy any additional requirements on the TOE itself, but rather on the operational environment. Following Table 10, the individual functional requirements are restated with any necessary operations completed.

Functional Component ID	Functional Component Name
FIA_UAU_SRV.1	Authentication via authentication server
FIA_UID_SRV.1	Identification via authentication server
FTP_ITC.1 (2)	Inter-TSF trusted channel

Table 13: Security Functional Requirements for Operational Environment

6.3.1 FIA_UAU_SRV.1 Authentication via authentication server

FIA_UAU_SRV.1.1 When invoked by the TSF, the [Remote Authentication Servers] in the *Operating environment* shall determine if the user has provided valid authentication data and pass the results of that determination back to the TOE.

6.3.2 FIA_UID_SRV.1 Identification via authentication server

FIA_UID_SRV.1.1 When invoked by the TSF, the [Remote Authentication Servers] in the *Operating environment* shall determine if the user has provided valid identification data and pass the results of that determination back to the TOE.

6.3.3 FTP_ITC.1 (2) Inter-TSF trusted channel [4]

FTP_ITC.1.1 (2) The ~~TSF~~ **remote trusted IT product** shall provide a communication channel between itself and ~~another trusted IT product~~ **the TSF of the TOE** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 (2) The TSF **of the TOE** shall permit *another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 (2) The ~~TSF~~ **remote trusted IT product** shall use a trusted channel for the following functions: [remote administration of the TOE via SSH or SSL/TLS]

6.4 Security Requirements Rationale

6.4.1 Rationale for Not Satisfying All Dependencies

This section includes a table of all the TOE security functional requirements and their associated dependencies with a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Dependency Satisfied
FAU_GEN.1 (1)	FPT_STM.1	Yes

[4] This SFR applies PD0108

SFR	Dependencies	Dependency Satisfied
FAU_GEN.1 (2)	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FCS_CKM.1(1)	FCS_COP.1 and FCS_CKM.4	Yes
FCS_CKM.1(2)	FCS_COP.1 and FCS_CKM.4	Yes
FCS_CKM.1(3)	FCS_COP.1 and FCS_CKM.4	Yes
FCS_CKM.2	FCS_CKM.1 and FCS_CKM.4	Yes
FCS_CKM.4	FCS_CKM.1	Yes
FCS_COP.1(1)	FCS_CKM.1 and FCS_CKM.4	Yes
FCS_COP.1(2)	FCS_CKM.1 FCS_CKM.4	Yes
FCS_COP.1(3)	FCS_CKM.1 FCS_CKM.4	Yes
FCS_COP.1(4)	FCS_CKM.1 FCS_CKM.4	Yes
FCS_COP.1(5)	FCS_CKM.1 FCS_CKM.4	No
FCS_COP.1(6)	FCS_CKM.1 FCS_CKM.4	No
FDP_IFC.1 (1)	FDP_IFF.1	Yes
FDP_IFF.1 (1)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFC.1 (2)	FDP_IFF.1	Yes
FDP_IFF.1 (2)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFC.1 (3)	FDP_IFF.1	Yes

SFR	Dependencies	Dependency Satisfied
FDP_IFF.1 (3)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFC.1 (4)	FDP_IFF.1	Yes
FDP_IFF.1 (4)	FDP_IFC.1 FMT_MSA.3	Yes
FDP_IFC.1 (5)	FDP_IFF.1	Yes
FDP_IFF.1 (5)	FDP_IFC.1 FMT_MSA.3	Yes
FIA_AFL.1	FIAJ_UAU.1	Yes via FIA_UAU_TRD.1
FIA_ATD.1	None	N/A
FIA_UID_TRD.1	None	N/A
FIA_UAU_TRD.1	FIA_UID.1 or FIA_UID_TRD.1	Yes
FMT_MOF.1 (1)	FMT_SMF.1 FMT_SMR.1	Yes
FMT_MOF.1 (2)	FMT_SMF.1 FMT_SMR.1	Yes
FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes, via FIA_UID_TRD.1.
FPT_ITT.1	None	N/A
FPT_FLS.1	None	N/A
FPT_STM.1	None	N/A
FTP_ITC.1 (1)	None	N/A
FRU_FLT.1	FPT_FLS.1	Yes
IDS_ANL.1	None	N/A
IDS_RCT.1	None	N/A

SFR	Dependencies	Dependency Satisfied
IDS_RDR.1	None	N/A
IDS_STG.1	None	N/A
IDS_STG.2	None	N/A

Table 14: SFR Dependencies

FIA_UAU.1 Timing of Authentication requires users to be authenticated by the TOE prior to performing certain actions. This dependency is satisfied by FIA_UAU_TRD.1 Timing of Authentication, which requires users to be authenticated by either the TOE or the Operating environment prior to performing certain actions.

Functional Component FIA_AFL.1 depends on FIA_UAU.1 Timing of Authentication which requires users to be authenticated by the TOE prior to performing certain actions. This dependency is satisfied by FIA_UAU_TRD.1 Timing of Authentication which requires users to be authenticated by either the TOE or the IT environment prior to performing certain actions.

Functional Component FMT_SMR.1 depends on FIA_UID.1 Timing of Identification, which requires users to be identified by the TOE prior to performing certain actions. This dependency is satisfied by FIA_UID_TRD.1 Timing of Identification, which requires users to be identified by either the TOE or the Operating environment prior to performing certain actions.

FCS_CKM.1 and FCS_CKM.4 is identified as a dependency for FCS_COP.1 (5) and FCS_COP.1(6). These hash cryptographic operations are implemented by the one-way hash functions (SHA-1 or MD5) that do not require cryptographic keys for operation. Therefore, the requirements FCS_COP.1 (5) and FCS_COP.1(6) are met without satisfying this dependency.

NOTE: Dependencies on SFRs for the Operating environment do not need to be met.

6.4.2 TOE SFR to TOE Security Objective Tracings

	O.PROTCT	O.IDACTS	O.EVENTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECRMT	O.TMSTMP	O.TRAFFIC	O.LOGCON
FAU_GEN.1 (1)									X					
FAU_GEN.1 (2)									X					
FAU_SAR.1					X									
FAU_SAR.2	X					X	X							
FAU_SAR.3					X									
FAU_SEL.1					X		X							
FAU_STG.2	X					X	X	X		X				
FAU_STG.4								X	X					
FCS_CKM.1 (1)	X										X			
FCS_CKM.1 (2)	X										X			
FCS_CKM.1 (3)														X
FCS_CKM.2	X										X			
FCS_CKM.4	X										X			
FCS_COP.1 (1)	X										X			
FCS_COP.1 (2)	X										X			
FCS_COP.1 (3)	X										X			
FCS_COP.1 (4)														X
FCS_COP.1 (5)	X									X				
FCS_COP.1 (6)										X	X			
FDP_IFC.1 (1)														X
FDP_IFF.1 (1)														X
FDP_IFC.1 (2)			X											
FDP_IFF.1 (2)			X											
FDP_IFC.1 (3)			X											
FDP_IFF.1 (3)			X											
FDP_IFC.1 (4)			X											
FDP_IFF.1 (4)			X											
FDP_IFC.1 (5)													X	

	O.PROTCT	O.IDACTS	O.EVENTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.SECRMT	O.TMSTMP	O.TRAFFIC	O.LOGCON
FDP_IFF.1 (5)													X	
FIA_AFL.1							X							
FIA_ATD.1							X							
FIA_UID_TRD.1						X	X							
FIA_UAU_TRD.1	X					X	X							
FMT_MOF.1 (1)	X					X	X							
FMT_MOF.1 (2)						X								
FMT_MSA.1						X								
FMT_MSA.3	X													
FMT_MTD.1	X					X	X			X				
FMT_SMF.1					X									
FMT_SMR.1							X							
FPT_ITT.1														X
FPT_FLS.1	X													
FPT_STM.1									X			X		
FTP_ITC.1 (1)											X			
FRU_FLT.1	X													
IDS_ANL.1		X												
IDS_RCT.1				X										
IDS_RDR.1					X	X	X							
IDS_STG.1	X					X	X	X		X				
IDS_STG.2								X						

Table 15: Mapping between TOE SFRs and Security Objectives

6.4.3 TOE SFR Rationale

O.PROTCT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized

users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

FAU_STG.1 ensures that generated audit data is securely stored for later review.

The TOE controls authorized users' management of security attributes [FMT_MSA.3]

Separate TOE components are required to authenticate each other when communicating [FCS_COP.1(5)].

FPT_FLS.1 ensures that when LX or ST appliances are installed and configured in an active/standby failover pair, the TOE preserves a secure state after connectivity is interrupted between the active appliance and the standby appliance.

FRU_FLT.1 ensures that when LX or ST appliances are installed and configured in an active/standby failover pair, management and event log collection services continue after connectivity is interrupted between the active appliance and the standby appliance.

O.IDACTS

The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.EVENTS

The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.

The TOE must collect event logs from IT System sources in the TOE operating environment [FDP_IFC.1/IFF.1 (2), FDP_IFC.1/IFF.1 (3), FDP_IFC.1/IFF.1 (4)]

O.RESPON

The TOE must respond appropriately to analytical conclusions.

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

O.EADMIN

The TOE must include a set of functions that allow effective management of its functions and data.

The TOE must provide the ability to review and manage the audit trail of an Analyzer [FAU_SAR.1, FAU_SEL.1]. The Analyzer must provide the ability for authorized administrators to view the Analyzer data [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]. The TOE must provide the capability to sort audit information [FAU_SAR.3].

O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

FMT_SMR.1 defines user roles of the TOE and associated accesses.

O.IDAUTH

The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of collected Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from unauthorized deletion as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]

FIA_UID_TRD.1 ensures that before any operations other than those mentioned in the requirement occurs on behalf of a user, the user's identity is verified by the TOE or Operating environment.

FIA_UAU_TRD.1 ensures that users are authenticated at the TOE by either the TOE or the TOE environment before any operations other than those mentioned in the requirement occurs on behalf of the user. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator.

FIA_AFL.1 exists to minimize guessing of authentication credentials by brute force method. A user account is locked for a time duration specified by an authorized administrator when a predefined number of consecutive unsuccessful login attempts are reached.

O.OFLOWS

The TOE must appropriately handle potential audit and Analyzer data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the

availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The Analyzer must prevent the loss of audit data in the event that its audit trail is full [IDS_STG.2].

O.AUDITS

The TOE must record audit records for data accesses and use of the Analyzer functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event that its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

FAU_GEN.1 outlines what data must be included in audit records and what events must be audited.

O.INTEGR

The TOE must ensure the integrity of all audit and Analyzer data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the Analyzer may query or add audit and Analyzer data [FMT_MTD.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected form interference that would prevent it from performing its functions [ADV_ARC.1]. The TOE computes a MD5 hash for each event log file it collects and stores the hash value in the database separately from the log itself. The TOE will check for that MD5 hash value in the database and if it already exists then it is considered to be a duplicate and does not replace the file FCS_COP.1(6).

O.TRAFFIC

The TOE filters the flow of all network traffic from IT entities attempting to interact with the TOE [FDP_IFC.1 (5), FDP_IFF.1 (5)].

O.SECRMT

The TOE ensures secure communication in support of remote administration over the web GUI and CLI [FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1 (6) FTP_ITC.1 (1)].

O.LOGCON

The TOE ensures the confidentiality and integrity of event log data when it is transferred between separate TOE components [FCS_CKM.1(3), FCS_COP.1(4), FDP_IFC.1(1), FDP_IFF.1(1), FPT_ITT.1].

O.TMSTMP

The TOE must ensure that the TOE generates a reliable time stamp. [FPT_STM.1].

6.4.4 SAR Rationale

The TOE and this ST are EAL2 augmented with ALC_FLR.2 and claims demonstrable conformance to the [IDSAPP] Protection Profile.

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the Analyzer may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the Analyzer will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

7 TOE Summary Specification

This section presents a description of how the TOE SFRs are satisfied.

TOE SFR	Description of how the TOE meets the SFR
FAU_GEN.1 (1) (2)	The TOE generates two types of audit records: appliance audit records and analyzer data. Appliance audit records are specific to the function and use of the appliance, allowing an administrator to monitor management actions and security related events. All appliance audit data is written to the database. The web GUI provides the Administrator the ability to view security audit data for the system. The audit data displayed and the data contained in the audit record include: the date and time of the event, the type of event, the subject identity, and the outcome of the event, indicating if it was a success or failure.
FAU_SAR.1	The TOE provides a web interface to review audit records generated by the TOE. Audit Records can be viewed via Index/RegEx Search, and Real-Time or Summary Reports by choosing the 'LogLogic Appliance' device type filter on the search or report setup page.
FAU_SAR.2	All users that successfully authenticated to the web interface can view audit data through report creation and viewing of real-time data.
FAU_SAR.3	The authorized Administrator can sort the audit data based on at least the following event attributes: date and time of the event, type of event, and success or failure of related event. Further, reports can be sorted in ascending or descending order based upon the options available in the Report type.
FAU_SEL.1	The TOE provides a Web GUI interface where an authorized administrator can allow or disallow all audit data collection for the local appliance.
FAU_STG.2	The TOE requires that authorized users and administrators be identified and authenticated prior to accessing security-related functions that control the stored audit data. CLI and GUI users must provide a user identifier and authentication data and be successfully authenticated prior to accessing the CLI or GUI. The TOE includes the ability to generate User Access reports that include user who is making inquiry and action taken.
FAU_STG.4	The TOE implements overwriting of oldest stored audit records and sends an alarms when audit storage exhaustion occurs. When disk storage exceeds 90 percent (audit and analyzer data) the TOE will purge the oldest stored audit records from the database to make room for new audit records. It will continue purging until disk storage is less than 90 percent exhausted. The TOE sends an administrative alert that can be sent as an SMTP or SYSLOG message if this occurs.
FCS_CKM.1(1)	The TOE generates cryptographic keys that are used to protect communications for SSHv.2 remote administration. The keys that are used are based on the RSA algorithm.
FCS_CKM.1(2)	The TOE generates cryptographic keys that are used to protect communications for SSLv.3/TLS remote administration. The keys that are used are based on the RSA algorithm.

FCS_CKM.1(3)	The TOE generates cryptographic keys that are used to protect communications for secure transfer of logs between TOE components. The keys that are used are based on the Blowfish algorithm.
FCS_CKM.2	The TOE implements the Diffie-Hellman key exchange to distribute cryptographic keys used for SSHv.2 remote TOE administration.
FCS_CKM.4	The TOE destroys all cryptographic keys stored by the TOE by overwriting an old key with new key.
FCS_COP.1 (1)	The TOE implements encryption and decryption of data exchanged during remote TOE CLI administration which provides confidentiality of the data transmitted.
FCS_COP.1 (2)	The TOE implements secure hashing of data exchanged during remote TOE CLI administration. This ensures data transmitted from one end arrives unaltered on the other end, providing integrity of the data transmitted.
FCS_COP.1 (3)	The TOE implements encryption and decryption of data exchanged during remote TOE administration to the web interface which provides confidentiality and integrity of the data transmitted.
FCS_COP.1 (4)	The TOE implements encryption and decryption of data exchanged during log transfer between TOE components using Blowfish which provides confidentiality and integrity of the data transmitted. The TOE also uses Blowfish to encrypt passwords when users are authenticated by an external authentication server.
FCS_COP.1 (5)	The TOE implements secure hashing of shared secret between TOE components. This ensures that the data is received by the correct component.
FCS_COP.1 (6)	The TOE computes a MD5 hash for each event log file it collects and stores the hash value in the database separately from the log itself. It will check for that MD5 hash value in the database and if it already exists then it is considered to be a duplicate and does not replace the file. The TOE uses MD5 to hash passwords when users are authenticated by a RADIUS or TACACS+ external authentication server.
FDP_IFC.1 (1) **FDP_IFF.1 (1)**	The TOE controls the forwarding of logs received and imposes a security policy to restrict the forwarding to another instance of the TOE (LX or ST device). The WebGUI allows the authorized administrator to create rules that perform the log forwarding based on the security attributes. Each IP packet is examined to determine if the attributes match the rule. These security attributes are source ip, destination ip, destination port, and valid authentication key. LogLogic TCP (port 5514) is a LogLogic proprietary file-based protocol used to forward events at 1 minute intervals. Any data sent to the local TCP 5514 port will be forwarded to the remote port through the tunnel.
FDP_IFC.1 (2)	The TOE controls event logs that transferred to itself from secure data sources in the operational environment and imposes a security policy to

FDP_IFF.1 (2)	restrict them. The WebGUI allows the authorized administrator to create rules to which the LX ensures it authenticates to the data source and the transfer is encrypted based on the following attributes: source, ip destination ip and matching protocol. Sftp, scp, ftps, and checkpoint LEA/CPMI are all outbound file transfer requests rules. HTTPS can be either an outbound file transfer request or can be used to receive files (inbound).
FDP_IFC.1 (3) **FDP_IFF.1 (3)**	The TOE controls event logs originating from data sources in the operational environment and imposes a security policy to restrict them. The WebGUI allows the authorized administrator to create rules to which the LX ensures the event logs are pulled based on the following attributes: source, ip destination ip and matching protocol of HTTP, FTP, CIFS or MS SQL queries.
FDP_IFC.1 (4) **FDP_IFF.1 (4)**	The TOE controls event logs originating from data sources in the operational environment and imposes a security policy to restrict them. The WebGUI allows the authorized administrator to create rules to which the LX ensures event logs are received based on the following attributes: source, ip destination ip, destination port equals 514 (SYSLOG) and matching protocol of TCP or UDP.
FDP_IFF.1 (5) **FDP_IFC.1 (5)**	The TOE controls IP network traffic it receives and imposes a security policy to filter that traffic. The WebGUI allows the authorized administrator to create rules to which the LX or ST ensures are filtered based on the information security attributes. Each IP packet is examined to determine if it matches the same information in the rule. These security attributes are source IP address, destination IP address, protocol (TCP or UDP), and Transport layer port. The values available for Transport Layer port are: Http Collector: 4433 (TCP) HTTP: 80 (TCP) HTTPS: 443 (TCP) Inbound LX Traffic: 5514 (ST Appliances only, TCP) Loglogic Tunnel: 11965 (TCP) NTP: 123 (UDP) RealTime Viewer: 4514 SSH: 22 (TCP) SSL: 4443 (TCP) SNMP: 161 (UDP) SNMP-Trap: 162 (UDP) SYSLOG: 514 (UDP) The TOE treats port 443 (HTTPS) differently in that the last rule for port 443 cannot be deleted. This prevents losing browser access to the TOE at the same time allowing access to port 443 to be restricted by rules. The TOE processes rules in descending order. Therefore, if you add a rule that might be superseded by a higher rules in the list, you must first

	delete the higher rule for the new rule to be effective.
FIA_AFL.1	The TOE ensures that if a configurable number of consecutive unsuccessful authentication attempts are made then Web user accounts are locked for a time duration of 1-9999 minutes as specified by an authorized administrator.
FIA_ATD.1	Security attributes corresponding to web GUI users are stored in the MySQL database. CLI attributes are stored in /etc/passwd file. The TOE maintains the user security attributes of identifier (User ID), password information (authentication data), and user privileges (authorizations) that form roles.
FIA_UAU_TRD.1 **FIA_UID_TRD.1**	The TOE requires that users be identified and authenticated prior to accessing security-related functions. CLI and GUI users must provide a user identifier and authentication data and be successfully authenticated prior to accessing the CLI or GUI The TOE can be configured to require that Web GUI users be authenticated by either the TOE or the IT environment. All web GUI users logging into the TOE are authenticated by the a local password authentication mechanism or an optional RADIUS/TACACS or Active Directory authentication server located in the operating environment. The TOE performs the following functions prior to identifying and authenticating themselves: • Display TOE login screen.
FMT_MOF.1 (1)	The TOE restricts all modifications to Analyzer functions and alerting to the Configuration Administrator roles. The Configuration Administrator is confirmed by requiring all users to successfully identify and authenticate themselves to the TOE against user profiles that contain a role security attribute. The role security attribute defines the types of actions that the user can carry out on the TOE and the TOE requires users to have the Configuration Administrator role to modify user role information.
FMT_MOF.1 (2)	The TOE restricts management functions to the roles as specified in table 9 All users are required to successfully identify and authenticate themselves to the TOE against user profiles that contain a role security attribute. The role security attribute defines the types of actions that the user can carry out on the TOE .
FMT_MSA.1	The TOE restricts all management of the information security attributes in the log transfer, network access control SFPs to Administrator and Configuration Administrator roles.
FMT_MSA.3	The TOE provides restrictive default values for the information flow security attributes which can be overridden and managed by users in the Administrator and Configuration Administrator roles. By default, the policy rule does not allow information to flow and does not allow default values to be specified.
FMT_MTD.1	The TOE allows the Administrator and Configuration Administrator to query, modify, or add Analyzer or TOE data and allows the Report Administrator to query Analyzer or TOE data.

FMT_SMF.1	The TOE provides management functions that allow administrators to define the parameters that control the operation of security-related aspects of the TOE as specified in table 10. The backup/restore functionality is permitted within the TOE evaluated configuration, but only as part of the HA failover pair synchronization process. The HA synchronization uses SCP.
FMT_SMR.1	There are two types of roles in the TOE: Web GUI roles and the Console CLI role. There are four Web GUI roles: Administrators, Configuration Administrators, Report Administrators, and User Administrators. Administrators have full access privileges and can make any device, user or report additions, modifications, or deletions they deem necessary. Configuration Administrators have full access to device configuration and can make any device additions, modifications, or deletions they deem necessary. Report Administrators have full access to reporting and can view or make any report additions, modifications, or deletions they deem necessary. User Administrators have full access privileges to the user database and can make any user additions, modifications, or deletions they deem necessary. The Console CLI administrator is the role required to use the Appliance CLI from the local serial connection or remote connection over SSH. Any user with the Appliance CLI password and physical access to the TOE is a Appliance CLI administrator.
FPT_ITT.1	The TOE secures TSF data that is transmitted within the TOE from disclosure or modification. The LX and ST appliances communicate over an encrypted tunnel when logs are transferred. All communication is encrypted with Blowfish encryption. Each appliance maintains an Authentication key. When a log transfer occurs, the key is used to authenticate the upstream device.
FPT_FLS.1	The TOE preserves a secure state when failover is configured and connectivity is lost. The connection is considered lost when ten consecutive heartbeats are not acknowledged within a specified timeframe. When a node joins a HA pair, the MySQL database on the active appliance is replicated to the standby appliance. The pair synchronize archived data (read-only) and active data (data currently being modified). This ensures that both Appliances have exactly the same data.
FPT_STM.1	The TOE has an internal system clock which is used to generate timestamps for its audit records and reports. The TOE provides NTP client and server functions for accurate sources of time and clock synchronization. When the TOE provides NTP server functionality for synchronization among TOE appliances, LX Appliances must use an ST Appliance as the source NTP server.
FTP_ITC.1 (1)	The TOE provides a trusted communication channel for remote administration via SSH v2 or SSLv3/TLS.
FRU_FLT.1	The TOE ensures management and event log collection capabilities continue when failover is configured and connectivity is lost. The connection is considered lost when ten consecutive heartbeats are not

	acknowledged within a specified timeframe. When a node joins a HA pair, the MySQL database on the active appliance is replicated to the standby appliance. The pair synchronize archived data (read-only) and active data (data currently being modified). This ensures that both Appliances have exactly the same data.
IDS_ANL.1	The TOE provides alerts to analyze and respond to security threats and anomalies. The Adaptive Baseline Alert establishes a baseline after 1 week from the activation time based on event logs received from IT sources. After the baseline is established, the baseline is adjusted every 15 minutes. The new value is averaged in with past baseline. An alert is triggered when the event log messages/second rate rises above, or falls below specified percentages of the nominal rate for the traffic. The maximum value for the lower threshold is 100 and the maximum value for the upper threshold is 999,999,999. The TOE provides Ratio Based Alerts. Ratio Based Alerts are triggered when the specified message count is above or below a specified percentage of total messages. For example, "Login Success message count is fewer than 10% of total messages." See table 11 for all available analytical alerts.
IDS_RCT.1	The TOE will send an alarm to web console, SNMP server, SYSLOG server, and email server when an alert is triggered by a rule. The Alert Viewer allows the user to: • view all alerts • filter shown alerts by alert category and priority • change the alert category to Acknowledged • delete the alerts permanently
IDS_RDR.1	Only successfully authenticated users can access the web GUI. Further, only users who hold the appropriate authorization can view the data. Using the web GUI, authorized Administrators and Report Administrators can view the overall status of the event log data collected including new Alerts and Message counters and rates. The authorized Administrators and Report Administrators can view the event log data directly using the Real-Time Viewer. The Real-Time viewer provides a scrolling display of all log messages as the Appliance receives them. Log messages can also be filtered. The authorized Administrator or Report Administrator can also execute reports that include the analytical results and other collected analyzer data. This data can also be searched. All data is presented in such a manner that it can be read and the contents of the data can be interpreted.
IDS_STG.1 **IDS_STG.2**	The TOE requires that users and administrators be identified and authenticated prior to accessing security-related functions that control the stored analyzer data. CLI and GUI users must provide a user identifier and authentication data and be successfully authenticated prior to accessing the CLI or GUI.

	The TOE implements overwriting of oldest stored analyzer data and sends an alarms when audit storage exhaustion occurs. When disk storage exceeds 90 percent (analyzer and audit data) the TOE will purge the oldest stored audit records from the database to make room for new analyzer/audit records. It will continue purging until disk storage is less than 90 percent exhausted. The TOE sends an administrative alert that can be sent as an SMTP or SYSLOG message if this occurs.

Table 16: TOE Summary Specification