National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

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 ST3010)

Report Number:	**CCEVS-VR-VID10333-2009**
Dated:	**July 9, 2009**
Version:	**1.2**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20878

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6757
Fort George G. Meade, MD 20755-6757

Acknowledgements

Validation Personnel:

Patrick Mallett
Franklin Haskell
The MITRE Corporation

The TOE evaluation was sponsored by:

LogLogic Inc.
110 Rose Orchard Way, Suite 200
San Jose, CA 95134

Evaluation Personnel:

Maria Tadeo
Abdul Qayyum
Arca Common Criteria Testing Laboratory

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the LogLogic v4.6.1 Open Log Management Platform. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the LogLogic v4.6.1 Open Log Management Platform was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during May 2009. The information in this report is largely derived from the Security Target (ST), written by LogLogic, and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product conforms to Common Criteria Version 3.1 Revision 2, Part 2 extended and Part 3 conformant, and meets the requirements for Evaluation Assurance Level (EAL) 2 augmented by ALC_FLR.2 and is conformant with the U.S. Government Protection Profile: Intrusion Detection System Analyzer for Basic Robustness Environments, Version 1.3, 25 July 2007. [IDSAPP]

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

1.1 TOE Summary

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 such as firewalls, VPN concentrators, servers, routers and switches, storage devices, and applications (both commercial and custom developed). 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 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 provides searching and flexible reporting via provided templates and up to 5,000 custom reports. The ST series of appliances archives unaltered logs for long-term retention. The LX and ST appliances communicate with each other 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 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
2. At least one LogLogic ST Appliance (There can be more than one ST deployed in the evaluated configuration.)
3. 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.

1.2 Validation Summary

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) Work Unit Verdicts), and reviewed successive versions of the ETR and Test Report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2 augmented by ALC_FLR.2 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) or candidate CCTLs, using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully-qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	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 ST3010
Protection Profile	None
Security Target	LogLogic v4.6.1 Open Log Management Platform Security Target, version 2.0 date June 30, 2009

Item	Identifier
Evaluation Technical Reports	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for 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 ST3010), document version 6.0, released June 30, 2009. • ALC (Life Cycle): ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.2 Evaluation Technical Report for LogLogic v4.6.1 Log Management and Intelligence Platform with one or more LX Appliance (Model Numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model Numbers ST2010 and ST3010), document version 3.0, released May 29, 2009. • AGD (Operational and Preparative Guidance): AGD_OPE.1; AGD_PRE.1 Evaluation Technical Report for LogLogic v4.6.1 Log Management and Intelligence Platform with one or more LX Appliance (Model Numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model Numbers ST2010 and ST3010), document version 2.0, released April 27, 2009. • ADV (Development Evaluation): ADV_FSP.2; ADV_TDS.1; ADV_ARC.1; Evaluation Technical Report for LogLogic v4.6.1 Log Management and Intelligence Platform with one or more LX Appliance (Model Numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model Numbers ST2010 and ST3010), document version 2.0, released May 29, 2009. • ATE (Functional Testing, Testing Coverage, and Independent Testing Evaluation): ATE_COV.1;ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for LogLogic v4.6.1 Log Management and Intelligence Platform with one or more LX Appliance (Model Numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model Numbers ST2010 and ST3010), document version 4.0, released June 19, 2009. • AVA (Vulnerability Assessment Evaluation): AVA_VAN.2; Evaluation Technical Report LogLogic v4.6.1 Log Management and Intelligence Platform with one or more LX Appliance (Model Numbers LX510, LX1010, and LX2010) and one or more ST Appliance (Model Numbers ST2010 and ST3010), document version 3.0, released May 29, 2009.
CC Version	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 2, September 2007. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 2, September 2007.
Applicable interpretations and precedents	Compliant with all international interpretations with effective dates on or before December 12, 2008.
Conformance Result	CC Part 2 extended and CC Part 3 conformant, EAL 2 augmented by ALC_FLR.2
Sponsor and Developer	LogLogic Inc 110 Rose Orchard Way, Suite 200 San Jose, CA 95134

Item	Identifier
Common Criteria Testing Lab (CCTL)	Savvis Federal Systems Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validators	Patrick Mallett, The MITRE Corporation Franklin Haskell, The MITRE Corporation Sunil Trivedi, The MITRE Corporation

Table 1: Evaluation Identifiers

3 Security Policy

The TOE addresses the following security policies which are relevant to the secure configuration and operation of the LogLogic v4.6.1 Open Log Management Platform.

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 Assumptions and Clarification of Scope

4.1 Usage Assumptions

This section helps define the scope of the security problem by identifying assumptions about the security aspects of the environment and/or of the manner in which the LogLogic v4.6.1 is intended to be used.

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.

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).

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.

4.2 Clarification of Scope

4.2.1 Validated Features

All the features of the LogLogic v4.6.1 are evaluated, except those specified below as not validated.

4.2.2 Features Not Validated

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 a NAS server or a SAN server in conjunction with a LogLogic ST Appliance as a dedicated storage system and optional encryption for raw data files.

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.

5 Architectural Information

The LogLogic v4.6.1 TOE is composed of two families of physically distinct components. The LX series, and the ST series. See section 5.1 of this report for details on the evaluated hardware models.

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 Administrator is presented with tab-based, hyperlinked web pages providing access control specific management functions.

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. When these clear text protocols are used, the TOE does not enforce protection of log data until the data is received by the TOE.
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 any 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

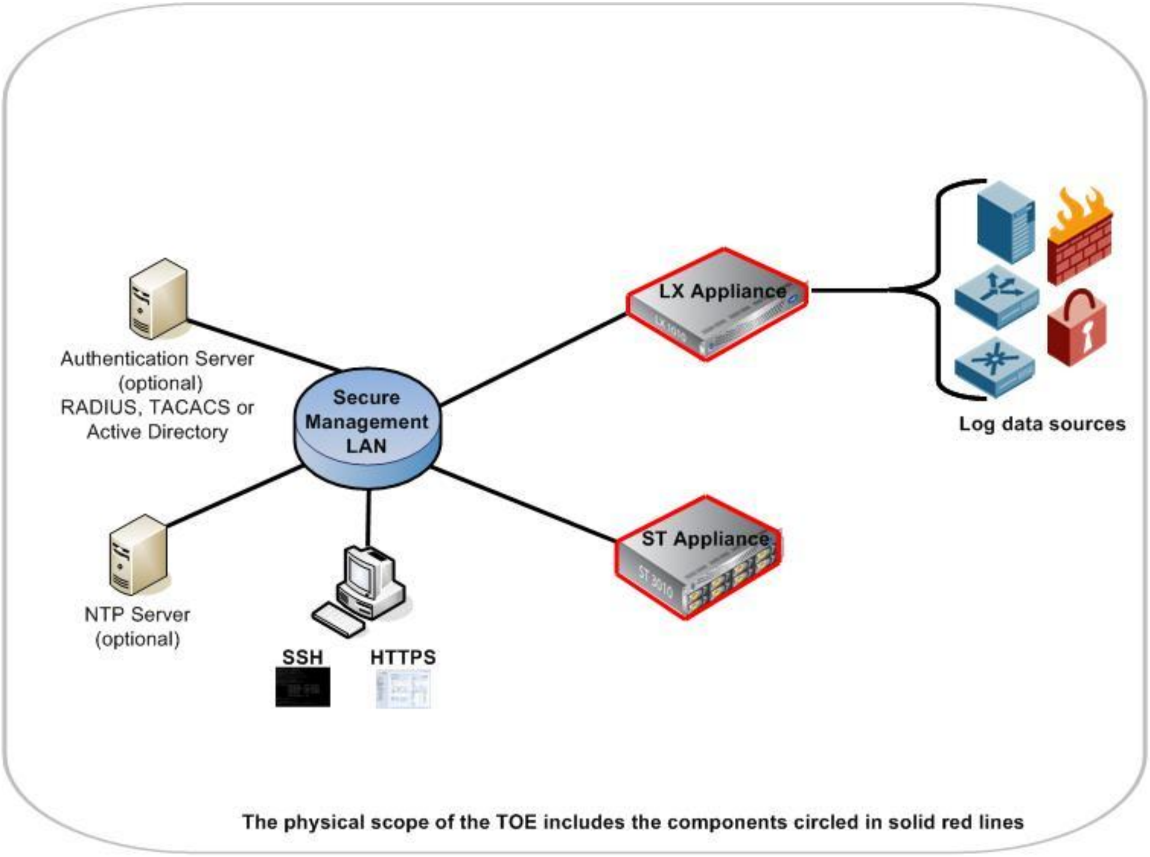
For each log file collected or compiled by the LogLogic appliance, the appliance computes a MD5 hash for each event log file it collects and stores the hash value in the database separately from the log itself. It will check for that MD5 hash value in the database and if it already exists then it is considered to be a duplicate and does not replace the file.

The 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, so log data older than 90 days on the ST appliance can be searched. When storage capacity on the appliance reaches 90% full, the oldest logs will begin to be overwritten, including both system events generated by the TOE as well as log source data collected by the TOE. Customers should be aware of their network traffic and acquire appliances with appropriate capacity to account for storage limitations.

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.

5.1 TOE Hardware and Software

Figure 4 shows a depiction of the TOE and its environment.



The physical scope of the TOE includes the components circled in solid red lines

Figure 1: TOE Physical Boundaries

5.1.1.1 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 2: 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 3: LogLogic v4.6.1 Software components

5.2 Environmental Components

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.
    - 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.
    - 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

6 Documentation

The hardware and software for the TOE are purchased as a single item. The software is preinstalled on the appliance. A documentation CD ROM and hard copy forms of release notes and supplemental guidance are included with the delivery of the pre-installed appliance. The following product documentation is included in the delivery:

- *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*
- *LogLogic 4.6.1 Release Notes, October 2008*
- *LogLogic v4.6.1 Supplemental Installation and Administrative Guidance for the Common Criteria Evaluated Configuration, version 1.0, June 30, 2009*

All of the documentation listed above is included within the scope of the evaluation and can be found either in the \Documentation directory of the CD ROM or delivered in hard-copy with the appliance. The CD ROM also contains documentation to assist administrators in the configuration of log source devices for optimal compatibility with LogLogic appliances. That documentation can be found in the \Documentation\LogSource\ directory of the CD ROM. Other documentation provided on the documentation CD ROM (found in \ComplianceSuiteEvaluationPack, and \WebServices) is not related to evaluated security functionality and is provided for customers who will not be running the product in the CC evaluated configuration.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.1 Developer Testing

As required for EAL2, the developer provided actual results of testing a subset of TSFI and each SFR. At least one test case was mapped to a subset of external interface. Many of the interfaces were exercised by multiple tests. An evaluation team review of all of the security functions and the mapping between security functions and tests confirmed that security functions were appropriately tested by the developer tests. Actual results were generated at the developer's development and testing facility San Jose, CA. The actual test results provided from the developer for this evaluation were generated on a deployment of LogLogic components consistent with the Security Target, and installed in accordance with the LogLogic v4.6.1 Supplemental Installation and Administrative Guidance for Common Criteria Evaluated Configuration guidance.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that a subset of TSF Interfaces was tested by the developer by creating a mapping of test cases to SFR's.

The evaluation team performed a subset of the developer's test suite and devised an independent set of team tests and penetration tests. The test cases (sample of vendor tests) and independent test that were run by the evaluation team with vendor engineers, covered 32 of 52 (61%) SFRs, included 8 out of 8 (100%) TSFs and 10 out of 12 (83%) TSFIs for the TOE

The evaluation team also performed flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. The specific penetration tests executed include the following:

- Used a port scanner to enumerate listening services on each of the distributed TOE components.
- Attempted privilege escalation by testing the limitations imposed on user group levels, and restricted access to privileged commands and operations.
- Checked for known vulnerabilities on each of the distributed TOE components network vulnerability scanners.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

The network configuration used for the execution of the CCTL testing is documented in the figure below.

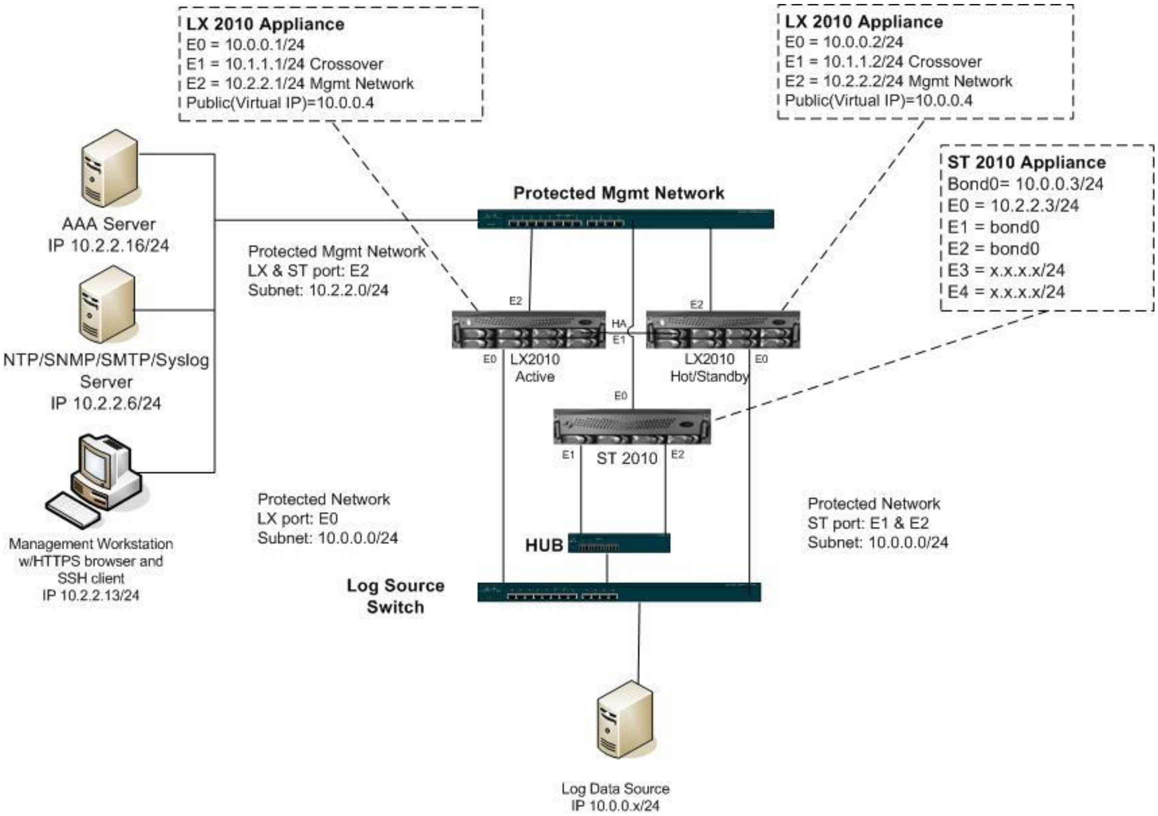


Figure 2: CCTL testing environment

8 Evaluated Configuration

The TOE consists of a minimum of two network appliances (one LX and one ST appliance) each executing the software described in table 4. 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 following conditions must be met for the TOE to be deployed in the evaluated configuration:

- 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.

Section 4.2 of this report list the features that interfere with the TOE security functionality claims and must be disabled or not configured for use in the evaluated configuration.

See section 5.2, Environmental Components, for details on the requirements for the TOE operational environment. 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.

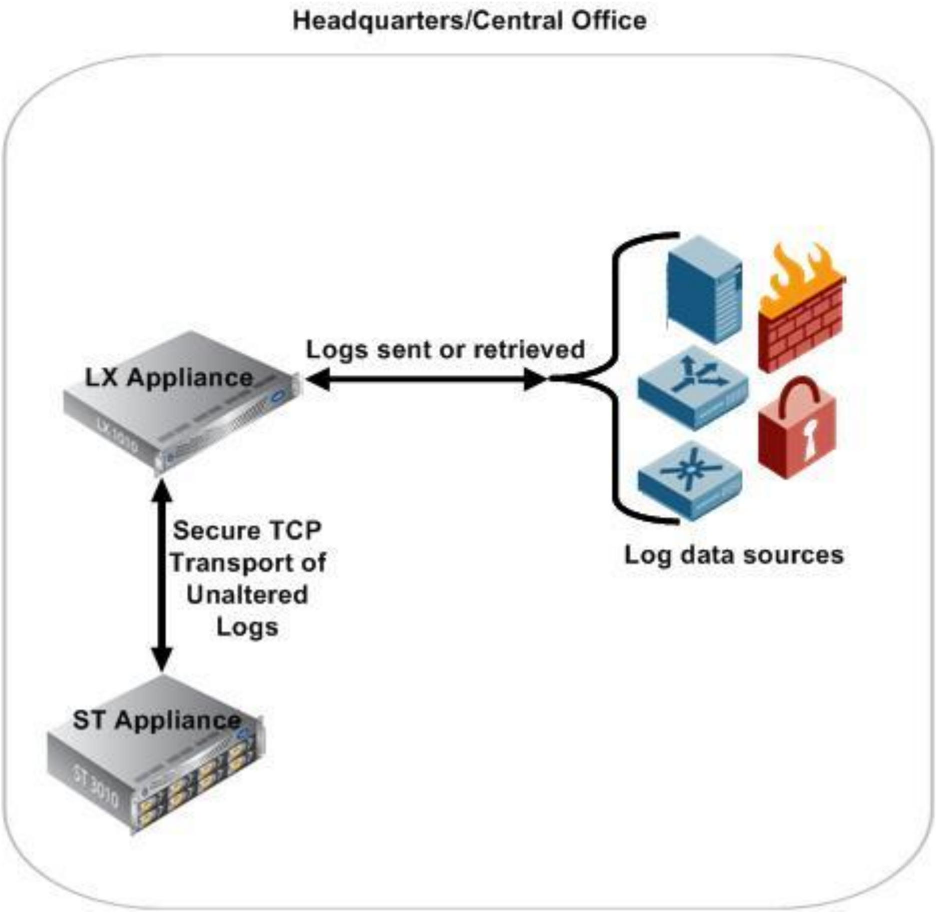


Figure 3: TOE Deployment Configuration #1

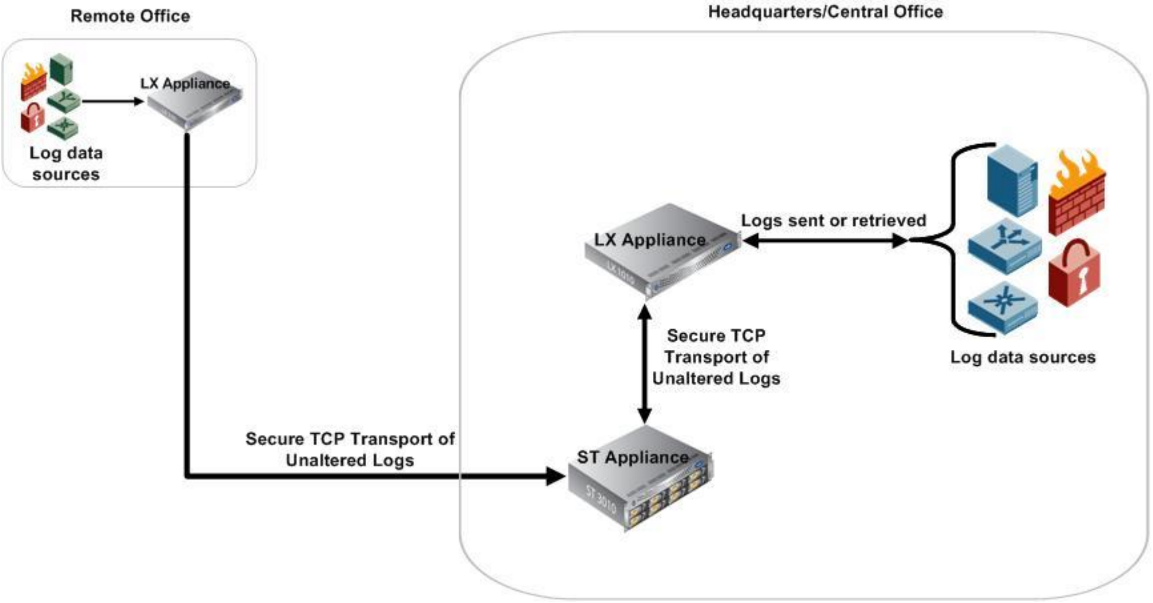

Remote Office
LX Appliance
Log data sources
Headquarters/Central Office
LX Appliance
Logs sent or retrieved
Secure TCP Transport of Unaltered Logs
Log data sources
Secure TCP Transport of Unaltered Logs
ST Appliance

Figure 4: TOE Deployment Configuration #2

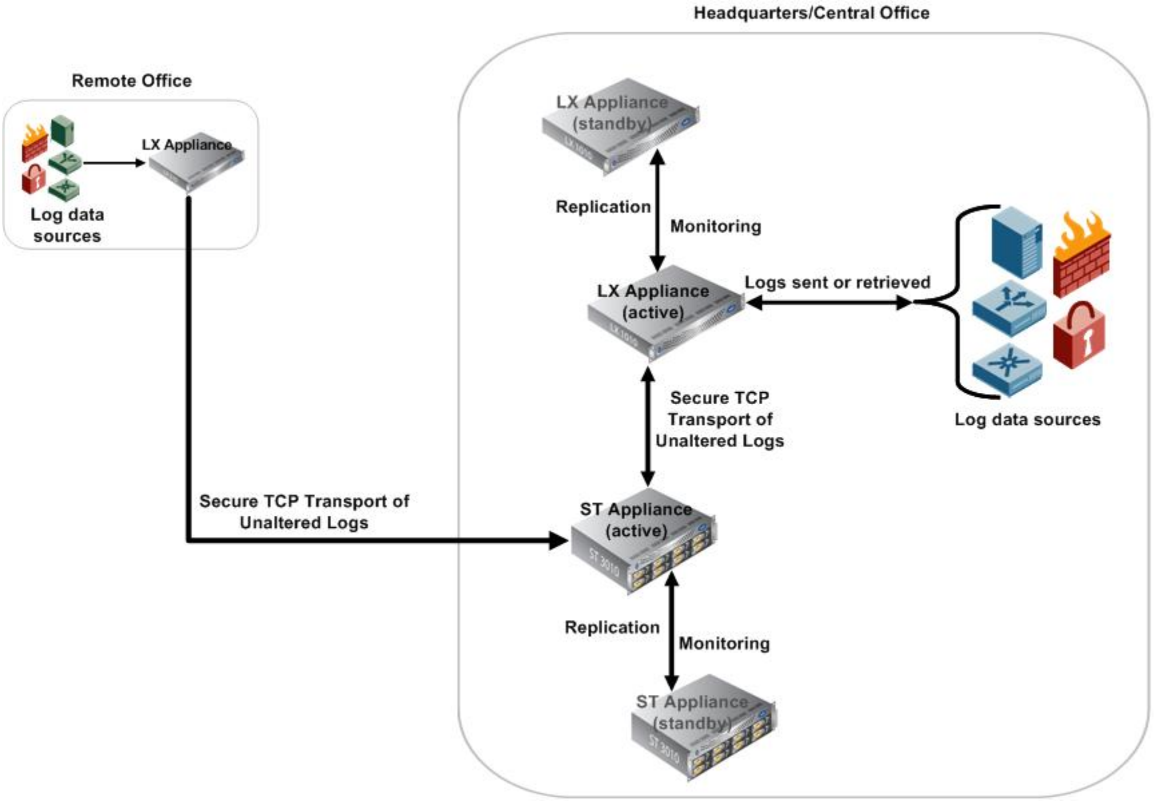


Figure 5: LX and ST appliances deployed in an optional failover configuration.

9 Results of Evaluation

The evaluation was conducted based upon CC, Version 3.1; CEM, Version 3.1, and all applicable NIAP CCEVS and International Interpretations in effect on December 12, 2008.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each Work Unit of each EAL 2 assurance component and for the augmented assurance component, ALC_FLR.2.

For Fail or Inconclusive Work Unit Verdicts that arose during evaluation, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. Through this iterative process, the Evaluation Team confirmed that each CEM Work Unit resulted in a Pass, and assigned an overall Pass verdict to the assurance component only when all of the Work Units for that component had been assigned a Pass verdict.

The evaluation determined the product to be CC Part 2 conformant and to meet the requirements for CC Part 3 for EAL 2 augmented by ALC_FLR.2. The details of the evaluation are recorded in the Evaluation Technical Reports (ETRs).

10 Validator Comments

The validator has reviewed the evaluation technical report and concludes of this evaluation the following comment:

The vendor offers many product families such as LX, MA, MX, and ST models and tools like Log Export API (LEA) server, LEA Firewall etc. The prospective customers must note that only LX (models: 510, 1010, 2010) and ST (Models: 2010, 3010) are CC evaluated product models. Specifically, only LX 2010 and ST 2010 were tested
The TOE does not provide protection of log data while it is in transit over the network to the TOE. The TOE only supports use of clear text protocols such as syslog for log collection. The TOE does not enforce protection of log data until the data is received by the TOE.

Logs stored in the ST appliance will begin to be overwritten when storage capacity reaches 90% full. Overwriting applies to system events generated by the TOE as well as log source data collected by the TOE. Customers should be aware of the volume of their event and log traffic and calculate the size and number of appliances needed to accommodate it. If system events and log data are to be kept for extended periods to support long term correlation and analysis, then the customer’s environment needs to have the capability of off-loading the logs to longer term storage.

All the features of the LogLogic v4.6.1 are not validated. Please see section 4.2.2 for the not validated features that must be disabled.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11 Security Target

LogLogic v4.6.1 Open Log Management Platform Security Target, Version 2.0, dated June 30, 2009.

12 List of 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
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

13 Bibliography

The following documents referenced during preparation of the validation report.

(1) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, Version 3.1 Revision 1.

(2) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2007, Version 3.1 Revision 2.

(3) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2007, Version 3.1 Revision 2.

(4) Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated September 2007, Version 3.1 Revision 2.

(5) LogLogic v4.6.1 Open Log Management Platform Security Target, Version 2.0, dated June 30, 2009.

(6) Compliant with all international interpretations with effective dates on or before June 24, 2008