National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Novell Inc.

Sentinel from Novell Version 5.1.1

Report Number: CCEVS-VR-06-0058
Dated: 30 December 2006
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validator

Patrick W. Mallett, PhD
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

SAVVIS Communications
ARCA Common Criteria Testing Laboratory
Sterling, VA

Table of Contents

1 EXECUTIVE SUMMARY

During the CC evaluation e-Security was purchased by Novell, Inc. For the purposes of the evaluation "e-Security Sentinel 5 v5.1.1" referenced in the CC documentation is equivalent to "Sentinel from Novell Version 5.1.1". The evaluation of the e-Security Sentinel 5 v5.1.1 was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed on 21 November 2006. The Security Target (ST) reflects this change in TOE Identification and Description only. The rest of the evaluation documentation does not reflect the name change.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (CEM) Version 2.3 for conformance to the Common Criteria for IT Security Evaluation Version 2.3. The TOE consists of the Sentinel Server and Sentinel Wizard, along with a database repository. Another optional component of e-Security Sentinel 5 v5.1.1, Sentinel Advisor, is not included in the TOE.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the Evaluation Technical Report (ETR) are consistent with the evidence adduced. This Validation Report is not an endorsement of the e-Security Sentinel 5 v5.1.1 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validator monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validator found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Therefore the validator concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The Arca CCTL evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

For this evaluation, it was appropriate for the Security Target to claim compliance with the external standard for AES and ARC4 for the definition of the encryption

algorithm. There are many ways of determining compliance with a standard. e-Security has chosen to make a developer claim of compliance. This means that there has been no independent verification (by either the evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithms actually meets the claimed standards. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements.

Evaluation Details

Evaluated Product:	e-Security Sentinel 5 v5.1.1
CCTL:	Arca Common Criteria Testing Laboratory
Evaluation Completion:	21 November 2006
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3, (ISO/IEC 15408:2005)
CEM:	Common Evaluation Methodology for Information Technology Security, Version 2.3, August 2005, CCIMB-2005-08-004.
Evaluation Assurance Class:	EAL 2

Interpretations

No national or international (CCIMB) interpretations were applicable to this evaluation.

2 OVERVIEW

e-Security Sentinel version 5.1.1 is a security event management system. It consists of four components: Sentinel Server, Sentinel Wizard, Sentinel Advisor, and a database repository. They work together to enable a view of security event information from a central enterprise perspective console and display. Sentinel Advisor, however, is not included in the Target of Evaluation (TOE). A description of the TOE components is provided in Section 6.

3 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1 Evaluation Identifiers

Evaluation Scheme:	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluation Completion:	21 November 2006
TOE:	E-Security Sentinel 5 v5.1.1
PP:	The TOE does not claim conformance to a PP.

ST:	E-Security Sentinel 5 v5.1.1 Security Target Version 0.34 Final
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)
CEM:	Common Evaluation Methodology for Information Technology Security, Version 2.3,
Developer:	e-Security 1921 Gallows Road Suit 700 Vienna, VA 22182
Evaluation Assurance Class:	EAL 2
CCTL:	SAVVIS Communications Arca Common Criteria Testing Laboratory 45901 Nokes Boulevard Sterling, VA 20166
Evaluation Team:	Abdul Qayyum (Lead Evaluator) Ken Dill Sean Heare Diann Carpenter Michelle Ruppel
Validator:	Patrick Mallett, Lead Validator The MITRE Corporation 7515 Colshire Drive McLean, VA 22102-7508

4 SECURITY POLICY

The Security Policy of the TOE is enforced by the security functions of the TOE. These security functions are described below.

Audit

Auditing of TOE Security functions is achieved in the following manner. The TOE generates two types of audit records: Performance and Internal Events. Auditing of TOE management and I&A actions is accomplished through the same interface as that used to audit enterprise information, the Sentinel Control Center (SCC). The internal audit records are sent via iSCALE and received by the Sentinel Server for correlation and are then passed to the database for permanent storage.

Identification and Authentication (I&A)

There are three roles defined for the TOE: an Operator (read only), Enterprise Information Administrator (read and sentinel server administration) and the System Administrator (full control). The System Administrator also has specific permissions assigned in the database beyond those assigned in the SCC GUI to allow it to manage the TOE data. The term “authorized administrator” refers to both the authorized System Administrator and authorized Enterprise Information Administrator. The term “authorized operator” shall refer to the Operator.

The Sentinel Control Center requires an authorized administrator or operator to authenticate using his/her provided user ID and password. The Sentinel Wizard requires an authorized administrator to authenticate using his/her provided user ID and password. The Sentinel Data Manager requires an authorized System Administrator to authenticate using his/her provided user ID and password.

These components take this information and pass it via the encryption mechanism of iSCALE to DAS, which inserts it in either Oracle or SQL Server (known as the Database). The Database validates the identification information, using its native user management systems. Each user of the TOE is defined as a Database user. Once the Database has validated the provided information, the response is passed back to requesting component.

Protection of TOE security functions

iSCALE provides protection of the TOE security functions. The traffic at the data packet level between the components of the TOE is encrypted using a shared secret cryptographic key (AES or ARC4).

The e-Security Sentinel architecture enables efficient data routing, since events are selectively routed through iSCALE to desired components like Sentinel servers and

Databases. iSCALE supports multi-threaded processing with a configurable number of available threads for event processing.

Data Protection

Data protection is provided by a combination of the Wizard Agent Builder where the Security Policies are managed, the Agents where they are enforced, iSCALE where all the TOE data is transported, and the database where the data is stored. The data flow into the TOE from the monitored security devices is filtered at the Wizard where the System Administrator configures the appropriate policy to allow the flow of data.

This policy is compiled and saved as an Agent with the appropriate IP address of the host, data flow pattern, and other required variables. The data, once the Agent has received it, is normalized according to the data import specifications of the authorized System Administrator. The data is then encrypted using the shared cryptographic key and passed via iSCALE[1] to either MS SQL Server or the Oracle Database for storage. iSCALE supports multi-threaded processing with a configurable number of available threads for efficient event processing. Either MS SQL Server or the Oracle Database stores all of the data generated by the monitored devices. User attribute data is also stored in either MS SQL Server or the Oracle Database including name, user ID and password, and default filter at a minimum. The user data is stored using the user management systems of the databases. Each user of the TOE is defined as a database user.

Management of TOE security functions

The management of TOE security functions takes place at the Sentinel Control Center, Sentinel Data Manager, and the Wizard Agent Builder. There are also some scripts that perform specific actions upon certain TOE Components. The Sentinel Control Center provides an interface into all aspects of TOE management including the real time correlation results, the system overview, incident lists, analysis

1

The cryptography used in this product has not been FIPS validated 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.

activities, and the administration activities of user creation / look and feel of the interface / user permissions. The Wizard Agent Builder allows the System Administrator to fully configure the Agents and Wizard Ports based on the items contained in the Accept Alerts SFP.

The Sentinel Data Manager (SDM) allows the authorized System Administrator to manage database archival and partitioning processes. The MS SQL Enterprise Manager and Oracle Client are used to manage the permissions of the users occupying the System Administrator role.

Enterprise Event Data

The TOE provides the ability to collect, store, and analyze alert data captured from devices around the enterprise. The Agents created and managed by the Wizard Host receive the data where it is normalized. The normalized data (now known as 'events') from the Agents is sent via iSCALE and received by the Sentinel Server. Review of the data generated by the Agents is performed using the Sentinel Control Center. The Sentinel Control Center provides the ability to review the data, in real time, against a timeline summary graph and 3D chart. Graphical depiction of event counts and severities is also available. The Sentinel Control Center also provides the ability to generate historical reports and incidents.

The data is stored in either MS SQL Server or the Oracle Database and managed through the Sentinel Data Manager (SDM).

5 THREATS AND ASSUMPTIONS

5.1 Assumptions

The assumptions are ordered into three groups outlined below.

Personnel Assumptions

A.LOWEXP	There is a low risk of an unauthorized individual attempting to exploit vulnerabilities in the TOE
A.NOEVIL	Administrators are not willfully negligent, but may make mistakes.
A.ADMIN_TRA	The authorized administrators will be trained in the secure usage of the TOE

A.REMOTE_ADMIN	The authorized administrators will only be able to access the TOE remotely from within the trusted network containing the TOE

Table 2 - Personnel Assumptions

Physical Environment Assumptions

A.PHYSEC	The pieces of the TOE will be housed securely
A.NETWORK_COMMUNICATION	The environment will provide reliable network communication between the pieces of the TOE and the monitored devices
A.COMPATIBLE_FORMAT	The devices in the enterprise will be configured to use following formats for data export. Generic Log File (Syslog, ASCII) Microsoft's Windows Event Log (Windows proprietary format) Serial SNMP v1,v2 & v3 TCP Socket ODBC JDBC Cisco's RDEP Checkpoint's OPSEC
A.SECURE_NETWORK	The TOE is used inside a secure trusted network for the use of managing alerts from other security products located on that network.

Table 3 - Physical Environment Assumptions

Operational Assumptions

A.SOLEPUR	The TOE environment will not store general purpose applications or public data
A.TIME_SRC	Time sources in the environment are assumed to be placed in a secure location and configured accurately so as to provide a trusted clock source for the TOE.
A.SEL_PRO	The TOE environment will be configured in such a manner as to prevent an unauthorized person from reading, modifying or destroying security critical TOE configuration data

A.AUDIT_STORAGE	The TOE environment will be configured in such a way as to prevent an unauthorized person from reading or modifying the TOE Audit Trail
A.OSLOGIN	The TOE environment will be configured in such a way to require authorized administrators to login

Table 4 - Operational Assumptions

5.2 Threats

The TOE or IT environment addresses the threats identified in the following sections.

Threats Addressed by the TOE

The TOE addresses the threats discussed below.
The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.UNAUTH_LOGIN	An unauthorized person logs into the Sentinel server, allowing them, through unauthorized use of the management functions, to disrupt the alert flow thus preventing the administrator from reacting to the alerts.
T.UNAUTH_AGENT_UPDATE	An unauthorized person updates an active Agent to stop and/or divert the alert flow.
T.UNAUTH_DATABASE_ACCESS	An unauthorized person accesses the database storing the alert flow modifying the alert record.
T.UNAUTH_REMOTE_ADMIN	An unauthorized person logs into the Sentinel server via the Sentinel Control Center remotely allowing them, through unauthorized use of the management functions, to disrupt the alert flow thus preventing the administrator from reacting to the alerts.
T.SECURITY_MANAGEMENT	The security functions of the TOE are unmanageable leading to missed security alerts.
T.ALERT_UNCOLLECTED	An alert from an enterprise device goes uncollected due to no applicable configured collection Agent preventing the administrator from reacting to the alert.
T.ALERT_UNREVIEWED	An alert from a monitored device is missed due to the inability to review the alert trail preventing the administrator from reacting to the alert.

T.ALERT_LOST	An alert from a monitored device is not able to be stored due to insufficient storage space preventing the administrator from reacting to the alert.
T.ALERT_MISSED	An alert from a monitored device is missed due to a communications failure preventing the administrator from reacting to the alert.
T.TRAFFIC_MODIFIED	An alert from a monitored device OR the data from a remote administration session is modified in transit by an unauthorized person masking unauthorized network activity.
T.NO_AUDIT	Unauthorized and authorized actions occur with no audit trail generation preventing an authorized administrator from reviewing the actions of others and allowing an attacker to escape detection.
T.NO_ACCOUN	The TOE audit trail is not recorded, preventing an authorized administrator from reviewing the actions of others and allowing an attacker to escape detection.
T.SEL_PRO	An unauthorized person may read, modify or destroy security critical TOE configuration Data.

Table 5 – Threats addressed by the TOE

Threats Addressed by Operating Environment

TE.MGMT_ERROR	An authorized administrator makes a mistake during the administration of the TOE and disrupts the alert flow.
TE.NO_ALERTS	No alerts are received from the devices in the Environment
TE.NO_ACCOUN	Authorized administrators do not review the audit log allowing an attacker to escape detection.
TE.EVENT_SEQUENCE	An authorized administrator is unable to distinguish the sequence of events and therefore cannot detect any alerts.

Table 6 – Threats to the Environment

Organizational Security Policies (OSP)

There are no Organizational Security Policies required for the TOE.

6 ARCHITECTURE INFORMATION

The TOE is e-Security Sentinel 5.1.1 (Sentinel 5 Sentinel Server (managed by the Sentinel Control Center), and Sentinel Wizard, along with a database repository which work together to deliver security event management via a central console. It's multi-platform infrastructure event management software. Another optional component of e-Security Sentinel 5 v5.1.1, Sentinel Advisor, is not included in the TOE.

6.1 Overview

Sentinel 5 collects alerts from devices or applications and provides both real-time and historical event analysis using the Sentinel Control Center console.

Sentinel Wizard

The Sentinel Wizard module is comprised of the Wizard Agent Builder and Wizard Agent Manager components. The Wizard Agent Builder is a GUI used to build, select, configure, and control Agents. Agents collect and normalize alerts from security devices and programs. These normalized alerts – known as events – are then sent to the Sentinel server over the protected iSCALE communication path for use in correlation, reporting, and incident response. In addition to running Agents on the local Wizard system, the Agent Builder can be used to upload, download, and control Agents on remote Wizard systems. The Wizard Builder is comprised of the following:

- An Agent: The receptor that collects, filters, and normalizes the raw alerts from security devices and programs and outputs normalized alerts, known as events, that can be correlated, reported, and used for incident response.
- Wizard Port: Enables an Agent to locate the security event data on the network by providing the IP address and other information about the source.

The Wizard Agent Manager is the back-end that manages Agents, generates system status messages, forwards events to Sentinel server, and performs global event filtering. A machine that has the Wizard Agent Manager installed is also referred to as a 'Wizard Host'. A Wizard Host becomes active once an Agent Builder has uploaded an Agent to the Wizard Agent Manager on this machine. The Wizard Agent Manager machine may host many Agents all collecting different types of data from different machines located throughout the enterprise.

Sentinel Server

The Sentinel Server is comprised of the communication server component, the Correlation Engine, and Base components. The communication server component establishes the iSCALE Message Bus. The iSCALE Message Bus is a Java Messaging Services (JMS) based framework through which the Wizard, Sentinel Console Center, DAS, and Sentinel Data Manager communicate. iSCALE is explicitly installed only on the Sentinel Server. The Wizard, Sentinel Console, DAS, and Sentinel Data Manager are not explicitly installed with iSCALE, however they do have sufficient built-in functionality to communicate with it. These TOE components communicate with each other using publisher/subscriber messaging. In this type of JMS communication, a publisher component publishes messages to topics, and a subscriber component subscribes to topics. iSCALE routes messages from publishers to subscribers based on topics they have registered. This allows a component to publish a message to a topic channel that multiple subscribers consume, without the publishing component knowing which process subscribes to it. Subscribers can receive published messages from publishers without knowing what publishers are available. For example, if a new Wizard is added to the system, no configuration is required on the Sentinel server. The only information needed during installation is the network location (host name and tcp port) where sentinel server is located. Once installed, these components provide for protected inter-TOE transfer of data. All TOE components with the exception of the Database communicate over iSCALE The Correlation Engine and Base components, along with DAS, are specialized message-based services known as java containers. A java container is a self-contained functional software entity that runs as java process within a JVM. The Correlation engine collects normalized events from the Wizard Agent Manager, correlates these events to find patterns, and then reports on real-time and historical information which can be viewed in the Sentinel Control Center. The Sentinel Server Base Components is comprised of:

- Watchdog Process: Manages all other Sentinel Server processes.
- Event Statistics Process: Manages Data used by the Active Views in the Sentinel Control Center.
- Data Synchronizer Process: Manages modification of data by multiple users.
- RuleLg Checker Process: Validates the syntax of filter and correlation rule expressions.
- Query Manager Process: Processes the requests for quick query and drill down data from the Control Center and passes the requests to the Data Access Service.

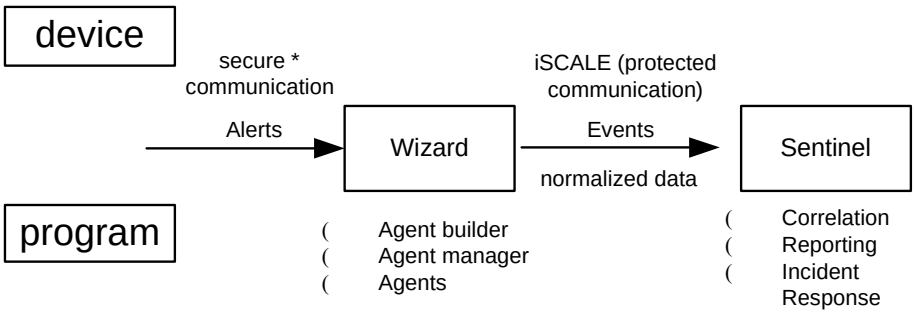

Figure 1 - Overview of Wizard & Sentinel functions

* Figure 1 – Secure implies that, for certain collection methods, e-Security has written SSL-based transports, Cisco IDS (RDEP) and Checkpoint (OPSEC LEA) specifically. All other transports are in clear text. These transport mechanisms are not part of the evaluated configuration.

DAS

DAS (Data Access Service): DAS communicates with the iSCALE message bus to process all events and requests to store configuration information and inserts them into the database. It also receives database query requests, processes it, and replies back. DAS manages the database as an object, in which metadata is defined to the backend database such that DAS does not need to understand protocols or how messages get routed. The operations of DAS include a default data access via JDBC and optionally high-performance event insert strategies using native connectors (i.e., OCI for Oracle 9i and ADO for Microsoft SQL Server).

Sentinel Control Center

Sentinel Control Center provides the central management console to view real-time or historical events and system overview of changes in activity triggered by Agent settings. It also provides administration of users, filters, correlated rules and security event management through incidents.

Database Server

The database server (SQL Server or Oracle) provides user authentication and dedicated storage for audit and event data.

Sentinel Data Manager

The Sentinel Data Manager is a graphical tool used to manage TOE and audit data. It allows the System Administrator to View/Add/Archive/Delete database partitions.

Note: The equivalent command line version of the Sentinel Data Manager is not part of the evaluated configuration.

6.2 Architecture Description

The following Diagram shows the distributed architecture of the e-Security 5.1.1 TOE.

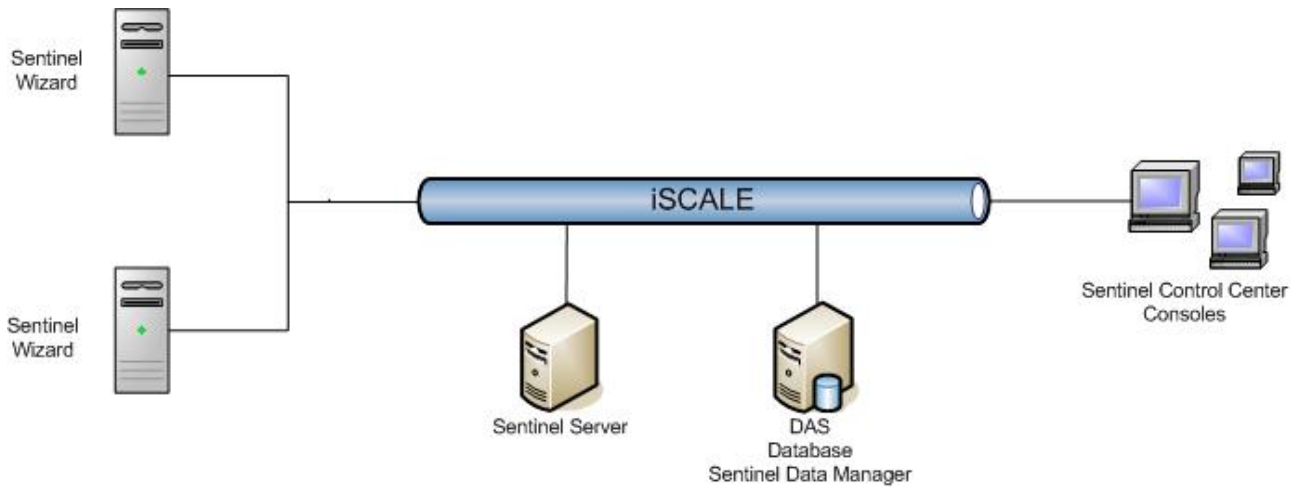

Figure 2 - e-Security Distributed architecture

Physical Boundaries

The TOE will consist of the following software based modules.

- One Sentinel Server.
- One or more Sentinel Wizards
- One or more Sentinel Control Center(s). This component can be installed both locally to the Sentinel Server and remotely.
- One Sentinel Data Manager Utility
- One Data Access Service (DAS)
- One Oracle OR One Microsoft SQL Server database.

The Agents configured and running on a Wizard Agent Manager are simply configuration parameters of the Accept Alerts SFP. They all use the same system

code to operate and perform their function of receiving Enterprise Alert Data and turning it into Enterprise Event Data through a normalization process.

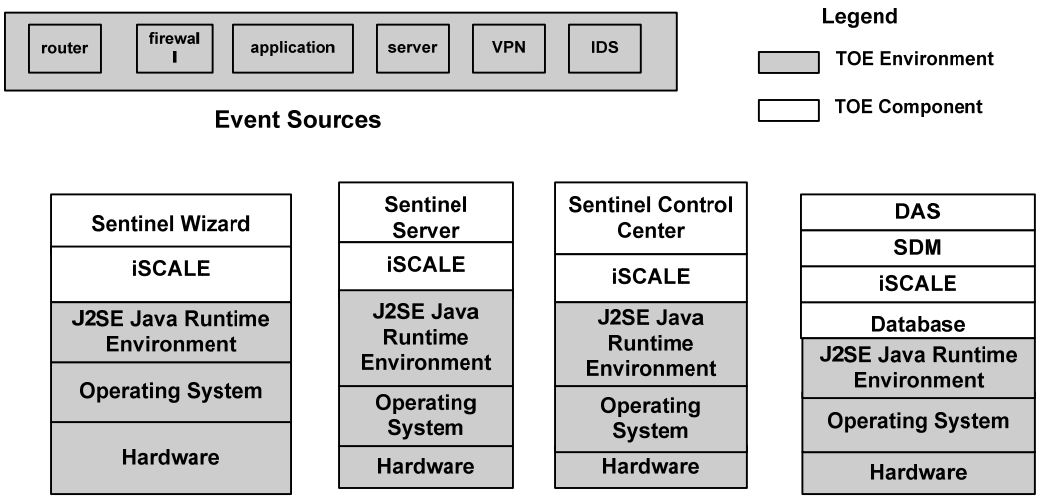

Figure 3 - TOE Boundary

Each physically separated TOE component communicates with each other using a logical communication path managed by iSCALE. The TOE is used inside a secure trusted network. For the purposes of the evaluation, data being generated by devices in the network is considered to belong to the administrator. Hence the Wizard takes this user data in, normalizes it and at this point it has become TOE data.

TOE Physical Components

This table contains versions of the software that are part of the TOE for the environmental requirements to run this software)

Software	Version
Sentinel Server	
Communication Server	Version 5.1.1
Base Services	Version 5.1.1
Correlation Engine	Version 5.1.1
Sentinel Wizard	
Agent Manager	Version 5.1.1
Agent Builder	Version 5.1.1
Sentinel Control Center	Version 5.1.1

Software	Version
Database	
Data Access Service (DAS)	Version 5.1.1
Sentinel Data Manager (SDM)	Version 5.1.1
Microsoft SQL Server -OR- Oracle	Version 2000 Enterprise Edition (SP3a) (Installed in Mixed Mode) * Version 9i Enterprise Edition with 9.2.0.6 mega patch set (32 bit mode) * Oracle Critical Patch Update - April 2006

***** Includes respective database management utility

Table 7 - TOE Physical Components

Environment Physical Requirements

The TOE environment requires the following hardware and software (OS's / versions / patches). The Hardware and Operating System are not part of the TOE. The table is broken out by requirements by TOE component.

Software	Hardware
Sentinel Control Center	
Windows 2000 Professional (SP4) Windows XP (SP1) Windows 2003 SP1 Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster) J2SE Java Runtime Environment 1.4.2	Single 1.1 GHZ CPU (Solaris) Single 3.2 GHZ CPU (Windows) 1 GB RAM
Sentinel Server (Communication Server, Base Services, Correlation Engine)	
Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster) Windows 2000 SP4 Windows 2003 SP1 J2SE Java Runtime Environment 1.4.2	Quad 1.1 GHZ CPU (Solaris) Quad 3.2 GHZ CPU (Windows) 4 GB of RAM

Software	Hardware
Sentinel Wizard (Agent Manager and Wizard Builder)	
Windows 2000 (SP4) Windows 2003 (SP1) Solaris 9 64bit Full Distribution plus OEM Support (May 03/05 Patch Cluster) J2SE Java Runtime Environment 1.4.2	Dual 3.2 GHZ CPU (Solaris) Dual 3.2 GHZ CPU (Windows) 2 GB RAM
Sentinel Database – (Windows/Microsoft SQL Server)	
Windows 2000 (SP4) Windows 2003 (SP1) Microsoft SQL Server 2000 (SP3a) J2SE Java Runtime Environment 1.4.2	Quad 3.2 GHZ CPU (Windows) 4GB RAM
Sentinel Database - (Solaris 9 /Oracle)	
Solaris 9 (May 03/05) Oracle 9i Enterprise on Solaris 9 (9.2.0.6 Patch) J2SE Java Runtime Environment 1.4.2	Quad 1.1 GHZ CPU (Solaris) 4GB RAM

Table 8 – TOE Environment Software and Hardware Requirements

7 DOCUMENTATION

During the course of the evaluation, the CCTL had access to an extensive amount of documentation and evidence.

Configuration Management Documentation

- e-Security Sentinel 5 v5.1.1, Configuration Management for e-Security Sentinel 5 v5.1.1, Version 1.8 ,November 20, 2006

Delivery and Operation Documentation

- Delivery Document for e-Security Sentinel 5, v5.1.1, November 20, 2006, v1.7

- Wrapper Document for e-Security Sentinel 5, v5.1.1, November 20, 2006, v0.6
- e-Security Sentinel 5 v5.1.1_DEL_Verdicts_EAL2 “e-Security_Sentinelv5.1.1_EAL2_ADO_DEL_Cycle3-Verdicts_20061101_Arca-v02.xls”
- e-Security Sentinel 5 v5.1.1_IGS-verdicts_EAL2 “e-Security_Sentinelv5.1.1_EAL2_ADO_IGS_Cycle2-Verdicts_20061030_Arca-Wrapper Document For e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006
- Sentinel 5.1.1 Install Guide For Solaris and Windows Volume I of V, September, 2005.
- Sentinel 5.1.1 Product Release Notes

Development Documentation

- Wrapper Document For e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006.
- Informal functional specification for e-Security Sentinel 5 v5.1.1, v.0.12, November, 20th, 2006.
- High Level Design for e-Security Sentinel 5 v5.1.1, v.0.08, November 20th, 2006.

Guidance Documentation

- E Sentinel 5.1.1 Install Guide For Solaris and Windows Volume I of V, September, 2005.
- Wrapper Document For e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006.
- Sentinel 5.1.1 Install Guide For Solaris and Windows Volume I of V, September, 2005.
- Sentinel 5.1.1 User's Guide For Solaris and Windows Volume II of V, September, 2005.
- Sentinel 5.1.1 Wizard User's Guide For Solaris and Windows Volume III of V, September, 2005
- Sentinel 5.1.1 User's Reference Guide For Solaris and Windows Volume IV of V, September, 2005.
- Sentinel 5.1.1 Product Release Notes

Tests Documentation

- Test Plan and Coverage Analysis For e-Security Sentinel 5 v5.1.1, v.0.7, November 20th, 2006.
- E-Security Sentinel 5 v5.1.1 Team Test Plan Version 5, 21 November 2006

Vulnerability Assessment Documentation

- Vulnerability Analysis for e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006.

Security Target

- E-Security Sentinel 5 v5.1.1 Security Target, Version 0.34 Final, 20 November 2006.

8 TESTING

The E-Security Sentinel 5 v5.1.1 Team Test Plan Version 5, 21 November 2006, provided the testing evidence for the evaluation of the TOE. The plan outlined the testing of the TOE's security functions to demonstrate that the TOE behaves as specified in the e-Security 5.1.1 design documentation and in accordance with the TOE security functional requirements in the ST. The testing approach was non-automated, i.e., manual input to a GUI.

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

8.1 Test Environment and Configuration

The test environment for e-Security Sentinel 5 v5.1.1 is a simulated network environment with four connected machines. The evaluation team used the vendor supplied testing environment as a basis for conducting its independent tests. The testing was done manually through the Administrative interfaces available to the TOE users. Each test was mapped to the SFRs. Each test and the test procedure was described in detail so that it was reproducible. For all tests, standard installation procedures were used as per the installation guides provided with the TOE.

8.1.1 TOE Identification

The evaluation team verified that the TOE's components were labeled consistently with their respective unique identifier. All test documentation had been labeled this way (as described in the CM document), as well.

8.1.2 TOE Installation

The evaluation team used the e-Security Sentinel 5 v5.1.1 installation manuals to ensure that all steps needed to bring the TOE up into a known state on each platform are used and confirmed. The TOE was installed in accordance with its installation procedures to ensure that these procedures would yield an implementation consistent with the ST. Each TOE external interface was described in the design documentation (e.g., Functional Specification) in terms of the relevant claims on the TOE that could be tested through the external interface. The ST and the Functional Specification (FSP) were used to demonstrate test coverage for security functional requirements and security relevant TOE external interfaces. A subset of SFRs and TSFIs was tested.

Testing involved installation and configuration of a TOE as described in the vendor test documentation. The evaluation team ensured that the installation was consistent with the configuration identified in the ST. All systems were installed by the evaluation team from original media, using default configurations or custom configurations where expressly required by TOE installation guidance. The results of this (installation and configuration) portion of testing were documented in the ADO_IGS portion of the Evaluation Technical Report for e-Security Sentinel 5 v5.1.1.

8.1.3 TOE Configurations

The configuration of the TOE that was used to test the TOE was created by the CCTL based on vendor testing environment provided in test documentation. This configuration is documented in Figure 1 below, and was used to execute the test sets. There are two differences in the environment setup by the evaluation team from the environment in the figure below used by the vendor. The evaluation team used Windows 2003 SP1 platform for machines A, B & C below. The evaluation team named the Machines A to D as ESEC-SVR1 to ESEC-SVR4. There are no other differences between the two testing environments. The CCTL used Microsoft SQL Server as the database repository.

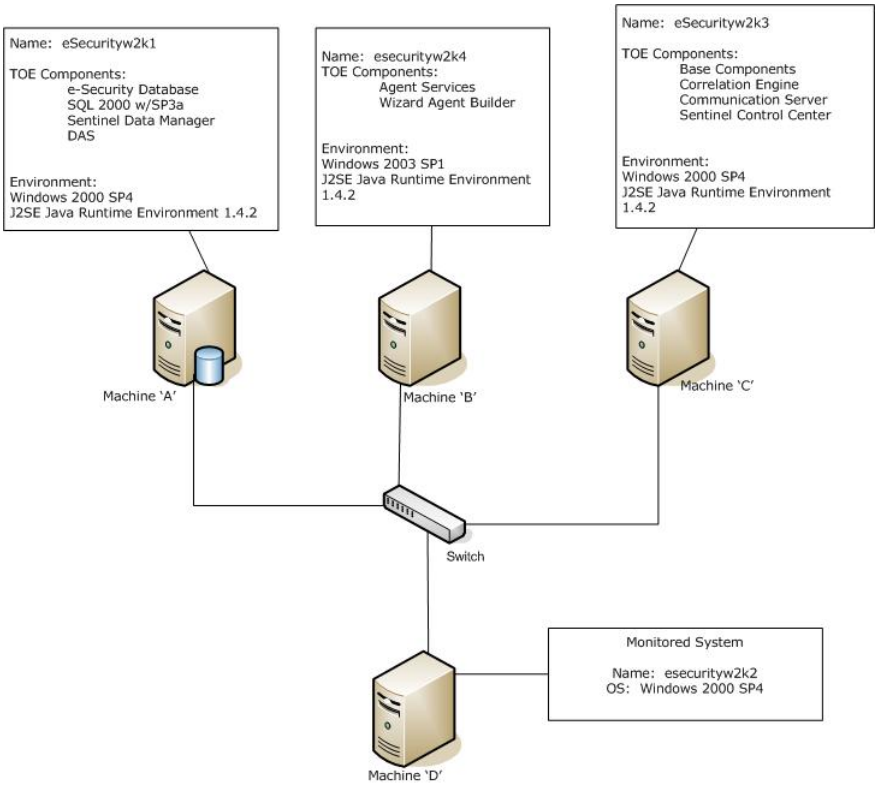

Figure 4: e-Security Sentinel 5 v5.1.1 testing environment

8.2 Test Coverage Analysis

The test team's approach to determining coverage was to verify that the vendor tests the security mechanisms of the TOE, exercising the external interfaces to the TOE and documenting the results. Each TOE external interface is described in design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, High-Level Design (HLD), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of a subset of SFRs for all appropriate EAL2 requirements for a subset of security relevant TOE external interfaces.

8.3 Independent Testing

For Independent testing, a set of functional tests designed to augment the vendor testing, was run by the lab. The evaluation team ran tests for 6 of 6 TSFs claimed in the ST. The evaluation team verified that these functions worked with proper inputs. The evaluation team also verified that these functions do not work with improper inputs. In addition, an independent penetration test and vulnerability tests were designed and tested. The results are detailed in section 4.4 of test plan document.

9 RESULTS OF THE EVALUATION

The evaluation was conducted based on the Common Criteria (CC), Version 2.3, and the Common Evaluation Methodology (CEM), Version 2.3. The evaluation confirmed that e-Security Sentinel 5 v5.1.1 is compliant with the Common Criteria Version 2.3 functional requirements (Part 2) and assurance requirements (Part 3) for EAL2.

The details of the evaluation are recorded in the CCTL's Evaluation Technical Reports (ETRs), which consist of the following documents. A separate ASE (Security Target Evaluation) ETR was produced for the ST. Evaluation results for the remaining assurance families are presented in separate ETR documents for each family:

- **ASE (Security Target Evaluation):** ASE Evaluation Technical Report for e-Security Sentinel 5 v5.1.1
- **ACM (Configuration Management Evaluation):** ACM_CAP.2 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
- **ADO (Delivery and Installation Evaluation):** ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for e-Security, version 5.0, November 21, 2006.
- **ADV (Functional Specification, High Level Design, and Correspondence Evaluation):** ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
- **AGD (Administrative and User Guidance Evaluation):** AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.

- **ATE (Functional Testing, Testing Coverage, and Independent Testing Evaluation):** ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
- **AVA (Vulnerability Analysis and Strength of Function Evaluation):** AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.

The validator followed the procedures outlined in the CCEVS Scheme Publication #3, *Guidance to Validators of IT Security Evaluations*. The validator observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator's observations support the evaluation team's conclusion that the e-Security Sentinel 5 v5.1.1 meets the claims stated in the Security Target.

The following components are not included in the Target of Evaluation (TOE), and have not been evaluated:

- Sentinel Advisor
- Third party software BusinessObjects Enterprise XI
- HP Service Desk
- Remedy
- Command Line version of the Sentinel Data Manager

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

11 SECURITY TARGET

The Security Target is identified here by reference.

- E-Security Sentinel 5 v5.1.1 Security Target, Version 0.34 Final, 20 November 2006.

12 BIBLIOGRAPHY

The validator used the following documents to produce this Validation Report:

1. ACM_CAP.2 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
2. ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for e-Security , version 5.0, November 21, 2006.
3. ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
4. AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
5. ASE Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, November 21, 2006.
6. ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
7. AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for e-Security Sentinel 5 v5.1.1, version 5.0, November 21, 2006.
8. Common Criteria Evaluation and Validation Scheme for IT Security, Scheme Publication #3, Version 1.0, January 2002.
9. Common Criteria for Information Technology Security Evaluation, Parts 1-3, Version 2.3, August 2005.
10. Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.
11. e-Security Sentinel 5 v5.1.1 ACM Verdicts, “e-Security_Sentinelv5.1.1_EAL2_ACM_CAP_Verdicts_Cyle3_103106_Arca-v02.xls”.
12. e-Security Sentinel 5 v5.1.1 ACM Verdicts, “e-Security_Sentinelv5.1.1_EAL2_ACM_CAP_Verdicts_Cyle3_103106_Arca-v02.xls”.
13. e-Security Sentinel 5 v5.1.1, Arca CCTL Team Test Plan, Version 5.0, November 21, 2006.
14. e-Security Sentinel 5 v5.1.1 ATE_COV_FUN document “e-security Sentinel & Wizard v5.1.1 ATE_FUN v.07.doc”.
15. e-Security Sentinel 5 v5.1.1, Configuration Management for e-Security Sentinel 5 v5.1.1, Version 1.8,November 20, 2006.
16. e-Security_Sentinel 5 v5.1.1_EAL2_ATE-COV-FUN_Cycle3-verdicts_200611906_Arca-v03.xls”.

17. e-Security Sentinel 5 v5.1.1 _FSP_Verdicts “e-Security_Sentinelv5_EAL2_ADV-FSP_Cycle6-verdicts_20061009_Arca-v02.xls”.
18. e-Security Sentinel 5 v5.1.1 Functional Specification, Version 0.12.
19. e-Security Sentinel 5 5.1.1 High Level Design, Version 0.8, 20 November 2006.
20. e-Security Sentinel 5 v5.1.1 _HLD_Verdicts “e-Security_Sentinelv5_EAL2_ADV-HLD_Cycle5-verdicts_20061009_Arca-v02.xls”.
21. e-Security Sentinel 5 v5.1.1_SOF_Verdicts_EAL2 “e-Security_Sentinel5v5.1.1_EAL2_AVA_SOF_Cycle2_Verdicts_20061026-v03.xls”.
22. e-Security Sentinel 5 v5.1.1 Security Target, v.034, November 20th, 2006
23. e-Security Sentinel 5 v5.1.1 ST Verdicts Sheet “e-Security_Sentinel&Wizard_v5.1.1_EAL2_ST_Cycle12-20061009-ArcaTeam-v02.xls”.
24. e-Security Strength of Function Analysis for e-Security Sentinel 5 v5.1.1, October 26, v0.3.
25. e-Security Sentinel 5 v5.1.1_VLA_Verdicts_EAL2 “e-Secuirty_Sentinel5v5.1.1_EAL2_AVA_VLA_Cycle2_Verdicts_20061031-v01.xls “.
26. e-Security Vulnerability Analysis for e-Security Sentinel 5 v5.1.1, October 27, 2006, v0.5.
27. Informal functional specification for e-Security Sentinel 5 v5.1.1, v.0.12, November, 20th, 2006.
28. Sentinel 5.1.1 Install Guide For Solaris and Windows, September 2005.
29. Sentinel 5.1.1 User's Guide, for Solaris and Windows, September 2005.
30. Sentinel 5.1.1 User's Reference Guide for Solaris and Windows, September 2005.
31. Sentinel 5.1.1 Product Release Notes .
32. Sentinel 5.1.1 Wizard User's Guide for Solaris and Windows, September 2005.
33. Strength of Function Analysis for e-Security Sentinel 5 v5.1.1, v.0.4 November 20th, 2006.

34. Test Plan and Coverage Analysis For e-Security Sentinel 5 v5.1.1, v.0.7, November 20th, 2006.

35. Vulnerability Analysis for e-Security Sentinel 5 v5.1.1, v.0.6, November 20th, 2006.

36. Wrapper Document for e-Security Sentinel 5 v5.1.1, v.0.6, November 20, 2006.