SecureVue v3.6.3 CP1

Security Target

Version 1.7

May 8, 2013

Simplified Security
Intelligence

Prepared By

CYGNACOM
SOLUTIONS

7925 Jones Branch Drive♦Suite 5200 ♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Table of Contents

Section **Page**

Table of Tables and Figures

Table / Figure **Page**

1 Security Target Introduction

1.1 Security Target Reference

ST Title: SecureVue, Version 3.6.3 CP1 Security Target

ST Version: Version 1.7

ST Date: May 8, 2013

ST Author: CygnaCom Solutions

1.1.1 References

Table 1-1 provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	***ID***
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	[CC]
eiQ SecureVue V3.6 User Guide	[EIQ-UG]
eiQ SecureVue V3.6 Deployment Guide	[EIQ-DEP]
eiQ SecureVue V3.6 Setup Guide	[EIQ-INSTALL]
SecureVue FIPS 140-2 Level 2 Security Policy, Dec 2008	[EIQ-FIPS]
SecureVue, Version 3.6 Security Target	[ST]
eIQ_SecureVue-ADV_FSP.2 Supp v1.0_Oct 15 2012.xls	[SecureVue GUI]

1.2 TOE Reference

TOE Identification: SecureVue, Version 3.6.3 CP1

TOE Vendor: EiQ Networks, Inc

1.3 TOE Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for SecureVue. The Target of Evaluation (TOE) is being evaluated at assurance level EAL2 augmented with ALC_FLR.2.

SecureVue from EiQ Networks is an IT security, risk and audit management platform that combines security information management (SIM) with governance, risk and compliance (GRC) to improve operational efficiency and reduce management complexity. Using an integrated model, SecureVue collects, correlates, archives, analyzes and reports on critical security and compliance data. Through end-to-end correlation, SecureVue transforms volumes of log, vulnerability, configuration, asset, performance, and flow data to automate incident identification and security breaches. Built-in network behavioral anomaly detection (NBA) automatically profiles flow data to identify anomalies. Additionally, a compliance library maps directly to specific regulations, best practices and control frameworks.

1.3.1 TOE Type

SecureVue from EiQ Networks combines enterprise network and security management with IT governance, risk and compliance (GRC). This is a software only TOE which requires the Basic license, which is based on number nodes being monitored, and a License for the Compliance policy package(s) required.

1.3.2 TOE Environment Dependencies

SecureVue can be installed in 3 deployment models: Standalone, Distributed, and Tiered. In the Standalone model the main components: Central Server and Data Collector can be installed on the same physical hardware or on separate machines. The Distributed model introduces a third component called the Data Processor. The Data Processor is installed on a separate machine and is in-between the Central Server and the Data Processor. The Tiered model allows for multiple servers (Global, Regional, Local Serverrs and Data Processors to support large enterprise deployments. All modes support high availability configuration options that are not in scope of this evaluation.

Agents are standalone executables to support the collection of information on a managed Windows or UNIX node. These Agents, which are installed directly on the managed node, are referred to as OSAgents.

The evaluated configuration of SecureVue will be a standalone network deployment (no high availability) that includes the Central Server and Data Collector installed on separate hardware platforms, and Agents (Window and UNIX Host OS).

These components require the following additional hardware/software from the operational environment:

Recommended System Requirements for SecureVue Server(s)

The SecureVue Central Servers must meet the following minimum system requirements:

- **Processor:** Dual Xeon Quad Core 2.0 GHz or higher
- **Memory:** 16 GB or higher
- **Storage:** 1 TB or higher on 15K RPM SCSI drives
- **Operating System:** 64-bit Windows 2003 SP2, Windows 2008 Server, Windows 2008 R2
- **Java:** Java (JRE) 1.6 r30 or higher
- Microsoft Office 2003 or 2007 is required to generate Microsoft Word or Excel reports.

SecureVue **Data Collector** minimum system requirements:

- **Processor:** P4 Processor 2.4 GHz or higher
- **Memory:** 1 GB or higher
- **Storage:** 50 GB or higher on 7200 RPM SATA drives
- **Operating System:** Windows Server 2003 SP2 or Windows Server 2008 or RedHat Enterprise Linux 5, CentOS (x86_64)

Note A: SecureVue v3.6 Data Collector is supported to run on VMWare ESX 4.x and ESXi platform but is out of scope of this evaluation.

Note B**:** For IPv6 systems or data collection, EiQ Networks' recommends using Windows Server 2008 as the operating system for SecureVue data collector.

SecureVue **Windows Agent** minimum system requirements:

Processor: P4 Processor 1.8 GHz or higher
Memory: 1 GB or higher
Storage: 500 MB or higher on 7200 RPM SATA drives
Operating System: Windows XP, Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Vista.

SecureVue **UNIX/Linux Agent** minimum system requirements:

Processor: P4 Processor 1.8 GHz or higher
Memory: 1 GB or higher
Storage: 500 MB or higher on 7200 RPM SATA drives
Operating System: RedHat-5 and above or Fedora OS, AIX 5.3, AIX 6.1, CentOS (x86_64), SUN Solaris SunOS_5.10

Optional third party servers that support the security functionality defined below:

- RADIUS Server can be integrated with the TOE to provide for an external authentication mechanism.
- Active Directory Server can be integrated with the TOE to import users and then invokes the AD as an external authentication mechanism.
- SNMP Server is needed to support the sending of an SNMP trap alert from the TOE.
- SMTP Server is needed to support the sending of an email alert from the TOE.

Hardware, OS, additional software (Java, MS office), and third party servers defined in this section are not in scope of the evaluation but were used to support the evaluation.

NOTE: The TOE does not support generic LDAP directory mechanisms. The TOE only claims integration capability with Active Directory and RADIUS. The TOE uses LDAPv3 to communicate with the AD server in order to import users.

1.4 TOE Description

1.4.1 Acronyms

This ST uses terms with the same meanings as given in the Common Criteria. Other terms, or terms with specific meaning for this ST are listed herein:

Table 1-2: Product Acronyms/Terminology

Acronym	Definition
API	Application Programming Interface that uses Remote Registry to interface
CPMI	Check Point Management Interface
DAS	Direct-attached-storage system
Device Group	A collection of devices with a unique name that can then be assigned to a user or user group
Devices	Any network asset such as a host, router, switch, firewall etc.
Forensics	Forensics analysis involves recording and analysis of network events in order to discover the source of security attacks or other problem incidents.
FTP	File Transfer Protocol
FTPS	(also known as *FTP Secure* and *FTP-SSL*) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.
ICMP	The Internet Control Message Protocol is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached. Notable exception to this is the Ping and TraceRoute user commands
IP	Internet Protocol is a protocol used for communicating data across packet-switched network.
IT Governance	IT Governance Establishes Decision Structures And Tracking Mechanisms
IT Risk Management	IT Risk Management Helps Mitigate Adverse Effects And Identifies Opportunities
IT Compliance	IT Compliance Establishes And Monitors IT Controls (Auditor function: compare real vs set of rules that determine compliance)
MIB	Management information base is a type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
NBA	Network behavior and Anomaly
NAS	Network-Attached-Storage

Acronym	Definition
Network Management	Network Management covers a wide variety of definitions. For this document it is scope to these terms. • **Security:** Ensuring that the network is protected from unauthorized users. • **Performance:** Eliminating bottlenecks in the network. • **Reliability:** Making sure the network is available to users and responding to hardware and software malfunctions. Also see IT Governance, IT Risk, and IT Compliance
Policies	A Policy is a systematic set of statements to govern the upcoming decisions and actions of the user.
Profiles	A profile is a set of instructions identifying the locations of the device logs, how data must be accessed, the method followed to analyze data, how IP addresses must be resolved, and customization of reports.
SAN	Storage-Area-Network
SIM	Security Information Management
SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
SMTP	Simple Mail Transfer Protocol is an Internet standard for electronic mail transmission across Internet Protocol networks.
SNMP	Simple Network Management Protocol a communication protocol between management stations, such as consoles, and managed objects (MIB objects), such as routers, gateways, and switches, makes use of MIBs.
SSL	Secure Sockets Layer, now Transport Layer Security, a communications protocol
TCP	Transmission Control Protocol is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components, with Internet Protocol (IP), of the suite, so that the entire suite is commonly referred to as *TCP/IP*.
TLS	Transport Layer Security and its predecessor, Secure Sockets Layer, are cryptographic protocols that provide security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Telnet	is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility.
Topology	Topology is the schematic description of the arrangement of a network, including its nodes and connecting lines.
User Group	Equivalent of user roles. A user is assigned to a user group (administrator, power-user, user) which then dictates to the TSF which functions and TSF data is available for the authenticated user to access. One user, assigned to the administrator user group, is also selected for the role of Super Admin.
WMI	Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

Table 1-3: CC Acronyms/Terminology

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.4.2 Product Description

SecureVue provides effective real-time management of all log, vulnerability, configuration, asset, performance and Network behavior and Anomaly (NBA) data collected from network devices, systems and applications. Collected data is then normalized across disparate devices, aggregated into a database and correlated for monitoring, alerting, reporting and forensic tasks. The evaluated configuration of SecureVue will be a standalone network deployment that includes the Central Server and Data Collector installed on separate hardware platforms, and Agents (Window and UNIX Host OS).

The remainder of the ST will only describe the standalone configuration (no high availability) and its components. The platforms that house the Central Server and/or the Data Collector software are expected to be dedicated to the functionality of the TOE (i.e. non-TOE-supporting software should not be installed).

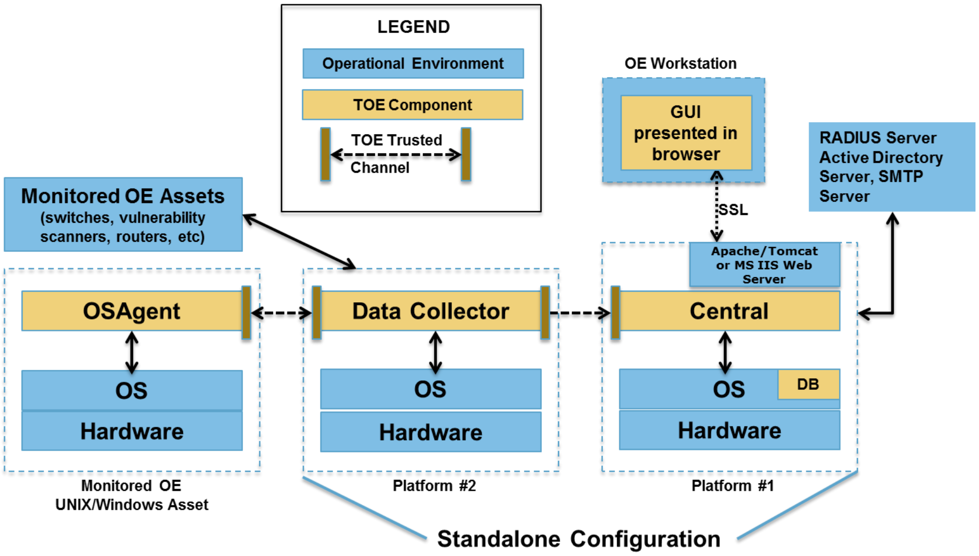


Figure 1: Scope of SecureVue

1.4.3 TOE Components

1.4.3.1 Central Server

The SecureVue Central Server is the nerve center of the solution performing all the data correlation and analytics, alert configuration, forensic analysis, GRC, and data archive management functions. The Central Server is responsible for the following security features: audit generation and review, management access control enforcement, identification and authentication (natively or invoking an external mechanism), secure role based management via web-based GUI, protection of TSF, trusted communication between components, trusted communications between Central Server and Browser for management GUI, management of monitored network, risk and compliance assessment of managed network.

This component is installed on its own platform as indicated in the figure above. The platform and OS is responsible for protecting the stored audit and TOE executables.

1.4.3.2 Data Collector

The Data Collector interfaces between the Central Server and all the network devices, systems and applications within a SecureVue deployment. It is responsible for collecting log, vulnerability, configuration, asset, performance and NBA data automatically from all configured network devices, compressing them into delta files and sending to the Central Server for correlation, display, forensics, reporting and archiving. The Data Collector automatically updates the delta files (extracts of an original log file that only contains data that has been logged since the last update) to the Central Server on a regular basis without intervention from the administrator. The collected data is transferred to Central server in encrypted format by using Central Server's provided unique communication key.

The Data Collector is responsible for the following security features: collecting network information from specified assets, trusted communication with central server and agents. The Data Collector is operationally managed by the Central server via the Central server's web browser management GUI.

This component will be installed on its own platform as indicated in the figure above.

1.4.3.3 Agents

An Agent (OSAgent) is an alternate way to collect host data for use in SecureVue. By installing the agent on an enterprise Windows/Linux asset, a user can collect Windows/Linux host data from that host. The Agent has the additional capability to monitor changes on folders, files, registry (Windows only) and USB devices in real-time.

NOTE: This host/asset could be considered hostile as the TOE administrator may not have direct control over this asset. This machine would be a multipurpose machine with non-administrative personnel having access and control over this machine.

The OSAgent keeps polling the DC every 5 minutes and in response the DC will send updates to OSAgent as requested in GUI, like adding/deleting/editing policies, changing run level, disabling agent etc. The collected agent data is transferred to DC in encrypted format by using DC provided unique communication key.

1.4.3.4 User Interfaces

1.4.3.4.1 Web-based graphical user interface

The SecureVue user interface is a web based graphical user interface through which all operational management and operational functions for the TOE are accessed. This interface is used by all account holders for access to the TOE. The capabilities available through the interface are restricted by a role-based Management Access Control policy. The GUI is used to configure and manage both the Central Server and Data Collector. The Data Collector's configuration and collection policies are created on the Central Server and then pushed to the Data Collector for implementation. The GUI does not directly communicate with the Data Collector.

The GUI is accessed via a standard web browser, such as Internet Explorer or Mozilla Firefox via https://serverIP. The interface is only accessible/displayed after successful Identification and Authentication.

1.4.3.4.2 Win32 executables

The TOE provides a Win32 executable (DCConf.exe) to re-configure the Data Collector parameters Start > Programs > SecureVue >Configure Data Collector. These parameters include the Data Collector IP address, SecureVue Server to report to, logfile maintenance, ports to listen, special configurations for Check point, Cisco IDS File ZSources, ISS, Profiler, and SNMP Trap and backup Data Collector information to name a few. The DCConf.exe does not require additional login after user has been authenticated on the platform. All features would be used outside the normal scope of operation or during installation/maintenance. Operationally the Data Collector is managed via the Central server's GUI through the Central Server. Therefore, for the purpose of this evaluation this executable was not tested and considered out of scope.

1.4.4 Trusted Channel between TOE components

The TSF includes a trusted communication infrastructure that provides trusted communication channels among its separately installed components. The 'trusted communication channel' ensures the two end points, (i.e., two components) are authenticated, their identity is associated to the data they transfer and that the data transferred is protected from modification and disclosure. The trusted communication channel between TOE components is established even if the components are installed on the same platform such as the Central Server and Data Collector can be installed on same platform.

Establishment of these trusted communications channels depend on the functionality of both the TOE (crypto module) and the Operational Environment (network infrastructure and host TCP/IP protocols)

SecureVue uses and provides the FIPS 140-2 validated (Certificate #1051) OpenSSL cryptographic module Version 1.2. The services used by SecureVue are Key Transfer, Communications, Database, File/Password-encryption, and Decryption of data between TOE components.

1.4.5 Data

The TSF data and includes the systems parameters set by Administrators to configure the security of the TOE, TOE user account data, data collected/received by the Data Collector, and any collected/received data from third-party source such as vulnerability scanners or SNMP agents. Collected/Received data becomes TSF data immediately upon receipt of this data.

For the purposes of this ST and the definitions of the security management SFR identified in Section 6 the TSF data will be classified into two types:

Administrative Data – Server configuration parameters, User Management (attributes), scoping of Device and Host for monitoring and management, the Data Collection configuration, licenses, all policies, audit trail etc. Administrative Data types include Meta Data (configuration data for TOE and Policies) and Audit logs.

Operational Data – Collected Data, Analyzed Data, and TOE generated data such as Alerts and Tickets, etc.. Operational Data types include the Raw Data, Forensic data, Forensic index, Report Data in db.

Any reports exported to the system are not subject to TOE access control. They are subject to the OS System's access control policy.

1.4.6 Users

The TOE supports 5 types of default user roles plus the ability to create custom roles:

- **Super Administrator:** There has to be one Super Administrator (also referred to as Super Admin) to manage the TOE. The Super Administrator is used to install the TOE. Once the TOE is installed the functionality of the Super Administrator is the same as the Administrator. However, when this role is assigned to an "administrator" user, the TOE prevents that user account from being deleted.
- **Administrator:** An Administrator can manage entire application with exclusive rights to control, create, delete, and edit even other users with customized privileges. Users from this group have most rights over SecureVue GUI. Users from this group can also initiate FIPS SELF-TEST and re-generate Communication Key commands. Only one administrator can be assigned the Super Administrator role.
- **Power User:** Users in this group can be classified as read-only admins. They cannot manage Devices, Hosts, Groups, Users, Topology and Licenses. The Power User can create, edit, delete and view profiles, however, access to Collection-based policies and generation of file-based profiles is restricted.
- **User:** User accounts in this group can only generate all or few instant reports sections depending on the privileges assigned in the user policy. This role's access to reports and functions can only be customized by the Super Admin.
- **Alert User:** User accounts in this group have access to just the Alerts portal in the main console. Can only view, acknowledge, and clear alerts to which they have been granted access. Cannot edit, copy, delete, or create alerts, and cannot access the rule templates.
- **Custom User Roles:** Administrators can create custom users roles by assigning privileges and permissions to existing roles or completely new roles. For example the Alert user is a custom user role with only have Alert privileges.

1.4.7 TOE Documentation

EIQ SecureVue 3.6.3 Deployment Guide,	March 6, 2013
EIQ SecureVue 3.6 User Guide,	May 14, 2012
EIQ SecureVue 3.6 Release Notes,	May 29, 2012
SecureVue® v3.6 CC Supplement Guide,	May 8, 2013
Release Notes SecureVue v3.6.3,	December 28, 2012
Release Notes SecureVue v3.6.3 CP1	March 6, 2013

1.4.8 Physical Scope of the TOE

The physical boundary of the TOE includes the entire product as commercially available from the developer.

The evaluated configuration of SecureVue will be a standalone network deployment (no high availability) that includes the Central Server and Data Collector installed on separate hardware platforms, Host OS Agents (Window, and UNIX), and user documentation.

The following subsection presents a bullet list of what is included in the TOE and what is excluded from the TOE.

1.4.8.1 In-Scope

TOE Components provided in install packages:

- Central Server
    - Web Based GUI
- Data Collector
- Host OS Agents (UNIX, Windows)

1.4.8.2 Out-of-Scope

TOE functionality considered out of scope

- High availability option
- Data Collector Configuration (DCConf.exe)
- Distributed and tiered deployments

OE software requirements/options provided on the installation disk:

- Apache Server Version 2.2.22 with OpenSSL (different from crypto module in the TOE software used for trusted communication between TOE components)

  Note: The evaluator verified that the trusted channel used between the browser and the Central Server (handshaking and cipher suite) uses FIPS certified algorithms.
- Tomcat Server Version 7.0.26.0

OE support not provided by TOE vendor:

- Microsoft IIS Web Server (optionally used instead of Apache server) v7.0 minimum
- Host OS for any of the TOE components
    - Network Protocols
- Third party software loaded on TOE
    - Java (JRE) 1.6 or higher
    - MS-Office (to generate reports in WORD or EXCEL formats)

  - Adobe Acrobat Reader 6.0 or higher (to view reports in PDF format)
- RADIUS Server
- Active Directory Server
- SNMP Server
- SMTP Server
- Any third party software in the IT Environment that supplies TOE with data
  - Profilers such as IDP, and NetFlow
  - Vulnerability scanners, such as Nessus
  - OS
  - Workflow Ticket management systems, such as Remedy
- Network infrastructure (switches, dns, dhcp, managed assets etc.)
- Host hardware for any of the TOE components

1.4.9 Logical Scope of the TOE

The security functionality provided by the IT Environment is also described in Section 4.2 Security Objectives for the Operational Environment. Section 7 TOE Summary Specification gives detailed information on how these security functions that make up the logical scope of the TOE are implemented..

The TOE provides the following security functionality:

- **Audit Generation and Review –** The Central Server generates its own audit for security events and administrator/user events that are performed. To view the audit records an administrator can use either the Administration tab → Diagnostics which has several options to view all user activity or search from the ForensicVue tab. These viewing functions give the administrator the ability to custom query (search and sort) the audit data but not modify or delete.
- **Management Access Control –** The Central Server implements an management access control policy based on user attributes and Roles to provide restricted administration. The management access control decision is manifested in the unrestricted or restricted presentation of the GUI's functions. The Data collectors completely rely on the OS for access control protection.
- **Identification and Authentication –** The Central Server enforces I&A prior to allowing any access to the GUI and TSF data. The TOE provides a native password capability that supports user lockout failure handling. The TOE also interfaces with:
  - the TOE's host OS to import local MS Windows users into the TOE and then invokes the OS for authentication decision for those user(s).
  - a Microsoft Active Directory (AD) server to import the external users into the TOE and then invokes the AD server to make the I&A decision for those user(s).
  - a RADIUS Server for the I&A decision (no import functionality).

The Central server is responsible for enforcing the I&A decision made natively or received from the configured external authentication mechanism. The OS, AD server, and RADIUS server are not in the scope but the TOE enforcement of the authentication decision and import services are.

The hardcoded native Password policy includes a defined lockout threshold along with a time interval (5 minutes) for which the number of failed logon attempts (3) can happen before user account is locked for a period of time (5 minutes).

- **Monitoring and Management of Network –** The TOE provides network monitoring and management IT network assets including: scheduling the collection of network management and security data, storing uploaded collection data, evaluation of the collected data, and sending notifications to appropriate personnel for significant events in the assessment process.
- **Risk and Compliance Assessment –** The TOE provides risk and compliance assessment of IT network assets including: collection of asset data, evaluation of the collected data, and sending notifications to appropriate personnel for significant events in the assessment process.
- **Secure Management –** The Central Server implements a web based GUI to provide the users with role based security functionality.
- **Trusted Channel –** Trusted communications between the distributed TOE components is supported via the operational environment network infrastructure and protocols. SecureVue uses and provides the FIPS 140-2 validated (Certificate #1051) OpenSSL cryptographic module Version 1.2 for the Key Transfer, Communications, Database, File/Password-encryption and decryption services. This module is contained in the Central server, Data Collector, and Agents.

  Communications to the browser is also encrypted. However, it uses another instantiation of OpenSSL that comes with Apache Server or uses the MS crypto module that comes with MS IIS web server. In either case, they are not the same as the FIPS certified cryptographic module that comes with the product.

  Note: The conformance to these cryptographic standards will not be included in the scope of the evaluation.
- **Protection of TSF *(TSF self-test)* –** The Central Server performs a number of power-up and conditional self-tests to ensure proper operation of the cryptographic module. Power-up tests include cryptographic algorithm known answer tests and integrity tests. The integrity tests are performed using a HMAC-SHA-256 digest calculated over the object code of SecureVue. Power-up tests are run automatically when the cryptographic module is initialized. Additionally, power-up tests may be executed at any time by the administrator requesting the cryptographic module to force re-run of self-tests.

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant. The assurance requirements contained in this ST meet EAL 2 augmented with ALC_FLR.2 as defined in the Common Criteria version 3.1 r3. The SecureVue product meets the requirements of this ST and provides for a medium level of robustness. Under the *Arrangements on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Securit*y, only CC requirements at or below EAL 4 are mutually recognized.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST claims conformance to EAL2 augmented with ALC_FLR.2.

2.4 Cryptographic Standard

SecureVue uses FIPS 140-2 validated (Certificate #1051) OpenSSL cryptographic module Version 1.2.

FIPS 140-2 validation certification for OpenSSL is available at:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1051.pdf

3 Security Problem Definition

This section defines the expected TOE security environment in terms of the threats, security assumptions, and the security policies that must be followed for the high robustness TOE.

3.1 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are as follows:

Table 3-1: Assumptions

Item	Assumption ID	Assumption Description
1	A.Admin	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
2	A.Manage	It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.
3	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.
4	A.Physical	It is assumed that the TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
5	A.ProtectComm	It is assumed that those responsible for the TOE will ensure the communications between the TOE components and remote users are protected to the level required for the operating environment.
6	A.ProtectDB	It is assumed that those responsible for the TOE will ensure that data stored in the databases used by the TOE will be protected from unauthorized access via the IT Environment interfaces.
7	A.ProtectFiles	It is assumed that those responsible for the TOE will ensure executable and data files used by the TOE will be protected from unauthorized access via the IT Environment interfaces.
8	A.ProtectPwd	It is assumed that users will protect their authentication data.

3.2 Threats

The TOE addresses the following threats:

Table 3-2: TOE Threats

Item	Threat ID	Threat Description
1	T.AssetRisks	Security risks, vulnerabilities and non-compliance may exist on the IT network assets that the TOE assesses, leading to a compromise of those assets.
2	T.Intercept	An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.

Item	Threat ID	Threat Description
3	T.Masquerade	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources via the TOE interfaces.
4	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
5	T.NoPrivilege	An authorized user may gain access to management functions or TSF data for which they have no privilege, resulting in the TSF data being compromised.
6	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

3.3 Organizational Security Policies

None.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.Access	The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.
2	O.Analyze	The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.
3	O.Attributes	The TOE will be able to store and maintain user attributes used for management access control decisions/enforcement.
4	O.Audit	The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.
5	O.Collect	The TOE will collect configuration data from the IT network assets.
6	O.CryptoComm	The TOE will provide cryptographic functions for secure communications between TOE components.
7	O.CryptoVerify	The TOE will provide a mechanism to verify the integrity and correct operation of the cryptographic modules during initialization and upon administrative execution.
8	O.Manage	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.
9	O.Notify	The TOE will notify responsible personnel when designated events occur in the assessment process.
10	O.Password	The TOE will be able to support an administrator defined password policy.
11	O.ProtectAuth	The TOE will provide protected authentication feedback.
12	O.RobustTOEAccess	The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.
13	O.TransProtect	The TOE will, in conjunction with the operational environment, establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Table 4-2: Security Objectives for the Operational Environment

Item	Environment Objective	Description
1	OE.AuthService*	The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

Item	Environment Objective	Description
2	OE.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.
3	OE.Operations	The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.
4	OE.Person	Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.
5	OE.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
6	OE.ProtectAudit	The Operational Environment will provide a means for secure storage and protection of the TOE audit information from unauthorized users via the Operational Environment interfaces.
7	OE.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
8	OE.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components and remote users are via a secure channel.
9	OE.ProtectDB	The Operational Environment will be configured by those responsible for the TOE to protect information stored in the database systems used by the TOE via the Operational Environment interfaces.
10	OE.ProtectFiles	The Operational Environment will be configured by those responsible for the TOE to protect executable and data files used by the TOE via the Operational Environment interfaces.
11	OE.TransProtect	The Operational Environment will, working in conjunction with the TOE, establish a trusted communications path which provides for protection of the data from modification or disclosure while being exchanged between TOE components.
12	OE.Time	The underlying operating system will provide reliable time stamps.

**Note: OE.AuthService is only applicable to the TOE if is configured to use an external authentication service. (i.e. RADIUS Server)*

4.3 Security Objectives Rationale

Table 4-3: Mapping of TOE Security Objectives to Threats/Policies

Item	TOE Objective	Threat
1	O.Access	T.NoPrivilege
2	O.Analyze	T.AssetRisks
3	O.Attributes	T.NoPrivilege
4	O.Audit	T.Undetect
5	O.Collect	T.AssetRisks
6	O.CryptoComm	T.Intercept
7	O.CyptoVerify	T.Intercept
8	O.Manage	T.Mismanage
9	O.Notify	T.AssetRisks
10	O.Password	T.Masquerade
11	O.ProtectAuth	T.Masquerade
12	O.RobustTOEAccess	T.Masquerade

Item	TOE Objective	Threat
13	O.TransProtect	T.Intercept

Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions

Item	Environment Objective	Threat/Policy/Assumption
1	OE.AuthService	T.Masquerade
2	OE.NoUntrusted	A.NoUntrusted
3	OE.Operations	A.Manage
4	OE.Person	A.Admin
5	OE.Physical	A.Physical
6	OE.ProtectAudit	T.Undetect
7	OE.ProtectAuth	A.ProtectPwd
8	OE.ProtectComm	A.ProtectComm
9	OE.ProtectDB	A.ProtectDB
10	OE.ProtectFiles	A.ProtectFiles
11	OE.Time	T.Undetect
12	OE.TransProtect	T.Intercept

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

Table 4-5: All Threats to Security Countered

Item	Threat ID	Objective	Rationale
1	T.AssetRisks Security risks, vulnerabilities and non-compliance may exist on the IT network assets that the TOE assesses, leading to a compromise of those assets.	O.Analyze The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.	This objective plays a role in mitigating this threat by analyzing the collected asset data for risks, vulnerabilities and non-compliance to security standards.
		O.Collect The TOE will collect configuration data from the IT network assets.	This objective also contributes to mitigating this threat by providing the TOE's analyzer with the appropriate configuration data collected from the assets.
		O.Notify The TOE will notify responsible personnel when designated events occur in the assessment process.	This objective also contributes to mitigating this threat by notifying the appropriate personnel when a significant event happens as a result of the analysis process on the collected data.

Item	Threat ID	Objective	Rationale
2	T.Intercept An attacker may gain access to and/or modify secure data while it is being transmitted between TOE components.	O.TransProtect The TOE will, in conjunction with the operational environment, establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.	This objective contributes to mitigating this threat by ensuring that the TOE only uses secure communications paths that have been established by the Operational Environment for the transmission of security data.
		O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components.	This objective contributes to mitigating this threat by ensuring that the TOE will provide the mechanisms encrypt the data being transmitted between TOE components.
		O.CryptoVerify The TOE will provide a mechanism to verify the integrity and correct operation of the cryptographic modules during initialization and upon administrative execution.	This objective contributes to mitigating this threat by ensuring that the cryptographic module used for the trusted communications has be integrity checked and correct operations.
		OE.TransProtect The Operational Environment will, working in conjunction with the TOE, establish a trusted communications path which provides for protection of the data from modification or disclosure while being exchanged between TOE components.	This objective also contributes to mitigating this threat by ensuring that the Operational Environment will support the use of secure mechanisms to establish the communication paths used by the TOE.
3	T.Masquerade A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.	O.Password The TOE will be able to support an administrator defined password policy.	This objective mitigates the threat by providing a policy to enforce strong user passwords and limiting brute force guessing attacks.
		O.ProtectAuth The TOE will provide protected authentication feedback.	This objective mitigates the threat by providing the masking of a user’s password to keep it from being overseen by another.

Item	Threat ID	Objective	Rationale
		O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.	This objective mitigates this threat by controlling the logical access to the TOE and its resources through the login process. By constraining how authorized users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective allows the TOE to correctly interpret information used during the authentication process so that it can make the correct decisions when identifying and authenticating users.
		OE.AuthService The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.	This objective mitigates the threat by allowing the use of an external user authentication service that is invoked by the TSF to support a Robust TOE Management Access control policy.
4	T.Mismanage Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	O.Manage The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.	This objective mitigates this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, it provides administrators with the capability to configure and operate the TOE via a GUI.
5	T.NoPrivilege A user may gain access to management functions or TSF data for which they are not authorized resulting in the TSF data being compromised.	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.	This objective mitigates this threat by limiting the functions a user can perform and the data they can access via the TOE interfaces through the use of user security roles and permissions.
		O.Attributes The TOE will be able to store and maintain user attributes used for management access control decisions/enforcement..	This objective also mitigates the threat by providing the capability to store and maintain user security roles and access permissions for each user account that will be used to control access of TSF data and functions.

Item	Threat ID	Objective	Rationale
6	T.Undetect Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.	O.Audit The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.	This objective mitigates this threat by providing the TOE with an audit logging function that keeps records of security significant events and provide a means to review.
		OE.ProtectAudit The Operational Environment will provide a means for secure storage and protection of the TOE audit information from unauthorized users via the Operational Environment interfaces.	This objective mitigates the threat by ensuring that the audit records cannot be accessed by unauthorized personnel through the Operational Environment interfaces (both through the DBMS and the operating systems of the TOE Servers).
		OE.Time The underlying operating system will provide reliable time stamps.	This objective contributes to mitigating the threat by providing each audit record with an accurate time stamp for ease of viewing and piecing together timelines.

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

Table 4-6: All Assumptions Upheld

Item	Assumption ID	Objective	Rationale
1	A.Admin It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.	OE.Person Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.	This objective provides for competent personnel to administer the TOE.
2	A.Manage It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.	OE.Operations The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.	This objective ensures that all TOE users follow the guidance for secure installation, configuration and operation procedures.
3	A.NoUntrusted It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.	OE.NoUntrusted The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.	This objective provides for the protection of the TOE from untrusted software and users.
4	A.Physical It is assumed that the TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.	OE.Physical Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.	This objective provides for the physical protection of the TOE software.
5	A.ProtectComm It is assumed that those responsible for the TOE will ensure the communications between the TOE components and remote users are protected to the level required for the operating environment.	OE.ProtectComm Those responsible for the TOE will ensure the communications between the TOE components and remote users are via a secure channel.	This objective provides for the configuration of secure communication paths between the TOE components and remote users by an authorized administrator. The Apache Server (provided with TOE) uses a different instantiation of OpenSSL than the included cryptographic module.

Item	Assumption ID	Objective	Rationale
6	A.ProtectDB It is assumed that those responsible for the TOE will ensure that data stored in the databases used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.	OE.ProtectDB The Operational Environment will be configured by those responsible for the TOE to protect information stored in the database systems used by the TOE via the Operational Environment interfaces.	This objective provides for the secure configuration of the databases by an authorized administrator to prevent unauthorized access to the stored data through the Operational Environment interfaces.
7	A.ProtectFiles It is assumed that those responsible for the TOE will ensure executable and data files used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.	OE.ProtectFiles The Operational Environment will be configured by those responsible for the TOE to protect executable and data files used by the TOE via the Operational Environment interfaces.	This objective provides for the secure configuration of the executable and data files by an authorized administrator to prevent unauthorized access to the TOE files through the Operational Environment interfaces.
8	A.ProtectPwd It is assumed that users will protect their authentication data.	OE.ProtectAuth Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.	This objective provides for all TOE users protecting their authentication data.

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXP" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FIA_UAU_EXP.2	Explicit: TSF user authentication before any action
2	FPT_ITT_EXP.1	Explicit: Partial Intra-TSF trusted channel among distributed TOE components
3	FPT_TST_EXP.1	Explicit: TSF Self-Testing
4	NMA_COL_EXP.1	Explicit: Asset data collection
5	NMA_EVL_EXP.1	Explicit: Asset data analysis and evaluation
6	NMA_NOT_EXP.1	Explicit: Security notifications

5.1 FIA_UAU_EXP.2 Explicit: TSF user authentication before any action

Extended Component Definition

Class

FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 3.

Family

User authentication (FIA_UAU)

Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

Management

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

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

Audit

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

Definition

FIA_UAU_EXP.2 Explicit: TSF user authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXP.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

Rationale

FIA_UAU_EXP.2 is modeled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXP.2 needed to be defined as an extended component because the standard component was broadened by adding the text *"either by the TSF or by an authentication service in the Operational Environment invoked by the TSF".*

Note: The definition and use of FIA_UAU_EXP.2 was approved by the validation team in a previous CygnaCom evaluation.

5.2 FPT_ITT_EXP.1 Explicit: Partial Inter-TSF trusted channel among distributed TOE components

Extended Component Definition

Class

FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 3.

Family

Inter-TSF trusted channel (FPT_ITT)

Family Behaviour

This family provides requirements that address protection of TSF data when it is transferred between separate parts of a TOE across an internal channel.

Management

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

- Configuring the actions that require trusted channel, if supported

Audit

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

- Minimal: Failure of the trusted channel functions
- Minimal: Identification of the initiator and target of failed trusted channel functions
- Basic: All attempted uses of the trusted channel functions
- Basic: Identification of the initiator and target of all trusted channel functions

Definition

FPT_ITT_EXP.1 Explicit: Partial Inter-TSF trusted channel among distributed TOE components

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT_EXP.1.1 The TSF shall establish, in conjunction with the Operational Environment, a trusted communication channel among its distributed component applications 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 using the encryption and certificate services from the Operational Environment.

FPT_ITT_EXP.1.2 The TSF shall use this trusted channel for all communication among its distributed application components.

Rationale

FPT_ITT_EXP.1 is modeled closely on the standard component FTP_ITC.1: Inter-TSF trusted channel. FPT_ITT_EXP.1 and FTP_ITT.1 Basic internal TSF data transfer protection. It was needed to be defined as an extended component because the standard component does not take into account the interdependency between the TOE and the Operational Environment to implement the trusted channel.

5.3 FPT_TST_EXP.1 Explicit: TSF Self-Testing

Extended Component Definition

Class

FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 3.

Family

TSF Self-Testing (FPT_TST)

Family Behaviour

The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. Examples are interfaces to enforcement functions, and sample arithmetical operations on critical parts of the TOE. These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. The actions to be taken by the TOE as the result of self-testing are defined in other families.

Management

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

- management of the conditions under which TSF self-testing occurs, such as during initial start-up, regular interval, or under specified conditions;
- management of the time interval if appropriate.

Audit

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

- Basic: Execution of the TSF self-tests and the results of the tests.

Definition

FTP_TST_EXP.1 Explicit: TSF Self-Testing

Hierarchical to: No other components.

Dependencies: FCS_COP.1

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests *[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and*

***[assignment: conditions under which self-test should occur]]* to verify the correct operation of the cryptographic module portion of the TSF.**

FPT_TST_EXP.1.2 The TSF shall run a suite of self-tests *[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and [assignment: conditions under which self-test should occur]]* to verify the integrity of the cryptographic module portion of the TSF.

FPT_TST_EXP.1.3 Upon detection of a test failure, the cryptographic module shall *[assignment: list events and conditions]*

Rationale

FPT_TST_EXP.1 is modeled closely on the standard component FPT_TST.1: TSF testing. It was needed to be defined as an extended component because the standard component did not take into accounts the failure procedures and verification of correct operation and integrity. The original also included the ability to check the integrity of the stored TSF executable code as a whole. The extended SFR only includes the particular cryptographic modules and not the product as a whole.

5.4 NMA_COL_EXP.1 Explicit: Asset data collection

Extended Component Definition

Class

NMA: Network management and assessment

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a risk and compliance assessment product. While most of the SFRs that follow were modeled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of risk and compliance assessment rather than intrusion detection.

Family

Asset data collection (NMA_COL)

Family Behaviour

This family defines the types of scanning of IT network assets supported by the TSF. This family also defines the asset information collected by the scanner components of the TOE. The scanners would generally collect static configuration information and send that onto an analytical component.

Management

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

- Configuration of the collected asset information by an administrator
- Configuration of the scanner operation by an administrator

Audit

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

- Minimal: error return from scanning process
- Basic: time of scan; successful/unsuccessful outcome of scan

Definition

NMA_COL_EXP.1 Explicit: Asset data collection

Hierarchical to: No other components

Dependencies: No dependencies

NMA_COL_EXP.1.1 The TSF shall be able to collect information of type *[assignment: list of data types]* from the IT network assets on the target network via the following methods *[assignment: list of collection methods].*

NMA_COL_EXP.1.2 At a minimum, the TSF shall collect and record the following information: *[assignment: list of asset information].*

Rationale

NMA_COL_EXP.1 is modeled on IDS_SCN.1 Scanner Data Collection (EXP) as defined in the IDS Scanner Protection Profile Version 1.3 July 25, 2007. This SFR was modified to be more general and also specify the collection of asset data via the listed methods of collection.

5.5 NMA_EVL_EXP.1 Explicit: Asset data analysis and evaluation

Extended Component Definition

Class

NMA: Network management and assessment

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a risk and compliance assessment product. While most of the SFRs that follow were modeled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of risk and compliance assessment rather than intrusion detection.

Family

Asset data analysis and evaluation (NMA_EVL)

Family Behaviour

This family defines the evaluation of the data collected from the scanning of IT network assets supported by the TSF. It describes the actions of the analytical component of a risk and compliance management TOE.

Management

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

- Configuration of any evaluation parameters or reporting of results by an administrator

Audit

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

- Basic: generation of evaluation results

Definition

NMA_EVL_EXP.1 Explicit: Asset data analysis and evaluation

Hierarchical to: No other components

Dependencies: NMA_COL_EXP.1

NMA_EVL_EXP.1.1 The TSF shall be capable of performing the following evaluation function(s) on the data collected from the IT network assets*: [assignment: list of evaluation functions].*

Rationale

NMA_EVL_EXP.1 is modeled on IDS_ANL.1 Analyzer analysis (EXP) as defined in IDS Analyzer Protection Profile Version 1.3 July 25, 2007. The SFR was made more general to specify the list of functions used for the evaluation and assessment of various types of risk and compliance data.

5.6 NMA_NOT_EXP.1 Explicit: Security notifications

Extended Component Definition

Class

NMA: Network management and assessment

This class was explicitly created. The families in this class specify the functional requirements that pertain to the security features of a risk and compliance assessment product. While most of the SFRs that follow were modeled on existing IDS requirements that have been used in validated Protection Profiles, these requirements needed further modification to meet the specific needs of risk and compliance assessment rather than intrusion detection.

Family

Security notifications (NMA_NOT)

Family Behaviour

This family defines the notifications generated by the TSF as a result of scanning IT network assets and analyzing the asset data. This family also defines the destination(s) of the notifications that are generated. The scanners would generally collect static configuration information and send that onto an analytical component which would cause the notifications to be generated.

Management

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

- Configuration of the notification destination by an administrator

Audit

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

- Basic: time notification generated, source and destination of notification, notification type

Definition

NMA_NOT_EXP.1 Explicit: Security notifications

Hierarchical to: No other components

Dependencies: NMA_EVL_EXP.1

NMA_NOT_EXP.1.1 The TSF shall send a visual notification to *[assignment: list where visual notifications are displayed]* when *[assignment: list of events]* occurs during the assessment process.

NMA_NOT_EXP.1.2 The TSF shall send a *[assignment: list notification types]* notification to *[assignment: list notification recipients]* when *[assignment: list of events]* occurs during the assessment process.

Rationale

NMA_NOT_EXP.1 is modeled on IDS_RCT.1 Analyzer react (EXP) as defined in IDS System Protection Profile Version 1.7 July 25, 2007. This SFR was modified to apply to the various events that can be generated by a risk and compliance assessment system rather than only the detection of an intrusion. This SFR uses the term “notification” rather than “alert” because the TOE sends this information via email (SMTP Server or native messaging within the product) and therefore cannot guarantee that the recipient will acknowledge or read the event information in a timely manner.

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

iteration: allows a component to be used more than once with varying operations;

assignment: allows the specification of parameters;

selection: allows the specification of one or more items from a list; and

refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text].***
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in <u>***italicized bold and underlined text***</u>.

Iterations are identified the inclusion of a suffix on the name of the element consisting of a parenthesized number indicating the iteration number. For example, fdp_ifc.2.1 (1) indicates the first iteration of fdp_ifc.2.1 while fdp_ifc.2.1 (2) indicates the second iteration.

Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: with italicized text at a smaller font size.*

Extended components defined in Section 5 have been denoted with the suffix "_EXP" following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5, and summarized in Table 6-1 below.

Table 6-1: Functional Components

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_SAR.1	Audit review
4	FAU_SAR.3	Selectable audit review
5	FCS_CKM.1	Cryptographic key generation
6	FCS_CKM.4	Cryptographic key destruction
7	FCS_COP.1	Cryptographic operation
8	FIA_AFL.1	Authentication failure handling

Item	SFR ID	SFR Title
9	FIA_ATD.1	User attribute definition
10	FIA_SOS.1	Verification of secrets
11	FIA_UAU_EXP.2	TSF user authentication before any action
12	FIA_UAU.5	Multiple authentication mechanisms
13	FIA_UAU.7	Protected authentication feedback
14	FIA_UID.2	User identification before any action
15	FMT_MTD.1	Management of TSF data
16	FMT_SMF.1	Specification of Management Functions
17	FMT_SMR.1	Security Roles
18	FPT_ITT_EXP.1	Explicit: Partial Inter-TSF trusted channel among distributed TOE components
19	FPT_TST_EXP.1	Explicit: TSF Self-testing
20	NMA_COL_EXP.1	Explicit: Asset data collection
21	NMA_EVL_EXP.1	Explicit: Asset data analysis and evaluation
22	NMA_NOT_EXP.1	Explicit: Security notifications

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) ***[list of auditable events***

Table 6-2: Audit Events for Central Servers

Item	SFR ID	Audit Event
1	FAU_GEN.1	System Startup System Shutdown
2	FAU_GEN.2	none
3	FAU_SAR.1	none
4	FAU_SAR.3	none
5	FCS_CKM.1	none
6	FCS_CKM.4	none
7	FCS_COP.1	none
8	FIA_AFL.1	Authentication failure handling

Item	SFR ID	Audit Event
9	FIA_ATD.1	Create/edit/delete user Create/edit/delete group.
10	FIA_SOS.1	Change <username> password
11	FIA_UAU_EXP.2	Login <username> user (successful) Log out of <username> user (successful)
12	FIA_UAU.5	none
13	FIA_UAU.7	none
14	FIA_UID.2	Login <username> user (successful) Log out of <username> user (successful)
15	FMT_MTD.1	Management of TSF data
16	FMT_SMF.1	Add/Edit/Delete Device Add/Edit/Delete Host Add/Edit/Delete Host Agent Add/Edit/Delete/Set Monitoring audit and Alert Policy Publish/Revoke monitor, audit (grc), and Alert policy on <ServerName> Add/Edit/Delete Agent Policy Add/Edit/Delete AD domain <Server>/<Domain> Add Regional Server Add/Edit/Delete Ticket Add/Edit/Delete <host/device> policy Add/Delete DataCollector Vulnerability Scanner options are changed Delete Profile Add/Edit/Delete object
17	FMT_SMR.1	none
18	FPT_ITT_EXP.1	none
19	FPT_TST_EXP.1	FIPS Self-test
20	NMA_COL_EXP.1	View Collection Stats for device <UID> View Collection Stats for host <UID> Run vulnerability scan for <UID> node on <ServerName>
21	NMA_EVL_EXP.1	none
22	NMA_NOT_EXP.1	none

].

**Application Note: The product doesn't have a specific event for startup and shutdown of the audit function. However, since the audit is started with the TOE it is met via the audit event for the Startup and Shutdown of the TOE.*

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[not specified].***

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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

6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other component

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[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.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[searching and sorting]*** of audit data based on

[All possible combinations of the following fields:

- ***User***
- ***TimeStamp***
- ***Activity]***

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[listed in Column 1 of Table 6-3]*** and specified cryptographic key sizes ***[listed in Column 2 of Table 6-3]*** that meet the following: ***[FIPS 140-2].***

Table 6-3: Cryptographic Support Parameters

Keys	***Bits***	***Known as***	***Description***
Self-Signed Cert	***1024***		***Facilitate Key transfer over SSL connection.***
RSA Public	***1024 Binary (DER) format***		***Validate Key request at time of Key transfer***
RSA Private	***1024 Binary (DER) format***		***Decrypt data which was encrypted using SSL Cert***
AES	***192***	***Database Key***	***Encryption/Decryption of database***
AES	***192***	***File/Password Key***	***Encryption/Decryption of passwords and files containing User credentials***
AES	***192***	***Communication Key***	***Encrypt/Decrypt communication between all components and executables***

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[zeroization]*** that meets the following: ***[FIPS 140-2].***

6.1.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform ***[operations listed in Column 4 of Table 6-4 Cryptographic Algorithms]*** accordance with a specified cryptographic algorithm ***[listed in Column 2 of Table 6-4 Cryptographic Algorithms]*** and cryptographic key sizes ***[listed in Column 2 of Table 6-4 Cryptographic Algorithms]*** that meet the following: ***[FIPS 140-2].***

Table 6-4: Cryptographic Algorithms

Algorithm Type	**Algorithm**	**FIPS Validation Certificate #**	**Use**
Symmetric Keys	AES (Advanced Encryption Standard) - 192 bit	#695	encrypt/decrypt operations
Asymmetric Keys	RSA (Rivest Shamir Adleman) – 2048 bit	Allowed in FIPS-mode for key-transport/establishment	key-transport and key-establishment methodologies
RNG	ANSI X9.31 -512 bit	#407	random number generation
hashing	SHA-256 bit	#723	For digest comparison of activation-password and also integrity check of raw-logs that are uploaded to Central
HMAC (Keyed-Hash Message Authentication Code)	HMAC-SHA-256 bit	#373	module integrity check

6.1.3 Class FIA: Identification and Authentication

6.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[3]*** unsuccessful authentication attempts occur related to ***[user login attempts].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall ***[refuse any login attempts from that user for 5 minutes].***

6.1.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

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

[Username,

Password,

Authentication mechanism

Email ID,

User Group (functional role)

Enable/Disable account flag

Device Group

Report Selections (based on role/group)].

6.1.3.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the parameters of the SecureVue Password Policy (See Table 6-5)].***

Table 6-5: SecureVue Password Policy Rules

Role	**Parameter Requirements**
Super Administrator	Must be alphanumeric with at least one special character, and number Minimum number of character required: 12 char Maximum number of character permitted: 31 char (Hardcoded values)
Administrator	Must be alphanumeric with at least one special character, and number Minimum number of character required: 12 char Maximum number of character permitted: 31 char (Hardcoded values)

Role	Parameter Requirements
Power User	Must be alphanumeric with at least one special character, and number Minimum number of character required: 8 char Maximum number of character permitted: 31 char (Hardcoded values)
User	Must be alphanumeric with at least one special character and number Minimum number of character required: 8 char Maximum number of character permitted: 31 char (Hardcoded values)
Alert User	Must be alphanumeric with at least one special character and number Minimum number of character required: 8 char Maximum number of character permitted: 31 char (Hardcoded values)

6.1.3.4 FIA_UAU_EXP.2 Explicit: TSF user authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXP.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.5 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide ***[Native Password Authentication, Invocation of external server authentication]*** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the ***[***

Following rules:

- ***Use Native Password Mechanism when enabled (default) AND no external authentication server is configured***

else

- ***Invoke authentication request to the optionally configured external authentication mechanism***

- ***Fail all login attempts if configured external authentication mechanism cannot be found***

Application Note: The external authentication servers are NOT part of the TOE.

6.1.3.6 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only

[

- ***display of the typed in account name (username)***
- ***typed in password displayed as dots***

]

to the user while the authentication is in progress.

6.1.3.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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

6.1.4 Class FMT: Security Management

6.1.4.1 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Table 6-6]*** the ***[TSF data as specified in Table 6-6]*** to ***[user security role as in Table 6-6].***

Table 6-6: Management of TSF data (Central Server)

Module	Task	Super Admin / Administrator	Power User	User	Alert User	TSF data See Section 1.4.5 operational/administrative
Dashboards	View/Manage Dashboard panels	√	√	√	×	operational data/ administrative data for Central
Alerts	View Alerts	√	√	×√*	√	operational data
	View/Manage Alerts Policies (rules)	√	√	×	×	administrative data for Central
Reports	View/Generate/Export Reports	√	√	×√*	×	operational data
	Create Custom Report	√	×	×	×	operational data/ administrative data for Central
Monitors (Log Events)	View/Manage Monitors	√	√	×√*	×	operational data/ administrative data for Central
Assets	View/Manage Asset Policy	√	√	×√*	×	operational data/ administrative data for Central
Configuration	View/Manage Configuration Policy	√	√	×√*	×	operational data/ administrative data for Central
Vulnerability	View/Manage Vulnerability Policy	√	√	×√*	×	operational data/ administrative data for Central
ForensicVue	View/Perform searches on event and user activity	√	√	×√*	×	operational data
UserVue	View/Manage Data Sources	√	×	×	×	operational data/ administrative data for Central
	View/ modify/ delete Data Sources	√	×√*	×√*	×	operational data/ administrative data for Central
	View/Manage WatchList	√	√	√	×	operational data/ administrative data for Central
	View/Perform Searches on User Activity	√	√	×√*	×	operational data
Workflow	View/Manage Tickets and nodes	√	√	×√*	×	operational data/ administrative data for Central
Traps	View/Manage Traps and Trap Policy	√	×	×	×	operational data/ administrative data for Central
Topology	Discover nodes/Manage nodes/View topology/manage snmp communities/customize views	√	×	×	×	operational data/ administrative data for Central
ComplianceVue	View Policy	√	×√*	×√*	×	operational data
	Manage Policy	√	×√*	×√*	×	administrative data for Central
Agents	Manage	√	×	×	×	administrative data for DC
Database Collectors	Manage	√	×	×	×	administrative data for DC
File Collectors	Manage	√	×	×	×	administrative data for DC

Module	Task	Super Admin / Administrator	Power User	User	Alert User	TSF data See Section 1.4.5 operational/administrative
Nodes	View monitored network assets	√	×√*	×√*	×	operational data
	Manage monitored network assets	√	×	×	×	administrative data for DC
Availability	View/Manage Process component policies	√	√	×√*	×	administrative data for DC
Collection Policies	View/Manage	√	×	×	×	administrative data for DC
Monitoring Policies	View/Manage	√	√	×	×	administrative data for DC
Diagnostics	Tools for managing/troubleshooting TOE	√	×	×	×	operational data/ administrative data for Central
Preferences	View/Manage Assign/switch admin account to super admin role	√	×	×	×	administrative data for Central
Licenses	Manage License	√	×	×	×	administrative data for Central
Universal Parser	Manage parser	√	×	×	×	administrative data for Central
Users	Manage/import users/ *Admin account assigned to Super Admin role cannot be deleted	√	×	×	×	administrative data for Central
Help	About/Help SecureVue	√	√	√	√	
Under <username> in upper right corner	Change Password (only available if natively authenticated user)	×	√	√	√	administrative data for Central
	Logout	√	√	√	√	

×√* These functions are not given be default. The User can be granted explicit access permission by the administrator to have this functionality and basically create a custom role.

Note: Manage equals the add, modify, delete functions.

6.1.4.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[operations as specified in Table 6-6].***

6.1.4.3 FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

- ***Super Administrator***
- ***Administrator***
- ***Power User***
- ***User***
- ***Alert User***
- ***Custom user roles***

].

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

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 FPT_ITT_EXP.1 Explicit: Partial Inter-TSF trusted channel among distributed TOE components

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT_EXP.1.1 The TSF shall establish, in conjunction with the Operational Environment, a trusted communication channel among its distributed component applications 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 using the encryption and certificate services from the Operational Environment.

FPT_ITT_EXP.1.2 The TSF shall use this trusted channel for all communication among its distributed application components.

6.1.5.2 FPT_TST_EXP.1 Explicit: TSF Self-testing

Hierarchical to: No other components.

Dependencies: FCS_COP.1

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests ***[during initial startup and at the request of the authorized use]*** to verify the correct operation of the cryptographic module portion of the TSF.

FPT_TST_EXP.1.2 The TSF shall run a suite of self-tests ***[during initial startup and at the request of the authorized use]*** to verify the integrity of the cryptographic module portion of the TSF.

FPT_TST_EXP.1.3 Upon detection of a test failure, the cryptographic module shall ***[***

(1) The cryptographic module will enter an Error State,

(2) All cryptographic operations are immediately disabled until the cryptographic module is reinitialized,

(3) Log file is created giving brief description of FIPS Self-Test Suite results, and

(4) Transitions to a Power-OFF state.

].

6.1.6 Class NMA: Network management and assessment

6.1.6.1 NMA_COL_EXP.1 Explicit: Asset data collection

Hierarchical to: No other components

Dependencies: No dependencies

NMA_COL_EXP.1.1 The TSF shall be able to collect information of type ***[listed in the "Type" column in Table 6-7]*** information from the IT network assets on the target network via the following methods ***[listed in the "Method Description" column in Table 6-7].***

Table 6-7: Method of data collection

Type	Method Description
Event	WMI – Windows Management Instrumentation service
	API – Uses Remote Registry
	External Collection Agent
Monitoring	Syslog
Performance	WMI
	SSH
	SNMP
Configuration	SSH
	Telnet
	CPMI (Check Point device)
	FTP
	FTPS
	File – residing on SecureVue Data collector
Asset	WMI

	SSH
	SNMP
Vulnerability	Importation of information from third-party vulnerability scanner
Topology	ICMP trace route
	TCP trace route
	SNMP

NMA_COL_EXP.1.2 At a minimum, the TSF shall collect and record the following information:

[

- ***IP address of an discovered device***
- ***date and time of the collection***
- ***Data Collector IP***
- ***Total count of events parsed***

].

6.1.6.2 NMA_EVL_EXP.1 Explicit: Asset data analysis and evaluation

Hierarchical to: No other components

Dependencies: NMA_COL_EXP.1

NMA_EVL_EXP.1.1 The TSF shall be capable of performing the following evaluation function(s) on the data collected from the IT network assets:

[

Table 6-8: Method of data analysis and evaluation

Group	Method Description
Monitoring	Event correlation
	Comparative Analysis
Vulnerability	Event correlation from third party scanner
	Comparative Analysis
Configuration (support for GRC)	Event correlation
	Comparative Analysis
	Risk assessment
Asset	Comparative Analysis
	Trend Analysis
NBA Detection	Comparative Analysis
	Usage Analysis
Performance	Statistical analysis
Forensics	Event correlation

].

6.1.6.3 NMA_NOT_EXP.1 Explicit: Security notifications

Hierarchical to: No other components

Dependencies: NMA_EVL_EXP.1

NMA_NOT_EXP.1.1 The TSF shall send a visual notification to ***[Alert Manager's display]*** when ***[the event(s) listed in Table 6-9]*** occurs during the assessment process.

NMA_NOT_EXP.1.2 The TSF shall send a ***[email, SNMP Trap]*** notification to ***[the assigned event notification recipient's Email ID, configured SNMP manager]*** when ***[the event(s) listed in Table 6-9]*** occurs during the assessment process.

Table 6-9: Security Notifications

Event
Alert when user account is locked.
Alert when the specified device or devices are down.
Alert when the event count from specified devices exceeds a specified threshold.
Alert when an unknown node is detected.
Alert when storage space is less than the specified disk space. It can be set to send either Warning or Critical e-mail alerts based on the availability of storage space.
Alert when the device (s) is inactive for more than the specified time.
Alert when the Host (s) is inactive for more than the specified time.

6.2 Security Assurance Requirements for the TOE

This evaluation is for an EAL2 augmented with ALC_FLR.2. Numbers in parenthesis indicate the augmented SARs (i.e those assurance measures that are above and beyond the base set required for the particular EAL. The assurance measures for this ST are as follows:

Table 6-10: EAL2 Assurance Components

Assurance class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	**EAL2**	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	1	**2**	3	4	5	5	6
	ADV_IMP				1	1	2	2

	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		**1**	2	3	4	5	6
Guidance documents	AGD_OPE	1	**1**	1	1	1	1	1
	AGD_PRE	1	**1**	1	1	1	1	1
Life-cycle support	ALC_CMC	1	**2**	3	4	4	5	5
	ALC_CMS	1	**2**	3	4	5	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR		**(2)**					
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	**1**	1	1	1	1	1
	ASE_ECD	1	**1**	1	1	1	1	1
	ASE_INT	1	**1**	1	1	1	1	1
	ASE_OBJ	1	**2**	2	2	2	2	2
	ASE_REQ	1	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	1	**1**	1	1	1	1	1
Tests	ATE_COV		**1**	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		**1**	1	1	1	2	2
	ATE_IND	1	**2**	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	**2**	2	3	4	5	5

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-11 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference, explicitly stated SFRs are denoted by an (Exp) following the reference, and Operational Environment are denoted by an OE.

Table 6-11: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	OE
2	FAU_GEN.2	User identity association	FAU_GEN.1 FIA_UID.1	1 14H
3	FAU_SAR.1	Audit Review	FAU_GEN.1	1
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
5	FCS_CKM.1	Cryptographic key generation	(FCS_CKM.2 or FCS_COP.1) FCS_CKM.4	7 6
6	FCS_CKM.4	Cryptographic key destruction	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	5
7	FCS_COP.1	Cryptographic operation	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) FCS_CKM.4	5 6
8	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	11
9	FIA_ATD.1	User attribute definition	none	
10	FIA_SOS.1	Verification of secrets	none	
11	FIA_UAU_EXP.2	TSF user authentication before any action	FIA_UID.1	14H
12	FIA_UAU.5	Multiple authentication mechanisms	none	
13	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	11
14	FIA_UID.2	User identification before any action	none	
15	FMT_MTD.1	Management of TSF data	FMT_SMR.1 FMT_SMF.1	17 16
16	FMT_SMF.1	Specification of Management Functions	none	
17	FMT_SMR.1	Security Roles	FIA_UID.1	14H
18	FPT_ITT_EXP.1	Explicit: Partial Inter-TSF trusted channel among distributed TOE components	None	
19	FPT_TST_EXP.1	Explicit: TSF Self-testing	FCS_COP.1	7
20	NMA_COL_EXP.1	Explicit: Asset data collection	none	
21	NMA_EVL_EXP.1	Explicit: Asset data analysis and evaluation	NMA_COL_EXP.1	20
22	NMA_NOT_EXP.1	Explicit: Security notifications	NMA_EVL_EXP.1	21

** Note: Reliable timestamps are provided by the hardware and OS of the platforms that host the TOE components. See OE.Time as defined in Table 4-2: Security Objectives for the Operational Environment.*

6.3.2 Functional Requirements

Table 6-12 traces each SFR back to the security objectives for the TOE.

Table 6-12: Mapping of TOE SFRs to TOE Security Objectives

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1	O.Audit
2	FAU_GEN.2	O.Audit
3	FAU_SAR.1	O.Audit
4	FAU_SAR.3	O.Audit
5	FCS_CKM.1	O.CryptoComm
6	FCS_CKM.4	O.CryptoComm
7	FCS_COP.1	O.CryptoComm
8	FIA_AFL.1	O.RobustTOEAccess
9	FIA_ATD.1	O.Attributes
10	FIA_SOS.1	O.Password
11	FIA_UAU_EXP.2	O.RobustTOEAccess
12	FIA_UAU.5	O.RobustTOEAccess
13	FIA_UAU.7	O.ProtectAuth
14	FIA_UID.2	O.RobustTOEAccess
15	FMT_MTD.1	O.Access O.Manage
16	FMT_SMF.1	O.Manage
17	FMT_SMR.1	O.Access
18	FPT_ITT_EXP.1	O.TransProtect
19	FPT_TST_EXP.1	O.CryptoVerify
20	NMA_COL_EXP.1	O.Collect
21	NMA_EVL_EXP.1	O.Analyze
22	NMA_NOT_EXP.1	O.Notify

Table 6-13 demonstrates that the SFRs meet all security objectives for the TOE. Rationale for each objective is included in the table.

Table 6-13: All TOE Objectives Met by Security Functional Requirements

Item	Objective ID	SFR ID	Rationale
1	O.Access The TOE will allow access to management functions and TSF data only to authorized users with the appropriate security attributes via the TOE interfaces.	FMT_MTD.1	FMT_MTD.1 specifies the administrative functions and the TSF data on which they operate as they are available to each of the defined administrative (security) roles for each of the administrative interfaces of the TOE.
		FMT_SMR.1	FMT_SMR.1 requires that the TSF maintain multiple administrative roles. The TSF is able to associate a human user with one or more administrative roles and these roles are used to restrict access (management access control) to the administrative functions and TSF data.

Item	Objective ID	SFR ID	Rationale
2	O.Analyze The TOE will be capable of analyzing the collected asset data to derive conclusions about risks and compliance of the IT network assets.	NMA_EVL_EXP.1	NMA_EVL_EXP.1 defines the evaluation functions that are performed by the TOE to analyze the collected asset data.
3	O.Attributes The TOE will be able to store and maintain user attributes used for management access control decisions/enforcement.	FIA_ATD.1	FIA_ATD.1 defines the attributes of users, including the username that is used by the TOE to determine a user’s identity, the password used for authentication, the account type that determines a user’s administrative role and the folders and projects assigned to that user which define the TSF data a user may access.
4	O.Audit The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.	FAU_GEN.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event.
		FAU_GEN.2	FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event.
		FAU_SAR.1	FAU_SAR.1 provides for an Audit Review capability
		FAU_SAR.3	FAU_SAR.3 provides for the Audit be reviewable based on searchable criteria.
5	O.Collect The TOE will collect configuration data from the IT network assets.	NMA_COL_EXP.1	NMA_COL_EXP.1 defines the information collected from the IT network assets and the methods by which it is collected
6	O.CryptoComm The TOE will provide cryptographic functions for secure communications between TOE components.	FCS_CKM.1	FCS_CKM.1 defines the key generation parameters for the cryptographic operations used for secure communications
		FCS_CKM.4	FCS_CKM.4 defines the method of destroying the keys used in the cryptographic operations used for secure communications
		FCS_COP.1	FCS_COP.1 defines the parameters of the cryptographic operations used by the TOE for secure communications
7	O.CryptoVerify The TOE will provide a mechanism to verify the integrity and correct operation of the cryptographic modules during initialization and upon administrative execution.	FPT_TST_EXP.1	FPT_TST_EXP.1 defines the requirement to provide a mechanism that will verify the integrity and the correct operation of the Cryptographic modules during initialization and when an administrator executes the mechanism. The TOE will not attain operational state if the initialization tests do not complete successfully. Initialization or execution follow a predefined set of procedures if a failure occurs.
8	O.Manage The TOE will provide all the functions and facilities	FMT_MTD.1	FMT_MTD.1 specifies the administrative functions and the TSF data on which they operate as they are available to each of the defined administrative (security) roles for each of the administrative interfaces of the TOE.

Item	Objective ID	SFR ID	Rationale
	necessary to support the administrators in their management of the security of the TOE.	FMT_SMF.1	FMT_SMF.1 requires the TSF be capable of performing the specified security management functions.
9	O.Notify The TOE will notify responsible personnel when designated events occur in the assessment process.	NMA_NOT_EXP.1	NMA_NOT_EXP.1 defines the events that generate notifications during the collection and analysis of the asset data and also defines the users to whom the notifications are sent.
10	O.Password The TOE will be able to support an administrator defined password policy.	FIA_SOS.1	FIA_SOS.1 defines the TOE's password policy including each parameter that can be configured by the administrator.
11	O.ProtectAuth The TOE will provide protected authentication feedback.	FIA_UAU.7	FIA_UAU.7 specifies that the user's password will be masked on input.
12	O.RobustTOEAccess The TOE will provide mechanisms that control a user's logical access to the TOE by identification and authentication of that user.	FIA_AFL.1	FIA_AFL.1 specifies that a user account will be disabled after a defined number of invalid login attempts thus preventing brute force attacks.
		FIA_UAU_EXP.2 FIA_UAU.5	FIA_UAU_EXP.2 requires that all TOE users authenticate themselves to the TOE either through the TSF's authentication mechanism or by a mechanism in the Operational Environment that has been invoked by the TSF before being able to access any TOE functionality or data.
		FIA_UID.2	FIA_UID.2 ensures that every user is identified before the TOE performs any mediated functions.
13	O.TransProtect The TOE will, in conjunction with the operational environment, establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components.	FPT_ITT_EXP.1	FPT_ITT_EXP.1 defines the TOE's role in secure communications between TOE components. The TOE establishes with the help of the underlying Operational Environment network infrastructure, to establish a secure channel that relies on encryption and certificate services provided by the TOE. The TOE then uses only this logically distinct and trusted channel for component to component data transmissions.

6.3.3 Assurance Rationale

Evaluation Assurance Level EAL2 augmented with ALC_FLR. was chosen to provide a moderate level of assurance due to the requirements of DoD customer.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7.1 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.9: Logical Scope of the TOE .

The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions From Logical Scope	Sub-Functions	SFRs
Audit Generation	SA-1 Audit Generation	FAU_GEN.1
		FAU_GEN.2
Audit Review	SA-2 Audit Review	FAU_SAR.1
		FAU_SAR.3
Identification and Authentication	IA-1 User Login Security	FIA_AFL.1
		FIA_SOS.1
		FIA_UAU.7
	IA-2 User Security Attributes	FIA_ATD.1
	IA-3 User Identification & Authentication	FIA_UAU_EXP.2
		FIA_UAU.5
		FIA_UID.2
Security Management And Access Control	SM-1 Management Functions	FMT_SMF.1
		FMT_MTD.1
	SM-2 Management Security Roles	FMT_SMR.1
	SM-3 Management Access Control	FMT_MTD.1
		FMT_SMR.1
Trusted Channels	TC-1 Trusted Communications	FCS_CKM.1
		FCS_CKM.4
		FCS_COP.1
		FPT_ITT_EXP.1
Monitoring and Management of Network and Risk and Compliance Assessment	RC-1 Asset Data Collection	NMA_COL_EXP.1
	RC-2 Risk and Compliance Evaluation	NMA_EVL_EXP.1
	RC-3 Asset Notifications	NMA_NOT_EXP.1
Protection of TSF	TSF-1 FIPS Self-test	FPT_TST_EXP.1

7.1.1 Security Audit Functions

7.1.1.1 SA-1: Audit Generation

(FAU_GEN.1, FAU_GEN.2)

The Central Server generates individual audit records of security significant events and associates each auditable event with the identity of the TOE user account that caused the event. This is generated and stored separately from the host OS's audit records. The TOE provides a decentralized auditing functionality. The Central Server stores the audit trail at the OS level within the SecureVue directory tree. The events recorded for each TOE component are found in the tables in FAU_GEN.1.

The following fields are recorded:

- **Time** (date and time of the event)
- **Subject Identity** (username and administrative role – if applicable)
- **Remote Address** (address of remote terminal - if applicable)
- **Type of Event** (event name)
- **Event Description** (includes event outcome)

  Additional information as specified in Table 6-2.

There is no audit generated from the Data Collectors.

Operational Environment Support

SA-1: Audit Generation is supported by the Operational Environment through:

- Protection of the stored Audit Records
- Reliable timestamps for the audit records

7.1.1.2 SA-2: Audit Review

(FAU_SAR.1, FAU_SAR.3)

To view the audit records an administrator or user given the correct permission can use either the Administration tab → Diagnostics which has several options to view all user activity or search from the ForensicVue tab. These viewing functions give the administrator the ability to custom query (search and sort) the audit data based on ***User, TimeStamp, and/or Activity.***

The administrators cannot modify or delete audit data through the TOE interfaces.

7.1.2 User I&A Functions

7.1.2.1 IA-1: User Login Security

(FIA_AFL.1, FIA_SOS.1, FIA_UAU.7)

The TOE employs password masking during input, and a password policy that controls the password length and complexity when the user has been set to authenticate via Native Password handling (see IA-3 for further authentication options). The password policy also includes hardcoded parameters for the implementation of a failed authentication handling (3 failed attempts = account lockout for 5 min.) mechanism and to force the re-authentication of a user after a period of non-activity to ensure login security.

The TOE controls the strength of authentication passwords through the parameters in the SecureVue password policy specified in Table 6-5: SecureVue Password Policy Rules.

The SecureVue Password Policy (FIA_SOS.1) is hardcoded and NOT configurable. The hardcoded values determine the length and character sets that need to make up an acceptable password and is different for each role. The more privileged the role the longer the password length requirement.

- For the Administrator and Super Administrator the password length has to have a minimum of 12 characters but no more than 31. The password must be made up of alphanumeric characters where 1 char must be a number and 1 char must be a special character. Administrators are forced to change password on initial login.

- For a Power User the password length has to have a minimum of 8 characters but no more than 31. The password must be made up of alphanumeric characters where 1 char must be a number and 1 char must be a special character.

- For the User the password length has to have a minimum of 8 characters but no more than 31. The password must be made up of alphanumeric characters where 1 char must be a number and 1 char must be a special character.

- For the Alert User the password length has to have a minimum of 8 characters but no more than 31. The password must be made up of alphanumeric characters where 1 char must be a number and 1 char must be a special character.

The following are other authentication failure handling parameters that are not configurable and are covered under FIA_AFL.1:

Maximum Failed Login Attempts The number of unsuccessful login attempts that may be made before the client IP address is locked out. Once the IP address is locked out, the TOE doesn't allow any login attempts coming from that user for a period of time. Hardcoded value of 3

Failed Login Time Frame The time frame allowed for unsuccessful login attempts is hardcoded at 5 minutes. A client will be locked out when the maximum failed login limit is met within the specified time frame. For example, if an individual attempts unsuccessfully login 3 times within 5 minutes, the user account is locked out for 5 minutes (hardcoded **Lockout Time** value). After 5 minutes (or a system reboot whichever happens first) the ability to login under that username is allowed again and the cycle of 3 attempts in 5 minutes starts again. There is no permanent lockout threshold.

(FIA_AFL.1)

In addition to the use of the policy parameters defined above, the TOE enhances user authentication security by masking the password upon input for username/password authentication or password creation. (FIA_UAU.7)

7.1.2.2 IA-2: User Security Attributes

(FIA_ATD.1)

The TSF maintains the following security attributes for each individual TOE user:

- **Username** (Login Name / Account Name)
- **Password** (Stored encrypted using AES DATABASE Key)
- **Authentication Mechanism** (Radius, AD, or native)
- **Enable/Disable account flag** (Disabled accounts cannot access the system)
- **Email ID** (Used for email notifications)
- **User Group** (Administrative Role / Security Role)
- **Device Group** (Used to restrict user to certain groups of devices)
- **Report Selection** (Used to restrict what reports a user can access based on role/group assignment)

The User Accounts page of the Dashboard Central Server GUI is used to create and modify all accounts. This information is stored in the Central Server database.

Central Server authenticated users may change their own passwords via the GUI.

7.1.2.3 IA-3: User Identification & Authentication

(FIA_UAU_EXP.2, FIA_UAU.5, FIA_UID.2)

Each individual must be successfully identified and authenticated with a username and password by the TSF or by an authentication service in the Operational Environment that has been invoked by the TSF before access is allowed to the TOE.

An administrator can add new user accounts to SecureVue by the following ways:

- Create a new user for native password handling (TOE authentication decision)
- Import Windows System Users (External authentication decision)
- Add Active Directory server (External authentication decision)
- Import Active Directory User (External authentication decision)
- Add RADIUS server (External authentication decision)

For native password authentication the TOE collects the I&A information from the potential user over a secure channel (https://ServerIP entered into browser) via a pop-up (Java applet) window. The secure channel is established in the operating environment between the browser and the Apache/Microsoft IIS server (both of which are out of scope).

Each user has the type of authentication assigned to it (AD, RADIUS, or Native). If a user is defined as AD or RADIUS and that server is down (can't be found) then the login query will result in a Fail decision.

The TOE's hardcoded password policy cannot be modified.

In all cases the Central server is responsible for enforcing the I&A decision.

An imported user has an account created in the TOE for binding a group assignment to that user. However, the I&A decision remains with the external source (OS, RADIUS, or AD server).

NOTE: The TOE does not support generic LDAP directory mechanisms. The TOE only claims integration capability with Active Directory and RADIUS. The TOE uses LDAPv3 to communicate with the AD server in order to import users.

Operational Environment Support

IA-3: User Identification & Authentication is supported by the Operational Environment through:

- Use of an optional RADIUS or Active Directory Server
- Trusted communications implementation to external authentication mechanism

7.1.3 Security Management Functions

7.1.3.1 SM-1: Management Functions

(FMT_SMF.1, FMT_MTD.1)

The TOE is capable of performing the security management functions as defined in Table 6-6: Management of TSF data (Central Server).

All management functions are limited to the administrative roles as defined in Section 7.1.3.2 SM-2: Management Security Roles below.

The management functions for the Central server are accessible through the Central Server's web based GUI.

The Data Collectors completely rely on the OS for access control protection.

Operational Environment Support

SM-1: Management Functions is supported by the Operational Environment through:

- Protection of TOE executables

7.1.3.2 SM-2: Management Security Roles

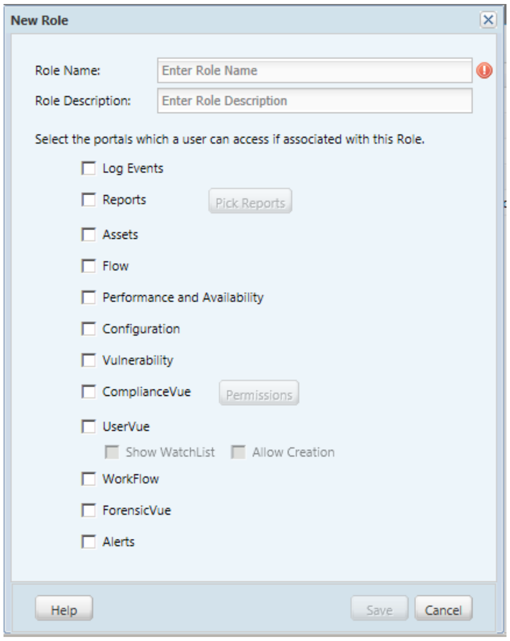
(FMT_SMR.1)

The TOE maintains administrative roles that determine the access an account holder has to the management functions and TSF data. All users of the TOE have access to management functions and TSF data and are considered administrators. The administrative role is determined by the User Group attribute of an individual's account.

The Management access control policy for the management functions and TSF data are described further in SM-3.

The TOE supports 5 types of default user roles plus the ability to create custom roles:

- **Super Administrator:** There has to be one Super Administrator (also referred to as Super Admin) to manage the TOE. The Super Administrator is used to install the TOE. Once the TOE is installed the functionality of the Super Administrator is the same as the Administrator. However, when this role is assigned to an "administrator" user, the TOE prevents that user account from being deleted.
- **Administrator:** An Administrator can manage entire application with exclusive rights to control, create, delete, and edit even other users with customized privileges. Users from this group have most rights over SecureVue GUI. Users from this group can also initiate FIPS SELF-TEST and re-generate Communication Key commands. Only one administrator can be assigned the Super Administrator role.
- **Power User:** Users in this group can be classified as read-only admins. They cannot manage Devices, Hosts, Groups, Users, Topology and Licenses. The Power User can create, edit, delete and view profiles, however, access to Collection-based policies and generation of file-based profiles is restricted.
- **User:** User accounts in this group can only generate all or few instant reports sections depending on the privileges assigned in the user policy. This role's access to reports and functions can only be customized by the Super Admin.
- **Alert User:** User accounts in this group have access to just the Alerts portal in the main console. Can only view, acknowledge, and clear alerts to which they have been granted access. Cannot edit, copy, delete, or create alerts, and cannot access the rule templates.
- **Custom User Roles:** Administrators can create custom users roles by assigning privileges and permissions to existing roles or completely new roles. For example the Alert user is a custom user role with only having the Alert privilege assigned.



New Role

Role Name: Enter Role Name

Role Description: Enter Role Description

Select the portals which a user can access if associated with this Role.

- □ Log Events
- □ Reports
- □ Assets
- □ Flow
- □ Performance and Availability
- □ Configuration
- □ Vulnerability
- □ ComplianceVue
- □ UserVue
  - □ Show WatchList □ Allow Creation
- □ WorkFlow
- □ ForensicVue
- □ Alerts

7.1.3.3 SM-3: Management Access Control

(FMT_MTD.1, FMT_SMR.1)

The TOE implements a role based access control policy (referred to as the SecureVue Management Access Control Policy in the ST).

A user group must be created (or use defaults) prior to assigning users to the group. When a user group is created the administrator has to assigned privileges and permissions to that group. This forms a role (i.e role name = group name).

When a user is created it has to be assigned to a user group (role) and saved.

After the user has successfully authenticated, the TOE determines if the function is available to that role. If the role does not have the privilege or permission the function is not activated (i.e the GUI doesn’t present the function).

7.1.4 Cryptographic Support

7.1.4.1 TC-1: Trusted Communications and Crypto Support

(FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_ITT_EXP.1)

The TSF includes a trusted communication infrastructure that provides trusted communication channels among its distributed application components. The ‘trusted communication channel’ among distributed application components ensures the two end points, (i.e., two components) are authenticated, their identity is associated to the data they transfer and that the data transferred is protected from modification and disclosure. The trusted communication channel between TOE components is established even if the components are installed on the same platform such as the Regional Server and Data Collector can be installed on same platform.

Establishment of these trusted communications channels depend on the functionality of both the TOE (crypto module) and the Operational Environment (network infrastructure and host TCP/IP protocols).

SecureVue uses FIPS 140-2 validated (Certificate #1051) OpenSSL cryptographic module Version 1.2. The services used by SecureVue are Key Transfer, Communications, Database, File/Password-encryption, and Decryption of data between TOE components.

During SecureVue Central's first boot-up, the Database AES Key, File-Encryption AES Key and Communication AES Key are generated (all are AES 192 bit keys). While installing Collector Servers, a request for these keys is sent to Central Server so that subsequent communication and data transfer between them can be done securely.

Communications between the TOE components is supported by the use of the operational environment's Transmission Control Protocol/Internet Protocol (TCP/IP) and network infrastructure. The Central Servers and Data Collector are designed to communicate with each other via an AES key specifically generated for communication. The component data is encrypted using the Communication Key and sent to other components. The transferred data is decrypted at the other end using the Communication Key.

Communications to the browser is support by the operational environment using Apache or Microsoft IIS Server. Apache includes the use of a separate instantiation of OpenSSL that is not part of the FIPS certified cryptographic module but is part of Apache installation. MS IIS uses the default MS crypto module provided with the OS. The trusted channel used between the browser and the Central Server (handshaking and cipher suite) uses of FIPS certified algorithms.

The crypto library supports zeroization for key destruction. Keys are generated according to Table 6-3.

7.1.4.1.1 Communication-encryption

A Communication AES Key is generated and updated at every boot-up of Central Server. Communication that involves commands, events transfer between Central Server, and Data Collector is encrypted using the Communication Key.

SecureVue GUI has an option to schedule generation of the Communication AES Key.

7.1.4.1.2 Decryption

SecureVue component data is encrypted using the Communication Key and sent to other components. The transferred data is decrypted at the other end using the Communication Key.

SecureVue decrypts the database internally using the DATABASE Key before it is displayed in the reports.

Operational Environment Support

TC-1: Trusted Communications is supported by the Operational Environment through:

- Network infrastructure
- TCP/IP protocols

7.1.5 Risk and Compliance Assessment Functions

7.1.5.1 RC-1: Asset Data Collection

(NMA_COL_EXP.1)

The information security and event management, through real-time monitoring and concise reporting solely depends on the policies enforced for event data collection. SecureVue provides a visual interface to create and manage the policies for specific event data collection. An Administrator can create and enforce the event collection policies and policy templates for effective event management. The Policy Manager contains the following tab for policy creation:

- **Collection:** Use this tab to create and manage policies to collect event data from specific host (s).
- **Template:** Use this tab to create templates, which can be used to create and manage policies for event collection with specific settings.

The Collection tab on the Policy Manager displays the list of available collection policies. An administrator can Add, Edit and Delete a collection policy from here. There are factory made ready-to-use, collection policies available in SecureVue, they are:

- **Collect All:** This policy is meant to collect all the events irrespective of the severity level from the configured device(s).
- **No Collection:** This policy disables the collection of all the events from the devices and hence no data is available for monitoring or reporting if this policy is enforced.
- **Monitoring Only:** This Policy is meant to collect and stream events of Debug and higher severity levels for monitoring. It also appends raw logs of attack events, virus events and the severity events of debug and higher to the Delta.
- **Performance Only:** This Policy is meant to collect all the performance data coming from the licensed Devices and Hosts (MIB) every 1 min using the SNMP agent over port 161.
- **Config Only:** This Policy is meant to collect all the configuration data on the licensed Devices and Hosts every 1 min using the SSH protocol over port 22.
- **Top Priority Events Only:** This Policy is meant to stream top priority events starting from warning to higher severity level for monitoring. The events of Debug and higher severity levels are collected. It also appends raw logs of attack events, virus events and the severity events of emergency and higher to the Delta.
- **Events and Config:** This Policy is meant to collect all the configuration data on the licensed Devices and Hosts every 1 min using the SSH protocol over port 22. The events of Debug and higher severity levels are collected.
- **Events and Performance:** This Policy is meant to collect all the performance data coming from the licensed Devices and Hosts every 1 min using the SNMP agent over port 161. The events of Debug and higher severity levels are collected.
- **Events and Vulnerabilities:** This Policy is meant to collect all the vulnerability data from the vulnerability scanners (such as Nessus) for vulnerability analysis. It stream events starting from warning to higher severity level for monitoring. The events of Debug and higher severity levels are

collected. It also appends raw logs of attack events, virus events and the severity events of emergency and higher to the Delta.

The Data Collector is responsible for the actual implementation of data collecting. Table 6-7 lists the different methods of collections and the minimum information collected is:

- ***IP address of an discovered device***
- ***date and time of the collection***
- ***Data Collector IP***
- ***Total count of events parsed***

The Central Server is responsible for the management of the collection policy.

Protocols used for collecting information. This table is detailed to show inbound and outbound data flow, subsystem (or module) and its purpose.

Protocol	RFC	Executable	*Inbound/ Outbound*	Description
Syslog	RFC 5424	Syslogserver.exe	*Inbound*	Syslog traffic over UDP/TCP
RDEP	RFC 3080		*Outbound*	API to collect from Cisco IDS devices
SDEE	NA		*Outbound*	API to collect from Cisco IPS devices
Flow	NA		*Inbound*	Netflow, CFlow, Natlog, Netsream, SFlow
LEA	NA	LeaServer.exe	*Outbound*	Log Export API to collect from Checkpoint devices
WMI	NA	HostCollector.exe	*Outbound*	Windows Management Interface to collect events and configuration from Windows hosts. Also used to collect performance metrics from windows hosts
API	NA		*Outbound*	Windows Eventlog API to collect events from windows hosts
Syslog	RFC 5424		*Inbound*	Collect syslog events from Unix hosts
Snare	NA		*Inbound*	Collect Snare events from windows hosts
ADSI	NA		*Outbound*	Collect userdetails from Active Directory repository
Radius	RFC 2865		*Inbound*	Collect userdetails from Radius repository
VMWare SDK	NA		*Outbound*	Collect configuration details from VMWare ESX/ESXi servers

DCOM	NA		*Outbound*	DCOM Interfaces used to connect to enumerations of windows updates on windows hosts.
SSH	RFC 4251		*Outbound*	Running remote commands on Unix hosts to collect config/asset information
SNMP	Various	SnmpMon.exe	*Outbound*	Get performance counters from any asset supporting SNMPv1,v2,v3
SNMPTrap	Various	SnmpTrapAgent.exe	*Inbound*	Receive SNMP traps sent by devices and process them as events.
SSH	RFC 4251	ConfigMon.exe	*Outbound*	Connect to any device using SSH to run commands and pull configuration information
Telnet	Various		*Outbound*	Connect to any device using Telnet to run commands and pull configuration information
FTP/SFTP	RFC 959		*Outbound*	Pull configuration using FTP.
NessusAPI	NA		*Outbound*	Use Nessus API to trigger vulnerability scans or pull results.
Rapid7API	NA		*Outbound*	Use Rapid7 API to trigger vulnerability scans or pull results.
QualysAPI	NA		*Outbound*	Use Qualys API to trigger vulnerability scans or pull results.
CPMI	NA		*Outbound*	CPMI to collect configuration from Checkpoint Management device
File	NA		*Inbound*	Process vulnerability scan results fed in form of flatfile/XML.
ODBC	NA	DBCollector.exe	*Outbound*	Vulnerability data from ISS Scanner Vulnerability data from Retina Log Events with virus/IDS/fw/spyware logs from CSA Log Events with C2 security logs from MSSQL Audit Agent Log Events with C2 security logs from Oracle Audit Agent Vulnerability data from STAT Guardian Log Events with virus/IDS/fw/spyware data from McAfee ePO

				Log Events with virus/IDS/fw/spyware from CA HIPS Vulnerability data from FoundStone Log Events with virus/IDS/fw/spyware data from Symantec Antivirus Vulnerability data from Retina REM

Operational Environment Support

RC-1: Asset Data Collection is supported by the Operational Environment through:

- Use of an optional third-party asset discovery/vulnerability scanner
- Use of an optional third-party enterprise management database
- Protocols

7.1.5.2 RC-2: Risk and Compliance Evaluation

(NMA_EVL_EXP.1)

The TOE performs the following evaluation functions on the collected IT network asset data:

Group	Method Description
Monitoring	Event correlation
	Comparative Analysis
Vulnerability	Event correlation from third party scanner
	Comparative Analysis
Configuration (support for GRC)	Event correlation
	Comparative Analysis
	Risk assessment
Asset	Comparative Analysis
	Trend Analysis
NBA Detection	Comparative Analysis
	Usage Analysis
Performance	Statistical analysis
	Trend analysis
Forensics	Event correlation

The analysis provided by the TOE is driven and governed by the same policies as the collection procedures. In SecureVue a policy is a formal set of rules to define the course of action that the user needs to take under specific circumstances. A rule can dictate— which devices or hosts to consider, what event type to filter or negate, which entities with what values to add and so on. The user can associate a severity level to the Policy created. A policy is created on the customized device and/or host based rules or the existing rule templates. On implementation of a policy the Administrator can choose to -- trigger an alert notification, or simply classify the Policy under an Event class by associating it to a report query. An Administrator can add, edit, copy or delete a Policy.

The analysis methodology include threshold verification, sequence matching, comparative (historical deltas), comparative against selected standards templates (for GRC Auditor function), and filtering based on policy or real time user input requests.

Note: The correctness and conformance of the standards templates to any government or commercial standard is by Vendor assertion; the correctness and conformance of the templates to any standard will not be part of this evaluation.

7.1.5.3 RC-3: Asset Notifications

(NMA_NOT_EXP.1)

An Alert if triggered is indication of an unwanted pattern/activity happening in the network. Administrator must be notified with these patterns in the form of alerts so that he can take corrective action in time.

When an alert is generated, it can viewed straight away on the Alert Manager (part of the GUI) by leaving the Alert Notification check box clear in the Configure Alert window or alternatively have it delivered by using any one or both the ways of notification, they are:

- E-mail
- SNMP Trap

Operational Environment Support

RC-3: Asset Notifications is supported by the Operational Environment through:

- Use of an optional SMTP Server
- Use of an option SNMP Server

7.1.6 Protection of TSF

7.1.6.1 TSF-1 FIPS Self-test

(FPT_TST_EXP.1)

SecureVue boot-up process performs a suite of self-tests to ensure the integrity and correct operation of the cryptographic algorithms. Power-up tests include cryptographic algorithm available answer tests and integrity tests. These tests are initiated automatically every time when SecureVue boots up (after power-off, reset, re-boot etc.). Availability of required Keys is verified as part of Power-Up Self-Tests. If these keys are not found or if any of the self-test fail, application does not initialize and enter in to an error state, preventing users from accessing the services and performing any cryptographic operations i.e. no FIPS mode cryptographic functionality will be available until after successful execution of all power-up tests. The integrity tests are performed using a HMAC-SHA-256 digest calculated over the object code of SecureVue.

An ***Administrator*** can also request the module to perform self-tests using the “FIPS Self-Test” button provided in the SecureVue GUI.

If the tests fail a Log file is created giving brief description of FIPS Self-Test Suite results, and Transitions to a Power-OFF state.