RedSeal Networks, Inc.™
RedSeal Platform v7.0.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1

Prepared for:

REDSEAL NETWORKS

RedSeal Networks, Inc.
940 Stewart Drive, Suite 101
Sunnyvale, CA 94085
United States of America

Phone: +1 888 845 8169
Email: info@redsealnetworks.com
http://www.redsealnetworks.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the RedSeal Platform v7.0.1, and will hereafter be referred to as the TOE throughout this document. The TOE is a security risk management solution that provides continuous monitoring of network access paths, configuration auditing for network devices, and provides corporate and standards-based policy compliance reports.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	RedSeal Networks, Inc. RedSeal Platform v7.0.1 Security Target
ST Version	Version 1
ST Author	Corsec Security, Inc.
ST Publication Date	7/9/2014
TOE Reference	RedSeal Platform v7.0.1 build 84; including RedSeal Server Manager v1.4.0 build 45
FIPS[1] 140-2 Status	Level 1, Validated cryptographic module, Certificate No. 2058

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

The RedSeal Platform is a Network Infrastructure Security Management (NISM) platform that continuously identifies critical attack risk and non-compliance in complex enterprise security infrastructure. It provides organizations with a firm understanding of where security is working, where improvement is needed, and where the greatest cyber-attack risks lie. This understanding, or "security intelligence", enables organizations to allocate resources where needed, embed security into daily operations, and take prioritized action to systematically reduce attack risk over time. At the heart of RedSeal is a visual, end-to-end model of complex security infrastructure. The model includes the network (routers, load balancers, wireless controllers, etc.) connected assets and attributes (hosts, vulnerabilities, business value, etc.) and security controls (firewalls) that protect those assets. Automated analytics then examine the model to deliver security intelligence that drives both immediate defensive action and longer term security strategy. Examples of RedSeal security analytics include access policy compliance (PCI, NERC, etc.), perimeter defense, network segmentation, secure device configuration, exposure-based vulnerability management, firewall rule optimization, security performance management, scan gap detection, and unmanaged device identification. The RedSeal Platform is comprised of a Server (available as software for Windows, a hardware appliance, or an OVA virtual appliance), a Client GUI compatible with user desktop operating systems, and an optional supervisory module for managing multi-server deployments (RedSeal Server Manager for Windows). RedSeal offers extensive human and machine interface options to enable integration with enterprise-class operations and systems. Integrations include leading network and security devices, vulnerability assessment scanners, configuration database management systems, ticketing and workflow management systems, endpoint management systems, GRC systems, SIEMs, syslog servers, GUI client and web-based human interfaces, and a published REST API for custom integration. All RedSeal components support LDAP and RADIUS[2] authentication.

RedSeal collects configuration files and vulnerability scans from the network and performs a set of network access checks against all known ingress points within an organization's network infrastructure. It uses this information to build a topology map. It then compares the configurations and data it receives against a set of "best practices" baselines and defined zone-based access policies, to identify high-risk security violations and policy compliance issues such as weak firewall policies, default passwords, insecure services, known vulnerabilities, and access permitted by the as-built network that violates zone access policies. RedSeal uses this information, user-defined values assigned to assets, and the asset exposure to threat sources and potential downstream access to provide risk scoring and annotated maps with potential attack vectors. It also provides advanced reporting capabilities, enabling network administration and security personnel to identify and mitigate configuration issues and other threats.

The RedSeal architecture is comprised of three major components: RedSeal Server, RedSeal Client, and RedSeal Server Manager. The RedSeal Client is used for the management of a single RedSeal Server, while the RedSeal Server Manager is used for the management of one-to-many RedSeal Servers.

The RedSeal Server component is comprised largely of a Java-based server (also called the RedSeal Server) as well as an Admin server which monitors and controls system processes and configuration. The RedSeal Server includes reporting and analytics engines as well as a Threat Reference Library (TRL). Additionally, an Apache Tomcat server provides a web-based reporting interface and exposes a Representational State Transfer (REST) Application Programming Interface (API) for third-party integration. The REST API is also used for management from the RedSeal Server Manager, over Hypertext Transfer Protocol Secure (HTTPS). The RedSeal Server component provides an Admin Graphical User Interface (GUI) for Windows, which provides initial configuration tasks. On the appliance- and virtual appliance versions, a Command Line Interface (CLI) provides initial configuration and database management, but has been strictly limited to provide only these functions. This CLI is accessed via a direct, serial connection. Lastly, a PostgreSQL server provides the backend for the RedSeal Server's application storage. RedSeal uses an object-relational mapping library and a business intelligence and data visualization toolkit to analyze and display network data.

[2] RADIUS – Remote Authentication Dial In User Service

Import of data from monitored networked assets is achieved using a plugin architecture comprised of two different types of plugins: Communications and Data. The Communications Plugins provide connectivity to external devices for facilitating data import, supporting a wide variety of protocols, including HTTPS, SMB[3], SSH[4], SCP[5], SFTP[6], JDBC[7], and other vendor-specific protocols to access device data directly from the device or from CMDBs[8]. The Data Plugins provide parsers for vendor-specific device configuration files and vulnerability scan data. RedSeal can monitor most layer 3 network devices with the use of these vendor-specific Data Plugins. The Data Plugins include specific commands and credentials needed for each type of device across a wide variety of vendors.

The RedSeal Server Manager enables centralized monitoring, administration, and management of one or more RedSeal Servers from a single administrative web interface, protected with HTTPS. It aims to improve operational efficiency in an organization through centralized administration, automation of administrative tasks, troubleshooting support, and monitoring key health indicators and security metrics across multiple RedSeal Servers. Management of the RedSeal Server is achieved using a REST API. RedSeal Server Manager users can be given permissions to monitor and manage all attached RedSeal Servers or can be assigned to specific RedSeal Servers. The graphical tool on the RedSeal Server Manager allows administrators to view the health of all attached RedSeal Servers, initiate backups and restores, and perform software updates. This tool also provides consolidated views of key security metrics and health indicators gathered from each RedSeal Server across the network to provide a common dashboard capable of showing an entire enterprise-class network and drilling down to detailed data. In addition, the Server Manager includes a Java Virtual Machine (JVM) with a FIPS-validated cryptographic module and a modified Apache Tomcat server. These components ensure protected communications between the Server Manager and its attached RedSeal Servers when using HTTPS with Transport Layer Security (TLS) v1.2. The RedSeal Server Manager also includes a MongoDB server to store monitored network reports received from the RedSeal Servers, RedSeal Server health indicators, and TRL updates.

The RedSeal Client is comprised solely of the Client User Interface (UI) application, which is a Java thick client. The RedSeal Client is downloaded from the RedSeal Server and is used to manage the RedSeal Server using HTTPS with TLS v1.2. The RedSeal Server also sends the Client topology and query results to display for Client users. The RedSeal Client allows users to view the network topology, drill down to determine the sources of modeling issues and risks, create zones and policies, analyze the network, and create reports describing risk and vulnerability data.

Due to the capabilities described above, RedSeal can assist any organization in understanding the degree of risk in their network infrastructure. RedSeal enables commercial organizations and Federal agencies to rapidly establish a risk management framework and continuously monitor a risk management program described in FISMA and underlying documents such as **NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations** and **NIST 800-137 Risk Management Framework**. With RedSeal, Federal agencies can access to quantifiable metrics that show current risk as well as risk trends. RedSeal's Zones and Policy enable Federal CIO's and CISO's to validate that their networks are compliant with organizational missions and business functions, as well as the requirements of federal legislation, directives, regulations, policies, and standards/guidelines. The Risk feature of RedSeal enables information security professional to quickly identify and quantify where the greatest risk resides in their environments, thus allowing them to focus their remediation and mitigation efforts on the most at risk parts of their IT infrastructure.

RedSeal also automates Continuous Monitoring / Auditing **NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems**, which encourages the use of automation to

[3] SMB – Server Message Block
[4] SSH – Secure Shell
[5] SCP – Secure Copy
[6] SFTP – Secure File Transfer Protocol
[7] JDBC – Java Database Connectivity
[8] CMDB – Configuration Management Database

provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

1.4.1 TOE Components

The following components comprise the software-only TOE:

- RedSeal Server v7.0.1
  - RedSeal Server
  - Admin Server
  - Apache Tomcat Server
  - JVM
  - PostgreSQL database
  - Communications Plugins
    - Concurrent Version System (CVS)
    - File Transfer Protocol (FTP)
    - HTTP(S)[9]
    - SCP
    - SFTP
    - SSH
    - Telnet
    - Windows File Share
  - Data Plugins
    - RedSeal Generic Security Device (GSD)
    - RedSeal Scan comma-separated value (CSV)
    - RedSeal XML and CSV Format
  - CLI (hardware appliance and virtual appliance)
- RedSeal Client v7.0.1 – a thick client UI that can be installed as a 32-bit or 64-bit process
- RedSeal Server Manager v1.4.0
  - Management Server
  - Apache Tomcat Server
  - JVM
  - Database

The TOE also supports a number of vendor-specific plugins, such as Cisco IOS and Juniper JunOS that were not evaluated. Vendor-specific Communications Plugins are also supported by the TOE, such as Tripwire and Qualys. These were also not evaluated. For a full list of the additional plugins available please see *RedSeal Plugin Guide* which is available at www.redsealnetworks.com/support. Figure 1 shows the deployment configuration of the TOE. No claims were made about secure communications between RedSeal Client and RedSeal Server or between RedSeal Server Manager and RedSeal Server.

[9] HTTP – Hyptertext Transfer Protocol or HTTPS – Hypertext Transfer Protocol Secure

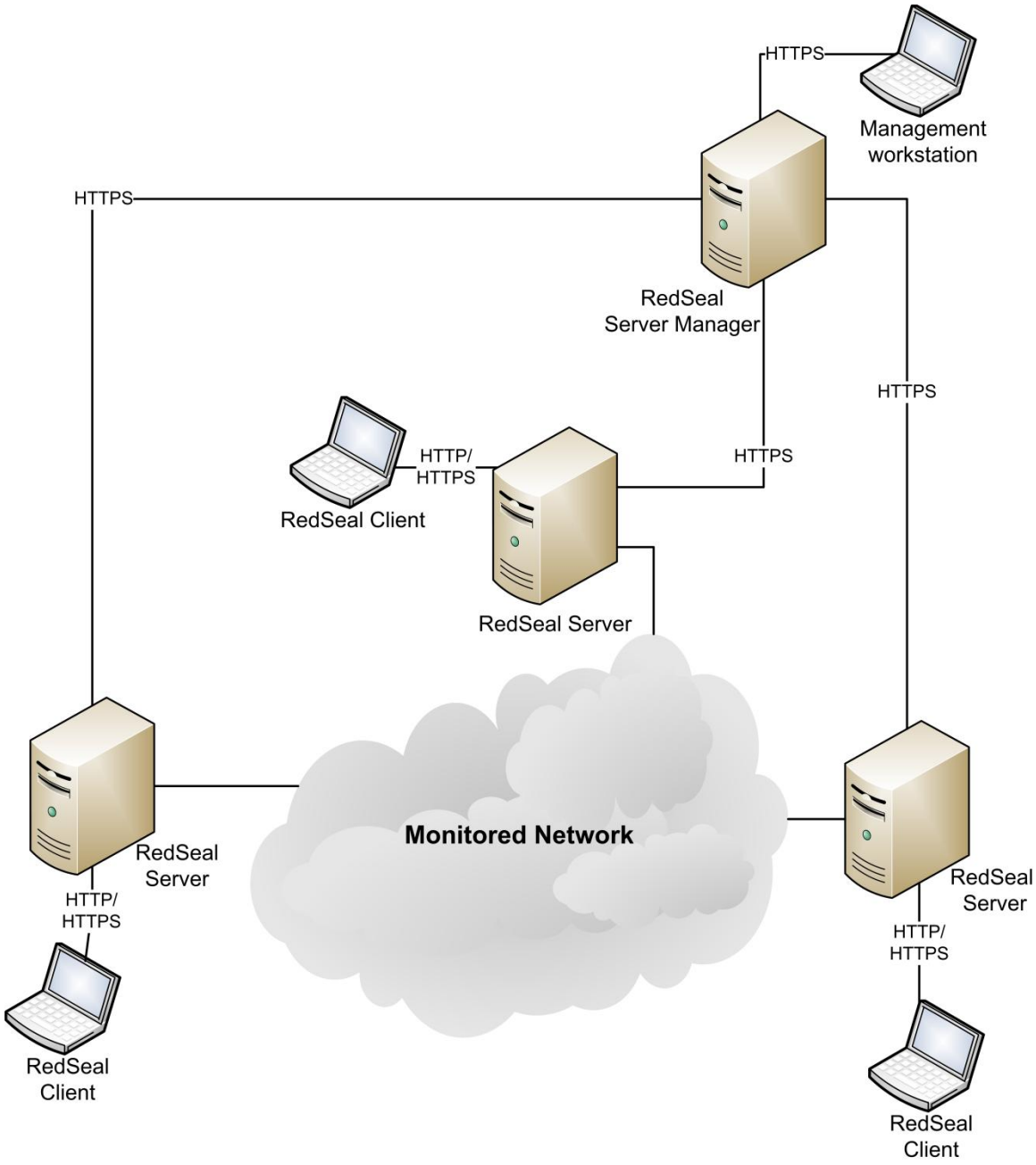

Figure 1 Deployment Configuration of the TOE

1.4.2 Brief Description of the Components of the TOE

The TOE consists of the following software components:

1.4.2.1 RedSeal Client

The RedSeal Client is a Java thick client that is downloaded from the RedSeal Server and used to manage a single instance of the RedSeal Server. The RedSeal Client can be installed as a 32-bit or 64-bit process depending on the underlying system.

1.4.2.2 RedSeal Server Manager

The RedSeal Server Manager is used to manage multiple RedSeal Servers. It monitors server health across multiple server instances. The RedSeal Server Manager imports analysis performed on RedSeal Servers for a more complete view of a larger network. Logs from each RedSeal Server can also be imported to the RedSeal Server Manager to assist in troubleshooting. The RedSeal Server Manager sends requests to RedSeal Servers, which return monitored network data to the RedSeal Server Manager.

The RedSeal Server Manager uses a MongoDB to provide database storage for summary information, attached RedSeal Server health indicators, and TRL updates. The attached RedSeal Servers send summary information in file format to the RedSeal Server Manager. This information is aggregated and used to build the graphical views for administrators. Detailed sensitive data such as data collection credentials and device configuration files are kept on RedSeal Servers and are not stored in this database.

1.4.2.3 Apache Tomcat

Both the RedSeal Server Manager and the RedSeal Server include Apache Tomcat. The Apache Tomcat server provides the web-based reporting interface and exposes a REST API for RedSeal Server Manager communications with the RedSeal Server and for third party integration.

1.4.2.4 JVM

Since all RedSeal software components are written in Java or Groovy, a JVM is required to run the components. The JVM is included within the TOE boundary. Within the JVM is a Java Cryptographic Extension that includes the RSA BSAFE Crypto-J v6.1 module that provides the FIPS 140-2 validated cryptographic algorithms for HTTPS with the TOE.

1.4.2.5 Communications Plugins

RedSeal Server uses communication method specific plugins to import device configurations and vulnerability scanner data from the attached network. These plugins determine the transport mechanism used to collect the data and include proprietary protocols such as Cisco® Security Manager and common communication protocols such as HTTP(S). Only the common communication plugins listed in 1.4.1 were tested as part of this evaluation. The available communication plugins for a selected device are shown when creating a Data Collection Task. The communication plugins initiate communications with devices on the network, as instructed by the RedSeal Server.

1.4.2.6 Data Plugins

There is a data plugin for each type of device that can be monitored. The available data plugins, by manufacturer and type, are shown when creating a Data Collection Task. A data plugin can be selected when creating a collection task or an Autodetect plugin can be used to automatically select the correct data plugin for a collection task. Each data plugin contains commands and pointers to credentials for importing that device type's configurations or scan data. While the TOE supports many manufacturer specific plugins, only the RedSeal generic plugins listed in 1.4.1 were tested as part of this evaluation.

1.4.2.7 RedSeal Server

The RedSeal Server controls data collection and analysis on the TOE. The RedSeal Client and RedSeal Server Manager communicate directly with the RedSeal Server to manage collection tasks, perform analysis, and create reports. For larger networks with organizational boundaries, multiple RedSeal Servers may be used to access segmented areas of the network. Multiple RedSeal Servers may also be employed to access the same or partially overlapping areas of the network, for example when one server is used for normal operations, while a different server is used for scenario planning. The RedSeal Server provides a limited CLI for server and database maintenance and appliance setup on the hardware appliance and virtual appliance platforms only. The CLI is accessed via a direct, serial connection.

1.4.2.8 Admin Server

The Admin Server, within the RedSeal Server performs server and database administration. The CLI on the hardware and virtual appliance, accesses this server process. The Admin Server is also responsible for communications with external authentication servers, when configured.

1.4.2.9 PostgreSQL Database

The RedSeal Server uses a PostgreSQL database to store collected data, analyses, and reports. Direct access to this database is not provided. Users can query the database only indirectly through the RedSeal Server's provided functions. Administrators can back up the database and perform purge tasks through the RedSeal Server or Admin Server.

1.4.3 TOE Environment

The TOE can come pre-installed on a RedSeal hardware appliance, as a software virtual appliance that runs on VMware ESX, or as a software package that runs on a Windows server. All RedSeal components are Java-based, so the same software can run on each of these platforms.

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 TOE Minimum Requirements

Category	Requirement
RedSeal Client UI	
JVM	Java Standard Edition 7, Update 45 or later can be 32-bit or 64-bit
Operating System (OS)	MAC OS X, Microsoft Windows 7, 8, or XP, or Microsoft Windows Server 2003, 2008, or 2012
Browser	Internet Explorer v8.0 or higher Firefox 3.6 or higher
Flash	Adobe Flash Player 8 or above
Hardware	100 MB[10] of disk space and 1GB[11] of RAM[12]
RedSeal Server	
OS	Options for Windows platforms are: Windows 7 Enterprise, Windows 8 Enterprise, Windows Server 2003, Windows Server 2008, or Windows Server 2012 For hardware appliance: CentOS v6.2 For virtual appliance: VMware ESX v5.0 or higher and CentOS v6.2
Hardware	300 GB disk space

[10] MB – Megabytes
[11] GB – Gigabytes
[12] RAM – Random Access Memory

Category	Requirement
	8 GB RAM
RedSeal Server Manager	
OS	Windows 7 or Windows Server 2008
Hardware	2GB disk space and 100 GB of disk for software repository 8 GB RAM
Manager Client	Microsoft Windows 7 with Google Chrome 20 or Firefox Mozilla 10
Network	
Authentication servers	LDAP[13] server
Network devices	The TOE must be attached to a network with one or more layer 3 network device to monitor.

Caveat: LDAP authentication was not evaluated in this evaluation. Only the secure connection between the TOE and LDAP server was evaluated for this evaluation.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE. No claims were made about secure communications between RedSeal Client and RedSeal Server or between RedSeal Server Manager and RedSeal Server.

The TOE is a NISM software platform with components that run on systems with the minimum software and hardware requirements listed in Table 2. The TOE can have numerous deployment scenarios since it presents a distributed architecture. Multiple instances of the RedSeal Server and RedSeal Client UI may be used in larger networks. A basic installation of the TOE within an enterprise network is depicted in the figure below.

For the purpose of CC testing, the deployment configurations listed in Table 3 were used.

Table 3 Configurations

Name	Description
Appliance Configuration	• One instance of RedSeal Client • One instance of RedSeal Server on a RedSeal Appliance • One instance of RedSeal Server Manager on a Windows platform
Windows Configuration	• One instance of RedSeal Client • One instance of RedSeal Server on a Windows platform (with no CLI) • One instance of RedSeal Server Manager on a Windows platform

[13] LDAP – Lightweight Directory Access Protocol

Name	Description
Virtual Configuration	• One instance of RedSeal Client • One instance of RedSeal Server on a virtual platform • One instance of RedSeal Server Manager on a Windows platform

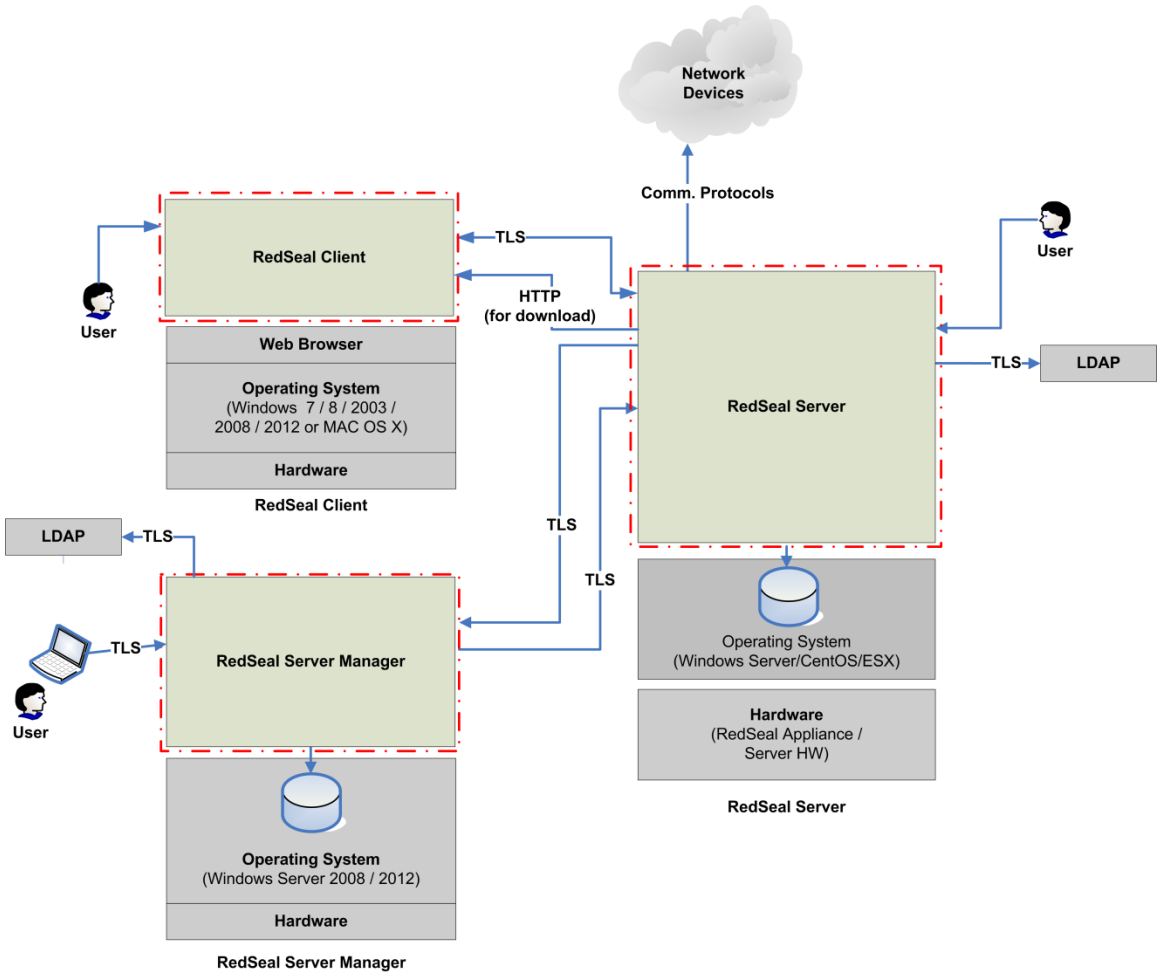

Figure 2 Physical TOE Boundary

1.5.1.1 TOE Software

The TOE is a NISM software platform. The TOE consists of at least one RedSeal Server v7.0.1, RedSeal Client UI v7.0.1, and a RedSeal Server Manager v1.4.0.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- RedSeal Networks User's Guide Version 7.0.1
- RedSeal Networks Installation and Administration Guide Version 7.0.1
- RedSeal Networks Release Notes, 7.0.1
- RedSeal Networks Data Import Plugins Guide Version 7.0.1
- RedSeal Server Manager Installation Guide 1.4.0
- RedSeal Server Manager User's Guide, Version 1.4.0

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions
- TOE Access
- Trusted Path/Channel
- Network Assessment

1.5.2.1 Security Audit

Audit generation occurs within the TOE for management events, user maintenance events, and data collection events. The TOE maintains multiple audit files that rotate logs, overwriting the oldest record when a threshold is reached. Audit records are stored in the PostgreSQL database on the RedSeal Server and are read-only for all users.

1.5.2.2 Cryptographic Support

The TOE includes a FIPS 140-2 validated cryptographic module that generates and destroys keys according to FIPS standards. Symmetric keys are generated using a Special Publication (SP) 800-90A Deterministic Random Bit Generator (DRBG). Asymmetric keys are generated according to FIPS 186-3. RedSeal uses the provided cryptographic algorithms for communications protocols, password wrapping, and TLS certificate generation.

1.5.2.3 Identification and Authentication

User's must be identified and authenticated prior to performing any action on the TOE. The TOE provides a local database for authentication.

1.5.2.4 Security Management

The TOE assigns users to the role of View, Model, or Admin on the RedSeal Client. A separate administrator account can access the CLI. The RedSeal Server Manager includes the roles Administrator, Centralized Platform Management (CPM) User, and Centralized Security Monitoring (CSM) User. The TOE only presents users with actions permitted by their roles. Audit log management, user authentication, and user account management can all be done by Admins on the RedSeal Client and Administrators on the RedSeal Server Manager. Database management can be done by administrators on the all interfaces.

1.5.2.5 Protection of the TSF

User and device passwords that are stored on the TOE are encrypted prior to storage. When passwords are sent to an external authentication server, they are sent over a secure protocol, ensuring that they cannot be disclosed or modified.

1.5.2.6 TOE Access

Users can configure the Client UI to timeout after a period of inactivity. Users on the Client interface are also presented with a warning banner after logging into the TOE. The users must accept the banner to access TOE functionality.

1.5.2.7 Trusted Path/Channel

The TOE uses its FIPS validated cryptographic module to provide a trusted channel between itself and external authentication servers and network devices. The TOE provides a trusted path to CLI administrators via a direct, serial connection.

1.5.2.8 Network Assessment

The RedSeal Platform collects configurations from network devices and stores details for each network device. It also collects vulnerability scan reports from the network. These are stored in the database with access allowed only through the RedSeal Server's query and reporting tools. The queries and reports can be requested from the Client UI or the RedSeal Server Manager. These queries are then sent to the RedSeal Server, where database access occurs, and the result is returned to the requesting user. The TOE performs analysis on this data to provide topology maps, reports, and compliance assessments. TOE users are alerted if a database storage threshold has been reached so that database maintenance can be performed to prevent data loss.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Network Time Protocol server
- Syslog server
- Admin GUI on Windows platform
- CLI access via SSH

2 Conformance Claims

This section and Table 4 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM as of 2013/09/01 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[15] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[16] and user data saved on or transitioning through the TOE. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 Threats

Name	Description
T.ADMIN ERROR	A TOE user may unintentionally install or configure the TOE incorrectly, resulting in ineffective security enforcement mechanisms.
T.FALREC	The TOE may fail to recognize non-TOE user potential attack points on the monitored network due to inaccurate data received from each data source.
T.FORGE	A non-TOE user may create a false policy causing the network analysis to incorrectly model the network.
T.MASQUERADE	A non-TOE user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.NACCESS	A non-TOE user may be able to view or modify data that is transmitted between parts of the TOE or between the TOE and a remote authorised external entity.
T.STORAGE	The TOE database may run out of storage space due to improper maintenance from a TOE users; causing audit or monitored network traffic data loss.

[15] IT – Information Technology
[16] TSF – TOE Security Functionality

Name	Description
T.TAMPERING	A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNATTEND	A TOE user on the Client UI may leave an authenticated session unattended, resulting in the possibility of a malicious or unauthorized user to mask their actions as the logged in user, resulting in a misconfiguration or alteration of the TSF behavior.
T.UNAUTH	A TOE user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 6 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 6 Organizational Security Policies

Name	Description
P.BANNER	The TOE client shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 7 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 7 Assumptions

Name	Description
A.TIMESTAMP	The IT environment provides all TOE components with the necessary reliable timestamps.
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system. The TOE is placed in the network so that is can access the required network objects.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

Name	Description
A.CRYTPO	The TOE environment will protect non-HTTPS communications between the TOE and monitored devices.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 8 below.

Table 8 Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.ALERT	The TOE will alert users if storage space in the database is reaching capacity.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of users, prevent unauthorized modification of the audit trail, and prevent loss of audit trail data.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.BANNER	The TOE client will display an advisory warning regarding use of the TOE.
O.INACTIVE	The TOE client must implement a robust mechanism for terminating user sessions after a period of inactivity.
O.MONITOR	The TOE will monitor the behavior and configurations of the network for anomalous activity.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.SEC_COMMS	The TOE must protect audit and system data as it shared over the external network.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 9 below lists the IT security objectives that are to be satisfied by the environment.

Table 9 IT Security Objectives

Name	Description
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The TOE environment will provide the capability to protect monitored system data as it is transmit to the TOE.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

4.2.2 Non-IT Security Objectives

Table 10 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 10 Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 11 identifies all extended SFRs implemented by the TOE

Table 11 Extended TOE Security Functional Requirements

Name	Description
EXT_FPT_APW.1	Protection of Administrator Passwords
EXT_NAS_MDC.1	Monitored Data Collection
EXT_NAS_ANL.1	Network Analysis
EXT_NAS_RDR.1	Restricted Data Review
EXT_NAS_STG.1	Prevention of Monitored Data Loss

5.1.2 Class FPT: Protection of the TSF

Families in this class address the requirements for functions providing integrity and management of mechanisms that constitute the TSF and of the TSF data as defined in CC Part 2.

5.1.2.1 Family EXT_FPT_APW: Protection of Passwords

Family Behaviour

Components in this family address the requirements for protection of passwords. This is a new family defined for the FPT class. The FPT class contains functional requirements that relate to the integrity of TSF data. The user's password is one element of TSF data that must be stored securely.

Component Leveling

Figure 3 Protection of Passwords family decomposition

EXT_FPT_APW.1 Protection of Passwords, requires local passwords to be stored in a protected form and requires the TOE to prevent reading of all plaintext passwords. It was modeled after the EXT_FPT_APW.1 SFR in the Network Protection Profile v1.1.

Management: FPT_APW_EXT.1

a) There are no management activities foreseen.

Audit: FPT_APW_EXT.1

a) There are no audit activities foreseen.

EXT_FPT_APW.1 Protection of Passwords
Hierarchical to: No other components
Dependencies: None.
FPT_APW_EXT.1.1
The TSF shall store local passwords in a protected form.
FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext passwords.

5.1.3 Class NAS: Network Assessment

Network Assessment involves collecting, storing, and monitoring data from devices on the attached network. The EXT_NAS: Network Assessment class was modeled after the CC FAU: Security audit class. The extended family EXT_NAS_RDR: restricted data review was modeled after the CC family FAU_SAR: Security audit review. The extended family and related components for EXT_NAS_MDC: monitored data collection were modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family and related components for EXT_NAS_ANL: network analysis were modeled after FAU_SAA: security audit analysis. The extended family and related components for EXT_NAS_STG: Prevention of monitored data loss was modeled after the CC family and related components for FAU_STG: Security audit event storage.

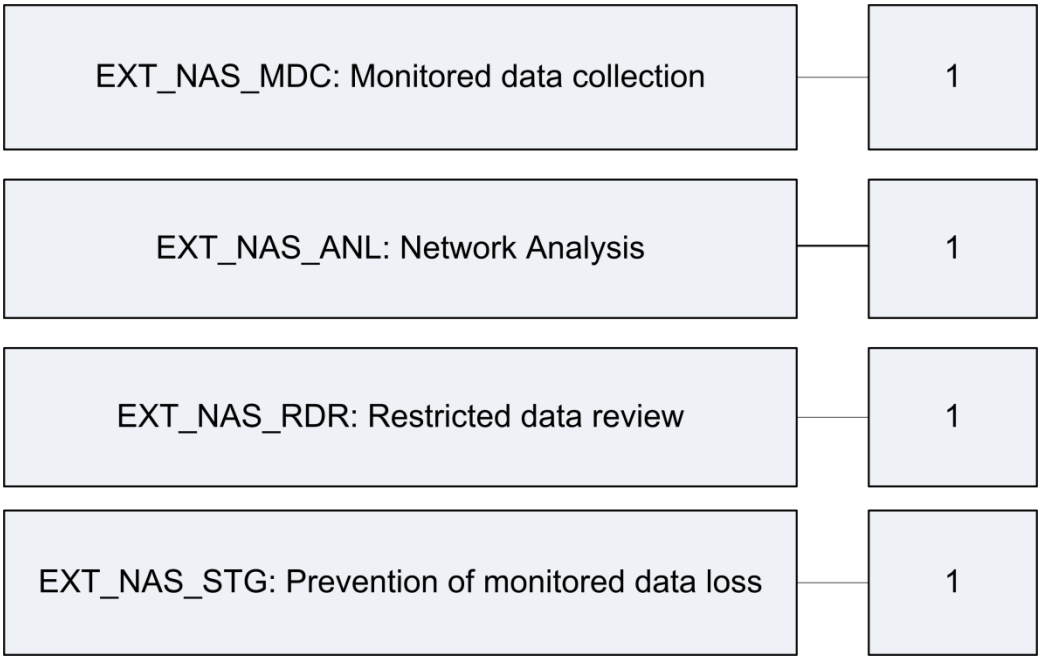

Figure 4 EXT_NAS: Network Assessment Class Decomposition

5.1.3.1 Monitored Data Collection (EXT_NAS_MDC)

Family Behaviour

This family defines the requirements for recording the information from the targeted network resources. This family identifies the level of monitored data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of configuration-related information that should be provided within various collected data record types.

Component Leveling

Figure 5 EXT_NAS Monitored data collection family decomposition

EXT_NAS_MDC.1 Monitored data collection, defines the level of events, and specifies the list of data that shall be recorded in each record.

Management: EXT_NAS_MDC.1

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

a) Configuration of the hosts and host data to be collected.

Audit: EXT_NAS_MDC.1

b) There are no auditable events foreseen

EXT_NAS_MDC.1 Monitored data collection
Hierarchical to: No other components
EXT_NAS_MDC.1.1

The TSF shall be able to collect the following information from the targeted IT System resource(s):

- Host names;
- IP[17] addresses and subnet masks in use;
- Interface names;
- Device type;
- Routing tables; and
- Configuration files or vulnerability scan data.

EXT_NAS_MDC.1.2

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

- Date and time of collection, device name, and the outcome (success or failure) of the collection.

Dependencies: None

[17] IP – Internet Protocol

5.1.3.2 Network Analysis (EXT_NAS_ANL)

Family Behaviour

This family defines the analysis the TOE performs on the collected network data. This family enumerates the types of analysis to be performed on the collected data.

Component Leveling

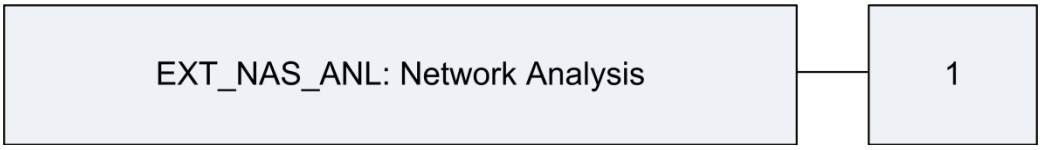

Figure 6 Network Analysis family decomposition

EXT_NAS_ANL.1 Network analysis, specifies the list of analyses the TOE will perform on the collected system data.

Management: EXT_NAS_ANL.1

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

a) Configuration of the analysis to be performed.

Audit: EXT_NAS_ANL.1

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

EXT_NAS_ANL.1 Network Analysis

Hierarchical to: No other components.

EXT_NAS_ANL.1.1

The TSF shall perform the following analysis function(s) on all data received from managed elements:

a) Configuration changes;
b) Best Practices and policy compliance; and
c) vulnerabilities identified;

Dependencies: EXT_NAS_MDC.1 Monitored Data Collection

5.1.3.3 Restricted data review (EXT_NAS_RDR)

Family Behaviour

This family defines the requirements for monitored data tools that should be available to authorized users to assist in the review of monitored data.

Component Leveling

Figure 7 Restricted data review family decomposition

EXT_NAS_RDR.1 Restricted data review, the TSF shall prohibit all users read access to monitored data, except for those user that have been granted explicit read-access.

Management: EXT_NAS_RDR.1

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the monitored data records.

Audit: EXT_NAS_RDR.1

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

a) Basic: Attempts to read monitored data that are denied.

b) Detailed: Reading of information from the monitored data records.

EXT_NAS_RDR.1 Restricted data review
Hierarchical to: No other components
EXT_NAS_RDR.1.1
The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.
EXT_NAS_RDR.1.2
The TSF shall provide the monitored data in a manner suitable for the user to interpret the information.
EXT_NAS_RDR.1.3
The TSF shall prohibit all users read access to the monitored data, except those users that have been granted explicit read-access.
Dependencies: EXT_NAS_MDC.1
EXT_NAS_ANL.1

5.1.3.4 Prevention of Monitored data loss (EXT_NAS_STG)

Family Behaviour

This family defines the requirements for monitored data storage to not exceed its capacity and therefore lose data. The requirement, require the TSF to alert authorized users to storage capacity thresholds.

Component Leveling

Figure 8 Prevention of Monitored data loss family decomposition

EXT_NAS_STG.1 Prevention of monitored data loss, the TSF shall define what actions the TSF will take if storage capacity has been reached.

Management: EXT_NAS_STG.1

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

a) Maintenance (enabling, disabling) of actions to be taken in the event that system data storage capacity has been reached.

Audit: EXT_NAS_STG.1

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

a) Basic: Actions taken if the storage capacity has been reached.

EXT_NAS_STG.1 Prevention of Monitored data loss
Hierarchical to: No other components
EXT_NAS_STG.1

The TSF shall [selection: ignore System data, prevent System data, except those taken by the authorized user with special rights, overwrite the oldest stored System data, alert users] if the storage capacity has been reached.

Dependencies: EXT_NAS_MDC.1 Monitored Data Collection

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 12 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
EXT_FPT_APW.1	Protection of Passwords				

Name	Description	S	A	R	I
FTA_SSL.3	TSF-initiated termination		✓	✓	
FTA_TAB.1	Default TOE access banners			✓	
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted Path	✓	✓		
EXT_NAS_MDC.1	Monitored Data Collection				
EXT_NAS_ANL.1	Network Analysis				
EXT_NAS_RDR.1	Restricted Data Review		✓		
EXT_NAS_STG.1	Prevention of Monitored data loss	✓			

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

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) [*system configuration changes on monitored devices, data collection, data analysis, modification of audit configuration, user login and log out events*].

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, [*host name or process name*].

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage
FAU_STG.4.1

The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: 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 [*Hash-based DRBG, DSA, and RSA*] and specified cryptographic key sizes [*128-, 256-bits for symmetric keys and 2048, 3072-bits for asymmetric keys*] that meet the following: [*SP 800-90A and FIPS 186-3*].

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: 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 [*overwriting*] that meets the following: [*FIPS 140-2*].

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations in Table 13*] in accordance with a specified cryptographic algorithm [*cryptographic algorithms in Table 13*] and cryptographic key sizes [*key sizes listed in Table 13*] that meet the following: [*standards listed in Table 13*].

Table 13 Cryptographic Operations

Cryptographic Operation	Cryptographic Algorithm	Key Size (bits)	Standard (Certificate #)
Digital Signature Generation/Verification	DSA, RSA PKCS[18]#1	2048, 3072	FIPS 186-3 Certificate # 1154 (RSA) and 701(DSA)
Encryption/Decryption	AES[19] in CBC[20] mode and 3DES[21] in CBC mode	128, 192, 256 Three key (168)	FIPS 197 Certificate # 2249 SP 800-67 Certificate #1408
Secure Hash	SHA[22]-1, -256, -512	N/A	FIPS 180-4 Certificate #1938
Message Authentication	HMAC[23] with SHA1, SHA256, SHA512	160, 256, 512	FIPS 198 Certificate #1378
Key Agreement	Diffie-Hellman	2048	SP 800-56A non-compliant

[18] PKCS – Public Key Cryptographic Standard
[19] AES – Advanced Encryption Standard
[20] CBC – Cipher Block Chaining
[21] 3DES – Triple Data Encryption Standard
[22] SHA – Secure Hash Algorithm
[23] HMAC – (keyed-)Hash Message Authentication Code

Cryptographic Operation	Cryptographic Algorithm	Key Size (bits)	Standard (Certificate #)
			(allowed in FIPS 140-2 mode)

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated action on behalf of that user

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies
FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated action on behalf of that user.

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behaviour of, modify the behaviour of] the functions [*security functions listed in Table 14*] to [*the roles listed in Table 14*].

Table 14 Management of Security Functions

Security Function	Role
Log configuration	Admin and Server Admin
User authentication	Admin and Administrator
Backup and restore of database	Admin, Server Admin, and CPM User
Modify system settings	Admin
Monitor server health, restart or reboot server	Admin, Server Admin, Administrator, and CPM User
Download logs	View, Admin, Model, Administrator, Server Admin, and CPM User

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [[*perform the operations listed in Table 15*]] the [*TSF data listed in Table 15*] to [*the roles listed in Table 15*].

Table 15 Management of TSF Data

Operation	TSF Data	Role
Create, Modify, Delete, Disable	User accounts	Admin and Administrator
Create, Modify, and Delete	Custom Best Practice Checks	Admin and Model
Run	Analysis engine	Admin and Model
Update	TRL	Admin and Model
Create, Modify, Delete	Device credentials, policies, and collection tasks	Admin and Model

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 management functions: [*management of TSF data, RedSeal Server management, management of collection tasks and data, and database backup*].

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 [*View, Model, Admin, Server Admin, Administrator, CPM User, and CSM User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

EXT_FPT_APW.1 Protection of Passwords
Hierarchical to: No other components.
Dependencies: None
EXT_FPT_APW.1.1
The TSF shall store local passwords in a protected form.
EXT_FPT_APW.1.2
The TSF shall prevent the reading of plaintext passwords.

6.2.6 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.3.1

The TSF shall terminate an interactive **client** session after a [*user defined interval*].

FTA_TAB.1 Default TOE access banners
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_TAB.1.1

Before establishing a **client** user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies
FTP_ITC.1.1
The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2
The TSF shall permit [the TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [*authentication and import of network device configurations*].

Application note: The trusted channel for importing network device data is only available when using only the HTTPS communication plugin.

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
Dependencies: No dependencies
FTP_TRP.1.1
The TSF shall provide a communication path between itself and [remote, local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure, [*no other types of integrity or confidentiality violation*]].
FTP_TRP.1.2
The TSF shall permit [local users, remote users] to initiate communication via the trusted path.
FTP_TRP.1.3
The TSF shall require the use of the trusted path for [initial user authentication, [*management of the TOE*]].

6.2.9 Class NAS: Network Assessment

EXT_NAS_MDC.1 Monitored Data Collection
Hierarchical to: No other components.
Dependencies: No dependencies
EXT_NAS_MDC.1.1

The TSF shall be able to collect the following information from the targeted IT System resource(s):

- Host names;
- IP addresses and subnet masks in use;
- Interface names;
- Device type;
- Routing tables; and
- Configuration files or vulnerability scan data.

EXT_NAS_MDC.1.2

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

- Date and time of collection, device name, and the outcome (success or failure) of the collection.

EXT_NAS_ANL.1 Network Analysis
Hierarchical to: No other components.
Dependencies: EXT_NAS_MDC.1 Monitored Data Collection
EXT_NAS_ANL.1.1

The TSF shall perform the following analysis function(s) on all data received from managed elements:

d) Configuration changes;
e) Best Practices and policy compliance; and
f) Vulnerabilities identified.

EXT_NAS_RDR.1 Restricted Data Review
Hierarchical to: No other components.
Dependencies: EXT_NAS_MDC.1 Monitored Data Collection
EXT_NAS_ANL.1 Network Analysis
EXT_NAS_RDR.1.1

The TSF shall provide [*View, Monitor, Admin, CSM User, and Administrator*] with the capability to read [*the data listed in below in Table 16*] from the Monitored data.

Table 16 Monitored Data Access

User Type	Access
View	Reports, topology data, database query results
Model	Reports (read and write access to their reports), topology data, database query results, collection tasks
Admin	Reports (read and write access to all), topology data, database query results, collection tasks
CSM User and Administrator	Roll-up reports for Risk, Vulnerable Hosts, Access Policy Violations, and Best Practice Violations on a per server basis

EXT_NAS_RDR.1.2

The TSF shall provide the Monitored data in a manner suitable for the user to interpret the information.

EXT_NAS_RDR.1.3

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

EXT_NAS_STG.1 Prevention of Monitored data loss

Hierarchical to: No other components

Dependencies: EXT_NAS_MDC.1 Monitored Data Collection

EXT_NAS_STG.1.1

The TSF shall [alert users] if the storage capacity threshold has been reached.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 17 Assurance Requirements summarizes the requirements.

Table 17 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security function. Hence, each security function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 18 lists the security functionality and their associated SFRs.

Table 18 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	EXT_FPT_APW.1	Protection of Passwords
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path
Network Assessment	EXT_NAS_MDC.1	Monitored Data Collection
	EXT_NAS_ANL.1	Network Analysis
	EXT_NAS_RDR.1	Restricted Data Review
	EXT_NAS_STG.1	Prevention of Monitored data loss

7.1.1 Security Audit

The TOE generates RedSeal Events that are used as a part of network analysis and log events that generates audit records. The RedSeal Server audit records are stored in multiple files:

- UI log – contains messages generated by actions taken on the RedSeal Client. This log is only viewable from the RedSeal Client
- Server log – contains messages related to server configuration, database management.
- Audit – contains system configuration changes made through either the client interface or the CLI
- Analyzer – contains messages on analysis events, including start time, finish time, success or failure, and data collection details.
- System – contains system related events including server stops, starts, and restores

The RedSeal Server Manager maintains an audit log that is stored in the MongoDB and contains messages related to administrative actions such as backups and restores of RedSeal Server databases and user activity such as login and logout.

Logs are rotated, overwriting the oldest events when the log is full. RedSeal Server logs allow an Admin to configure the number of log files and the size of log files that are kept before rotation. RedSeal Server Manager logs have a hardcoded threshold. The TOE audit records contain the following information:

- Data and time of the event
- Host or process name
- Type (i.e. category and action) of the event
- Subject username if applicable
- Description (i.e. action performed, success or failure, etc.) of event

Audit records are stored in the filesystem on the RedSeal Server for all logs except the UI log and the Server Manager log. The UI log is stored on the client's host system. The TOE provides read-only access to the audit files for all users. The TOE will overwrite audit data starting with the oldest data when the log rotation limit is reached.
TOE Security Functional Requirements Satisfied: FAU-GEN.1, FAU_STG.1, FAU_STG.4.

7.1.2 Cryptographic Support

The TOE includes a FIPS 140-2 validated (certificate #2058) cryptographic module. All cryptographic operations are performed using this module. The module uses a Hash-based DRBG and is capable of generating 128, 256, and 512 bits keys for use in management sessions, internal communications between components, and communications with monitored hosts. The module generates asymmetric keys according to FIPS 186-3. The module destroys all keys in accordance with FIPS 140-2 zeroization methods. The TOE is also capable of generating TLS certificates, performing signature generation and verification, and hashing. The Diffie-Hellman algorithm can be used for key agreement in the TLS negotiations as described in SP 800-56A. This algorithm was not tested as part of the FIPS validation, but is allowed in the modules FIPS mode without testing.
TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 Identification and Authentication

The TOE requires user to be identified and authenticated prior to accessing the TSF functionality. Users are authenticated by the TOE using a local database. LDAP and RADIUS authentication are also supported, but were not evaluated as a part of this evaluation. An authorized administrator can select a user's authentication method when adding new users. The LDAP server must be configured to run using TLS.
TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

The TOE provides the following roles:

- View – A Client UI users that has access to view topologies and reports and download log files. This role does not have any management functions.
- Model – A Client UI user that can run analysis, manage data collection, create custom best practice checks, and perform the tasks of the View user.
- Admin – A Client UI users that can perform the tasks of the Model user and additionally perform database, log, and user management.
- Server Admin – A CLI administrator that can perform actions only on the server itself. This administrator can perform database management, starting and stopping the server, and performing updates.
- Administrator – A Server Manager Administrator has access only to the Server Manager and can create and manage users, associate the users with RedSeal Servers, monitor RedSeal Servers, and view analysis data from these servers.
- CPM User – A CPM User has access only to the Server Manager and can view attached Servers, upgrade software, view logs, restart servers, and perform backups.
- CSM User – A CSM User has access only to the Server Manager and can view health and analysis data sent from those servers.

The TOE associates users with their role after authentication. The Client UI only presents users with functions for which their role has permissions as described in Table 15.

Audit logs on the TOE can be configured through either the Admin tab on the Client UI or the CLI on the server. The Admin role can modify user authentication for the Client UI. The Administrator role can modify user authentication for the RedSeal Server Manager. The Admin, Server Admin, and CPM User can backup and restore the database. The Admin, Server Admin, Administrator, and CPM User can monitor the server health and restart or reboot the RedSeal Server. The Admin and Server Admin roles can configure logs. Only the Admin role can modify system settings.
TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

Locally stored passwords on the RedSeal Server are wrapped using a 128-bit AES key to prevent plaintext reading. Locally stored passwords on the RedSeal Server Manager are wrapped using a password based key derivation function to prevent plaintext reading. Passwords for remote authentication are sent only over secure channels, ensuring that they cannot be disclosed.
TOE Security Functional Requirements Satisfied: EXT_FPT_APW.1.

7.1.6 TOE Access

The RedSeal Client UI offers a user defined inactivity timeout. When the period of inactivity is surpassed the TOE will display a warning and then terminate the user's session. The user will have to re-authenticate in order to regain access.

Admins can configure a TOE access banner that is shown to all users on the Client UI. Users must accept the banner after authenticating to gain access to the TOE.
TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_TAB.1.

7.1.7 Trusted Path/Channels

The TOE provides trusted channels between itself and external authentication servers and those network devices that support secure communications. The trusted channel to the network devices allows device configurations to be imported into the TOE in a secure manner. The RedSeal server uses:

- TLS for communications with LDAP servers
- HTTPS for communications with network devices that support these protocols

These protocols all rely on the FIPS 140-2 validated library for their cryptographic algorithms.

The RedSeal Server Manager also provides a trusted path between administrators and the web interface using HTTPS. These protocols also rely on the FIPS 140-2 validated algorithms. Lastly, administrators connect to the CLI on the RedSeal Server using the trusted path of a direct, serial connection.
TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

7.1.8 Network Assessment

The TOE collects data from layer 3 network devices and vulnerability scanners. The collected data includes configuration files (for layer 3 network devices), routing tables, and vulnerability scan reports (from vulnerability scanners) from attached network devices. A data collection task is created by a user and calls the network devices using the communications plugin and credentials supplied in the collection task. The TOE collects host names, IP addresses, interface names, device types, routing tables, and configuration files from the devices to analyze the network. Each collection task generates an audit message in the UI log that details the date and time of collection, device name, and the success or failure of the connection.

The analysis performed on this data includes a list of best practices and policy compliance, vulnerabilities identified, and configuration changes made since the last collection. The RedSeal Threat Reference Library is also used to determine vulnerabilities and threats to a network.

Both the collected data and the reports and analysis generated from that data are stored in the Postgres SQL database on the RedSeal Server. The TOE does not allow direct access to the Postgres SQL database. Data can only be pulled from the database using the reports and queries available on the Client UI and the RedSeal Server Manager. Users in the View group can view reports, but have read-only access to the Public folder in the Reporting tab. Users in the Model group can manage data collection tasks, perform analysis, and have read and write access to reports generated by them. Admin users have access to all reports and analysis data. On the RedSeal Server Manager, the CSM User and Administrator can view roll-ups of each RedSeal Server's overall risk score, top best practice violations, top access policy violations, and the top vulnerable hosts from each RedSeal Server.

The homepage of the Client UI includes an Overall Health section. This monitors the database status and alerts users if the storage threshold is reached. The database must be periodically purged to remove stale data and ensure the database storage threshold is not exceeded.
TOE Security Functional Requirements Satisfied: EXT_NAS_MDC.1, EXT_NAS_ANL.1, EXT_NAS_RDR.1, EXT_NAS_STG.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 19 below provides a mapping of the objects to the threats they counter.

Table 19 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN ERROR A TOE user may unintentionally install or configure the TOE incorrectly, resulting in ineffective security enforcement mechanisms.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN mitigates this threat by ensuring the TOE provides management functions and restricts these function to TOE users with appropriate privileges.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE mitigates this threat by ensuring that all administrators are properly trained and follow TOE guidance.
T.FALREC The TOE may fail to recognize non-TOE user potential attack points on the monitored network due to inaccurate data received from each data source.	O.MONITOR The TOE will monitor the behavior and configurations of the network for anomalous activity.	The O.MONITOR objectives mitigates this threat by ensuring that the TOE receives correct information from data sources and properly analyzes the information to detect anomalous activity.
	OE.SD_PROTECTION The TOE environment will provide the capability to protect monitored system data as it is transmit to the TOE.	OE.SD_PROTECTION mitigates this threat by ensuring that the TOE environment protects monitored network data as it is transmitted to the TOE.

Threats	Objectives	Rationale
T.FORGE A non-TOE user may create a false policy causing the network analysis to incorrectly model the network.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE mitigates this threat by requiring the TOE to identify and authenticate all users prior to performing an action on the TOE.
	O.INACTIVE The TOE client must implement a robust mechanism for terminating user sessions after a period of inactivity.	O.INACTIVE mitigates this threat by requiring user session to timeout after a period of inactivity. This ensures that unauthorized users cannot hijack an authenticated user's account and create a false policy.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat through the TOE protecting its system data, which includes policy creation.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE mitigates this threat by requiring all authorized users to be properly trained and follow all guidance.
T.MASQUERADE A non-TOE user may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE counters this threat.
T.NACCESS A non-TOE user may be able to view or modify data that is transmitted between parts of the TOE or between the TOE and a remote authorised external entity.	O.SEC_COMMS The TOE must protect audit and system data as it shared over the external network.	The objective O.SEC_COMMS ensures that TSF data transmitted between the external network and the TOE is kept secure from modification and disclosure.
T.STORAGE The TOE database may run out of storage space due to improper maintenance from a TOE users; causing audit or monitored network traffic data loss.	O.ALERT The TOE will alert users if storage space in the database is reaching capacity.	The O.ALERT objective mitigates this threat by requiring the TOE to alert users when storage capacity reaches a defined threshold.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance.	OE.MANAGE ensures that administrators follow all guidance, including proper database back-up procedures.

Threats	Objectives	Rationale
	TOE administrators will ensure the system is used securely.	
T.TAMPERING A non-TOE user may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of users, prevent unauthorized modification of the audit trail, and prevent loss of audit trail data.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE and TOE environment are protected from external interference or tampering.
T.UNATTEND A TOE user on the Client UI may leave an authenticated session unattended, resulting in the possibility of a malicious or unauthorized user to mask their actions as the logged in user, resulting in a misconfiguration or alteration of the TSF behavior.	O.INACTIVE The TOE client must implement a robust mechanism for terminating user sessions after a period of inactivity.	The O.INACTIVE objective mitigates this threat by requiring the TOE to timeout all user session's after a configurable timeout period.
T.UNAUTH A TOE user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.

Threats	Objectives	Rationale
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of users, prevent unauthorized modification of the audit trail, and prevent loss of audit trail data.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 20 below gives a mapping of policies and the objectives that support them.

Table 20 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.BANNER The TOE client shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.BANNER The TOE client will display an advisory warning regarding use of the TOE.	O.BANNER ensures that an advisory warning is displayed regarding the use of the TOE.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 21 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 21 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.TIMESTAMP The IT environment provides all TOE components with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system. The TOE is placed in the network so that is can access the required network objects.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	The TOE must be placed in the network so that it has access to the required network objects. OE.TRAFFIC ensures this.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

Assumptions	Objectives	Rationale
A.CRYTPO The TOE environment will protect non-HTTPS communications between the TOE and monitored devices.	OE.SD_PROTECTION The TOE environment will provide the capability to protect monitored system data as it is transmit to the TOE.	OE.SD_PROTECTION satisfies the assumption that the environment provides protects non-HTTPS communications between the TOE and monitored systems.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A class of EXT_NAS requirements was created to specifically address monitoring and analyzing the attached network. The CC FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of monitored network data and provide for requirements about collecting, reviewing, and managing this data. These requirement's dependencies have been noted in 5.1.3. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

A family of EXT_FPT_APW: Protection of Passwords was created to address the protection of passwords stored on the TOE. This requirement was based on the FPT_APW_EXT requirement in the Network Device Protection Profile. The purpose of this requirement is to ensure that passwords, which are TSF data, are not stored in plaintext on the TOE. Storage of these passwords in plaintext could jeopardize their integrity. This requirement is dependent on the FCS_COP.1 requirement to provide the cryptographic operation that makes the password non-plaintext. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.4.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 22 below shows a mapping of the objectives and the SFRs that support them.

Table 22 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	EXT_NAS_RDR.1 Restricted Data Review	The requirement meets the objective by establishing roles with differing permissions for access to review monitored data and by providing the analyzed data in a manner suitable for interpretation.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ALERT The TOE will alert users if storage space in the database is reaching capacity.	EXT_NAS_STG.1 Prevention of Monitored data loss	The requirement meets the objective by requiring the TSF to alert users if the database storage capacity is meeting a defined threshold.
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of users, prevent unauthorized modification of the audit trail, and prevent loss of audit trail data.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to any TSF function is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to any TSF function is allowed.
O.BANNER The TOE client will display an advisory warning regarding use of the TOE.	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that a banner is displayed to client users prior to identification and authentication.
O.INACTIVE The TOE client must implement a robust mechanism for terminating user sessions after a period of inactivity.	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that client user sessions are terminated after a configurable inactivity time.
O.MONITOR The TOE will monitor the behavior and configurations of the network for anomalous activity.	EXT_NAS_ANL.1 Network Analysis	The requirement meets the objective by requiring the TOE to perform a set of analytics on collected network data to highlight anomalous activity.
	EXT_NAS_MDC.1 Monitored Data Collection	The requirement meets the objective by requiring the TOE to collect data from network objects.
	EXT_NAS_RDR.1 Restricted Data Review	This requirement meets the objective by providing the monitored data in a readable format to user's with the proper permissions.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	EXT_FPT_APW.1 Protection of Passwords	This requirement meets the objective by storing local passwords in encrypted form and ensuring that no unauthorised users or IT entities can access the passwords.
	EXT_NAS_STG.1 Prevention of Monitored data loss	The requirement meets the objective by requiring the TSF to alert users if the database storage capacity threshold has been reached, therefore allowing administrators to purge data and back up the database to avoid loss of data.

Objective	Requirements Addressing the Objective	Rationale
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that no one may delete or alter information in the audit logs.
	FCS_CKM.4 Cryptographic key destruction	This requirement meets the objective by providing a method to destroy cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorised person or IT entity.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to TSF data.
O.SEC_COMMS The TOE must protect audit and system data as it shared over the external network.	FCS_CKM.1 Cryptographic key generation	This requirement supports O.SEC_COMMS by providing secure keys for use in the network protocols used to protect transmitted TSF data.

Objective	Requirements Addressing the Objective	Rationale
	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.SEC_COMMS by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorised person or IT entity.
	FCS_COP.1 Cryptographic operation	This requirement meets the objective by providing algorithms for cryptographic operations used to encrypt and decrypt TSF data when sent over the network.
	FTP_ITC.1 Inter-TSF trusted channel	This requirement meets the objective by ensuring that trusted IT entities have a secure communications channel established with the TOE prior to exchanging data.
	FTP_TRP.1 Trusted Path	This requirement meets the objective by ensuring that TOE users have a trusted path for communications with the TOE.

8.4.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.4.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 23 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 23 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	OE.TIME ensures that timestamps are provided by the operating environment, therefore this dependency is met.
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed. FIA_UID.2 is hierarchical to FIA_UID.1and therefore meets this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed. FIA_UID.2 is hierarchical to FIA_UID.1and therefore meets this dependency.
EXT_FPT_APW.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	
EXT_NAS_MDC.1	No dependencies	✓	
EXT_NAS_ANL.1	EXT_NAS_MDC.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
EXT_NAS_RDR.1	EXT_NAS_ANL.1	✓	
	EXT_NAS_MDC.1	✓	
EXT_NAS_STG.1	EXT_NAS_MDC.1	✓	

9 Acronyms

This section and Table 24 define the acronyms used throughout this document.

9.1 Acronyms

Table 24 Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMDB	Configuration Management Database
CPM	Centralized Platform Management
CSM	Centralized Security Monitoring
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GB	Gigabytes
GUI	Graphical User Interface
HMAC	(keyed-)Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
JDBC	Java Database Connectivity
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
MB	Megabytes
NISM	Network Infrastructure Security Management
OS	Operating System
OSP	Organizational Security Policy
PKCS	Public Key Cryptographic Standard

Acronym	Definition
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
REST	Representational State Transfer
SAR	Security Assurance Requirement
SCP	Secure Copy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SMB	Server Message Block
SP	Special Publication
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TRL	Threat Reference Library
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com