Riverbed Technology
Cascade Profiler v9.6
Security Target

Evaluation Assurance Level (EAL): EAL3+
Document Version: 0.26

Prepared for:

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105
United States of America

Phone: +1 415 247 8800
Email: support@riverbed.com
http://www.riverbed.com

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the organization of the ST. The TOE is the Riverbed Cascade Profiler v9.6 and will hereafter be referred to as the TOE or "Profiler" throughout this document. The TOE is a software-only distributed network performance management and network behavioral analysis solution that is designed to provide superior network and application visibility to help respond to IT[1] performance problems faster. In addition, Cascade Profiler protects the critical applications and services inside an enterprise network. This enterprise network will be referred to as the target network throughout this document. Cascade Profiler v9.6 collects data from devices such as switches, routers, and WAN[2] optimization devices. It then combines that data with advanced behavioral analytics to proactively detect problems.

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 functions 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 Summary 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 and Terms (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	Riverbed Technology Cascade Profiler v9.6Security Target
ST Version	Version 0.26
ST Author	Corsec Security
ST Publication Date	2/7/2013
TOE Reference	Riverbed Cascade Profiler v9.6

[1] Information Technology
[2] Wide Area Network

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Cascade Profiler offers an enterprise-wide network and application visibility solution, covering all data centers, offices, and mobile users. It collects flow and packet data in a non-intrusive way (i.e. without using agents), and uses it to discover applications and track their performance. Riverbed's solution uses fully-dynamic behavioral analytics to track performance over time and proactively alert the administrator to any deviations from normal behavior. To troubleshoot a problem, authorized users can drill down through multi-resolution views, from macro flows at the top level for executive-level reporting, through application-level flows to micro flows (packet-based views) and full packet captures. An authorized user can also view a full graphical representation of network assets and their dependencies, to assist with current performance problems and help plan future IT investments.

Cascade Profiler v9.6 allows organizations to assess, accelerate, and adapt network performance with a full set of application-centric, site-centric, and business-centric views that it provides. These views help managers address critical IT challenges, such as network monitoring and troubleshooting, application performance, security threats and WAN optimization and analysis. In addition, Cascade Profiler v9.6 allows enterprises to proactively monitor end-user activity in real-time.

1.3.1 Product Components

In order to provide a thorough analysis of the target network while maintaining scalability, Cascade Profiler v9.6 is separated into five components: Cascade Profiler v9.6, Cascade Sensor, Cascade Sensor-VE, Cascade Gateway, and Cascade Express. These components will be referred to as Profiler, Express, Sensor, Sensor-VE, Gateway, and Express respectively throughout this document. The Cascade Profiler v9.6 product components are provided to customers as software pre-installed on an appliance (Sensor-VE is not pre-installed but is available for download). The software for the Profiler, Sensor, and Gateway is provided on the same model of appliance. The license string will activate whether the software will run as the Profiler, Sensor, or Gateway. Sensor-VE is a virtual Sensor running on a VMware virtual machine. Cascade Profiler v9.6 Express is an all-in-one-product that provides Profiler, Sensor, and Gateway functionality. The product components are managed via a web browser. By pointing an SSL[3]-enabled web browser to a particular component, a Graphical User Interface (GUI) used for management is displayed. This management interface which is on each product component Profiler, Sensor, Sensor-VE, Gateway, and Express will be referred to as the User Interface throughout this document.

1.3.1.1 Cascade Profiler

The Cascade Profiler v9.6 performs the actual analysis of network traffic and data. The Cascade Sensors (see section 1.3.1.2 below) are used to gather data from the network and users. The Sensors provide "packet capture and inspection" functionality – they retrieve and analyze actual network traffic on the wire (rather than receiving NetFlow from a switch or router). The Sensors perform some initial analysis of the traffic they are observing, and then send the processed data to the Profiler for detailed analysis. Sensors communicate with the Profilers via a proprietary protocol called Riverbed's MNMP protocol which is wrapped in a TLS tunnel. Using mirror ports on switches and/or passive taps on lines, Sensors provide Cascade Profiler v9.6 with statistics for the following network traffic characteristics:

- Connections between hosts on the monitored segments of the target network
- Source and destination IP addresses and port numbers used in the connections
- Protocols
- Applications being served on hosts

[3] Secure Sockets Layer

- Traffic volumes in connections, packets, bytes, or bits per second
- Performance metrics

Sensor communications with the Profiler are compressed and encrypted.

Cascade Profiler can also be deployed as in an Enterprise mode, called Enterprise Profiler. Enterprise Profiler is installed on separate hardware appliances to handle greater data throughput. The code for both Profiler and Enterprise Profiler are the same and only are configured differently. In the case of Enterprise Profiler, the Cascade Profiler is installed and separated on at least three machines in order to run efficiently. The Cascade Profiler will balance tasks between the three parts of itself in order to handle Profiler tasks on a greater scale.

1.3.1.2 Cascade Sensor

The Cascade Sensors are used to gather data from the network and users. The Sensors provide "packet inspection" functionality – they retrieve and analyze actual network traffic on the wire (rather than receiving NetFlow from a switch or router). The Sensors perform some initial analysis of the traffic they are observing, and then send the processed data to the Profiler for detailed analysis. Sensors communicate with the Profilers via a proprietary protocol that uses an TLS tunnel. Using mirror ports on switches and/or passive taps on lines, Sensors provide Cascade Profiler v9.6 with statistics for the following network traffic characteristics:

- Connections between hosts on the monitored segments of the target network
- Source and destination IP addresses and port numbers used in the connections
- Protocols
- Applications being served on hosts
- Traffic volumes in connections, packets, bytes, or bits per second
- Performance metrics

Sensor communications with the Profiler are compressed and encrypted.

1.3.1.3 Cascade Sensor-VE

The Riverbed Cascade Sensor-VE is a virtual edition of the Sensor[4]. The Sensor-VE provides nearly the same functionality as the Cascade Sensor, with the exception of Layer 7 fingerprinting. In addition, Sensor-VE takes the form of a VMware virtual machine which is designed to run on the Riverbed Services Platform (RSP), a VMware Server platform provided as part of a Riverbed Steelhead appliance. It monitors the LAN and AUX interfaces of the Steelhead appliance. Sensor-VE communications with the Profiler are compressed and encrypted.

1.3.1.4 Cascade Gateway

The Cascade Gateways collect flows from infrastructure devices, combine them, and perform some limited pre-processing, encrypt the data, and then report it to the Profilers. The flows collected includes traffic data from NetFlow, sFlow[5], IPFIX, or many other equivalent flow sources, hereafter referred to as "flows" in the rest of this document. Data sent from the Gateways to the Profilers are encrypted using TLS before being transmitted, and all components use a shared encryption key. Gateway communications with the Profiler are compressed and encrypted.

[4] Sensor-VE is not a part of the TOE and therefore not included in the evaluated configuration.
[5] sFlow is a technology for monitoring network, wireless and host devices.

1.3.1.5 Cascade Express

The Express is a low-capacity "all-in-one" device which provides Profiler, Sensor, and Gateway functionality in one appliance. Express obtains traffic information from taps or mirror ports on the monitored network, or from flow sources. Express can use flows directly from switches, routers, or other devices installed at key points in the network. The data source devices must first be configured to send their data to Express.

1.3.1.6 Cascade OS

The Cascade OS is the underlying operating system which is Linux based with Riverbed patches and provides the operating system functionality to the TOE. The OS provides the kernel and common services for execution of the Profiler, Sensor, Gateway, and Express applications. The Cascade OS provides a command line interface for command line access to the TOE that is not a part of the evaluated configuration.

1.3.1.7 Riverbed Services Platform

The Riverbed Services Platform provides the underlying hypervisor to the Sensor-VE component. This allows the Sensor to run in a virtualized environment.

1.3.2 Typical Deployment

Figure 1 below shows a typical Cascade Profiler v9.6 deployment. The Cascade Gateway collects network flows and sends the condensed data to the Cascade Profiler. The Cascade Profiler complements this information with layer 7 application data retrieved from a Cascade Profiler v9.6 Sensor, plus performance data for optimized links (collected from remote Cascade Sensor-VE software running on Steelheads in remote offices). The result is visibility into business application performance across optimized and non-optimized environments.

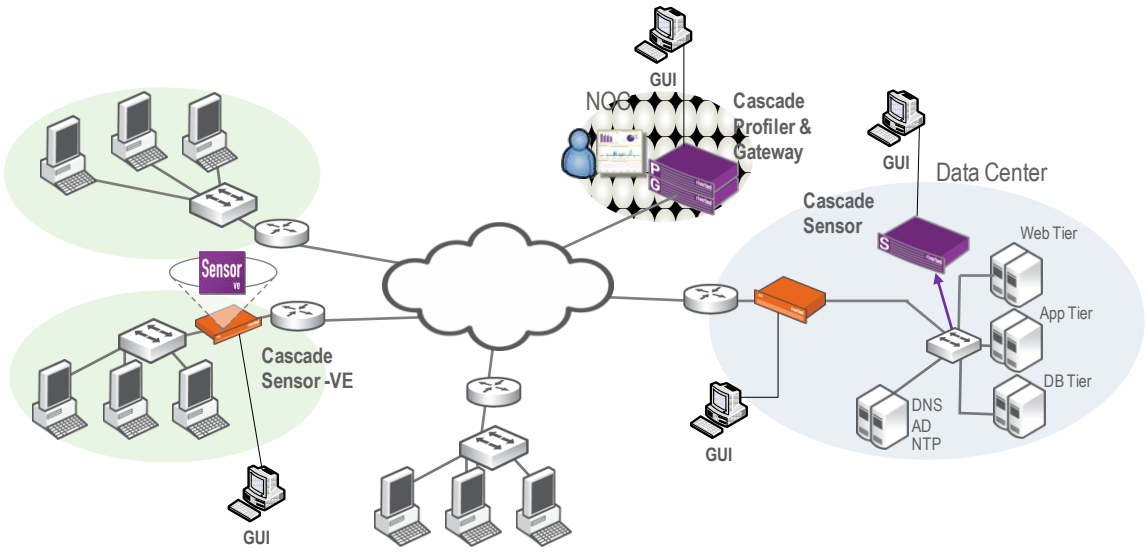

Figure 1 Typical Cascade Profiler v9.6 Deployment[6]

[6] NOC – Network Operations Center

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 product, and defining the specific evaluated configuration.

The TOE is software only TOE type and includes the Cascade Profiler v9.6 Software, Linux-based operating system, and OpenSSL Object Module v2.0rc1. The TOE includes all of the components and functionality described above in section 1.3.1, except for the features and functionality listed below in section 1.4.1 and section 1.5. Table 2 identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

1.4.1 TOE Environment

It is assumed that there will be no untrusted users or software on the TOE Server components. In addition, the Cascade Profiler v9.6 appliance component is intended to be deployed in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g., badge access, fire control, locks, alarms, etc.).

Cascade Profiler, Sensor, and Gateway rely on a PostgreSQL database to provide storage of the collected information and configuration data. See Table 2 in section 1.5.1 for a detailed description of the environment relied upon by the TOE components.

The underlying Cascade OS (in the TOE environment) synchronizes the time between the OS and the NTP server. The TOE will synchronize its time with the one retrieved by the Cascade OS.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE 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 and the constituents of the TOE Environment. The TOE is software-only, and the TOE Components are the same as the product components specified in section 1.3.1. Each product component can be deployed separately as a Profiler, Gateway, or Sensor. In addition, Express can be deployed as an all-in-one component that runs all of the TOE Components on one machine.

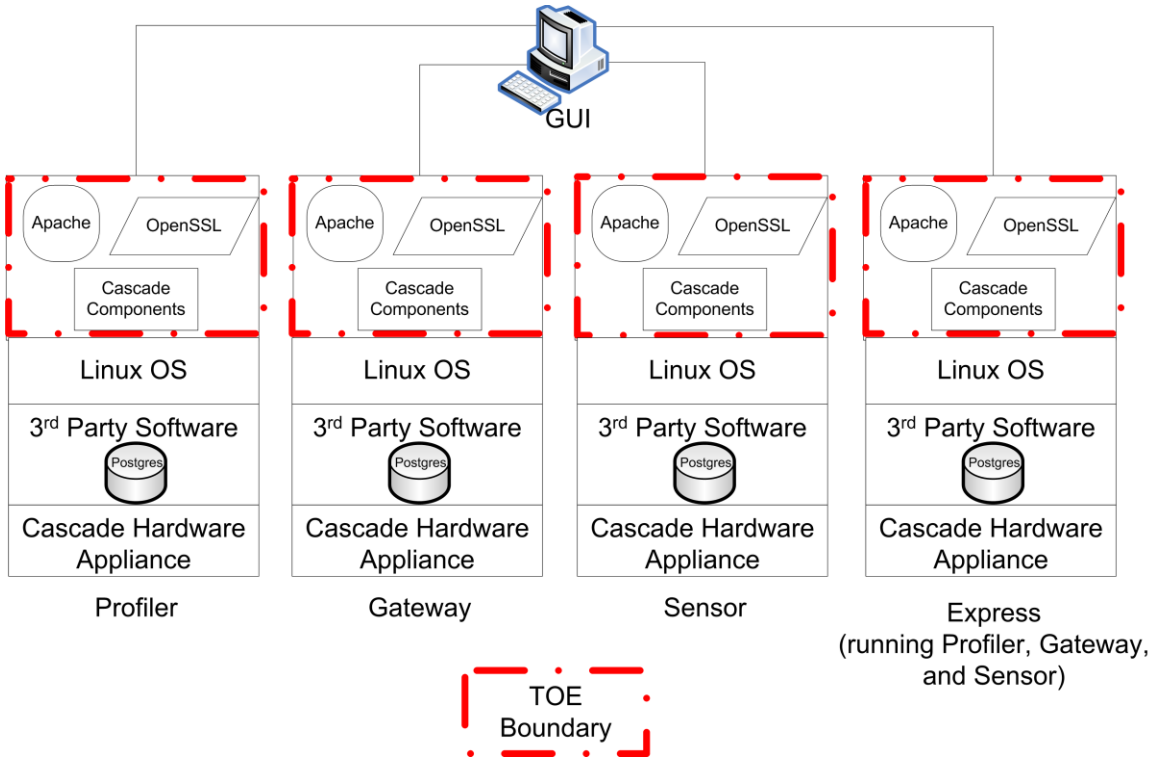

Figure 2 Physical TOE Boundary

The TOE Boundary includes all the Riverbed-developed software-only parts of the Cascade Profiler, Sensor, and Gateway product offering, OpenSSL FIPS Object Module v2.0rc1, and Apache Web Server v2.2 web server software that is bundled with the Cascade Profiler, Sensor, and Gateway components. The TOE Boundary does not include the underlying Cascade OS[7], PostgreSQL database nor the Steelhead appliance hardware or the browser that is used to remotely access the GUI. Table 2 below specifies which elements of the product suite are included in the TOE boundary as well as the TOE minimum requirements.

Table 2 TOE Minimum Requirements

Requirement	TOE	TOE Environment
Cascade Profiler v9.6	✓	
OpenSSL FIPS Object Module v2.0rc1	✓	
Apache Web Server v2.2	✓	
Cascade OS v6.1		✓
postgreSQL v8.4		✓
Cascade Profiler v9.6 hardware appliance		✓
Riverbed Steelhead hardware appliance		✓
Microsoft Internet Explorer 7 and 8or Firefox 3.6.x, 8.1 Web Browser With HTML 4, JavaScript 1.5.		✓

[7] Operating System

In the case of Enterprise Profiler, the Cascade Profiler is installed and separated on at least three machines in order to run efficiently. The Cascade Profiler will balance tasks between the three parts of itself in order to handle Profiler tasks on a greater scale. The TOE Boundary still includes the Cascade Profiler but is extended to three or more machines depending on deployment.

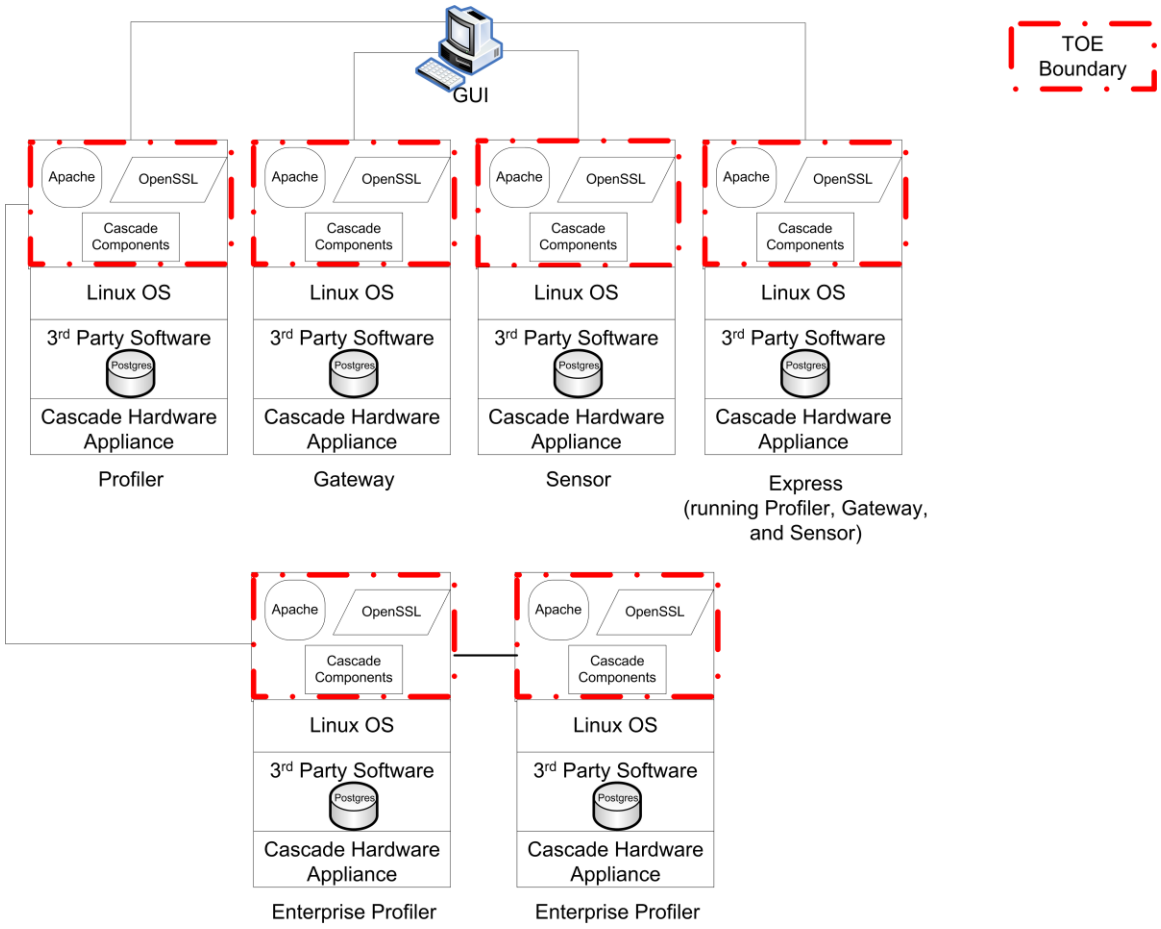

Figure 3 Physical TOE Boundary - Enterprise Profiler Deployment

1.5.1.1 Guidance Documentation

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

- Cascade Profiler v9.6 Quick Start Guide v 9.6 March 2012
- Cascade Profiler v9.6 Installation Guide v 9.6 July 2012
- Cascade Profiler v9.6 Release Notes v9.6
- Cascade Profiler v9.6 and Cascade Profiler v9.6 Express User's Guide Version 9.6 July 2012
- Cascade Profiler v9.6 Sensor and Cascade Profiler v9.6 Gateway User's Guide Version 9.6 July 2012

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:

1.5.2.1 Security Audit

The TOE generates audit records for the actions of the authorized administrators within the User Interface. Security relevant Administrator actions within the User Interface are audited. The TOE provides an authorized administrator access to view the audit logs created as a result of Administrator actions through the User Interface. The User Interface provides for searches, sorting, and ordering of audit data.

1.5.2.2 Cryptographic Support

Data encryption and decryption is provided by the TOE. Session communications are secured via TLS. The TOE generates its own certificate which is then shared among the distributed components. In addition, locally stored passwords are hashed. All of the above encryption is provided by an OpenSSL Object Module v2.0rc1, which was FIPS 140-2 validated (FIPS Certificate No. 1747). For more information, see. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747 FIPS Certificate No. 1747. The OpenSSL Object Module used by the TOE was tested using the Cascade OS 6.1 (32-bit) on Intel Pentium T4200 (x86) processors.

The cryptographic functions provided by the TOE include key generation, key zeroization, encryption/decryption, cryptographic signatures, cryptographic hashing, keyed-hash message authentication, and random bit generation. All cryptographic algorithm implementations have been validated by the NIST[8]-run Cryptographic Algorithm Validation Program (CAVP). All cryptographic functions in the OpenSSL Object Module are implemented in the TOE with the same executable module that was FIPS 140-2 validated, and per CMVP Implementation guidance G.5 maintains the FIPS 140-2 validation status in the TOE.

1.5.2.3 Identification and Authentication

The TOE provides functionality that allows Administrators to verify their claimed identity. The Identification and Authentication TSF[9] ensures that only legitimate Administrators can gain access to the configuration settings and management settings of the TOE. Administrators must log in with a valid user name and password before the TOE will permit the Administrators to manage the TOE. Passwords expire based on Administrator-configured parameters. While a user enters their password, only bullets are viewable for the characters entered as the password.

1.5.2.4 Security Management

The TOE provides a set of commands for Administrators to manage the security functions, configuration, and other features of the TOE components. The Security Management function specifies user roles with defined access for the management of the TOE components.

1.5.2.5 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of traffic flows. Another protection mechanism is that all functions of the TOE are confined to the TOE itself. The TOE is completely self-contained and therefore maintains its own execution domain.

The TOE implements HTTPS for protection of the management user interfaces. HTTPS (TLS) connections are used to protect all communication between the Profiler and User Interface. HTTPS protects data transfer and leverages cryptographic capabilities to prevent replay attacks. The management communication channels between the Profiler and remote entity are distinct from other communication channels and provide assured identification of both endpoints. In addition, the communications are protected from modification and disclosure.

[8] National Institute of Standards and Technology
[9] TSF = TOE Security Functionality

A hash is used to verify all software updates that are applied to the TOE.

1.5.2.6 TOE Access

The TOE automatically logs out a user from the User Interface after an Administrator-specified amount of idle time.

1.5.2.7 Trusted path/channel

The communications between the Profiler and the remote User Interface is secured via a trusted path using TLS.

1.5.2.8 Network Performance Management

The TOE collects traffic data on a network and performs analysis on the collected data. The collected data is analyzed against configured policies which allow the administrator to perform flow analysis, packet analysis, and calculate performance metrics. The TOE is capable of performing analysis on both live and previously saved network traffic.

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

Most features and functionality of the Cascade Profiler v9.6 product are part of the evaluated configuration of the TOE. The features that are not included in the TOE are as follows:

- Sensor VE
- RADIUS Authentication
- Shell Interface will be disabled in the evaluated configuration.
- Riverbed Services Platform
- Cascade OS
- Command Line Interface
- Riverbed Connection Utility

2 Conformance Claims

This section provides 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 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2011/08/03 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None. However, the claims in this Security Target have been largely based on the Network Device PP (Security Requirements for Network Devices Protection Profile 10 December 2010 Version 1.0).
Evaluation Assurance Level	EAL3+ 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[10] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into four 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.)
- TOE failure: The threat of the TOE failing in its operations or exhausting its resources which leads to a failure of TOE operations.
- External IT Entities: External IT entities that are being used by malicious attackers to adversely affect the security of the TOE.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[11] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 4 Threats

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.DATA_COMPROMISE	An unauthorized user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.FAIL_NETANAL	The TOE may fail to identify the network traffic flow conditions as requested by the administrator.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may

[10] IT – Information Technology
[11] TSF – TOE Security Functionality

Name	Description
	masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

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. There are no OSPs defined for this ST.

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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 Assumptions

Name	Description
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.TIME	The TOE will be provided a mechanism (through use of an NTP server) in order for the TOE to maintain the correct time.

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 as follows:

Table 6 Security Objectives for the TOE

Name	Description
O.ANALYZE	The TOE will apply analytical processes and information to derive conclusions about the network (past, present, or future).
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.SCAN	The TOE will collect network traffic information from the network interface card.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the Administrator to be unaltered and (optionally) from a trusted source.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 IT Security Objectives

Name	Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.TIME	The TOE environment will provide reliable timestamps to the TOE through the use of an NTP server in order to provide the TOE with reliable timestamps.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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 8 Non-IT Security Objectives

Name	Description
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

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 9 identifies all extended SFRs implemented by the TOE

Table 9 Extended TOE Security Functional Requirements

Name	Description
FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization
FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism
FPT_PTD_EXT.1	Extended: Management of TSF Data
FPT_TUD_EXT.1	Extended: Trusted Update
FTA_SSL_EXT.1	Extended: TSF-initiated session locking
NPM_ANL_EXT.1	Extended: Analysis
NPM_SDC_EXT.1	Extended: System data collection

5.1.1 Class FCS: Cryptographic Support

Families in this class address the requirements for functions to implement cryptographic functionality as defined in CC Part 2.

5.1.1.1 Family FCS_CKM_EXT[12]: Extended: Cryptographic Key Management

Family Behavior

A cryptographic key must be managed throughout its life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

Components in this family address the requirements for managing cryptographic keys as defined in CC Part 2. This section defines the extended components for the FCS_CKM_EXT family and is considered to be part of the CC Part 2 FCS_CKM family.

Component Leveling

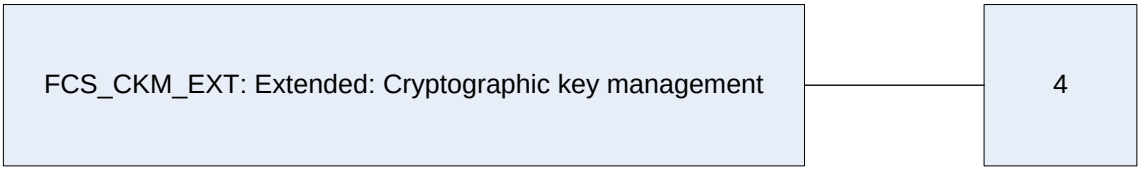

Figure 4 Extended: Cryptographic key management family decomposition

The extended FCS_CKM_EXT.4 component is considered to be part of the CC Part 2 FCS_CKM family.

FCS_CKM_EXT.4 Cryptographic key zeroization, requires cryptographic keys and cryptographic critical security parameters to be zeroized. It was modeled after FCS_CKM.4.

Management: FCS_CKM_EXT.4

a) There are no management activities foreseen.

Audit: FCS_CKM_EXT.4

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

a) Minimal: Failure on invoking the cryptographic key zeroization functionality.

FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization

Hierarchical to: No other components

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSP[13]s when no longer required.

[12] FCS_CKM_EXT is considered to be included in the existing CC Part 2 FCS_CKM family. The "EXT" defines this is an extended component only and is included in the component leveling diagram and family name for consistency purposes.

[13] Critical Security Parameters

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

5.1.2 Class FIA: Identification and Authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity as defined in CC Part 2.

5.1.2.1 Family FIA_UAU_EXT[14]: Extended: User Authentication

Family Behavior

This family defines the types of user authentication mechanisms supported by the TSF.

This section defines the extended components for the FIA_UAU_EXT family and is modeled after CC Part 2 FIA_UAU family.

Component Leveling

Figure 5 Extended: User Authentication family decomposition

The extended FIA_UAU_EXT.5 component is considered to be part of the FIA_UAU family as defined in CC Part 2.

FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism, requires a local password-based authentication mechanism and the capability for passwords to expire. In addition, other authentication mechanisms can be specified. It was modeled after the CC Part 2 FIA_UAU.5 component.

Management: FIA_UAU_EXT.5

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

a) Reset a user password by an administrator;
b) Management of the authentication mechanisms;
c) Management of the rules for authentication if multiple authentication mechanisms are provided.

Audit: FIA_UAU_EXT.5

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

a) Minimal: Unsuccessful use of the authentication mechanism.
b) Basic: All use of the authentication mechanisms.

[14] FIA_UAU_EXT is considered to be part of the existing CC Part 2 FIA_UAU family. The "EXT" defines this is an extended component only and is included in the component leveling diagram and family name for consistency purposes.

FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism

Hierarchical to: No other components

FIA_UAU_EXT.5.1

The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: *other authentication mechanism(s)*], none] to perform user authentication.

FIA_UAU_EXT.5.2

The TSF shall ensure that users with expired passwords are [selection: required to create a new password after correctly entering the expired password, locked out until their password is reset by an administrator].

Dependencies: No dependencies.

5.1.3 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.

5.1.3.1 Family FPT_PTD_EXT: Extended: Management of TSF Data

Components in this family address the requirements for managing and protecting TSF data, such as passwords and keys. This is a new family defined for the FPT Class, and is modeled after the FAU_STG family.

Component Leveling

Figure 6 Extended: Management of TSF Data family decomposition

FPT_PTD_EXT.1 Extended: Management of TSF Data, requires preventing selected TSF data from being read by any user or subject.

Management: FPT_PTD_EXT.1

a) There are no management activities foreseen.

Audit: FPT_PTD_EXT.1

a) There are no auditable activities foreseen.

FPT_PTD_EXT.1 Extended: Management of TSF Data
Hierarchical to: No other components
FPT_PTD_EXT.1.1
The TSF shall prevent reading of [assignment: *TSF data*].
Dependencies: No dependencies.

5.1.3.2 Family FPT_TST_EXT[15]: Extended: TSF testing

Components in this family address the requirements for self-testing the TSF for selected correct operation.

The extended FPT_TST_EXT.1 component is considered to be part of the FPT_TST_EXT family, and is considered part of the CC Part 2 FPT_TST family.

Component Leveling

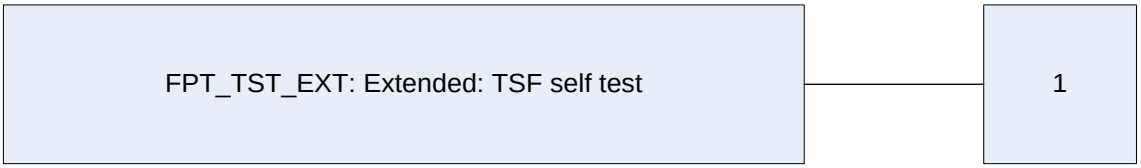

Figure 7 TSF testing family decomposition

FPT_TST _EXT.1 Extended: TSF testing, requires a suite of self tests to be run during initial start-up in order to demonstrate correct operation of the TSF. It was modeled after FPT_TST.1.

Management: FPT_TST _EXT.1

a) management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions;

Audit: FPT_TST _EXT.1

a) Minimal: Indication that TSF self-test was completed.

FPT_TST_EXT.1 Extended: TSF testing
Hierarchical to: No other components
FPT_TST_EXT.1.1
The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.
Dependencies: No dependencies.

[15] FPT_TST_EXT is considered to be included in the existing CC Part 2 FPT_TST family. The "EXT" defines this is an extended component only and is included in the component leveling diagram and family name for consistency purposes.

5.1.3.3 Extended: Trusted Update

Components in this family address the requirements for updating the TOE software. This is a new family defined for the FPT Class and is modeled after the FPT_ITI family.

Component Leveling

Figure 8 Extended: Trusted Update family decomposition

FPT_TUD_EXT.1 Extended: Trusted Update requires management tools be provided to update the TOE software, including the ability to verify the updates prior to installation. This component is modeled after the CC Part 2 FPT_ITI.1 component.

Management: FPT_TUD_EXT.1

a) There are no management activities foreseen.

Audit: FPT_ TUD_EXT.1

a) When upgrade occurs.

FPT_ TUD_EXT.1 Extended: Trusted Update
Hierarchical to: No other components
FPT_TUD_EXT.1.1
The TSF shall provide security administrators[16] the ability to query the current version of the TOE software.
FPT_TUD_EXT.1.2
The TSF shall provide security administrators the ability to initiate updates to TOE software.
FPT_TUD_EXT.1.3
The TSF shall provide a means to verify /software updates to the TOE using a [selection: digital signature mechanism, published hash] prior to installing those updates.
Dependencies: FCS_COP.1 Cryptographic operation.

[16] The security administrator is also considered to be the Administrator role in Profiler. Security administrator is language from the Network Devices Protection Profile (NDPP).

5.1.4 Class FTA: TOE Access

Families in this class address the requirements for functions that control the establishment and existence of a user session as defined in CC Part 2.

5.1.4.1 Family FTA_SSL_EXT[17]: Extended: TSF-initiated Session Locking

Components in this family address the requirements for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

The extended FTA_SSL_EXT.1 component is considered to be part of the FTA_SSL_EXT family, and is considered part of the CC Part 2 FTA_SSL family.

Component Leveling

Figure 9 Extended: TSF-initiated Session Locking family decomposition

FTA_SSL_EXT.1 Extended: TSF-initiated Session Locking, requires system initiated locking of an interactive session after a specified period of inactivity. It was modeled after the CC Part 2 FTA_SSL.1 and FTA_SSL.3 components.

Management: FTA_SSL_EXT.1

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

a) Specification of the time of user inactivity after which lock-out occurs for an individual user.
b) Specification of the default time of user inactivity after which lock-out occurs.

Audit: FTA_SSL_EXT.1

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

a) Minimal: Successful unlocking of an interactive session.
b) Basic: Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 Extended: TSF-initiated Session Locking
Hierarchical to: No other components
FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [selection:

- lock the session – disable any activity of the user's data access display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session;
- terminate the session]

after a Security Administrator-specified time period of inactivity.

[17] FTA_SSL_EXT is considered to be included in the existing CC Part 2 FTA_SSL family. The "EXT" defines this is an extended component only and is included in the component leveling diagram and family name for consistency purposes.

Dependencies: FIA_UAU.1 Timing of authentication.

5.1.5 Class NPM: Network Performance Management

Network Performance Management functions involve the collection of network packet data and the analysis of this collected data. The EXT_NPM: Network Performance Management function class was modeled after the CC FAU: Security audit class. The extended family and related components for NPM_SDC_EXT: System data collection was modeled after the CC family and related components for FAU_GEN: Security audit data generation. The extended family NPM_ANL_EXT: Analysis was modeled after the family FAU_SAA: Potential violation analysis.

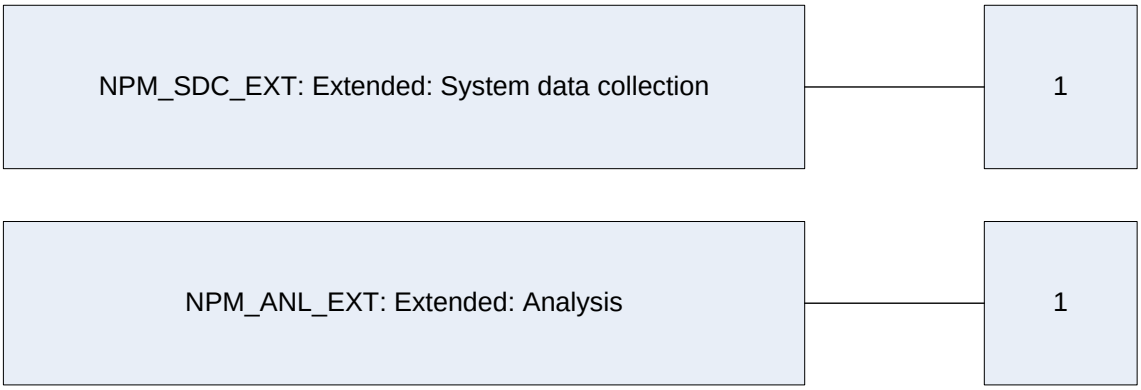

Figure 10 EXT_NPM: Network Performance Management Function Class Decomposition

5.1.5.1 Family NPM_SDC_EXT: Extended: System data collection

Family Behaviour

This family defines the requirements for recording the occurrence of network performance management events that take place under TSF control. This family identifies the level of system data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of related information that should be provided within various network performance management event record types.

Component Leveling

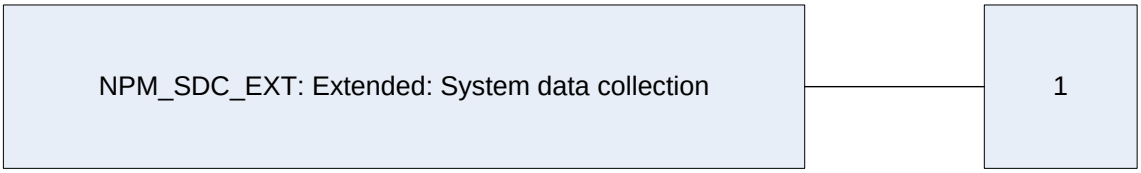

Figure 11 Extended: System data collection family decomposition

NPM_SDC_EXT.1 System data collection, defines the level of NPM events, and specifies the list of data that shall be recorded in each record. It was modeled after the CC Part 2 FAU_GEN.1 component.

Management: NPM_SDC_EXT.1

a) There are no management activities foreseen.

Audit: NPM_SDC_EXT.1

a) There are no auditable events foreseen.

NPM_SDC_EXT.1 Extended: System data collection
Hierarchical to: No other components
NPM_SDC_EXT.1.1

The TSF shall be able to collect the following information from the targeted IT System resource(s):
[assignment: *data accesses, service requests, network packets, security configuration changes, attempts to breach IPS policy; and no other events*.]

NPM_SDC_EXT.1.2

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

- Date and time of the flow, IP source and destination, IP protocol, and the size of the flow.

Dependencies: No dependencies.

5.1.5.2 Family NPM_ANL_EXT: Extended: Analysis

Family Behaviour

This family defines the analysis the TOE performs on the collected network packet data. This family enumerates the types of analytical functions that shall be executed on the data collected.

Component Leveling

Figure 12 Extended: Analysis family decomposition

NPM_ANL_EXT.1 analysis, specifies the list of analyses the TOE will perform on the collected application data. It was modeled after the CC Part 2 FAU_SAA.4 component.

Management: NPM_ANL_EXT.1

a) Maintenance of the analysis functions by (adding, modifying, deletion) of policies from the set of policies.

Audit: NPM_ANL_EXT.1

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

NPM_ANL_EXT.1 Extended: Analysis
Hierarchical to: No other components
NPM_ANL_EXT.1.1
The TSF shall perform the following analysis function(s) on a subset network data collected:

- [*assignment: analytical functions*.]

Dependencies: NPM_SDC_EXT.1

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. In keeping with the presentation of the NDPP[18] and these conventions, in the event a refinement is within an assignment, it will be depicted as ***bold italicized*** text, and when a refinement is within a selection, it will be depicted in **bold underlined** text.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.
- Iterations are identified by appending a number in parentheses following the component title. For example, FAU_GEN.1(1) Audit Data Generation would be the first iteration and FAU_GEN.1(2) Audit Data Generation would be the second iteration.
- Although this ST is not claiming conformance with the NDPP, it has been written to closely follow it. As a result the formatting of the SFRs will match where possible with the NDPP.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓	✓	
FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization				
FCS_COP.1(1)	Cryptographic operation (for data		✓		✓

[18] Security Requirements for Network Devices Protection Profile 10 December 2010 Version 1.0

Name	Description	S	A	R	I
	encryption/decryption)				
FCS_COP.1(2)	Cryptographic operation (for cryptographic signature)		✓	✓	✓
FCS_COP.1(3)	Cryptographic operation (for cryptographic hashing)		✓	✓	✓
FCS_COP.1(4)	Cryptographic operation (for keyed-hash message authentication)		✓	✓	✓
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism	✓			
FIA_UAU.6	Re-authenticating		✓		
FIA_UAU.7	Protected Authentication Feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1(1)	Basic Internal TSF Data Transfer Protection (Disclosure)	✓		✓	✓
FPT_ITT.1(2)	Basic Internal TSF Data Transfer Protection (Modification)	✓		✓	✓
FPT_PTD_EXT.1(1)	Extended: Management of TSF Data (for reading of authentication data)		✓		✓
FPT_PTD_EXT.1(2)	Extended: Management of TSF Data (for reading of all symmetric keys)		✓		✓
FPT_RPL.1	Replay Detection		✓		
FPT_TST_EXT.1	Extended: TSF testing				
FPT_TUD_EXT.1	Extended: Trusted Update	✓			
FTA_SSL_EXT.1	Extended: TSF-initiated session locking	✓		✓	
FTP_TRP.1(1)	Trusted Path (Prevention of Disclosure)	✓	✓	✓	✓
FTP_TRP.1(2)	Trusted Path (Detection of Modification)	✓	✓	✓	✓
NPM_SDC_EXT.1	Extended: System data collection		✓		
NPM_ANL_EXT.1	Extended: Analysis		✓		

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.

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 [basic] level of audit; and
c) [*Specifically defined auditable events listed in Table 11*].

Table 11 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records.	
FAU_SAR.3	Unsuccessful attempts to read information from the audit records.	
FCS_CKM.1	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM_EXT.4	Failure on invoking the cryptographic key zeroization functionality.	
FCS_COP.1(1)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FCS_COP.1(2)	Success and failure, and the type of cryptographic operation.	
FCS_COP.1(3)	Failure on invoking functionality.	
FCS_COP.1(4)	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FDP_IFF.1	All decisions on requests for information flow.	
FDP_IFC.1	None.	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions take and the subsequent, if appropriate restoration to the normal state.	No additional information.
FIA_ATD.1	None.	
FIA_SOS.1	Rejection by the TSF of any tested secret; Rejection or acceptance by the TSF of any tested secret.	
FIA_UAU.2	Unsuccessful use of the authentication mechanism; All use of the user authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU_EXT.5	Unsuccessful use of the authentication mechanism; All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.6	Failure of reauthentication; All reauthentication	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identify provided; All use of the user identification mechanism, including the user identity provided.	
FMT_MSA.1	All modifications of the values of security attributes.	
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules; all modifications of the intial values of security attributes.	
FMT_MTD.1	All modifications to the values of TSF data.	
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role.	
FPT_PTD_EXT.1(1)	None.	
FPT_PTD_EXT.1(2)	None.	
FPT_RPL.1	Detected replay attacks.	
FPT_TUD_EXT.1	When upgrade occurs.	
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond "success" or "failure".
FTP_TRP.1(1)	Failures of the trusted path functions; Identification of the user associated with all trusted path failure if available; All attempted uses of the trusted path functions; Identification of the user associated with all trusted path invocations, if available.	
FTP_TRP.1(2)	Failures of the trusted path functions; Identification of the user associated with all trusted path failure if available; All attempted uses of the trusted path functions; Identification of the user associated with all trusted path invocations, if available.	

FAU_GEN.1.2

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

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

c) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 11]*.

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

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

Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*administrator users*] with the capability to read [*all*] from the audit records.

FAU_SAR.1.2

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

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

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

Dependencies: **FAU_SAR.1 Audit review**

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to apply [*searches, sorting, ordering*] of audit data based on [*specific attributes contained in security audit logs*].

Dependencies: **FAU_SAR.1 Audit review**

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1

The TSF shall generate **asymmetric** cryptographic keys in accordance with a ~~specified cryptographic key generation algorithm~~ **domain parameter generator and a random number generator** ~~and specified cryptographic key sizes~~ that meet the following: [

a) *ANSI X9.80 (3 January 2000), "Prime Number Generation, Primality Testing, and Primality Certificates" using random integers with deterministic tests, or constructive generation methods*

b) *Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.*

c) *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"*]

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

FCS_CKM_EXT.4 Extended: Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

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

FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)

Hierarchical to: No other components.

FCS_COP.1.1(1)

The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in ECB, CBC, CFB8, CFB128, OFB modes*] and cryptographic key sizes [*128-bits, 256-bits, and* [*192 bits, no other key sizes*] that meet the following: [

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- *NIST SP 800-38A*]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(2) Cryptographic operation (for cryptographic signature)

Hierarchical to: No other components.

FCS_COP.1.1(2)

The TSF shall perform [*cryptographic signature services***]** in accordance with a specified cryptographic algorithm [*Rivest Shamir Adleman (RSA) with a key size (modulus) of 2048 bits*] and ~~cryptographic key sizes~~ that meet the following: [*FIPS PUB 186-3, "Digital Signature Standard", FIPS PUB 186-2, "Digital Signature Standard"*]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

Hierarchical to: No other components.

FCS_COP.1.1(3)

The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-384, SHA-512*] and ~~cryptographic key~~ **message digest** sizes [*160, 256, 384, 512 bits*] that meet the following: [*FIPS Pub 180-3, "Secure Hash Standard."*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)

Hierarchical to: **No other components.**

FCS_COP.1.1(4)

The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*], ~~and~~ cryptographic key sizes [*160, 256, 384, 512 bits*], **message digest sizes 160, 256, 384, 512 bits** that meet the following: [*FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"*].

Dependencies: **[FDP_ITC.1 Import of user data without security attributes, or**
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [an administrator configurable positive integer within *(1-31)*] unsuccessful authentication attempts occur related to [*user's attempts to use the User Interface*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock out the user account for 30 minutes*].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*user name, password, role*].

Dependencies: No dependencies.

FIA_SOS.1[19] Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [

1. *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");*
2. *Minimum password length shall settable by the Administrator, and support passwords of 8 characters or greater;*
3. *Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Administrator.*
4. *Passwords shall have a maximum lifetime, configurable by the Administrator.*
5. *12 or more prior passwords may be remembered to prevent repeats.*

].

Dependencies: No dependencies

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

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

Dependencies: FIA_UID.1 Timing of identification

[19] FIA_SOS.1 was used to meet the same functionality as defined in FIA_PMG_EXT.1 from the NDPP.

FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism
Hierarchical to: No other components.
FIA_UAU_EXT.5.1
The TSF shall provide a local password-based authentication mechanism, [none] to perform user authentication.
FIA_UAU_EXT.5.2
The TSF shall ensure that users with expired passwords are [required to create a new password after correctly entering the expired password].
Dependencies: No dependencies

FIA_UAU.6 Re-authenticating
Hierarchical to: No other components.

FIA_UAU.6.1
The TSF shall re-authenticate the user under the conditions [*when the user changes their password and session termination*].
Dependencies: No dependencies.

FIA_UAU.7 Protected Authentication Feedback
Hierarchical to: No other components.
FIA_UAU.7.1
The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.
Dependencies: FIA_UAU.1

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

6.2.4 The Class FMT: Security Management

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1
The TSF shall restrict the ability to [*manage as detailed in Table 12 below*] the [*TSF data*] to the [*Security Administrators as detailed in Table 12 below*].

Table 12 Management of TSF Data

Operation	TSF Data	Authorized Role
User Interface		
Configure	Global account settings	Administrator
View	User activities log	Administrator
Grant	Users the permissions to run user reports	Administrator
Manage	User accounts	Administrator

Operation	TSF Data	Authorized Role
Set	Passwords	Administrator
Manage	Groups, alert thresholds, event detection tuning and reporting, traffic reporting	Operator
Run	Traffic reports	Administrator, Operator, Monitor
View	Dashboard page	Administrator, Operator, Monitor, Dashboard Viewer
View	All reports	Administrator, Operator, Monitor, Dashboard Viewer
Set	User change password	Administrator, Operator , Monitor, Dashboard Viewer
View	Event detail report	Administrator, Operator, Monitor, Dashboard Viewer, Event Viewer
View, Upload, Generate, Exchange	Certificates	Administrator

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
- *Management of TSF data (FMT_MTD.1)*
- *Management of security attributes (FMT_MSA.1)*
- *Ability to update the TOE, and to verify the updates using hash function capability (FCS_COP.1(2))*]

Dependencies: **No dependencies**

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles: [*see Table 13 below for a listing of roles*].

Table 13 Roles

Roles
Profiler and Express User Interface
Administrator
Operator
Monitor
Dashboard Viewer
Event Viewer
Sensor User Interface
Administrator

Roles
Operator
Monitor
Gateway User Interface
Administrator
Operator
Monitor

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection (Disclosure)

Hierarchical to: No other components.

FPT_ITT.1.1(1)

The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services: SSL**.

Dependencies: No dependencies

FPT_ITT.1(2) Basic Internal TSF Data Transfer Protection (Modification)

Hierarchical to: No other components.

FPT_ITT.1.1(2)

The TSF shall ~~protect detect TSF data from~~ **detect [**modification**] of TSF data** when it is transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services: SSL**.

Dependencies: No dependencies

FPT_PTD_EXT.1(1) Extended: Management of TSF Data (for reading authentication data)

Hierarchical to: No other components.

FPT_PTD_EXT.1.1(1)

The TSF shall prevent reading of [*plaintext passwords*].

Dependencies: No dependencies

FPT_PTD_EXT.1(2) Extended: Management of TSF Data (for reading of all symmetric keys)

Hierarchical to: No other components.

FPT_PTD_EXT.1.1(2)

The TSF shall prevent reading of [*all pre-shared keys, symmetric key, and private keys*].

Dependencies: No dependencies

FPT_RPL.1 Replay Detection
Hierarchical to: No other components.

FPT_RPL.1.1
The TSF shall detect replay for the following entities: [*network packets encrypted via SSL/TLS and terminated at the TOE*].
FPT_RPL.1.2
The TSF shall perform: [*reject the data*] when replay is detected.
Dependencies: No dependencies

FPT_TST_EXT.1 Extended: TSF Testing
Hierarchical to: No other components.

FPT_TST_EXT.1.1
The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.
Dependencies: No dependencies

FPT_ TUD_EXT.1 Extended: Trusted Update
Hierarchical to: No other components

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify software updates to the TOE using a **[**published hash**]** prior to installing those updates.
Dependencies: FCS_COP.1 Cryptographic operation

6.2.6 Class FTA: TOE Access

FTA_SSL_EXT.1 Extended: TSF-initiated session locking
Hierarchical to: No other components.

FTA_SSL_EXT.1.1
The TSF shall, for local interactive sessions, [terminate the session] after a Security Administrator-specified time period of inactivity.

Dependencies: FIA_UAU.1 Timing of authentication

6.2.7 Class FTP: Trusted Path/Channels

FTP_TRP.1(1) Trusted Path (Prevention of Disclosure)
Hierarchical to: No other components.

FTP_TRP.1.1(1)
The TSF shall provide a communication path between itself and [remote] ~~users~~ **administrators using HTTPS** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure].
FTP_TRP.1.2(1)
The TSF shall permit [remote ~~*users*~~ ***administrators***] to initiate communication via the trusted path.
FTP_TRP.1.3(1)
The TSF shall require the use of the trusted path for [*all remote administrative actions*].

Dependencies: No dependencies

FTP_TRP.1(2) Trusted Path (Detection of Modification)
Hierarchical to: No other components.

FTP_TRP.1.1(2)
The TSF shall provide a communication path between itself and [*remote*] ~~users~~ **administrators using HTTPS** that is logically distinct from other communication paths and provides assured identification of its end points and ~~protection of the communicated data from~~ **detection of** [*modification*] **of the communicated data**.
FTP_TRP.1.2(2)
The TSF shall permit [remote ~~*users*~~ ***administrators***] to initiate communication via the trusted path.
FTP_TRP.1.3(2)
The TSF shall require the use of the trusted path for [*all remote administrative actions*].

Dependencies: No dependencies

6.2.8 Class NPM: Network Performance Management

NPM_SDC_EXT.1 Extended: System data collection
Hierarchical to: No other components.

NPM_SDC_EXT.1.1
The TSF shall be able to collect the following information from the targeted IT System resource(s): [*network packets*].
NPM_SDC_EXT.1.2
At a minimum, the TSF shall collect and record the following information:
- Date and time of the flow, IP source and destination, IP protocol, and the size of the flow.

Dependencies: No dependencies

NPM_ANL_EXT.1 Extended: Analysis
Hierarchical to: No other components.

NPM_ANL_EXT.1.1
The TSF shall perform the following analysis function(s) on a subset of network data collected: [*Statistical analysis metrics*].
Dependencies: NPM_SDC_EXT.1 Extended: System data collection

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 EAL3 augmented with ALC_FLR.2.

Table 14 EAL3+ 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.3 Authorisation controls
	ALC_CMS.3 Implementation Representation CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw Reporting Procedures
	ALC_LCD.1 Developer defined life-cycle model
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary 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 Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 15 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic operation (for keyed-hash message authentication)
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU_EXT.5	Extended: Password-based Authentication Mechanism
	FIA_UAU.6	Re-authenticating
	FIA_UAU.7	Protected Authentication Feedback

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
Protection of the TSF	FPT_ITT.1(1)	Basic Internal TSF Data Transfer Protection (Disclosure)
	FPT_ITT.1(2)	Basic Internal TSF Data Transfer Protection (Modification)
	FPT_PTD_EXT.1(1)	Extended: Management of TSF Data (for reading of authentication data)
	FPT_PTD_EXT.1(2)	Extended: Management of TSF Data (for reading of all symmetric keys)
	FPT_RPL.1	Replay Detection
	FPT_TST_EXT.1	Extended: TSF testing
	FPT_TUD_EXT.1	Extended: Trusted Update
Security Management	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_SSL_EXT.1	Extended: TSF-initiated session locking
Trusted path/channels	FTP_TRP.1(1)	Trusted Path (Prevention of Disclosure)
	FTP_TRP.1(2)	Trusted Path (Detection of Modification)
Network Performance Management	NPM_SDC_EXT.1	Extended: System data collection
	NPM_ANL_EXT.1	Extended: Analysis

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. As administrators manage and configure the TOE, their activities are tracked and recorded as audit records and are stored in the PostgreSQL database. Table 11 Auditable Events provides a detailed listing of the auditable events for each security functional requirement of the TOE.

The TOE provides auditing of administrator actions that occur within each of the User Interfaces. The User Interfaces provide an authorized administrator access to view the audit logs created as a result of administrator actions through the User Interface and via the reporting features. In the User Interface, the System-Audit Trail view details each operation that has been run. Only authorized administrators with the appropriate role and permissions can review the security audit logs.

The TSF provides the capability to perform selectable audit review on audited events and this functionality is limited to the Administrator role. Selectable audit review can be performed on audit trail event data.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3.

7.1.2 Cryptographic Support

The Cryptographic Support TSF function provides cryptographic functions to implement SSL/TLS which secures the communication channel between the Profiler and the other TOE Components, and between Profiler and web browsers. TLS is a network protocol that allows data to be exchanged using a secure channel between two networked devices and provides confidentiality and integrity of data sent over an unsecure network. The Cryptographic Support TSF also supports the TOE hashing functionality.

The TOE implements HTTPS for protection of the management user interfaces. HTTPS (TLS) connections are used to protect all communication between the Profiler and the User Interface.
The SSL/TLS used by the TOE is provided by an OpenSSL Object Module v2.0, which was FIPS 140-2 validated. For more information, see. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747, FIPS Certificate No. 1747. The key generation and destruction services provided by the OpenSSL FIPS Object Module v2.0rc1 were validated in a FIPS evaluation and the software remains unchanged in the TOE. During the build process, the checksum was verified to ensure that the software was unchanged from the one that sought FIPS validation. This functionality implemented in the cryptographic module maintains the evaluation status from FIPS certificate 1747. The TOE uses the following cryptographic algorithms that have been FIPS validated:

Table 16 Cryptographic Algorithms

Algorithm	Validation Certificate	Usage
AES	1884	encrypt/decrypt
DSA	589	sign and verify
RNG (ANSI X9.31 Appendix A.2.4 using AES)	985	random number generation
RSA (X9.31, PKCS #1.5, PSS)	960	sign and verify
SHA-1 SHA-256 SHA-384 SHA-512	1655	hashing
HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	1126	message integrity

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1) FCS_COP.1(2), FCS_COP.1(3), and FCS_COP.1(4).

7.1.3 Identification and Authentication

The User Interface on the TOE is utilized in accessing this function. The TOE must perform successful identification and authentication of the TOE administrator user before the TSF grants the user access to other TOE security functions. Administrator user authentication is enforced through the use of a password with strict password quality metrics. Cascade Profiler, Sensor, and Gateway maintain the security attributes as defined in FIA_ATD.1 in section 6.2.3 for each administrator user. The Cascade Profiler v9.6 specifies password length, case sensitivity, and requirement for non-alphabetic characters. The Cascade Profiler v9.6 specifies the number (12 or more) of previous passwords the appliance should save

and test to ensure that the user is not recycling a small set of passwords. Also Cascade Profiler v9.6 specifies the lifespan of a password. When a password expires, the user is forced to change it upon their next login.

Cascade Profiler v9.6 provides several password protection functions such as:

- All administrator passwords are set to expire based on an administrator configurable parameter of the number of days.
- Once an administrator user password expires, the administrator must input their old password and input a new password that meets the password quality metrics as described above.
- While the administrator user password is being entered, it is provided on screen as asterisks to avoid over the shoulder password compromise.
- All users will be locked out upon exceeding the administrator configurable threshold for unsuccessful authentication attempts.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU_EXT.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2.

7.1.4 Security Management

Security management specifies how the TOE manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and system data. For a detailed listing of TSF data managed by the TOE see Table 12 Management of TSF Data of this ST. The TOE provides authorized administrators with a GUI console referred to as the User Interface to easily manage the security functions and TSF data of the TOE.

It should be noted that in Riverbed Profiler, roles are ranked. Any operation permitted to a 'lower-ranked' role is also available to all roles above that role with only a few restrictions. For example, the Administrator role also has the ability to do the operations of the Operator, Monitor, Dashboard Viewer, and Event Viewer roles. In addition, all Operators are also Monitors, Dashboard Viewers, and Event Viewers. All Monitors are also Dashboard Viewers and Event Viewers. Both the Dashboard Viewer role and Event Viewer role do not comprise any access privileges of the other roles.

The Security Administrator role is also considered to be the Administrator role. The Administrator role has the capability to manage the behavior of all of the Security Functions provided by the TOE (Security Audit, Identification and Authentication, Security Management, and Protection). Cascade Profiler v9.6 provides several roles each with different permissions and access to the User Interface and TOE Functionality. Below is a detailed description of each user role and their access to Cascade Profiler v9.6:

- **Administrator** – Administrators set up Cascade Profiler v9.6 and Sensor on the network, set up user accounts, monitor Cascade Profiler v9.6 and Sensor status and usage, and perform backup operations. A user with an Administrator account can access all Cascade Profiler v9.6 functionality. Only those with Administrator accounts can specify mitigation actions, view the user activities log, grant users the ability to run user reports, specify global account settings, manage user accounts, and set passwords other than their own.
- **Operator** – Operators are responsible for the operational configuration of Cascade Profiler v9.6 and Sensor. This includes managing groups, alerting thresholds, event detection tuning, traffic reporting and event reporting. Operators can also modify Cascade Profiler v9.6 Sensor network settings, allocate disk storage space for logs, and run vulnerability scans. However, they cannot specify mitigation actions, view the audit trail page, specify global account settings, or modify user accounts or other people's passwords.
- **Monitor** – Monitors check the Dashboard page for new events or unexpected activity. They can run traffic reports and view all Reports pages. They can also view Cascade Profiler v9.6 and Sensor status page. The only settings pages that Monitors can change are UI Preferences and Change Password. Typically, a user with a Monitor account is in a network operations center.

- **Dashboard Viewer** – Dashboard viewers can log in and view the displays on the Dashboard page. They cannot navigate away from the Dashboard page except to go to the UI Preferences and Change Password pages. Additionally, right-click menus and reporting links are not active for Dashboard Viewer accounts.
- **Event Viewer** – Event Viewers can use their login name and password to view an Event Detail report which URL they have obtained from a network management system. They cannot take any actions on the event or navigate away from the Event Detail report.

The Gateway only provides one administrator account for configuring the Gateway and checking its status.

TOE Security Functional Requirements Satisfied: FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of the TOE.

For protection of data transmitted between the workstation accessing the User Interface and TOE when accessed remotely is secured via HTTPS. This prevents the data that is transmitted from being compromised through disclosure and modification. In addition, when the TOE communicates with a distributed TOE component all communications are over a secure SSL3.1/TLS channel. This also prevents replay attacks since the HTTPS/TLS sessions use a random nonce.

Profiler maintains the time that the other TOE Components synchronize their date and time from the Profiler.

Passwords are protected from being read in plain text format. Locally used passwords are stored in one-way hash form only using SHA-512 by calling the FIPS 140-2 cryptographic module. User input is then hashed and compared against the stored value. These stored passwords are prevented from being displayed in audit logs or in the User Interface in plaintext or hashed forms. Additionally, standard UNIX protections are used for the password shadow file. Regarding stored passwords for third-party applications, some passwords need to be stored on the device such as for SNMP[20] access to remote switches or routers. In these cases, passwords are hidden via a shared secret key which is used to AES encrypt the password before it is stored in the database by calling the FIPS 140-2 cryptographic module. Likewise, these stored passwords are prevented from being displayed in audit logs or in the User Interface in plaintext or hashed forms.

The TOE provides self-tests for the cryptographic modules referenced in Section 7.1.2.

The TOE provides authorized administrators the ability to query the current version of the TOE software, and to initiate software updates. The TOE provides hashes of the TOE software updates to ensure that only valid updates will be installed on the TOE.

TOE Security Functional Requirements Satisfied: FPT_ITT.1(1), FPT_ITT.1(2), FPT_PTD_EXT.1(1), FPT_PTD_EXT.1(2), FPT_RPL.1, FPT_TST_EXT.1, FPT_TUD_EXT.1

[20] Simple Network Management Protocol

7.1.6 TOE Access

Based on an administrator configurable amount of time, when an administrator takes no action on the User Interface pages, the User Interface will log the administrator out. The administrator must then login with a valid username and password before gaining access to the User Interface.

TOE Security Functional Requirements Satisfied: FTA_SSL_EXT.1.

7.1.7 Trusted Path/Channels

Cascade Profiler v9.6 provides trusted channels for all data from disclosure or modification while in transit between TOE components and between TOE components and some authorized IT entities. All communications between the Cascade Profiler v9.6 components are secured via TLS. TLS is used to provide trusted channels between separate parts of the TOE, between the TOE and authorized IT entities and to prevent the data from disclosure and modification. The TOE implements HTTPS and TLS for protection of the management user interfaces. The TOE generates its own certificate which is then shared among the distributed components. The TOE uses a FIPS-approved and FIPS validated cryptographic algorithms to implement the above cryptographic functions.

The cryptographic functionality within the TOE component is used to secure the sessions between the TOE and authorized IT entities. For SNMP[21] queries, SNMPv3 is used which uses TLS for securing the session.

TOE Security Functional Requirements Satisfied: FTP_TRP.1(1), FTP_TRP.1(2)

7.1.8 Network Performance Management

Cascade Profiler v9.6 collects network flow data and analyzes the collected network flow data. Both Sensor and Gateway collect traffic flow data for use by the Cascade Profiler v9.6. Expresss can also accept flow information from Sensor and Gateway components, although Express is designed primarily to operate as a stand-alone component in smaller network environment and has some Sensor and Gateway capabilities built-in.

The Gateway is deployed in a local or remote network to receive traffic data from NetFlow, sFlow, IPFIX, or Packeteer FDR sources. The Gateway aggregates the data, compresses it, encrypts it, and then transmits it to Cascade Profiler v9.6 or Express.

The Sensor monitors network traffic and provides statistics to a Cascade Profiler v9.6 or Express for aggregation and analysis. Additionally, the Sensor displays traffic statistics on graphs, tables and lists. The Profiler or Express uses the statistics to analyze traffic volumes and connection patterns throughout the network it is monitoring. One or more Sensor appliances monitor traffic using taps or mirror ports.

TOE Security Functional Requirements Satisfied: NPM_SDC_EXT.1, NPM_ANL_EXT.1.

[21] Simple Network Management Protocol

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3. This ST does not conform to any PP.

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 and 8.2.2 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 17 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	O.TOE_ADMINISTRATION counters this threat by ensuring that only authorized Administrators are able to log in and configure the TOE, and the TOE provides protections for logged-in Administrators.
	OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN counters this threat by ensuring that the TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
T.DATA_COMPROMISE An unauthorized user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	O.PROTECTED_COMMUNICATIONS counters this threat by providing protected communication channels for Administrators, other parts of a distributed TOE, and authorized IT entities
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	O.TOE_ADMINISTRATION counters this threat by ensuring that only authorized Administrators are able to log in and configure the TOE, and the TOE provides protections for logged-in Administrators.
T.FAIL_NETANAL The TOE may fail to identify the network traffic flow conditions as	O.ANALYZE The TOE will apply analytical processes and information to	O.ANALYZE counters this threat by applying analytical processes and information on collected

Threats	Objectives	Rationale
requested by the administrator.	derive conclusions about the network (past, present, or future).	network traffic to derive conclusions (past, present, or future).
	O.SCAN The TOE will collect network traffic information from the network interface card.	O.SCAN counters this threat by collecting information from the network interface card for use in applying analytical processes on the information.
T.TSF_FAILURE Security mechanisms of the TOE may fail, leading to a compromise of the TSF.	O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	O.TSF_SELF_TEST counters this threat by ensuring that the TOE provides self-tests on a subset of its security functionality to ensure it is operating properly.
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.	O.SESSION_LOCK The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.	O.SESSION_LOCK counters this threat by ensuring that if a user leaves the TOE Console unattended, the user will be logged out.
T.UNAUTHORIZED_UPDATE A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.	O.VERIFIABLE_UPDATES The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the Administrator to be unaltered and (optionally) from a trusted source.	O.VERIFIABLE_UPDATES counters this threat by ensuring that TOE updates can be verified by an Administrator.
T.UNDETECTED_ACTIONS Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.	O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data.	O.SYSTEM_MONITORING counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.

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 Assumptions

Table 18 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.NO_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE satisfies this assumption by ensuring that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	OE.PHYSICAL satisifes the assumption that the TOE environment provides physical security commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN satisfies the assumption that the users who manage the TOE are trusted and follow all guidance.
A.TIME The TOE environment must provide reliable timestamps to the TOE through the use of an NTP server.	OE.TIME The TOE environment will provide reliable timestamps to the TOE through the use of an NTP server in order to provide the TOE with reliable timestamps.	OE.TIME satisfies the assumption that the TOE environment will include an NTP server for the TOE to synchronize its time with.

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

The extended requirements are defined in section 5. These SFRs exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

Although this ST is not compliant with the NDPP, some of the NDPP SFRs have been included. The following explicitly stated SFRs were taken directly from the NDPP: FCS_CKM_EXT.4, FIA_UAU_EXT.5, FPT_TUD_EXT.1, and FTA_SSL_EXT.1.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ANALYZE The TOE will apply analytical processes and information to derive conclusions about the network (past, present, or future).	NPM_ANL_EXT.1 Extended: Analysis	The requirement meets the objective by ensuring the TOE analyzes the collected data.
O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate cryptographic keys for use during cryptographic operations.
	FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization	The requirement meets the objective by ensuring that the TOE can zeroize cryptographic keys.
	FCS_COP.1(1) Cryptographic operation (for data encryption/decryption)	The requirement meets the objective by ensuring that the TOE can perform encryption and decryption in accordance with the defined algorithms and key sizes.
	FCS_COP.1(2) Cryptographic operation (for cryptographic signature)	The requirement meets the objective by ensuring that the TOE can perform cryptographic signature services in accordance with the defined algorithms and key sizes.
	FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)	The requirement meets the objective by ensuring that the TOE can perform cryptographic hashing services in accordance

Objective	Requirements Addressing the Objective	Rationale
		with the defined algorithms and key sizes.
	FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)	The requirement meets the objective by ensuring that the TOE can perform cryptographic hashing services in accordance with the defined algorithms and key sizes.
	FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection (Disclosure)	The requirement meets the objective by ensuring that the TOE protects TSF data from disclosure when transmitted between separate parts of the TOE.
	FPT_ITT.1(2) Basic Internal TSF Data Transfer Protection (Modification)	The requirement meets the objective by ensuring that the TOE detects modification of TSF data when transmitted between separate parts of the TOE.
	FPT_PTD_EXT.1(1) Extended: Management of TSF Data (for reading of authentication data)	The requirement meets the objective by ensuring that the TOE prevents reading of plaintext passwords.
	FPT_PTD_EXT.1(2) Extended: Management of TSF Data (for reading of all symmetric keys)	The requirement meets the objective by ensuring that the TOE prevents reading of all specificed cryptographic keys.
	FPT_RPL.1 Replay Detection	The requirement meets the objective by ensuring that the TOE detects replay of network packets that have been encrypted via SSL/TLS.
	FTP_TRP.1(1) Trusted Path (Prevention of Disclosure)	The requirement meets the objective by ensuring that the TOE provides a trusted path between itself and authorized IT entities from disclosure.
	FTP_TRP.1(2) Trusted Path (Detection of Modification)	The requirement meets the objective by ensuring that the TOE provides a trusted path between itself and authorized IT entities from modification.
O.SCAN The TOE will collect network traffic information from the network interface card.	NPM_SDC_EXT.1 Extended: System data collection	The requirement meets the objective by ensuring that the TOE collects system data from the network interface card.

Objective	Requirements Addressing the Objective	Rationale
O.SESSION_LOCK The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.	FTA_SSL_EXT.1 Extended: TSF-initiated session locking	The requirement meets the objective by ensuring that the TOE logs the user out of the session. The user will then have to re-authenticate to the TOE.
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit 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_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that only authorized users are able to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that authorized users are able to search and sort the logs.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring after an administrator-specified number of unsuccessful authentication attempts, the user account is disabled.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by ensuring that the TOE maintains the user's security attributes.
	FIA_SOS.1 Verification of secrets	The requirement meets the objective by ensuring that the TOE enforces that passwords meet the required password quality metrics.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE ensures that a user must be successfully authenticated before

Objective	Requirements Addressing the Objective	Rationale
		being allowed access to TOE management functions.
	FIA_UAU_EXT.5 Extended: Password-based Authentication Mechanism	The requirement meets the objective by ensuring that the TOE provides a local password based authentication.
	FIA_UAU.6 Re-authenticating	The requirement meets the objective by ensuring that the TOE re-authenticates the user under the specified conditions.
	FIA_UAU.7 Protected Authentication Feedback	The requirement meets the objective by ensuring that the TOE provides obscured feedback while the user is authenticating.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE ensures that a user must be successfully identified before being allowed access to the TOE management functions.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	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.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	FPT_TST_EXT.1 Extended: TSF testing	The requirement meets the objective by ensuring that the TOE provides some self-tests on a subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the Administrator to be unaltered and (optionally) from a trusted source.	FCS_COP.1(2) Cryptographic operation (for cryptographic signature)	The requirement meets the objective by ensuring that the TOE collects information from the managed machines.
	FCS_COP.1(3) Cryptographic operation (for	The requirement meets the objective by ensuring that the

Objective	Requirements Addressing the Objective	Rationale
	cryptographic hashing)	TOE can perform cryptographic hashing services in accordance with the defined algorithms and key sizes.
	FPT_TUD_EXT.1 Extended: Trusted Update	The requirement meets the objective by ensuring that TOE updates can be verified by an administrator.

8.5.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package augmented with ALC_FLR.2. EAL3+ was selected as the assurance level because the TOE is a commercial product whose users require a moderate level of independently assured security. The TOE is targeted to be deployed at an environment with good physical access security (A.PHYSICAL) and competent administrators (A.TRUSTED_ADMIN), where EAL 3 should provide adequate assurance. Within such environments it is assumed that attackers will have basic attack potential. As such, EAL3 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users.
This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 20 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, the TOE maintains a reliable timestamp through use of a NTP server in the IT environment.
FAU_GEN.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2 is hierarchical to FIA_UID.1.
	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	Although FCS_CKM.4 is not in the ST, FCS_CKM_EXT.4 provides coverage.
	FCS_COP.1(3)	✓	
	FCS_COP.1(2)	✓	
	FCS_COP.1(4)	✓	
	FCS_COP.1(1)	✓	
FCS_CKM_EXT.4	FCS_CKM.1	✓	
FCS_COP.1(1)	FCS_CKM.4	✓	Although FCS_CKM.4 is not in the ST, FCS_CKM_EXT.4 provides coverage.
	FCS_CKM.1	✓	
FCS_COP.1(2)	FCS_CKM.1	✓	
	FCS_CKM.4	✓	Although FCS_CKM.4 is not in the ST, FCS_CKM_EXT.4 provides coverage.
FCS_COP.1(3)	FCS_CKM.4	✓	Although FCS_CKM.4 is not in the ST, FCS_CKM_EXT.4 provides coverage.
	FCS_CKM.1	✓	
FCS_COP.1(4)	FCS_CKM.1	✓	
	FCS_CKM.4	✓	Although FCS_CKM.4 is not in the ST, FCS_CKM_EXT.4 provides coverage.
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2 is hierarchical to FIA_UAU.1.
FIA_ATD.1	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2 is hierarchical to FIA_UID.1.

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU_EXT.5	No dependencies	✓	
FIA_UAU.6	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2 is hierarchical to FIA_UAU.1.
FIA_UID.2	No dependencies	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UIA_EXT.1 provides coverage for user identification and authentication which supersedes FIA_UID.1.
FPT_ITT.1(1)	No dependencies	✓	
FPT_ITT.1(2)	No dependencies	✓	
FPT_PTD_EXT.1(1)	No dependencies	✓	
FPT_PTD_EXT.1(2)	No dependencies	✓	
FPT_RPL.1	No dependencies	✓	
FPT_TST_EXT.1	No dependencies	✓	
FPT_TUD_EXT.1	FCS_COP.1(3)	✓	
FTA_SSL_EXT.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2 is hierarchical to FIA_UAU.1.
FTP_TRP.1(1)	No dependencies	✓	
FTP_TRP.1(2)	No dependencies	✓	
NPM_SDC_EXT.1	FPT_STM.1	✓	
NPM_ANL_EXT.1	NPM_SDC_EXT.1	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 21 Acronyms

Acronym	Definition
AUX	Auxilary
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
FDR	Flow Detail Records
GUI	Graphical User Interface
IPFIX	Internet Protocol Flow Information Export
IT	Information Technology
LAN	Local Area Network
MNMP	Mazu Networks Management Protocol
NDPP	Network Devices Protection Profile
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
QOS	Quality of Service
RSP	Riverbed Services Platform
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VE	Virtual Edition
WAN	Wide Area Network

9.2 Terminology

Table 22 Terms

Name	Definition
NetFlow	NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information. NetFlow has become an industry standard for traffic monitoring and is supported by many platforms.
Network flows	The information collected by the TOE.
sFlow	sFlow is a technology for monitoring network, wireless and host devices.
Target network	The domain of network and managed devices to be analyzed by the TOE.
WAN	Wide Area Network

9.3 Documentation References

Table 23 Documentation References

ID	Definition
NDPP	Security Requirements for Network Devices Protection Profile 10 December 2010 Version 1.0
Profiler User Guide	Cascade Profiler v9.6 and Cascade Profiler v9.6 Express User's Guide Version 9.6 July 2012
Sensor	Cascade Sensor and Cascade Gateway User's Guide Version 9.6 July 2012

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