Riverbed Technology

Riverbed SteelHead CX with RiOS 9.1.4

Security Target

December 2016

199 Fremont Street
San Francisco, CA 94105
Phone: (415) 247-8801
http://www.riverbed.com

Document prepared by:

Ark Infosec Labs, Inc.
www.arkinfosec.net

Document prepared for:

CGI Global IT Security Labs.

1410 Blair Place, 7th floor
Ottawa, ON K1J 9B9, Canada
www.cgi.com/securitylab

Document History

Version	Date	Author	Description
1.0	Jan 18, 2016	L Turner	Release for evaluation.
1.1	Feb 25, 2016	L Turner	Address evaluator observations.
1.2	Mar 21, 2016	L Turner	Address evaluator observations.
1.3	Mar 22, 2016	L Turner	Address evaluator observations.
1.4	Jun 20, 2016	L Turner	Address evaluator observations.
1.5	July 28, 2016	M Lanoue	TOE Version update.
1.6	Aug 11, 2016	L Turner	Clarify user roles.
1.7	Nov 8, 2016	L Turner	Address evaluator observations.
1.8	Dec 12, 2016	L Turner	Final clarifications.
1.9	Dec 15, 2016	L Turner	Update guidance references.
2.0	Dec 19, 2016	L Turner	Finalized for certification.

Table of Contents

1 Introduction 5

1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 5

2 TOE Description 7

2.1 Type 7
2.2 Overview and Usage 7
2.3 Security Functions 9
2.4 Physical Scope 10
2.5 Logical Scope 14

3 Security Problem Definition 15

3.1 Threats 15
3.2 Organizational Security Policies 15
3.3 Assumptions 15

4 Security Objectives 17

4.1 Objectives for the Operational Environment 17
4.2 Objectives for the TOE 17

5 Security Requirements 19

5.1 Conventions 19
5.2 Extended Components Definition 19
5.3 Functional Requirements 19
5.4 Assurance Requirements 29

6 TOE Summary Specification 31

6.1 Security Audit 31
6.2 Secure Communications 31
6.3 User Data Protection 33
6.4 Security Management 33
6.5 Cryptographic Module 35

7 Rationale 36

7.1 Security Objectives Rationale 36
7.2 Security Requirements Rationale 38
7.3 TOE Summary Specification Rationale 45

List of Tables

Table 1: Evaluation identifiers 5
Table 2: Terminology 5
Table 3: TOE Appliance Models 13
Table 4: TOE Guidance Documents 13
Table 5: Threats 15
Table 6: Assumptions 15
Table 7: Operational environment objectives 17
Table 8: Security objectives 17
Table 9: Summary of SFRs 19
Table 10: Assurance Requirements 29
Table 11: Security Audit SFRs 31

Table 12: Security Communication SFRs 32
Table 13: User Data Protection SFRs 33
Table 14: Security Management SFRs 34
Table 15: Cryptographic Module SFRs 35
Table 16: Security Objectives Mapping 36
Table 17: Suitability of Security Objectives 36
Table 18: Security Requirements Mapping 38
Table 19: Suitability of SFRs 39
Table 20: Dependencies 43
Table 21: Map of SFRs to TSS Security Functions 45

1 Introduction

1.1 Overview

1 Riverbed SteelHead CX with RiOS 9.1.4 is a Wide Area Network (WAN) optimization solution designed to reduce bandwidth and increase performance of network dependent applications.

2 This Security Target (ST) defines the Riverbed SteelHead CX with RiOS 9.1.4 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Riverbed SteelHead CX with RiOS 9.1.4
Security Target	Riverbed SteelHead CX with RiOS 9.1.4 Security Target, v2.0

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 4

b) CC Part 2 conformant

c) CC Part 3 conformant

d) Evaluation Assurance Level (EAL) 2 augmented (ALC_FLR.1)

1.4 Terminology

Table 2: Terminology

Term	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
LZW	Lempel-Ziv-Welch compression
OSP	Organizational Security Policy

Term	Definition
PP	Protection Profile
RBM User	Role Based Management User
SDR	Scalable Data Referencing
SFP	Security Function Policy
ST	Security Target
TA	Transaction Acceleration
TOE	Target of Evaluation
TP	Transaction Prediction
TSF	TOE Security Functionality
WAN	Wide Area Network
WDS	Wide Area Data Services - application acceleration, WAN optimization, Wide Area File Services, QoS, traffic shaping and web caching.
QoS	Quality of Service
RiOS	Riverbed Optimization System
VWE	Virtual Window Expansion

2 TOE Description

2.1 Type

4 The TOE is a network appliance, OS, and application software (RiOS) that provide WAN optimization. The TOE type is WAN Optimization.

2.2 Overview and Usage

5 The TOE transparently applies a proprietary algorithm to optimize performance of network traffic and applications across an enterprise network. The TOE optimizes only outbound traffic. However, in a typical deployment the SteelHead CX is deployed in pairs, with each member of the pair optimizing its outbound traffic to other. In this typical deployment, the TOE communicates with a peer SteelHead CX at the other end of the WAN.

6 The TOE uses TLS to protect optimized user traffic across the WAN. Underlying cryptography is implemented by a Federal Information Processing Standard (FIPS) 140-2 validated cryptography module.

7 The TOE provides QoS, which allows administrators to control the prioritization of different types of network traffic and to ensure that SteelHead CXs give certain network traffic priority over other types of traffic. In addition to standard QoS services, the SteelHead CX offers a QoS service that allows administrators to set the minimum bandwidth for certain applications that require a constant data rate. The TOE is able to provide these applications with the minimum acceptable bandwidth the applications require because the TOE separates bandwidth and priority in defining QoS rules. In addition to QoS, the Path Selection feature can route traffic over different links based on established rules.

8 The TOE can be deployed in a number of configurations depending on the individual requirements of the network where the TOE is being deployed. A typical deployment called Physical In-Path deployment is shown below. In the Physical In-Path deployment, the Steelhead Appliance is located physically in the data stream between clients and servers. Other deployment scenarios are depicted and explained in the *Riverbed Steelhead Appliance Deployment Guide*.

9 The SteelHead CX's management interfaces are role-based and are restricted to authorized administrators. The SteelHead CX's management and access control functions control access to the various commands available through a Command Line Interface (CLI) and a web-based Graphical User Interface (GUI). Each interface provides identification and authentication functionality for administrators. The SteelHead CX is transparent to end users.

10 Figure 1 below shows the details of the Physical In-Path deployment configuration of the TOE.

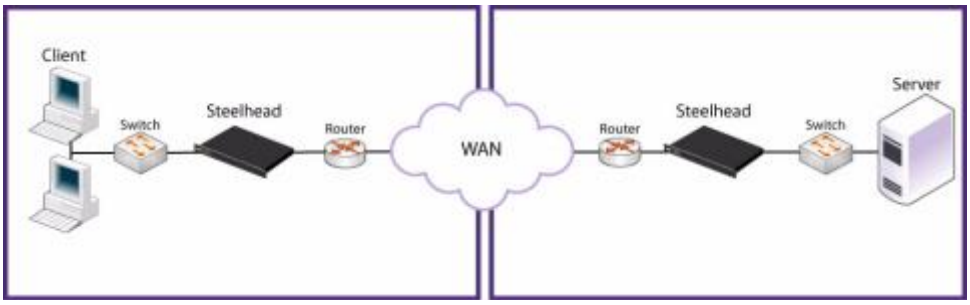

Figure 1: Physical In-Path Configuration

2.2.1 Key Concepts

11 This section presents the key concepts necessary to understanding the way the SteelHead CX functions. The SteelHead CX works through Transaction Acceleration (TA). TA is composed of three components: Scalable Data Referencing (SDR), Virtual Window Expansion (VWE), and Transaction Prediction (TP).

2.2.1.1 Scalable Data Referencing

12 SDR refers to the proprietary algorithm the TOE uses to optimize bandwidth. SDR breaks up TCP data into data chunks that the TOE stores in a data store (non-volatile memory). The TOE assigns a unique integer label as a reference to each data chunk, and then sends the reference and data chunk to the peer SteelHead CX across the WAN. If the TOE must transmit the same byte sequence again, the TOE sends the integer reference instead. The peer SteelHead CX uses the reference to reconstruct the original data chunk. The TOE and its peer maintain the correlation of data to references in their respective data stores in a structure known as a secure vault.

13 When the TOE first sends data across a network, all data and labels are new and are sent to the SteelHead CX on the far side of the network. The TOE creates new labels whenever the TOE must send new data chunks across the network. If the TOE has already sent a data chunk across the network, the TOE only sends the reference in place of the data chunk.

14 One use of the SteelHead CX is to optimize files being sent across the network. Different files from either the same or different applications can share the same reference if the underlying bits are common to both (for example, if a text file and an executable file both contain the bit sequence 01011101). The underlying bits that compose files might be the same if the same text is used in multiple files, or if two different applications code different information with the same binary sequences.

15 The TOE compresses the data and accompanying references with conventional compression algorithms (such as Lempel-Ziv-Welch (LZW)) if the compression will improve performance.

2.2.1.2 Virtual Window Expansion

16 VWE refers to the TOE's ability to repack TCP datagrams into larger packets in a new TCP session. This allows the TOE to buffer data until a larger effective byte sequence can be sent, optimizing the use of bandwidth by reducing the overhead of sending less data per round trip time.

2.2.1.3 Transaction Prediction

17 TP allows the TOE to reduce the overhead that normally occurs during session handshakes by pipe-lining transactions. During TP, the TOE predicts when a specific exchange is likely to take place based on a history of transactions. If the TOE determines that there is a high likelihood that a future transaction will occur, the TOE performs that transaction immediately. By pipe-lining transactions, the overhead of waiting for each step to travel across the WAN is greatly reduced. The TOE is programmed with sufficient knowledge of individual protocols to determine when it is "safe" (i.e. when performing TP will not cause problems) to pipe-line transactions.

2.3 Security Functions

18 The TOE provides the following security functions:

a) **Security Audit.** The SteelHead CX provides functionality for generation and viewing of audit records. The SteelHead CX administrators can view all audit information from the audit logs, as well as search the audit records. The SteelHead CX provides reliable time stamps that it will use to record the accurate time for audit records.

b) **Secure Communications.** The SteelHead CX provides TLS protection on a secure channel between SteelHead CXs. In addition, the TOE uses HTTPS (web) and SSH (CLI) to secure management connections. The TOE also uses SNMPv3 with AES to protect SNMP messages (SNMP traps generated by the TOE are excluded from the scope of evaluation).

c) **User Data Protection.** The SteelHead CX implements functionality for controlling access and traffic information flows. Access to the SteelHead CX requires an authorized username and role. Access to the management functions on the SteelHead CX is partitioned according to the administrator's role. The SteelHead CX enforces an Optimization Policy that applies a set of rules to TCP traffic passing through the SteelHead CX. Within the Optimization Policy there exists a subset of rules that an administrator can apply to prioritize TCP and UDP traffic passing through the SteelHead CX.

d) **Security Management.** The SteelHead CX provides functionality that allows administrators to manage the SteelHead CX Security Function, including security function behavior and security attributes. The Security Management function specifies the roles defined for managing the SteelHead CX and how administrators assume the roles. The SteelHead CX terminates an inactive administrator session after a preconfigured time period, depending on which interface is being used (the CLI or the GUI). Administrators must re-authenticate after being logged out. This prevents an unauthorized individual from gaining access to the SteelHead CX management functions through an unattended session.

e) **Cryptographic Module.** A FIPS 140-2 validated cryptographic module performs all cryptographic operations.

2.4 Physical Scope

19 The TOE comprises the hardware and software of the SteelHead CX. Figure 2 illustrates the physical scope of the TOE and identifies the components of the TOE Environment.

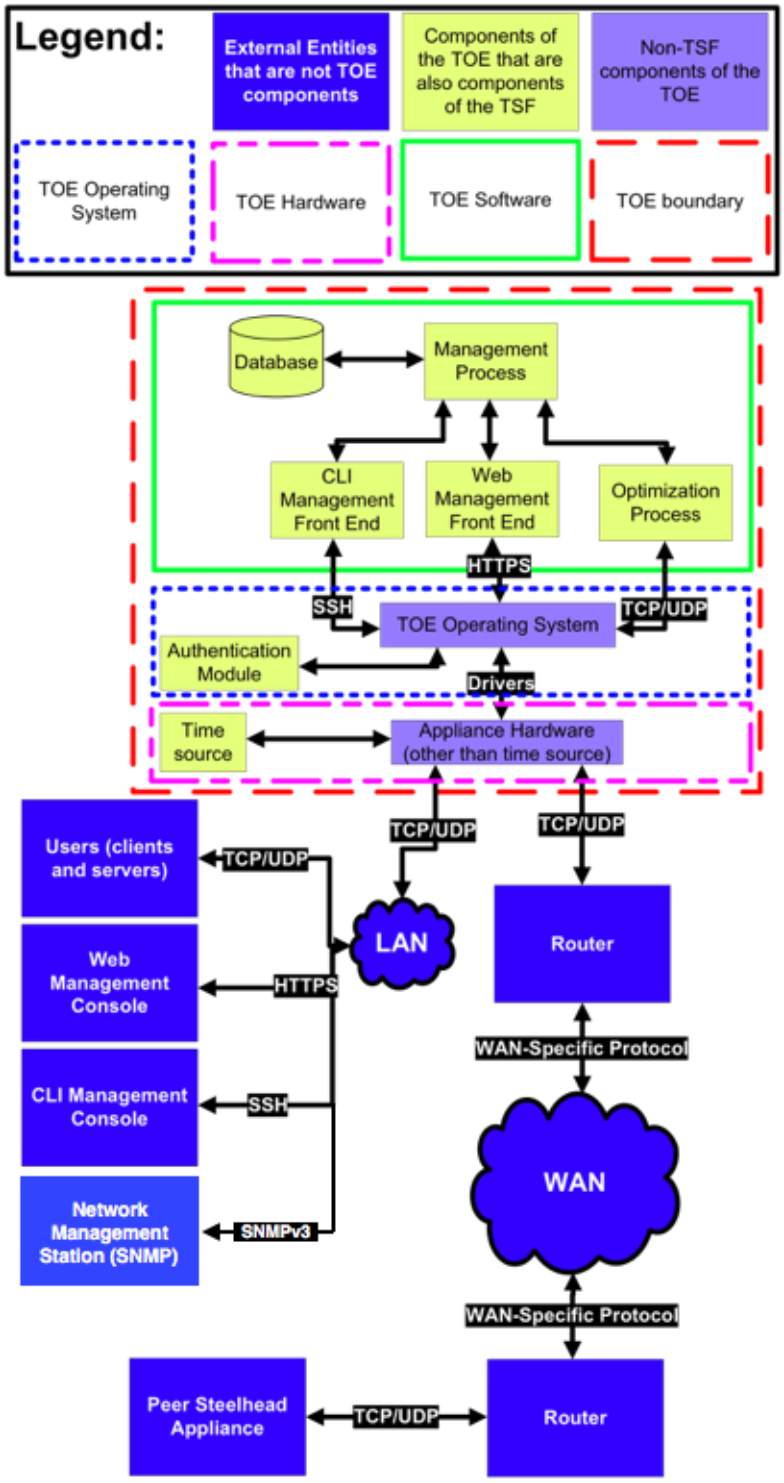

Figure 2: TOE Physical Scope

2.4.1 TOE Components

20 The following SteelHead CX components are part of the TOE and the TOE Security Functionality (TSF):

a) **Management Interfaces**

i) **Web GUI.** The TOE includes a web-based GUI that provides administrators with a set of forms and buttons to manage the TOE. The interface is organized through tabs and menus into the major functional categories of the TOE. The GUI requires administrators to be authenticated before providing any management functionality. Administrators must access the GUI through a web browser that supports Secure Hypertext Transfer Protocol (HTTPS).

a. Administrators can manage optimization services, host settings, advanced networking configurations, proxy file service (if available), port labels, reports, logging, date and time, authentication, licenses, secure vault, scheduled jobs, the configuration manager, start and stop services, and restart and shut down the appliance through the GUI.

b. Administration supports the roles identified in section 2.4.3.

ii) **Command Line Interface.** The TOE includes a CLI that provides administrators with a set of text-based commands to manage the TOE. The CLI requires administrators to authenticate before providing any management functionality. Remote access to the CLI is protected through SSH, and an SSH client is required to access the CLI.

a. The administrator is given monitor permissions upon first authenticating through the CLI. Administrators with read-only permissions are limited to viewing the system configuration and logs and may execute a limited set of CLI commands. The administrator must explicitly request the Administrator role by entering the enable and configure commands. Only administrators who assume the Administrator role can configure the TOE through the CLI.

iii) **SNMP Interface.** The TOE supports SNMPv3 with AES for status monitoring by a Network Management Station. SNMP traps generated by the TOE are excluded from the scope of evaluation.

b) **Managers**

i) The TOE has a centralized architecture with all parts residing within the same physical hardware. However, there are several processes that act as managers of certain data:

a. **Data manager**. Handles requests for data in the local database. Requests come in via a proprietary database connector. The database holds system information, statistics, and configuration files.

b. **Configuration manager.** Handles all configuration changes, actions taken on the appliance, and any events that occur that require the SteelHead CX to perform processing.

c) **Services**

i) **Network services.** RiOS (all of the components within the green box in Figure 2) supports a suite of network services including basic packet filtering, QoS, optimization of traffic, etc. These services use various protocols to ensure that the appropriate rules are applied to user traffic. Network services implement an administrator-definable Optimization Policy.

ii) **Management services.** RiOS allows authorized administrators to access the security functionality for the TOE configuration. Administrators can view the configuration and make changes as necessary. These changes are handled through the GUI and the CLI.

iii) **Reporting and logging services.** RiOS allows authorized administrators to view complex statistics on the history of user traffic that has gone through the TOE. Administrators can view reports on many different statistics and specify variables about the data shown (such as showing data starting from a certain date). The logging services allow the TOE to keep formatted audit records and display them to authorized administrators in a human-readable format.

2.4.2 Data

21 The TOE works with four kinds of data:

a) **User data.** All data that TOE users send over the network that passes through the TOE. User data may be stored on the TOE in the encrypted data store in the form of SDR references. When the TOE receives user data, the TOE applies the Optimization Security Function Policy (SFP) to the data. Any operations that the TOE performs on user data are a result of administrator-defined rules in the Optimization SFP.

b) **Management data.** All data that TOE administrators send to or request from the TOE. Management data includes all system settings and logs that are sent to be displayed on an administrator's workstation, and any commands an administrator sends to the TOE. Access to management data is regulated by the Access Control SFP. An Administrator is not given access to data that the administrator is not authorized to access.

c) **TSF data.** All data stored in the secure vault and all configuration data that affects the TSFs (such as Optimization SFP rules). TSF data is managed through the Management Interfaces as a result of commands given by administrators. Access to TSF data is regulated by the Access Control SFP.

d) **System data.** All configuration data on the system that is not related to enforcement of the TSFs (such as licenses, scheduled jobs, and startup/shutdown of the appliance). System data is managed through the Management Interfaces as a result of commands given by administrators. Access to system data is regulated by the Access Control SFP.

22 All TSF and system data resides within the local database or in configuration files on the local file system. It may be that some types of data overlap, for example, some management data may also be TSF data.

2.4.3 Users and Administrators

23 A SteelHead CX user is anyone who sends TCP or UDP traffic through the TOE. Users have no roles and do not need to be aware of the presence of the TOE on the

network. All user traffic is generated by client devices that users are working from and servers that these clients are communicating with.

24 A SteelHead CX administrator is anyone who connects to one of the TOE Management Interfaces who is authorized to manage the TOE. Administrators are divided into the following roles:

a) **Administrator.** An administrator that has read-write access to all TOE settings and data.

b) **Monitor.** An administrator that has read-only access to TOE settings and data (with the exception that the Monitor role can execute the 'no authentication policy login max-failures' and 'no authentication policy password expire' CLI commands).

25 These roles are the same for both Management Interfaces. For CLI users to attain read-write privileges, they must enter the enable command.

2.4.4 Appliance Models

26 Table 3 identifies the SteelHead CX models that are addressed by this Security Target.

Table 3: TOE Appliance Models

Model	Processor Family	Processor	Clock / Cores	Chassis	Firmware
CX570	Intel Pentium (Gladden Ivy Bridge)	Intel Pentium B925C	2.0 GHz (2 cores)	Desktop	RiOS 9.1.4
CX770	Intel Xeon E3 v2 (Ivy Bridge)	Intel Xeon E3-1125Cv2	2.5 GHz (4 cores)	Desktop	RiOS 9.1.4
CX3070	Intel Xeon E5 v2 (Ivy Bridge)	Intel Xeon E5-2609v2	2.5 GHz (4 cores)	1RU	RiOS 9.1.4
CX5070	Intel Xeon E5 v2 (Ivy Bridge)	Intel Xeon E5-2630v2	2.6 GHz (2x 6 cores)	2RU	RiOS 9.1.4
CX7070L/M	Intel Xeon E5 v2 (Ivy Bridge)	Intel Xeon E5-2650v2	2.6 GHz (2x 8 cores)	2RU	RiOS 9.1.4
CX7070H	Intel Xeon E5 v2 (Ivy Bridge)	Intel Xeon E5-2690v2	2.6 GHz (2x 10 cores)	2RU	RiOS 9.1.4

2.4.5 Guidance Documents

27 The TOE includes the guidance documents identified in Table 4.

Table 4: TOE Guidance Documents

Name	Version / Part No.
Network and Storage Card Installation Guide	712-00018-21
SteelHead Deployment Guide	712-00003-21

Name	Version / Part No.
Getting Started Guide	712-00102-14
SteelHead Installation and Configuration Guide	712-00001-21
Rack Installation Guide	712-00010-21
Riverbed Command Line Interface Reference Manual	712-00002-23
Upgrade and Maintenance Guide	712-00016-21
SteelHead Management Console User's Guide	712-00007-21
FIPS Administrator's Guide	712-00047-03
Riverbed SteelHead CX with RiOS 9.1.4 Operational User Guidance and Preparative Procedures	v0.9, 13 December 2016
Riverbed SteelHead CX with RiOS 9.1.4 Monitor Role CLI Reference	v1.0, 13 December 2016

2.4.6 Non-TOE Components

28 The TOE operates with the following components in the environment in addition to standard networking equipment:

a) Application clients

b) Application servers

c) Network Management Station (SNMP)

2.5 Logical Scope

29 The logical scope of the TOE comprises the security functions defined in section 2.3.

2.5.1 Unevaluated Features

30 The Riverbed SteelHead CX contains software and hardware components that are included with the product but are not part of the evaluated configuration:

a) Hypertext Transfer Protocol (HTTP) Management,

b) Telnet-server Management interface

c) REST API

d) IPSec

e) TLS versions other than TLS 1.2

f) SNMP versions other than SNMPv3

g) Virtual In-Path deployments

h) Out-Of-Path deployments

i) RBM User

3 Security Problem Definition

3.1 Threats

31 Table 5 identifies the threats addressed by the TOE.

Table 5: Threats

Identifier	Description
T.MASQUERADE	An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for it.
T.SYSDATA	An attacker who is not a TOE administrator could access and interpret TSF data stored on the TOE in the secure vault.
T.NACCESS	An attacker may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.
T.LATENCY	A high volume of user traffic may overwhelm the communications link between users and the IT systems they are attempting to access.

3.2 Organizational Security Policies

32 There are no Organizational Security Policies (OSPs) that are addressed by the TOE.

3.3 Assumptions

33 Table 6 identifies the assumptions related to the TOE's environment.

Table 6: Assumptions

Identifier	Description
A.INSTALL	It is assumed that the TOE will be installed and configured at an appropriate point in the network according to the appropriate installation guides.
A.NETCON	It is assumed that the TOE environment provides the network connectivity required to allow the TOE to provide secure Wide Area Data Services (WDS).
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.

Identifier	Description
A.MANAGE	It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.FIREWALL	It is assumed that all ports needed for proper operation of the TOE will be opened at the firewall.

4 Security Objectives

4.1 Objectives for the Operational Environment

34 Table 7 identifies the objectives for the operational environment.

Table 7: Operational environment objectives

Identifier	Description
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.FIREWALL	The Firewall must have all ports needed for proper operations of the TOE opened.
OE.MANAGE	Sites deploying the TOE will provide administrators for the TOE who are not careless, negligent, or willfully hostile, are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely, including management of the audit trail.
OE.PHYCAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.AUDIT	Authorized managers of the audit facilities must ensure that the audit facilities are used and managed effectively. In particular, audit logs should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future. Also, the audit logs should be archived in a timely manner to ensure that the machine does not run out of audit log data storage space.
OE.REVIEW	The configuration of the TOE will be inspected on a regular basis to ensure that the configuration continues to meet the organization's security policies in the face of: Changes to the TOE configuration • Changes in the security objectives • Changes in the threats presented by the hostile network • Changes (additions and deletions) in the services available between the hostile network and the corporate network

4.2 Objectives for the TOE

35 Table 8 identifies the security objectives for the TOE.

Table 8: Security objectives

Identifier	Description
O.AUTHENTICATE	The TOE must require administrators to authenticate before gaining access to the TOE interfaces.

Identifier	Description
O.LOG	The TOE must record events of security relevance at the “not specified level” of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail. The TOE must be able to provide reliable timestamps for its own use in order to record events in the correct order in which they occurred.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.
O.SECVAULT	The TOE must encrypt keys and certificates stored on the TOE in a secure vault and restrict access to the secure vault to authorized administrators only.
O.SEC_COMMS	The TOE must protect the confidentiality of WAN traffic, as specified by the Optimization Policy, and communication with remote administrators.
O.OPTIMIZE	The TOE must optimize traffic flowing through the TOE according to the rules defined in the Optimization Policy.

5 Security Requirements

5.1 Conventions

36 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

5.2 Extended Components Definition

37 There are no extended components defined for this ST.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes

Requirement	Title
FMT_MSA.3(a)	Static attribute initialization
FMT_MSA.3(b)	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FMT_SMR.3	Assuming roles
FPT_STM.1	Reliable time stamps
FTA_SSL.3	TSF-initiated termination
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted Path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) Login, Logout, Change Password, System Failures.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *additional details specified in the above table.*

Application Note: Audit of logout event is applicable to the CLI only.

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide *Administrators and Monitors* with the capability to read *all recorded information* 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.

FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply *searches* of audit data based on *an administrator-specified keyword or string*.

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

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

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *listed in the table below* and specified cryptographic key sizes *listed in the table below* that meet the following: *standards listed in the table below*.

Algorithm	Key Size	Standards (RNG)	CAVP (RNG)
3DES	168	SP800-90 DRBG	#310
AES	128, 192, 256		
RSA	2048		
DSA	2048, 3072		
ECDSA	Curves: P-224, P-384, P-521.		

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

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

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

FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform *cryptographic operations shown in the table below* in accordance with a specified cryptographic algorithm *shown in the table below* and cryptographic key sizes *shown in the table below* that meet the following: *standards shown in the table below*.

Operation	Algorithm	Key Size	Standards	CAVP
Symmetric encryption and decryption	3DES CBC	168	SP 800-67	#1485
	AES ECB, CFB, GCM & CBC	128, 192, 256	FIPS 197	#2374
Asymmetric encryption and decryption	RSA	2048	FIPS 186-2	#1229
	DSA	2048, 3072	FIPS 186-4	#745
	ECDSA	Curves: P-224, P-384, P-521.	FIPS 186-2	#392
Message Digest	SHA-1, SHA-2 (224, 256, 384, 512)	N/A	FIPS 180-3	#2046
Message Authentication	HMAC	160-512	FIPS-198	#1476
Random Number Generation	SP 800-90 DRBG: Hash DRBG	N/A	SP 800-90	#310

Operation	Algorithm	Key Size	Standards	CAVP
	HMAC DRBG, no reseed CTR DRBG (AES), no derivation function			

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the *Access Control SFP* on

Subjects: Administrators attempting to establish an interactive session with the TOE

Objects: User interface menu items, rules, services, product features, CLI commands, SSL Certificates

Operations: All interactions between the subjects and objects identified above

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the *Access Control SFP* to objects based on the following:

Subject attributes:

- *Role*
- *Identification (ID)*

and Object attributes:

- *Permissions assigned to objects*
- *Absence of permissions assigned to objects*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If a subject with the Administrator role requests access to an object then access is granted.*
- *If a subject with the monitor role requests read access to an object, then access is granted.*
- *If none of the above rules apply, access is denied.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*.

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *Optimization SFP* on

- *SUBJECTS: external IT entities that send or receive information through the TOE*
- *INFORMATION: traffic flowing through the TOE*
- *OPERATIONS: Optimize, pass-through, deny, discard*

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the *Optimization SFP* based on the following types of subject and information security attributes:

Subject Attributes:

- *IP address*

Information Attributes:

- *Source IP address*
- *Destination IP address*
- *Port number*
- *Virtual Local Area Network (VLAN) tag ID*
- *TLS status*
- *Application protocol*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules

hold: *Apply the appropriate operation based on the information attributes evaluated against the policy rules*.

FDP_IFF.1.3 The TSF shall enforce the: *no additional rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *the TOE will permit all information flows without applying any other rules when in Bypass Mode*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *none*.

5.3.4 Identification and Authentication (FIA)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each ~~user~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each ~~user~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

5.3.5 Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

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

FMT_MOF.1.1 The TSF shall restrict the ability to <u>determine the behavior of, disable, enable, modify the behavior of</u> the functions *shown in the table below* to *the roles show in the table below*:

Role	Permissions
Monitor	View all settings and logs.
Administrator	View all settings and logs, determine the behavior of, disable, enable, modify the behavior of system

Role	Permissions
	settings, the Access Control SFP, and the Optimization SFP, modify administrator passwords.

Application note: The Monitor role can execute the following CLI commands:

- no authentication policy login max-failures
- no authentication policy password expire
- alarms reset-all
- no service cloud-accel application * svcgroup * enable
- service cloud-accel application * svcgroup * enable

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the *Access Control SFP, Optimization SFP* to restrict the ability to *manage* the security attributes:

Access Control SFP attributes

- *Role*
- *Identification (ID)*
- *Permissions*

Optimization SFP attributes

- *Optimization Policy Rules*

to *Administrator*.

FMT_MSA.3(a) Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Access Control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *authorized administrator* to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(b) Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Optimization SFP* to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *authorized administrator* to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Manage audit functions*
- *Manage users, roles and permissions*
- *Manage optimization policies*
- *Manage time*
- *Manage cryptographic functions*
- *Manage trusted paths and trusted channels*

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

- *Monitor*
- *Administrator*

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

FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: *Administrator role from the CLI in user mode*.

5.3.6 Protection of the TSF (FPT)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.3.7 TOE Access (FTA)

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after an *administrator-defined time interval of administrator inactivity between 1 and 43200 minutes for the GUI or between 1 and 1440 minutes for the CLI*.

Application Note: A value of 0 disables session termination.

5.3.8 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the TSF, another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *TLS communications with a peer appliance, SNMPv3 communication with an SNMP Network Management Station*.

Application Note: Peer appliance refers to another Riverbed SteelHead CX appliance as listed in Table 3.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *remote administration via HTTPS (web GUI) and SSH (CLI)*.

5.4 Assurance Requirements

38 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2+ (ALC_FLR.1).

Table 10: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.1	Flaw Remediation Procedures
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
Tests	ATE_COV.1	Evidence of Coverage

Assurance Class	Components	Description
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Security Audit

39 The Security Audit function provides the TOE with the functionality for generation and viewing of audit records.

Table 11: Security Audit SFRs

SFR	Fulfillment
FAU_GEN.1	The TOE generate audit records for the following events occurring at the GUI or CLI: • Login • Logout (CLI only) • Change Password The TOE will also log system failures. The TOE records the date and time of the event, the type of event, the subject identity (for actions initiated by subjects) and the outcome (success or failure) of the event. Auditing of GUI events cannot be disabled – logs of the startup and shutdown of the TOE therefore signify the start and stop of audit functions.
FAU_SAR.1	The SteelHead CX GUI provides a means to view audit records stored on the TOE. All administrator roles can view audit records through the logging screens in the GUI or through the show logging command in the CLI. Audit records are displayed in a human-readable format. Administrators can specify a keyword or string that is used to search the audit records.
FAU_SAR.3	
FPT_STM.1	The TOE contains a hardware chip that an administrator can set to the current date and time. The chip provides time stamps to the TOE as requested. To set the system time an administrator must have write privileges and be authenticated through one of the Management Interfaces.

6.2 Secure Communications

40 The SteelHead CX provides TLS protection on a secure channel between SteelHead CXs. In addition, the TOE uses HTTPS (web) and SSH (CLI) to secure management connections and SNMPv3 with AES for communication with a Network Management Station (SNMP traps generated by the TOE are excluded from the scope of evaluation).

Table 12: Security Communication SFRs

<table>
<tr><th>SFR</th><th>Fulfillment</th></tr>
<tr><td>FTP_ITC.1</td><td>The TOE can be configured to use TLS to secure communications between SteelHead CXs.

TLS

The TOE supports TLS 1.2. When in FIPS Mode (evaluated configuration) the TOE supports the following ciphersuites:

<table>
<tr><th></th><th>KeyExch:</th><th>Auth:</th><th>Enc.:</th><th>Mac:</th></tr>
<tr><td>ECDHE-RSA-AES256-GCM-SHA384</td><td>ECDH</td><td>RSA</td><td>AESGCM(256)</td><td>AEAD</td></tr>
<tr><td>ECDHE-ECDSA-AES256-GCM-SHA384</td><td>ECDH</td><td>ECDSA</td><td>AESGCM(256)</td><td>AEAD</td></tr>
<tr><td>ECDHE-RSA-AES256-SHA384</td><td>ECDH</td><td>RSA</td><td>AES(256)</td><td>SHA384</td></tr>
<tr><td>ECDHE-ECDSA-AES256-SHA384</td><td>ECDH</td><td>ECDSA</td><td>AES(256)</td><td>SHA384</td></tr>
<tr><td>ECDH-RSA-AES256-GCM-SHA384</td><td>ECDH/RSA</td><td>ECDH</td><td>AESGCM(256)</td><td>AEAD</td></tr>
<tr><td>ECDH-ECDSA-AES256-GCM-SHA384</td><td>ECDH/ECDSA</td><td>ECDH</td><td>AESGCM(256)</td><td>AEAD</td></tr>
<tr><td>ECDH-RSA-AES256-SHA384</td><td>ECDH/RSA</td><td>ECDH</td><td>AES(256)</td><td>SHA384</td></tr>
<tr><td>ECDH-ECDSA-AES256-SHA384</td><td>ECDH/ECDSA</td><td>ECDH</td><td>AES(256)</td><td>SHA384</td></tr>
<tr><td>AES256-GCM-SHA384</td><td>RSA</td><td>RSA</td><td>AESGCM(256)</td><td>AEAD</td></tr>
<tr><td>AES256-SHA256</td><td>RSA</td><td>RSA</td><td>AES(256)</td><td>SHA256</td></tr>
<tr><td>ECDHE-RSA-AES128-GCM-SHA256</td><td>ECDH</td><td>RSA</td><td>AESGCM(128)</td><td>AEAD</td></tr>
<tr><td>ECDHE-ECDSA-AES128-GCM-SHA256</td><td>ECDH</td><td>ECDSA</td><td>AESGCM(128)</td><td>AEAD</td></tr>
<tr><td>ECDHE-RSA-AES128-SHA256</td><td>ECDH</td><td>RSA</td><td>AES(128)</td><td>SHA256</td></tr>
<tr><td>ECDHE-ECDSA-AES128-SHA256</td><td>ECDH</td><td>ECDSA</td><td>AES(128)</td><td>SHA256</td></tr>
<tr><td>ECDH-RSA-AES128-GCM-SHA256</td><td>ECDH/RSA</td><td>ECDH</td><td>AESGCM(128)</td><td>AEAD</td></tr>
<tr><td>ECDH-ECDSA-AES128-GCM-SHA256</td><td>ECDH/ECDSA</td><td>ECDH</td><td>AESGCM(128)</td><td>AEAD</td></tr>
<tr><td>ECDH-RSA-AES128-SHA256</td><td>ECDH/RSA</td><td>ECDH</td><td>AES(128)</td><td>SHA256</td></tr>
<tr><td>ECDH-ECDSA-AES128-SHA256</td><td>ECDH/ECDSA</td><td>ECDH</td><td>AES(128)</td><td>SHA256</td></tr>
<tr><td>AES128-GCM-SHA256</td><td>RSA</td><td>RSA</td><td>AESGCM(128)</td><td>AEAD</td></tr>
<tr><td>AES128-SHA256</td><td>RSA</td><td>RSA</td><td>AES(128)</td><td>SHA256</td></tr>
<tr><td>AES256-SHA</td><td>RSA</td><td>RSA</td><td>AES(256)</td><td>SHA1</td></tr>
<tr><td>AES128-SHA</td><td>RSA</td><td>RSA</td><td>AES(128)</td><td>SHA1</td></tr>
<tr><td>DES-CBC3-SHA</td><td>RSA</td><td>RSA</td><td>3DES(168)</td><td>SHA1</td></tr>
</table>

SNMPv3 with AES

TOE appliance status may be monitored from an SNMPv3 Network Management Station (other SNMP versions are supported but are disabled in the evaluated configuration). SNMPv3 is implemented using the User Security Model with ciphersuite CFB 128-AES-128 and authentication protocol HMAC-SHA-96 as defined by RFC3414 and RFC3826. The SNMPv3 protocol is used to authenticate each SNMP message, as well as provide encryption of the data – the TOE requires that authPriv (authentication and privacy) be enabled for all SNMPv3 messages. No configuration changes can be made via SNMPv3. SNMP traps generated by the TOE are excluded from the scope of evaluation.</td></tr>
</table>

SFR	Fulfillment
FTP_TRP.1	The TOE uses TLS/HTTPS to protect the Web GUI and SSH to protect the CLI. **TLS/HTTPS** The TOE supports TLS 1.2. When in FIPS Mode (evaluated configuration) the TOE supports the following ciphersuites: (see table above). **SSHv2** Remote access to the TOE CLI is protected using SSHv2 with the following allowed cryptographic parameters: • 3des-cbc, aes{128,192,256}-{cbc,ctr} • hmac-sha1, hmac-sha2-{256,512}

6.3 User Data Protection

41 The User Data Protection function implements an Access Control SFP for authorized administrators attempting to access TOE management functions and an Optimization SFP on user traffic flowing through the TOE.

Table 13: User Data Protection SFRs

SFR	Fulfillment
FDP_ACC.1	The TOE enforces an Access Control SFP on all access requests to the TOE management functions. This functionality is provided by the TOE access control mechanisms. The Access Control SFP enforces access roles based on the role of the authenticated administrator. Administrators with the monitor role have read-only access to TOE data. Administrators with the Administrator role have read-write access to TOE data. Administrators can only modify data that can be modified through one of the Management Interfaces.
FDP_ACF.1	
FDP_IFC.1	The TOE enforces an Optimization SFP on user data flowing through the TOE. The user data is network traffic. The Optimization SFP functionality is provided by the combination of Optimization and other network rules in place on the TOE (such as QoS rules or allow/deny/discard rules). The Optimization SFP enforces rules on subjects that send or receive traffic through the TOE. The rules determine what types of operations should be applied to the traffic as the traffic is flowing through the TOE based on: source IP address, destination IP address, port number, VLAN tag ID, TLS status, and application protocol. Authorized administrators define the rules that dictate how traffic flows through the TOE.
FDP_IFF.1	

6.4 Security Management

42 The Security Management function specifies the management of several aspects of the TSF, including security function behavior and security attributes. The permissions of the administrator roles are also defined here.

Table 14: Security Management SFRs

SFR	Fulfillment
FIA_UID.2 FIA_UAU.2	The TOE requires all administrators to authenticate themselves to the TOE before allowing access to the Management Interfaces. Administrators cannot perform any actions before identifying and authenticating themselves. Once an administrator provides correct authentication credentials to the TOE, the TOE will mediate access to the management functions of the TOE based on the administrator's role.
FMT_MOF.1 FMT_MSA.1	The TOE provides the capability for administrators to view, modify the behavior of, determine the behavior of, disable, and enable The Access Control SFP, the Optimization SFP, the system settings, and the administrator passwords. Administrators with the monitor role can view all settings and logs and execute the following CLI commands: • no authentication policy login max-failures • no authentication policy password expire • alarms reset-all • no service cloud-accel application * svcgroup * enable • service cloud-accel application * svcgroup * enable Monitors can also view and generate reports through the GUI. Administrators with the Administrator role have full access to modify all system settings and TSF settings. The different categories of settings that can be managed are: optimization service, host settings, advanced networking, proxy file service, port labels, reports, logging, date and time, authentication, licenses, secure vault, scheduled jobs, configuration manager, service availability, and system state.
FMT_MSA.3(a) FMT_MSA.3(b)	The TOE uses restrictive default values for the Access Control SFP. This means that the Access Control SFP rejects all non-authorized commands by default. The TOE uses permissive default values for the Optimization SFP. This means that the Optimization SFP will forward traffic through the TOE by default if optimization is not enabled or no specific rule is in place to block the traffic. The TOE allows administrators to enforce rules and settings to change the way the Optimization SFP handles traffic.
FMT_SMF.1	The TOE allows authorized administrators to manage the TSFs, security attributes, and TSF data on the TOE. Administrators manage these items through the Management Interfaces.
FMT_SMR.1 FMT_SMR.3	The TSF maintains a list of permissions for the Administrator and monitor roles. When an administrator authenticates through the Management Interfaces, the administrator is assigned one of these roles. When using the CLI, the administrators have read-only access upon initial authentication, and write privileges must be requested through the enable command.

SFR	Fulfillment
FTA_SSL.3	The TOE is capable of terminating an inactive session after a configurable time interval of administrator inactivity through the GUI, defaulting to 1000 minutes. The TOE allows administrators with appropriate permissions to modify this value to any positive integer greater than 0 and less than 43,200. The CLI can have an inactivity timeout value between 1 and 1440 minutes. Specifying a value of 0 disables session termination. When the TOE terminates an inactive session, the administrator must log in again through the main login screen.

6.5 Cryptographic Module

43 The TOE includes the following FIPS 140-2 validated cryptographic module that handles all cryptographic functions:

a) Riverbed Cryptographic Security Module v1.0, CMVP Certificate #2099. Reference: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2099.pdf
Vendor Affirmation: Riverbed affirms equivalency between the tested RiOS 8.6 and RiOS 9.1.4 and affirms that the module has been implemented in accordance with the Security Policy.

Table 15: Cryptographic Module SFRs

SFR	Fulfillment
FCS_CKM.1	The cryptographic module is capable of generating keys for Triple-DES, AES-128, AES-192, AES-256, RSA-1024, RSA-2048, DSA-1024, and HMAC (160 bits to 512 bits). The method of key generation is the SP 800-90 standard.
FCS_CKM.4	The cryptographic module is capable of destroying keys using the FIPS 140-2 zeroization method of destroying keys.
FCS_COP.1	The cryptographic module is capable of performing: • Symmetric encryption and decryption with Triple-DES and AES-128, AES-192, and AES-256 • Asymmetric encryption with RSA-2048 • Message digest with SHA-1 and SHA-2 • Random number generation with SP 800-90 DRBG

7 Rationale

7.1 Security Objectives Rationale

44 Table 16 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 16: Security Objectives Mapping

	T.MASQUERADE	T.UNAUTH	T.NO_AUDIT	T.SYSDATA	T.NACCESS	T.LATENCY	A.INSTALL	A.NETCON	A.LOCATE	A.MANAGE	A.NOEVIL	A.FIREWALL
O.AUTHENTICATE	X	X		X								
O.LOG		X	X									
O.ADMIN		X										
O.SECVAULT				X								
O.SEC_COMMS					X							
O.OPTIMIZE						X						
OE.TRAFFIC								X				
OE.FIREWALL												X
OE.MANAGE							X			X	X	
OE.PHYCAL									X			
OE.AUDIT										X		
OE.REVIEW										X		

45 Table 17 provides the justification to show that the security objectives are suitable to address the security problem.

Table 17: Suitability of Security Objectives

Element	Justification
T.MASQUERADE	O.AUTHENTICATE counters this threat by ensuring that the TOE is able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.

Element	Justification
T.UNAUTH	O.AUTHENTICATE counters this threat by ensuring that administrators are identified and authenticated prior to gaining access to TOE security data. O.LOG counters this threat by ensuring that unauthorized attempts to access the TOE are recorded. O.ADMIN counters this threat by ensuring that access to TOE security data is limited to those users with access to the management functions of the TOE.
T.NO_AUDIT	O.LOG counters this threat by ensuring that an audit trail of management events on the TOE is preserved. O.LOG ensures that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.
T.SYSDATA	O.AUTHENTICATE counters this threat by ensuring that external entities attempting to access data stored on the TOE be authenticated before that access is allowed. O.SECVAULT counters this threat by encrypting sensitive information stored in the secure vault, making it impossible for an attacker to interpret the data without the appropriate cryptographic keys and algorithms.
T.NACCESS	O.SEC_COMMS counters this threat by allowing the TOE to create a secure channel to protect information sent to a trusted external IT entity.
T.LATENCY	O.OPTIMIZE counters this threat by allowing the TOE to apply an Optimization Policy on traffic flowing through the TOE, greatly increasing the efficiency of bandwidth across a communication link.
A.INSTALL	OE.MANAGE upholds this assumption by ensuring that the TOE administrators read and follow the guidance for installation and deployment of the TOE.
A.NETCON	OE.TRAFFIC upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration to provide secure WDS.
A.LOCATE	OE.PHYCAL upholds this assumption by ensuring that the environment provides protection against physical attack.
A.MANAGE	OE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.AUDIT upholds this assumption by ensuring that administrators assigned to manage the TOE will review the audit logs on a regular basis and take the appropriate actions when breaches of security are detected.

Element	Justification
	OE.REVIEW upholds this assumption by ensuring that administrators assigned to manage the TOE will review the configuration on a regular basis to ensure that it accurately reflects the intended configuration.
A.NOEVIL	OE.MANAGE upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all administrator guidance.
A.FIREWALL	OE.FIREWALL upholds this assumption by ensuring that all ports necessary for the operation of the TOE are opened.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

46 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 18: Security Requirements Mapping

	O.AUTHENTICATE	O.LOG	O.ADMIN	O.SECVAULT	O.SEC_COMMS	O.OPTIMIZE
FAU_GEN.1		X				
FAU_SAR.1		X	X			
FAU_SAR.3		X				
FCS_CKM.1				X	X	
FCS_CKM.4				X	X	
FCS_COP.1				X	X	
FDP_ACC.1				X		
FDP_ACF.1				X		

	O.AUTHENTICATE	O.LOG	O.ADMIN	O.SECVAULT	O.SEC_COMMS	O.OPTIMIZE
FDP_IFC.1					X	X
FDP_IFF.1					X	X
FIA_UAU.2	X		X			
FIA_UID.2	X		X			
FMT_MOF.1			X			
FMT_MSA.1			X			
FMT_MSA.3(a)			X	X		
FMT_MSA.3(b)						X
FMT_SMF.1			X			
FMT_SMR.1			X			
FMT_SMR.3			X			
FPT_STM.1		X				
FTA_SSL.3	X					
FTP_ITC.1					X	
FTP_TRP.1					X	

Table 19: Suitability of SFRs

Objective	Addressed By	Rationale
O.AUTHENTICATE	FIA_UAU.2 User authentication before any action	This requirement supports O.AUTHENTICATE by requiring all TOE administrators to authenticate before any other TSF-mediated actions are performed.

Objective	Addressed By	Rationale
	FIA_UID.2 User identification before any action	This requirement supports O.ATHENTICATE by ensuring the TOE administrators are identified before any other TSF-mediated actions are performed.
	FTA_SSL.3 TSF-initiated termination	This requirement supports O.AUTHENTICATE by ensuring TOE administrators are logged off after an administrator-defined period of inactivity, ensuring that unauthenticated entities do not gain access to the TOE through an unattended session.
O.LOG	FAU_GEN.1 Audit data generation	This requirement supports O.LOG by requiring the TOE to produce audit records for the system security events and for actions caused by enforcement of the Access Control and Optimization Policies.
	FAU_SAR.1 Audit review	This requirement supports O.LOG by requiring the TOE to make the recorded audit records available for review.
	FAU_SAR.3 Selectable audit review	This requirement supports O.LOG by allowing administrators to perform searches of the audit records using a keyword string.
	FPT_STM.1 Reliable time stamps	This requirement supports O.LOG by ensuring that the TOE can provide reliable time stamps for its own use. The time stamps allow the TOE to place events in the order that they occurred.
O.ADMIN	FAU_SAR.1 Audit review	This requirement supports O.ADMIN by requiring the TOE to make the recorded audit records available for review.
	FIA_UAU.2 User authentication before any action	This requirement supports O.ADMIN by ensuring that the TOE administrators are authenticated before any other TSF-mediated actions are performed.

Objective	Addressed By	Rationale
	FIA_UID.2 User identification before any action	This requirement supports O.ADMIN by ensuring the TOE administrators are identified before any other TSF-mediated actions are performed.
	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.ADMIN by specifying which functions of the TOE can be managed, and defining which roles can manage those functions.
	FMT_MSA.1 Management of security attributes	This requirement supports O.ADMIN by allowing authorized TOE administrators to manage the TOE security attributes.
	FMT_MSA.3(a) Static attribute initialization	This requirement supports O.ADMIN. The Access Control Policy is restrictive by default, limiting access to authorized administrators only.
	FMT_SMF.1 Specification of management functions	This requirement supports O.ADMIN by specifying that the TOE supports the management functions of the TOE.
	FMT_SMR.1 Security roles	This requirement supports O.ADMIN by supporting two roles: administrator and monitor.
	FMT_SMR.3 Assuming roles	This requirement supports O.ADMIN by requiring CLI administrators to explicitly request enable privileges before being granted full administrative rights to the CLI.
O.SECVAULT	FCS_CKM.1 Cryptographic key generation	This requirement supports O.SECVAULT by requiring that cryptographic keys are generated according to an assigned standard.
	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.SECVAULT by ensuring that cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	This requirement supports O.SECVAULT by requiring cryptographic operations be performed according to the specified

Objective	Addressed By	Rationale
		algorithms with the specified key sizes.
	FDP_ACC.1 Subset access control	This requirement supports O.SECVAULT by defining the subjects, objects, and operations the Access Control Policy is based on.
	FDP_ACF.1 Security attribute based access control	This requirement supports O.SECVAULT by defining the attributes of subjects and objects that the Access Control Policy is based on.
	FMT_MSA.3(a) Static attribute initialisation	This requirement supports O.SECVAULT by specifying that the Access Control Policy shall be applied restrictively. This means that administrators attempting to authenticate with the TOE must use correct login credentials to be granted access to the TOE interfaces controlling the secure vault.
O.SEC_COMMS	FCS_CKM.1 Cryptographic key generation	This requirement supports O.SEC_COMMS by requiring that cryptographic keys are generated according to an assigned standard.
	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.SEC_COMMS by ensuring that cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	This requirement supports O.SEC_COMMS by requiring cryptographic operations be performed according to the specified algorithms with the specified key sizes.
	FDP_IFC.1 Subset information flow control	This requirement supports O.SEC_COMMS by defining the types of subjects, information, and operations for the Optimization Policy that is applied to traffic flowing through the TOE.
	FDP_IFF.1 Simple security attributes	This requirement supports O.SEC_COMMS by defining a list of attributes of subjects and

Objective	Addressed By	Rationale
		information for the Optimization Policy that is applied to traffic flowing through the TOE.
	FTP_ITC.1 Inter-TSF trusted channel	This requirement supports O.SEC_COMMS by providing a trusted channel through protected information can be exchanged securely with a remote trusted IT entity.
	FTP_TRP.1	This requirement supports O.SEC_COMMS by requiring that communication with remote administrators be secured.
O.OPTIMIZE	FDP_IFC.1 Subset information flow control	This requirement supports O.OPTIMIZE by defining the types of subjects, information, and operations for the Optimization Policy that is applied to traffic flowing through the TOE.
	FDP_IFF.1 Simple security attributes	This requirement supports O.OPTIMIZE by defining a list of attributes of subjects and information for the Optimization Policy that is applied to traffic flowing through the TOE.
	FMT_MSA.3(b) Static attribute initialization	This requirement supports O.OPTIMIZE by specifying that the Optimization Policy shall be applied permissively to traffic flowing through the TOE. This means that data that can't be optimized (because it has already been optimized or because it is encrypted by an unknown key or algorithm) will be passed through the TOE unmodified.

Table 20: Dependencies

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FAU_SAR.3	FAU_SAR.1	Met

SFR	Dependency	Rationale
FCS_CKM.1	FCS_CKM.4	Met
	FCS_COP.1	Met
FCS_CKM.4	FCS_CKM.1	Met
FCS_COP.1	FCS_CKM.4	Met
	FCS_CKM.1	Met
FDP_ACC.1	FDP_ACF.1	Met
FDP_ACF.1	FMT_MSA.3(a)	Met
	FDP_ACC.1	Met
FDP_IFC.1	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met
	FMT_MSA.3(b)	Met
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2
FIA_UID.2	None	Met
FMT_MOF.1	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.1	FDP_ACC.1	Met
	FDP_IFC.1	Met
	FMT_SMF.1	Met
	FMT_SMR.1	Met
FMT_MSA.3(a)	FMT_SMR.1	Met
	FMT_MSA.1	Met
FMT_MSA.3(b)	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	Met
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2

SFR	Dependency	Rationale
FMT_SMR.3	FMT_SMR.1	Met
FPT_STM.1	None	Met
FTA_SSL.3	None	Met
FTP_ITC.1	None	Met
FTP_TRP.1	None	Met

7.3 TOE Summary Specification Rationale

47 Table 21 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 21: Map of SFRs to TSS Security Functions

	Security Audit	Secure Communications	User Data Protection	Secure Management	Cryptographic Module
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.3	X				
FCS_CKM.1					X
FCS_CKM.4					X
FCS_COP.1					X
FDP_ACC.1			X		
FDP_ACF.1			X		
FDP_IFC.1			X		
FDP_IFF.1			X		
FIA_UAU.2				X	

	Security Audit	Secure Communications	User Data Protection	Secure Management	Cryptographic Module
FIA_UID.2				X	
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.3(a)				X	
FMT_MSA.3(b)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FMT_SMR.3				X	
FPT_STM.1	X				
FTA_SSL.3				X	
FTP_ITC.1		X			
FTP_TRP.1		X			