Riverbed Technology, Inc.
Steelhead Appliance v4.1

Security Target

Evaluation Assurance Level: 4+
Document Version: 0.8

Prepared for:

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Phone: (415) 247-8801

http://www.riverbed.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2008-09-17	Greg Milliken	Initial draft.
0.2	2008-12-23	Greg Milliken	Addressed verdicts for OR 1 and OR 2.
0.3	2009-07-02	Greg Milliken	Changes to address OR 4 and CB OR 1, plus additional scheme requirements.
0.4	2009-07-17	Greg Milliken	Addressed additional lab verdicts.
0.5	2009-08-13	Greg Milliken	Changes to address OR 4 and removed 5010 from the list of products being evaluated.
0.6	2009-10-19	Greg Milliken	Changes to address OR-7.
0.7	2009-12-15	Greg Milliken	Excluded Proxy File Service from the evaluation.
0.8	2010-06-11	Greg Milliken	Various end-of-evaluation changes.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Riverbed Steelhead Appliance v4.1, and will hereafter be referred to as the TOE or Steelhead Appliance throughout this document. The TOE is a network appliance, Operating System (OS), and application software that provide WAN optimization and Quality of Service (QoS) mechanisms. The TOE can also protect traffic that the TOE is exchanging with another instance of the TOE via Transport Layer Security (TLS) protection. Optimization and protection are provided through the Riverbed Optimization System (RiOS).

The appliance models being evaluated are the Steelhead Appliance model numbers 520, 1020, 1520, 2020, 3020, 3520, 5520, 6020, 250, 550, 1050, 2050, 5050, and 6050. The models differ in size, bandwidth capacity, number of Transmission Control Protocol (TCP) connections that can be optimized[1], disk storage size, data store capacity, and several other features (such as Redundant Array of Independent Disks (RAID) and hot swappable disks). The appliances that support RAID ship with the RAID preconfigured. Two-disk systems use RAID 0, and systems with more than two disks use RAID 10.

1.1 Purpose

This ST provides a mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:

- Security Target 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.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims.
- Security Problem Definition (Section 3) – Describes the threats, 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 Definition (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 Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

[1] The TOE does not optimize User Datagram Protocol (UDP) traffic, but does apply QoS rules to UDP traffic.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	Riverbed Technology, Inc. Steelhead Appliance v4.1 Security Target
ST Version	Version 0.8
ST Author	Corsec Security, Inc. Greg Milliken and Amy Nicewick
ST Publication Date	2010/06/11
TOE Reference	Riverbed Steelhead Appliance v4.1 fips-b
Keywords	WAN bandwidth optimization, traffic protection, TLS, Riverbed, Steelhead Appliances, transparent, application acceleration, IT Consolidation, faster WAN backup, QoS, WAN optimization.

1.3 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 a network appliance, OS, and application software (RiOS) that provide WAN optimization. The TOE type is WAN Optimization. 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 Appliance 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 Appliance at the other end of the WAN.

The TOE can use TLS to protect network data passing through the TOE and across a WAN. The TOE uses TLS to protect Scalable Data Referencing (SDR) references and other sensitive TOE data before the data and references leave the TOE. SDR is a proprietary optimization algorithm. TLS is implemented by a Federal Information Processing Standard (FIPS) 140-2 validated cryptography module based on a modified version of OpenSSL.

Steelhead appliances accelerate TLS traffic by removing TLS protection, optimizing the packets, and then replacing TLS protection before sending the traffic across the WAN. These optimizations are bi-directional, ensuring that all traffic is protected from origination to destination in both directions.

The TOE provides QoS, which allows administrators to control the prioritization of different types of network traffic and to ensure that Steelhead Appliances give certain network traffic priority over other types of traffic. In addition to standard QoS services, the Steelhead Appliance 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.

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*.

The Steelhead Appliance's management interfaces are role-based and are restricted to authorized administrators. The Steelhead Appliance'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 Appliance is transparent to end users.

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

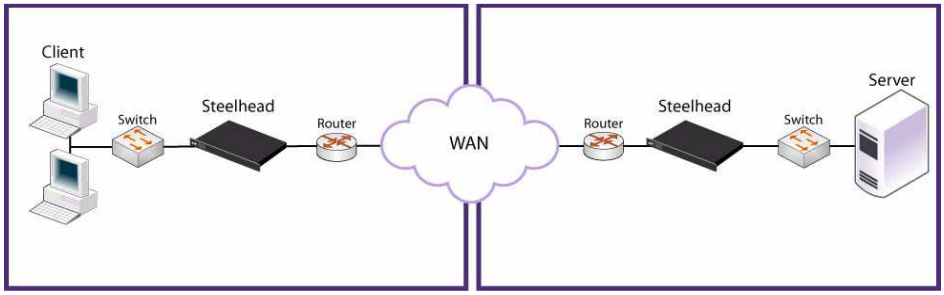

Figure 1 – Physical In-Path Deployment Configuration of the TOE

The Steelhead Appliance can provide the following services:

- apply optimizations to network traffic,
- apply TLS protection to optimized traffic,
- guarantee a minimum bandwidth to latency-sensitive application traffic.

1.3.1 Steelhead Appliance v4.1 Concepts

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

1.3.1.1 Scalable Data Referencing

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 Appliance across the WAN. If the TOE must transmit the same byte sequence again, the TOE sends the integer reference instead. The peer Steelhead Appliance 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.

When the TOE first sends data across a network, all data and labels are new and are sent to the Steelhead Appliance 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.

One use of the Steelhead Appliance 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.

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

1.3.1.2 Virtual Window Expansion

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 in each round-trip.

1.3.1.3 Transaction Prediction

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.

1.3.2 TOE Environment

The TOE is intended to be deployed in a physically secure cabinet, room or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is meant to optimize and protect data traveling across a WAN. For the TOE to operate correctly, all optimized and protected traffic must traverse the TOE, and the TOE must be connected to the network in one of the appropriate deployment configurations. The TOE environment is required to provide for this configuration.

In order for traffic to be properly optimized and protected, a peer Steelhead Appliance must be present at the opposite end of the WAN. This peer Steelhead Appliance is not included within the TOE boundary, and is part of the TOE environment.

The TOE is managed through a CLI and a web-based GUI. Administrators must access these interfaces from a trusted workstation that supports Secure Shell (SSH) and a web browser that supports Javascript and cookies. The CLI and web GUI are part of the TOE. The administrator accesses these through an SSH client and a standard web browser. The administrator workstation is part of the TOE environment.

1.4 TOE Description

This section will primarily address the physical and logical components of the TOE included in the evaluation.

1.4.1 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 an operating system and software application that run on the Steelhead Appliance hardware (the hardware is also part of the TOE). The operating system is the CentOS 4 distribution of Linux. The hardware varies by model. RAID is part of the TOE for models that include RAID configurations. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- The TOE,
- A peer Steelhead Appliance installed at the other end of the network,

- Application clients,
- Application servers.

The TOE hardware appliances are differentiated as follows:

Table 2 – Hardware Specifications for x20 Models

Model Number	520	1020	1520	2020	3020	3520	5520	6020
Profile	1U	1U	1U	1U	3U	3U	3U	3U
WAN Capacity	1 Mbps	2 Mbps	4 Mbps	10 Mbps	20 Mbps	45 Mbps	155 Mbps	310 Mbps
WAN Capacity (High-speed)	1 Mbps	2 Mbps	4 Mbps	10 Mbps	20 Mbps	45 Mbps	800 Mbps	800 Mbps
Optimized TCP Connections	330	700	1100	2000	3500	6000	15000	40000
Total Disk	250 GB	250 GB	250 GB	500 GB	1 TB	1.5 TB	1.5 TB	7 TB
Data Store Capacity	80 GB	80 GB	80 GB	150 GB	250 GB	512 GB	700 GB	3.4 TB
RAID	No	No	No	No	Yes	Yes	Yes	Yes
Front Swappable Disks	No	No	No	No	Yes	Yes	Yes	Yes
RAM	2 GB	2 GB	2 GB	4 GB	6 GB	6 GB	8 GB	16 GB
Slots	1	1	1	1	3	3	3	3
Max # of Bypass Ports	6	6	6	6	16	16	16	16

Table 3 – Hardware Specifications for x50 Models

Model Number	250	550	1050	2050	5050	6050
Profile	Desktop	Desktop	1U	1U	3U	3U
Optimized WAN Capacity	1-2 Mbps	2-4 Mbps	8-20 Mbps	45 Mbps	90-155 Mbps	310 Mbps
Optimized TCP Connections	30-200	300-600	800-2300	2500-6000	7500-18000	50000
Raw Capacity	120 GB	160 GB	250-500 GB	1 TB	2-3 TB	8 TB
Data Store Capacity	40 GB	80 GB	100-200 GB	400 GB	600-800 GB	3.5 TB
RSP Partition	55 GB	55 GB	100-200 GB	75 GB	100-150 GB	150 GB
Storage Fault Tolerance	No	No	Optional RAID	RAID	RAID	RAID
Front Swappable Drives	No	No	1-2 default 4 if RAID	4	8-12	16
RAM	1 GB	2 GB	2-4 GB	6 GB	8 GB	24 GB
Expansion Slots (PCI-e)	No	No	1	1	4	4
Onboard Bypass ports (Copper)	2	2	4	4	4	4
Max # of Bypass Ports	2	2	8	8	20	20

Figure 2 below shows the typical configuration of the Steelhead Appliance. Clients and servers on a Local Area Network (LAN) communicate through the Steelhead Appliance across a WAN to other clients and servers. Unlabeled lines represent internal connections. Communications between the TOE Software and TOE OS are represented in terms of the flow of application data.

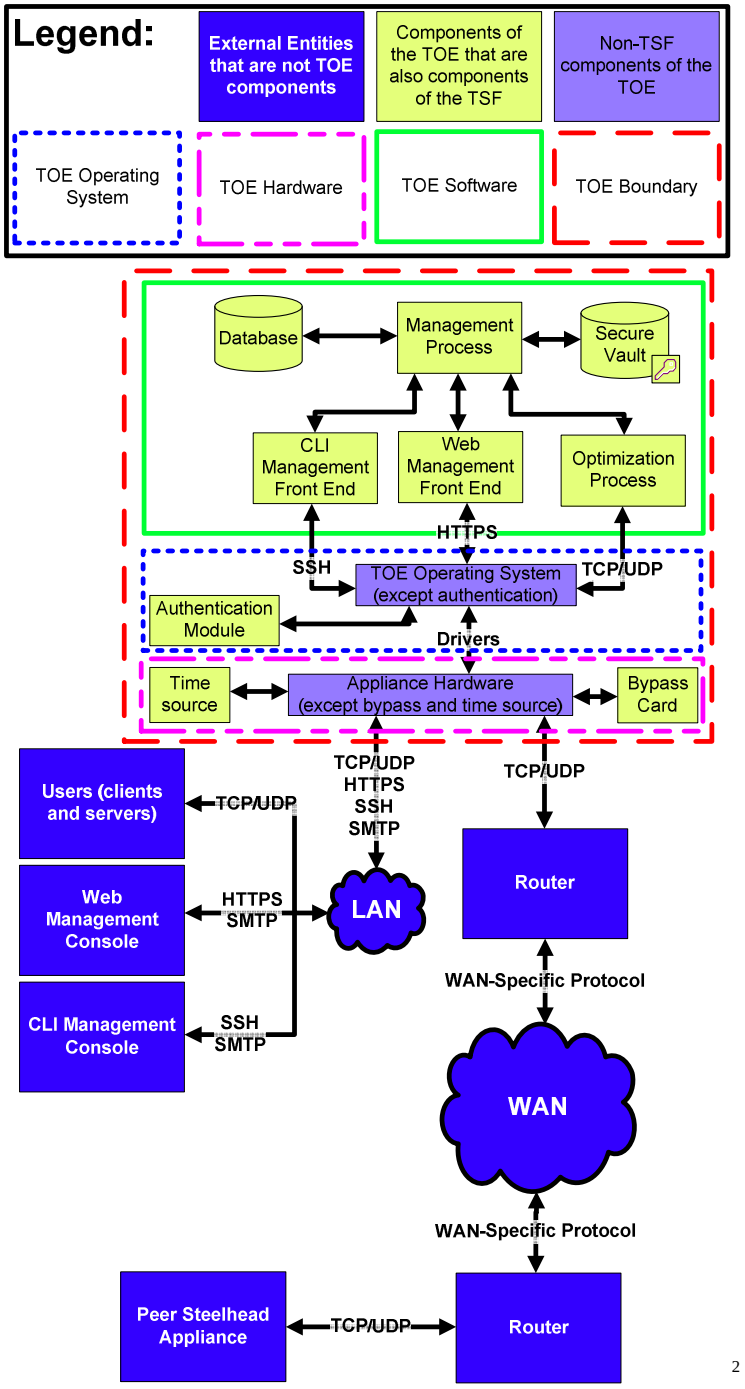

Figure 2 – Physical TOE Boundary

[2] The Web Management Front End pictured in the diagram provides the web GUI functionality on the TOE. The administrator accesses the web interface via a web browser on the web management console.

1.4.2 Steelhead Appliance TOE Components

The following Steelhead Appliance components are part of the TOE and the TOE Security Function (TSF):

- Management Interfaces
    - 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).
        - Administrators can manage optimization services, host settings, advanced networking configurations, 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.
        - Administration supports two roles: read-only (monitor) and read-write (admin). Only the admin role is allowed to change configuration settings on the appliance. The monitor role is limited to viewing the system configuration and reports.
    - 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.
        - The administrator is given monitor permissions upon first authenticating through the CLI. Administrators with read-only permissions are limited to viewing the system configuration. The administrator must explicitly request the admin role by entering the enable and configure commands. Only administrators who assume the admin role can configure the TOE through the CLI.
- Managers
    - 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:
        - 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.
        - Configuration manager – handles all configuration changes, actions taken on the appliance, and any events that occur that require the Steelhead Appliance to perform processing.
- Services
    - 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.
    - 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.

- 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.

- Other services – The TOE provides services to accommodate the Netflow protocol for sending internet protocol traffic collected by the TOE during its normal operation. The TOE provides administrators with the ability to securely copy configuration files and log files from the TOE to an administrator workstation.

In addition to the components listed above, the Steelhead Appliance includes the following optional interfaces to enhance the security functionality of the system:

- Simple Mail Transfer Protcol (SMTP) Interface is used by the TOE to email administrators if configured to do so. Possible reasons the TOE might send an email are for system resource overutilization alarms or if the secure vault needs to be unlocked.

1.4.2.1 Users and Administrators

A Steelhead Appliance 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.

A Steelhead Appliance administrator is anyone who connects to one of the TOE Management Interfaces who is authorized to manage the TOE. Administrators are divided into two roles:

- Admin: An administrator that has read-write access to all TOE settings and data,
- Monitor: An administrator that has read-only access to TOE settings and data.

These roles are the same for both Management Interfaces. For CLI users to attain read-write privileges, they must enter the enable command while logged in as the Admin role.

1.4.2.2 Data

The TOE works with four kinds of data:

- 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 Functional 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.
- 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.
- 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.
- 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.

All TSF and system data resides within the local database or in configuration files on the local file system.

1.4.3 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted channels

1.4.3.1 Security Audit

The Steelhead Appliance provides functionality for generation and viewing of audit records. As administrators manage and configure the Steelhead Appliance, the Steelhead Appliance tracks their activities by recording audit records into the logs. The Steelhead Appliance records all security-relevant configuration settings and changes to ensure accountability of the administrators' actions.

The Steelhead Appliance admin can view all audit information from the audit logs, as well as search the audit records.

1.4.3.2 Cryptographic Support

The Steelhead Appliance provides TLSv1 protection on a secure channel between two or more Steelhead Appliances. The secure channel allows the Steelhead Appliances to pass sensitive information to each other while addressing the threats of unauthorized disclosure and modification. The Steelhead Appliance generates and destroys keys securely. A FIPS 140-2 validated cryptographic module performs all cryptographic operations. Cryptographic modules are divided among the following appliances:

Table 4 – Cryptographic Module FIPS 140-2 Certificate Numbers by Appliance Grouping

Appliances	Certificate Number
520, 1020, 1520, 2020	Pending
3020, 3520, 5520, 6020	Pending
250, 550	Pending
1050, 2050	Pending
5050, 6050	Pending

1.4.3.3 User Data Protection

The Steelhead Appliance implements functionality for controlling access and traffic information flows. Access to the Steelhead Appliance requires an authorized username and role. Access to the management functions on the Steelhead Appliance is partitioned according to the administrator's role. The Steelhead Appliance enforces an Optimization Policy that applies a set of rules to TCP traffic passing through the Steelhead Appliance. 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 Appliance.

The TOE has a bypass mode that it enters when an error occurs on the TOE. While in bypass mode, the TOE forwards traffic without processing or applying rules to the traffic. Bypass mode is implemented in the TOE hardware in the form of a bypass card.

1.4.3.4 Identification and Authentication

The Steelhead Appliance provides functionality to allow administrators to verify their claimed identity. This ensures that only legitimate administrators of the Steelhead Appliance can gain access to the configuration and management settings. The OS uses a pluggable authentication module to handle authentication for the system.

1.4.3.5 Security Management

The Steelhead Appliance provides functionality that allows administrators to manage the Steelhead Appliance Security Function, including security function behavior and security attributes. The Security Management function specifies the roles defined for managing the Steelhead Appliance and how administrators assume the roles.

1.4.3.6 Protection of the TSF

The Steelhead Appliance provides reliable time stamps that it will use to record the accurate time for audit records. The operating system retrieves time stamps from a hardware clock.

1.4.3.7 TOE Access

The Steelhead Appliance 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 Appliance management functions through an unattended session.

1.4.3.8 Trusted channels

The Steelhead Appliance can open a trusted channel between itself and another Steelhead Appliance for intercepted TLS-encrypted traffic. The Steelhead Appliance protects the channel with TLSv1. The TLS cryptographic operations used to protect traffic on the trusted channel are performed by a FIPS 140-2 validated cryptographic module. If the TOE is in Bypass Mode, this functionality is not available.

1.4.4 Bypass Mode

Riverbed installs a bypass card in every Steelhead Appliance to prevent a single point of failure. If the Steelhead Appliance enters an unstable state, the Steelhead Appliance goes into Bypass Mode. While in Bypass Mode, the Steelhead Appliance does not perform any processing on traffic. The TOE cannot optimize or block regular or TLS traffic while the TOE is in Bypass Mode, but traffic does pass through the TOE without modification. Once an administrator removes the conditions that caused the unstable state, the Steelhead Appliance resumes normal operation.

1.4.5 Physical and Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

The Riverbed Steelhead Appliance contains software and hardware components that are included with the product but are not part of the evaluated configuration. These components are not available in FIPS mode or are only used during installation. These are not identified in Figure 2.

These components are:

- Hypertext Transfer Protocol (HTTP) Management,
- Telnet Server Management

Additionally, the product guidance and marketing material mentions functionality that requires third-party products in order to be utilized. Some of the supported third-party products lack security features that enable them to be used in a secure fashion.

These components are:

- SNMP v1 and v2c,
- Remote syslog,
- Message Digest 5 (MD5) used in Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System + (TACACS+) implementations,
- File Transfer Protocol, and
- Proxy File Service.

Excluded functionality is either disabled by default (as indicated), or can be disabled with the listed CLI commands:

- HTTP – no web http enable
- Telnet – disabled by default
- SNMP v1 and v2c – no snmp-server enable
- Remote syslog – disabled by default
- Proxy File Service – disabled by default

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 5 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2008/07/02 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 4+ augmented with Flaw Remediation (ALC_FLR.1)

3 Security Problem Definition

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:

- 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 assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE administrators: 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 and parameters, and no physical access to the TOE.
- TOE administrators: 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 and parameters, and physical access to the TOE. (TOE administrators are, however, assumed not to be willfully hostile to the TOE).

Threat agents are assumed to have an attack potential of enhanced-basic. The IT assets requiring protection are the user data, TSF data, system data, and management data saved on or transitioning through the TOE and the hosts on the protected network, as well as WAN bandwidth. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 – Security Objectives.

The following threats are applicable:

Table 6 – Threats

Name	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 or administrator 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

There are no Organizational Security Policies (OSPs) 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 7 – Assumptions

Name	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 WAN optimization.
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.
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. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate.
A.NTP	The TOE Environment should provide protection to ensure that NTP information communicated from an NTP source to the TOE cannot be modified by an attacker.
A.ADM_DATA	The TOE Environment should provide protection to ensure that log data, usage statistics, configuration data, and email messages communicated between the TOE and an administrator workstation cannot be viewed or modified by an attacker.
A.NETFLOW	It is assumed that the Netflow collector and administrator workstation are located within the same controlled access facility.
A.EXT_AUTH	It is assumed that the TOE and RADIUS or TACACS+ authentication servers are located within the same controlled access facility.

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 8 – Security Objectives for the TOE

Name	Description
O.AUTHENTICATE	The TOE must require administrators to authenticate before gaining access to the TOE interfaces.
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.TLS	The TOE must use TLS to protect the confidentiality of traffic while it is being transmitted between the TOE and another trusted IT product as specified by the Optimization Policy.
O.OPTIMIZE	The TOE must optimize traffic flowing through the TOE according to the rules defined in the Optimization Policy.

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 9 – IT Security Objectives

Name	Description
OE.FIREWALL	The Firewall must have all ports needed for proper operations of the TOE opened.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

OE.NTP	NTP servers providing time information to the TOE should be on the local network and inaccessible to non-administrators.
OE.ADM_DATA	The TOE Environment must provide appropriate mechanisms to protect the transfer of log data, usage statistics, configuration data, and email messages between the TOE and an administrator workstation.
OE.NETFLOW	Administrator workstations must be within the same controlled access facility as the Netflow collector.
OE.EXT_AUTH	The TOE must be within the same controlled access facility as the RADIUS and TACACS+ authentication servers.

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 10 – Non-IT Security Objectives

Name	Description
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

5 Extended Components Definition

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

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

Table 11 – Extended TOE Security Functional Requirements

Name	Description
FTC_ITC.1 (EXP)	**Inter-TSF trusted communications channel**

5.1.1 Class FTC: Trusted channels

Trusted channels involves trusted communications channels between two endpoints where communications may be initiated by either side of the channel.

The FTC: Trusted channels class was modeled after the CC FTP: Trusted Path/Channels class. The extended family and related components for FTC_ITC: Inter-TSF trusted communications channel were modeled after the CC family and related components for FTC_ITC: Inter-TSF trusted channel.

Figure 3 – FTC: Trusted channels

5.1.1.1 FTC_ITC: Inter-TSF trusted communications channel

Family Behaviour

This family defines the requirements for setting up a trusted channel for secure communications between the TOE and another trusted IT device.

Component Leveling

Figure 4 – FTC_ITC: Inter-TSF trusted communications channel family deomposition

FTC_ITC.1: Inter-TSF trusted communications channel requires that the TSF provide a trusted communication channel between itself and another trusted IT product.

Management: FTC_ITC.1 (EXP)

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

a) Configuring the actions that require trusted channel, if supported.

Audit: FTC_ITC.1 (EXP)

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

a) Minimal: Failure of the trusted channel functions.

b) Minimal: Identification of the initiator and target of failed trusted channel functions.

c) Basic: All attempted uses of the trusted channel functions.

d) Basic: Identification of the initiator and target of all trusted channel functions.

FTC_ITC.1 (EXP) Inter-TSF trusted communications channel

Hierarchical to: No other components.

FTC_ITC.1.1 (EXP)

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.

FTC_ITC.1.2 (EXP)

The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTC_ITC.1.3 (EXP)

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

FTC_ITC.1.4 (EXP)

The TSF shall not provide the trusted channel while the TOE is in Bypass Mode.

Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 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 Parts 2 and 3 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 italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

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

Table 12 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_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	✓	✓		
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		✓
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		✓		
FTC_ITC.1 (EXP)	Inter-TSF trusted communications channel	✓	✓		

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:

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [Login, logout, change passwords, system failure].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*the admin role*] 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~~ **administrator** to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

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

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 cryptographic keys in accordance with a specified cryptographic key generation algorithm [*the key generation algorithms listed in the Key Generation Method column of Table 13*] and specified cryptographic key sizes [*the key sizes listed in the Cryptographic Key Size column of Table 13*] that meet the following: [*the standards listed in the Standards column of Table 13*].

Table 13 – Cryptographic Key Generation Standards

Key Generation Method	Padding Scheme	Cryptographic Key Size	Standards
X9.31	None (a pseudo-random function is used repeatedly to generate a sufficient sized key)	All key sizes specified in the Key Sizes (bits) column of Table 14 below.	X9.31 (cert #595)

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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*].

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 14*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 14*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 14*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 14*].

Table 14 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES (3-Key) Electronic Codebook (ECB), Cipher Block Chaining (CBC)	168	FIPS 46-3 (cert #792)
	AES[3] (128, 192, 256) ECB and CBC	128, 192, 256	FIPS-197 (cert #1044)
Asymmetric encryption and decryption	RSA[4] (up to 2048 bits)	1024, 2048	FIPS 186-2 for Sign/Verify (cert #498)
Message Digest	SHA[5]-1[6]	N/A	FIPS 180-2 (cert #994)
Message Authentication	HMAC[7]	160-512	FIPS-198 (cert #586)
Random Number Generation	ANSI[8] X9.31 RNG[9]	N/A[10]	X9.31 (cert #595)

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

[3] AES – Advanced Encryption Standard

[4] RSA – Rivest, Shamir, Adelman (encryption algorithm)

[5] SHA – Secure Hashing Algorithm

[6] SHA-1 has been deemed by the Candian government to be unsuitable for use in Protected C data or higher environments as of January 1, 2009. SHA-1 will be classified as unsuitable for Protected A and B or higher environments as of January 1, 2011. Please see Communications Security Establishment Canada (CSEC) Alert 11D for more information.

[7] HMAC – Hashed Message Authentication Code

[8] ANSI – American National Standards Institute

[9] RNG –Random Number Generator

[10] Randon number generators do not use keys.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

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

].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *Role*
2. *Identification (ID)*

and Object attributes:

1. *Permissions assigned to objects*
2. *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:

[

1. If a subject with the admin role requests access to an object then access is granted.
2. If a subject with the monitor role requests read access to an object other than system logs, then access is granted.
3. 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~~ **no** additional rules.~~: [rules, based on security attributes, that explicitly authorize access of subjects to objects]~~.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on **no additional access control rules** ~~the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]~~.

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Optimization SFP*] on

1. SUBJECTS: external IT entities that send or receive information through the TOE,
2. INFORMATION: traffic flowing through the TOE, and
3. OPERATIONS: Optimize, pass-through, deny, discard].

Dependencies: **FDP_IFF.1 Simple security attributes**

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*Optimization SFP*] based on the following types of subject and information security attributes:

[

Subject (external IT entities that send or receive information through the TOE) Attributes:

A. *IP[11] address*

Information Attributes:

1. *Source IP address*
2. *Destination IP address*
3. *Port number*
4. *Virtual Local Area Network (VLAN) tag ID*
5. *TLS status*
6. *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: [A*pply the appropriate operation based on the information attributes evaluated against the policy rules*].

FDP_IFF.1.3

The TSF shall enforce **no additional information flow control rules** ~~the [assignment: additional information flow control SFP 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 **no additional rules** ~~the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]~~.

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

[11] IP – Internet Protocol

6.2.4 Class FIA: Identification and Authentication

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~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

Dependencies: FIA_UID.1 Timing of identification

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~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [**perform the actions listed under Permissions in Table 15 below**] the functions [**listed under Permissions in Table 15 below**] to [**the roles specified under Role in Table 15 below**].

Table 15 – Management of Security Functions Behaviour

Role	Permissions
Monitor	View all settings.
Admin	View all settings and logs, determine the behaviour of, disable, enable, modify the behaviour of system settings, the Access Control SFP, and the Optimization SFP, modify administrator passwords.

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Access Control SFP, Optimization SFP*] to restrict the ability to [*manage*] the security attributes [*attributes relating to optimization service, host settings, advanced networking, port labels, reports, logging, date and time, authentication, licenses, secure vault, scheduled jobs, configuration manager, service availability, system state*] to [*authorized administrators*].

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.3(a) Static attribute initialisation

Hierarchical to: No other components.

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.

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

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

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.

Dependencies: FMT_MSA.1 Management of security attributes
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 security functions and management of security attributes*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*monitor*, *admin*].

FMT_SMR.1.2

The TSF shall be able to associate ~~users~~ **administrators** with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

FMT_SMR.3.1

The TSF shall require an explicit request to assume the following roles: [*admin role from the CLI in user mode*].

Dependencies: FMT_SMR.1 Security roles

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Dependencies: No dependencies

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

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*].

Dependencies: No dependencies

6.2.8 Class FTP: Trusted channels

FTC_ITC.1 (EXP) Inter-TSF trusted communications channel

Hierarchical to: No other components.

FTC_ITC.1.1 (EXP)

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.

FTC_ITC.1.2 (EXP)

The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTC_ITC.1.3 (EXP)

The TSF shall initiate communication via the trusted channel for [*communications protected with TLS*].

FTC_ITC.1.4 (EXP)

The TSF shall not provide the trusted channel while the TOE is in Bypass Mode.

Dependencies: No dependencies

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 EAL 4 augmented with ALC_FLR.1. Table 16 – Assurance Requirements summarizes the requirements.

Table 16 – Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM[12] Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.1 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular 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_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample

[12] CM – Configuration Management

Assurance Requirements	
	ATE_DPT.2 Testing: Security Enforcing Modules
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused 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 17 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	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
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FMT_SMR.3	Assuming roles

Protection of the TSF	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted channels	FTC_ITC.1 (EXP)	Inter-TSF trusted communications channel

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into logs. The TOE records user connections that travel through the TOE as well. All security-relevant configuration settings, changes, and activities are recorded to ensure accountability of the administrator's or user's actions (for example if users attempt to misuse network protocols).

FAU_GEN.1:

The TOE has the ability to generate audit records for startup and shutdown of the audit function. The TOE logs messages from startup to shutdown. The TOE can generate records for other management and system events, such as changes to the system settings. 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. Audit records are generated by the various TOE components where the event occurs. The TOE provides reliable time stamps so that the TOE can accurately record the time each event occurred.

FAU_SAR.1, FAU_SAR.3:

The Steelhead Appliance GUI provides a means to view audit records stored on the TOE, and is part of the TOE[13]. All administrators with the admin role 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.

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

7.1.2 Cryptographic Support

The TOE provides TLS functionality for secure communications between the TOE and a peer Steelhead Appliance. TLS provides encryption of information being passed along a secure link. The TOE supports TLSv1. The TOE includes a FIPS 140-2 validated cryptographic module that handles all cryptographic functions.

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 X9.31 standard.

FCS_CKM.4:

[13] The web browser used to view the web GUI and the SSH client used to communicate with the CLI are not part of the TOE.

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-1024 and RSA-2048,
- Digital signature with DSA-1024,
- message digest with SHA-1,
- random number generation with X9.31.

Triple-DES can be used as an optional cipher choice during TLS communications. AES is used for TLS, the encrypted secure vault file system, and encrypting the SDR data. RSA is used for key exchange during TLS and signature verification of X.509 certificates. DSA is present in the cryptographic library; however, DSA is not currently used in the evaluated configuration of the TOE. SHA-1 is used for certificate hashing. SHA-1 is also used in HMAC to compute TLS keys. HMAC is used to check TLS message data integrity, and is part of the function used to generate TLS keys. ANSI X9.31 is used to generate random numbers for TLS and key generation.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 User Data Protection

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.

FDP_ACC.1, FDP_ACF.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 configuration data. Administrators with the admin role have read-write access to TOE data. Administrators can only modify data that can be modified through one of the Management Interfaces.

FDP_IFC.1, FDP_IFF.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.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1.

7.1.4 Identification and Authentication

The Identification and Authentication function provides functionality for the TOE to verify a claimed administrator identity. This ensures that the administrator has the appropriate privileges associated with the assigned role. Only authenticated administrators will be allowed access to the TOE and TOE security functions. Administrators must be identified and authenticated prior to performing any other TSF-mediated actions on the TOE.

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.

TOE Security Functional Requirements Satisfied: FIA_UID.2, FIA_UAU.2.

7.1.5 Security Management

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.

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 only view all settings. Monitors can also view and generate reports through the GUI. Administrators with the admin 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, 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 admin and monitor roles. When an administrator authenticates through the Management Interfaces, the administrator is assigned one of these roles. When using the CLI, the administrator is assigned the admin or monitor role upon initial authentication, and the admin role must requested read-write privileges by entering the enable and configure commands.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3(a), FMT_MSA.3(b), FMT_SMF.1, FMT_SMR.1, FMT_SMR.3.

7.1.6 Protection of the TSF

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.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.7 TOE Access

The TOE Access function controls the termination of an administrator's session. TOE Access provides TSF-initiated termination of an interactive session. The administrator must log in again to gain access to the TOE management functions.

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.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

7.1.8 Trusted channels

The Trusted channels function guarantees a secure channel that the TOE can use to communicate with a trusted external IT entity. Likewise, the external entity can initiate communications to the TOE via this secure channel. The TOE supports a secure channel to a peer Steelhead Appliance.

FTC_ITC.1 (EXP):

The TOE is capable of protecting the traffic exchanged between the TOE and a trusted peer Steelhead Appliance with TLS. Both the TOE and the peer Steelhead Appliance may initiate communication of optimized TLS traffic on the trusted channel as traffic moves in both directions across the WAN. If the customer wishes to optimize TLS traffic, administrators can configure the TOE to allow optimization of TLS traffic. When a client or server initiates TLS protected communications, the TOE will break the TLS path into three parts: client to Steelhead, Steelhead to Steelhead, and Steelhead to server. This way, TLS traffic is still protected end-to-end, but the Steelhead Appliance can optimize the protected traffic.

If the TOE enters Bypass Mode, then the encrypted tunnel functionality is unavailable until the TOE leaves Bypass Mode.

TOE Security Functional Requirements Satisfied: FTC_ITC.1 (EXP).

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 Revision 2. There are no extended SFRs contained within this ST.

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate that the mappings between the threats, polices, and assumptions to the security objectives is 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 18 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	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.
T.UNAUTH A user or administrator may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	O.AUTHENTICATE counters this threat by ensuring that administrators are identified and authenticated prior to gaining access to TOE security data.
	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.LOG counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	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.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 An attacker may perform security-relevant operations on the TOE without being held accountable for it.	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	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.

	record events in the correct order in which they occurred.	
T.SYSDATA An attacker who is not a TOE administrator could access and interpret TSF data stored on the TOE in the secure vault.	O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	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 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.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 An attacker may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.	O.TLS The TOE must use TLS to protect the confidentiality of traffic while it is being transmitted between the TOE and another trusted IT product as specified by the Optimization Policy.	O.TLS counters this threat by allowing the TOE to create a secure channel by adding TLS protection to information sent to a trusted 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.	O.OPTIMIZE The TOE must optimize traffic flowing through the TOE according to the rules defined in the Optimization Policy.	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.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 19 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
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.	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.MANAGE upholds this assumption by ensuring that the TOE administrators read and follow the guidance for installation and deployment of the TOE.

A.NETCON It is assumed that the TOE environment provides the network connectivity required to allow the TOE to provide secure WAN optimization.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration to provide secure WAN optimization.
A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.	OE.PHYCAL Those responsible for the TOE must ensure that the TOE is protected from any physical attack.	OE.PHYCAL upholds this assumption by ensuring that the environment provides protection against physical attack.
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.	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.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 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.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.
	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	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 It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	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.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 It is assumed that all ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate.	OE.FIREWALL The Firewall must have all ports needed for proper operations of the TOE opened.	OE.FIREWALL upholds this assumption by ensuring that all ports necessary for the operation of the TOE are opened.
A.NTP The TOE Environment should provide protection to ensure that NTP information communicated from an NTP source to the TOE cannot be modified by an attacker.	OE.NTP NTP servers providing time information to the TOE should be on the local network and inaccessible to non-administrators.	OE.NTP upholds this assumption by ensuring that NTP information remains on the local protected network.
A.ADM_DATA The TOE Environment should provide protection to ensure that log data, usage statistics, configuration data, and email messages communicated between the TOE and an administrator workstation cannot be viewed or modified by an attacker.	OE.ADM_DATA The TOE Environment must provide appropriate mechanisms to protect the transfer of log data, usage statistics, and configuration data between the TOE and an administrator workstation.	OE.ADM_DATA upholds this assumption by ensuring that the Environment provides adequate protection for sensitive data being transferred between the TOE and an administrator workstation.
A.NETFLOW It is assumed that the Netflow collector and administrator workstation are located within the same controlled access facility.	OE.NETFLOW Administrator workstations must be within the same controlled access facility as the Netflow collector.	OE.NETFLOW upholds this assumption by ensuring that the administrator workstation and Netflow collector are located within the same controlled access facility.
A.EXT_AUTH It is assumed that the TOE and RADIUS or TACACS+ authentication servers are located within the same controlled access facility.	OE.EXT_AUTH The TOE must be within the same controlled access facility as the RADIUS and TACACS+ authentication servers.	OE.EXT_AUTH upholds this assumption by ensuring that the TOE and RADIUS/TACACS+ authentication servers are located within the same controlled access facility.

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

8.3 Rationale for Extended Security Functional Requirements

A family of FTP requirements was created to specifically address the way the TOE handles trusted channel communications while in Bypass Mode. The trusted channels family of the CC (FTP) was used as a model for creating the requirement. The requirement has no dependencies since the stated requirement embodies all the necessary security functions. The requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs 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 20 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must require administrators to authenticate before gaining access to the TOE interfaces.	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.
	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 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	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

must be able to provide reliable timestamps for its own use in order to record events in the correct order in which they occurred.		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 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.	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.
	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 initialisation	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: admin 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 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.	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 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.TLS The TOE must use TLS to protect the confidentiality of traffic while it is being transmitted between the TOE and another trusted IT product as specified by the Optimization Policy.	FCS_CKM.1 Cryptographic key generation	This requirement supports O.TLS by requiring that cryptographic keys are generated according to an assigned standard.
	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.TLS by ensuring that cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	FCS_COP.1 Cryptographic operation	This requirement supports O.TLS 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.TLS 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.TLS 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 initialisation	This requirement supports O.TLS by specifying that the Optimization Policy shall be applied permissively to traffic flowing through the TOE. This means that encrypted information will pass through without being modified if the cryptographic key or algorithm is unknown to the TOE, or if the TOE is configured to not modify the traffic.
	FTC_ITC.1 (EXP) Inter-TSF trusted communications channel	This requirement supports O.TLS by providing a trusted channel through which TLS protected information can be exchanged securely with a remote trusted IT entity.
O.OPTIMIZE The TOE must optimize traffic flowing through the TOE according to the rules defined in the Optimization Policy.	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 initialisation	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.

8.5.2 Security Assurance Requirements Rationale

EAL 4+ was selected because it is best suited to addressing the stated security objectives. EAL 4+ challenges vendors to use best (rather than average) commercial practices. EAL 4+ allows the vendor to evaluate their product at a detailed level, while still benefitting from the Common Criteria Recognition Agreement. The chosen assurance level is appropriate for the threats defined in the environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 21 lists each requirement that the TOE claims conformance with, any other requirements each requirement depends on, and an indication of whether the dependency is met. As the table indicates, all dependencies have been met.

Table 21 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3(a)	✓	
	FDP_ACC.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3(b)	✓	
FIA_UAU.2	FIA_UID.1	✓	Though FIA_UID.1 is not being claimed, FIA_UID.2 is being claimed, and is hierarchical to FIA_UID.1.
FIA_UID.2	None	Not applicable	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	

	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MSA.3(b)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Though FIA_UID.1 is not being claimed, FIA_UID.2 is being claimed, and is hierarchical to FIA_UID.1.
FMT_SMR.3	FMT_SMR.1	✓	
FPT_STM.1	None	Not applicable	
FTA_SSL.3	None	Not applicable	
FTC_ITC.1 (EXP)	None	Not applicable	

9 Acronyms and Terminology

9.1 Acronyms

Table 22 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cypher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CSEC	Communications Security Establishment Canada
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ID	Identification
IP	Internet Protocol
IT	Information Technology

Acronym	Definition
LAN	Local Area Network
LZW	Lempel-Ziv-Welch
MD5	Message Digest 5
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAID	Redundant Array of Independent Disks
RiOS	Riverbed Optimization System
RNG	Random Number Generator
RSA	Rivest, Shamir, Adelman (encryption algorithm)
SAR	Security Assurance Requirement
SDR	Scalable Data Referencing
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hashing Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TA	Transaction Acceleration

Acronym	Definition
TACACS+	Terminal Access Controller Access Control System +
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TLS	Transport Layer Security
TP	Transaction Prediction
TSF	TOE Security Function
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VWE	Virtual Window Expansion
WAFS	Wide Area File Services
WAN	Wide Area Network