Certification Report

EAL 4+ Evaluation of Riverbed Steelhead Appliance v4.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-107-CR
Version: 1.0
Date: 28 June 2010
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratory located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 28 June 2010, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following registered trademark:

- Linux is a registered trademark of Linus Torvalds.

TABLE OF CONTENTS

Executive Summary

Riverbed Steelhead Appliance v4.1 (hereafter referred to as Steelhead Appliance v4.1), from Riverbed Technology, Incorporated, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Steelhead Appliance v4.1 comprises a family of network appliance models that provides Wide Area Network Optimization services including traffic acceleration, traffic quality of service, and traffic protection. Steelhead Appliance v4.1 uses FIPS 140-2 validated cryptography for traffic protection. Steelhead Appliance v4.1 evaluated models comprise the 520, 1020, 1520, 2020, 3020, 3520, 5520, 6020, 250, 550, 1050, 2050, 5050, and 6050.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 11 June 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Steelhead Appliance, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Steelhead Appliance evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Riverbed Steelhead Appliance v4.1 (hereafter referred to as Steelhead Appliance v4.1), from Riverbed Technology, Incorporated.

2 TOE Description

The TOE comprises application software, a Linux based operating system, and a cryptographic module running on the hardware appliances 520, 1020, 1520, 2020, 3020, 3520, 5520, 6020, 250, 550, 1050, 2050, 5050, and 6050.

Steelhead Appliance v4.1 is deployed in pairs as shown in Figure 1 below. A proprietary Scalable Data Referencing (SDR) algorithm is applied to optimize traffic between Appliances. Quality of service features may be used to prioritize network traffic and to set minimum bandwidths for traffic requiring a constant data rate. Steelhead Appliance v4.1 uses FIPS 140-2 validated cryptography for the protection of traffic exchanged between appliance pairs, and between the appliances and the clients and servers communicating through appliance pairs.

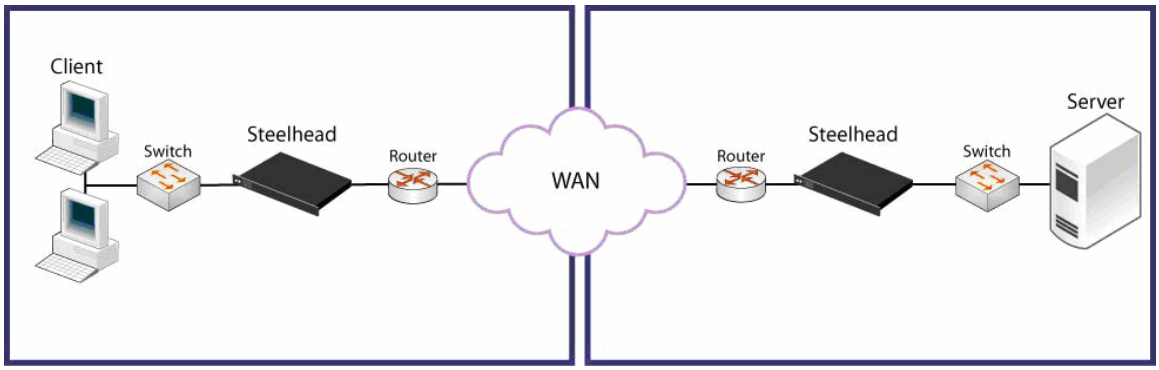

Figure 1 – Steelhead Appliance v4.1 Deployment

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Steelhead Appliance v4.1 is identified in Section 7 of the Security Target (ST).

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Steelhead 520, Steelhead 1020, Steelhead 1520 and Steelhead 2020 Appliances	*Pending* [2]
Steelhead 5050 and 6050 Appliances	*Pending*
Steelhead 3020, Steelhead 3520, Steelhead 5520 and Steelhead 6020 Appliances	*Pending*
Steelhead 250 and Steelhead 550 Appliances	*Pending*
Steelhead 1050 and Steelhead 2050 Appliances	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Steelhead Appliance v4.1:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	#792
Advanced Encryption Standard (AES)	FIPS 197	#1044
Rivest Shamir Adleman (RSA)	FIPS 186-2	#498
Secure Hash Algorithm (SHA-1)	FIPS 180-2	#994
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	#586
Random Number Generation	ANSI X9.31	#595

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Riverbed Technology, Inc. Steelhead Appliance v4.1 Security Target
Version: 0.8
Date: 11 June 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

Steelhead Appliance v4.1 is:

a. *Common Criteria Part 2 extended* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST: FTC_ITC.1: Inter-TSF trusted communications channel.
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic* Flaw Remediation

6 Security Policy

Steelhead Appliance v4.1 implements an Administrative Access Policy that defines the rules for access to administrative functions, a Quality of Service Policy that allows administrators to prioritize network traffic giving certain network traffic priority over other traffic, and a Wide Area Network (WAN) Optimization Policy that defines the rules for traffic optimization and acceleration.

In addition, Steelhead Appliance v4.1 implements policies pertaining to security audit, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, TOE access, and trusted channels. Further details on these security policies may be found in Section 1.4 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Steelhead Appliance v4.1 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and

- It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be installed and configured at an appropriate point in the network according to the appropriate installation guides;

- The TOE environment provides the network connectivity required to allow the TOE to provide secure WAN optimization;

- The TOE is located within a controlled access facility and is physically available to authorized administrators only;

- 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;

- The TOE Environment will ensure that NTP information communicated from an NTP source to the TOE cannot be modified by an attacker;

- The TOE Environment provides 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; and

- The TOE and the RADIUS or TACACS+ authentication server are located within the same controlled access facility.

7.3 Clarification of Scope

Steelhead Appliance v4.1 does not optimize User Datagram Protocol (UDP) traffic, but does apply quality of service rules to UDP traffic.

8 Evaluated Configuration

The TOE comprises the application software 4.1.10-fips-b, the CentOS 4 distribution of Linux, and a cryptographic module running on the hardware appliances 520, 1020, 1520, 2020, 3020, 3520, 5520, 6020, 250, 550, 1050, 2050, 5050, and 6050. There are fourteen evaluated configurations as follows:

Hardware Identifier (Model)	Software Identifier	Cryptographic Module	TOE Identifier
520	4.1.10-fips-b	Steelhead 520, Steelhead 1020, Steelhead 1520 and Steelhead 2020 Appliances	520/4.1.10-fips-b
1020	4.1.10-fips-b	Steelhead 520, Steelhead 1020, Steelhead 1520 and Steelhead 2020 Appliances	1020/4.1.10-fips-b
1520	4.1.10-fips-b	Steelhead 520, Steelhead 1020, Steelhead 1520 and Steelhead 2020 Appliances	1520/4.1.10-fips-b
2020	4.1.10-fips-b	Steelhead 520, Steelhead 1020, Steelhead 1520 and Steelhead 2020 Appliances	2020/4.1.10-fips-b
3020	4.1.10-fips-b	Steelhead 3020, Steelhead 3520, Steelhead 5520 and Steelhead 6020 Appliances	3020/4.1.10-fips-b
3520	4.1.10-fips-b	Steelhead 3020, Steelhead 3520, Steelhead 5520 and Steelhead 6020 Appliances	3520/4.1.10-fips-b
5520	4.1.10-fips-b	Steelhead 3020, Steelhead 3520, Steelhead 5520 and Steelhead 6020 Appliances	5520/4.1.10-fips-b
6020	4.1.10-fips-b	Steelhead 3020, Steelhead 3520, Steelhead 5520 and Steelhead 6020 Appliances	6020/4.1.10-fips-b
250	4.1.10-fips-b	Steelhead 250 and Steelhead 550	250/4.1.10-fips-b

Hardware Identifier (Model)	Software Identifier	Cryptographic Module	TOE Identifier
		Appliances	
550	4.1.10-fips-b	Steelhead 250 and Steelhead 550 Appliances	550/4.1.10-fips-b
1050	4.1.10-fips-b	Steelhead 1050 and Steelhead 2050 Appliances	1050/4.1.10-fips-b
2050	4.1.10-fips-b	Steelhead 1050 and Steelhead 2050 Appliances	2050/4.1.10-fips-b
5050	4.1.10-fips-b	Steelhead 5050 and 6050 Appliances	5050/4.1.10-fips-b
6050	4.1.10-fips-b	Steelhead 5050 and 6050 Appliances	6050/4.1.10-fips-b

The publication entitled FIPS/CC Administrator's Guide 712-00047-01 describes the procedures necessary to install and operate Steelhead Appliance v4.1 in its evaluated configuration.

9 Documentation

The following documents are provided to the consumer:

- Riverbed Technology, Inc. Steelhead Appliance v4.1 Security Target v0.8;
- Riverbed Command-Line Interface Reference Manual 720-00002 (PUB-00003);
- Hardware Owner's Manual 720-00101 (PUB-00050);
- Maintenance Guide 710-00016 (PUB-00044);
- Riverbed Steelhead Management Console User's Guide 720-00001 (PUB-00001);
- Safety and Compliance Guide 710-00004 (PUB-00009);
- Riverbed Steelhead Appliance Deployment Guide 720-00006 (PUB-00018);
- Riverbed Getting Started Guide 710-00102 (PUB-00048);

- Riverbed Steelhead Appliance Installation and Configuration Guide 710-00001 (PUB-00002);
- Rack Installation Guide (Steelhead Series 3000,5000, and 6000, and Interceptor2 Systems) 710-00010 (PUB-00033);
- Bypass Card Installation Guide 710-00018 (PUB-00026);
- Riverbed SSL Administrators guide v.4.1 February 2008 part number 712-0030-01; and
- FIPS/CC Administrator's Guide 712-00047-01.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Steelhead Appliance v4.1, including the following areas:

Development: The evaluators analyzed the Steelhead Appliance v4.1 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Steelhead Appliance security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Steelhead Appliance v4.1 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Steelhead Appliance v4.1 configuration management system and associated documentation was performed. The evaluators found that the Steelhead Appliance v4.1 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Steelhead Appliance v4.1 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Steelhead Appliance v4.1 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Riverbed Technology, Incorporated for Steelhead Appliance v4.1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Steelhead Appliance v4.1. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the Steelhead Appliance in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of DOMUS IT Security Laboratory test goals:

a. Repeat of Developer's Tests: The evaluator repeated all the developer tests to gain a deeper understanding of the TOE and its interfaces. All security functions and interfaces were exercised.

b. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data;

c. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only;

d. Security Management: The objective of these tests is to ensure that authorized individuals are able to manage the TOE in a secure manner; and

e. Protection of the TSF: The objective of this test is to ensure that the TOE can be configured to reflect the correct time settings.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Reconnaissance and exploratory testing to observe application behavior using Firecookie and Wireshark;
- Use of automated vulnerability scanning tools (NESSUS and NMAP) to discover potential network, platform and application layer vulnerabilities;
- Use of automated SQL injection tools (WEBSCARAB) to determine SQL injection vulnerabilities;
- Capture and analysis of session ID cookies to determine susceptibility to prediction; and
- Attempts to bypass authentication and authorization controls.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

11.4 Conduct of Testing

Steelhead Appliance v4.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Steelhead Appliance v4.1 behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

Consumers should review the security aspects of the intended environment (defined in Section 3.3 of the ST) and the functionality excluded from evaluation (detailed in Section 1.4.5 of the ST) when deploying Steelhead Appliance v4.1.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTP	Network Time Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
RADIUS	Remote Authentication Dial In User Service
SDR	Scalable Data Referencing
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TOE	Target of Evaluation
UDP	User Datagram Protocol
WAN	Wide Area Network
WDS	Wide Area Data Services

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. Riverbed Technology, Inc. Steelhead Appliance v4.1 Security Target, v0.8, June 11, 2010.

e. Evaluation Technical Report Version 1.2 Riverbed Technology, Inc. Steelhead Appliance v4.1, June 11, 2010.