Riverbed Technology, Inc.

Steelhead 250 and Steelhead 550 Appliances
(Hardware Versions: 250 and 550; Firmware Version: 4.1.10)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 1.2

Prepared for:
Riverbed Technology, Inc.

199 Fremont Street
San Francisco, CA 94105

Phone: (415) 247-8800
Fax: (415) 247-8801
http://www.riverbed.com

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Steelhead 250 and 550 Appliances from Riverbed Technology, Inc. This Security Policy describes how the Steelhead 250 and 550 Appliances meet the security requirements of the Federal Information Processing Standards (FIPS) Publication 140-2 and how to run the modules in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the modules.

FIPS 140-2 details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website (http://csrc.nist.gov/groups/STM/index.html), which is maintained by the National Institute of Standards and Technology (NIST) and the Communication Security Establishment Canada (CSEC).

The Steelhead 250 and 550 Appliances are referred to in this document as the Steelhead Appliances, the appliances, the cryptographic modules, or the modules.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Riverbed website (http://www.riverbed.com) contains information on the full line of products from Riverbed.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence Document
- Finite State Machine
- Validation Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Riverbed. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Riverbed and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Riverbed.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 Steelhead 250 and 550 Appliances

2.1 Overview

Riverbed Technology, Inc. is one of the industry leaders in wide-area data solutions (WDS). The Steelhead family of appliances provides application acceleration and accelerated data transfer over a wide area network (WAN), overcoming bandwidth and geographical limitations to improve productivity and enable global collaboration.

The Steelhead Appliances are powered by the Riverbed Optimization System, or RiOS. RiOS employs a combination of data reduction, Transmission Control Protocol (TCP) traffic optimization, and application-level protocol optimizations. Together, these technologies, along with RiOS management capabilities, provide a comprehensive solution for enterprise WDS.

Figure 1 shows a typical deployment scenario for Steelhead Appliances.

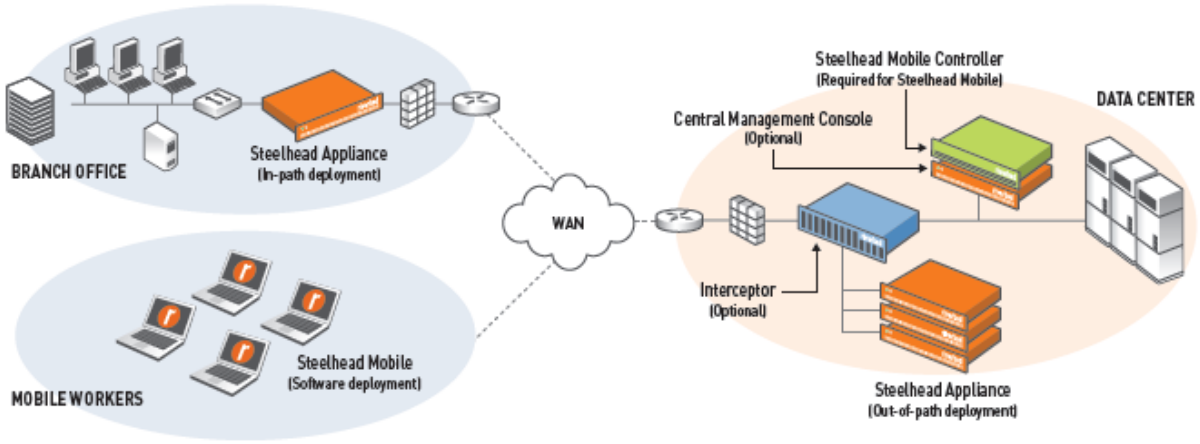

Figure 1 – Typical Steelhead Appliance Deployment

The Steelhead Appliances offer support for network traffic acceleration over Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections, remote authentication via RADIUS[1] and TACACS+[2], IPsec[3]-protected WAN traffic, AES[4] encryption of data-at-rest, and secure device registration.

[**NOTE**: Because the underlying library providing the cryptographic functions for IPsec was not tested, the appliances' IPsec functionality is not allowed and must not be used when the module is running in its FIPS-Approved mode of operation.]

The Riverbed Steelhead Appliances feature a variety of models ranging from sub-1U desktop systems to 5U rack mounted systems. All of the models provide top-performance data optimization with 1Mbps speed. This document focuses on the Steelhead 250 and 550 Appliances. These sub-1U form factor appliances are targeted for use in small to mid-size office environments, supporting up to an estimated 450 users. The appliances share a common enclosure, which is pictured in Figure 2 below.

[1] RADIUS – Remote Authentication Dial In User Service
[2] TACACS+ – Terminal Access Controller Access-Control System Plus
[3] IPsec – Internet Protocol Security
[4] AES – Advanced Encryption Standard

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 2 – Steelhead 250 and 550 Appliances

See Table 1 below for a comparison of model specifications.

Table 1 – Model Specifications for the Steelhead 250 and 550 Appliances

Feature	250	550
WAN Capacity	1 Mbps	2 Mbps
WAN Capacity (High-Speed)	1 Mbps	2 Mbps
Total Disk Capacity	120 GB	160 GB
Data Store Capacity	40 GB	80 GB
Memory	1 GB	2 GB
Maximum # of Network Ports	2	2

Per FIPS 140-2, the cryptographic modules are classified as multi-chip standalone cryptographic modules. They are validated at the following FIPS 140-2 Section levels:

Table 2 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Specification

The Steelhead 250 and 550 Appliances are hardware modules that are defined as multiple-chip standalone embodiments. They consist of the Steelhead software running on a typical server platform. The cryptographic boundary is defined by the server's metal chassis (including any required baffles), which surrounds all the hardware and software components.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Cryptographic functionality for the modules is provided by the Riverbed Steelhead Cryptographic Engine v1.0. This engine provides the FIPS-Approved algorithms listed in Table 3 below.

Table 3 – Algorithms Provided by Steelhead Cryptographic Engine

Approved or Allowed Security Functions	Certificate number
Symmetric Key Algorithm	
Advanced Encryption Standard (AES) 128-, 192-, 256-bit in CTR[5], CBC[6] and ECB[7] modes	1044
Triple-DES[8] – 112- and 192-bit in CBC mode	792
Secure Hashing Algorithm (SHA)	
SHA-1	994
Message Authentication Code (MAC) Function	
Keyed-Hash Message Authentication Code with SHA-1 (HMAC SHA-1)	586
Pseudo Random Number Generator (PRNG)	
ANSI[9] X9.31 Appendix A.2.4 PRNG	595
Asymmetric Key Algorithm	
RSA[10] PKCS[11] #1 sign/verify: 1024- and 2048-bit	498
Diffie-Hellman (DH) key agreement: 1024-bit[12]	N/A
RSA encrypt/decrypt[13] for key transport: 1024- and 2048-bit	N/A

The additional algorithms that are implemented in the modules but disabled in FIPS mode of operation are listed below. These algorithms are either non-Approved functions or have not been tested for algorithm certificate:

- Message Digest 5 (MD5)
- Digital Signature Algorithm (DSA)
- IPsec-supporting algorithms
  - Data Encryption Standard (DES)
  - Rivest Cipher 4 (RC4)
  - IDEA
  - CAST
  - Blowfish
  - HMAC-Tiger
  - Elliptic Curve Diffie-Hellman
- RC2

[5] CTR – Counter
[6] CBC – Cipher-Block Chaining
[7] ECB – Electronic Codebook
[8] DES – Data Encryption Standard
[9] ANSI – American National Standards Institute
[10] RSA – Rivest, Shamir, and Adleman
[11] PKCS – Public Key Cryptography Standard
[12] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)
[13] Caveat: RSA (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.3 Module Interfaces

The modules have several ports at the front and rear panels. The following is a list of the physical ports available for the modules in the FIPS mode of operation:

- Ethernet ports:
  - Primary (PRI) (10/100/1000 Base-T, auto-negotiating)
  - Auxiliary (AUX) (10/100/100Base-T, auto-negotiating)
  - LAN (10/100/1000 Base-TX)
  - WAN (10/100/1000 Base-TX)
- Universal Serial Bus (USB) ports to connect a keyboard and mouse
- Console port for serial communication

The front panel of the modules is populated with USB ports, a serial console port, Ethernet ports, and light-emitting diodes (LEDs) as shown in Figure 3 below.

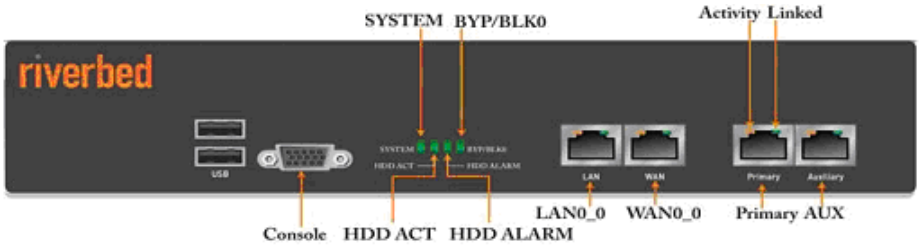

Figure 3 – Front Panel of Steelhead 250 and 550 Appliances

The modules' LEDs provide indications of operational status. System health status information is provided by the System LED, and is indicated by the following:

- Normal – blue
- Minor alarm – yellow
- Major alarm – red
- System boot – yellow

Failure of FIPS self-tests are shown in red on the System LED.

The rear panel of the modules is populated with a power supply connection as shown in Figure 4.

Figure 4 – Rear Panel of Steelhead 250 and 550 Appliances

Ports and interfaces on the modules can be categorized as the following FIPS 140-2 logical interfaces:

- Data input
- Data output
- Control input
- Status output
- Power

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 4 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Steelhead 250 and 550 Appliances Port/Interface
Data Input	Ethernet ports
Data Output	Ethernet ports
Control Input	Ethernet ports, serial console port, USB port
Status Output	Ethernet ports, serial console port, System LED
Power	Power connection

2.4 Roles and Services

The modules support role-based authentication. There are two roles in the modules that operators may assume: a Crypto-Officer (CO) role and User role.

2.4.1 Crypto-Officer Role

The Crypto-Officer installs/uninstalls, configures, and monitors the modules. This can be accomplished locally or remotely. Locally, the CO can employ the available Command Line Interface (CLI) via the serial console port. The CO may also access the modules' Graphical User Interface (GUI) remotely via the LAN Ethernet port over a secure channel (TLS[14] v1.0 or SSH[15] v2.0).

Descriptions of the services available to the Crypto-Officer role, as well as the type of access required, are provided in the Table 5 below. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 5 – Crypto-Officer Services

Service	Description	Key/CSP
Configure In-Path Rules	Configure in-path rules that enable specific IP addresses and ports on which traffic passes through optimized	None
Configure Optimization Features	Configure general optimization service settings	None
Configure Asymmetric Routing	Configure asymmetric route detection, which automatically detects and reports asymmetric routing conditions and caches this information to avoid losing connectivity between a client and a server	None

[14] TLS – Transport Layer Security
[15] SSH – Secure Shell

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Key/CSP
Configure Connection Forwarding	Enable connection forwarding only in asymmetric networks; that is, in networks in which a client request traverses a different network path than the server response	None
Configure Netflow	NetFlow enables to collect traffic flow data and gather it on NetFlow collectors. You can gather reoptimization and post-optimization data on traffic flows for custom reports.	None
Apply Quality-of-Service (QoS) Policies	Apply QoS policies to allocate bandwidth and latency priorities	None
Modify QoS Classes	Modifying the QoS classes	None
Configure QoS Marking	Configure QoS marking	None
Configure Simplified Routing	Simplified routing collects the IP address for the next hop MAC address from each packet it receives to use in addressing traffic	None
Configure Web Cache Communication Protocol (WCCP)	WCCP enables to redirect traffic that is not in the direct physical path between the client and the server	None
Start Service	Start the optimization service	None
Stop Service	Stop the optimization service	None
Restart Service	Restart the optimization service	None
Configure Scheduled Jobs	View completed, pending, inactive jobs, as well as jobs that were not completed because of an error.	None
Upgrade or Revert Firmware	Upgrade or revert to a backup version of the firmware	- Firmware Authentication Key (R)
Manage Licenses	Install new license, view a list of active licenses, and update or remove expired licenses	None
View Permissions	Display system permissions and add or change login password	None
Manage Configuration Files	Save, activate, import, and revert configurations	None
Manage Authentication	Configure authentication services	None
Configure Web Settings	Modify Management Console Web user interface settings	None
View Reports And Logs	Display system reports and user and system logs	None
Perform Self-Tests	Perform self-tests on demand	None
Show Status	Displays current status of the modules	None
Zeroization	Reset to factory settings; zeroize all ephemeral keys and Critical Security Parameters (CSPs) within the modules	- Steelhead private key (W) - Steelhead public key (W) - Administrator password (W) - Monitor password (W)

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Key/CSP
Establish Secure Session	Establish a secure session for data transmission	- Steelhead private key (X) - Steelhead public key (X) - Key Establishment key pair (R, W) - TLS Session Authentication key (R, W) - TLS Session key (R, W) - SSH Session Authentication Key (R, W) - SSH Session Key (R, W)

2.4.2 User Role

The User role is used to view system logs to monitor system activity in order to troubleshoot problems. The User role service is described in Table 6 below.

Table 6 – User Services

Service	Description	Type of Access
View Status Reports	Displays status reports	N/A

2.4.3 Authentication Mechanisms

The Crypto Officer authenticates to the modules using a user ID and password. Users authenticate themselves with a user ID/password combination. RSA digital certificate authentication is used during TLS sessions. Table 7 lists the authentication mechanisms used by the modules.

Table 7 – Authentication Mechanisms Employed by the Module

Type of Authentication	Authentication Strength
Password	Passwords are required to be at least 6 characters long. The maximum password length is 64 characters. Alphanumeric characters can be used with repetition, which gives a total of 62 characters to choose from. The chance of a random authentication attempt falsely succeeding is no less than 1 in 62^6, or 1 in 56,800,235,584. MD5 hashes are used for authentication via RADIUS and TACACS+. MD5 hashes are typically represented as 32-digit hexadecimal values. The chance of a random authentication attempt falsely succeeding is 1 in 16^{32}, or 1 in 3.4028×10^{38}
RSA Certificate	Certificates used as part of TLS are (at a minimum) 1024 bits. The chance of a random attempt falsely succeeding is 1 in 2^{80}, or 1 in 1.2089×10^{24}.

2.5 Physical Security

The Steelhead 250 and 550 Appliances are multi-chip standalone cryptographic modules. The modules are contained in hard metal chasses which are defined as the cryptographic boundary of the modules. The modules' chasses are opaque within the visible spectrum. The enclosures of the modules have been designed to satisfy level 2 physical security requirements.

The chasses covers are the only removable component of the modules, and there are only a limited set of ventilation holes in the chasses. To provide FIPS-compliant physical security, the modules are delivered with a tamper-evident kit which contains tamper-evident labels and security panels in the form of louvered baffles. When properly applied to the chasses, the tamper-evident labels provide physical evidence of attempts to remove the chasses covers, while

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

the security panels obscure the view of the internal components of the module. The proper application of the tamper-evident kit is detailed in the "Secure Operation" section of this document.

2.6 Operational Environment

The operational environment requirements do not apply to the Steelhead 250 and 550 Appliances, because the modules do not provide a general-purpose operating system (OS) to the user. The OS has a limited operational environment and only the modules' custom written image can be run on the system. The modules provide a method to update the firmware in the modules with a new version. This method involves downloading a RSA digitally signed firmware update to the modules.

2.7 Cryptographic Key Management

Two security-related protocols are employed by the Approved mode of the modules: SSH v2.0 and TLS v1.0. Table 8 introduces cryptographic keys, key components, and CSPs involved in these two protocols. The modules support the following critical security parameters:

Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Steelhead private key	RSA 1024- or 2048-bit private key	Internally generated or imported electronically	Never exits the modules	Stored in plaintext on the hard disk Resides in volatile memory in plaintext	By command or overwriting with another key	- Peer Authentication of TLS sessions - Key transport for TLS session
Steelhead public key	RSA 1024- or 2048-bit public key	Internally generated or imported electronically in plaintext during TLS handshake protocol	Exits electronically in plaintext during TLS handshake protocol	Stored in plaintext on the hard disk Resides in volatile memory in plaintext	By command or overwriting with another key	- Peer Authentication of TLS sessions - Key transport for TLS session
Key Establishment key pair	Diffie-Hellman 2048-bit keys	Internally generated	Public exponent electronically in plaintext, private component not exported	Resides in volatile memory in plaintext	Power cycle of modules	Key agreement for SSH sessions
TLS Session Key	Triple-DES ECB/CBC 2 or 3 key AES ECB/CBC 128-, 192-, 256-bits key	Internally generated or entered electronically in encrypted form	Exported electronically in encrypted form	Resides in volatile memory in plaintext	Power cycle of modules	Data encryption/decryption for TLS sessions

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Session Authentication Key	HMAC-SHA1 key	Internally generated or entered electronically in encrypted form	Never exists the module	Resides in volatile memory in plaintext	Power cycle of modules	Data authentication for TLS sessions
SSH Session Key	Triple-DES ECB/CBC 2 or 3 key AES ECB/CBC 128-, 192-, 256-bits key	Internally generated	Never exits the modules	Resides in volatile memory in plaintext	Power cycle of modules	Data encryption/decryption for SSH sessions
SSH Session Authentication Key	HMAC-SHA1 key	Internally generated	Never exists the module	Resides in volatile memory in plaintext	Power cycle of modules	Data authentication for SSH sessions
Administrator Passwords	String of characters	Entered electronically	Never exits the module	Hashed value stored on hard drive	By command	Administrator (Crypto-Officer) login
ANSI X9.31 PRNG seed	16 bytes of seed value	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle of modules	Used in seeding FIPS-Approved RNG
ANSI X9.31 PRNG key	2-key Triple DES – 16 bytes	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Power cycle of modules	Used in seeding FIPS-Approved RNG
Data Storage Key	AES-128, 192, 256	Internally generated	Never exits the module	Resides on disk in plaintext	Reset Factory	Encrypted data storage on modules
Boot Loader password	Password	Set by Crypto-Officer	Never exits the module	Resides on disk in encrypted	Reset Factory	Used to prevent boot process changes
Firmware Authentication Key	1024 bit RSA public key	Hard coded	Never exits the module	Embedded in Code in plaintext	Not Zeroized	Authenticate firmware updates

2.8 Electromagnetic Interference/Electromagnetic Compatibility

The modules were tested and found conformant to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self-Tests

The cryptographic modules perform the following self-tests at power-up: a firmware integrity test and cryptographic algorithm tests. Each self-test event result, regardless of the outcome, can be viewed by the CO using the GUI or CLI.

- **Firmware integrity check using MD5 Error Detection Code (EDC)**

  The modules first perform the Firmware Integrity Test during power-up. If the image is verified successfully, then the modules display the following message before proceeding with KATs.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

"*** Image integrity test succeeded!"

Upon failure, a Firmware Integrity Test failure message is shown. The message is as below:

"*** Image integrity test failed!"

- **Cryptographic algorithm tests**
  - AES Known Answer Test (KAT)
  - Triple-DES KAT
  - HMAC SHA-1 KAT
  - RSA sign/verify KAT
  - PRNG KAT

The modules also perform these tests at power-up. If any of the self-tests fails to complete successfully, its process is shutdown immediately after displaying the following message over the management interface:

"FIPS selftests failed, reason: [reason] shutdown [process name] now"

Table 9 lists the reasons for the failure of self-tests.

Table 9 – Status Output Messages for Power-Up Test

Power-Up Test	Error Message
PRNG KAT	"RNG test error!"
AES KAT	"AES test error!"
Triple-DES KAT	"3DES test error!"
HMAC SHA-1 KAT	"HMAC test error!"
RSA KATs for sign/verify and encrypt/decrypt	"RSA test error!"
CRNGT (performed at power-up)	"RAND_Bytes Failed"

Individual success messages are not logged for each KAT, but the processes log an overall success message after all KATs are passed. The success message is "[process name] passed FIPS selftests."

The operator can initiate power-up self-tests by simply rebooting the modules at any time. No data output or cryptographic operations are possible when the module enters the critical error state. Intervention from the CO is required to clear this error state by restarting the modules. If the error message persists as the result of a hard error, then the modules must be returned to Riverbed for service.

- **Conditional self-tests**
  - RSA pairwise consistency test for sign/verify (performed each time that an RSA public/private keypair is generated)
  - Continuous PRNG Test (CRNGT)
  - Firmware upgrade test using RSA digital signature verification

These tests are performed while the modules are in their operation state. Failure of the RSA pairwise consistency check, CRNGT, or firmware upgrade takes the module into the soft error state. No data output or cryptographic operations are possible when the module enters the soft error state. Since conditional self-test failures do not result in terminal errors, they can be cleared if the failed test is re-executed successfully. For conditional self-tests, the error messages in Table 10 are displayed.

Table 10 – Status Output Messages for Failed Conditional Self-Tests

Conditional Self-Test	Error Message

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Conditional Self-Test	Error Message
Pairwise Consistency Test	"FIPS_R_PAIRWISE_TEST_FAILED"
CRNGT	"RAND_R_PRNG_STUCK"
Firmware Load Test	"Failed to validate image file"

2.10 Design Assurance

Riverbed uses Subversion v1.4 to manage changes to source code files. Riverbed's Information Technology (IT) team is responsible for managing access to the Subversion source repository and documentation. Additionally, Microsoft Visual SourceSafe version 6.0 is used to provide configuration management for the module's FIPS documentation. Visual SourceSafe provides access control, versioning, and logging.

All the firmware components within the cryptographic modules are implemented using high-level C language.

The security during delivery is guaranteed by trusted carriers such as FedEx, DHL, and UPS. The Crypto-Officer should check the package for any irregular tears or opening. If the Crypto-Officer suspects tampering, he/she should immediately contact Riverbed Technology, Inc.

2.11 Mitigation of Other Attacks

In a FIPS mode of operation, the modules do not claim to mitigate any additional attacks.

2.12 Cryptographic Module Security Policy

As stated above, this Security Policy specifies the following for the cryptographic modules:

- identification and authentication policy
- services provided to the supported authorized roles
- "show status" and "self-test" services
- allowed type(s) of access to the CSPs
- the physical security mechanisms implemented

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Secure Operation

The Steelhead 250 and 550 Appliances meet the Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in a FIPS-Approved mode of operation.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for initialization and security-relevant configuration and management of the modules. Please see Riverbed's Administration Guide for more information on configuring and maintaining the modules. The Crypto-Officer receives the module from the vendor via trusted delivery services (UPS, FedEx, etc.). The appliance will be accompanied by the following:

- Media and Documents
  - Packing slip
  - Getting Started Guide
  - FIPS Administrator's Guide
  - Steelhead Appliance Installation and Configuration Guide
  - Steelhead Management Console User's Guide
  - Riverbed Command-Line Interface Reference Manual
  - Management Tools software CD[16] (Steelhead Management Console and Steelhead Central Management Console)
- Tamper-evident kit
- Rack mount kit

Riverbed documentation can also be downloaded from the Riverbed Technical Support Web site located at https://support.riverbed.com. The website also includes Riverbed Knowledge Base which is a database of known issues, how-to documents, system requirements, and common error messages.

The Crypto-Officer is responsible for the proper initial setup of the Management Tool software and for ensuring that the module is running securely in its FIPS mode of operation. Instructions to put the module in its FIPS mode of operation are provided in the "Initialization" section below.

3.1.1 First-Time Authentication

In order to perform the required initialization and configuration functions, the Crypto-Officer must first authenticate to the module. The module provides a default username/password for first-time access to the module. The procedure by which the operator is authenticated upon accessing the module for the first time can be found in the *Steelhead Appliance Installation and Configuration Guide*, which accompanies the module.

Note that it is the responsibility of the Crypto-Officer to change the default password after first use. Guidance on setting the administrative password can be found in the *FIPS/CC Administrator's Guide*.

3.1.2 Initialization

The Crypto-Officer must follow the steps below to initialize the appliance in FIPS mode:

A. **Run the FIPS validated image**: The CO must check whether the appliance is running a FIPS-mode image or not on both partitions of the system by following the steps given below. FIPS mode images contain the string "fips" in the image name.

[16] CD – Compact Disc

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Connect to the Steelhead CLI. For detailed information, see the *Riverbed Command-Line Interface Reference Manual*.

2. To enter configuration mode, enter the following set of commands at the system prompt:
   - amnesiac > enable
   - amnesiac # show images

To upgrade the system image to a signed FIPS-mode image the steps given below must be followed:

1. Log in to the Management Console. For detailed information about connecting to the Management Console, see the *Steelhead Management Console User's Guide*.

2. Choose **Setup - Upgrade Software** to display the Upgrade Software page.

3. Under "Install Upgrade from:", specify a URL or browse to a Local File and click "Install Upgrade". The signed FIPS-mode image is installed on the Backup Version (partition 2) of the system.

4. To switch to the new signed FIPS-mode image on the Backup Version, click "Switch to Backup Version".

5. To reboot the appliance, choose **Setup - Reboot Appliance** and click "Reboot Appliance". You will be logged out of the Management Console. Rebooting can take a couple of minutes.

6. Reconnect to the Management Console and choose **Setup - Software Upgrade** to view the booted image on the system.

7. To install the signed FIPS-mode image on the Backup Version (partition 1) of the system, under "Install Upgrade from:", specify a URL or browse to a Local File and click "Install Upgrade". The signed FIPS-mode image is installed on the Backup Version (partition 1) of the system.

B. **Restore the system to the manufactured state:** This state will zeroize all keys and CSPs that may have been created in non-FIPS mode.

C. **Reconfigure the basic system settings:** Basic settings includes:

- Define a default gateway IP Address
- Set a Crypto-Officer password
- Define a Host Name
- Add a DNS Server

D. **Configure the Steelhead Appliance for FIPS Compliance**: Configure the following services run the module in FIPS mode of operation.

- Disable HTTP[17] and enable HTTPS[18] only. The Steelhead appliance uses port 443 for HTTPS protocol over TLS v1.0.
- Enable SSL v3.1 (TLS v1.0) and ensure that only FIPS-Approved algorithms appear in the SSL Ciphers Lists (this list can be found under the GUI menu option **Configure** > **Optimization** > **SSL Ciphers**).
- Disable SSL v2 and SSL v3.
- Ensure Internet Protocol Security (IPsec) is disabled.

[17] HTTP – Hypertext Transfer Protocol
[18] HTTPS – Secure Hypertext Transfer Protocol

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Ensure Telnet is disabled.
- Ensure Simple Network Management Protocol (SNMP) v2 is disabled.
- Ensure the Boot Order cannot be changed by adding a boot loader password.

For detailed descriptions and instructions for each of the steps mentioned above, please see Chapter 3 of the FIPS Administrator's Guide.

E. **Configure SSL v3.1 (TLS v1.0)**: The following section describes the basic steps for configuring SSL v3.1 for RiOS

1. Log in to the Management Console on the client-side and server-side Steelhead appliances.
2. Add the SSL license to the client-side and server-side Steelhead appliances.
3. Add an in-path rule on client-side Steelhead appliance to intercept port 443 (the TLS/SSL default port).
4. Enable SSL on both the client-side and server-side Steelhead appliance.
5. Generate or import a private key and certificate on both the client-side and server-side Steelhead appliance.
6. View and copy the new private key and certificate.
7. Create a peer trust relationship by installing the client-side Steelhead appliance self-signed certificate on the server-side Steelhead appliance and vice versa.
8. Generate or import the proxy certificate for the SSL server.
9. Import any Certificate Authorities (CAs), if necessary (for example, if the server certificate is self-signed or needs an intermediate CA).

F. **Install the tamper-evident kit**: The tamper-evident kit is comprised of the following components:

- Security panels: The kit comes with includes a right and left panel that must be secured to the outside of the appliance. These louvered baffles ensure that no one can view the internal components of the Steelhead appliances. To install the panels:
  1. Power down the appliance.
  2. Disconnect the appliance from the electrical outlet and peripherals.
  3. Facing the back of the chassis, attach the Right Security Panel to the outside of the chassis and secure with two screws.
  4. Repeat step 3 for the left side of the chassis.

  Installing the louvered panels does not alter the way the Steelhead Appliances are installed.
- Tamper-evident seals: The tamper-evident seals ensure that no one can tamper with the components of the Steelhead appliances without leaving some form of evidence. The modules require seven seals to be placed around the chassis to meet FIPS requirements. Figure 5 and Figure 6 below show the required label placement.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 5 – Tamper-Evident Seal Placement (Top View)

Figure 6 – Tamper-Evident Seal Placement (Left Side View)

It is recommended that the tamper-evident kit be installed after the initial configuration of the modules is complete.

The tamper-evident seals are serially-numbered. The CO must maintain a record of the location of each seal and the corresponding serial number in order to remain FIPS-compliant.

To prepare the chassis for the placement a seal, the surface where the seal will be located should first be wiped with a mild solution of rubbing alcohol and distilled water. Seals should be allowed to cure for at least 48 hours.

For detailed instructions to install the tamper-evident kit on the appliances, see Chapter 2, "Installing the Tamper-Evident Kit," of the FIPS Administrator's Guide.

3.1.3 FIPS Mode Verification

To ensure that the modules have been properly initialized, connect to the Steelhead CLI and enter the following set of commands:

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config) # show ip security <<confirm Internet Protocol security (IPSec) is disabled>>
IP security enabled:    no
PFS enabled:            yes
IKE rekeying interval:  240
```


© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Encryption policy: des <<only used if IPSEC is enabled>>
Authentication policy: hmac_md5 <<only used if IPSEC is enabled>>
amnesiac (config) # show telnet-server <<confirm Telnet server management access is disabled>>
Telnet server enabled: **no**
amnesiac (config) # show snmp <<confirm SNMP server is set to the default settings>>
SNMP enabled: no
System location:
System contact:
Read-only community: riverbed
Traps enabled: yes
Interface listen enabled: **no**
Trap interface: primary
No Listen Interfaces.
No trap sinks configured.
amnesiac (config) # show web <<confirm TLSv1 is enabled and SSLv2 and SSLv3 is disabled>>
Web-based management console enabled: **yes**
HTTP enabled: no
HTTP port: 80
HTTPS enabled: **yes**
HTTPS port: 443
Configure Mode TRAP: yes
Inactivity timeout: 1000 minutes
Session timeout: 1000 minutes
Session renewal threshold: 500 minutes
Timeout during report auto-refresh: yes
SSLv2 enabled: **no**
SSLv3 enabled: no
70 FIPS/CC Administrator's Guide
Configuring the Steelhead Appliance for FIPS Compliance
TLSv1 enabled: **yes**
Listen enabled: yes
No Listen Interfaces.

NOTE: The **bold** items must be verified and must match the settings above for the modules to be FIPS 140-2 Level 2 compliant.

3.1.4 Management

The Crypto-Officer is responsible for making sure the modules are running in their Approved mode of operation. While in a FIPS-Approved mode, only FIPS-Approved and Allowed algorithms may be used. Non-FIPS-Approved services are disabled in FIPS mode of operation. The Crypto-Officer is able to monitor and configure the module via the web GUI or the CLI. Detailed instructions to monitor and troubleshoot the appliances are provided in the FIPS Administrator's Guide. The Crypto-Officer should monitor the modules' status regularly for FIPS mode of operation.

3.1.4.1 Status Verification

The CO can check the current status of the modules by logging in through a secure TLS or SSH session. The CO can then use the available interface (GUI or CLI, respectively) to view the current connections served, users logged in, and general data flow statistics. Locally, the CO may view the same information via serial console port or connecting a keyboard and display directly. The System LED is provided to give an indication of the current health status of the modules.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.1.4.2 Power-Up Self-Test Execution

The power-up self-tests are automatically performed at power-up. Administrators can manually execute the power-up self-tests by rebooting the hardware modules, and the status can be viewed via the management GUI as shown below in Figure 7.

Alarm	Status
Admission Control	[OK]
Asymmetric Routing	[OK]
Connection Forwarding Alarms	[OK]
CPU Utilization	[OK]
Data Store	[OK]
Hardware Error	[OK]
Fan Error	[OK]
IPMI	[OK]
Licensing	[OK]
Link State	[DISABLED]
Memory Error	[OK]
Memory Paging	[OK]
Neighbor Incompatibility	[OK]
Network Bypass	[OK]
NFS V2/V4 Alarm	[OK]
Optimization Service	[OK]
FIPS Self Test	[OK]
Prepopulation or Proxy File Service configuration error	[OK]
Prepopulation or Proxy File Service operation failed	[OK]
Software Version Mismatch	[OK]
Secure Vault	[OK]
SSL Alarms	[OK]
System Disk Full	[OK]
Temperature	[OK]

Figure 7 – Power-Up Self-Test Status

The status page can be viewed by choosing the following GUI menu option:
Reports > **Diagnostics** > **Alarm Status**

If any irregular activity is noticed or the modules are consistently reporting errors, then Riverbed Customer Support should be contacted.

3.1.4.3 Key/CSP Zeroization

The modules' CLI offers a "reset factory" service, which resets all configurable parameters in the appliances to the manufactured default settings (thus zeroizing keys and CSPs) and halts the appliances. All ephemeral keys are zeroized when the associated session is terminated or by power cycling the modules. Steelhead RSA public/private keypairs can also be zeroized by overwriting with another keypair.

3.1.4.4 Maintenance of Physical Security

It is the Crypto-Officer's responsibility to ensure that the physical security posture of the modules is maintained. To accomplish this, the CO has the following responsibilities:

- The CO must visually inspect the modules periodically for signs of tampering (including seals that have been voided, peeled off, or damaged in any way).
- The CO must periodically review the serial number log and compare those recorded to those that are applied to ensure that no labels have been replaced.
- The CO must secure and have control at all times of any unused seals.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- The CO must have direct control and observation of any changes to the module such as reconfigurations of where the tamper evident seals or security panels are placed to ensure that (1) the security of the module is maintained during such changes and (2) the module is returned to a FIPS-Approved state.

3.2 User Guidance

The User does not have the ability to configure sensitive information on the modules. Although the User does not have any ability to modify the configuration of the modules, they should report to the Crypto-Officer if any irregular activity is noticed.

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Acronyms and Abbreviations

Table 11 – Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AUX	Auxiliary
CBC	Cipher Block Chaining
CD	Compact Disc
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Conditional Random Number Generator Test
CSEC	Communication Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name System
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Megabits Per Second
MD	Message Digest

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
NIST	National Institute of Standards and Technology
OS	Operating System
PFS	Proxy File Service
PKCS	Public Key Cryptography Standard
PRI	Primary
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RC	Rivest Cipher
RiOS	Riverbed Optimization System
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
WAN	Wide Area Network
WDS	Wide-area Data Solutions

© 2010 Riverbed Technology, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com