Ribcage 1100 and 2800

BACKBONE SECURITY.COM, INC.

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation
Date: 6/4/2004

Table of Contents

1. Introduction

This is a non-proprietary FIPS PUB 140-2 Security Policy for the Ribcage 1100, software revision 2.2 FIPS, hardware revision 3.0 and Ribcage 2800, software revision 2.2 FIPS, hardware revision 3.0. The Ribcage 1100 and Ribcage 2800 are multiple-chip standalone cryptographic modules, which meet security FIPS 140-2 Level 2 requirements. The cryptographic boundary of the Ribcage 1100 and Ribcage 2800 is the metal enclosure of the unit.

The Ribcage 1100 and Ribcage 2800 are functionally identical, and differ only in speed and performance. For purposes of this document, both devices will be collectively referred to as the “Ribcage” or the “module”. More information on the Ribcage is available from the Backbone Security.com website at http://www.backbonesecurity.com

This Security Policy describes how the Ribcage meets the Level 2 security requirements as specified in FIPS PUB 140-2.

2. Abbreviations and Definitions

3DES	–	Triple DES (Data Encryption Standard)
AES	–	Advanced Encryption Standard
CLI	–	Command Line Interface
CRC32	–	Cyclic Redundancy Check (32-bit)
CSP	–	Critical Security Parameter
DES	–	Data Encryption Standard
ESP	–	Encapsulating Security Payload
FIPS	–	Federal Information Processing Standard
HMAC	–	Hashed Message Authentication Code
IPSec	–	Internet Protocol Security
PKCS	–	Public Key Cryptography Standards
PRNG	–	Pseudo-Random Number Generator
PUB	–	Publication
RSA	–	Rivest, Shamir, Adleman
SHA	–	Secure Hash Algorithm
SSH	–	Secure Shell

3. Identification and Authentication Policy

Ribcage Roles and Authentication

The Ribcage supports two authorized roles for operators: a User role and a Crypto Officer role. All roles in the module use role-based authentication. Initial Crypto Officer authentication to the module is controlled by a factory default password.

The User role is represented by data streams that are authenticated on a per-packet basis. For data arriving on the private network side, the source and destination IP addresses of each packet are compared with the enabled channels as configured by the Crypto Officer. For data arriving on the public network side, the IPSec-secured packets are authenticated using HMAC-SHA-1 and then are compared with the configured channel list.

The Crypto Officer role allows an operator to perform administrative functions such as initialize the module, input or generate cryptographic keys and CSPs, and perform auditing. Crypto Officer functionality is provided via the Ribcage Command Line Interface (CLI) either through SSH or through a serial console connection.

The Crypto Officer role is protected with a password that must be entered whenever an operator wants to assume the role of Crypto Officer. To remain in FIPS mode (see Section 8), the Crypto Officer password must have a length of at least six printable ASCII characters, and must not be a dictionary word. The Ribcage will notify the operator if an attempt is made to choose a new password which violates these rules.

4. Access Control Policy

The Ribcage allows access to Crypto-Officer functionality, and subsequently read/write access to the keys and CSPs in the device, via the Ribcage Command Line Interface (CLI) through SSH or a serial console connection. An operator must authenticate to the Crypto Officer role to use the CLI. The User role of the Ribcage provides access to the IPSec services of the module through the Ethernet ports.

Crypto Officer Services Provided by Ribcage

Services	Description	Input	Output	Keys/CSPs Access
Login	An operator can authenticate to the Crypto Officer role.	"root" account name and CO password	Crypto Officer role authentication	Read CO password
Encryption/ Decryption	Crypto Officer data is encrypted and decrypted using 3DES as defined by the SSH protocol when accessing Crypto Officer services through the Ethernet ports.	SSH and CO authentication data	CLI prompt	Read/write PRNG seed key, and all SSH keys and key parameters
Define Security Policy and System Configuration	The Crypto Officer can define the rules for encrypted traffic flow in addition to general system configuration.	Commands and configuration files	Application of configuration settings	
Set/Unset FIPS Mode	The Crypto Officer can configure the unit to operate in FIPS mode.	"`fips enable`" or "`fips disable`" CLI commands	Configuration of FIPS mode	
Show Status	The Crypto Officer can have the module report back its FIPS-related status.	"`fips showstatus`" CLI command	FIPS status of module	
Zeroize Keys	The Crypto Officer can have the module zeroize all cryptographic keys and CSPs (except the CO password – see Change Password).	"`fips zeroize`" CLI command	Zeroization of all keys and CSPs	Delete all keys and CSPs
Self Tests	The Crypto Officer can initiate self-tests and view the results.	"`fips selftest`" CLI command	Status of self-tests	
Help	The Crypto Officer can get general help or help on a specific CLI command	"`help`" CLI command	A listing off all available CLI command or context-specific help	

Services	Description	Input	Output	Keys/CSPs Access
Change Password	The Crypto Officer can change the CO password	“`passwd`” CLI command	CO password changed	Delete old CO password and write new CO password
System Network Configuration	The Crypto Officer can configure the network adapters and network settings for the module.	“`ethconfig`” “`gateway`” and “`iface`” CLI commands	Results of CLI commands	
Edit Configuration File	Edit raw configuration data of module	“`editconf`” CLI command	Editing interface for configuration file	
Apply Settings	The Crypto Officer can have the module parse its configuration file and apply all settings.	“`rcparse`” CLI command	Results of CLI command	
Modify IPSec Subsystem	The Crypto Officer can modify the IPSec subsystem by adding connections, removing connections, and listing live or listening connections	“`vpn`” CLI command	Results of CLI command	Read/write PRNG seed key, IPSec IKE keys, shared-secrets and client RSA public keys. Write IPSec ESP keys
Start/Stop/ Restart Services	The Crypto Officer can start, stop, or restart services running on the module	“`start`”, “`stop`”, or “`restart`” CLI commands	Results of CLI commands	
Network Utilities	The Crypto Officer can run various network utilities to check for network connectivity and configuration of networking	“`ping`”, “`traceroute`”, “`route`”, “`firewall`” CLI commands	Results of CLI commands	
Log Maintenance	The Crypto Officer can perform various maintenance operations on the log files, such as viewing and clearing	“`log`” CLI command	Results of CLI command	Read/delete system logs
Reset Unit to Factory-Default Settings	The Crypto Officer can reset the module to its factory-default settings	“`resetribcage`” command	Results of CLI command	Delete all keys and CSPs

Services	Description	Input	Output	Keys/CSPs Access
Shutdown Module	The Crypto Office can shut the module down.	"`poweroff`" CLI command	The module begins the shutdown process	
Restart module	The Crypto Officer can restart the module	"`reboot`" CLI command	The module begins the reboot process	

User Services Provided by Ribcage

Services	Description	Input	Output	Keys/CSPs Access
IPSec	Data sent by a User is secured as defined by the IPSec standard using 3DES or AES encryption/decryption and HMAC-SHA1 authentication.	IPSec inputs and data	IPSec outputs and data	Read IPSec ESP keys (HMAC and secret keys)

Module Ports and Interfaces

Physical Port	Logical Interface
"Public" Ethernet Port	Data Input, Data Output
"Private" Ethernet Port	Data Input, Data Output, Control Input, Status Output
Serial "Console" Port	Control Input, Status Output
Front Panel Green LED	Status Output (Module Power)
Front Panel Yellow LEDs	Status Output (Ethernet Port Activity)

Cryptographic Keys and CSPs of Ribcage

The Ribcage uses the following cryptographic keys and other CSPs:

Key or CSP	Description	Source/Storage
IPSec RSA Key Pair	The Ribcage uses an RSA key pair for authentication during the IKE protocol.	Internally generated and stored on hard disk
IPSec Diffie Hellman Key Parameters	The Ribcage uses Diffie Hellman for key agreement during the IKE protocol.	Internally generated and stored on system SDRAM
SSH RSA Key Pair	The Ribcage uses an RSA key pair for authentication during the SSH protocol.	Internally generated and stored on hard disk
SSH Diffie Hellman Key Parameters	The Ribcage uses Diffie Hellman for key agreement during the SSH protocol.	Internally generated and stored on system SDRAM
Client RSA Public Keys	The Ribcage can input the RSA public keys of IPSec clients for authentication during the IKE protocol.	Electronically input and stored on hard disk
IPSec Shared-Secrets	The Ribcage can input “shared-secrets” (passphrases) for authentication during the IKE protocol.	Electronically input and stored on hard disk
IPSec Secret Keys	The Ribcage uses secret keys (AES or 3DES) for data confidentiality during the IPSec IKE and ESP protocols.	Diffie Hellman key agreement and stored on system SDRAM
IPSec HMAC Keys	The Ribcage uses HMAC keys (HMAC-SHA-1) for data integrity during the IPSec IKE and ESP protocols.	Diffie Hellman key agreement and stored on system SDRAM
SSH Secret Keys	The Ribcage uses secret keys (3DES) for data confidentiality during the SSH protocol.	Diffie Hellman key agreement and stored on system SDRAM
SSH HMAC Keys	The Ribcage uses HMAC keys (HMAC-SHA-1) for data integrity during the SSH protocol.	Diffie Hellman key agreement and stored on system SDRAM
PRNG seed key	The Ribcage uses the PRNG specified in FIPS 186-2, Appendix 3.2.	Internally generated and stored on hard disk
Crypto Officer Password	The Ribcage’s Crypto Officer role is protected by a password.	Manually or electronically input and stored on hard disk

Cryptographic Algorithms of Ribcage

The Ribcage supports the following FIPS-approved algorithms:

3DES (FIPS 46-3) – Certificate Number 208
AES (FIPS 197) – Certificate Number 94
SHA-1 (FIPS 180-2) – Certificate Number 184
HMAC-SHA-1 (FIPS 198) – Certificate Number 184, vendor affirmed
RSA – PKCS#1, vendor affirmed

The Ribcage also supports the use of the Diffie-Hellman key agreement algorithm in FIPS mode.

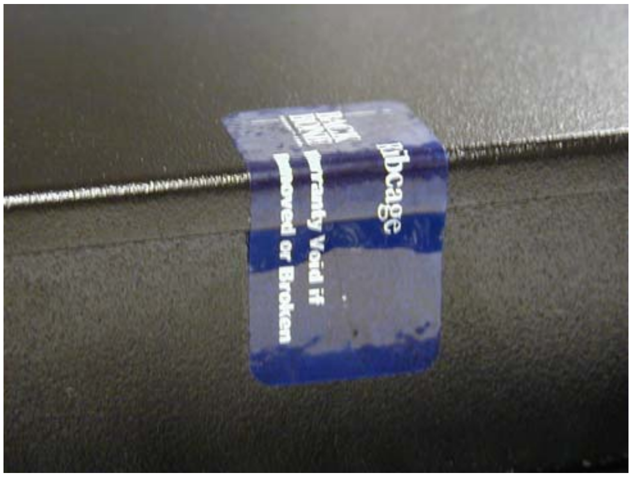
The Ribcage contains the following algorithms which cannot be used in FIPS mode:

HMAC-SHA-256
HMAC-SHA-512
HMAC-MD5

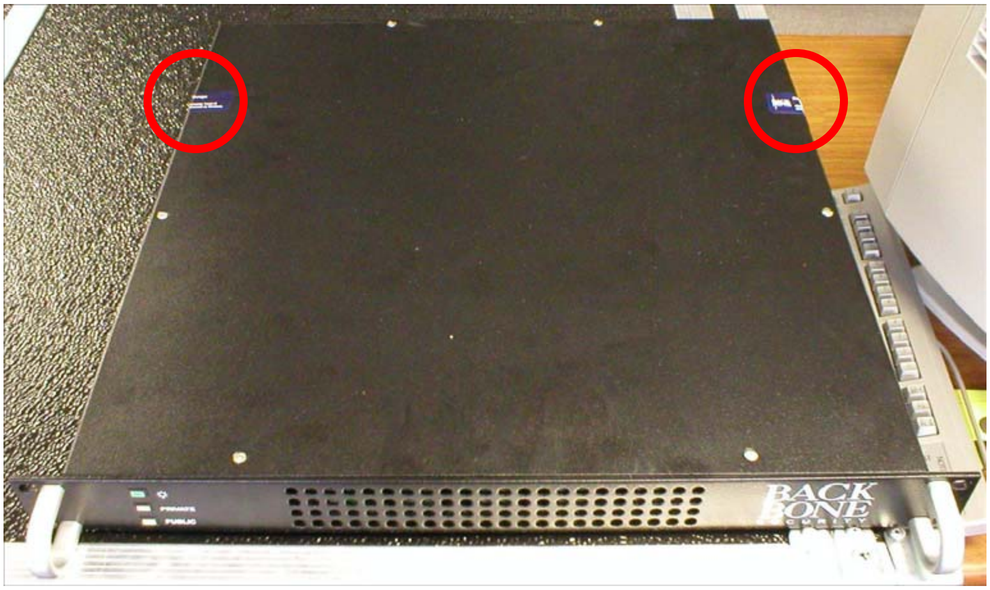
5. Physical Security Policy

Physical Security Mechanisms

The Ribcage is a multi-chip standalone module. The module consists of production-grade components, which include standard passivation techniques. The Ribcage is encased in a metal enclosure, which is fastened together by screws. There are two tamper-evident seals applied to opposite sides of the removable cover, which will indicate whether the enclosure has been opened.



Close-up of tamper-evident seal



Top-view of Ribcage indicating locations of seals.

6. Mitigation of Other Attacks Policy

The Ribcage does not specifically mitigate any other attacks.

7. Self-Tests

The Ribcage performs the following self-tests on startup or on-demand if requested by the Crypto Officer:

- 3DES Known Answer Test
- AES Known Answer Test
- HMAC-SHA-1 and RSA Known Answer Test
- PRNG Known Answer Test
- CRC32 File Integrity Test

In addition, an RSA pair-wise consistency test is performed whenever an RSA key pair is generated, and the PRNG implements a continuous RNG test which runs as random data is generated.

8. FIPS Initialization and FIPS Mode Operational Policy

To ensure that the Ribcage hardware has not been tampered with, the tamper-evident seals should be inspected periodically. See pictures in "Physical Security Policy" section for specific locations of seals.

When initializing the Ribcage for FIPS-compliant operational use, the Crypto Officer shall place the module into FIPS mode. To check the status of FIPS mode, the "`fips showstatus`" CLI command is used. If not enabled, FIPS mode is set by invoking the "`fips enable`" CLI command.

The Crypto Officer shall change the default Crypto Officer password to a new FIPS-compliant password which meets all password rules (see Section 3) – the password must be at least six printable ASCII characters and must not be a dictionary word.

To operate the Ribcage in FIPS mode, the Crypto Officer shall also:

Select the 3DES or AES algorithm for IPSec services
Select the HMAC-SHA-1 algorithm for IPSec services