Cisco Systems, Inc.

FIPS 140-2 Non-Proprietary Security Policy

Cisco Systems Libreswan Cryptographic Module

Software Version 3.20 and 3.25

Document Version 1.5

Contents

1 Introduction

This document is the non-proprietary Security Policy for the Cisco Systems Libreswan Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 1 module.

2 Cryptographic Module Specification

2.1 Module Overview

The Cisco Systems Libreswan Cryptographic Module (hereafter referred to as "the module") is a software library implementing the cryptographic algorithms. The module provides cryptographic services to other network entities implementing the IKEv1 and IKEv2 protocols.

Note: This security policy only covers the IKE key derivation, which is a part of the IPSEC protocol family.

The logical module boundary is depicted in the software block diagram below.

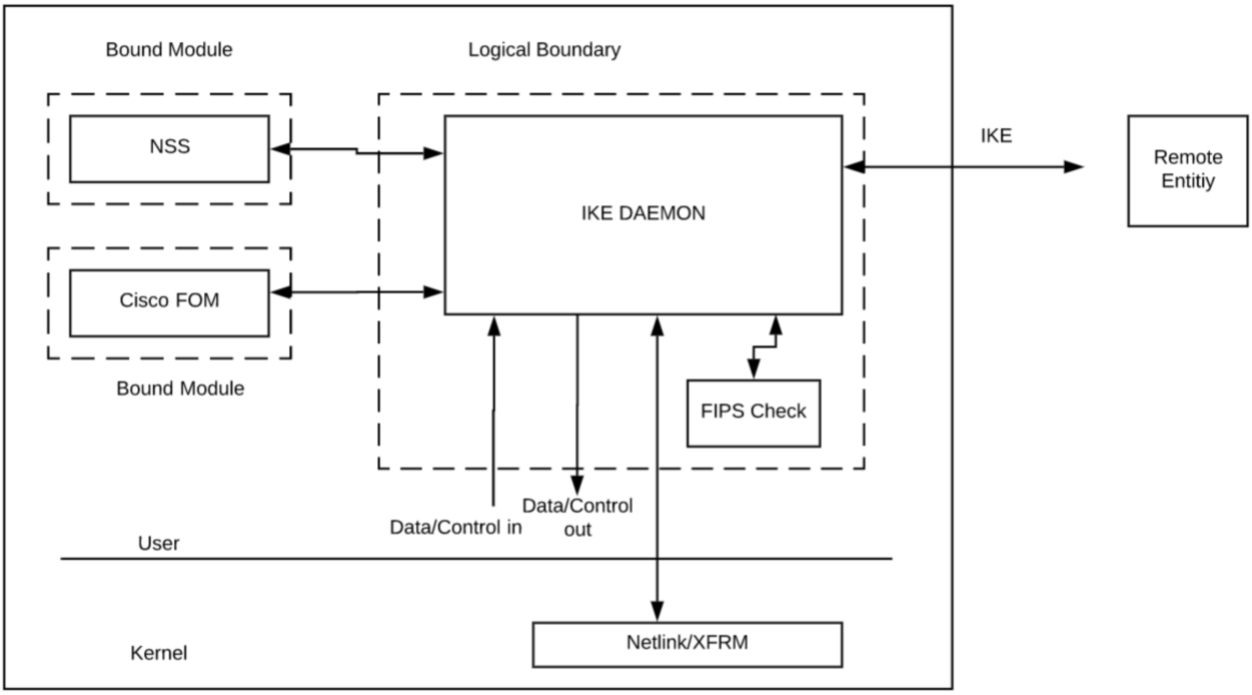

Figure 1 - Software Block Diagram

Note: In the figure above, the Cisco Systems Libreswan Cryptographic Module is comprised of the blocks labeled "IKE DAEMON" and "FIPS Check."

The module is aimed to run on a general-purpose computer; the physical boundary is the surface of the case of the target platform, as shown in the diagram below:

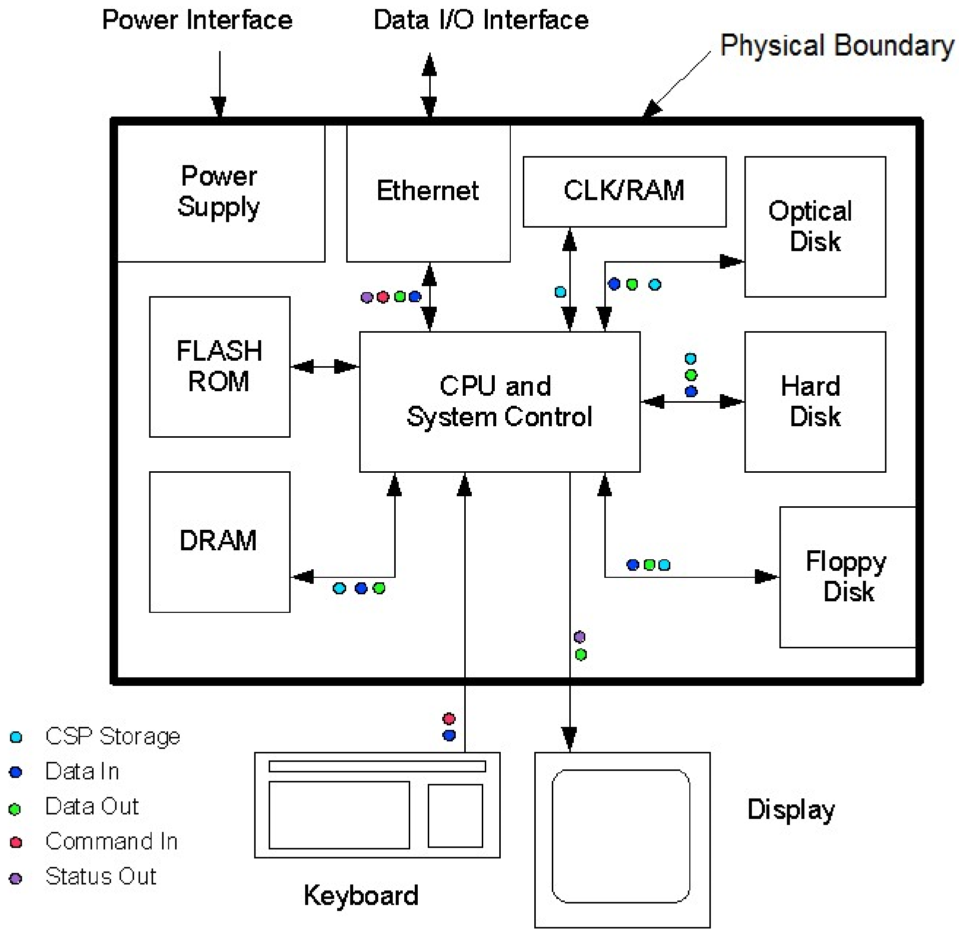

Figure 2 - Hardware Block Diagram

The components within the cryptographic boundary comprising the module are listed as follows:

- Cisco Systems Libreswan Cryptographic Module (version 3.20 and 3.25). This consists of IKE Daemon found at /usr/libexec/ipsec/.
- Fipscheck (version 1.4.1), that includes fipscheck library and application. Fipscheck performs the integrity validation of the IKE Daemon binary.

The following components which act as bound modules need to be installed for the Cisco Systems Libreswan Cryptographic Module to operate:

- The bound module Cisco Systems NSS Module with FIPS 140-2 Certificate #3554 (hereafter referred to as the “NSS module”) provides cryptographic algorithms used by the IKE Daemon. The IKE Daemon uses the NSS module in accordance with the Security Rules stated in the Cisco Systems NSS Module Security Policy.
- The bound module Cisco FIPS Object Module with FIPS 140-2 Certificate #2984 (hereafter referred to as the “FOM module”) provides HMAC SHA-256 algorithm required by fipscheck application and library for integrity check.

2.2 FIPS 140-2 Validation

For the purpose of the FIPS 140-2 validation, the module is a software-only, multi-chip standalone cryptographic module validated at security level 1. The table below shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard.

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1

Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 1 - Security Levels

The module has been tested on the following platforms:

Hardware Platform	**Processor**	**Operating System**
Cisco UCS M4	Intel Xeon E5-2600	CentOS Linux 7.4
Cisco UCS M5	Intel Xeon Bronze	CentOS Linux 7.4

Table 2 – Tested Platforms

The physical boundary is the surface of the case of the target platform. The logical boundary is depicted in Figure 1: software block diagram.

2.3 Modes of Operation

The module only supports the FIPS approved mode and is in FIPS approved mode after initialization and power-on self-tests succeed.

The module verifies its integrity using a HMAC-SHA-256 digest operation and compares the value with the build time pre-computed value. If the digests match, the power-up self-tests are successful.

3 Cryptographic Module Ports and Interfaces

As a software-only module, the module does not have physical ports. For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which it runs.

The logical interfaces through which applications request services are summarized in following table:

Logical interface	Physical Interface	Description
Data input	Ethernet ports of the hardware platform	IKE Network Port/Protocol
Data output	Ethernet ports of the hardware platform	IKE Network Port/Protocol
Control input	Ethernet ports of the hardware platform	IKE Network Port/Protocol, Configuration Files (/etc/ipsec.conf, /etc/ipsec.d/, /etc/ipsec.secrets)
Status output	Ethernet ports of the hardware platform	Log File, IKE Network Port/Protocol

Table 3 – Logical Interfaces

4 Roles, Services and Authentication

4.1 Roles

The module supports the following roles:

- **User role**: performs key derivation and negotiates IKE to establish security association.
- **Crypto Officer role**: performs module installation and configuration, manages IKE Daemon, self tests and show status.

The module is a Security Level 1 software-only cryptographic module and does not implement authentication. The User and Crypto Officer roles are implicitly assumed by the entity accessing the module services. The User role is assumed by the underlying server application that makes calls to the module on behalf of one or more external clients.

4.2 Services

The module supports services available to users in the available roles. All services are described in detail in the user documentation.

The following table shows the available services, the roles allowed ("CO" stands for Crypto Officer and "U" stands for User), the Critical Security Parameters (CSPs) involved and how they are accessed in the FIPS mode.

"R" stands for Read permission, "W" stands for Write permission, "E" stands for execute, and "Z" stands for Zeroization of the module:

Service	Notes	Bound module	Role	CSPs	Access
Install and Configure the module	N/A	N/A	CO	Shared secret	R, W
Manage Pluto IKE Daemon start, stop, etc.	Commands	N/A	CO	Shared secret IKE SA Tunnel Encryption Keys IKE SA Tunnel Integrity Keys IPSEC SA Tunnel Encryption Keys IPSEC SA Tunnel Integrity Keys	R, W
Zeroization	N/A	N/A	CO	Shared secret IKE SA Tunnel Encryption Keys IKE SA Tunnel Integrity Keys IPSEC SA Tunnel Encryption Keys IPSEC SA Tunnel Integrity Keys	Z
Negotiate IKE to establish security associations (SAs)	SP 800-135 Key Derivation Function (KDF) in IKEv1 and IKEv2	N/A Cisco Systems NSS Module Cisco Systems NSS Module	U	Shared secret IKE SA Tunnel Encryption Keys IKE SA Tunnel Integrity Keys IPSEC SA Tunnel Encryption Keys IPSEC SA Tunnel Integrity Keys	R, W, E
Self-tests	N/A	Cisco FIPS Object Module Cisco FIPS Object Module	CO	HMAC SHA-256 keys for integrity check	R, E
Show Status	N/A	N/A	CO	None	N/A

Table 4 – Services available in FIPS mode

Note: Only the SP 800-135 Key Derivation Function has been validated by CAVP.

The following table identifies the applicable CAVP certificates for each algorithm:

Algorithm	Modes/Options	CAVS Cert(s).	Bounded Module
IKE KDF	IKEv1/IKEv2	C84 (CVL)	N/A
SHS	SHA-1 SHA-256 SHA-512	C503	Cisco Systems NSS Module
	SHA-256	C8	Cisco FIPS Object Module

HMAC	HMAC-SHA1 (MAC: 80, 96, 128, 160; KS < BS; KS = BS; KS > BS) HMAC-SHA2-256 (MAC: 128, 192, 256; KS < BS; KS = BS; KS > BS) HMAC-SHA2-384 (MAC: 192, 256, 320, 384; KS < BS; KS = BS; KS > BS) HMAC-SHA2-512 (MAC: 256, 320, 384, 448, 512; KS < BS; KS = BS; KS > BS)	C503	Cisco Systems NSS Module
	HMAC-SHA2-256	C8	Cisco FIPS Object Module

Table 5 – Available Algorithm Modes and CAVP certificates

There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table

4.3 Authentication

The module is a Security Level 1 software-only cryptographic module and does not implement authentication. The role is implicitly assumed based on the service requested.

5 Physical Security

The module is comprised of software only and thus does not claim any physical security.

6 Operational Environment

6.1 Applicability

The module operates in a modifiable operational environment per FIPS 140-2 level 1 specifications. The module runs on a commercially available general-purpose operating system executing on the hardware specified in section 2.2.

6.2 Policy

The operating system is restricted to a single operator (concurrent operators are explicitly excluded). The application that request cryptographic services is the single user of the module, even when the application is serving multiple clients.

In FIPS Approved mode, the ptrace system call, the debugger (gdb), and strace shall be not used.

7 Cryptographic Key Management

The application that uses the module is responsible for appropriate destruction and zeroization of the key material. The library provides functions for key allocation and destruction, which overwrites the memory that is occupied by the key information with "zeros" before it is deallocated.

7.1 CSPs/Keys

The module does not implement any random number generator nor provides key generation. The module only provides key derivation through the implementation of the SP 800-135 KDF.

The table below lists the CSPs/keys used by the module:

Keys/CSPs	Type	Usage	Key Generation	Key Storage	Key Entry/Output	Key Zeroization
Shared secret according to the IKE protocol	Shared secret	Used as part of the IKE derivation process	N/A. This secret is passed to the module.	Ephemeral	IKE Network Port/Protocol	Close of IKE SA
IKE SA Tunnel Encryption Keys	AES 128, 192, and 256 bits	Used by the calling process for IKE tunnel encryption	N/A derived from shared secret by using KDF. The key itself is never used by the module, only derived.	Ephemeral	N/A	Close of IKE SA
IKE SA Tunnel Integrity Keys	HMAC with at least 112-bit keys	Used by the calling process for IKE tunnel integrity	N/A derived from shared secret by using KDF. The key itself is never used by the module, only derived.	Ephemeral	N/A	Close of IKE SA
IPSEC SA Tunnel Encryption Keys	AES 128, 192, and 256 bits	Used by the calling process for IPsec tunnel encryption	N/A derived from shared secret by using KDF. The key itself is never used by the module, only derived.	Ephemeral	N/A	Close of IPSEC SA
IPSEC SA Tunnel Integrity Keys	HMAC with at least 112-bit keys	Used by the calling process for IPsec tunnel integrity	N/A derived from shared secret by using KDF. The key itself is never used by the module, only derived.	Ephemeral	N/A	Close of IPSEC SA
HMAC SHA-256 keys for integrity check	HMAC key 256-bits	Used to provide module integrity	N/A – installed as part of the module	Persistently stored in plaintext	N/A – Key is only used for integrity verification	Overwriting with zeros

Table 6 – Keys/CSPs

7.2 Key / CSP Storage

CSPs are provided to the module by the calling process and are destroyed when released by the appropriate IKE Network Port/Protocol. The module does not perform persistent storage of keys.

7.3 Key / CSP Zeroization

For volatile memory, memset is included in deallocation operations. There are no restrictions when zeroizing any cryptographic keys and CSPs.

8 EMI/EMC

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B, class A. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

9 Self Tests

9.1 Power-Up Tests

The module performs power-up tests at module initialization which includes the software integrity test to ensure that the module is not corrupted. The self-tests are triggered automatically without any user intervention.

While the module is performing the power-up tests, services are not available, and input or output is not possible: the module is single-threaded and will not return to the calling application until the self-tests are completed successfully.

9.1.1 Integrity Tests

The integrity check is performed by the fipscheck application using the HMAC-SHA-256 algorithm implemented by the FOM module. The FOM module computes an HMAC SHA-256 value for the fipscheck utility, as well as all applications forming the Libreswan module.

The integrity verification is performed as follows:

The Libreswan application links with the library libfipscheck.so which is intended to execute fipscheck application to verify the integrity of the Libreswan application file using the HMACSHA-256. Upon calling the FIPSCHECK_verify() function provided with libfipscheck.so, the fipscheck application is loaded and executed, and the following steps are performed:

- Fipscheck loads the FOM module, which performs its own integrity check using the HMAC SHA-256 algorithm;
    - Fipscheck performs the integrity check of its own application file using the HMAC SHA-256 algorithm provided by the FOM module;
- Fipscheck automatically verifies the integrity of libfipscheck.so library before processing requests of calling applications;
- The fipscheck application performs the integrity check of the Libreswan application file as follows:
    - The fipscheck computes the HMAC SHA-256 checksum of the file from the command line and compares the computed value to the stored value.
    - The fipscheck application returns the appropriate exit value based on the comparison result: zero if the checksum is OK, which is enforced by the libfipscheck.so library. Otherwise, an error code will be shown, which puts the module into the error state.

If any of the above steps fails, an error code (a non-zero value) will be returned and the module enters the error state. In Error state, all output is inhibited and no cryptographic operation is allowed. The Module needs to be reinitialized in order to recover from the Error state.

9.1.2 Cryptographic Algorithm Tests

The power-up self-tests for the SP 800-135 KDF are covered by the SHS Known-Answer-Tests (KAT) and HMAC Known-Answer-Tests (KAT) performed by the Cisco Systems NSS Module. If any of the power-up self-tests fail, the Module enters the Error state. In the Error state, all outputs are inhibited and no cryptographic operation is allowed.

9.1.3 Self-Test Summary

In summary, the following self-tests are performed by the module:

- Software integrity test (provided by Cisco FIPS Object Module)
- SHA-1 KAT (Cisco Systems NSS Module)
- SHA-256 KAT (Cisco Systems NSS Module)
- SHA-384 KAT (Cisco Systems NSS Module)
- SHA-512 KAT (Cisco Systems NSS Module)
- HMAC-SHA-1 KAT (Cisco Systems NSS Module)
- HMAC-SHA-256 KAT (Cisco Systems NSS Module)
- HMAC-SHA-384 KAT (Cisco Systems NSS Module)
- HMAC-SHA-512 KAT (Cisco Systems NSS Module)

10 Guidance

The following guidance items are to be used for assistance in maintaining the module's validated status while in use.

10.1 Crypto Officer Guidance

NOTE: All cryptographic functions for the Cisco Systems Libreswan Cryptographic Module will be provided by a copy of a FIPS 140-2 validated version of the NSS module. The FOM module is used to perform integrity verification.

- To start and stop the module, use the (service ipsec) command.
- ikelifetime must not be larger than 1 hour.
- salifetime must not be larger than 1 hour.
- Stopping the module will zeroize the ephemeral CSPs and keys.
- To check FIPS 140-2 module status, read the Pluto debug data using the ipsec_barf command
- Keys are zeroized by closing the associated IKE or IPSec SA. This happens automatically when the SA is closed.

To bring the Module into FIPS approved mode, perform the following:

- Install the dracut-fips package: install dracut-fips
- Recreate the INITRAMFS image: dracut -f

After regenerating the initramfs, the Crypto Officer has to append the following string to the kernel command line by changing the setting in the boot loader: fips=1

10.2 User Guidance

There is no User Guidance as the user role is assumed by the underlying server application that makes calls to the module on behalf of one or more external clients.

10.3 Handling Self-Test Errors

FOM and NSS self-test failures may prevent Libreswan from operating. See the Guidance section in the FOM and NSS Security Policies for instructions on handling FOM or NSS self-test failures.

Power-up self-test errors are non-fatal errors that transition the module into an error state. The application must be restarted or reinstalled to recover from these errors. Libreswan outputs NSS error codes that can be used to determine the cause of the errors. In the case of integrity test failure, Libreswan enters an error state and outputs the following error:

FIPS integrity verification test failed.

The only recovery from this type of failure is to reinstall the Libreswan module.

--- End of Document ---