Cisco CSS Series 11000 Secure Content Accelerator/SonicWALL SSL-RX FIPS 140-2 Security Policy

Level 2

August 12, 2003

Copyright Notice

Table of Contents

Introduction

The Cisco 11000 Series Secure Content Accelerator (SCA)/SonicWALL SSL-RX (hereafter referred to as "the cryptographic module") is a multi-chip standalone cryptographic module. The cryptographic module provides TLS off-loading, from networked web servers. The module accelerates not only RSA operations, but all cryptographic functions including symmetric ciphers, message digests, and random number generation for faster network performance when utilizing these functions. The cryptographic module is used to accelerate TLS transactions in a network environment.

The following is a picture of the module:

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports Interfaces	2
Roles, Services, and Authentication	2
Finite State Machine	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Roles and Services

The cryptographic module provides a User role and a Cryptographic Officer role. The cryptographic module does not provide a Maintenance role.

The User role is called "access-level" in vendor documentation. The User role is authenticated using the access-level password. The User role can query status and non-critical configuration.

User Role Services

- Show Status – monitor, ping, set, show, traceroute
- Show Non-critical Configuration – show
- Session Management – clear, cls, enable, exit, finished, no, paws, quit, terminal
- Self-test Initiation – power cycle

The Cryptographic Officer role is called "enable-level" in vendor documentation. The Cryptographic Officer role is authenticated using the access-level and enable-level password. The Cryptographic Officer role can configure keys, certificates, security policies and TLS servers on the cryptographic module as well query all status and configuration.

Crypto Officer Services

- Create and Configure Keys, Certificates, Security Policies, and TLS Servers – quick-start
- Show Status - monitor, ping, set, show, traceroute
- Update and Show Configuration – configure, copy, erase, fips, refresh, write
- Session Management – clear, cls, disable, enable, exit, finished, no, paws, quit, refresh, terminal
- Self-test Initiation - reload

Separation of roles is enforced by requiring one or more passwords for the roles. The User role requires the use of an access-level password. The Cryptographic Office role requires the use of both the access-level and enable-level passwords. Only one user can access the device at a time using the serial console interface.

The cryptographic module provides several security services. The cryptographic module provides the Cryptographic Officer role the ability to manage private keys, certificates, TLS servers, and both access- and enable-level passwords. The cryptographic module allows the User role to query device and TLS server configuration and status.

When operated in FIPS mode, the cryptographic module provides only FIPS 140-2 compliant services. FIPS mode is entered using the "fips enable" command. When in FIPS mode, the string "[FIPS]" is prepended to the configuration manager prompt. The following cryptographic services are supported in FIPS mode:

- DES CBC-mode (as a legacy algorithm used to be compatible with older systems)
- TDES CBC-mode
- RSA signing and verification
- RSA encryption/decryption (key wrapping, as a part of the TLS transport protocol)

- HMAC-SHA-1
- DRNG – FIPS 186-2, Appendix 3.1 with the SHA-based 'G' function
- NDRNG – Non-FIPS Approved, hardware based

When not operated in FIPS mode, the cryptographic module provides SSL v2 and SSL v3 servers in addition to TLS servers. The cryptographic module also provides the following cryptographic services: RC2, RC4, MD5, and Diffie-Hellman.

The Cryptographic Officer role can load, store and remove private keys and certificates on the cryptographic module. The device supports RSA key/certificate pairs of any length greater than 512 bits.

The Cryptographic Officer role may create, edit, store, and delete TLS servers. TLS servers may be configured using the following cryptographic algorithms:

- DES in CBC mode with SHA-1 message authentication
- 3DES in CBC mode with SHA-1 message authentication
- RSA

Physical Ports and Logical Interfaces

Ethernet Ports and Data Input and Data Output Interfaces

The cryptographic module consists of two 10/100Mbit Ethernet ports. There is a server Ethernet port and a network Ethernet port. The cryptographic module provides data input and output interfaces as defined by the configured TLS servers. TLS servers can be configured to provide plaintext and ciphertext connections using the Ethernet ports.

Serial Ports and Control Input and Status Output Interfaces.

The cryptographic module consists of two RS-232 serial ports. There is a console serial port and an AUX serial port. The console serial port is used for local configuration. The console serial port represents the control input and status output interfaces. There are no services that utilize the AUX serial port by the firmware.

Controls and Status Indicators

The cryptographic module provides dual power supplies. Two power supply indicator lights are used to indicate which power supply is currently in use. One of the power supply indicators is illuminated at any time.

The cryptographic module provides a Test LED which is illuminated during the POST.

The cryptographic module provides the standard Ethernet status indicators. For each Ethernet interface there are Link, Rx, and Tx indicator lights.

Security Rules

The cryptographic module has the following security rules:

- The cryptographic module provides two distinct operator roles: User role and Cryptographic Officer role.
- The cryptographic module provides role-based authentication relying upon passwords. All operators at the User role use the same password. All operators at the Cryptographic Officer rule use the same access- and enable-level passwords.

Passwords must be at least eight characters long. This makes the probability less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur for each attempt. After three successive unsuccessful password verification tries, the cryptographic module pauses for one second before additional password entry attempts can be reinitiated. This makes the probability less than one in 100,000 that a random attempt will succeed or a false acceptance will occur in a one-minute period.

- The following cryptographic algorithm self-tests are performed by the cryptographic module at power-up:
  - Software integrity test (using CRC EDC)
  - DES-CBC Known Answer Test
  - Triple DES-CBC Known Answer Test
  - SHA-1 Known Answer Test
  - HMAC-SHA-1 Known Answer Test
  - RSA Signing and Verification Known Answer Test
  - RSA Encryption and Decryption Known Answer Test
  - Monobit Test for randomness: count the number of ones in the 20,000 bit stream; denote this quantity as X; the cryptographic module passed the test if $9,654 < X < 10,346$.
  - Poker Test for randomness: evaluate ($X = (16 / 5000) * (\text{the sum of } [f(i)^2] \; i = 0 \text{ to } 15) - 5000$); the device passed the test if $1.03 < X < 57.4$.
  - Runs Test for randomness: a 20,000-bit sample stream is evaluated; the test is passed if the intervals between the runs of 1-6 consecutive zeros or ones falls within the following values:
    1: 2,267-2733
    2: 1,079-1,421
    3: 502-748
    4: 223-402
    5: 90-223
    6: + 90-223
  - Long Run Test for randomness: a 20,000-bit sample stream is evaluated; the cryptographic module passes the test if no runs of 34 or more consecutive zeros or ones are found.
- The following conditional tests are performed by the module:
  - Continuous Random Number Generator Test on DRNG and NDRNG.
  - Pairwise consistency test for public/private key pairs.
- When a new firmware image is loaded, the cryptographic module verifies the 256-bit RSA signed SHA-1 hash of the image. If this verification fails, the firmware image loading is aborted.

If any of the tests described above fail, the cryptographic module enters the error state. No security services are provided in the error state. Upon successful completion of the Diagnostic State, the cryptographic module enters the Service Phase. Security services are only provided in the Service State. No TLS servers are started until all tests are successfully completed. This effectively inhibits the data output interface. If all tests are completed successfully, the Configuration Manager presents the password prompt on the serial console.

The RSA implementation is PKCS #1.

The module supports electronic key entry and manual key transport.

Definition of Critical Security Parameters

The following are the Critical Security Parameters (CSP) contained in the cryptographic module:

- Data encryption keys: DES/TDES keys used to encrypt data.
- Public/private key pairs for encryption: RSA key pairs used in TLS process.
- Public/private key pairs for signing: RSA key pairs used for signing.
- DRNG seed keys: seed keys used with the DRNG specified in the FIPS 186-2, Appendix 3.1, with the SHA-based 'G' function.
- DRNG state: the state maintained by the DRNG.
- Authentication information: Passwords used for operator authentication.

Definition of CSP Modes of Access

Table 2 — CSP Modes of Access describes the methods of accessing the individual CSPs. All operations require the user to be in the Cryptographic Officer role.

Table 2 — CSP Modes of Access

Access Method	Public/Private Keys	Data encryption keys	DRNG seed keys and state	Authentication Information
Import/upload	RSA keys can be imported into the cryptographic module.	Data encryption keys are generated on the module, not loaded or imported.	DRNG seed keys and state information can never be imported or uploaded.	No password information can be imported or uploaded from other sources.
Viewing	Keys loaded on the cryptographic module can never be viewed by the operator.	Data encryption keys cannot be viewed by the operator.	DRNG seed keys and state information can never be viewed.	Passwords can never be viewed by the user. When passwords are entered for configuration or verification, they are not viewable on the monitor.
Download	Keys loaded on the cryptographic module can never be downloaded.	Data encryption keys cannot be downloaded.	DRNG seed keys and state information can never be downloaded.	Passwords can never be downloaded.

Access Method	Public/Private Keys	Data encryption keys	DRNG seed keys and state	Authentication Information
Removal/deletion	Keys loaded on the cryptographic module can be deleted by the commands described in the previous section, or when the "FailSafe" password is used, as described in the user guidance, all private key information is deleted.	Data encryption keys can be deleted by the commands described in the previous section, or when the "FailSafe" password is used, as described in the user guidance, all private key information is deleted.	DRNG seed keys and state can be deleted by the commands described in the previous section, or when the "FailSafe" password is used, as described in the user guidance, all private key information is deleted	Passwords are deleted when new ones are configured or when the "FailSafe" password is used, all password information is deleted.

Table 3—Operator/Role Matrix presents the valid roles for any operator of the cryptographic module.

Table 3—Operator/Role Matrix

Operator	Roles	
Any operator	User Role, with appropriate password	Cryptographic Officer Role, with appropriate passwords

Table 4—Role/Services Matrix displays the cryptographic module services appropriate for each user role.

Table 4—Role/Services Matrix

Role	Service
User Role	Query device statistics and basic configuration
Cryptographic Officer Role	Manage private keys, certificates, TLS servers, access- and enable-level passwords, and device configuration

Cryptographic Boundary

The Cryptographic Boundary includes the entire device.

The components that are included within the Cryptographic Boundary are displayed in the Functional Block Diagram.

Physical Security

The entire module is encased in within an opaque, metal enclosure that is not intended to be opened. The module provides tamper evidence by means of tamper evident labels applied on the lower edge of the side of the enclosure. The location of the tamper evident labels is indicated with the arrow below:

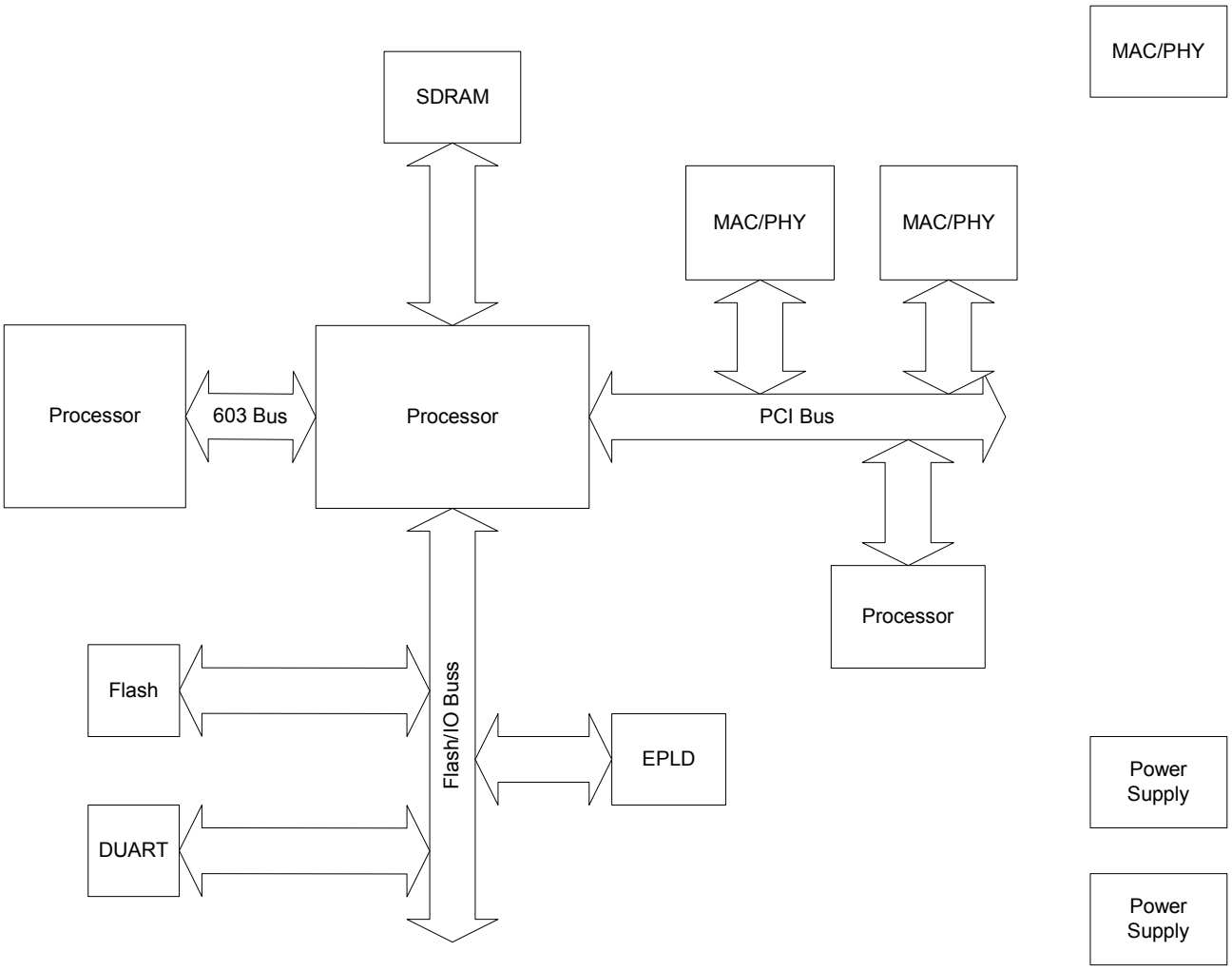
Initialization of the Module

The cryptographic module enters this state when power is first applied to the module. The module performs processor, memory management unit, internal peripheral, and security feature initialization necessary prior to operation of the module.

The module prompts the operator for the password the first time it is initialized. The operator must configure a password to be used to access the module in the future. This procedure must be completed to enter the Crypto Officer role and configure any of the cryptographic parameters on the module.

The cryptographic module will not provide any Cryptographic Officer or User services in this state.

Functional Block Diagram



All CSP's are stored in NVRAM. All CSP's are used by TLS servers and the configuration manager in the CPU and RAM. CSP's are never used by the Ethernet interfaces (MAC/PHY's). The Ethernet interfaces pass TLS traffic as required by the TLS servers.

The Power Supplies provide power to all components.

The third MAC/PHY is not used in the stand-alone implementation.

