



Cisco Firepower Management Center (FMC) Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy Level 1 Validation

Version 0.3

April 28, 2017

Table of Contents

| | | |
|----------|---|-----------|
| 1 | INTRODUCTION | 3 |
| 1.1 | PURPOSE | 3 |
| 1.2 | MODULE VALIDATION LEVEL | 3 |
| 1.3 | REFERENCES | 3 |
| 1.4 | TERMINOLOGY | 4 |
| 1.5 | DOCUMENT ORGANIZATION..... | 4 |
| 2 | CISCO FIREPOWER MANAGEMENT CENTER..... | 5 |
| 2.1 | CRYPTOGRAPHIC MODULE CHARACTERISTICS | 5 |
| 2.2 | CRYPTOGRAPHIC BOUNDARY | 5 |
| 2.3 | MODULE INTERFACES | 6 |
| 2.4 | APPLIANCE FS750, FS1500, FS2000, FS3500 AND FS4000 OVERVIEW | 7 |
| | 750 Front View | 7 |
| | 750 Rear View | 7 |
| | 1500 Front View | 8 |
| | 1500 Rear View | 9 |
| | 3500 Front View | 10 |
| | 3500 Rear View | 10 |
| | 2000 and 4000 Front View | 11 |
| | 2000 and 4000 Rear View..... | 11 |
| 2.5 | ROLES AND SERVICES | 12 |
| 2.6 | USER SERVICES | 12 |
| 2.7 | CRYPTO OFFICER SERVICES | 13 |
| 2.8 | NON-FIPS MODE SERVICES | 13 |
| 2.9 | UNAUTHENTICATED SERVICES..... | 14 |
| 2.10 | CRYPTOGRAPHIC KEY/CSP MANAGEMENT | 14 |
| 2.11 | CRYPTOGRAPHIC ALGORITHMS | 17 |
| | Approved Cryptographic Algorithms | 17 |
| | Non-FIPS Approved Algorithms Allowed in FIPS Mode | 17 |
| | Non-Approved Cryptographic Algorithms | 18 |
| 2.12 | SELF-TESTS..... | 18 |
| 3 | SECURE OPERATION..... | 19 |
| 3.1 | CRYPTO OFFICER GUIDANCE - SYSTEM INITIALIZATION/CONFIGURATION | 19 |

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for the Cisco Firepower Management Center (FMC) Cryptographic Module running firmware version 6.1, referred to in this document as Firepower Management Center (FMC). This security policy describes how this module meets the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation. This Security Policy may be freely distributed.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/groups/STM/index.html>.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

| No. | Area Title | Level |
|-----|---|----------|
| 1 | Cryptographic Module Specification | 1 |
| 2 | Cryptographic Module Ports and Interfaces | 1 |
| 3 | Roles, Services, and Authentication | 3 |
| 4 | Finite State Model | 1 |
| 5 | Physical Security | 1 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key management | 1 |
| 8 | Electromagnetic Interface/Electromagnetic Compatibility | 1 |
| 9 | Self-Tests | 1 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |
| | Overall module validation level | 1 |

Table 1 Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Firepower Management Center Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2IG and additional rules imposed by Cisco Systems, Inc. More information is available from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following websites:

<http://www.cisco.com/c/en/us/products/index.html>

<http://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html>

<http://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html>

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Firepower Management Center Cryptographic Module is referred to as Cisco Firepower Management Center Cryptographic Module, Cisco Firepower Management Center CM, FMC Module, Module, CM or the System.

1.5 Document Organization

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

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco Firepower Management Center Cryptographic Module identified in section 1.1 above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco Firepower Management Center

The Firepower Management Center provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection, easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks.

The Management Center is the centralized point for event and policy management for the following solutions:

- Cisco Firepower Next-Generation Firewall (NGFW)
- Cisco ASA with FirePOWER Services
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Advanced Malware Protection (AMP)

The Firepower Management Center aggregates and correlates network traffic information and performance data, assessing the impact of events on particular hosts. You can monitor the information that your device reports, and assess and control the overall activity that occurs on your network. The FMC also controls the network management features on your devices: switching, routing and NAT.

There are five Cisco Firepower Management Center models. Each model varies in terms of how many devices they can manage, how many events they can store and how many hosts and users they can monitor. Choice is based on the number of sensor appliances to be monitored (both physical and virtual), the number of hosts in the environment, and the anticipated security events rate.

Firepower Management Center with the Firepower Management Center Cryptographic Module running on the Fire Linux OS is self-contained and identified as Firepower Management Center providing TLSv1.2 and SSHv2 services. Firepower Management Center runs on the following platforms:

| Cisco Management Center (Hardware) Appliances | | |
|---|----------------------------|---|
| Platform Part Number | Max number sensors managed | Product Description |
| FS750-K9 | 10 | Cisco FireSIGHT Management Center 750 Chassis, 1RU |
| FS1500-K9 | 35 | Cisco FireSIGHT Management Center 1500 Chassis, 1RU |
| FS2000-K9 | 70 | Cisco FireSIGHT Management Center 2000 Chassis, 1RU |
| FS3500-K9 | 150 | Cisco FireSIGHT Management Center 3500 Chassis, 1RU |
| FS4000-K9 | 300 | Cisco FireSIGHT Management Center 4000 Chassis, 1RU |

Table 1: Firepower Appliances

2.1 Cryptographic Module Characteristics

The Cisco Firepower Management Center Cryptographic Module is contained in Firepower Management Center on a non-modifiable Fire Linux OS 6.1.

2.2 Cryptographic Boundary

The Cisco Firepower Management Center CM is a multi-chip standalone crypto module running on FS750, FS1500, FS2000, FS3500 and FS4000 appliances. The cryptographic boundary is defined as-the entire modules' chassis unit encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case.

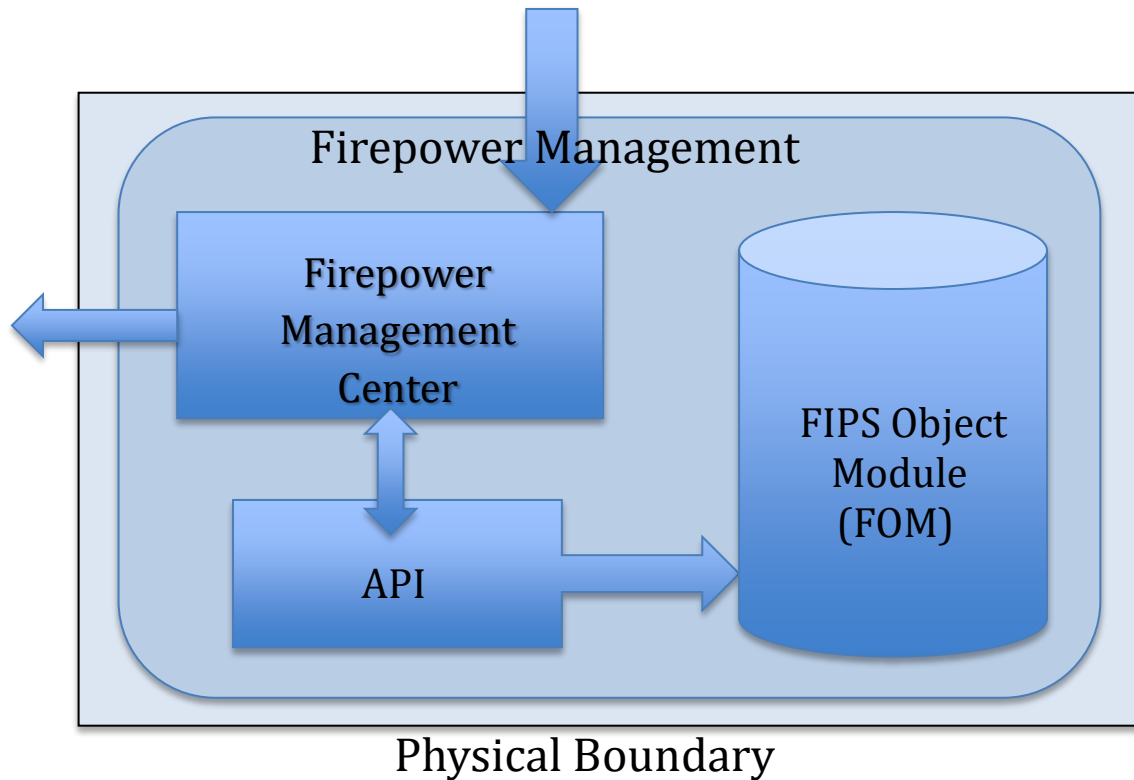


Diagram 1 Firepower Management Center Block Diagram

2.3 Module Interfaces

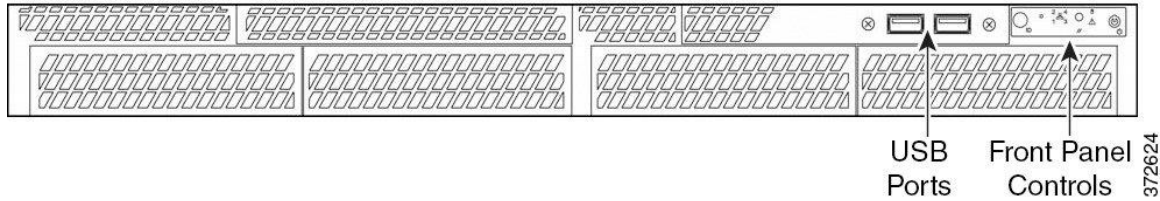
The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following table:

| FIPS 140-2 Logical Interface | FS750/1500/2000/3500/4000 |
|------------------------------|--|
| Data Input | USB ports Serial port VGA port Ethernet ports |
| Data Output | USB ports Serial port VGA port Ethernet ports |
| Control Input | USB ports Serial port Ethernet ports |
| Status Output | USB ports Serial port VGA port Ethernet ports LEDs |

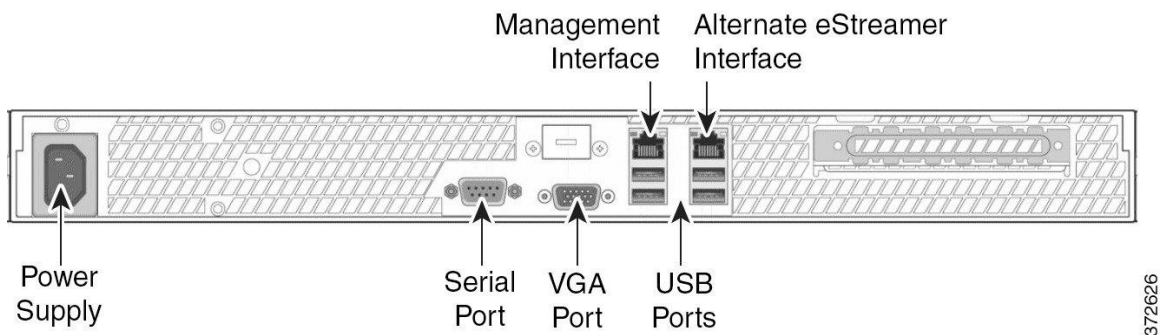
Table 2 Hardware/Physical Boundary Interfaces

2.4 Appliance FS750, FS1500, FS2000, FS3500 and FS4000 overview

750 Front View

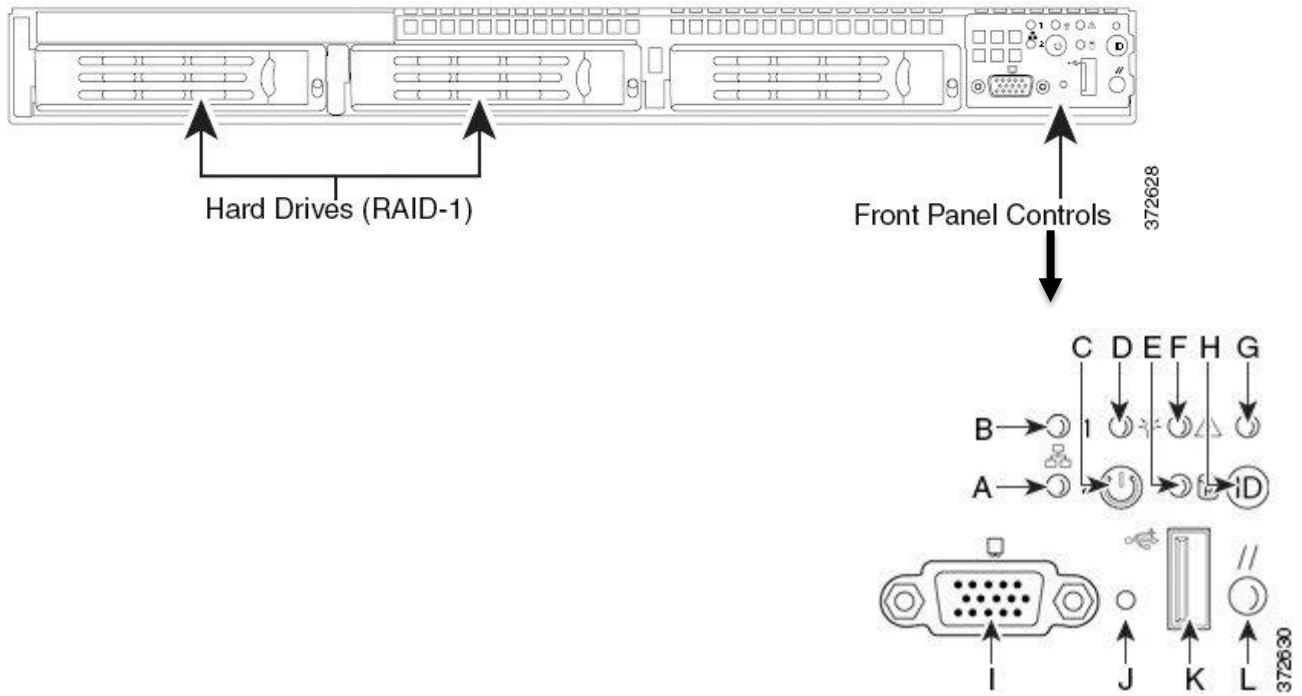


750 Rear View



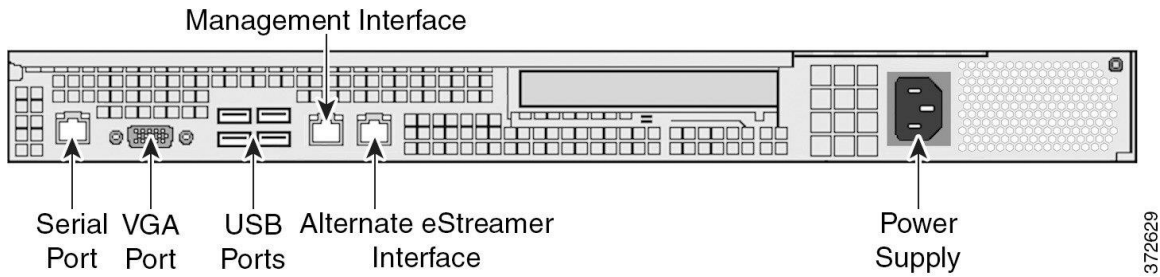
| Feature | Description |
|---|---|
| Front Control Panel | LED (NIC activity, Drive status, system status, power), Interrupt button, Reset button, Power button |
| Power supply | Provides power to the Management Center through an AC power source. |
| VGA port, USB ports | Allows attachment of a monitor, keyboard, and mouse to the device. |
| Serial port | Allows establishment of a direct workstation-to-appliance connection for direct access to all of the management services on the appliance. The serial port is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| 10/100/1000Mbps Ethernet management interface | Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| Alternate eStreamer interface | Provides an alternate interface for the eStreamer client. |

1500 Front View



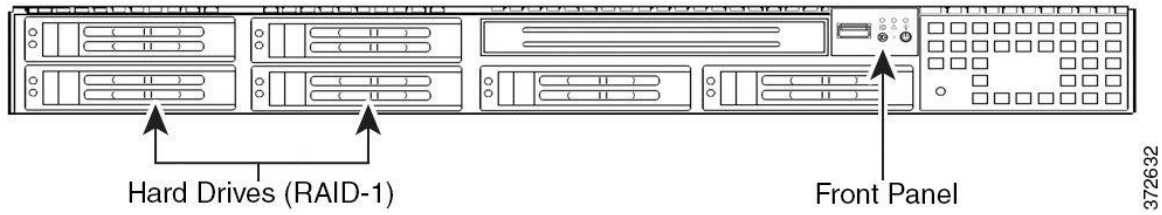
| | | | |
|---|-------------------------|---|---------------------------------|
| A | NIC 2 activity LED | G | ID LED |
| B | NIC 1 activity LED | H | ID button |
| C | Power button | I | Video connector (not available) |
| D | Power/sleep LED | J | Non-maskable interrupt button |
| E | Fixed disk drive status | K | USB 2.0 connector |
| F | System status LED | L | Reset button |

1500 Rear View



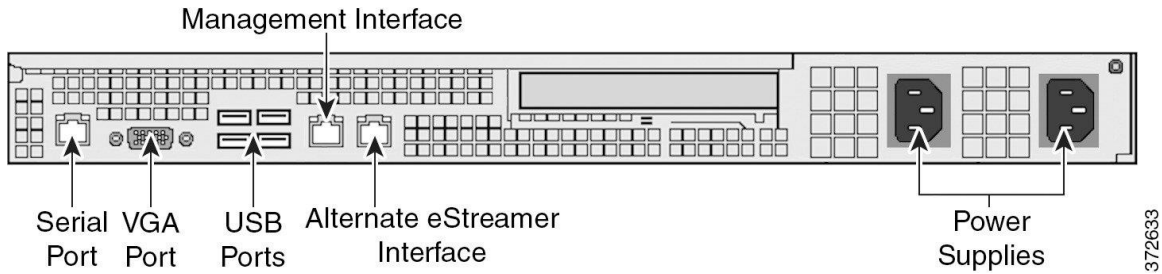
| Feature | Description |
|---|---|
| Hard Drives | 2 Removable hard drives, (RAID-1) |
| Front Panel Control | LED (NIC activity, Drive status, system status, power), Interrupt button, Reset button, Power button, USB (not in use) |
| Power supply | Provides power to the Management Center through an AC power source. |
| VGA port USB ports | Allows attachment of a monitor, keyboard, and mouse to the Management Center. |
| Serial port | Allows establishment of a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the appliance. The serial port is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| 10/100/1000Mbps Ethernet management interface | Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| Alternate eStreamer interface | Provides an alternate interface for the eStreamer client. |

3500 Front View



372632

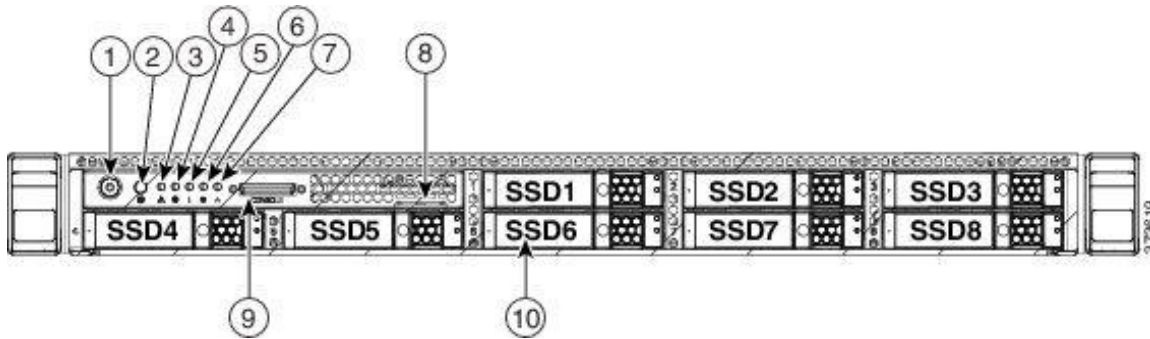
3500 Rear View



372633

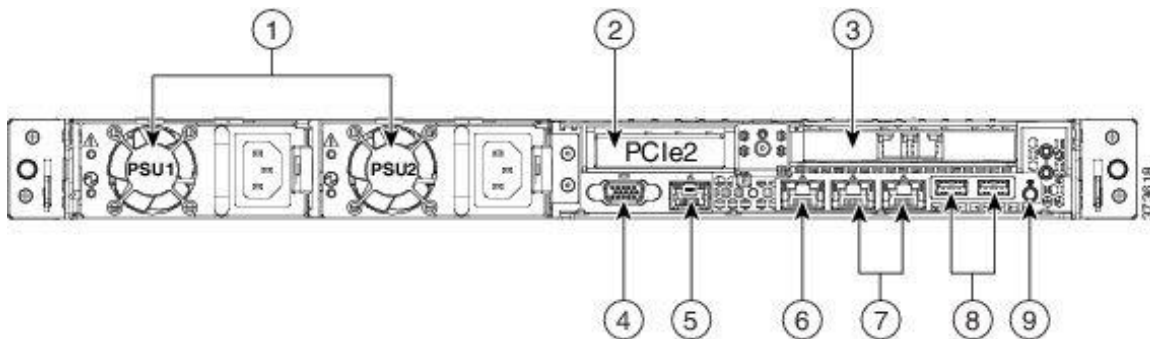
| Feature | Description |
|---|---|
| Hard Drives | 4 Removable hard drives, (RAID-1) |
| Front Panel Control | LED (NIC activity, Drive status, system status, power), Interrupt button, Reset button, Power button, USB (not in use) |
| VGA port USB ports | Allows attachment of a monitor, keyboard, and mouse to the Management Center. |
| Serial port | Allows establishment of a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the appliance. The serial port is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| 10/100/1000Mbps Ethernet management interface | Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes only and is not intended to carry service traffic. |
| Alternate eStreamer interface | Provides an alternate interface for the eStreamer client. |
| Redundant power supplies | Provides power to the appliance through an AC power source. |

2000 and 4000 Front View



| | | | |
|---|-------------------------------|----|--|
| 1 | Power button/Power status LED | 6 | Supply status LED |
| 2 | Power button/Power status LED | 7 | Network link activity LED |
| 3 | System status LED | 8 | Pull-out asset tag |
| 4 | Fan status LED | 9 | KVM connector (used with KVM cable that provides two USB, one VGA, and one serial connector) |
| 5 | Temperature status LED | 10 | Drives, hot-swappable (up to eight 2.5-inch drives) |

2000 and 4000 Rear View



| | | | |
|---|--|---|---|
| 1 | Power supplies (two) | 6 | 1Gb Ethernet default management interface |
| 2 | Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane) | 7 | Dual 1-Gb Ethernet ports (LAN1 and LAN2) |
| 3 | Dual 10-Gb Ethernet ports | 8 | USB ports |
| 4 | VGA video connector | 9 | Rear Identification button/LED |
| 5 | Serial port (RJ-45 connector) | | – |

2.5 Roles and Services

The appliances can be accessed in one of the following ways:

- SSH v2
- HTTPS/TLS

Authentication is identity-based. Each user is authenticated by the module upon initial access to the module. As required by FIPS 140-2, there are two roles in the security appliances that operators may assume: Crypto Officer role and User role. The administrator of the security appliances assumes the Crypto Officer role in order to configure and maintain the module using Crypto Officer services, while the Users exercise only the basic User services.

The User and Crypto Officer passwords and all shared secrets must each be at a minimum eight (8) characters long. There must be at least one special character and at least one number character (enforced procedurally) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing $94 \times 93 \times 92 \times 91 \times 90 \times 89 \times 32 \times 10$. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 8.65×10^{31} attempts per second, which far exceeds the operational capabilities of the module to support.

2.6 User Services

A User enters the system by accessing the console port using either Serial Console, SSH or HTTPS/TLS. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an HTTPS/TLS session. This session is authenticated using RSA digital signature authentication mechanism. The services available to the User role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

| Services | Description | Keys/CSPs Access |
|-----------------------|---|--|
| Status Functions | View state of interfaces and protocols, version of FMC | Operator password (r, w, d) |
| Terminal Functions | Adjust the terminal session (e.g., lock the terminal, adjust flow control). | Operator password (r, w, d) |
| Directory Services | Display directory of files kept in flash memory. | Operator password (r, w, d) |
| Self-Tests | Execute the FIPS 140 start-up tests on demand. | N/A |
| SSH Functions | Negotiation and encrypted data transport via SSH. | Operator password, DH private DH public key, DH Shared Secret, ECDH private ECDH public key, ECDH Shared Secret, SSH RSA private key, SSH RSA public key, SSH session key, DRBG Seed, DRBG entropy input, DRBG V, DRBG Key (r, w, d) |
| HTTPS Functions (TLS) | Negotiation and encrypted data transport via HTTPS | ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS traffic keys DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d) |

Table 3 User Services

2.7 Crypto Officer Services

The Crypto Officer (CO) role is responsible for the configuration and maintenance of the security. The services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

| Services | Description | Keys/CSPs Access |
|--------------------------|---|---|
| Configure the Security | Define network interfaces and settings, create command aliases, set the protocols the module will support, enable interfaces and network services, set system date and time, and load authentication information. | ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS traffic keys, DRBG Seed, DRBG entropy input, DRBG V, DRBG Key (r, w, d) |
| Define Rules and Filters | Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction. | Operator password, Enable password (r, w, d) |
| View Status Functions | View the module configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status. | Operator password, Enable password (r, w, d) |
| HTTPS/TLS (TLS v1.2) | Configure HTTPS/TLS parameters, provide entry and output of CSPs. | ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS traffic keys, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d) |
| SSH v2 | Configure SSH v2 parameter, provide entry and output of CSPs. | DH private DH public key, DH Shared Secret, ECDH private ECDH public key, ECDH Shared Secret, SSH RSA private key, SSH RSA public key, SSH session key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d) |
| Self-Tests | Execute the FIPS 140 start-up tests on demand | N/A |
| User services | The Crypto Officer has access to all User services. | Operator password (r, w, d) |
| Zeroization | Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 7, Zeroization column. | All CSPs (d) |

Table 4 Crypto Officer Services

2.8 Non-FIPS mode Services

The cryptographic module in addition to the above listed FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the Non-Approved services in Section 2.8, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

| Services ¹ | Non-Approved Algorithms |
|-----------------------|--|
| SSH | Hashing: MD5, MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman |
| TLS | Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman |

Table 5 Non-approved algorithms in the Non-FIPS mode services

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

All services available can be found at <http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60.pdf>. This site lists all configuration guides.

2.9 Unauthenticated Services

The services for someone without an authorized role are to view the status output from the module's LED pins and cycle power.

2.10 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the

Crypto Officer role login, and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual distribution are used for pre-shared keys whereas protocols such as TLS and SSH are used for electronic distribution.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the password. The Crypto Officer needs to be authenticated to store keys. Only an authenticated Crypto Officer can view the keys. All Diffie-Hellman (DH)/ECDH keys agreed upon for individual tunnels are directly associated with that specific tunnel. RSA public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them. The /dev/urandom device extracts bits from the urandom pool. This output is used directly to seed the NIST SP 800-90A CTR_DRBG.

| Name | CSP Type | Size | Description/Generation | Storage | Zeroization |
|--------------------|--------------------|----------|--|------------------|------------------------|
| DRBG entropy input | SP800-90A CTR_DRBG | 384-bits | This is the entropy for SP 800-90A CTR_DRBG. Software based entropy source used to construct seed. | DRAM (plaintext) | Power cycle the device |

¹ These approved services become non-approved when using any non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

| Name | CSP Type | Size | Description/Generation | Storage | Zeroization |
|---------------------------------|-----------------------|--------------------------------|--|----------------------|-----------------------------|
| DRBG Seed | SP800-90A CTR_DRBG | 384-bits | Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from software-based entropy source. | DRAM (plaintext) | Power cycle the device |
| DRBG V | SP800-90A CTR_DRBG | 128-bits | The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function. | DRAM (plaintext) | Power cycle the device |
| DRBG Key | SP800-90A CTR_DRBG | 256-bits | Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG. | DRAM (plaintext) | Power cycle the device |
| Diffie-Hellman Shared Secret | DH | 2048, 3072, 4096 bits | The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement. | DRAM (plaintext) | Power cycle the device |
| Diffie Hellman private key | DH | 224, 256, or 379 bits | The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG. | DRAM (plaintext) | Power cycle the device |
| Diffie Hellman public key | DH | 2048, 3072, 4096 bits | The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement. | DRAM (plaintext) | Power cycle the device |
| EC Diffie-Hellman Shared Secret | EC DH | Curves: P-256, P-384, P-521 | The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol. | DRAM (plaintext) | Power cycle the device |
| EC Diffie Hellman private key | EC DH | Curves: P-256, P-384, P-521 | The private key used in EC Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG. | DRAM (plaintext) | Power cycle the device |
| EC Diffie Hellman public key | EC DH | Curves: P-256, P-384, P-521 | The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement. | DRAM (plaintext) | Power cycle the device |
| Operator password | Password | 8 plus characters | The password of the User role. This CSP is entered by the User. | NVRAM (plaintext) | Overwrite with new password |

| Name | CSP Type | Size | Description/Generation | Storage | Zeroization |
|-----------------------|---|---|--|---------------------------------------|--|
| Enable password | Password | 8 plus characters | The password of the CO role. This CSP is entered by the Crypto Officer. | NVRAM (plaintext) | Overwrite with new password |
| SSHv2 RSA Private Key | RSA | 2048 bits | The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG. | DRAM (plaintext) | Automatically when SSH session is terminated |
| SSHv2 RSA Public Key | RSA | 2048 bits | The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module. | DRAM (plaintext) | Automatically when SSH session is terminated |
| SSHv2 Session Key | Triple-DES/AES | 192 bits Triple-DES or 128/192/256 bits AES | This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH). | DRAM (plaintext) | Automatically when SSH session is terminated |
| ECDSA private key | ECDSA | Curves: P-256, P-384, P-521 | Key pair generation, signature generation/Verification. Used in HTTPS connections. This key is generated by calling SP 800-90A DRBG. | DRAM (plaintext) | Automatically when TLS session is terminated |
| ECDSA public key | ECDSA | Curves: P-256, P-384, P-521 | Key pair generation, signature generation/Verification. This key is generated by calling SP 800-90A DRBG. | DRAM (plaintext) | Automatically when TLS session is terminated |
| TLS RSA private key | RSA | 2048 bits | Identity certificates for the security appliance itself and also used in TLS negotiations. This key was generated by calling FIPS approved DRBG. | DRAM (plaintext) NVRAM (plaintext) | Automatically when TLS session is terminated |
| TLS RSA public key | RSA | 2048 bits | Identity certificates for the security appliance itself and also used in TLS negotiations. This key was generated by calling FIPS approved DRBG. | DRAM (plaintext) | Automatically when TLS session is terminated |
| TLS pre-master secret | Shared Secret | At least eight characters | Shared secret created/derived using asymmetric cryptography from which new HTTPS session keys can be created. This key entered into the module in cipher text form, encrypted by RSA public key. | DRAM (plaintext) | Automatically when TLS session is terminated |
| TLS traffic keys | Triple-DES/AES/AES-GCM128/192/256 HMAC-SHA1/256/384/512 | 192 bits Triple-DES or 128/192/256 bits AES | Used in HTTPS connections. Generated using TLS protocol. This key was derived in the module. | DRAM (plaintext) | Automatically when TLS session is terminated |

| Name | CSP Type | Size | Description/Generation | Storage | Zeroization |
|--------------------|--------------|----------|--|---|--|
| Integrity test key | HMAC SHA-512 | 512 bits | A hard coded key used for firmware power-up/load integrity verification. | Hard coded for firmware integrity testing | Zeroized by erase flash (or replacing), write to startup config, followed by a module reboot |

Table 6 Cryptographic Keys and CSPs

2.11 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm implementations:

| Algorithms | Algorithm Implementations Cisco FMC FOM |
|---|--|
| AES (128/192/256 CBC, GCM) | 4266 |
| Triple-DES (CBC, 3-key) | 2307 |
| SHS (SHA-1/256/384/512) | 3512 |
| HMAC (SHA-1/256/384/512) | 2811 |
| RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits) | 2297 |
| ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521) | 995 |
| DRBG (AES256_CTR) | 1337 |
| CVL Component (TLS, SSH) | 1008 |

Table 7 Approved Cryptographic Algorithms and Associated Certificate Number

Note:

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module uses basically a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.
- 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.
- The SSH and TLS protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 of encryption strength)
- NDRNG
- HMAC MD5 is allowed in FIPS mode strictly for TLS

- MD5 is allowed in FIPS mode strictly for TLS

Non-Approved Cryptographic Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- DES
- Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- HMAC MD5
- HMAC-SHA1 is not allowed with key size under 112-bits
- MD5
- RC4
- RSA (key wrapping; non-compliant less than 112 bits of encryption strength)

Note: The non-approved algorithms HMAC MD5 and MD5 are not allowed in FIPS mode when not used with TLS.

2.12 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly.

Self-tests performed

- POST tests
 - AES Known Answer Test (Separate encrypt and decrypt)
 - AES-GCM Known Answer Test (Separate encrypt and decrypt)
 - DRBG Known Answer Test (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
 - FIPS 186-4 ECDSA Sign/Verify Test
 - HMAC Known Answer Tests
 - HMAC-SHA1 Known Answer Test
 - HMAC-SHA256 Known Answer Test
 - HMAC-SHA384 Known Answer Test
 - HMAC-SHA512 Known Answer Test
 - FIPS 186-4 RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
 - SHA-1 Known Answer Test
 - Firmware Integrity Test (HMAC-SHA512)
 - Triple-DES Known Answer Tests (Separate encrypt and decrypt)
- Conditional tests
 - RSA pairwise consistency test (encrypt/decrypt and sign/verify)
 - ECDSA pairwise consistency test
 - CRNGT for SP800-90A DRBG
 - CRNGT for NDRNG

The security appliances perform all power-on self-tests automatically when the power is applied. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the security module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a security module reboot.

3 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Crypto Officer Guidance - System Initialization/Configuration

The Cisco Firepower Cryptographic Module version 6.1 was validated with Cisco Firepower Management Center. The software installation version Sourcefire_Defense_Center_S3-6.1.0-330-Restore.iso and the patch file Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh are the only allowable images for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following steps:

Step 1: For all Management Centers, the setup process must be completed by logging into the Management Center's web interface and specifying initial configuration options on a setup page. The administrator password must be changed, specifying network settings if not already completed, and accepting the EULA.

Log in using admin as the username and Admin123 as the password. Change the password - use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

After completing the initial setup, the only user on the system is the admin user, which has the Administrator role and access.

Step 2: Choose System > Configuration (*Choose SSH, HTTPS or a combination of these options to specify which ports you want to enable for these IP addresses*). For more details, see http://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/system_configuration.html#ID-2241-00000370

Step 3: System>Licenses>Smart Licenses, add and verify licenses (*Firepower Management Center Configuration Guide provides more detailed information*)

Install Triple-DES/AES SMART license to use Triple-DES and AES (for data traffic and SSH).

Step 4: System > Configuration; Devices > Platform Settings; STIG Compliance, choose Enable STIG Compliance; Click on save

Step 5: system reboot; Reboot the security appliances. After reboot, the system is in FIPS mode of operation.