



Cisco Systems, Inc.

Cisco Secure Firewall Threat Defense Cryptographic Module (FPR 4200 Series)

FIPS 140-3 Non-Proprietary Security Policy

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2021-2025 Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Table of Contents

| | |
|--|----|
| 1 General | 4 |
| 1.1 Overview | 4 |
| 1.2 Security Levels | 5 |
| 2 Cryptographic Module Specification | 5 |
| 2.1 Description | 5 |
| 2.2 Tested and Vendor Affirmed Module Version and Identification | 6 |
| 2.3 Excluded Components | 7 |
| 2.4 Modes of Operation | 7 |
| 2.5 Algorithms | 7 |
| 2.6 Security Function Implementations | 10 |
| 2.7 Algorithm Specific Information | 15 |
| 2.8 RBG and Entropy | 16 |
| 2.9 Key Generation | 16 |
| 2.10 Key Establishment | 17 |
| 2.11 Industry Protocols | 17 |
| 3 Cryptographic Module Interfaces | 17 |
| 3.1 Ports and Interfaces | 17 |
| 4 Roles, Services, and Authentication | 18 |
| 4.1 Authentication Methods | 18 |
| 4.2 Roles | 20 |
| 4.3 Approved Services | 20 |
| 4.4 Non-Approved Services | 39 |
| 4.5 External Software/Firmware Loaded | 39 |
| 4.6 Cryptographic Output Actions and Status | 39 |
| 4.7 Additional Information | 39 |
| 5 Software/Firmware Security | 39 |
| 5.1 Integrity Techniques | 39 |
| 5.2 Initiate on Demand | 39 |
| 6 Operational Environment | 40 |
| 6.1 Operational Environment Type and Requirements | 40 |
| 7 Physical Security | 40 |
| 7.1 Mechanisms and Actions Required | 40 |
| 7.2 User Placed Tamper Seals | 40 |
| 7.3 Filler Panels | 43 |
| 8 Non-Invasive Security | 44 |

| | |
|--|----|
| 9 Sensitive Security Parameters Management..... | 44 |
| 9.1 Storage Areas | 44 |
| 9.2 SSP Input-Output Methods..... | 45 |
| 9.3 SSP Zeroization Methods..... | 46 |
| 9.4 SSPs | 46 |
| 9.5 Transitions..... | 62 |
| 10 Self-Tests..... | 63 |
| 10.1 Pre-Operational Self-Tests | 63 |
| 10.2 Conditional Self-Tests..... | 63 |
| 10.3 Periodic Self-Test Information..... | 68 |
| 10.4 Error States | 71 |
| 11 Life-Cycle Assurance | 71 |
| 11.1 Installation, Initialization, and Startup Procedures..... | 71 |
| 11.2 Administrator Guidance | 73 |
| 11.3 Non-Administrator Guidance..... | 73 |
| 12 Mitigation of Other Attacks | 73 |

List of Tables

| | |
|---|----|
| Table 1: Security Levels | 5 |
| Table 2: Tested Module Identification – Hardware | 6 |
| Table 3: Modes List and Description | 7 |
| Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation..... | 9 |
| Table 5: Approved Algorithms - Nitrox-V GC | 9 |
| Table 6: Vendor-Affirmed Algorithms | 9 |
| Table 7: Security Function Implementations..... | 15 |
| Table 8: Entropy Certificates | 16 |
| Table 9: Entropy Sources..... | 16 |
| Table 10: Ports and Interfaces | 18 |
| Table 11: Authentication Methods | 20 |
| Table 12: Roles..... | 20 |
| Table 13: Approved Services | 39 |
| Table 14: Mechanisms and Actions Required | 40 |
| Table 15: Storage Areas | 45 |
| Table 16: SSP Input-Output Methods..... | 46 |
| Table 17: SSP Zeroization Methods..... | 46 |
| Table 18: SSP Table 1 | 53 |
| Table 19: SSP Table 2..... | 62 |
| Table 20: Pre-Operational Self-Tests | 63 |
| Table 21: Conditional Self-Tests | 68 |
| Table 22: Pre-Operational Periodic Information..... | 68 |
| Table 23: Conditional Periodic Information..... | 71 |
| Table 24: Error States | 71 |

List of Figures

| | |
|--|----|
| Figure 1 FPR 4215, 4225, 4245 | 6 |
| Figure 2. FPR-4200 Front view | 41 |
| Figure 3. FPR-4200 Back view..... | 41 |
| Figure 4. FPR-4200 Left view..... | 41 |
| Figure 5. FPR-4200 Right view | 41 |
| Figure 6. FPR-4200 Bottom view | 42 |
| Figure 7. FPR-4200 Top view | 42 |
| Figure 8 Opacity Shield Brackets | 44 |

1 General

1.1 Overview

This is Cisco Systems, Inc. non-proprietary security policy for the Cisco Secure Firewall Threat Defense Cryptographic Module (FPR 4200 Series) (hereinafter referred to as FTD or Module), version 7.4. The following details how this module meets the security requirements of FIPS 140-3, SP 800-140 and ISO/IEC 19790 for a Security Level 2 hardware cryptographic module.

The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. The following table indicates the actual security levels for each area of the cryptographic module.

1.2 Security Levels

| Section | Title | Security Level |
|---------|---|----------------|
| 1 | General | 2 |
| 2 | Cryptographic module specification | 2 |
| 3 | Cryptographic module interfaces | 2 |
| 4 | Roles, services, and authentication | 3 |
| 5 | Software/Firmware security | 2 |
| 6 | Operational environment | N/A |
| 7 | Physical security | 2 |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 2 |
| 10 | Self-tests | 2 |
| 11 | Life-cycle assurance | 2 |
| 12 | Mitigation of other attacks | N/A |
| | Overall Level | 2 |

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

This module is a multi-chip standalone hardware cryptographic module identified as Firewall Threat Defense (FTD) which houses ASA and Firepower solutions with underlying operating system identified as Linux 4 (also referred to as Firepower eXtensible Operating System or FX-OS throughout this document). The module is operated in a limited operational environment.

FTD delivers enterprise-class firewall for businesses, improving security at the Internet edge, high performance and throughput for demanding enterprise data centers. The FTD solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security and secure unified communications, HTTPS/TLSv1.2, SSHv2, IPsec/IKEv2, SNMPv3 and Cryptographic Cipher Suite B using the ASA Cryptographic Module.

Module Type: Hardware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The Tested Operational Environment Physical Perimeter (TOEPP) is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case as shown in the figures below and in the Physical Security section. The cryptographic boundary encompasses the entire TOEPP. The FPR 4215, FPR 4225, and FPR 4245 all have the same exterior appearance. Where they differ is in Firewall throughput, IPS throughput, IPsec VPN throughput and number of VPN peers allowed.

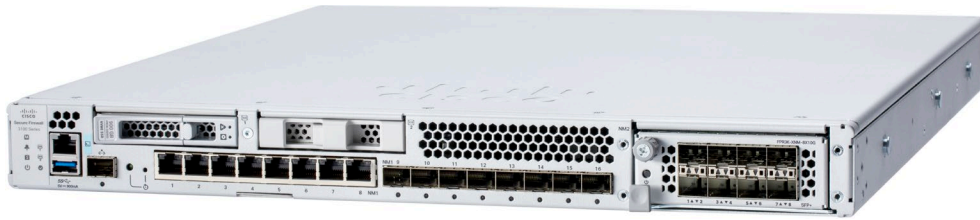


Figure 1 FPR 4215, 4225, 4245

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|--------------------------|------------------|------------------|---|----------|
| FRP 4215 | FPR-4215 | 7.4 | AMD EPYC 7543 (Zen 3), Marvell Cavium Nitrox V CNN5560-900BG676-C45-G | |
| FRP 4225 | FPR-4225 | 7.4 | AMD EPYC 7763 (Zen 3), Marvell Cavium Nitrox V CNN5560-900BG676-C45-G | |
| FRP 4245 | FPR-4245 | 7.4 | AMD EPYC 7763 (Zen 3), Marvell Cavium Nitrox V CNN5560-900BG676-C45-G | |

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

| Mode Name | Description | Type | Status Indicator |
|----------------------------|--|----------|---|
| Approved Mode of Operation | The module is always in the approved mode of operation after initial operations are performed. | Approved | Approved mode indicator: "FIPS is currently enabled." |

Table 3: Modes List and Description

The module has one approved mode of operation and is always in the approved mode of operation after initial operations are performed (See Section 11). The module does not claim implementation of a degraded mode of operation. Section 4 provides details on the service indicator implemented by the module.

2.5 Algorithms

Approved Algorithms:

CiscoSSL FOM Cryptographic Implementation

| Algorithm | CAVP Cert | Properties | Reference |
|--------------------------|-----------|--|----------------------|
| AES-CBC | A4446 | Direction - Decrypt, Encrypt Key Length - 128, 192, 256 | SP 800-38A |
| AES-GCM | A4446 | Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 | SP 800-38D |
| Counter DRBG | A4446 | Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA KeyGen (FIPS186-4) | A4446 | Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates | FIPS 186-4 |
| ECDSA SigGen (FIPS186-4) | A4446 | Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 | FIPS 186-4 |
| ECDSA SigVer (FIPS186-4) | A4446 | Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512 | FIPS 186-4 |

| Algorithm | CAVP Cert | Properties | Reference |
|----------------------------|-----------|--|-------------------|
| HMAC-SHA-1 | A4446 | Key Length - Key Length: 256-448 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-224 | A4446 | Key Length - Key Length: 256-448 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A4446 | Key Length - Key Length: 256-448 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A4446 | Key Length - Key Length: 256-448 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A4446 | Key Length - Key Length: 256-448 Increment 8 | FIPS 198-1 |
| KAS-ECC-SSC Sp800-56Ar3 | A4446 | Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KAS-FFC-SSC Sp800-56Ar3 | A4446 | Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 Scheme - dhEphem - KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KDF IKEv2 (CVL) | A4446 | Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 3072 Hash Algorithm - SHA-1 | SP 800-135 Rev. 1 |
| KDF SNMP (CVL) | A4446 | Password Length - Password Length: 256, 64 | SP 800-135 Rev. 1 |
| KDF SSH (CVL) | A4446 | Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256 | SP 800-135 Rev. 1 |
| RSA KeyGen (FIPS186-4) | A4446 | Key Generation Mode - B.3.4 Modulo - 2048, 3072 Hash Algorithm - SHA2-256 Private Key Format - Standard | FIPS 186-4 |
| RSA SigGen (FIPS186-4) | A4446 | Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072 | FIPS 186-4 |
| RSA SigVer (FIPS186-4) | A4446 | Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072 | FIPS 186-4 |
| Safe Primes Key Generation | A4446 | Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096 | SP 800-56A Rev. 3 |
| SHA-1 | A4446 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-224 | A4446 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A4446 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-384 | A4446 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |

| Algorithm | CAVP Cert | Properties | Reference |
|----------------------------|-----------|--|-------------------|
| SHA2-512 | A4446 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |
| TLS v1.2 KDF RFC7627 (CVL) | A4446 | Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 | SP 800-135 Rev. 1 |

Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation

Nitrox-V GC

| Algorithm | CAVP Cert | Properties | Reference |
|---------------|-----------|--|-------------------|
| AES-CBC | C1026 | Direction - Decrypt, Encrypt Key Length - 128, 192, 256 | SP 800-38A |
| AES-GCM | C1026 | Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256 | SP 800-38D |
| Hash DRBG | C1026 | Prediction Resistance - No Mode - SHA2-512 | SP 800-90A Rev. 1 |
| HMAC-SHA-1 | C1026 | - | FIPS 198-1 |
| HMAC-SHA2-256 | C1026 | - | FIPS 198-1 |
| HMAC-SHA2-384 | C1026 | - | FIPS 198-1 |
| HMAC-SHA2-512 | C1026 | - | FIPS 198-1 |
| SHA-1 | C1026 | Message Length - Message Length: 0-51200 Increment 8 | FIPS 180-4 |
| SHA2-256 | C1026 | Message Length - Message Length: 0-51200 Increment 8 | FIPS 180-4 |
| SHA2-384 | C1026 | Message Length - Message Length: 0-102400 Increment 8 | FIPS 180-4 |
| SHA2-512 | C1026 | Message Length - Message Length: 0-102400 Increment 8 | FIPS 180-4 |

Table 5: Approved Algorithms - Nitrox-V GC

Vendor-Affirmed Algorithms:

| Name | Properties | Implementation | Reference |
|------|---------------------|----------------|----------------------------------|
| CKG | Key Type:Asymmetric | N/A | SP 800-133r2 Section 4, Method 1 |

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---------------------------------|-------------------|--|--|---|
| KAS-ECC- KeyGen (SSHv2) | KAS-KeyGen CKG | KAS ECC keygen used in SSHv2 service | Bit-strength Caveat:Provides between 128 and 256 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) CKG: () |
| KAS-FFC- KeyGen (SSHv2) | KAS-KeyGen CKG | KAS FFC keygen used in SSHv2 service | Bit-strength Caveat:Provides between 112 and 152 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) Safe Primes Key Generation: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 CKG: () |
| KAS-ECC- KeyGen (TLSv1.2) | KAS-KeyGen CKG | KAS ECC keygen used in TLSv1.2 service | Bit-strength Caveat:Provides between 128 and 256 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) CKG: () |
| KAS-FFC- KeyGen (TLSv1.2) | KAS-KeyGen CKG | KAS FFC keygen used in TLSv1.2 service | Bit-strength Caveat:Provides between 112 and 152 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) Safe Primes Key Generation: (A4446) Safe Prime Groups: ffdhe2048, ffdhe3072, |

| Name | Type | Description | Properties | Algorithms |
|----------------------------|-------------------|--|---|---|
| | | | | ffdhe4096 CKG: () |
| KAS-ECC- KeyGen (IKEv2) | KAS-KeyGen CKG | KAS ECC keygen used in TLSv1.2 service | Bit-strength Caveat:Provides between 128 and 256 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) CKG: () |
| KAS-FFC- KeyGen (IKEv2) | KAS-KeyGen CKG | KAS FFC keygen used in IKEv2 service | Bit-strength Caveat:Provides between 112 and 152 bits encryption strength | Counter DRBG: (A4446) Hash DRBG: (C1026) Safe Primes Key Generation: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 CKG: () |
| KAS-ECC (SSHv2) | KAS-Full | KAS-ECC for SSHv2 service | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | KDF SSH: (A4446) KAS-ECC-SSC Sp800-56Ar3: (A4446) |
| KAS-FFC (SSHv2) | KAS-Full | KAS-FFC SSHv2 service | Bit-strength Caveat:Provides between 112 and 152 bits of encryption strength | KDF SSH: (A4446) KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 |
| KAS-ECC (TLSv1.2) | KAS-Full | KAS-ECC for TLSv1.2 service | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | TLS v1.2 KDF RFC7627: (A4446) KAS-ECC-SSC Sp800-56Ar3: (A4446) |
| KAS-FFC (TLSv1.2) | KAS-Full | KAS-FFC for TLSv1.2 service | Bit-strength Caveat:Provides | TLS v1.2 KDF RFC7627: |

| Name | Type | Description | Properties | Algorithms |
|---------------------------------|----------|---|---|---|
| | | | between 112 and 152 bits of encryption strength | (A4446) KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: ffdhe2048, ffdhe3072, ffdhe4096 |
| KAS-ECC (IKEv2) | KAS-Full | KAS-ECC for IKEv2 Service | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | KAS-ECC-SSC Sp800-56Ar3: (A4446) KDF IKEv2: (A4446) |
| KAS-FFC (IKEv2) | KAS-Full | KAS-FFC for IKEv2 service | Bit-strength Caveat:Provides between 112 and 152 bits of encryption strength | KAS-FFC-SSC Sp800-56Ar3: (A4446) Domain Parameter Generation Methods: MODP-2048, MODP-3072, MODP-4096 KDF IKEv2: (A4446) |
| KTS (TLSv1.2 with AES and HMAC) | KTS-Wrap | KTS via TLSv1.2 service by using AES and HMAC | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | AES-CBC: (A4446) HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) |
| KTS (TLSv1.2 with AES-GCM) | KTS-Wrap | KTS via TLSv1.2 service by using AES-GCM | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | AES-GCM: (A4446) |

| Name | Type | Description | Properties | Algorithms |
|--|---------------------------|---|---|--|
| KTS (SSHv2 with AES and HMAC) | KTS-Wrap | KTS via SSHv2 service by using AES and HMAC | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | AES-CBC: (A4446) HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446) |
| KTS (SSHv2 with AES-GCM) | KTS-Wrap | KTS via SSHv2 service by using AES-GCM | Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength | AES-GCM: (A4446) |
| RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | AsymKeyPair-KeyGen CKG | RSA KeyGen for SSHv2, TLSv1.2, and IKEv2 services | | RSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) Hash DRBG: (C1026) CKG: () |
| ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | AsymKeyPair-KeyGen CKG | ECDSA KeyGen for TLSv1.2 and IKEv2 services | | ECDSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) Hash DRBG: (C1026) CKG: () |
| RSA SigGen (SSHv2, TLSv1.2, IKEv2) | DigSig-SigGen | RSA SigGen for SSHv2, TLSv1.2, and IKEv2 services | | RSA SigGen (FIPS186-4): (A4446) |
| ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) | DigSig-SigGen | ECDSA SigGen for TLSv1.2, and IKEv2 services | | ECDSA SigGen (FIPS186-4): (A4446) |
| RSA SigVer (SSHv2, TLSv1.2, and IKEv2) | DigSig-SigVer | RSA SigVer for SSHv2, TLSv1.2, and IKEv2 services | | RSA SigVer (FIPS186-4): (A4446) |
| ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) | DigSig-SigVer | ECDSA SigVer for TLSv1.2 and IKEv2 services | | ECDSA SigVer (FIPS186-4): (A4446) |
| Block Cipher (SSHv2) | BC-Auth BC-UnAuth | Block Cipher for SSHv2 service | | AES-CBC: (A4446) |

| Name | Type | Description | Properties | Algorithms |
|--------------------------|----------------------|---|------------|--|
| | | | | AES-GCM: (A4446) |
| Block Cipher (TLSv1.2) | BC-Auth BC-UnAuth | Block Cipher for TLSv1.2 service | | AES-GCM: (A4446) AES-CBC: (A4446) |
| Block Cipher (IPSec/IKE) | BC-Auth BC-UnAuth | Block Cipher for IPSec/IKEv2 service | | AES-CBC: (A4446, C1026) AES-GCM: (A4446, C1026) |
| Block Cipher (SNMPv3) | BC-UnAuth | Block Cipher for SNMPv3 service | | AES-CBC: (A4446) KDF SNMP: (A4446) |
| MAC (SSHv2) | MAC | MAC for SSHv2 service | | HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446) |
| MAC (TLSv1.2) | MAC | Message Authentication for TLSv1.2 services | | HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) |
| MAC (IPSec/IKEv2) | MAC | Message Authentication for IPSec/IKEv2 services | | HMAC-SHA2-256: (A4446, C1026) HMAC-SHA2-384: (A4446, C1026) HMAC-SHA2-512: (A4446, C1026) SHA2-256: (A4446, C1026) SHA2-384: (A4446, C1026) SHA2-512: (A4446, C1026) HMAC-SHA-1: |

| Name | Type | Description | Properties | Algorithms |
|--------------------|------|---|------------|---|
| | | | | (C1026) SHA-1: (C1026) |
| MAC (SNMPv3) | MAC | Message Authentication for SNMPv3 service | | HMAC-SHA-1: (A4446) SHA-1: (A4446) KDF SNMP: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) HMAC-SHA2-224: (A4446) SHA2-224: (A4446) |
| Firmware Load Test | MAC | MAC for firmware load test | | HMAC-SHA2-512: (A4446) |

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

- For TLSv1.2, the module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1 following RFC 5288. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are.

In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- The module was algorithm tested based on the FIPS 186-4 standard for Digital Signatures. According to IG C.K, this module is 186-5 compliant as all 186-4 CAVP tests performed are mathematically identical to the 186-5 CAVP tests. The Module does not support 186-4 DSA or RSA X9.31 for Signature Generation or Signature Verification.

2.8 RBG and Entropy

| Cert Number | Vendor Name |
|-------------|---------------------|
| E3 | Cisco Systems, Inc. |

Table 8: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|-----------------------------|--------------|--|-------------|--------------------|------------------------|
| Cisco Jitter Entropy Source | Non-Physical | AMD EPYC 7543 (Zen 3), AMD EPYC 7763 (Zen 3) | 256 bits | Full Entropy | A2810 (SHA3-256) |

Table 9: Entropy Sources

The module implements two approved DRBGs based on SP800-90Arev1, including CRT_DRBG with Algo Cert. #A4446, and HASH_DRBG with Algo Cert. #C1026.

Those two DRBGs are used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

Each DRBG is seeded by the entropy source described in the table above. The CTR_DRBG (AES-128/192/256) enables Derivation Function capability, and the HASH_DRBG (SHA2-512) doesn't support Prediction Resistance. Each DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the cryptographic keys generation while in the approved mode.

The Cisco JENT entropy source implementation generates an output that is considered to have full entropy. More information can be found in the public use document for ESV cert #E3.

2.9 Key Generation

The module generates RSA, ECDSA, ECDH, and DH asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 CTR DRBG or NIST SP 800-90Arev1 Hash DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-FFC Shared Secret Computation:
 - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.
 - The module supports the use of the safe primes defined in RFC 4419 (SSH), RFC 7919 (TLS) and RFC 3526 (IKE).

SSH (RFC 4419):

MODP-2048 (ID = 14)

MODP-3072 (ID = 15)

MODP-4096 (ID = 16)

TLS (RFC 7919):

ffdhe2048 (ID = 256)

ffdhe3072 (ID = 257)

ffdhe4096 (ID = 258)

IKE (RFC 3526):

MODP-2048 (ID = 14)

MODP-3072 (ID = 15)

MODP-4096 (ID = 16)

- KAS-ECC Shared Secret Computation:
 - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, SNMPv3 and IPsec/IKEv2 industrial protocols. Please refer to the Security Function Implementations Table for more information. No parts of IPsec/IKEv2, SNMPv3, SSH and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

| Physical Port | Logical Interface(s) | Data That Passes |
|--|----------------------|--|
| Ethernet Port, SFP28 (1/10/25G) port, and Console Port | Data Input | Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data. |
| Ethernet Port, SFP28 (1/10/25G) port, and Console Port | Data Output | Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data. |
| Ethernet Port, SFP28 (1/10/25G) port, Console Port and RESET | Control Input | Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data. |
| Ethernet Port, SFP28 (1/10/25G) port, Console Port and LEDs | Status Output | Status Information output from the module. |
| N/A | Control Output | N/A |
| Power | Power | Provide the Power Supply to the module. |

Table 10: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above. The module's data output interface will be disabled when performing pre-operational self-tests, loading new firmware, zeroizing keys, or when in an error state.

4 Roles, Services, and Authentication

4.1 Authentication Methods

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|-----------------------|---|--------------------------------|--|--|
| Password | The minimum length is eight (8) characters (94 possible characters). The configuration supports at most ten failed attempts to authenticate in a one-minute period. | Password Based | The probability that a random attempt will succeed or a false acceptance will occur is $1/(94^8)$ which is less than $1/1,000,000$. | The probability of successfully authenticating to the module within one minute is $10/(94^8)$, which is less than $1/100,000$. |
| RSA-Based Certificate | The modules support RSA public-key based authentication | RSA SigVer (FIPS186-4) (A4446) | The probability that a random attempt will | the probability of successfully authenticating to the |

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|-------------------------|---|----------------------------------|---|---|
| | mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is $1/(2^{112})$ which is less than $1/1,000,000$. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is $17,000 * 60 = 1,020,000/(2^{112})$, which is less than $1/100,000$. | | succeed is $1/(2^{112})$. Please refer to Description section in this table for more details | module within a one minute period is $17,000 * 60 = 1,020,000/(2^{112})$. Please refer to Description section in this table for more details |
| ECDSA-Based Certificate | The modules support ECDSA public-key based authentication mechanism using a minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is $1/(2^{128})$ which is less than $1/1,000,000$. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the | ECDSA SigVer (FIPS186-4) (A4446) | The probability that a random attempt will succeed is $1/(2^{128})$ which is less than $1/1,000,000$. Please refer to Description section in this table for more details | the probability of successfully authenticating to the module within a one minute period is $17,000 * 60 = 1,020,000/(2^{128})$. Please refer to Description section in this table for more details |

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|-------------|---|--------------------|-----------------------|---------------------|
| | module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000. | | | |

Table 11: Authentication Methods

The module implements identity-based authentication. The module supports Crypto Officer role and the User role. The module also allows the concurrent operators.

4.2 Roles

| Name | Type | Operator Type | Authentication Methods |
|----------------|----------|---------------|--|
| Crypto Officer | Identity | CO | Password RSA-Based Certificate ECDSA-Based Certificate |
| User | Identity | User | Password RSA-Based Certificate ECDSA-Based Certificate |

Table 12: Roles

4.3 Approved Services

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|--------------------|---|------------------------------------|--------------------------------------|--|--------------------|---|
| Show Status | Provide Module's current status (return codes and/or syslog messages) | Global Indicator or syslog message | Command used to show Module's Status | Module's Operational Status | None | Crypto Officer User |
| Show Version | Provide Module's name and version information | Console message | Command to show version | Module's ID and versioning information | None | Crypto Officer User |
| Perform Self-Tests | Perform Self-Tests (Pre-operational self-test) | Global Indicator or syslog message | Command to trigger Self-Test | Status of the self-tests results | None | Crypto Officer User Unauthenticated |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------|-----------------------------|----------------|-------------------------------|--------------------------------|--------------------|---|
| | and Conditional Self-Tests) | | | | | |
| Perform Zeroization | Perform Zeroization | Syslog message | Command to zeroize the module | Status of the SSPs zeroization | None | Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State (V, Key): Z - DRBG Internal State (V, C): Z - User Password: Z - Crypto Officer Password: Z - RADIUS Secret: Z - Firmware Load Test Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--------------------|--|
| | | | | | | Z - SSH ECDH Shared Secret: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLS DH Private Key: Z - TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--------------------|---|
| | | | | | | Shared Secret: Z - TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - IPSec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|-------------------|-----------------------------------|-----------|-----------------------------------|--|--------------------|--|
| | | | | | | Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED: Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z |
| Configure Network | Sets configuration of the systems | None | Commands to configure the network | Status of the completion of network configuration status | None | Crypto Officer |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|-------------------------------|--------------------------|---|----------------------------------|---|--|--|
| Crypto Officer Authentication | CO Role Authentication | N/A | CO Authentication Request | Status of the CO authentication | None | Crypto Officer - Crypto Officer Password: W,Z |
| User Authentication | User Role Authentication | N/A | User role authentication request | Status of the User role authentication | None | User - User Password: W,Z |
| Configure SSHv2 Function | Configure SSHv2 Function | Global Indicator and SSHv2 configuration success status message | Commands to configure SSHv2 | Status of the completion of the SSHv2 configuration | KAS-ECC-KeyGen (SSHv2) KAS-FFC-KeyGen (SSHv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 | Crypto Officer - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: G,W,E - SSH ECDH Private Key: G,W,E - SSH ECDH Public Key: G,R,W - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: G,W,E - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - SSH ECDSA Private Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------------------------|---------------------------------------|--|-------------------------------|---|--|---|
| | | | | | and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (SSHv2) MAC (SSHv2) | G,W,E - SSH ECDSA Public Key: G,R,W - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |
| Configure HTTPS over TLSv1.2 Function | Configure HTTPS over TLSv1.2 Function | Global Indicator and HTTPS over TLSv1.2 configuration success status message | Commands to configure TLSv1.2 | Status of the completion of TLSv1.2 configuration | KAS-ECC- KeyGen (TLSv1.2) KAS-FFC- KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES- GCM) RSA KeyGen | Crypto Officer - TLS DH Private Key: G,W,E - TLS DH Public Key: G,R,W - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: G,W,E - TLS ECDH Private Key: G,W,E - TLS ECDH Public Key: G,R,W |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|---|--|
| | | | | | (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (TLSv1.2) MAC (TLSv1.2) | - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: G,W,E - TLS ECDSA Private Key: G,W,E - TLS ECDSA Public Key: G,R,W - TLS RSA Private Key: G,W,E - TLS RSA Public Key: G,R,W - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|--------------------------------|--------------------------------|--|-----------------------------------|---|---|--|
| Configure IPsec/IKEv2 Function | Configure IPsec/IKEv2 Function | Global Indicator with IPsec/IKEv2 configuration success status message | Commands to configure IPsec/IKEv2 | Status of the completion of IPsec/IKEv2 configuration | KAS-ECC-KeyGen (IKEv2) KAS-FFC-KeyGen (IKEv2) KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (IPsec/IKEv2) MAC (IPsec/IKEv2) | Crypto Officer - IPsec/IKE DH Private Key: G,W,E - IPsec/IKE DH Public Key: G,R,W - IPsec/IKE Peer DH Public Key: W,E - IPsec/IKE DH Shared Secret: G,W,E - IPsec/IKE ECDH Private Key: G,W,E - IPsec/IKE ECDH Public Key: G,R,W - IPsec/IKE Peer ECDH Public Key: W,E - IPsec/IKE ECDH Shared Secret: G,W,E - IPsec/IKE ECDSA Private Key: G,W,E - IPsec/IKE ECDSA Public Key: G,R,W - IPsec/IKE RSA Private Key: G,W,E - IPsec/IKE RSA Public Key: G,R,W - IPsec/IKE Pre-shared |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------------|---------------------------|--|-------------------------------------|--|--|--|
| | | | | | | Secret: G,W,E - SKEYSEED: G,W,E - IPsec/IKE Session Encryption Key: G,W,E - IPsec/IKE Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |
| Configure SNMPv3 Function | Configure SNMPv3 Function | Global Indicator and SNMPv3 configuration success status message | Commands to configure SNMPv3 | Status of the completion of SNMPv3 configuration | Block Cipher (SNMPv3) MAC (SNMPv3) | Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E |
| Run SSHv2 Function | Execute SSHv2 Function | Global Indicator and successful SSHv2 log message | Initiate SSHv2 tunnel establishment | Status of SSHv2 tunnel establishment | KAS-ECC- KeyGen (SSHv2) KAS-FFC- KeyGen (SSHv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) | Crypto Officer - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--|---|
| | | | | | KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (SSHv2) MAC (SSHv2) | Key: W,E - SSH DH Shared Secret: G,W,E - SSH ECDH Private Key: G,W,E - SSH ECDH Public Key: G,R,W - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: G,W,E - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - SSH ECDSA Private Key: G,W,E - SSH ECDSA Public Key: G,R,W - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--------------------|--|
| | | | | | | Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E User - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: G,W,E - SSH ECDH Private Key: G,W,E - SSH ECDH Public Key: G,R,W - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: G,W,E - SSH RSA Private Key: E - SSH RSA Public Key: R - SSH ECDSA Private Key: E - SSH ECDSA Public Key: R |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------------------|-------------------------------------|--|---|--|---|---|
| | | | | | | <ul style="list-style-type: none"> - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |
| Run HTTPS over TLSv1.2 Function | Execute HTTPS over TLSv1.2 function | Global Indicator and successful HTTPS over TLSv1.2 log message | Initiate TLSv1.2 tunnel establishment request | Status of TLSv1.2 tunnel establishment | KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen | Crypto Officer <ul style="list-style-type: none"> - TLS DH Private Key: G,W,E - TLS DH Public Key: G,R,W - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: G,W,E - TLS ECDH Private Key: G,W,E - TLS ECDH Public Key: G,R,W - TLS Peer ECDH Public Key: W,E - TLS ECDH |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|---|--|
| | | | | | (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (TLSv1.2) MAC (TLSv1.2) | Shared Secret: G,W,E - TLS ECDSA Private Key: G,W,E - TLS ECDSA Public Key: G,R,W - TLS RSA Private Key: G,W,E - TLS RSA Public Key: G,R,W - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E User - TLS DH Private Key: G,W,E - TLS DH Public Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--------------------|--|
| | | | | | | G,R,W - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: G,W,E - TLS ECDH Private Key: G,W,E - TLS ECDH Public Key: G,R,W - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: G,W,E - TLS ECDSA Private Key: E - TLS ECDSA Public Key: R - TLS RSA Private Key: E - TLS RSA Public Key: R - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------------------|-------------------------------------|--|---|--|---|--|
| | | | | | | Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |
| Run IPSec/IKEv 2 Function | Execute IPsec/IKEv 2 Function | Global Indicator and successful IPsec/IKE v2 log message | Initiate IPsec/IKEv 2 tunnel establishm ent request | Status of IPSec/IKE v2 tunnel establishm ent | KAS-ECC- KeyGen (IKEv2) KAS-FFC- KeyGen (IKEv2) KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA | Crypto Officer - IPSec/IKE DH Private Key: G,W,E - IPSec/IKE DH Public Key: G,R,W - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: G,W,E - IPSec/IKE ECDH Private Key: G,W,E - IPSec/IKE ECDH Public Key: G,R,W - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: G,W,E - IPSec/IKE ECDSA Private Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--|--|
| | | | | | SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (IPSec/IKE) MAC (IPSec/IKE v2) | G,W,E - IPSec/IKE ECDSA Public Key: G,R,W - IPSec/IKE RSA Private Key: G,W,E - IPSec/IKE RSA Public Key: G,R,W - IPSec/IKE Pre-shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKE Session Encryption Key: G,W,E - IPSec/IKE Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E User - IPSec/IKE DH Private Key: G,W,E - IPSec/IKE DH Public Key: G,R,W - IPSec/IKE Peer DH |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|------|-------------|-----------|--------|---------|--------------------|---|
| | | | | | | Public Key: W,E - IPSec/IKE DH Shared Secret: G,W,E - IPSec/IKE ECDH Private Key: G,W,E - IPSec/IKE ECDH Public Key: G,R,W - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: G,W,E - IPSec/IKE ECDSA Private Key: E - IPSec/IKE ECDSA Public Key: R - IPSec/IKE RSA Private Key: E - IPSec/IKE RSA Public Key: R - IPSec/IKE Pre-shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKE Session Encryption Key: G,W,E - IPSec/IKE |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---------------------|--------------------------------|---|--|---------------------------------------|---------------------------------------|--|
| | | | | | | Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State (V, Key): G,W,E - DRBG Internal State (V, C): G,W,E |
| Run SNMPv3 Function | Execute SNMPv3 Function | Global Indicator and successful SNMPv3 log message | Initiate SNMPv3 tunnel establishment request | Status of SNMPv3 tunnel establishment | Block Cipher (SNMPv3) MAC (SNMPv3) | Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E User - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: G,W,E - SNMPv3 Authentication Key: G,W,E |
| Firmware Load Test | Execute the Firmware Load Test | Global indicator and successful Firmware Loading status message | Commands to load new firmware image | Outcome of the Firmware Load Test | Firmware Load Test | Crypto Officer - Firmware Load Test Key: R |

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using HMAC-SHA2-512 (HMAC Cert. #A4446) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware loaded into the module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.7 Additional Information

The module supports unauthenticated service. The unauthenticated User/Operators can trigger the self-test service by power-cycling the module, and is able to observe the module's LEDs status.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is provided in the form of binary executable code. To ensure firmware security, the module is protected by RSA 2048 bits with SHA2-512 (RSA Cert. #A4446) algorithm. A Firmware Integrity Test Key (non-SSP) was preloaded to the module's binary at the factory and used for firmware integrity test only at the pre-operational self-test. The module uses the RSA 2048 bits modulus public key to verify the digital signature. If the firmware integrity test fails, the module would enter to an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the tested platform to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|----------------------|---|
| Tamper labels (10) with Part number: AIR-AP-FIPSKIT= | Recommend 30 Days | Visible inspection of platform for residual evidence of tampering |
| Opacity shield (1) with Part number: FPR4200-FIPS-KIT | Recommend 30 Days | Visible inspection of platform for evidence of tampering, removal or access |
| Production grade components | N/A | N/A |

Table 14: Mechanisms and Actions Required

The module utilizes a production-grade enclosure and removable cover along with tamper evidence labels as the physical security mechanisms.

Applying Tamper Evidence Labels

Step 1: Turn off and unplug the module.

Step 2: Clean the chassis of any grease, dirt, oil or any other material other than the surface coating from manufacture before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Step 3: Apply a label to cover the module as shown in the figures below.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word "FIPS" may appear if the label was peeled back.

7.2 User Placed Tamper Seals

Number: Ten (10)

Placement:



Figure 2. FPR-4200 Front view



Figure 3. FPR-4200 Back view



Figure 4. FPR-4200 Left view



Figure 5. FPR-4200 Right view



Figure 6. FPR-4200 Bottom view



Figure 7. FPR-4200 Top view

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

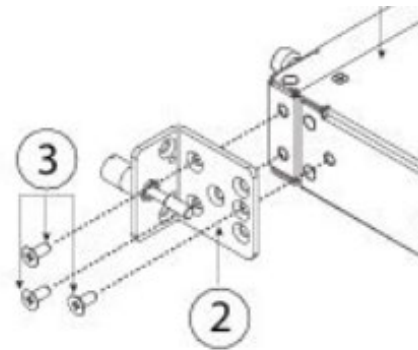
Part Numbers: AIR-AP-FIPSKIT=

7.3 Filler Panels

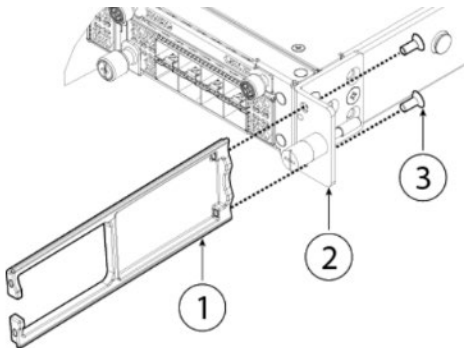
FPR 4215, FPR 4225 and FPR 4245 Opacity Shield

FPR4200-FIPS-KIT=

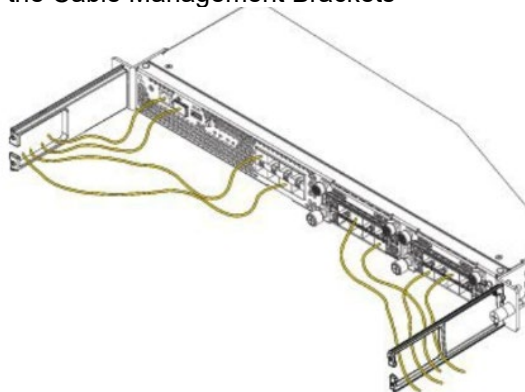
Step 1: Attach the Slide Rail Locking Bracket, #2 in diagram to the Side of the Chassis using the countersink screws #3 in diagram.



Step 2: Attach the Cable Management Bracket (#1) to the Slide Rail Locking Bracket (#2) using the countersink screws (#3)



Step 3: Route the Cables through the Cable Management Brackets



Step 4: Attach the FIPS Opacity Shield (#1) to the Cable Management Brackets (#3) using the countersink screws (#2)

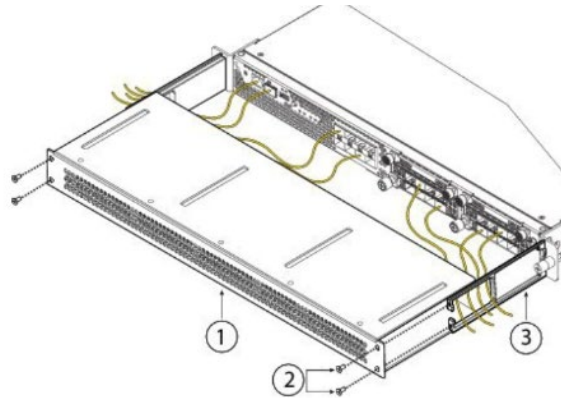


Figure 8 Opacity Shield Brackets

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

| Storage Area Name | Description | Persistence Type |
|-------------------|---------------------|------------------|
| DRAM | Volatile Memory | Dynamic |
| Flash | Non-Volatile Memory | Static |

Table 15: Storage Areas

9.2 SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|-------------|-------------------|------------|---------------------------------|
| Peer Public Key Input | External (Outside of the Module's Boundary) | Module | Plaintext | Automated | Electronic | |
| Module Public Key Output | Module | External (Outside of the Module's Boundary) | Plaintext | Automated | Electronic | |
| Password/Secret Input via SSHv2 encrypted by GCM | External (Outside of the Module's Boundary) | Module | Encrypted | Automated | Electronic | KTS (SSHv2 with AES-GCM) |
| Password/Secret Input via SSHv2 encrypted by AES and HMAC | External (Outside of the Module's Boundary) | Module | Encrypted | Automated | Electronic | KTS (SSHv2 with AES and HMAC) |
| Password/Secret Input via TLS encrypted by GCM | External (Outside of the Module's Boundary) | Module | Encrypted | Automated | Electronic | KTS (TLSv1.2 with AES-GCM) |
| Password/Secret Input via TLS encrypted by AES and HMAC | External (Outside of the Module's Boundary) | Module | Encrypted | Automated | Electronic | KTS (TLSv1.2 with AES and HMAC) |

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---------------------|---------------------------------------|---|---------------------------------------|
| Zeroization Command | CO issues zeroization service | the zeroization command will erase all SSPs stored in the DRAM or in the Flash of the module. | CO issues command 'format everything' |
| Session termination | Zeroization upon session termination | Session termination will automatically zeroize all session based temporary SSPs | Terminate session |
| Reboot | Zeroization upon rebooting the module | Reboot to zeroize all temporary SSPs stored in Module's DRAM | Reboot |

Table 17: SSP Zeroization Methods

Performing the zeroization command will explicitly zeroize the module returning the “System restarted due to disks being reformatted.” status message upon completion.

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|------------------------------|-------------------------|------------------------------|---------------------------|--------------|----------------|---|
| DRBG Entropy Input | Used to seed the DRBG | 384 bits - at least 256 bits | Entropy Input - CSP | | | Counter DRBG (A4446) Hash DRBG (C1026) |
| DRBG Seed | Used in DRBG Generation | 256 bits - 256 bits | DRBG Seed - CSP | | | Counter DRBG (A4446) Hash DRBG (C1026) |
| DRBG Internal State (V, Key) | Used in DRBG Generation | 256 bits - 256 bits | DRBG Internal State - CSP | | | Counter DRBG (A4446) |
| DRBG Internal State (V, C) | Used in DRBG Generation | 256 bits - 256 bits | DRBG Internal State - CSP | | | Hash DRBG (C1026) |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|-------------------------|---|--|---------------------------|------------------------|---------------------------------|---------------------------------|
| User Password | User authentication | 8-30 Characters - 8-30 Characters | Authentication Data - CSP | | | |
| Crypto Officer Password | Crypto Officer authentication | 8-30 Characters - 8-30 Characters | Authentication Data - CSP | | | |
| RADIUS Secret | RADIUS Server Authentication | 16 Characters - 16 Characters | Authentication Data - CSP | | | |
| Firmware Load Test Key | Used for Firmware Load Test | 112 bits - 112 bits | Public Key - CSP | | | Firmware Load Test |
| SSH DH Private Key | Used to derive the SSH DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Private Key - CSP | KAS-FFC-KeyGen (SSHv2) | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| SSH DH Public Key | Used to derive SSH DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Public Key - PSP | | KAS-FFC-KeyGen (SSHv2) | |
| SSH Peer DH Public Key | Used to derive SSH DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Public Key - PSP | | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| SSH DH Shared Secret | Used to derive SSH Session Encryption Keys, SSH Session | MODP-2048, MODP-3072, MODP-4096 - | Shared Secret - CSP | | KAS-FFC-SSC Sp800-56Ar3 (A4446) | KDF SSH (A4446) |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|--------------------------|---|--|---------------------|---|------------------------------------|----------------------------------|
| | Authentication Keys | 112-152 bits | | | | |
| SSH ECDH Private Key | Used to derive the SSH ECDH Shared Secret | Curves: 256, 384, 521 bits - 128 to 256 bits | Private Key - CSP | KAS-ECC-KeyGen (SSHv2) | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |
| SSH ECDH Public Key | Used to derive SSH ECDHE Shared Secret | Curves: 256, 384, 521 bits - 128-256 bits | Public Key - PSP | | KAS-ECC-KeyGen (SSHv2) | |
| SSH Peer ECDH Public Key | Used to derive SSH DH Shared Secret | Curves: 256, 384, 521 bits - 128 to 256 bits | Public Key - PSP | | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |
| SSH ECDH Shared Secret | Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys | Curves: 256, 384, 521 bits - 128 to 256 bits | Shared Secret - CSP | | KAS-ECC-SSC Sp800-56Ar3 (A4446) | KDF SSH (A4446) |
| SSH RSA Private Key | Used for SSH session authentication | Modulus 2048 and 3072 bits - 112-128 bits | Private Key - CSP | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | | RSA SigGen (FIPS186-4) (A4446) |
| SSH RSA Public Key | Used for SSH sessions authentication | Modulus 2048 and 3072 bits - 112-128 bits | Public Key - PSP | | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | |
| SSH ECDSA Private Key | Used for SSH session authentication | Curves: 256, 384, 521 bits - 128 to 256 bits | Private Key - CSP | ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | | ECDSA SigGen (FIPS186-4) (A4446) |
| SSH ECDSA Public Key | Used for SSH sessions authentication | Curves: 256, 384, 521 bits - 128 to 256 bits | Public Key - PSP | | ECDSA KeyGen (FIPS186-4) (A4446) | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|--------------------------------|--|--|---------------------|--------------------------|------------------------------------|------------------------------------|
| SSH Session Encryption Key | Used for SSH Session confidentiality protection | 128-256 bits - 128-256 bits | Session Key - CSP | | KAS-ECC (SSHv2) KAS-FFC (SSHv2) | Block Cipher (SSHv2) |
| SSH Session Authentication Key | Used for SSH Session integrity protection | 160-256 bits - 160-256 bits | Session Key - CSP | | KAS-ECC (IKEv2) KAS-FFC (IKEv2) | MAC (SSHv2) |
| TLS DH Private Key | Used to Derive TLS DH Shared Secret | ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits | Private Key - CSP | KAS-FFC-KeyGen (TLSv1.2) | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| TLS DH Public Key | Used to Derive TLS DH Shared Secret | ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits | Public Key - PSP | | KAS-FFC-KeyGen (TLSv1.2) | |
| TLS Peer DH Public Key | Used to derive TLS DH Shared Secret | ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits | Public Key - PSP | | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| TLS DH Shared Secret | Used to Derive TLS Session Encryption Key and TLS Session Authentication Key | ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits | Shared Secret - CSP | | KAS-FFC-SSC Sp800-56Ar3 (A4446) | TLS v1.2 KDF RFC7627 (A4446) |
| TLS ECDH Private Key | Used to Derive TLS ECDH Shared Secret | Curves P-256, P-384, and P-521 - 128-256 bits | Private Key - CSP | KAS-ECC-KeyGen (TLSv1.2) | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|--------------------------|--|---|---------------------|---|---|----------------------------------|
| TLS ECDH Public Key | Used to Derive TS ECDH Shared Secret | Curves P-256, P-384, and P-521 - 128-256 bits | Public Key - PSP | | KAS-ECC-KeyGen (TLSv1.2) | |
| TLS Peer ECDH Public Key | Used to derive IKE ECDH Shared Secret | Curves: P-256, P-384, P-521 - 128-256 bits | Public Key - PSP | | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |
| TLS ECDH Shared Secret | Used to Derive TLS Session Encryption Key and TLS Session Authentication Key | Curves p-256, P-384, P-521 - 128-256 bits | Shared Secret - CSP | | KAS-ECC-SSC Sp800-56Ar3 (A4446) | TLS v1.2 KDF RFC7627 (A4446) |
| TLS ECDSA Private Key | Used to support CO and Admin HTTPS interfaces | Curves P-256, P-384, P-521 - 128-256 bits | Private Key - CSP | ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | | ECDSA SigGen (FIPS186-4) (A4446) |
| TLS ECDSA Public Key | Used to support CO and User HTTPS Interfaces | Curves P-256, P-384, P-521 - 128-256 bits | Public Key - PSP | | ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | |
| TLS RSA Private Key | Used to support CO and Admin HTTPS Interfaces | Modulus 2048 and 3072 bits - 112-128 bits | Private Key - CSP | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | | RSA SigGen (FIPS186-4) (A4446) |
| TLS RSA Public Key | Used to support CO and User HTTPS interfaces | Modulus 2048 and 3072 bits - 112-128 bits | Public Key - PSP | | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | |
| TLS Master Secret | Used to protect HTTPS Session. | 384 bits - 384 bits | Master Secret - CSP | | | TLS v1.2 KDF RFC7627 (A4446) |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|--------------------------------|---|--|---------------------|------------------------|--|---------------------------------|
| | Pre-master secret | | | | | |
| TLS Session Encryption Key | Used to protect HTTPS Session. TLS Master secret | 128-256 bits - 128-256 bits | Session Key - CSP | | KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) | Block Cipher (TLSv1.2) |
| TLS Session Authentication Key | Used to protect HTTPS Session. TLS master secret | 160-384 bits - 160-384 bits | Session Key - CSP | | KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) | MAC (TLSv1.2) |
| IPSec/IKE DH Private Key | Used to derive IPSec/IKE DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Private Key - CSP | KAS-FFC-KeyGen (IKEv2) | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| IPSec/IKE DH Public Key | Used to derive IPSec/IKE DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Public Key - PSP | | KAS-FFC-KeyGen (IKEv2) | |
| IPSec/IKE Peer DH Public Key | Used to derive IPSec/IKE DH Shared Secret | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Public Key - PSP | | | KAS-FFC-SSC Sp800-56Ar3 (A4446) |
| IPSec/IKE DH Shared Secret | Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys | MODP-2048, MODP-3072, MODP-4096 - 112-152 bits | Shared Secret - CSP | | KAS-FFC-SSC Sp800-56Ar3 (A4446) | KDF IKEv2 (A4446) |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|--------------------------------|--|---|---------------------|---|---|----------------------------------|
| IPSec/IKE ECDH Private Key | Used to derive IPSec/IKE ECDH Shared Secrets | Curves P-256, P-384, P-521 - 128-256 bits | Private Key - CSP | KAS-ECC-KeyGen (IKEv2) | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |
| IPSec/IKE ECDH Public Key | Used to derive IPSec/IKE ECDH Shared Secrets | Curves P-256, P-384, P-521 - 128-256 bits | Public Key - PSP | | KAS-ECC-KeyGen (IKEv2) | |
| IPSec/IKE Peer ECDH Public Key | Used to derive IPSec/IKE ECDH Shared Secrets | Curves P-256, P-384, P-521 - 128-256 bits | Public Key - PSP | | | KAS-ECC-SSC Sp800-56Ar3 (A4446) |
| IPSec/IKE ECDH Shared Secret | Used to derive IPSec/IKE ECDH Shared Secrets | Curves P-256, P-384, P-521 - 128-256 bits | Shared Secret - CSP | | KAS-ECC-SSC Sp800-56Ar3 (A4446) | KDF IKEv2 (A4446) |
| IPSec/IKE ECDSA Private Key | Used for IPSec/IKE peer authentication | Curves P-256, P-384, P-521 - 128-256 bits | Private Key - CSP | ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | | ECDSA SigGen (FIPS186-4) (A4446) |
| IPSec/IKE ECDSA Public Key | Used for IPSec/IKE peer authentication | Curves P-256, P-384, P-521 - 128-256 bits | Public Key - PSP | | ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) | |
| IPSec/IKE RSA Private Key | Used for IPSec/IKE peer authentication | Modulus 2048 or 3072 - 112 or 128 bits | Private Key - CSP | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | | RSA SigGen (FIPS186-4) (A4446) |
| IPSec/IKE RSA Public Key | Used for IPSec/IKE peer authentication | Modulus 2048 or 3072 - 112 or 128 bits | Public Key - PSP | | RSA KeyGen (SSHv2, TLSv1.2, IKEv2) | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|----------------------------------|--|---|-----------------------------|--------------|------------------------------------|--------------------------|
| IPSec/IKE Pre-shared Secret | Used for IPSec/IKE peer authentication | 16-32 bytes characters - 16-32 bytes characters | shared secret - CSP | | | |
| SKEYSEED | Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key | 160 bits - 160 bits | Keying Material - CSP | | | KDF IKEv2 (A4446) |
| IPSec/IKE Session Encryption Key | Used to secure IPSec/IKEv2 session confidentiality | 128-256 bits - 128-256 bits | Session Key - CSP | | KAS-ECC (IKEv2) KAS-FFC (IKEv2) | Block Cipher (IPSec/IKE) |
| IPSec/IKE Authentication Key | Used to secure IPSec/IKEv2 session integrity | 160-512 bits - 160-512 bits | Session Key - CSP | | KAS-ECC (IKEv2) KAS-FFC (IKEv2) | MAC (IPSec/IKEv2) |
| SNMPv3 Shared Secret | Used for SNMPv3 user authentication | 8-32 characters - N/A | Authentication Secret - CSP | | | |
| SNMPv3 Encryption Key | Used to protect SNMPv3 traffic confidentiality | 128 bits - 128 bits | Encryption Key - CSP | | KDF SNMP (A4446) | Block Cipher (SNMPv3) |
| SNMPv3 Authentication Key | Used to secure SNMPv3 traffic integrity | 160-384 bits - 160-384 bits | Authentication Key - CSP | | KDF SNMP (A4446) | MAC (SNMPv3) |

Table 18: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|------------------------------|--|-----------------|------------------|--|--|
| DRBG Entropy Input | | DRAM:Plaintext | Until Reboot | Zeroization Command Session termination Reboot | DRBG Seed:Used With DRBG Internal State (V, Key):Used With DRBG Internal State (V, C):Used With |
| DRBG Seed | | DRAM:Plaintext | Until Reboot | Zeroization Command Session termination Reboot | DRBG Entropy Input:Used With DRBG Internal State (V, Key):Used With DRBG Internal State (V, C):Used With |
| DRBG Internal State (V, Key) | | DRAM:Plaintext | Until Reboot | Zeroization Command Session termination Reboot | DRBG Entropy Input:Used With DRBG Seed:Used With |
| DRBG Internal State (V, C) | | DRAM:Plaintext | Until Reboot | Zeroization Command Session termination Reboot | DRBG Entropy Input:Used With DRBG Seed:Used With |
| User Password | Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 | Flash:Encrypted | | Zeroization Command | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|-------------------------|--|-----------------|------------------|---------------------|--------------|
| | encrypted by AES and HMAC | | | | |
| Crypto Officer Password | Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC | Flash:Encrypted | | Zeroization Command | |
| RADIUS Secret | Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC | Flash:Encrypted | | Zeroization Command | |
| Firmware Load Test Key | | Flash:Plaintext | | N/A | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|--------------------------|--------------------------|----------------|------------------------|--|---|
| SSH DH Private Key | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With |
| SSH DH Public Key | Module Public Key Output | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH DH Private Key:Paired With |
| SSH Peer DH Public Key | Peer Public Key Input | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH DH Private Key:Used With |
| SSH DH Shared Secret | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH DH Private Key:Derived From SSH DH Public Key:Derived From |
| SSH ECDH Private Key | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With |
| SSH ECDH Public Key | Module Public Key Output | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH ECDH Private Key:Paired With |
| SSH Peer ECDH Public Key | Peer Public Key Input | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination | SSH ECDH Private Key:Used With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|--------------------------------|--------------------------|-----------------|------------------------|--|---|
| | | | | n Reboot | |
| SSH ECDH Shared Secret | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH ECDH Private Key:Derived From SSH ECDH Public Key:Derived From |
| SSH RSA Private Key | | Flash:Plaintext | | Zeroization Command | SSH RSA Public Key:Paired With |
| SSH RSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | SSH RSA Private Key:Paired With |
| SSH ECDSA Private Key | | Flash:Plaintext | | Zeroization Command | SSH ECDSA Public Key:Paired With |
| SSH ECDSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | SSH ECDSA Private Key:Paired With |
| SSH Session Encryption Key | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH Session Authentication Key:Used With |
| SSH Session Authentication Key | | DRAM:Plaintext | While SSH tunnel is on | Zeroization Command Session termination Reboot | SSH Session Encryption Key:Used With |
| TLS DH Private Key | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS DH Public Key:Paired With TLS Peer DH Public Key:Used With |
| TLS DH Public Key | Module Public Key Output | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination | TLS DH Private Key:Paired With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|--------------------------|--------------------------|-----------------|------------------------|--|---|
| | | | | n Reboot | |
| TLS Peer DH Public Key | Peer Public Key Input | DRAM:Plaintext | while TLS tunnel is on | Zeroization Command Session termination Reboot | TLS DH Private Key:Used With |
| TLS DH Shared Secret | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From |
| TLS ECDH Private Key | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Public Key:Paired With TLS Peer ECDH Public Key:Used With |
| TLS ECDH Public Key | Module Public Key Output | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Private Key:Paired With |
| TLS Peer ECDH Public Key | Peer Public Key Input | DRAM:Plaintext | while TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Private Key:Used With |
| TLS ECDH Shared Secret | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From |
| TLS ECDSA Private Key | | Flash:Plaintext | | Zeroization Command | TLS ECDSA Public Key:Paired With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|--------------------------------|--------------------------|-----------------|---------------------------------|--|---|
| TLS ECDSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | TLS ECDSA Private Key:Paired With |
| TLS RSA Private Key | | Flash:Plaintext | | Zeroization Command | TLS RSA Public Key:Paired With |
| TLS RSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | TLS RSA Private Key:Paired With |
| TLS Master Secret | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS ECDH Shared Secret:Derived From |
| TLS Session Encryption Key | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS Session Authentication Key:Used With |
| TLS Session Authentication Key | | DRAM:Plaintext | While TLS tunnel is on | Zeroization Command Session termination Reboot | TLS Session Encryption Key:Used With |
| IPSec/IKE DH Private Key | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE DH Public Key:Paired With IPSec/IKE Peer DH Public Key:Used With |
| IPSec/IKE DH Public Key | Module Public Key Output | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE DH Private Key:Paired With |
| IPSec/IKE Peer DH Public Key | Peer Public Key Input | DRAM:Plaintext | while IPSec/IKE tunnel is on | Zeroization Command Session | IPsec/IKE DH Private Key:Used With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---------------------------------------|-----------------------------|-----------------|--|--|---|
| | | | | termination Reboot | |
| IPSec/IKE DH Shared Secret | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | SKEYSEED:Used With |
| IPSec/IKE ECDH Private Key | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE ECDH Public Key:Paired With IPSec/IKE Peer ECDH Public Key:Used With |
| IPSec/IKE ECDH Public Key | Module Public Key Output | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE ECDH Private Key:Paired With |
| IPSec/IKE Peer ECDH Public Key | Peer Public Key Input | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE ECDH Private Key:Used With |
| IPSec/IKE ECDH Shared Secret | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | SKEYSEED:Used With |
| IPSec/IKE ECDSA Private Key | | Flash:Plaintext | | Zeroization Command | IPSec/IKE ECDSA Public Key:Paired With |
| IPSec/IKE ECDSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | IPSec/IKE ECDSA Private Key:Paired With |
| IPSec/IKE RSA Private Key | | Flash:Plaintext | | Zeroization Command | IPSec/IKE RSA Public Key:Paired With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|----------------------------------|--|-----------------|---------------------------------|--|--|
| IPSec/IKE RSA Public Key | Module Public Key Output | Flash:Plaintext | | Zeroization Command | IPSec/IKE RSA Private Key:Paired With |
| IPSec/IKE Pre-shared Secret | Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC | Flash:Encrypted | While IPSec/IKE v2 tunnel is on | Zeroization Command | SKEYSEED:Derived to |
| SKEYSEED | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From IPSec/IKE Pre-shared Secret:Derived From |
| IPSec/IKE Session Encryption Key | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination Reboot | IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From |
| IPSec/IKE Authentication Key | | DRAM:Plaintext | While IPSec/IKE v2 tunnel is on | Zeroization Command Session termination | IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---------------------------|--|-----------------|---------------------------|--|--|
| | | | | n Reboot | Shared Secret:Derived From |
| SNMPv3 Shared Secret | Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC | Flash:Encrypted | While SNMPv3 tunnel is on | Zeroization Command | SNMPv3 Encryption Key:Derive To SNMPv3 Authentication Key:Derive To |
| SNMPv3 Encryption Key | | DRAM:Plaintext | While SNMPv3 tunnel is on | Zeroization Command Session termination Reboot | SNMPv3 Shared Secret:Derived From |
| SNMPv3 Authentication Key | | DRAM:Plaintext | While SNMPv3 tunnel is on | Zeroization Command Session termination Reboot | SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With |

Table 19: SSP Table 2

9.5 Transitions

- SHA-1
The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to SHA2, which is available in this module.
- FIPS 186-4/186-5

As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5. This means that no timeline exists in which any of the implemented algorithms will transition from approved to non-approved.”

10 Self-Tests

10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|--------------------------------|------------------------------------|-------------|-----------------|---------------------------|------------|
| RSA SigVer (FIPS186-4) (A4446) | RSA SigVer 2048 bits with SHA2-512 | KAT | SW/FW Integrity | Module is in normal state | RSA SigVer |

Table 20: Pre-Operational Self-Tests

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module’s status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.2 Conditional Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|-----------------|-------------|-----------|---------------------------|-----------------------|------------|
| AES-CBC Encrypt KAT (A4446) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-CBC Decrypt KAT (A4446) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |
| AES-GCM Authenticated Encrypt KAT (A4446) | 256 bits | KAT | CAST | Module is in normal state | Authenticated Encrypt | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|--------------------------------|-------------|-----------|---------------------------|-----------------------|------------|
| AES-GCM Authenticated Decrypt KAT (A4446) | 256 bits | KAT | CAST | Module is in normal state | Authenticated Decrypt | Power Up |
| Counter DRBG Instantiate KAT (A4446) | AES-128 | KAT | CAST | Module is in normal state | Instantiate KAT | Power Up |
| Counter DRBG Generate KAT (A4446) | AES-128 | KAT | CAST | Module is in normal state | Generate KAT | Power Up |
| Counter DRBG Reseed KAT (A4446) | AES-128 | KAT | CAST | Module is in normal state | Reseed KAT | Power Up |
| ECDSA SigGen (FIPS186-4) KAT (A4446) | P-256 curve with SHA2-256 | KAT | CAST | Module is in normal state | ECDSA SigGen KAT | Power Up |
| ECDSA SigVer (FIPS186-4) KAT (A4446) | P-256 curve with SHA2-256 | KAT | CAST | Module is in normal state | ECDSA SigVer KAT | Power Up |
| HMAC-SHA-1 KAT (A4446) | SHA-1 | KAT | CAST | Module is in normal state | HMAC-SHA-1 | Power Up |
| HMAC-SHA2-256 KAT (A4446) | SHA2-256 | KAT | CAST | Module is in normal state | HMAC-SHA2-256 | Power Up |
| HMAC-SHA2-384 KAT (A4446) | SHA2-384 | KAT | CAST | Module is in normal state | HMAC-SHA2-384 | Power Up |
| HMAC-SHA2-512 KAT (A4446) | SHA2-512 | KAT | CAST | Module is in normal state | HMAC-SHA2-512 | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A4446) | P-256 Curve | KAT | CAST | Module is in normal state | Primitive Z KAT | Power Up |
| KAS-FFC-SSC Sp800-56Ar3 KAT (A4446) | MODP-2048 | KAT | CAST | Module is in normal state | Primitive Z KAT | Power Up |
| RSA SigGen (FIPS186-4) KAT (A4446) | 2048 bit modulus with SHA2-256 | KAT | CAST | Module is in normal state | RSA SigGen KAT | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|--------------------------------|-------------|-----------|---------------------------|-----------------|------------|
| RSA SigVer (FIPS186-4) KAT (A4446) | 2048 bit modulus with SHA2-256 | KAT | CAST | Module is in normal state | RSA SigVer KAT | Power Up |
| KDF IKEv2 KAT (A4446) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| KDF SNMP KAT (A4446) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| KDF SSH KAT (A4446) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| TLS v1.2 KDF RFC7627 KAT (A4446) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| SHA-1 KAT (A4446) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| AES-CBC Encrypt KAT (C1026) | 128 bits | KAT | CAST | Module is in normal state | Encrypt KAT | Power Up |
| AES-CBC Decrypt KAT (C1026) | 128 bits | KAT | CAST | Module is in normal state | Decrypt KAT | Power Up |
| AES-GCM Authenticated Encrypt KAT (C1026) | 128 bits | KAT | CAST | Module is in normal state | Encrypt KAT | Power Up |
| AES-GCM Authenticated Decrypt KAT (C1026) | 128 bits | KAT | CAST | Module is in normal state | Decrypt KAT | Power Up |
| Hash DRBG Instantiate KAT (C1026) | SHA2-512 | KAT | CAST | Module is in normal state | Instantiate KAT | Power Up |
| Hash DRBG Generate KAT (C1026) | SHA2-512 | KAT | CAST | Module is in normal state | Generate KAT | Power Up |
| Hash DRBG Reseed KAT (C1026) | SHA2-512 | KAT | CAST | Module is in normal state | Reseed KAT | Power Up |
| HMAC-SHA-1 KAT (C1026) | SHA-1 | KAT | CAST | Module is in normal state | HMAC-SHA-1 | Power Up |
| HMAC-SHA2-256 KAT (C1026) | SHA2-256 | KAT | CAST | Module is in normal state | HMAC-SHA2-256 | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|--------------------------------------|---------------------------|-------------|-----------|---------------------------|---------------|--|
| HMAC-SHA2-384 KAT (C1026) | SHA2-384 | KAT | CAST | Module is in normal state | HMAC-SHA2-384 | Power Up |
| HMAC-SHA2-512 KAT (C1026) | SHA2-512 | KAT | CAST | Module is in normal state | HMAC-SHA2-512 | Power Up |
| SHA-1 KAT (C1026) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| ECDSA KeyGen (FIPS186-4) PCT (A4446) | Curve P-256 with SHA2-256 | PCT | PCT | Module is in normal state | ECDSA | Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use. |
| RSA KeyGen (FIPS186-4) PCT (A4446) | 2048 bit Modulus | PCT | PCT | Module is in normal state | RSA | Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use. |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A4446) | Curve P-256 with SHA2-256 | PCT | PCT | Module is in normal state | N/A | Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use. |
| KAS-FFC-SSC Sp800- | MODP-2048 | PCT | PCT | Module is in normal state | N/A | Performs all required pair-wise |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|--------------------------|-------------|------------|---------------------------|---|--|
| 56Ar3 PCT (A4446) | | | | | | consistency tests on the newly generated key pairs before the first operational use. |
| Firmware Load Test | HMAC-SHA2-512 | KAT | SW/FW Load | Module is in normal state | N/A | When firmware has been uploaded to the module |
| Entropy 90B Start-up Repetition Count Test (RCT) | Repetition Count Test | RCT | CAST | Module is in normal state | Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time | Power Up |
| Entropy 90B Start-up Adaptive Proportion Test (APT) | Adaptive Proportion Test | APT | CAST | Module is in normal state | Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source | Power Up |
| Entropy 90B Continuous Repetition Count Test (RCT) | Repetition Count Test | RCT | CAST | Module is in normal state | Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time | Entropy data is generated from the Entropy Source - Continuous |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|--------------------------|-------------|-----------|---------------------------|---|--|
| Entropy 90B Continuous Adaptive Proportion Test (APT) | Adaptive Proportion Test | APT | CAST | Module is in normal state | Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source | Entropy data is generated from the Entropy Source - Continuous |

Table 21: Conditional Self-Tests

The module performs on-demand self-tests initiated by the operator, by powering off and powering the module back on. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|--------------------------------|-------------|-----------------|-------------------|-----------------|
| RSA SigVer (FIPS186-4) (A4446) | KAT | SW/FW Integrity | Recommend 60 Days | Reboot |

Table 22: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|-------------|-----------|-------------------|-----------------|
| AES-CBC Encrypt KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-CBC Decrypt KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-GCM Authenticated Encrypt KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-GCM Authenticated Decrypt KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| Counter DRBG Instantiate KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|--------------------------------------|-------------|-----------|-------------------|-----------------|
| Counter DRBG Generate KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| Counter DRBG Reseed KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| ECDSA SigGen (FIPS186-4) KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| ECDSA SigVer (FIPS186-4) KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA-1 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-256 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-384 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-512 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| KAS-FFC-SSC Sp800-56Ar3 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| RSA SigGen (FIPS186-4) KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| RSA SigVer (FIPS186-4) KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| KDF IKEv2 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| KDF SNMP KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| KDF SSH KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| TLS v1.2 KDF RFC7627 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |
| SHA-1 KAT (A4446) | KAT | CAST | Recommend 60 Days | Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|-------------|-----------|-------------------|-----------------|
| AES-CBC Encrypt KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-CBC Decrypt KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-GCM Authenticated Encrypt KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| AES-GCM Authenticated Decrypt KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| Hash DRBG Instantiate KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| Hash DRBG Generate KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| Hash DRBG Reseed KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA-1 KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-256 KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-384 KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| HMAC-SHA2-512 KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| SHA-1 KAT (C1026) | KAT | CAST | Recommend 60 Days | Reboot |
| ECDSA KeyGen (FIPS186-4) PCT (A4446) | PCT | PCT | Recommend 60 Days | Reboot |
| RSA KeyGen (FIPS186-4) PCT (A4446) | PCT | PCT | Recommend 60 Days | Reboot |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A4446) | PCT | PCT | Recommend 60 Days | Reboot |
| KAS-FFC-SSC Sp800-56Ar3 PCT (A4446) | PCT | PCT | Recommend 60 Days | Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|-------------|------------|--------|-----------------|
| Firmware Load Test | KAT | SW/FW Load | N/A | N/A |
| Entropy 90B Start-up Repetition Count Test (RCT) | RCT | CAST | N/A | N/A |
| Entropy 90B Start-up Adaptive Proportion Test (APT) | APT | CAST | N/A | N/A |
| Entropy 90B Continuous Repetition Count Test (RCT) | RCT | CAST | N/A | N/A |
| Entropy 90B Continuous Adaptive Proportion Test (APT) | APT | CAST | N/A | N/A |

Table 23: Conditional Periodic Information

10.4 Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|-------------|--|-------------------|-------------------|-------------|
| Error State | If self-test tests fail, the module is put into an error state | Self-test failure | Reboot the module | System Halt |

Table 24: Error States

If any of the above-mentioned self-tests fail, the module reports the error and enters the Error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The validated module firmware was installed onto the respective test platforms listed in Table 2 above. The Crypto Officer must configure and enforce the following initialization steps:

Step 1: The Crypto Officer must install opacity shields as described in section 7 above.

Step 2: The Crypto Officer must apply tamper evidence labels as described in section 7 above.

Step 3: The Crypto Officer must securely store any unused tamper evidence labels.

Note: Each module has a Type A USB 2.0 port, but it is considered to be disabled once the Crypto Officer has applied the TEL #7.

Step 4: Crypto officer shall perform zeroization operation if the module was previously used before the approved mode configuration.

Step 5: The Crypto Officer shall configure the module to be managed by the Firepower Management Center (FMC), and follow the procedure below from the FMC:

- a) Choose **Devices > Platform Settings** and create or edit a Firepower policy.
- b) On the left click **“UCAPL/CC Compliance”**.
- c) Choose **“CC”** from the dropdown under **“Enable UCAPL/CC Compliance”**.
- d) Click **“Save”** to save the changes.
- e) Click **“Deploy”** and select **“Deploy All”**.

Step 6: The module will automatically reboot, and will be placed in the approved mode once it is done rebooting.

Step 7: Crypto Officer can verify the version installed and running
> show version

Step 8: Crypto Officer can verify the module is in approved mode:
> show fips

Step 9: Assign users a Privilege Level of basic.

Step 10: Configure IP address for unit and all distant endpoints from the FMC.

Step 11: Define RADIUS shared secret keys that are at least 8 characters long and secure traffic between the security module and the RADIUS server via secure (IPSec, TLS) tunnel.

Note: Perform this step only if RADIUS is configured, otherwise proceed.

Step 12: Configure the security module so that any remote connections via Telnet are secured through IPSec.

Step 13: Configure the security module so that only approved algorithms are used for all security connections (SSHv2, TLSv1.2, SNMPv3 and IPSec/IKEv2).

Step 14: Configure the security module so that error messages can only be viewed by Crypto Officer.

Step 15: Enable HTTPS with TLS. HTTPS with TLS should always be used for Web-based management.

Step 16: Ensure that installed digital certificates are signed using approved algorithms.

Step 17: Save and reboot the module.

11.2 Administrator Guidance

Specific Administrator guidance for using Multi-Instance Mode on Secure Firewall 4200 can be found here: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/threat-defense/use-case/multi-instance-sec-fw/multi-instance-sec-fw.html>

11.3 Non-Administrator Guidance

Specific Non-Administrator guidance can be found in the Cisco Secure Firewall 4200 Datasheet: <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/secure-firewall-4200-ds.html>

12 Mitigation of Other Attacks

N/A for this module.