Palo Alto Networks Core Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.3

Revision Date: June 27, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. General

The table below provides the security levels of the various sections of FIPS 140-3 in relation to the Palo Alto Networks Core Crypto Module (hereafter referred to as the Module).

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, Authentication	1
5	Software / Firmware Security	1
6	Operational Environment	1
7	Physical Security	N/A
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

Table 1 - Security Levels

2. Cryptographic Module Specification

The Palo Alto Networks Core Crypto Module is a software cryptographic module that can run on various environments. The module is designed to run on various hardware devices (multi-chip standalone embodiment) and contains a cryptographic boundary. The cryptographic boundary includes all of the logical software components of the module. The physical perimeter is defined by the enclosure around the hardware on which it runs. See below for more details regarding the platforms.

Once initialized, the module provides only an Approved mode of operation that only includes Approved algorithms and key sizes. There is no mechanism to enable non-Approved algorithms or functions. The module is built into PAN-OS/Panorama/WildFire 10.2 and 11.0. It is delivered with the respective Device OS. There is no standalone delivery of the module as a software library. The vendor's internal development process guarantees that the correct version of the module goes with its intended OS.

The Module's software version for this validation is 1.0 and is defined as a software cryptographic module – the cryptographic boundary (CB) includes all of the software components of the module. The physical perimeter (PP) is defined by the enclosure around the host hardware platform.

The module includes the following files that compose the module:

- libssl.so.1.1 and libcrypto.so.1.1, libssl_dpt13.so.1.1 and libcrypto_dpt13.so.1.1, fips_selftest, fips_selftest_dp bg_intg_fips.py, panfastdgst

Non-Compliant State

Failure to follow the directions in the Approved Mode of Operation above and Section 11 will result in the module operating in a non-compliant state.

Note: For Operational Environments which use Panorama or WildFire as the Operating System in Table 2, algorithms from A4207 are not supported.

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	PAN-OS 10.2	PA-410	Intel Denverton C3436L	N/A
2	PAN-OS 11.0	PA-410	Intel Denverton C3436L	N/A
3	PAN-OS 11.0	PA-415	Intel Denverton C3436L	N/A
4	PAN-OS 10.2	PA-440	Intel Denverton C3558R	N/A
5	PAN-OS 11.0	PA-440	Intel Denverton C3558R	N/A
6	PAN-OS 11.0	PA-445	Intel Denverton C3558R	N/A
7	PAN-OS 10.2	PA-450	Intel Denverton C3758R	N/A
8	PAN-OS 11.0	PA-450	Intel Denverton C3758R	N/A
9	PAN-OS 10.2	PA-460	Intel Denverton C3758R	N/A
10	PAN-OS 11.0	PA-460	Intel Denverton C3758R	N/A
11	PAN-OS 10.2	PA-220	Marvell CN7130	N/A
12	PAN-OS 10.2	PA-220R	Marvell CN7130	N/A
13	PAN-OS 10.2	PA-820	Marvell CN7240	N/A
14	PAN-OS 11.0	PA-820	Marvell CN7240	N/A
15	PAN-OS 10.2	PA-850	Marvell CN7240	N/A
16	PAN-OS 11.0	PA-850	Marvell CN7240	N/A
17	PAN-OS 11.0	PA-1410	Intel Atom C5325	N/A
18	PAN-OS 11.0	PA-1420	Intel Atom C5325C1	N/A
19	PAN-OS 10.2	PA-3410	Intel Atom P5332	N/A
20	PAN-OS 11.0	PA-3410	Intel Atom P5332	N/A
21	PAN-OS 10.2	PA-3420	Intel Atom P5342	N/A
22	PAN-OS 11.0	PA-3420	Intel Atom P5342	N/A
23	PAN-OS 10.2	PA-3430	Intel Atom P5352	N/A
24	PAN-OS 11.0	PA-3430	Intel Atom P5352	N/A
25	PAN-OS 10.2	PA-3440	Intel Atom P5362	N/A
26	PAN-OS 11.0	PA-3440	Intel Atom P5362	N/A
27	PAN-OS 10.2	PA-5410	AMD EPYC 7352	N/A
28	PAN-OS 11.0	PA-5410	AMD EPYC 7352	N/A
29	PAN-OS 10.2	PA-5420	AMD EPYC 7452	N/A
30	PAN-OS 11.0	PA-5420	AMD EPYC 7452	N/A
31	PAN-OS 10.2	PA-5430	AMD EPYC 7642	N/A
32	PAN-OS 11.0	PA-5430	AMD EPYC 7642	N/A
33	PAN-OS 11.0	PA-5440	AMD EPYC 7742	N/A
34	PAN-OS 10.2	PA-5450	Intel Xeon D-2187NT	N/A

35	PAN-OS 11.0	PA-5450	Intel Xeon D-2187NT	N/A
36	PAN-OS 10.2	PA-3220	Intel Pentium D1517 / CN7350	N/A
37	PAN-OS 11.0	PA-3220	Intel Pentium D1517 / CN7350	N/A
38	PAN-OS 10.2	PA-3250	Intel Pentium D1517 / CN7350	N/A
39	PAN-OS 11.0	PA-3250	Intel Pentium D1517 / CN7350	N/A
40	PAN-OS 10.2	PA-3260	Intel Pentium D1517 / CN7360	N/A
41	PAN-OS 11.0	PA-3260	Intel Pentium D1517 / CN7360	N/A
42	PAN-OS 10.2	PA-5220	Intel Xeon D-1548 / CN7885	N/A
43	PAN-OS 11.0	PA-5220	Intel Xeon D-1548 / CN7885	N/A
44	PAN-OS 10.2	PA-5250	Intel Xeon D-1567 / CN7890	N/A
45	PAN-OS 11.0	PA-5250	Intel Xeon D-1567 / CN7890	N/A
46	PAN-OS 10.2	PA-5260	Intel Xeon D-1567 / CN7890	N/A
47	PAN-OS 11.0	PA-5260	Intel Xeon D-1567 / CN7890	N/A
48	PAN-OS 10.2	PA-5280	Intel Xeon D-1567 / CN7890	N/A
49	PAN-OS 11.0	PA-5280	Intel Xeon D-1567 / CN7890	N/A
50	PAN-OS 10.2	PA-7050	Intel Xeon D-1567 / CN7890	N/A
51	PAN-OS 11.0	PA-7050	Intel Xeon D-1567 / CN7890	N/A
52	PAN-OS 10.2	PA-7080	Intel Xeon D-1567 / CN7890	N/A
53	PAN-OS 11.0	PA-7080	Intel Xeon D-1567 / CN7890	N/A
54	Panorama 10.2	M-200	Intel Xeon E5-2620 V4	N/A
55	Panorama 11.0	M-200	Intel Xeon E5-2620 V4	N/A
56	Panorama 10.2	M-300	Intel Xeon 4310	N/A
57	Panorama 11.0	M-300	Intel Xeon 4310	N/A
58	Panorama 10.2	M-600	Intel Xeon E5-2680 V4	N/A
59	Panorama 11.0	M-600	Intel Xeon E5-2680 V4	N/A
60	Panorama 10.2	M-700	Intel Xeon 4316	N/A
61	Panorama 11.0	M-700	Intel Xeon 4316	N/A
62	WildFire 10.2	WF-500	Intel Xeon E5-2620	N/A
63	WildFire 11.0	WF-500	Intel Xeon E5-2620	N/A
64	WildFire 10.2	WF-500-B	Intel Xeon 4316	N/A
65	WildFire 11.0	WF-500-B	Intel Xeon 4316	N/A
66	PAN-OS 10.2 with VMware ESXi v7.0	Dell PowerEdge R740	Intel Gold 6248	N/A
67	PAN-OS 11.0 with VMware ESXi v7.0	Dell PowerEdge R740	Intel Gold 6248	N/A
68	PAN-OS 10.2 with KVM on Ubuntu 20.04	Dell PowerEdge R740	Intel Gold 6248	N/A
69	PAN-OS 11.0 with KVM on Ubuntu 20.04	Dell PowerEdge R740	Intel Gold 6248	N/A

70	PAN-OS 10.2 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Gold 6248	N/A
71	PAN-OS 11.0 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Gold 6248	N/A
72	Panorama 10.2 with VMware ESXi v7.0	Dell PowerEdge R740	Intel Gold 6248	N/A
73	Panorama 11.0 with VMware ESXi v7.0	Dell PowerEdge R740	Intel Gold 6248	N/A
74	Panorama 10.2 with KVM on Ubuntu 20.04	Dell PowerEdge R740	Intel Gold 6248	N/A
75	Panorama 11.0 with KVM on Ubuntu 20.04	Dell PowerEdge R740	Intel Gold 6248	N/A
76	Panorama 10.2 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Gold 6248	N/A
77	Panorama 11.0 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Gold 6248	N/A

Table 2 - Tested Operational Environments

#	Operating System	Hardware Platform
1	PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Amazon Web Services (AWS)	x86 Architecture *(Note: Specific processor/hardware is dependent on Instance/Machine Type selected for operation system)*
2	PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Microsoft Azure	
3	PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Google Cloud Platform (GCP)	
4	PAN-OS VM-Series 11.1 or 11.2 with VMware ESXi v7.0	Dell PowerEdge R740
5	PAN-OS VM-Series 11.1 or 11.2 with KVM on Ubuntu 20.04	Dell PowerEdge R740
6	PAN-OS VM-Series 11.1 or 11.2 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740
7	Panorama Virtual Appliance 11.1 or 11.2 with VMware ESXi v7.0	Dell PowerEdge R740
8	Panorama Virtual Appliance 11.1 or 11.2 with KVM on Ubuntu 20.04	Dell PowerEdge R740
9	Panorama Virtual Appliance 11.1 or 11.2 with Microsoft Hyper-V Server 2019	Dell PowerEdge R740
10	PAN-OS 11.1 or PAN-OS 11.2	PA-410, PA-415, PA-440, PA-445, PA-450, PA-460, PA-415-5G, PA-455, PA-450R, PA-410R, PA-450R-5G
11	PAN-OS 11.1	PA-820, PA-850
12	PAN-OS 11.1 or PAN-OS 11.2	PA-1410, PA-1420
13	PAN-OS 11.1 or PAN-OS 11.2	PA-3410, PA-3420, PA-3430, PA-3440
14	PAN-OS 11.1 or PAN-OS 11.2	PA-5410, PA-5420, PA-5430, PA-5440, PA-5445
15	PAN-OS 11.1 or PAN-OS 11.2	PA-5450

16	PAN-OS 11.1	PA-3220, PA-3250, PA-3260
17	PAN-OS 11.1 or PAN-OS 11.2	PA-5220, PA-5250, PA-5260, PA-5280
18	PAN-OS 11.1 or PAN-OS 11.2	PA-7050, PA-7080
19	PAN-OS 11.1 or PAN-OS 11.2	PA-7500
20	Panorama 11.1 or Panorama 11.2	M-200, M-300, M-600, M-700
21	WildFire 11.1 or WildFire 11.2	WF-500, WF-500-B

Table 3 - Vendor Affirmed Operational Environments

The cryptographic modules support the following Approved algorithms. Only the algorithms, modes, and key sizes specified in this table are used by the module. The CAVP certificate may contain more tested options than listed in this table.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A1791	Conditioning Component AES-CBC-MAC SP 800-90B	AES-CBC-MAC	128 bits	Vetted conditioning component for ESV Cert. #E69
A2138				Vetted conditioning component for ESV Cert. #E70
A2153				Vetted conditioning component for ESV Cert. #E68
A2165				Vetted conditioning component for ESV Cert. #E65, E66, E72, E73
A2518				Vetted conditioning component for ESV Cert. #E64
A2541				Vetted conditioning component for ESV Cert. #E71
A4206, A4207	AES-CBC [SP 800-38A]	CBC	128, 192 and 256 bits	Encryption Decryption
A4206, A4207	AES-GCM [SP 800-38D]	GCM	128 and 256 bits Note: 192 tested, but not used	Encryption Decryption
A4206, A4207	Counter DRBG [SP 800-90Arev1]	CTR DRBG	AES 256 bits with Derivation Function Enabled	Random Bit Generator
A4206, A4207	ECDSA KeyGen (FIPS 186-4)	ECDSA KeyGen	P-256, P-384, P-521	Key Generation
A4206, A4207	ECDSA KeyVer (FIPS 186-4)	ECDSA KeyVer	P-256, P-384, P-521	Public Key Validation
A4206, A4207	ECDSA SigGen (FIPS 186-4)	ECDSA SigGen	P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Generation
A4206, A4207	ECDSA SigVer (FIPS 186-4)	ECDSA SigVer	P-256, P-384, P-521 with SHA-1, SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Verification
A4206, A4207	HMAC-SHA-1 [FIPS 198-1]	HMAC	HMAC-SHA-1 with λ=96, 160	Authentication for protocols
A4206, A4207	HMAC-SHA2-224 [FIPS 198-1]	HMAC	HMAC-SHA2-224 with λ=224	Authentication for protocols
A4206, A4207	HMAC-SHA2-256	HMAC	HMAC-SHA2-256 with λ=256	Authentication for protocols

	[FIPS 198-1]			
A4206, A4207	HMAC-SHA2-384 [FIPS 198-1]	HMAC	HMAC-SHA2-384 with λ=384	Authentication for protocols
A4206, A4207	HMAC-SHA2-512 [FIPS 198-1]	HMAC	HMAC-SHA2-512 with λ=512	Authentication for protocols
A4206, A4207	KAS-ECC-SSC Sp800-56Ar3	KAS	ephemeralUnified: P-256/P-384/P-521	Key Exchange
A4206, A4207	KAS-FFC-SSC SP 800-56Ar3	KAS	dhEphem: MODP-2048/3072/4096	Key Exchange
A4206	RSA KeyGen (FIPS 186-4)	RSA KeyGen (FIPS 186-4)	2048, 3072, and 4096 bits	Key Pair Generation
A4206, A4207	RSA SigGen (FIPS 186-4)	RSA SigGen (FIPS 186-4)	2048, 3072, and 4096-bit with hashes SHA2-256/384/512	Signature Generation
A4206, A4207	RSA SigVer (FIPS 186-4)	RSA SigVer (FIPS 186-4)	2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1/SHA2-224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not supported for ANSI X9.31	Signature Verification
A4206, A4207	SHA-1 [FIPS 180-4]	SHA	SHA-1	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A4206, A4207	SHA2-224 [FIPS 180-4]	SHA2	SHA-224	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A4206, A4207	SHA2-256 [FIPS 180-4]	SHA2	SHA-256	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A4206, A4207	SHA2-384 [FIPS 180-4]	SHA2	SHA-384	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A4206, A4207	SHA2-512 [FIPS 180-4]	SHA2	SHA-512	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A4206, A4207	Safe Primes Key Generation [RFC 3526]	Safe Primes Key Generation	MODP-2048/3072/4096	Safe Primes Key Generation
A4206, A4207	Safe Primes Key Verification [RFC 3526]	Safe Primes Key Verification	MODP-2048/3072/4096	Safe Primes Key Verification
A4206, A4207	TLS v1.2 KDF RFC7627 (CVL)	TLS v1.2 KDF RFC7627	TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384	TLS
AES Cert. #A4206 and	KTS [SP 800-38F]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key	AES-CBC plus HMAC 128 or 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping

HMAC Cert. #A4206		wrapping and unwrapping) per IG D.G.		
AES Cert. #A4207 and HMAC Cert. #A4207	KTS [SP 800-38F]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	AES-CBC plus HMAC 128 or 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping
AES-GCM Cert. #A4206	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	AES-GCM 128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping
AES-GCM Cert. #A4207	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	AES-GCM 128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping
ESV Cert. #E27	SP 800-90B	ESV	AMD Random Number Generator	Entropy
ESV Cert. #E64			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E65			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E66			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E68			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E69			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E70			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E71			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E72			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E73			Palo Alto Networks DRNG Entropy Source	
ESV Cert. #E128			Octeon III Entropy Source	
ESV Cert. #E130			Palo Alto Networks RTC Entropy Source	
KAS-ECC-SSC Cert. #A4206, TLS v1.2 KDF RFC7627 Cert. #A4206	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A4207, TLS v1.2 KDF RFC7627 Cert. #A4207	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A4206, TLS v1.2 KDF RFC7627 Cert. #A4206	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	MODP-2048/3072/4096 2048-bit to 4096-bit key providing 112 bits to 150 bits of encryption strength	Key Exchange with protocol KDF

KAS-FFC-SSC Cert. #A4207, TLS v1.2 KDF RFC7627 Cert. #A4207	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	MODP-2048/3072/4096 2048-bit to 4096-bit key providing 112 bits to 150 bits of encryption strength	Key Exchange with protocol KDF
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-133 and IG D.H.	Key Generation Note: The seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG

Table 4 - Approved Algorithms

The module does not have any algorithms that fall under:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with the ciphersuites from section 3.3.1 of SP 800-52rev2 and in accordance with Section 4 of RFC 5288 for TLS key establishment, and ensures when the nonce_explicit part of the IV exhausts all possible values for a given session key, that a new TLS handshake is initiated per sections 7.4.1.1 and 7.4.1.2 of RFC 5246. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
    - From this RFC 5288, the GCM cipher suites in use are TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- No parts of the TLS protocol, other than the KDF, have been tested by the CAVP/CMVP.

The module is compliant to IG C.F:

The module utilizes Approved modulus sizes 2048, 3072, and 4096 bits for RSA signatures. This functionality has been CAVP tested as noted above. The minimum number of Miller Rabin tests for each modulus size is implemented according to Table C.2 of FIPS 186-4. For modulus size 4096, the module implements the largest number of Miller-Rabin tests shown in Table C.2. RSA SigVer is CAVP tested for all three supported modulus sizes as noted above. The module does not perform FIPS 186-2 SigVer. All supported modulus sizes are CAVP testable and tested as noted above. The module does not implement RSA key transport in the approved mode.

In all the above cases, the nonce_explicit is always generated deterministically. AES GCM keys are zeroized when the module is power-cycled. For each new TLS session, a new AES GCM key is established.

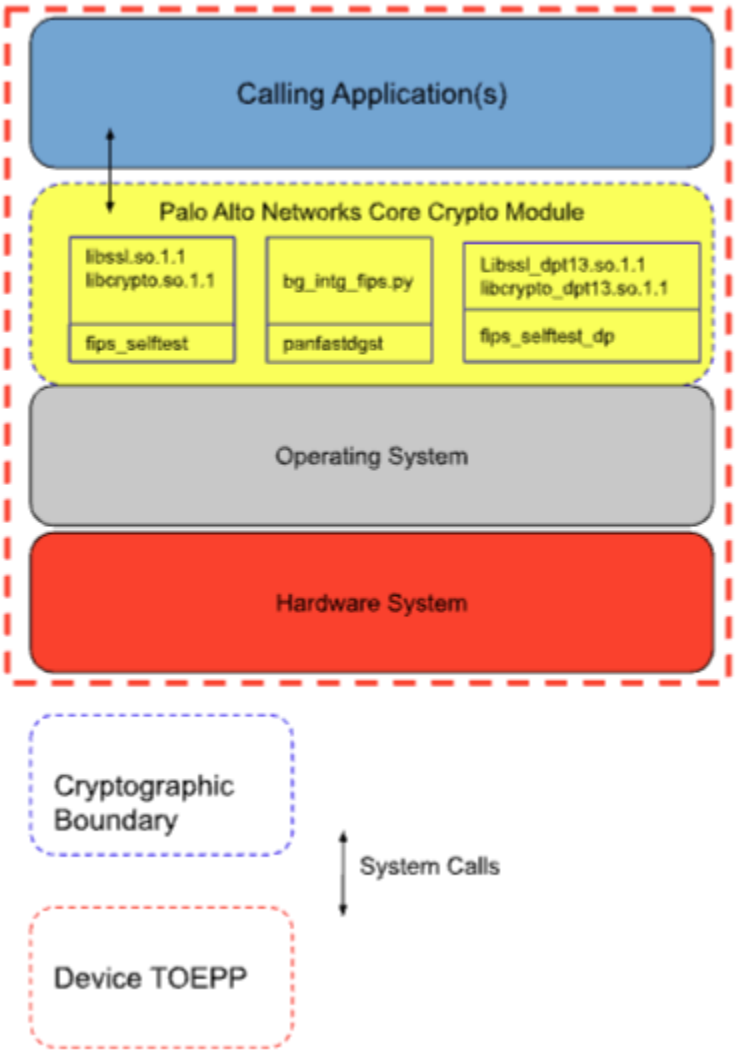

Figure 1 - Cryptographic Boundary

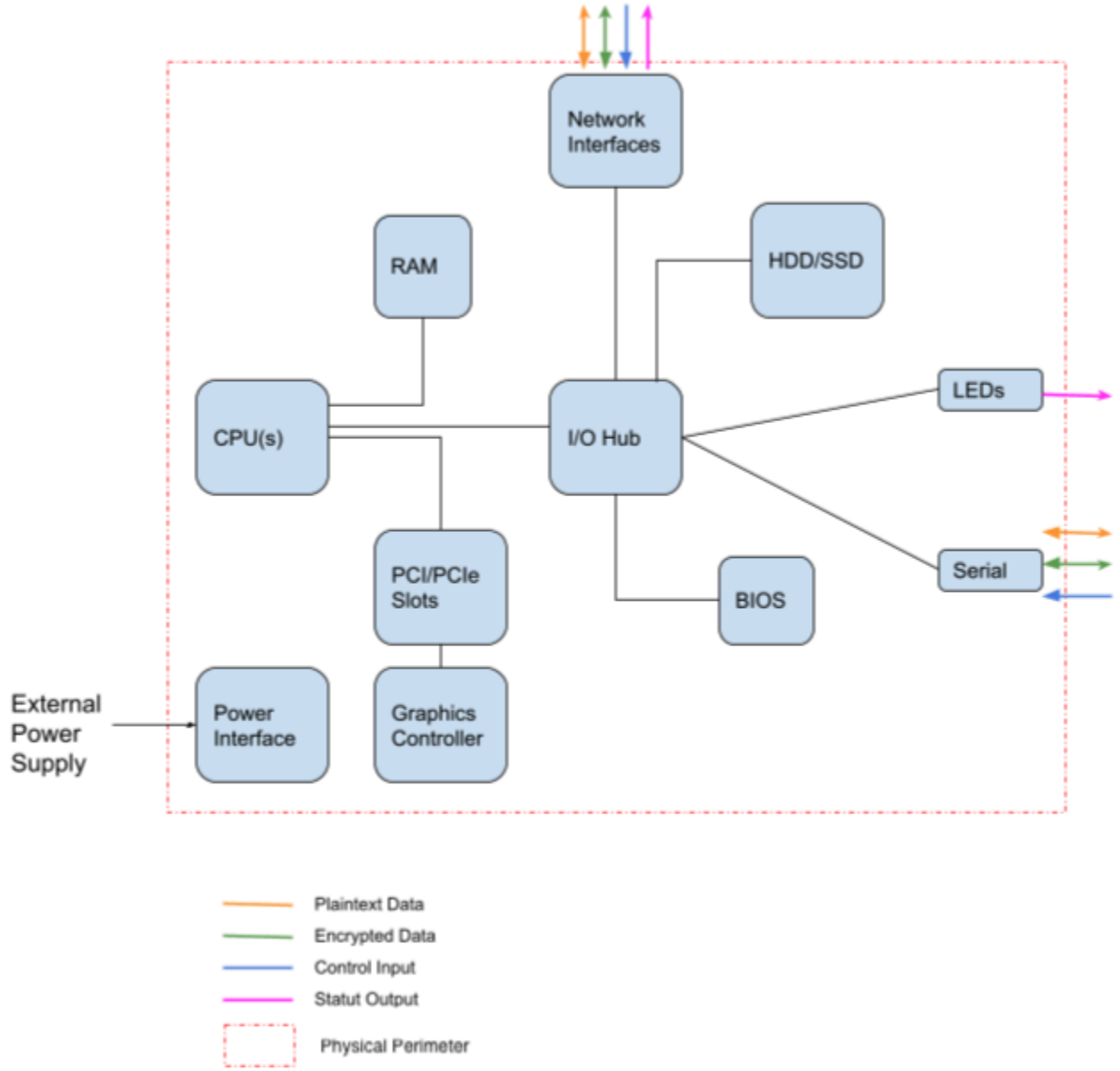

Figure 1A - Physical Perimeter

3. Cryptographic Module Interfaces

The module is a software module and does not have any physical ports, but the hardware platform that the module executes on has physical ports.

The module does not support a control output interface.

Physical Port	Logical Interface	Data that passes over port/interface
Physical ports of the tested platform	Status Output	API return values
Physical ports of the tested platform	Data Input	API input parameters
Physical ports of the tested platform	Data Output	API output parameters and return values
Physical ports of the tested platform	Control Input	API input parameters

Table 5 - Ports and Interfaces

4. Roles, Services, and Authentication

Roles

The module implements only one role, which is the Crypto Officer (CO) role. There is no User role supported.

The module does not support operator authentication. The CO role is implicitly assumed by the entity accessing services implemented by the module. No further authentication is required.

The module does not provide a maintenance role or bypass capability.

Services

The Approved services supported by the module are noted in the following table:

Role	Service	Input	Output
CO	Initialize	API to initialize module	Status of initialization of module
CO	Self-test	API for running self-test	Status of the self-test results
CO	Show Status	API for show status	Module's status information
CO	Show Module Version	API for module version	Module's name and version
CO	Zeroize	API for zeroization	Status of zeroization
CO	Random Number Generation	API for random number generator	Random number provided
CO	Asymmetric Key Generation	API for asymmetric key generation	Module generated asymmetric key
CO	Symmetric Encrypt/Decrypt	API for encrypting/decrypting	Module performs encrypt/decrypting with a symmetric key
CO	Message Digest	API for message digest	Module provides hash for calling application
CO	Keyed Hash	API for keyed hash	Module provides keyed hash for calling application
CO	Key Wrapping	API for key wrapping	Module provides key wrapping service for calling application
CO	Digital Signature	API for digital signature	Module performs digital signature functions for calling application
CO	Crypto Protocols	API for TLS crypto protocol	Module provides crypto protocol processing for calling application

Table 6 - Roles, Service Commands, Input and Output

The following table defines the relationship between access to SSPs and the different module services. The module performs key generation in accordance with the applicable protocol/algorithm. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG. The calling application is responsible for storage of generated keys returned by the module.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Initialize	Module performs initialization procedures for Approved mode	N/A	N/A	CO	N/A	Global indicator ("FIPS-CC" mode) and System logs
Self-test	Performs self-tests including software integrity verification	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4)	Software Integrity Verification Key	CO	E	Global indicator ("FIPS-CC" mode) and System logs
Show Status	Function that provides module status information	N/A	N/A	CO	N/A	Global indicator ("FIPS-CC" mode) and System logs
Show Module Version	Function that provides the module's name and version	N/A	N/A	CO	N/A	Global indicator ("FIPS-CC" mode) and System logs
Zeroize	Function that destroys all SSPs	N/A	All keys and SSPs	CO	Z	Zeroization indicator
Random Number Generation	Used for random number generation	Counter DRBG, ESV	DRBG Seed	CO	G/E	Global indicator ("FIPS-CC" mode) and System logs
			DRBG V			
			Entropy Input String			
			DRBG Key			
Asymmetric Key Generation	Used to generate asymmetric keys	CKG, Counter DRBG, ESV RSA KeyGen (FIPS 186-4) ECDSA KeyGen (FIPS 186-4)	RSA Private Keys, RSA Public Keys ECDSA Private Keys, ECDSA Public Keys, CA Certificates	CO	G/W/E	Global indicator ("FIPS-CC" mode) and System logs
			DRBG Seed		G/E	
			DRBG V			
			Entropy Input String			
			DRBG Key			
Symmetric Encrypt/Decrypt	Used to encrypt/decrypt data	AES-CBC AES-GCM	TLS Encryption Keys	CO	W/E	Global indicator ("FIPS-CC" mode) and System logs
Message Digest	Used to generate a SHA message digest	SHA2-256 SHA2-384 SHA2-512	N/A	CO	N/A	Global indicator ("FIPS-CC" mode) and System logs
Keyed Hash	Used to generate or verify data integrity with HMAC	HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys	CO	G/R/W/E	Global indicator ("FIPS-CC" mode) and System logs
Key Wrapping	Used to encrypt or decrypt a key value on behalf of the calling application	KTS: AES-GCM	TLS Encryption Keys	CO	R/E	Global indicator ("FIPS-CC" mode) and System logs
		KTS: AES-CBC				
		KTS: HMAC-SHA 2-256 HMAC-SHA 2-384	TLS HMAC Keys			
Digital Signature	Used to generate or verify RSA/ECDSA digital signatures	RSA SigGen	RSA Private Keys	CO	G/R/W/E	Global indicator ("FIPS-CC" mode) and System logs
		RSA SigVer	RSA Public Keys			
		ECDSA SigGen	ECDSA Private Keys			
		ECDSA SigVer	ECDSA Public Keys			

		Counter DRBG, ESV		DRBG Seed		G/E	Global indicator ("FIPS-CC" mode) and System logs
				DRBG V			
				Entropy Input String			
				DRBG Key			
Crypto Protocols	Used to support crypto protocols for TLS	KAS-ECC-SSC KAS-FFC-SSC	TLS v1.2 KDF RFC7627	TLS Pre-Master Secret	CO	G/E/Z	Global indicator ("FIPS-CC" mode) and System logs
			TLS v1.2 KDF RFC7627	TLS Master Secret			
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components			
				TLS DHE/ECDHE Public Components			
		KTS	HMAC-SHA 2-256 HMAC-SHA 2-384	TLS HMAC Keys			
			AES-CBC	TLS Encryption Keys			
		KTS	AES-GCM				
		Counter DRBG, ESV		DRBG Seed		G/E	
				DRBG V			
				Entropy Input String			
				DRBG Key			

Table 7 - Approved Services

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Note: There is no table for non-Approved services as the module only supports Approved services.

5. Software/Firmware Security

The module performs the Software Integrity test by using HMAC-SHA-256 (HMAC Cert. #A4206) and ECDSA signature verification (ECDSA Cert. #A4206) during the Pre-Operational Self-Test.

6. Operational Environment

The module will operate in a modifiable operational environment per the FIPS 140-3 definition. The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The external application that makes calls to the module is the single user of the module, even when the application is serving multiple clients.

For a listing of tested environments, see Table 2 and Table 3 above. The module is also available in other environments besides the tested environment if the module's show status outputs the proper name and version as noted in Section 11.

The CMVP allows user porting of a validated software module to an operational environment which was not included as part of the validation testing. An operator may install and run the Palo Alto Networks Crypto Module on any general purpose computer (GPC) or platform using the specified hypervisor and operating system on the validation certificate or other compatible operating and/or hypervisor system and affirm the modules continued FIPS 140-3 validation compliance.

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an operational environment not listed on the validation certificate.

7. Physical Security

There are no applicable FIPS 140-3 physical security requirements as this is a software module.

8. Non-Invasive Security

No approved non-invasive attack mitigation test metrics are defined at this time.

9. Sensitive Security Parameters

The following table details all the sensitive security parameters utilized by the module.

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related Keys
CA Certificates	112 bits minimum	RSA SigVer (FIPS 186-4), ECDSA SigVer (FIPS 186-4) Cert. #A4206, A4207	DRBG, FIPS 186-4	Imported/Exported through API calls	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)
RSA Public Keys	112 bits minimum	RSA SigVer (FIPS 186-4) RSA Cert. #A4206, A4207	DRBG, FIPS 186-4	Imported/Exported through API calls	N/A	HDD/RAM – plaintext	Zeroize Service	RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication.

								(RSA 2048, 3072, or 4096-bit)
RSA Private Keys	112 bits minimum	RSA SigGen (FIPS 186-4) Cert. #A4206, A4207	DRBG, FIPS 186-4	Imported/Exported through API calls	N/A	RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)
ECDSA Public Keys	128 bits minimum	ECDSA SigVer (FIPS 186-4) Cert. #A4206, A4207	DRBG, FIPS 186-4	Imported/Exported through API calls	N/A	HDD/RAM – plaintext	Zeroize Service	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)
ECDSA Private Keys	128 bits minimum	ECDSA SigGen (FIPS 186-4) Cert. #A4206, A4207	DRBG, FIPS 186-4	Imported/Exported through API calls	N/A	RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)
TLS DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC, KAS-FFC-SSC Cert. #A4206, A4207	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)
TLS DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC, KAS-FFC-SSC Cert. #A4206, A4207	DRBG, SP 800-56A Rev. 3	Imported/Exported through API calls	N/A	N/A	Zeroize at session termination	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521)
TLS Pre-Master Secret	N/A	TLS v1.2 KDF RFC7627 Cert. #A4206, A4207	KAS SP 800-56A Rev. 3	N/A	TLS	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS Master Secret along with client and server random nonces
TLS Master Secret	N/A	TLS v1.2 KDF RFC7627 Cert. #A4206, A4207	TLS v1.2 KDF RFC7627	N/A	TLS	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS session keys
TLS Encryption Keys	128 bits minimum	AES-CBC, AES-GCM Cert. #A4206, A4207	TLS v1.2 KDF RFC7627	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)
TLS HMAC Keys	160 bits minimum	HMAC-SHA2-256, HMAC-SHA2-384 Cert. #A4206, A4207	TLS v1.2 KDF RFC7627	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	HMAC keys used in TLS connections (SHA-1, 256, 384) (160, 256, 384 bits)
Software Integrity Verification Key	128 bits	HMAC-SHA2-256,	N/A	N/A	N/A	HDD - plaintext	N/A	Used to check the integrity of

(not considered an SSP)		ECDSA SigVer (FIPS 186-4) Cert. #A4206, A4207						crypto-related code. (HMAC-SHA-256 and ECDSA P-256)
DRBG Seed	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A4206, A4207	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	DRBG seed coming from the entropy source Seed length = 384 bits
DRBG V	128 bits	CKG (vendor affirmed), Counter DRBG Cert. #A4206, A4207	Constructed as per SP 800-90A	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state (V) used in the generation of a random values
DRBG Key	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A4206, A4207	Constructed as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG State (Key) used in the generation of random values
Entropy Input String	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A4206, A4207	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	DRBG input string coming from the entropy source Input length = 384 bits

Table 10 - Sensitive Security Parameters

Note: SSPs are implicitly zeroized when power is lost, or explicitly zeroized by the zeroize service. In the case of implicit zeroization, the SSPs are implicitly overwritten with random values due to their ephemeral memory being reset upon power loss. For the zeroization service and zeroization at session termination, the SSP's memory location is overwritten with random values.

Entropy Source	Minimum number of bits of entropy	Details
AMD Random Number Generator	256 bits	The module uses entropy provided by AMD's entropy source, which is covered by ESV Cert. #E27. There are no configuration settings needed for this entropy source as per the ESV PUD. Source produces 0.312358 bits of entropy per 128 bit output. Each seed is 384 bits in size. Module provides a minimum of 256 bits of entropy when initialized as per the rules in Section 11.
Palo Alto Networks DRNG Entropy Source	256 bits	The module uses entropy provided by the following ESV Certificates: E64, E65, E66, E68, E69, E70, E71, E72, E73. There are no configuration settings needed for this entropy source as per the ESV PUD. Source produces full entropy in the 384 bit seed.
Octeon III Entropy Source	256 bits	The module uses entropy provided by the following ESV Certificates: E128. Source produces 0.5066 bits of entropy per bit output. Each seed is 384 bits in size. Module provides a minimum of 256 bits of entropy when initialized as per the rules in Section 11.
Palo Alto Networks RTC Entropy Source	256 bits	The module uses entropy provided by the following ESV Certificates: E130. Source produces 0.5069 bits of entropy. Each seed is 384 bits in size. Module provides a minimum of 256 bits of entropy when initialized as per the rules in Section 11.

Table 11 - Non-Deterministic Random Number Generation Specification

Note: These entropy sources are provided by the platforms themselves listed in Table 2 and Table 3, which are external to the module itself.

10. Self-Tests

The cryptographic module automatically performs the following tests below when the module is loaded (i.e. at power on or reboot). The operator can command the module to perform the pre-operational and cryptographic algorithm self-tests by cycling power of the module; these tests do not require any additional operator action.

Algorithm	Self-Test Details
Software Integrity Test	HMAC-SHA-256 Digital signature verification using ECDSA P-256 Note: The ECDSA and HMAC-SHA-256 KATs are performed prior to the Software integrity test

Table 12 - Pre-Operational Self-Test

Algorithm	Self-Test Details
AES	KAT using AES ECB 128 bits (Encrypt) Note: Only used for satisfying self-test requirements.
AES	KAT using AES ECB 128 bits (Decrypt) Note: Only used for self-test.
AES	KAT using AES CMAC 128 bits (Self-tested, but not used)
AES GCM	KAT using AES GCM 256 bits (Encrypt)
AES GCM	KAT using AES GCM 256 bits (Decrypt)
DRBG	KAT: CTR_DRBG (256 bits) Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed (i.e. instantiate/generate/reseed)
ECDSA	KAT using P-256, P-384, P-521 (Sign/Verify)
HMAC	KAT using HMAC-SHA-1/256/384/512
RSA	KAT using RSA 2048 bits and SHA-256 (Sign/Verify) KAT using RSA 2048 bits with SHA-256 (Encrypt/Decrypt) (Self-tested, but not used)
SHA	KAT using SHA-1/256/384/512
SP 800-56Arev3 KAS-ECC-SSC	KAT using KAS-ECC-SSC (Shared Secret Computation) primitive Z value (P-256/384)
SP 800-56Arev3 KAS-FFC-SSC	KAT using KAS-FFC-SSC (Shared Secret Computation) primitive Z value (2048 bits)
SP 800-135 KDF	KAT for TLS 1.2 KDF

Table 13 - Conditional Cryptographic Algorithm Self-Tests

Algorithm	Self-Test Details
ECDSA	ECDSA Pair-Wise Consistency Test (PCT)
RSA	RSA Pair-Wise Consistency Test (PCT)

Table 14 - Conditional Pair-Wise Consistency Tests

Algorithm	Self-Test Details
SP 800-56Arev3 KAS-ECC-SSC /KAS-FFC-SSC	SP 800-56Arev3 Assurance Tests based on Sections 5.5.2, 5.6.2, and 5.6.3

Table 15 - Conditional Critical Function Tests

Error Handling

In the event of a conditional test failure, the module will output a description of the error. These are summarized below.

Table 16 - Errors and Indicators

Cause of Error	Error State Indicator
Conditional Cryptographic Algorithm Self-Test or Software Integrity Test Failure	FIPS-CC mode failure. <Algorithm test> failed.
Conditional Pairwise Consistency or Critical Functions Test Failure	System log prints an error message.

11. Life-Cycle Assurance

The module is provided directly to solution developers, and is not directly available for the general public to download. The Palo Alto Networks Core Crypto Module is not distributed as a standalone library, and can only be used in conjunction with the platforms listed in Table 2 and Table 3. For details regarding secure installation, initialization, startup, and operation of the module, see below. The steps below are required to place the module in a compliant state. Failure to do so will result in the module operating in a non-compliant state.

Secure Operation

The module is initialized via the following procedure:

1. During the initial boot-up, break the boot sequence by entering “maint” to access the main menu
    a. Note: PAN-OS / Panorama / WildFire version 10.2 or 11.0 is required to access APIs of the module
2. Select “Continue”
3. Select “Set FIPS-CC Mode” option to enter “FIPS-CC” mode (i.e. Approved mode)
4. Select “Enable FIPS-CC Mode”
5. When prompted, select “Reboot” and the module will re-initialize and continue into “FIPS-CC” mode
    a. The module will perform all necessary self-tests as part of initialization

6. The module will provide a status output indicator via the PAN-OS/Panorama/WildFire API that queries the module, and provide the following:
    a. “FIPS-CC Failure”: In event of an initialization failure, the module will provide this output
    b. “FIPS-CC mode enabled successfully”: Module provides this output if initialization is successful

The module’s show status can be seen by initiating the following command, which provides the name of the module and version:

- Enter “debug system crypto-module-version”
    - The module will output the name and version:
        - Palo Alto Networks Core Crypto Module
        - Version 1.0

End of Life / Sanitization

Cryptographic Officers should follow the procedure below for secure destruction of the module. Note: PAN-OS/Panorama/WildFire 10.2 or 11.0 is required to access the APIs of the module.

1. Command the module to enter maintenance-mode (Note: This is not the FIPS 140-3 maintenance mode)
2. Once reboot is complete, select “Continue” and select “Factory Reset”
3. The module will perform the zeroization procedure and provide the following output once complete:
    a. “Factory Reset Status: Success”

Vendor Imposed Security Rules

1. For platforms with an AMD processor, the Crypto Officer is required to allow a system uptime of 273 hours to pass before using services to ensure proper instantiation of the DRBG.
2. For platforms with a C7XXX processor or using the RTC entropy source (WF-500), the Crypto Officer is required to allow a system uptime of 1 hour to pass before using services to ensure proper instantiation of the DRBG.

System uptime is checked via the OS CLI using the command: “show system info | match uptime”

12. Mitigation of Other Attacks

The module is not designed to mitigate any specific attacks outside the scope of FIPS 140-3. These requirements are not applicable.

Appendix A - References

[FIPS 140-3] FIPS Publication 140-3 Security Requirements for Cryptographic Modules