Palo Alto Networks

Palo Alto Networks Core Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 19
2.4 Modes of Operation 19
2.5 Algorithms 20
2.6 Security Function Implementations 24
2.7 Algorithm Specific Information 29
IG C.H Conformance: 29
IG C.F Conformance: 29
IG C.K Conformance: 30
IG D.G Conformance: 30
2.8 RBG and Entropy 30
2.9 Key Generation 33
2.10 Key Establishment 33
2.10.1 Key Agreement 33
2.10.2 Key Transport 33
2.11 Industry Protocols 34
3 Cryptographic Module Interfaces 34
3.1 Ports and Interfaces 34
4 Roles, Services, and Authentication 34
4.1 Authentication Methods 34
4.2 Roles 34
4.3 Approved Services 34
4.4 Non-Approved Services 41
4.5 External Software/Firmware Loaded 41
5 Software/Firmware Security 41
5.1 Integrity Techniques 41
5.2 Initiate on Demand 42

6 Operational Environment 43
6.1 Operational Environment Type and Requirements 43
7 Physical Security 43
8 Non-Invasive Security9 Sensitive Security Parameters Management 43
9.1 Storage Areas 43
9.2 SSP Input-Output Methods 43
9.3 SSP Zeroization Methods 44
9.4 SSPs 44
10 Self-Tests 51
10.1 Pre-Operational Self-Tests 51
10.2 Conditional Self-Tests 51
10.3 Periodic Self-Test Information 56
10.4 Error States 59
11 Life-Cycle Assurance 60
11.1 Installation, Initialization, and Startup Procedures 60
11.2 Administrator Guidance 60
11.3 Non-Administrator Guidance 60
11.6 End of Life 60
12 Mitigation of Other Attacks 61

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 8
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 19
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 19
Table 5: Modes List and Description 20
Table 6: Approved Algorithms 23
Table 7: Vendor-Affirmed Algorithms 23
Table 8: Security Function Implementations 29
Table 9: Entropy Certificates 30
Table 10: Entropy Sources 32
Table 11: Ports and Interfaces 34
Table 12: Roles 34
Table 13: Approved Services 41
Table 14: Storage Areas 43
Table 15: SSP Input-Output Methods 44

Table 16: SSP Zeroization Methods 44
Table 17: SSP Table 1 49
Table 18: SSP Table 2 50
Table 19: Pre-Operational Self-Tests 51
Table 20: Conditional Self-Tests 56
Table 21: Pre-Operational Periodic Information 57
Table 22: Conditional Periodic Information 59
Table 23: Error States 59

List of Figures

Figure 1 - Cryptographic Boundary 7

1 General

1.1 Overview

This document may freely be reproduced and distributed in its entirety.

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).

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and 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
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

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, 11.0, 11.1 and 11.2. 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 or 1.1 (see note under operational environments) 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

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The Palo Alto Networks Core Crypto Module is a software cryptographic module that runs on various hardware devices (multi-chip standalone embodiment).

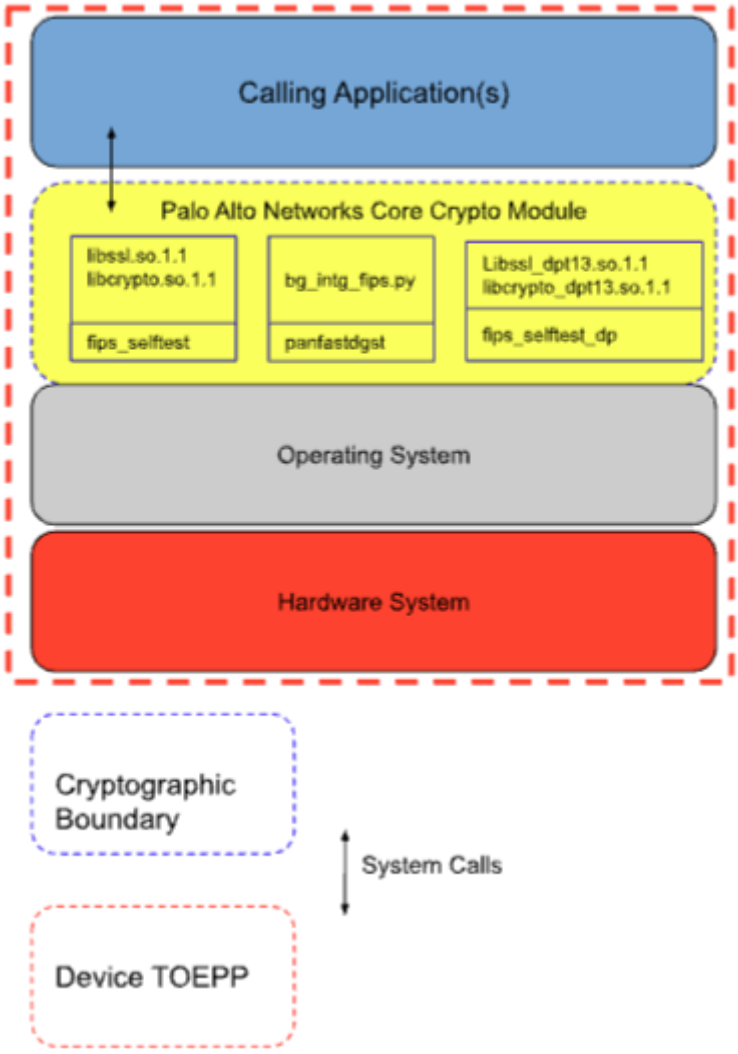

Figure 1 - Cryptographic Boundary

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical perimeter (PP) is defined by the enclosure around the host hardware platform.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
bg_intg_fips.py, fips_selftest, libcrypto.so.1.1, libcrypto_dpt13.so.1.1, libssl.so.1.1, libssl_dpt13.so.1.1, panfastdgst	1.0 (x86_64)	N/A	Yes
bg_intg_fips.py, fips_selftest, libcrypto.so.1.1, libcrypto_dpt13.so.1.1, libssl.so.1.1, libssl_dpt13.so.1.1, panfastdgst	1.0 (MIPS64)	N/A	Yes
bg_intg_fips.py, fips_selftest, libcrypto.so.1.1, libssl.so.1.1, panfastdgst	1.0 (Panorama/WildFire x86_64)	N/A	Yes
bg_intg_fips.py, fips_selftest, libcrypto.so.1.1, libcrypto_dpt13.so.1.1, libssl.so.1.1, libssl_dpt13.so.1.1, panfastdgst	1.1 (x86_64)	N/A	Yes

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 10.2	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (x86_64)
PAN-OS 10.2	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (x86_64)
PAN-OS 10.2	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (x86_64)
PAN-OS 10.2	PA-220	Marvell CN7130	No	N/A	1.0 (MIPS64)
PAN-OS 10.2	PA-220R	Marvell CN7130	No	N/A	1.0 (MIPS64)
PAN-OS 10.2	PA-3220	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-3250	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-3260	Intel Pentium D1517 / CN7360	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-3410	Intel Atom P5332	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-3420	Intel Atom P5342	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-3430	Intel Atom P5352	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-3440	Intel Atom P5362	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-410	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-440	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-450	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-460	Intel Denverton C3758R	No	N/A	1.0 (x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 10.2	PA-5220	Intel Xeon D-1548 / CN7885	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-5250	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-5260	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-5280	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-5410	AMD EPYC 7352	No	N/A	1.1 (x86_64)
PAN-OS 10.2	PA-5420	AMD EPYC 7452	No	N/A	1.1 (x86_64)
PAN-OS 10.2	PA-5430	AMD EPYC 7642	No	N/A	1.1 (x86_64)
PAN-OS 10.2	PA-5450	Intel Xeon D-2187NT	No	N/A	1.0 (x86_64)
PAN-OS 10.2	PA-7050	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-7080	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 10.2	PA-820	Marvell CN7240	No	N/A	1.0 (MIPS64)
PAN-OS 10.2	PA-850	Marvell CN7240	No	N/A	1.0 (MIPS64)
PAN-OS 11.0	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (x86_64)
PAN-OS 11.0	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (x86_64)
PAN-OS 11.0	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (x86_64)
PAN-OS 11.0	PA-1410	Intel Atom C5325	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-1420	Intel Atom C5325C1	No	N/A	1.0 (x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.0	PA-3220	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-3250	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-3260	Intel Pentium D1517 / CN7360	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-3410	Intel Atom P5332	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-3420	Intel Atom P5342	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-3430	Intel Atom P5352	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-3440	Intel Atom P5362	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-410	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-415	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-440	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-445	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-450	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-460	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-5220	Intel Xeon D-1548 / CN7885	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-5250	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-5260	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.0	PA-5280	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-5410	AMD EPYC 7352	No	N/A	1.1 (x86_64)
PAN-OS 11.0	PA-5420	AMD EPYC 7452	No	N/A	1.1 (x86_64)
PAN-OS 11.0	PA-5430	AMD EPYC 7642	No	N/A	1.1 (x86_64)
PAN-OS 11.0	PA-5440	AMD EPYC 7742	No	N/A	1.1 (x86_64)
PAN-OS 11.0	PA-5450	Intel Xeon D-2187NT	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-7050	PA-7050	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-7080	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.0	PA-820	Marvell CN7240	No	N/A	1.0 (x86_64)
PAN-OS 11.0	PA-850	Marvell CN7240	No	N/A	1.0 (x86_64)
PAN-OS 11.1	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (x86_64)
PAN-OS 11.1	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (x86_64)
PAN-OS 11.1	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (x86_64)
PAN-OS 11.1	PA-1410	Intel Atom C5325	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-1420	Intel Atom C5325C1	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3220	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3250	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3260	Intel Pentium D1517 / CN7360	No	N/A	1.0 (x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.1	PA-3410	Intel Atom P5332	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3420	Intel Atom P5342	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3430	Intel Atom P5352	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-3440	Intel Atom P5362	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-410	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-410R	Intel Denverton C3508	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-410R-5G	Intel Denverton C3508	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-415	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-415-5G	Intel Atom C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-440	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-445	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-450	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-450R	Intel Atom C3708	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-450R-5G	Intel Atom C3708	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-455	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-460	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-5220	Intel Xeon D-1548 / CN7885	No	N/A	1.0 (x86_64) 1.0 (MIPS64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.1	PA-5250	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.1	PA-5260	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.1	PA-5280	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.1	PA-5410	AMD EPYC 7352	No	N/A	1.1 (x86_64)
PAN-OS 11.1	PA-5420	AMD EPYC 7452	No	N/A	1.1 (x86_64)
PAN-OS 11.1	PA-5430	AMD EPYC 7642	No	N/A	1.1 (x86_64)
PAN-OS 11.1	PA-5440	AMD EPYC 7742	No	N/A	1.1 (x86_64)
PAN-OS 11.1	PA-5445	AMD EPYC 7713P	No	N/A	1.1 (x86_64)
PAN-OS 11.1	PA-5450	Intel Xeon D-2187NT	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-7050	PA-7050	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-7080	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.1	PA-7500	Intel Atom P5752, Intel Xeon D-2798NX, Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.1	PA-820	Marvell CN7240	No	N/A	1.0 (MIPS64)
PAN-OS 11.1	PA-850	Marvell CN7240	No	N/A	1.0 (MIPS64)
PAN-OS 11.2	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (x86_64)
PAN-OS 11.2	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.2	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (x86_64)
PAN-OS 11.2	PA-1410	Intel Atom C5325	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-1420	Intel Atom C5325C1	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-3220	Intel Pentium D1517 / CN7350	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.2	PA-3410	Intel Atom P5332	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-3420	Intel Atom P5342	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-3430	Intel Atom P5352	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-3440	Intel Atom P5362	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-410	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-410R	Intel Denverton C3508	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-410R-5G	Intel Denverton C3508	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-415	Intel Denverton C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-415-5G	Intel Atom C3436L	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-440	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-445	Intel Denverton C3558R	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-450	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-450R	Intel Atom C3708	No	N/A	1.0 (x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
PAN-OS 11.2	PA-450R-5G	Intel Atom C3708	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-455	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-455-5G	Intel Denverton C3708	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-460	Intel Denverton C3758R	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-5220	Intel Xeon D-1548 / CN7885	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.2	PA-5250	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.2	PA-5260	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.2	PA-5280	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
PAN-OS 11.2	PA-5410	AMD EPYC 7352	No	N/A	1.1 (x86_64)
PAN-OS 11.2	PA-5420	AMD EPYC 7452	No	N/A	1.1 (x86_64)
PAN-OS 11.2	PA-5430	AMD EPYC 7642	No	N/A	1.1 (x86_64)
PAN-OS 11.2	PA-5440	AMD EPYC 7742	No	N/A	1.1 (x86_64)
PAN-OS 11.2	PA-5445	AMD EPYC 7713P	No	N/A	1.1 (x86_64)
PAN-OS 11.2	PA-5450	Intel Xeon D-2187NT	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-7050	PA-7050	No	N/A	1.0 (x86_64)
PAN-OS 11.2	PA-7080	Intel Xeon D-1567 / CN7890	No	N/A	1.0 (x86_64) 1.0 (MIPS64)
Panorama 10.2	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (Panorama/WildFire x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Panorama 10.2	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (Panorama/WildFire x86_64)
Panorama 10.2	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (Panorama/WildFire x86_64)
Panorama 10.2	M-200	Intel Xeon E5-2620 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 10.2	M-300	Intel Xeon 4310	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 10.2	M-600	Intel Xeon E5-2680 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 10.2	M-700	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	M-200	Intel Xeon E5-2620 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	M-300	Intel Xeon 4310	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	M-600	Intel Xeon E5-2680 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.0	M-700	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (Panorama/WildFire x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Panorama 11.1	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	M-200	Intel Xeon E5-2620 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	M-300	Intel Xeon 4310	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	M-600	Intel Xeon E5-2680 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.1	M-700	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	Dell PowerEdge R740	Intel Gold 6248	No	KVM on Ubuntu 20.04	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	Dell PowerEdge R740	Intel Gold 6248	No	Microsoft Hyper-V Server 2019	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	M-200	Intel Xeon E5-2620 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	M-300	Intel Xeon 4310	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	M-600	Intel Xeon E5-2680 V4	No	N/A	1.0 (Panorama/WildFire x86_64)
Panorama 11.2	M-700	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 10.2	WF-500	Intel Xeon E5-2620	No	N/A	1.0 (Panorama/WildFire x86_64)

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
WildFire 10.2	WF-500-B	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.0	WF-500	Intel Xeon E5-2620	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.0	WF-500-B	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.1	WF-500	Intel Xeon E5-2620	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.1	WF-500-B	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.2	WF-500	Intel Xeon E5-2620	No	N/A	1.0 (Panorama/WildFire x86_64)
WildFire 11.2	WF-500-B	Intel Xeon 4316	No	N/A	1.0 (Panorama/WildFire x86_64)

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Amazon Web Services (AWS)	x86 Architecture
PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Google Cloud Platform (GCP)	x86 Architecture
PAN-OS VM-Series or Panorama Virtual Appliance 10.2, 11.0, 11.1, or 11.2 on Microsoft Azure	x86 Architecture

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

N/A

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module has one approved mode of operation and is always in approved mode after initialization	Approved	Global indicator ("FIPS-CC")

Table 5: 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.

Mode Change Instructions and Status:

See Life-Cycle Assurance section.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4206	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A4207	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4206	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
AES-GCM	A4207	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A4206	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
Counter DRBG	A4207	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4206	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-4)	A4207	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4206	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4207	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4206	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4207	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4206	Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4207	Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA2-256	A4206	MAC - MAC: 256 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4207	MAC - MAC: 256 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4206	MAC - MAC: 384 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4207	MAC - MAC: 384 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4206	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A4207	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	A4206	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096 Hash Function Z - SHA2-256, SHA2-384	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		Scheme - dhEphem - KAS Role - initiator, responder	
KAS-FFC-SSC Sp800-56Ar3	A4207	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096 Hash Function Z - SHA2-256, SHA2-384 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA KeyGen (FIPS186-4)	A4206	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Fixed Fixed Public Exponent - 010001 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4206	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigGen (FIPS186-4)	A4207	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4206	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
RSA SigVer (FIPS186-4)	A4207	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
Safe Primes Key Generation	A4206	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Generation	A4207	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A4206	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A4207	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA-1	A4206	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA-1	A4207	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-224	A4206	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4207	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A4206	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4207	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A4206	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4207	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A4206	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4207	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4206	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.2 KDF RFC7627 (CVL)	A4207	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Note: For Operational Environments which use Panorama or WildFire as the Operating System in Table 2.2, algorithms from A4207 are not supported. Only the algorithms specified in the table above are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG		N/A	Section 4 Example 1

Table 7: 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
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A4206, A4207)
KAS-ECC (TLSv1.2)	KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A4206, A4207) TLS v1.2 KDF RFC7627: (A4206, A4207) HMAC-SHA2-256: (A4206, A4207) HMAC-SHA2-384: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-256: (A4206, A4207)
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service	P-256 curve:128 bits of encryption strength P-384 curve:192 bits of encryption strength P-521 curve:256	Counter DRBG: (A4206, A4207) CKG: ()

Name	Type	Description	Properties	Algorithms
			bits of encryption strength	
KAS-FFC (TLSv1.2)	KAS-Full	Full KAS-FFC Key Agreement used for TLSv1.2 service	IG :IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation :IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology providing 128, 192, or 256 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A4206, A4207) TLS v1.2 KDF RFC7627: (A4206, A4207) Safe Primes Key Generation: (A4206, A4207) Safe Primes Key Verification: (A4206, A4207)
KAS-FFC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS FFC keygen used in TLSv1.2 service	2048-bit key:112 bits of encryption strength	Counter DRBG: (A4206, A4207) CKG: ()
KTS (TLSv1.2 with AES and HMAC)	BC-Auth	KTS via TLSv1.2 service by using AES and HMAC	128-bit key:128 bits of encryption strength 256-bit key:256 bits of encryption strength	AES-CBC: (A4206, A4207) HMAC-SHA2-256: (A4206, A4207) HMAC-SHA2-384: (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207)

Name	Type	Description	Properties	Algorithms
KTS (TLSv1.2 with AES-GCM)	BC-Auth	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	AES-GCM: (A4206, A4207) AES-CBC: (A4206, A4207)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A4206, A4207) HMAC-SHA2-384: (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A4206, A4207) AES-GCM: (A4206, A4207)
TLS ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2		ECDSA KeyGen (FIPS186-4): (A4206, A4207) Counter DRBG: (A4206, A4207) CKG: ()
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-4):

Name	Type	Description	Properties	Algorithms
				(A4206, A4207) SHA2-224: (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-512: (A4206, A4207)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-4): (A4206, A4207) SHA-1: (A4206, A4207) SHA2-224: (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-512: (A4206, A4207) ECDSA KeyVer (FIPS186-4): (A4206, A4207)
TLS RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-4): (A4206) Counter DRBG: (A4206,

Name	Type	Description	Properties	Algorithms
				A4207) CKG: ()
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-4): (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-512: (A4206, A4207)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-4): (A4206, A4207) SHA-1: (A4206, A4207) SHA2-224: (A4206, A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-512: (A4206, A4207)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		TLS v1.2 KDF RFC7627: (A4206, A4207) HMAC-SHA2-256: (A4206, A4207) HMAC-SHA2-384: (A4206,

Name	Type	Description	Properties	Algorithms
				A4207) SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207)
Hash	SHA	Hashing for the message digest operation		SHA2-256: (A4206, A4207) SHA2-384: (A4206, A4207) SHA2-512: (A4206, A4207)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

IG C.H Conformance:

GCM is used in the context of TLS:

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with 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, 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.

In all of 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.

IG C.F Conformance:

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.

IG C.K Conformance:

The CAVP testing for Certs. #A4206 and #A4207 was performed prior to the transition date for this IG. Additionally, The FIPS 186-4 CAVP implemented in this module tests are mathematically identical to FIPS 186-5 tests.

IG D.G Conformance:

The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS.

2.8 RBG and Entropy

Cert Number	Vendor Name
E27	Advanced Micro Devices
E128	Palo Alto Networks, Inc.
E130	Palo Alto Networks, Inc.
E162	Palo Alto Networks, Inc.
E64	Palo Alto Networks, Inc.
E65	Palo Alto Networks, Inc.
E66	Palo Alto Networks, Inc.
E68	Palo Alto Networks, Inc.
E69	Palo Alto Networks, Inc.
E70	Palo Alto Networks, Inc.
E71	Palo Alto Networks, Inc.
E72	Palo Alto Networks, Inc.
E73	Palo Alto Networks, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
AMD Random Number Generator	Physical	EPYC 7xx2 Family	128 bits	1.31221 bits	
Octeon III Entropy Source (CN7xxx)	Physical	Cavium OCTEON III CN7130 (cnMIPS64), Cavium OCTEON III CN7350	80 bits	40.535 bits	

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
		(cnMIPS64), Cavium OCTEON III CN7880 (cnMIPS64)			
Palo Alto Networks DRNG Entropy Source - Broadwell 16-Core Die with FCBGA1667 Package	Physical	Intel Corporation Intel(R) Xeon(R) Broadwell-16 FCBGA1667 Intel(R) Xeon(R) D-1557 Processor	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Broadwell 8-Core Die with FCBGA1667 Package	Physical	Intel Corporation Intel(R) Pentium(R), Intel(R) Xeon(R) Broadwell-8 FCBGA1667 Intel(R) Xeon(R) D-1520 Processor	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Broadwell EP 10-Core Die with FCLGA2011 Package	Physical	Intel Corporation Intel(R) Core(R), Intel(R) Xeon(R) Broadwell-EP-10 FCLGA2011 Intel(R) Xeon(R) E5-2620 V4 Processor	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Broadwell EP 15-Core Die with FCLGA2011 Package	Physical	Intel Corporation Intel(R) Xeon(R) Broadwell-EP-15 FCLGA2011 Intel(R) Xeon(R) E5-2690 V4 Processor	128 bits	128 bits	CAVP Cert. #A2165 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Denverton 16 Core Die with FCBGA1310 Package	Physical	Intel Corporation Intel(R) Atom(R) Denverton-16 FCBGA1310 Intel(R) Atom(R) C3958 Processor	128 bits	128 bits	CAVP Cert. #A2153 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Ice Lake 28-Core Die with FCLGA4189 Package	Physical	Intel Corporation Intel(R) Xeon(R) Ice Lake-28 FCLGA4189 Intel(R) Xeon(R) Gold 5315Y Processor	128 bits	128 bits	CAVP Cert. #A2518 (AES-CBC-MAC)

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Palo Alto Networks DRNG Entropy Source - Intel Xeon D-22 Series Processor Core Die with FCBGA2579 Package	Physical	Intel® Xeon® D-2738 Processor	128 bits	128 bits	CAVP Cert. #A2518 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Skylake 28 Core Die with FCLGA3647 Package	Physical	Intel Corporation Intel(R) Xeon(R) Skylake-28 FCLGA3647 Intel(R) Xeon(R) Platinum 8276CL Processor	128 bits	128 bits	CAVP Cert. #A1791 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Skylake-18 Core Die with FCBGA2518 Package	Physical	Intel Corporation Intel(R) Xeon(R) Skylake-18 FCBGA2518 Intel(R) Xeon(R) D-2191 Processor	128 bits	128 bits	CAVP Cert. #2138 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Snow Ridge 24-Core Die with FCBGA2106 Package	Physical	Intel Corporation Intel(R) Atom(R) Snow Ridge-24 FCBGA2106 Intel(R) Atom(R) P5322 Processor	128 bits	128 bits	CAVP Cert. #2541 (AES-CBC-MAC)
Palo Alto Networks RTC Entropy Source	Non-Physical	WildFire 10 on Intel Xeon E5-2620 for WF-500, WildFire 11 on Intel Xeon E5-2620 for WF-500	80 bits	40.5555 bits	

Table 10: Entropy Sources

The AMD RNG is estimated to provide a minimum of 1.31221 bits of entropy per 128-bit output. Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) is directly seeded with 7569408 bits of data from the RDSEED instruction for 77,598 bits of entropy. Therefore, the AES-256 Counter DRBG is fully seeded upon initial instantiation.

The Intel DRNG utilizes a vetted conditioner (AES-CBC-MAC) that outputs full entropy (128-bits per 128-bits of output). Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the Intel DRNG entropy source. Therefore, it is fully seeded with 384 bits of entropy.

The Octeon III Entropy Source is estimated to provide a minimum of 0.50668693116 bits per bit of output. Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the entropy source. Therefore, the DRBG is initially seeded with at least 194 bits of entropy upon initial instantiation of the DRBG. This is greater than the 112-bit minimum, but less than the maximum-security strength of the CTR DRBG. Therefore, the module requires the caveat "The module generates SSPs (e.g., keys) whose strengths are modified by available entropy".

The Palo Alto Networks RTC Entropy Source is estimated to provide a minimum of 0.5069 bits per bit of output. Upon boot, the AES-256 Counter DRBG (security strength of 256-bits) requests 384-bits from the entropy source. Therefore the DRBG is initially seeded with at least 194 bits of entropy upon initial instantiation of the DRBG. This is greater than the 112-bit minimum, but less than the maximum security strength of the CTR DRBG. Therefore, the module requires the caveat "The module generates SSPs (e.g., keys) whose strengths are modified by available entropy".

2.9 Key Generation

The module implements CKG where seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG.

2.10 Key Establishment

2.10.1 Key Agreement

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

- KAS-ECC Shared Secret Computation
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.
- KAS-FFC Shared Secret Computation
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 150 bits of encryption strength.

2.10.2 Key Transport

The module implements the following approved key transport methods as specified in FIPS 140-3 IG D.G, the underlying algorithms of which have been CAVP tested and validated:

-SP 800-38F Key Transport using AES CBC for encryption and HMAC for authentication. (Approved method #2 from IG D.G).

- SP 800-38F Key Transport using AES GCM for encryption and authentication. (Approved method #2 from IG D.G).

2.11 Industry Protocols

The module supports the TLS v1.2 industrial protocol. Please refer to the SSPs table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Status Output	API return values
N/A	Data Input	API input parameters
N/A	Data Output	API output parameters and return values
N/A	Control Input	API input parameters

Table 11: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 12: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Asymmetric Key Generation	Used to generate asymmetric keys	Global indicator ("FIPS-CC"	API for asymmetric key generation	Module generated asymmetric key	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen	Crypto Officer - CA Certificates:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		mode) and System logs			(TLSv1.2) TLS RSA KeyGen TLS ECDSA KeyGen	G,R,W,E - DRBG Key: G,W,E - DRBG Seed: G,E - DRBG V: G,W,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E
Crypto Protocols	Used to support crypto protocols for TLS	Global indicator ("FIPS-CC" mode) and System logs	API for TLS crypto protocol	Module provides crypto protocol processing for calling application	DRBG Function KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen	Crypto Officer - DRBG Key: G,W,E - DRBG Seed: G,E - DRBG V: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (TLSv1.2) Session Encryption/Decryption (TLSv1.2) TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLSv1.2 Keying Materials Development	- ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - RSA Public Keys: G,R,W,E - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryption Keys: G,E,Z - TLS HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z - AES-GCM IV: G,R,W,E,Z
Digital Signature	Used to generate or verify RSA/ECDSA digital signatures	Global indicator ("FIPS-CC" mode) and System logs	API for digital signature	Module performs digital signature functions for calling application	TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA SigGen TLS RSA SigVer	Crypto Officer - DRBG Key: G,W,E - DRBG Seed: G,E - DRBG V: G,W,E - ECDSA Private Keys: G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - RSA Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Keys: G,W,E - RSA Public Keys: G,R,W,E
Initialize	Module performs initialization procedures for Approved mode	Global indicator ("FIPS-CC" mode) and System logs	API to initialize module	Status of initialization of module	None	Crypto Officer
Key Wrapping	Used to encrypt or decrypt a key value on behalf of the calling application	Global indicator ("FIPS-CC" mode) and System logs	API for key wrapping	Module provides key wrapping service for calling application	Session Encryption/Decryption (TLSv1.2) Session Authentication (TLSv1.2)	Crypto Officer - TLS Encryption Keys: G,E,Z - TLS HMAC Keys: G,E,Z
Keyed Hash	Used to generate or verify data integrity with HMAC	Global indicator ("FIPS-CC" mode) and System logs	API for keyed hash	Module provides keyed hash for calling application	Session Authentication (TLSv1.2)	Crypto Officer - TLS HMAC Keys: G,E,Z
Message Digest	Used to generate a SHA message digest	Global indicator ("FIPS-CC" mode) and System logs	API for message digest	Module provides hash for calling application	Hash	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Random Number Generation	Used for random number generation	Global indicator ("FIPS-CC" mode) and System logs	API for random number generator	Random number provided	DRBG Function	Crypto Officer - DRBG Key: G,W,E - DRBG Seed: G,E - DRBG V: G,W,E - Entropy Input String: G,E
Self-Test	Performs self-tests including software integrity verification	Global indicator ("FIPS-CC" mode) and System logs	API for running self-test	Status of the self-test results	None	Crypto Officer - Software integrity verification key: W,E
Show Module Version	Function that provides the module's name and version	Global indicator ("FIPS-CC" mode) and System logs	API for module version	Module's name and version	None	Crypto Officer
Show Status	Function that provides module status information	Global indicator ("FIPS-CC" mode) and System logs	API for show status	Module's status information	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Symmetric Encrypt/Decrypt	Used to encrypt/decrypt data	Global indicator ("FIPS-CC" mode) and System logs	API for encrypting/decrypting	Module performs encrypt/decrypting with a symmetric key	Session Encryption/Decryption (TLSv1.2)	Crypto Officer - TLS Encryption Keys: G,E,Z
Zeroize	Function that zeroizes all SSPs	Zeroization indicator	API for zeroization	Status of zeroization	None	Crypto Officer - CA Certificates: Z - DRBG Key: Z - DRBG Seed: Z - DRBG V: Z - ECDSA Private Keys: Z - ECDSA Public Keys: Z - Entropy Input String: Z - RSA Private Keys: Z - RSA Public Keys: Z - Software integrity verification key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS DHE/ECDHE Private Components: Z - TLS DHE/ECDHE Public Components: Z - TLS Encryption Keys: Z - TLS HMAC Keys: Z - TLS Master Secret: Z - TLS Pre-Master Secret: Z

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

Not applicable, the module does not provide capability to load external software.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Software Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A4206) during the Pre-Operational Self-Test. The module's executable code is in the form of the compiled software image loaded.

5.2 Initiate on Demand

The cryptographic module automatically performs the software integrity and conditional cryptographic algorithm self-tests 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.

6 Operational Environment

6.1 Operational Environment Type and Requirements

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 processes spawned by the cryptographic module are owned by the cryptographic module. An operator may only use the calling application for API calls to the module, but has no control over processes spawned by the module.

Type of Operational Environment: Modifiable

7 Physical Security

N/A

8 Non-Invasive Security9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
HDD	Non-Volatile Memory	Static
RAM	Volatile Memory	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key Input	External (outside of module's boundary)	HDD	Plaintext	Manual	Electronic	
Key Output	HDD	External (outside of	Plaintext	Manual	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		module's boundary)				

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle / Session Termination	Operator powers the module off or session terminates	Powering off the module or terminating the session will erase all SSPs stored in the RAM of the module.	Command via module's CLI or unplugging power of hardware device
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the RAM or in the Flash of the module.	Entering into maintenance mode and selecting Factory Reset

Table 16: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CA Certificates	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)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Public Key - PSP	TLS RSA KeyGen TLS ECDSA KeyGen		TLS RSA SigGen TLS RSA SigVer
DRBG Key	AES 256 CTR DRBG state	256 bits - 256 bits	DRBG Key - CSP	Counter DRBG (A4206)		Counter DRBG (A4206)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Key used in the generation of a random values			Counter DRBG (A4207)		Counter DRBG (A4207)
DRBG Seed	DRBG seed coming from the entropy source Seed length = 384 bits	384 bits - 256 bits	DRBG Seed - CSP	Entropy Source		Counter DRBG (A4206) Counter DRBG (A4207)
DRBG V	AES 256 CTR DRBG state V used in the generation of a random values	128 bits - 128 bits	DRBG Internal State V value - CSP	Counter DRBG (A4206) Counter DRBG (A4207)		Counter DRBG (A4206) Counter DRBG (A4207)
ECDSA Private Keys	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)	256 bits, 384 bits, 521 bits - 128 bits, 192 bits, 256 bits	Private Key - CSP	TLS ECDSA KeyGen		TLS ECDSA SigGen
ECDSA Public Keys	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer	256 bits, 284 bits, 521 bits - 256 bits, 284 bits, 521 bits	Public Key - PSP	TLS ECDSA KeyGen		TLS ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication. (ECDSA P-256, P-384, or P-521)					
Entropy Input String	Entropy input string coming from the entropy source Input length	384 bits (Palo Alto Networks DRNG Entropy Source), 77,598 bits (AMD Random Number Generator), 194 bits (Octeon III Entropy Source/Palo Alto Networks RTC Entropy Source) - 256 bits (Palo Alto Networks DRNG Entropy Source/AMD Random Number Generator), 194 bits (Octeon III Entropy Source/Palo Alto Networks RTC Entropy Source)	DRBG CSP - CSP	Entropy Source		Counter DRBG (A4206) Counter DRBG (A4207)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA Private Keys	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)	2048 bits, 3072 bits, 4096 bits - 112 bits,128 bits, 150 bits	Private Key - CSP	TLS RSA KeyGen		TLS RSA SigGen
RSA Public Keys	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)	2048 bits, 3072 bits, 4096 bits - 112 bits,128 bits, 150 bits	Public Key - PSP	TLS RSA KeyGen		TLS RSA SigVer
Software integrity verification key	key Used to check the integrity of all software code (HMAC-SHA-256 and ECDSA P-256)	128 bits - 128 bits	Integrity verification key - Neither	Pre-Loaded		
TLS DHE/ECDHE Private Components	Ephemeral Diffie-Hellman private FFC or EC	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits,	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2)		TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	component used in TLS (DHE 2048, 3072, 4096, ECDHE P-256, P-384, P-521)	521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits		KAS-FFC-KeyGen (TLSv1.2)		
TLS DHE/ECDHE Public Components	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, 3072, 4096, ECDHE P-256, P-384, P-521)	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits; 128 bits,192 bits, 256 bits	Public Key - PSP	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS Encryption Keys	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)	128 bits, 256 bits - 128 bits, 256 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	Session Encryption/Decryption (TLSv1.2)
TLS HMAC Keys	HMAC keys used in TLS connections (HMAC-SHA2-256/384) (256, 384 bits)	256 bits, 384 bits - 256 bits, 384 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	Session Authentication (TLSv1.2)
TLS Master Secret	Secret value used to derive the TLS session keys	384 bits - 384 bits	Master Secret - CSP		KAS-ECC (TLSv1.2) KAS-FFC	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					(TLSv1.2)	
TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces	2048 bits; 256 bits, 384 bits, 521 bits - 112 bits; 256 bits, 384 bits, 521 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
AES-GCM IV	Initialization vector used with SP 800-38D AES-GCM	96 bits - 96 bits	Initialization Vector - PSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	KTS (TLSv1.2 with AES-GCM)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CA Certificates	Key Input Key Output	HDD:Plaintext RAM:Plaintext	Duration of use	Zeroization Command Power Cycle / Session Termination	
DRBG Key		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
DRBG Seed		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
DRBG V		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
ECDSA Private Keys		HDD:Plaintext		Zeroization Command	
ECDSA Public Keys	Key Input Key Output	HDD:Plaintext		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Entropy Input String		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
RSA Private Keys		HDD:Plaintext		Zeroization Command	
RSA Public Keys	Key Input Key Output	HDD:Plaintext RAM:Plaintext	Duration of use	Zeroization Command	
Software integrity verification key		HDD:Plaintext		N/A	
TLS DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
TLS DHE/ECDHE Public Components	Key Input Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
TLS Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
TLS HMAC Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
TLS Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
TLS Pre-Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	
AES-GCM IV	Key Input Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session Termination	

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A2406)	P-256	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
ECDSA SigVer (FIPS186-4) (A2407)	P-256	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
HMAC-SHA2-256 (A2406)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum
HMAC-SHA2-256 (A2407)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES GCM (A4206) Decrypt	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
KAS-ECC-SSC Sp800-56Ar3 (A4206)	256 bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
AES ECB (A4206)	128 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES ECB (A4207)	128 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES GCM (A4206)	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						self-test command
AES GCM (A4206) Decrypt	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES GCM (A4207)	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command
AES GCM (A4207) Decrypt	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
Counter DRBG (A4206)	N/A	KAT	CAST	Self-test output message	SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests	After each power-on or via self-test command
Counter DRBG (A4207)	N/A	KAT	CAST	Self-test output message	SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests	After each power-on or via self-test command
ECDSA / KAS-ECC (A4206)	256 Bit Minimum	PCT	PCT	System log messages	ECDSA / KAS-ECC pairwise consistency test	On session
ECDSA / KAS-ECC (A4207)	256 Bit Minimum	PCT	PCT	System log messages	ECDSA / KAS-ECC pairwise consistency test	On session
ECDSA Sign (A4206)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
ECDSA Sign (A4207)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						self-test command
ECDSA Verify (A4206)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
ECDSA Verify (A4207)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-256 (A4206)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-256 (A4207)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-384 (A4206)	384 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-384 (A4207)	384 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-512 (A4206)	512 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
HMAC-SHA2-512 (A4207)	512 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-ECC-SSC Sp800-56Ar3 (A4207)	256 bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KAS-FFC-SSC Sp800-56Ar3 (A4206)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KAS-FFC-SSC Sp800-56Ar3 (A4207)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KDF TLS (A4206)	N/A	KAT	CAST	Self-test output message	TLSv1.2 with SHA-256	After each power-on or via self-test command
KDF TLS (A4207)	N/A	KAT	CAST	Self-test output message	TLSv1.2 with SHA-256	After each power-on or via self-test command
RSA KeyGen (FIPS186-4) (A4206)	2048 Bit Minimum	PCT	PCT	System log messages	RSA pairwise consistency test	On session
RSA Sign (A4206)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
RSA Sign (A4207)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA Verify (A4206)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
RSA Verify (A4207)	2048 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
Safe Primes Key Generation (A4206)	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
Safe Primes Key Generation (A4207)	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
SHA-1 (A4206)	160 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA-1 (A4207)	160 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-256 (A4206)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-256 (A4207)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A4206)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-384 (A4207)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-512 (A4206)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-512 (A4207)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SP 800-90B RCT/APT Health Tests on Entropy Source	SP 800-90B, section 4 health tests	Fault-Detection	CAST	Self-test output message	Health tests done on entropy source	After each power-on or via self-test command
SP 800-56A Rev 3 Assurance Tests	N/A	Critical Functions	Critical Function	System log messages	Assurance tests for SP 800-56A Rev3	On session

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A2406)	KAT	SW/FW Integrity	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A2407)	KAT	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A2406)	KAT	SW/FW Integrity	On Demand	Manually
HMAC-SHA2-256 (A2407)	KAT	SW/FW Integrity	On Demand	Manually

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES GCM (A4206) Decrypt	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
AES ECB (A4206)	KAT	CAST	On Demand	Manually or Scheduled
AES ECB (A4207)	KAT	CAST	On Demand	Manually or Scheduled
AES GCM (A4206)	KAT	CAST	On Demand	Manually or Scheduled
AES GCM (A4206) Decrypt	KAT	CAST	On Demand	Manually or Scheduled
AES GCM (A4207)	KAT	CAST	On Demand	Manually or Scheduled
AES GCM (A4207) Decrypt	KAT	CAST	On Demand	Manually or Scheduled
Counter DRBG (A4206)	KAT	CAST	On Demand	Manually or Scheduled
Counter DRBG (A4207)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA / KAS-ECC (A4206)	PCT	PCT	On session	On session
ECDSA / KAS-ECC (A4207)	PCT	PCT	On session	On session
ECDSA Sign (A4206)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA Sign (A4207)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA Verify (A4206)	KAT	CAST	On Demand	Manually or Scheduled

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA Verify (A4207)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
KAS-FFC-SSC Sp800-56Ar3 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
KAS-FFC-SSC Sp800-56Ar3 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
KDF TLS (A4206)	KAT	CAST	On Demand	Manually or Scheduled
KDF TLS (A4207)	KAT	CAST	On Demand	Manually or Scheduled
RSA KeyGen (FIPS186-4) (A4206)	PCT	PCT	On session	On session
RSA Sign (A4206)	KAT	CAST	On Demand	Manually or Scheduled
RSA Sign (A4207)	KAT	CAST	On Demand	Manually or Scheduled
RSA Verify (A4206)	KAT	CAST	On Demand	Manually or Scheduled
RSA Verify (A4207)	KAT	CAST	On Demand	Manually or Scheduled
Safe Primes Key Generation (A4206)	PCT	PCT	On session	On session
Safe Primes Key Generation (A4207)	PCT	PCT	On session	On session

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA-1 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
SHA-1 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A4206)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A4207)	KAT	CAST	On Demand	Manually or Scheduled
SP 800-90B RCT/APT Health Tests on Entropy Source	Fault-Detection	CAST	On Demand	Manually
SP 800-56A Rev 3 Assurance Tests	Critical Functions	Critical Function	On session	On session

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Conditional Pairwise Consistency or Critical Functions Test Failure	Module fails a PCT or critical functions test	PCT / Critical functions test	Reset session	System log prints an error message.
Self-Test / Integrity Test Failure	Module fails a self-test or integrity test	Self-test or Integrity Test failure	Reboot Module or Factory Reset	FIPS-CC mode failure. <Algorithm test> failed.

Table 23: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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
    1. Note: PAN-OS / Panorama / WildFire version 10.2, 11.0, 11.1 or 11.2 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
    1. 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:
    1. “FIPS-CC Failure”: In event of an initialization failure, the module will provide this output
    2. “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 (example):
        - Palo Alto Networks Core Crypto Module
        - Version 1.0

Failure to follow the directions above will result in the module operating in a non-compliant state.

11.2 Administrator Guidance

N/A

11.3 Non-Administrator Guidance

N/A

11.6 End of Life

Cryptographic Officers should follow the procedure below for secure destruction of the module. Note: PAN-OS/Panorama/WildFire 10.2, 11.0, 11.1 or 11.2 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:
    1. “Factory Reset Status: Success”

Note: Following the completion of this procedure, the module will be placed back into an uninitialized state.

12 Mitigation of Other Attacks

N/A.