Palo Alto Networks, Inc.

Panorama Virtual Appliance 11.1 and 11.2

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 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 11
2.7 Algorithm Specific Information 17
IG C.H Conformance: 17
IG C.F Conformance: 18
IG C.K Conformance: 18
2.8 RBG and Entropy 18
2.9 Key Generation 18
2.10 Key Establishment 19
2.11 Industry Protocols 19
3 Cryptographic Module Interfaces 19
3.1 Ports and Interfaces 19
4 Roles, Services, and Authentication 20
4.1 Authentication Methods 20
4.2 Roles 21
4.3 Approved Services 21
4.4 Non-Approved Services 35
4.5 External Software/Firmware Loaded 35
5 Software/Firmware Security 35
5.1 Integrity Techniques 35
5.2 Initiate on Demand 35
6 Operational Environment 36
6.1 Operational Environment Type and Requirements 36
7 Physical Security 36
8 Non-Invasive Security 36

9 Sensitive Security Parameters Management 36
9.1 Storage Areas 36
9.2 SSP Input-Output Methods 36
9.3 SSP Zeroization Methods 37
9.4 SSPs 38
9.5 Transitions 54
10 Self-Tests 54
10.1 Pre-Operational Self-Tests 54
10.2 Conditional Self-Tests 55
10.3 Periodic Self-Test Information 58
10.4 Error States 60
10.5 Operator Initiation of Self-Tests 60
11 Life-Cycle Assurance 60
11.1 Installation, Initialization, and Startup Procedures 60
11.2 Administrator Guidance 62
11.3 Non-Administrator Guidance 62
11.4 Design and Rules 62
11.5 End of Life 62
12 Mitigation of Other Attacks 63

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 7
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 7
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 8
Table 5: Modes List and Description 8
Table 6: Approved Algorithms 10
Table 7: Vendor-Affirmed Algorithms 10
Table 8: Security Function Implementations 17
Table 9: Entropy Certificates 18
Table 10: Entropy Sources 18
Table 11: Ports and Interfaces 19
Table 12: Authentication Methods 21
Table 13: Roles 21
Table 14: Approved Services 35
Table 15: Storage Areas 36
Table 16: SSP Input-Output Methods 37
Table 17: SSP Zeroization Methods 37
Table 18: SSP Table 1 46
Table 19: SSP Table 2 54
Table 20: Pre-Operational Self-Tests 54
Table 21: Conditional Self-Tests 58
Table 22: Pre-Operational Periodic Information 58
Table 23: Conditional Periodic Information 60
Table 24: Error States 60

List of Figures

Figure 1 - Block Diagram 6

1 General

1.1 Overview

The Panorama Virtual Appliance 11.1 and 11.2 from Palo Alto Networks Inc., hereafter referred to as “Panorama VM” or the “cryptographic module” are multi-chip standalone cryptographic modules designed to fulfill FIPS 140-3 level 1 requirements. The Panorama VM provides centralized monitoring and management of multiple Palo Alto Networks next-generation (NG) firewalls and Wildfire appliances.

For purposes of this validation, the exact software versions of the module tested were 11.1.3 and 11.2.5. The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-3. This document may freely be reproduced and distributed in its entirety.

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	3
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	3
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Panorama Virtual Appliances provide centralized management and visibility of Palo Alto Networks next generation firewalls. From a central location, you can gain insight into applications, users, and content traversing the firewalls. The knowledge of what is on the network, in conjunction with safe application enablement policies, maximizes protection and control while minimizing administrative effort. Your security team can centrally perform analysis, reporting, and forensics with the aggregated data over time, or on data stored on the local firewall.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The Panorama Virtual Appliance is a software cryptographic module and requires an underlying general-purpose computer (GPC) environment. The module consists of a GPC (multi-chip standalone embodiment) with the cryptographic boundary defined below. The cryptographic boundary (CB) includes all of the software components of the module, which are included in the file name in Section 11 (Panorama_pc-11.1.3 and Panorama_pc-11.2.5, respectively) and also the configuration file that resides on the virtual machine's virtual disk. The physical perimeter (PP) is defined by the enclosure around the host GPC on which it runs. Figure 1 depicts the boundary and illustrates the hardware components of a GPC.

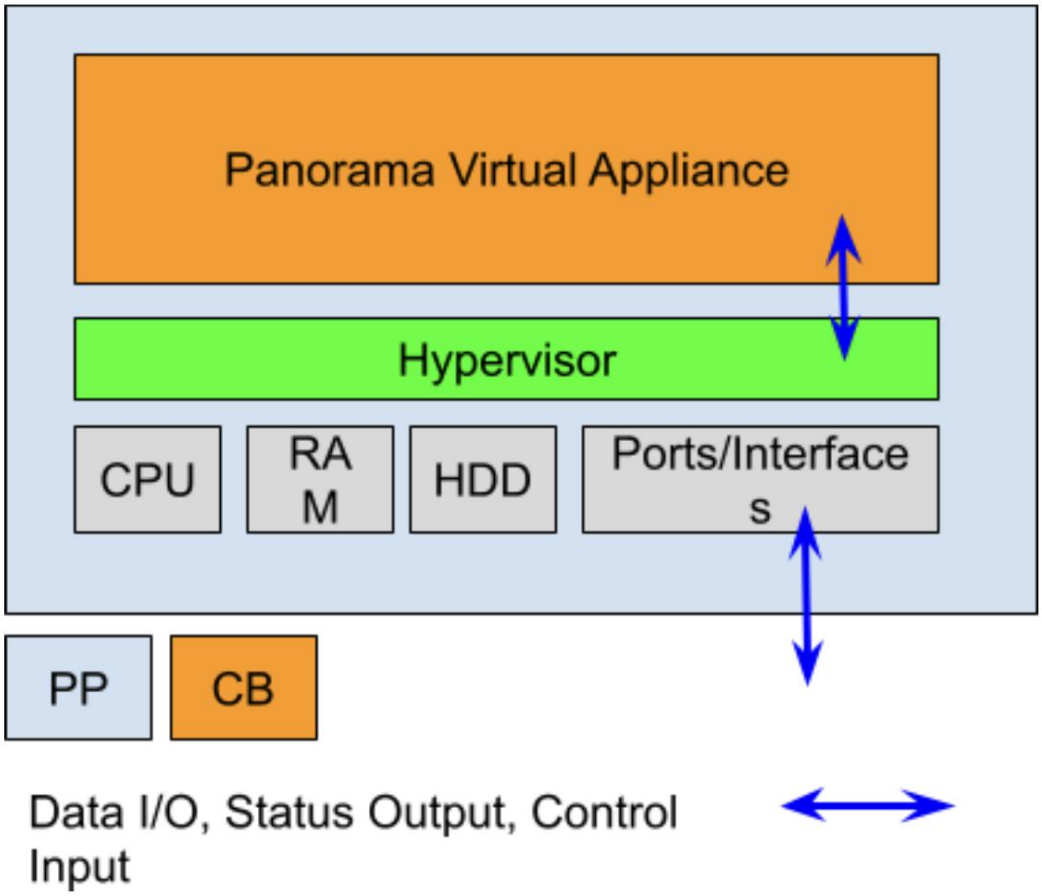

Figure 1 - Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

See above.

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
Panorama_pc-11.1.3	11.1.3	N/A	Yes
Panorama_pc-11.2.5	11.2.5	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:

The module is a modifiable operational environment as per FIPS 140-3 Level 1 specifications. The hypervisor environment provides an isolated operating environment and is the single operator of the virtual machine.

The tested operating environments isolate virtual systems into separate isolated process spaces. Each process space is logically separated from all other processes by the operating environments software and hardware. The module functions entirely within the process space of the isolated system as managed by the single operational environment. This implicitly meets the FIPS 140-3 requirement that only one (1) entity at a time can use the cryptographic module.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
N/A	Dell PowerEdge R740	Intel Gold 6248	No	Hyper-V 2019 on Microsoft Hyper-V Server 2019	11.1.3 11.2.5
N/A	Dell PowerEdge R740	Intel Gold 6248	No	KVM 4 on Ubuntu 20.04	11.1.3 11.2.5
N/A	Dell PowerEdge R740	Intel Gold 6248	No	VMware ESXi v7.0	11.1.3 11.2.5

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

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

Operating System	Hardware Platform
Amazon Web Services (AWS)	x86 Architecture (Note: Specific processor/hardware is dependent on Instance/Machine Type selected for operation system)
Google Cloud Platform (GCP)	x86 Architecture (Note: Specific processor/hardware is dependent on Instance/Machine Type selected for operation system)
Microsoft Azure	x86 Architecture (Note: Specific processor/hardware is dependent on Instance/Machine Type selected for operation system)

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

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

N/A

2.4 Modes of Operation

Modes List and Description:

The module only operates in an approved mode of operation and is in the approved mode when installed, initialized and configured per section 11.1 of the Security Policy.

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

Mode Change Instructions and Status:

See Life-Cycle Assurance section.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3454	Direction - Decrypt, Encrypt	SP 800-38A
AES-CFB1	A3454	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3454	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB8	A3454	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A3454	Direction - Decrypt, Encrypt	SP 800-38A
AES-GCM	A3454	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
Counter DRBG	A3454	Prediction Resistance - No, Yes Mode - AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3454	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3454	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3454	Curve - P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A3454	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A3454	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3454	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3454	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3454	Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3454	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	A3454	Domain Parameter Generation Methods - MODP-2048, MODP-3072, MODP-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
KDF SNMP (CVL)	A3454	Password Length - Password Length: 64, 2048	SP 800-135 Rev. 1
KDF SSH (CVL)	A3454	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A3454	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3454	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A3454	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A3454	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A3454	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA-1	A3454	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-224	A3454	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3454	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3454	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3454	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3454	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Note: 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 (SP 800-133rev2)	Key Type: Symmetric and Asymmetric	N/A	Cryptographic Key Generation; SP 800-133rev2 and IG D.H (symmetric keys and asymmetric seeds) from 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
CKG	CKG	Symmetric key generation for AES		Counter DRBG: (A3454) CKG (SP 800-133rev2): ()
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A3454)
KAS-ECC (SSH)	KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 service	IG:D.F, 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 between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3454) KDF SSH: (A3454)

Name	Type	Description	Properties	Algorithms
KAS-ECC (TLSv1.2)	KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	P-256 curve: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 between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3454) TLS v1.2 KDF RFC7627: (A3454)
KAS-ECC-KeyGen (SSH)	KAS-KeyGen	KAS ECC keygen used in SSHv2 service		Counter DRBG: (A3454)
KAS-ECC-KeyGen (TLSv1.2)	KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service		Counter DRBG: (A3454)
KAS-FFC (SSH)	KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 service	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 between 128 and 256 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A3454) KDF SSH: (A3454)
KAS-FFC (TLSv1.2)	KAS-Full	Full KAS-FFC Key Agreement used for TLSv1.2 service	IG:D.F Scenario 2 path 2, split Key Confirmation:No Key Derivation:2.4.B SP 800-135rev1	KAS-FFC-SSC Sp800-56Ar3: (A3454) TLS v1.2 KDF RFC7627: (A3454)

Name	Type	Description	Properties	Algorithms
			CVL Caveat:Key establishment methodology providing between 128 and 256 bits of security strength	Safe Primes Key Generation: (A3454) Safe Primes Key Verification: (A3454)
KAS-FFC-KeyGen (SSH)	KAS-KeyGen	KAS FFC keygen used in SSHv2 service		Counter DRBG: (A3454)
KAS-FFC-KeyGen (TLSv1.2)	KAS-KeyGen	KAS FFC keygen used in TLSv1.2 service		Counter DRBG: (A3454)
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-CBC: (A3454) HMAC-SHA2-256: (A3454) HMAC-SHA2-384: (A3454) SHA2-256: (A3454) SHA2-384: (A3454)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A3454)
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key	AES-CBC: (A3454) HMAC-SHA2-256: (A3454) HMAC-

Name	Type	Description	Properties	Algorithms
			establishment methodology provides between 128 and 256 bits of security strength	SHA2-384: (A3454) SHA2-256: (A3454) SHA2-384: (A3454)
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:Approved Key Wrapping Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A3454)
Session Authentication (SMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A3454) HMAC-SHA2-224: (A3454) SHA-1: (A3454) SHA2-224: (A3454)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A3454) HMAC-SHA2-256: (A3454) HMAC-SHA2-512: (A3454) SHA-1: (A3454) SHA2-256: (A3454) SHA2-512: (A3454)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A3454) HMAC-

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A3454) SHA2-256: (A3454) SHA2-384: (A3454)
Session Encryption/Decryption (SNMPv3)	BC-Auth BC-UnAuth	SNMPv3 session protection		AES-CFB1: (A3454) AES-CFB8: (A3454) AES-CFB128: (A3454)
Session Encryption/Decryption (SSH)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CBC: (A3454) AES-CTR: (A3454) AES-GCM: (A3454)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A3454) AES-GCM: (A3454)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A3454)
Software Load Test	DigSig-SigVer	Signature verification for software load test		RSA SigVer (FIPS186-4): (A3454) Modulus: RSA 2048 with SHA2-256 SHA2-256: (A3454)
SSH ECDSA KeyGen	AsymKeyPair-KeyGen	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-4): (A3454) Counter DRBG: (A3454)

Name	Type	Description	Properties	Algorithms
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-4): (A3454)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-4): (A3454)
SSH RSA KeyGen	AsymKeyPair-KeyGen	RSA KeyGen for SSHv2		RSA KeyGen (FIPS186-4): (A3454) Counter DRBG: (A3454)
SSH RSA SigGen	DigSig-SigGen	RSA SigGen for SSHv2		RSA SigGen (FIPS186-4): (A3454)
SSH RSA SigVer	DigSig-SigVer	RSA SigVer for SSHv2		RSA SigVer (FIPS186-4): (A3454)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys		KDF SSH: (A3454)
TLS ECDSA KeyGen	AsymKeyPair-KeyGen	ECDSA KeyGen for TLSv1.2		ECDSA KeyGen (FIPS186-4): (A3454) Counter DRBG: (A3454)
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-4): (A3454)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-4): (A3454)
TLS RSA KeyGen	AsymKeyPair-KeyGen	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-4): (A3454) Counter

Name	Type	Description	Properties	Algorithms
				DRBG: (A3454)
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-4): (A3454)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		TLS v1.2 KDF RFC7627: (A3454)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

IG C.H Conformance:
GCM is used in the context of TLS, SSH:

- 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.
- For SSH, the module meets Scenario 1 of IG C.H. The module conforms to RFCs 4252, 4253, and 5647. The fixed field is 32 bits in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 64 bits in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 264 is exhausted. (It would take hundreds of years for this to occur.)

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 or SSH 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 Cert. #A3454 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.

2.8 RBG and Entropy

Cert Number	Vendor Name
E69	Palo Alto Networks

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
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	128	A1791 (AES-CBC-MAC)

Table 10: Entropy Sources

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.

2.9 Key Generation

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

2.10 Key Establishment

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.

2.11 Industry Protocols

- TLS 1.2
- SSHv2
- SNMPv3

No parts of the SSH, TLS and SNMP protocols, other than the KDFs, have been tested by the CAVP/CMVP.

3 Cryptographic Module Interfaces

The modules are multi-chip standalone modules with ports and interfaces as shown below. The modules do not implement a control output interface.

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Status Output	Self-test status output
N/A	Data Input Data Output Control Input Control Output Status Output	HTTPS, TLS, SNMP and SSH traffic data.

Table 11: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits	RSA SigVer (FIPS186-4) (A3454)	With a minimum modulus size of 2048, the probability that a random attempt will succeed is 1/(2^112).	The probability of successfully authenticating to the module within a one-minute period is 288,000,000/(2^112). The module supports at most 4,800,000 new sessions per second.
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a minimum ECDSA curve of P-256	ECDSA SigVer (FIPS186-4) (A3454)	With a minimum curve of P-256, the probability that a random attempt will succeed is 1/(2^128).	The probability of successfully authenticating to the module within a one-minute period is 288,000,000/(2^112). The module supports at most 4,800,000 new sessions per second.
Password	Password based authentication	Password Based	The minimum length is eight (8) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(95^8).	The probability of successfully authenticating to the module within one minute is 10/(95^8). The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period.
Pre-Shared Secret	PSK authentication	Password Based	The pre-shared key authentication method has a minimum security strength of 95^6. The probability of successfully authenticating to the module is 1/(95^6). The number of	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(95^6).

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			authentication attempts is limited by the number of new connections per second supported (4,800,000) on the fastest platform of the Palo Alto Networks firewalls.	

Table 12: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret
User	Role	User	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret

Table 13: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration	Configuration/ System Logs	Input configurations for other setup functions	Module uses configuration	KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC	Crypto Officer - CO, User Password: G,W,E - DRBG Key: G,E - DRBG Seed: G,E - DRBG V: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(SSH) KAS-ECC (TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer Session Encryption/Decryption (SSH)	- ECDSA Private Keys: G,W,E - Entropy Input String: G,E - RSA Private Keys: G,W,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Ke: G,R,W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Session Encryption/Decryption (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Authentication (SMPv3) SSHv2 Keying Materials Development TLSv1.2 Keying Materials Development SNMPv3 Keying Materials Development DRBG Function CKG	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 Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating	Configuration/ System Logs	Input configuration for various cryptographic functions	Module uses the configuration for cryptographic purposes	KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (SSH) KAS-ECC	Crypto Officer - Authentication Key: G,E,Z - CA Certificates: G,R,W,E - CO, User Password: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	User accounts and additional CO accounts				(TLSv1.2) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer Session Encryption/Decryption (SSH) Session Encryption/Decryption (TLSv1.2) Session	- DRBG Key: G,E - DRBG Seed: G,R,W,E - DRBG V: G,E - ECDSA Private Keys: G,W,E - ECDSA Public Key: G,E - Entropy Input String: G,E - Protocol Secrets: W,E - Public key for software load test: W,E - RSA Private Keys: G,W,E - Session Key: G,E,Z - SNMPv3 Authentication Secret: W,E - SNMPv3 Privacy Secret: W,E - SSH Client

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Encryption/Decryption (SNMPv3) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Authentication (SMPv3) SSHv2 Keying Materials Development TLSv1.2 Keying Materials Development SNMPv3 Keying Materials Development DRBG Function CKG	Public Key: W,E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Ke: G,R,W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z - TLS DHE/ECDHE Public Components: G,R,W,E,Z - TLS Encryptio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Keys: G,E,Z - TLS HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
Self-Tests	Initiates self-tests and integrity test	System Logs	Self-test command or rebooting the module	Status of the self-tests	None	Crypto Officer - Software integrity verification key : E
Show Status	Provides status information of the module	Configuration/ System Logs	Initiate show status command	Module provides status output of module	None	Crypto Officer - CO, User Password: G,W,E - DRBG Key: G,E - DRBG Seed: E - DRBG V: G,E - ECDSA Private Keys: G,E - Entropy Input String: G,E - RSA Private Keys: E - SSH DHE/ECDHE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - 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 Keys: G,E,Z - TLS Master Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - TLS Pre-Master Secret: G,E,Z Unauthenticated - CO, User Password: G,E,Z - DRBG Key: G,E - DRBG Seed: E - DRBG V: G,E - ECDSA Private Keys: G,E - Entropy Input String: G,E - RSA Private Keys: E - SSH DHE/ECDHE Private Components: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Session Authentication Keys: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Session Encryption Keys: G,E,Z - 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 Keys: G,E,Z - TLS Master Secret: G,Z - TLS Pre-Master Secret: G,E,Z
Show Status (LEDs)	Provides status of the module	LEDs	N/A	Status of the module via LEDs	None	Unauthenticated
Show Version	Shows the version of the module	Version displayed via System Logs / CLI / UI	Input command for version	Module displays version information	None	Crypto Officer Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Software Update	Provides a method to update the software of the module	Configuration/ System Logs	Uploading new software	Status of the updated software installation	Software Load Test	Crypto Officer - Public key for software load test: E
View Other Configuration	Read-only of non-security relevant configuration	Configuration/ System Logs	Initiate command to read configuration	Module provides configuration details	None	Crypto Officer - CO, User Password: W,E User - CO, User Password: W,E
Zeroize	Destroys all keys in the module	Zeroization indicator	Initiating zeroization command	Status of the zeroization process	None	Crypto Officer - Authentication Key: Z - CA Certificates: Z - CO, User Password: E,Z - DRBG Key: Z - DRBG Seed: Z - DRBG V: Z - ECDSA Private Keys: Z - ECDSA Public Key: Z - Entropy Input String: Z - Protocol

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secrets: Z - Public key for software load test: Z - RSA Private Keys: Z - RSA Public Keys: Z - Session Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Privacy Secret: Z - Software integrity verification key : Z - SSH Client Public Key: Z - SSH DHE/ECDHE Private Components: Z - SSH DHE/ECDHE Public Components: Z - SSH Host Public Ke: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Session Authentication Keys: Z - SSH Session Encryption Keys: Z - 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 Unauthenticated - Authentication Key: Z - CA Certificates: Z - CO, User Password: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key: Z - DRBG Seed: Z - DRBG V: Z - ECDSA Private Keys: Z - ECDSA Public Key: Z - Entropy Input String: Z - Protocol Secrets: Z - Public key for software load test: Z - RSA Private Keys: Z - RSA Public Keys: Z - Session Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Privacy Secret: Z - Software integrity verification key : Z - SSH Client Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - SSH DHE/ECDHE Private Components: Z - SSH DHE/ECDHE Public Components: Z - SSH Host Public Ke: Z - SSH Session Authentication Keys: Z - SSH Session Encryption Keys: Z - TLS DHE/ECDHE Private Components: Z - TLS DHE/ECDHE Public Components: Z - TLS Encryption Keys: Z - TLS HMAC Keys: Z - TLS Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: Z - TLS Pre-Master Secret: Z

Table 14: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using RSA 2048 bits with SHA2-256 (RSA Cert. #A3454) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate into the module before loading any firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails.

5 Software/Firmware Security

5.1 Integrity Techniques

The module's executable code is in the form of the compiled firmware image loaded onto the module.

The module performs the Software Integrity test by using HMAC-SHA-256 (HMAC Cert..#A3454) during the Pre-Operational Self-Test. In addition, the module also conducts a software load test by using RSA 2048 with SHA-256 (Cert. #A3454) for the new validated software to be uploaded into the module.

Any software loaded into this module that is not shown on the module certificate is out of scope of this validation and requires a separate FIPS 140-3 validation.

5.2 Initiate on Demand

The pre-operational self-tests can be initiated by power cycling the module. When this is performed, the module automatically runs the cryptographic algorithm self-tests in addition to the pre-operational firmware integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

7 Physical Security

The module is a software only module; FIPS 140-3 physical security requirements are not applicable.

8 Non-Invasive Security

Not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Module Public Key Output	HDD	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	

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

Table 16: 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 CLI or WebUI or by unplugging module
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 17: SSP Zeroization Methods

Once the module is rebooted and zeroization is initiated, the module cannot be accessed in any way and the zeroization process cannot be stopped, thus the SSPs would not be compromised during the time of zeroization. The Crypto Officer shall be in control of the module until the zeroization process is complete.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Authentication Key	HMAC-SHA-1/224/256/384/512 Authentication protocol k	160 - 512 bits - 160 - 512 bits	Session Key - CSP - CSP	KDF SNMP (A3454)		Session Authentication (SMPv3)
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 - 4096 bits - 112 bits - 152 bits	Public Key - PSP	DRBG Function		TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA SigGen
CO, User Password	Authentication string with a minimum length of eight (8) characters.	8 characters minimum - N/A	Authentication Data - CSP - CSP			
DRBG Key	AES 256 CTR DRBG state Key used in the generation of a random values	256 bits - 256 bits	DRBG Key - CSP - CSP	Entropy as per SP 800-90B		DRBG Function
DRBG Seed	DRBG seed coming from the entropy	384 bits -	DRBG Seed - CSP - CSP	Entropy as per		DRBG Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	source Seed length = 384 bits	256 bits		SP 800-90B		
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 - CSP	Entropy as per SP 800-90B		DRBG Function
ECDSA Private Keys	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)	128 - 256 bits - 128 - 256 bits	Private Key - CSP	DRBG Function TLS ECDSA KeyGen		TLS ECDSA SigGen
ECDSA Public Key	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)	128 - 256 bits - 128 - 256 bits	Public Key - PSP	DRBG Function TLS ECDSA KeyGen		TLS ECDSA SigVer
Entropy Input String	Entropy input string coming from the entropy source Input length = 384 bits	384 bits - 256 bits	DRBG - CSP - CSP	Entropy as per SP 800-90B		DRBG Function
Protocol Secrets	Secrets used by RADIUS or TACACS+	8 characters	Authentication Data -			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(8 characters minimum)	minimum -	CSP - CSP			
Public key for software load test	Used to authenticate software/firmware and content to be installed on the firewall (RSA 2048 with SHA-256)	2048 bits - 112 bits	Public Key - PSP - PSP	Pre-Loaded		Software Load Test
RSA Private Keys	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)	2048 - 4096 bits - 112 bits - 152 bits	Private Key - CSP	DRBG Function 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 - 4096 bits - 112 bits - 152 bits	Public Key - PSP	DRBG Function		
Session Key	Privacy protocol encryption key (AES 128/192/256 CFB)	128 - 256 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF SNMP (A3454)		Session Encryption/Decryption (SNMPv3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SNMPv3 Authentication Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP - CSP			SNMPv3 Keying Materials Development
SNMPv3 Privacy Secret	Used to support SNMPv3 services (Minimum 8 characters)	8 characters minimum - N/A	Authentication Key - CSP - CSP			SNMPv3 Keying Materials Development
Software integrity verification key	Used to check the integrity of all software code (HMAC-SHA-256 and ECDSA P-256) (Note: This is not considered an SSP)	256 bits - 256 bits	Public Key - PSP - Neither	Pre-loaded		
SSH Client Public Key	Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits)	2048 - 4096 bits - 112 bits - 152 bits	Public Key - PSP - PSP			SSH RSA SigVer
SSH DHE/ECDHE Private Components	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)	2048 bits - 112 bits	Private Key - CSP - CSP	DRBG Function KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				56Ar3 (A3454)		
SSH DHE/ECDHE Public Components	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)	2048 bits - 112 bits	Public Key - PSP - PSP	DRBG Function KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development
SSH Host Public Ke	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)	2048 - 4096 bits - 112 bits - 152 bits	Public Key - PSP - PSP	DRBG Function ECDSA KeyGen (FIPS186-4) (A3454) ECDSA SigGen (FIPS186-4) (A3454) RSA KeyGen (FIPS186-4) (A3454) RSA SigGen (FIPS186-4) (A3454)		SSH ECDSA SigVer SSH RSA SigVer
SSH Session	Authentication keys used in all SSH	160, 256, or 512	Session Key - CSP - CSP	KDF SSH (A3454)	KAS-ECC (SSH)	Session Authentication (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Authentication Keys	connections to the security module's command line interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)	bits - 160, 256, or 512 bits			KAS-FFC (SSH) KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	
SSH Session Encryption Keys	Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: AES CBC or CTR) (128 or 256 bits: AES GCM)	128 - 256 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF SSH (A3454)	KAS-ECC (SSH) KAS-FFC (SSH) KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	Session Encryption/Decryption (SSH)
TLS DHE/ECDHE Private Components	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-	2048 bits - 4096 bits - 112 bits - 152 bits	Private Key - CSP	DRBG Function KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	256, P-384, P-521)			FFC-SSC Sp800-56Ar3 (A3454)		
TLS DHE/ECDHE Public Components	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521	2048 bits - 4096 bits - 112 bits - 152 bits	Public Key - PSP	DRBG Function KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	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 - 256 bits - 128 - 256 bits	Session Key - CSP - CSP	TLS v1.2 KDF RFC7627 (A3454)	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KAS-ECC-SSC Sp800-56Ar3	TLSv1.2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					(A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	
TLS HMAC Keys	HMAC keys used in TLS connections (HMAC-SHA2-256/384) (256, 384 bits)	256 - 384 bits - 256 - 384 bits	Session Key - CSP - CSP	TLS v1.2 KDF RFC7627 (A3454)	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	Session Authentication (TLSv1.2)
TLS Master Secret	Secret value used to derive the TLS session keys	384 bits - N/A	Master Secret - CSP - CSP	TLS v1.2 KDF RFC7627 (A3454)	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	384 bits - N/A	Shared Secret - CSP	KAS-ECC-SSC Sp800-56Ar3 (A3454) KAS-FFC-SSC Sp800-56Ar3 (A3454)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Authentication Key		HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
CA Certificates	Peer Public Key Input Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
CO, User Password	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Encrypted		Zeroization Command	
DRBG Key		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	Entropy Input String:Paired With DRBG Seed:Paired With DRBG V:Paired With
DRBG Seed		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	Entropy Input String:Paired With DRBG Key:Paired With DRBG V:Paired With
DRBG V		RAM:Plaintext	Duration of use	Power Cycle /	Entropy Input String:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	DRBG Seed:Paired With DRBG Key:Paired With
ECDSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command Power Cycle / Session Termination	ECDSA Public Key:Paired With
ECDSA Public Key	Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	ECDSA Private Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
Entropy Input String		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	DRBG Seed:Paired With DRBG Key:Paired With DRBG V:Paired With
Protocol Secrets	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	
Public key for software load test		HDD:Plaintext			
RSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command Power Cycle /	RSA Public Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM			Session Termination	
RSA Public Keys	Module Public Key Output Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	RSA Private Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Session Key		HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SNMPv3 Authentication Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	
SNMPv3 Privacy Secret	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
Software integrity verification key		HDD:Plaintext			
SSH Client Public Key	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secret Input via TLSv1.2 encrypted by AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	
SSH DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Paired With
SSH DHE/ECDHE Public Components	Peer Public Key Input Module Public Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session	SSH DHE/ECDHE Private Components:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Termination	
SSH Host Public Ke		HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	
SSH Session Authentication Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Derived From SSH DHE/ECDHE Private Components:Derived From
SSH Session Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Public Components:Derived From SSH DHE/ECDHE Private Components:Derived From
TLS DHE/ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS DHE/ECDHE Public Components:Paired With
TLS DHE/ECDHE Public Components	Peer Public Key Input Module Public Key Output	RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS DHE/ECDHE Private Components:Paired With
TLS Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Master Secret:Derived From
TLS HMAC Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Master Secret:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	TLS Pre-Master Secret:Derived From
TLS Pre-Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	

Table 19: SSP Table 2

9.5 Transitions

Key Sizes

- Key sizes with a security strength less than 128-bits will be non-Approved for all uses starting January 1, 2031.

SHA-1

- The module implements SHA-1 for use in non-digital signature applications. This implementation will be non-Approved for all uses starting January 1, 2031.

10 Self-Tests

The cryptographic module performs the following tests below. The operator can command the module to perform the pre-operational and cryptographic algorithm self-tests by cycling power of the module. The pre-operational and conditional self-tests are performed automatically and do not require any additional operator action.

10.1 Pre-Operational Self-Tests

Verified with HMAC-SHA-256 and ECDSA P-256.
Note: the ECDSA and HMAC-SHA-256 KATs are performed prior to the Software integrity test.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A3454)	P-256	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
HMAC-SHA2-224 (A3454)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum

Table 20: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3454) (Decrypt)	128 bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES-GCM (A3454) (Decrypt)	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES-GCM (A3454) (Encrypt)	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command
Counter DRBG (A3454)	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	256 Bit Minimum	PCT	PCT	System log messages	ECDSA / KAS-ECC pairwise consistency test	On session
ECDSA SigGen (FIPS186-4) (A3454)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
ECDSA SigVer (FIPS186-4) (A3454)	256 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
HMAC-SHA-1 (A3454)	160 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-224 (A3454)	224 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-256 (A3454)	256 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-384 (A3454)	384 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-512 (A3454)	512 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
KAS-ECC-SSC Sp800-56Ar3 (A3454)	256 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KAS-FFC-SSC Sp800-56Ar3 (A3454)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KDF SSH (A3454)	N/A	KAT	CAST	Self-test output message	SSHv2 with SHA-256	After each power-on or via self-test command
RSA	2048 Bit Minimum	PCT	PCT	System log messages	RSA pairwise consistency test	On session
RSA SigGen (FIPS186	2048 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
-4) (A3454)						self-test command
RSA SigVer (FIPS186-4) (A3454)	2048 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
Safe Primes Key Generation (A3454)	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
SHA-1 (A3454)	160 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-256 (A3454)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-384 (A3454)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-512 (A3454)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
Software Load Test	2048 Bit	FW Load Test	SW/FW Load	System log messages	Software load test on content load	On session
SP 800-90B RCT/APT Health Tests on	N/A	Fault-Detection Test	CAST	Self-test output message	Health tests done on entropy source	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy Source						
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
TLS v1.2 KDF RFC7627 (A3454)	N/A	KAT	CAST	Self-test output message	TLSv1.2 with SHA-256	After each power-on or via self-test command

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A3454)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled
HMAC-SHA2-224 (A3454)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3454) (Decrypt)	KAT	CAST	On Demand	Manually or Scheduled
AES-GCM (A3454) (Decrypt)	KAT	CAST	On Demand	Manually or Scheduled
AES-GCM (A3454) (Encrypt)	KAT	CAST	On Demand	Manually or Scheduled
Counter DRBG (A3454)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA / KAS-ECC	PCT	PCT	On session	On session

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-4) (A3454)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA SigVer (FIPS186-4) (A3454)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA-1 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-224 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
KAS-FFC-SSC Sp800-56Ar3 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
KDF SSH (A3454)	KAT	CAST	On Demand	Manually or Scheduled
RSA	PCT	PCT	On session	On session
RSA SigGen (FIPS186-4) (A3454)	KAT	CAST	On Demand	Manually or Scheduled
RSA SigVer (FIPS186-4) (A3454)	KAT	CAST	On Demand	Manually or Scheduled
Safe Primes Key Generation (A3454)	PCT	PCT	On session	On session
SHA-1 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A3454)	KAT	CAST	On Demand	Manually or Scheduled
Software Load Test	FW Load Test	SW/FW Load	On session	On session

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SP 800-90B RCT/APT Health Tests on Entropy Source	Fault-Detection Test	CAST	On Demand	Manually or Scheduled
SP 800-56A Rev 3 Assurance Tests	Critical Functions	Critical Function	On session	On session
TLS v1.2 KDF RFC7627 (A3454)	KAT	CAST	On Demand	Manually or Scheduled

Table 23: 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.
Conditional Software Load Test Failure	Signature verification fails on software load	Signature verification failure	N/A	System prints Invalid image 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 24: Error States

In the event of a conditional test failure, the module will output a description of the error.

10.5 Operator Initiation of Self-Tests

Perform a power cycle or via the 'Self-Tests' service

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The vendor provided life-cycle assurance documentation describes configuration management, design, finite state model, development, testing, delivery & operation, end of life procedures, and guidance. For details regarding the approved mode of operation, see “Approved Mode of Operation". For details regarding secure installation, initialization, startup, and operation of the module, see below.

Installation Instructions

The module can be retrieved by downloading Panorama _pc-11.1.3 and _pc11.2.5 from the support site: https://support.paloaltonetworks.com/Support/Index, and a checksum (SHA-256) is available to ensure the module is correct:

Alternatively, the module version can be obtained by running the following commands via CLI (as an authorized administrator):

1. request system software check
2. request system software download version 11.x
3. request system software install version 11.x
4. request restart system

Palo Alto Network provides an Administrator Guide for additional information noted in the “References” section of this Security Policy.

The following procedure will initialize the modules into the Approved mode of operation:

- During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select “Continue.”
- Select the “Set FIPS-CC Mode” option to initialize the Approved mode.
- Select “Enable FIPS-CC Mode”.
- When prompted, select “Reboot” and the module will re-initialize and continue into the Approved mode of operation
- (FIPS-CC mode).
- The module will reboot.
- In “FIPS-CC” mode, the console port is available only as a status output port.
    - Once the module has finished booting, the Crypto Officer can authenticate using the default credentials that come with the module
    - Once authenticated, the module will automatically require the operator to change their password; and the default credential is overwritten

The module will automatically indicate the Approved mode of operation in the following manner:

- Status output interface will indicate “**** FIPS-CC MODE ENABLED ****” via the CLI session.
- Status output interface will indicate “FIPS-CC mode enabled successfully” via the console port.
- The module will display “FIPS-CC” at all times in the status bar at the bottom of the web interface.
- The module will display “fips-cc” when “show system info” is entered via the CLI

Note: Disabling FIPS-CC mode causes a complete factory reset, which is described in the Zeroization section below.

Non-Compliant State

Failure to follow the directions in the Approved Mode of Operation above or rules noted in Section 11 will result in the module operating in a non-compliant state, which is considered out of scope of this validation.

11.2 Administrator Guidance

The Administrator Guidance can be obtained from Palo Alto Network's public site:

https://docs.paloaltonetworks.com/panorama/11-1/panorama-admin

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

In FIPS-CC mode, the following rules shall apply:

1. The operator should not enable or use TLSv1.3
    1. Checked via CLI using "show profiles" command
2. If using RADIUS, it must be configured using TLS.
    1. Checked via CLI using "show shared" command
3. If using TACACS+, configure the service route via an IPSec tunnel, and ensure the TACACS+ server is configured for a minimum password length of eight (8) characters or greater.
    1. Checked via CLI using "show deviceconfig" command
4. When FIPS-CC mode is enabled, the operator shall not install plugins.
    1. Checked via CLI using "show plugins installed"

11.5 End of Life

The following procedure will zeroize the module:

- Access the module's CLI via SSH, and command the module to enter maintenance mode; the module will reboot
    - Note: Establish a serial connection to the console port
- After reboot, select "Continue."
- Select "Factory Reset"
- The module will perform a zeroization, and provide the following message once complete:
    - "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

This module is not designed to mitigate other attacks outside the scope of FIPS 140-3.