Palo Alto Networks, Inc.

PAN-OS 10.2 VM-Series

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 6
2.3 Excluded Components 7
2.4 Modes of Operation 7
2.5 Algorithms 8
2.6 Security Function Implementations 11
2.7 Algorithm Specific Information 23
2.7.1 IG C.H Conformance 23
2.7.2 IG C.F Conformance 24
2.7.3 IG C.K Conformance 24
2.8 RBG and Entropy 24
2.9 Key Generation 25
2.10 Key Establishment 25
2.11 Industry Protocols 25
3 Cryptographic Module Interfaces 25
3.1 Ports and Interfaces 25
4 Roles, Services, and Authentication 26
4.1 Authentication Methods 26
4.2 Roles 27
4.3 Approved Services 28
4.4 Non-Approved Services 44
4.5 External Software/Firmware Loaded 44
5 Software/Firmware Security 44
5.1 Integrity Techniques 44
5.2 Initiate on Demand 45
6 Operational Environment 45
6.1 Operational Environment Type and Requirements 45
7 Physical Security 45
7.1 Mechanisms and Actions Required 45

7.5 EFP/EFT Information 45
7.6 Hardness Testing Temperature Ranges 45
8 Non-Invasive Security 46
9 Sensitive Security Parameters Management 46
9.1 Storage Areas 46
9.2 SSP Input-Output Methods 46
9.3 SSP Zeroization Methods 47
9.4 SSPs 48
10 Self-Tests 67
10.1 Pre-Operational Self-Tests 67
10.2 Conditional Self-Tests 67
10.3 Periodic Self-Test Information 71
10.4 Error States 73
10.5 Operator Initiation of Self-Tests 73
11 Life-Cycle Assurance 73
11.1 Installation, Initialization, and Startup Procedures 73
11.2 Administrator Guidance 74
11.3 Non-Administrator Guidance 74
11.4 Design and Rules 75
11.6 End of Life 75
12 Mitigation of Other Attacks 75

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 6
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 7
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 7
Table 5: Modes List and Description 8
Table 6: Approved Algorithms 10
Table 7: Vendor-Affirmed Algorithms 10
Table 8: Security Function Implementations 23
Table 9: Entropy Certificates 24
Table 10: Entropy Sources 24
Table 11: Ports and Interfaces 26
Table 12: Authentication Methods 27
Table 13: Roles 27
Table 14: Approved Services 44
Table 15: EFP/EFT Information 45
Table 16: Hardness Testing Temperatures 45
Table 17: Storage Areas 46
Table 18: SSP Input-Output Methods 47
Table 19: SSP Zeroization Methods 47
Table 20: SSP Table 1 56
Table 21: SSP Table 2 67
Table 22: Pre-Operational Self-Tests 67
Table 23: Conditional Self-Tests 71
Table 24: Pre-Operational Periodic Information 71
Table 25: Conditional Periodic Information 73
Table 26: Error States 73

List of Figures

No table of figures entries found.

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 PAN-OS VM-Series.

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:

The module provides network security by enabling enterprises to see and control applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies, found in Palo Alto Networks' enterprise firewalls, enable enterprises to create business-relevant security policies – safely enabling organizations to adopt new applications, instead of the traditional “all-or-nothing” approach offered by traditional port-blocking firewalls used in many security infrastructures.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

The PAN-OS VM-Series is a software cryptographic module that requires an underlying general purpose computer (GPC) environment

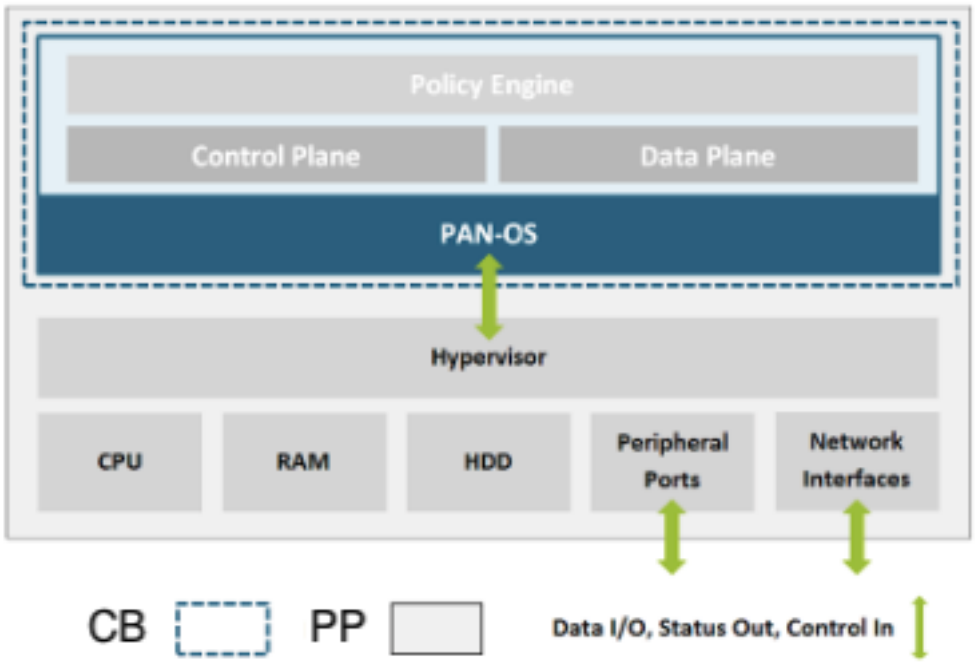

Figure 1 - Cryptographic Boundary

Tested Operational Environment's Physical Perimeter (TOEPP) :

The TOEPP for the module is defined by the enclosure around the host GPC on which it runs.

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
PanOS_vm-10.2.8-h4	10.2.8-h4	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)
N/A	Dell PowerEdge R740	Intel Xeon Gold 6248	No	Hyper-V 2019 on Microsoft Hyper-V Server 2019	10.2.8-h4
N/A	Dell PowerEdge R740	Intel Xeon Gold 6248	No	KVM 4 on Ubuntu 20.04	10.2.8-h4
N/A	Dell PowerEdge R740	Intel Xeon Gold 6248	No	VMware ESXi v7.0	10.2.8-h4

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:

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	A2907	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A2907	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-CTR	A2907	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - No Counter Tests Performed - No	SP 800-38A
AES-GCM	A2907	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A2907	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A2907	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A2907	Curve - P-256, P-384, P-521	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigGen (FIPS186-4)	A2907	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2907	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	A2907	MAC - MAC: 160 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A2907	MAC - MAC: 224 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A2907	MAC - MAC: 256 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A2907	MAC - MAC: 384 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2907	MAC - MAC: 512 Key Length - Key Length: 256-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A2907	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	A2907	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
KDF IKEv2 (CVL)	A2907	Initiator Nonce Length - Initiator Nonce Length: 128-256 Increment 8 Responder Nonce Length - Responder Nonce Length: 128-256 Increment 8 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 256, 384, 2048 Derived Keying Material Length - Derived Keying Material Length: 800-3072 Increment 8 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A2907	Password Length - Password Length: 64, 2048 Engine ID - 80001F8804303030303030343935323630	SP 800-135 Rev. 1
KDF SSH (CVL)	A2907	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A2907	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
RSA KeyGen (FIPS186-4)	A2907	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)	A2907	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A2907	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
Safe Primes Key Generation	A2907	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A2907	Safe Prime Groups - MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA-1	A2907	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-224	A2907	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2907	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A2907	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2907	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

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	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: (A2907) CKG: () Key Type: Symmetric
IPSec/IKE ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for IPSec/IKEv2		ECDSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: ()
IPSec/IKE ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for IPSec/IKEv2		ECDSA SigGen (FIPS186-4): (A2907) Counter DRBG: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
IPSec/IKE ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for IPSec/IKEv2		ECDSA SigVer (FIPS186-4): (A2907) ECDSA

Name	Type	Description	Properties	Algorithms
				KeyVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
IPSec/IKE Keying Materials Development	KAS-135KDF	IPSec/IKE session keying materials, used to derive IPSec/IKE session keys		KDF IKEv2: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) HMAC-SHA2-512: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
IPSec/IKE RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for IPSec/IKEv2		RSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: ()
IPSec/IKE RSA SigGen	DigSig-SigGen	RSA SigGen for IPSec/IKEv2		RSA SigGen (FIPS186-4): (A2907) SHA2-256: (A2907) SHA2-384: (A2907)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A2907)
IPSec/IKE RSA SigVer	DigSig-SigVer	RSA SigVer for IPSec/IKEv2		RSA SigVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
KAS-ECC (IPSec/IKE)	KAS-Full	Full KAS-ECC Key Agreement used for IPSec/IKEv2 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 between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A2907) KDF IKEv2: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) HMAC-SHA2-512: (A2907)
KAS-ECC (SSH)	KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 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	KAS-ECC-SSC Sp800-56Ar3: (A2907) KDF SSH: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)

Name	Type	Description	Properties	Algorithms
			methodology providing between 128 and 256 bits of security strength	SHA2-512: (A2907)
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 providing between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A2907) KDF TLS: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
KAS-ECC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS ECC keygen used in IPSec/IKEv2 service	Curves:P-256, P-384, and P-521 Encryption Strength:128, 192, or 256 bits	Counter DRBG: (A2907) CKG: ()
KAS-ECC-KeyGen (SSH)	CKG KAS-KeyGen	KAS ECC keygen used in SSHv2 service	Curves:P-256, P-384, and P-521 Encryption Strength:128, 192, or 256 bits	Counter DRBG: (A2907) CKG: ()
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS ECC keygen used in TLSv1.2 service	Curves:P-256, P-384, and P-521 Encryption Strength:128, 192, or 256 bits	Counter DRBG: (A2907) CKG: ()
KAS-FFC (IPSec/IKE)	KAS-Full	Full KAS-FFC Key Agreement used for IPSec/IKEv2 service	IG:IG D.F Scenario 2 Path 2, split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A2907) KDF IKEv2: (A2907) SHA2-256: (A2907) SHA2-384:

Name	Type	Description	Properties	Algorithms
			Caveat:Key establishment methodology providing between 112 and 150 bits of security strength	(A2907) SHA2-512: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) HMAC-SHA2-512: (A2907)
KAS-FFC (SSH)	KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 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 112 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A2907) KDF SSH: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
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 112 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A2907) KDF TLS: (A2907) Safe Primes Key Generation: (A2907) Safe Primes Key Verification: (A2907) HMAC-SHA2-256: (A2907) HMAC-

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
KAS-FFC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS FFC keygen used in IPSec/IKEv2 service	Key Sizes:2048, 3072, and 4096-bits Key Strengths:112, 128, or 150-bits	Counter DRBG: (A2907) CKG: ()
KAS-FFC-KeyGen (SSH)	CKG KAS-KeyGen	KAS FFC keygen used in SSHv2 service	Key Size:2048-bits Key Strength:112-bits	Counter DRBG: (A2907) CKG: ()
KAS-FFC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS FFC keygen used in TLSv1.2 service	Key Size:2048-bits Key Strength:112-bits	Counter DRBG: (A2907) CKG: ()
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 providing between 128 and 256 bits of security strength	AES-CBC: (A2907) HMAC-SHA2-224: (A2907) HMAC-SHA2-256: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
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 providing between 128 and	AES-GCM: (A2907) AES-CBC: (A2907)

Name	Type	Description	Properties	Algorithms
			256 bits of security strength	
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 establishment methodology providing between 128 and 256 bits of security strength	AES-CBC: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
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 providing between 128 and 256 bits of security strength	AES-GCM: (A2907) AES-CBC: (A2907)
Session Authentication (IPSec/IKE)	MAC	IPSec/IKE session authentication		HMAC-SHA-1: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) HMAC-SHA2-512: (A2907) SHA-1: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)

Name	Type	Description	Properties	Algorithms
Session Authentication (SNMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A2907) HMAC-SHA2-224: (A2907) SHA-1: (A2907) SHA2-224: (A2907)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-512: (A2907) SHA-1: (A2907) SHA2-256: (A2907) SHA2-512: (A2907)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	IPSec/IKE session protection		AES-CBC: (A2907) AES-GCM: (A2907)
Session Encryption/Decryption (SNMPv3)	BC-Auth BC-UnAuth	SNMPv3 session protection		AES-CFB128: (A2907)
Session Encryption/Decryption (SSH)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CBC: (A2907) AES-CTR: (A2907)

Name	Type	Description	Properties	Algorithms
				AES-GCM: (A2907)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A2907) AES-GCM: (A2907)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A2907) SHA-1: (A2907)
Software Load Test	DigSig-SigVer	Signature verification for software load test		RSA SigVer (FIPS186-4): (A2907) SHA2-256: (A2907)
SSH ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: ()
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-4): (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907) Counter DRBG: (A2907)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-4): (A2907) ECDSA

Name	Type	Description	Properties	Algorithms
				KeyVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
SSH RSA KeyGen	AsymKeyPair-KeyGen CKG	SSH KeyGen for SSHv2		RSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: ()
SSH RSA SigGen	DigSig-SigGen	RSA SigGen for SSHv2		RSA SigGen (FIPS186-4): (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
SSH RSA SigVer	DigSig-SigVer	RSA SigVer for SSHv2		RSA SigVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used		KDF SSH: (A2907) SHA-1:

Name	Type	Description	Properties	Algorithms
		to derive SSHv2 session keys.		(A2907) SHA2-256: (A2907) SHA2-512: (A2907)
TLS ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2		ECDSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: ()
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-4): (A2907) Counter DRBG: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-4): (A2907) ECDSA KeyVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A2907)
TLS RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-4): (A2907) Counter DRBG: (A2907) CKG: () KDF TLS: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-4): (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-4): (A2907) SHA-1: (A2907) SHA2-224: (A2907) SHA2-256: (A2907) SHA2-384: (A2907) SHA2-512: (A2907)

Name	Type	Description	Properties	Algorithms
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		KDF TLS: (A2907) HMAC-SHA2-256: (A2907) HMAC-SHA2-384: (A2907) SHA2-256: (A2907) SHA2-384: (A2907)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 IG C.H Conformance

GCM is used in the context of TLS, IPsec/IKEv2, 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 IPsec/IKEv2, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with RFCs 4106 and 7296 (RFC 5282 is not applicable, as the module does not use GCM within IKEv2 itself). During operational testing, the module was tested against an independent version of IPsec with IKEv2 and found to behave correctly.

● 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.

2.7.2 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.

2.7.3 IG C.K Conformance

The CAVP testing for Cert. #A2907 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-bits	128-bits	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

The module supports the following industry protocols:

- TLS 1.2
- SSHv2
- IPSec and IKEv2
- SNMPv3

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Power	Power supplies
N/A	Status Output	Self-test status output

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input Data Output Control Input Status Output	HTTPS, TLS, SNMP, IPsec, 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) (A2907)	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/(2112). 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) (A2907)	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/(2112). 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/(958).	The probability of successfully authenticating to the module within one minute is 10/(958). The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Pre-Shared Secret	PSK authentication	Password Based	The pre-shared key authentication method has a minimum security strength of 956. The probability of successfully authenticating to the module is 1/(956). The number of 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.	The probability of successfully authenticating to the module within a one minute period is 288,000,000/(956).

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	Identity	User	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret
Remote Access VPN (RA VPN)	Identity	CO	RSA-Based Certificate ECDSA-Based Certificate Password Pre-Shared Secret
Site-to-Site VPN (S-S VPN)	Identity	CO	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 (IPSec/IKE) KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH) KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (IPSec/IKE) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Encryption/De	Crypto Officer - CO, User, RA VPN Password: G,W,E - DHE/ECDHE Shared Secret Z: G,R,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : G,W,E - Entropy Input String: G,E - IKEv2 SKEYSEED: G,R,E - RSA Private Keys: G,W,E - SSH Client Public Key: W,E - SSH DHE/ECDHE Private Componen

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					cryption (SSH) Session Encryption/Decryption (TLSv1.2) SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLSv1.2 Keying Materials Development	ts: G,E,Z - SSH DHE/ECDHE Public Components: G,R,W,E,Z - SSH Host Public Key: G,R,W,E - SSH Session Authentication Keys: G,E,Z - SSH Session Encryption Keys: G,E,Z - TLS Encryption 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/mod	Configuration/ System Logs	Input configuration for various cryptographic functions	Module uses the configuration for cryptographic purposes	KAS-ECC (IPSec/IKE) KAS-ECC (SSH) KAS-ECC (TLSv1.2) KAS-ECC-KeyGen (SSH)	Crypto Officer - CA Certificates: G,R,W,E - CO, User, RA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ifying security policy, including creating User accounts and additional CO accounts				KAS-ECC-KeyGen (TLSv1.2) KAS-FFC (IPSec/IKE) KAS-FFC (SSH) KAS-FFC (TLSv1.2) KAS-FFC-KeyGen (SSH) KAS-FFC-KeyGen (TLSv1.2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) Session Authentication (SNMPv3) Session Authentication (SSHv2) Session Authentication (TLSv1.2) Session Encryption/Decryption (SNMPv3) Session Encryption/Decryption (SSH) Session Encryption/De	VPN Password: G,W,E - DHE/ECDHE Shared Secret Z: G,R,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : G,W,E - ECDSA Public Keys: G,R,W,E - Entropy Input String: G,E - IKEv2 SKEYSEED: G,R,E - Protocol Secrets: W,E - Public key for software content load test: W,E - RSA Private Keys: G,W,E - RSA Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					cryption (TLSv1.2) SNMPv3 Keying Materials Development SSH ECDSA KeyGen SSH ECDSA SigGen SSH ECDSA SigVer SSH RSA KeyGen SSH RSA SigGen SSH RSA SigVer SSHv2 Keying Materials Development TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLSv1.2 Keying Materials Development	Keys: G,R,W,E - SNMPv3 Authentication Key: G,E - SNMPv3 Authentication Secret: W,E - SNMPv3 Privacy Secret: W,E - SNMPv3 Session Key: G,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 Key: G,R,W,E - SSH Session Encryption Keys:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						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,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
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, RA VPN Password: G,W,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : 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 - SSH Session Encryption Keys: G,E,Z - TLS DHE/ECDHE Private Components: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- 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 Unauthenticated User - CO, User, RA VPN Password: G,W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : E - Entropy Input String: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- 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 - 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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						HMAC Keys: G,E,Z - TLS Master Secret: G,E,Z - TLS Pre-Master Secret: G,E,Z
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
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 content 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, RA VPN Password: E User - CO, User, RA VPN Password: E
VPN	Provide network access for remote users or site-to-site connection	Configuration/ System Logs	Initiating VPN connections	Module provides VPN connection	KAS-ECC-KeyGen (IPSec/IKE) KAS-FFC-KeyGen (IPSec/IKE) KAS-ECC	Remote Access VPN (RA VPN) - CA Certificates: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(IPSec/IKE) IPSec/IKE RSA KeyGen IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer IPSec/IKE ECDSA KeyGen IPSec/IKE ECDSA SigGen IPSec/IKE ECDSA SigVer Session Encryption/Decryption (IPSec/IKE) Session Authentication (IPSec/IKE) IPSec/IKE Keying Materials Development CKG	- DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : E - ECDSA Public Keys: W,E - Entropy Input String: G,E - RA VPN IPSec Authentication : G,E,Z - RA VPN IPSec Session Keys: G,E,Z - RSA Private Keys: E - RSA Public Keys: W,E - S-S VPN IPSec Pre-Shared Keys: W,E - S-S VPN IPSec/IKE DHE or ECDHE Private Components: G,E,Z - S-S VPN

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						IPSec/IKE DHE or ECDHE Public Components: G,R,W,E, Z - S-S VPN IPSec/IKE Session 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,E,Z - TLS Pre-Master Secret: G,E,Z Site-to-Site VPN

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(S-S VPN) - CA Certificates: W,E - DRBG Key: G,E - DRBG Seed : G,E - DRBG V: G,E - ECDSA Private Keys : E - ECDSA Public Keys: W,E - Entropy Input String: G,E - RA VPN IPSec Authentication : G,E,Z - RA VPN IPSec Session Keys: G,E,Z - RSA Private Keys: E - RSA Public Keys: W,E - S-S VPN IPSec Pre-Shared Keys: W,E - S-S VPN IPSec/IKE DHE or ECDHE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Components: G,E,Z - S-S VPN IPSec/IKE DHE or ECDHE Public Components: G,R,W,E,Z - S-S VPN IPSec/IKE Session 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,E,Z - TLS Pre-Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret: G,E,Z
Zeroize	Destroys (Zeroizes) all keys in the module	Zeroization indicator	Initiating zeroization command	Status of the zeroization process	None	Unauthenticated - CA Certificates: Z - CO, User, RA VPN Password: Z - DHE/ECDHE Shared Secret Z: Z - DRBG Key: Z - DRBG Seed : Z - DRBG V: Z - ECDSA Private Keys : Z - ECDSA Public Keys: Z - Entropy Input String: Z - IKEv2 SKEYSEED: Z - Protocol Secrets: Z - Public key for software content load test: Z - RA VPN

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						IPSec Authentication : Z - RA VPN IPSec Session Keys: Z - RSA Private Keys: Z - RSA Public Keys: Z - S-S VPN IPSec Pre-Shared Keys: Z - S-S VPN IPSec/IKE Authentication Keys: Z - S-S VPN IPSec/IKE DHE or ECDHE Private Components: Z - S-S VPN IPSec/IKE DHE or ECDHE Public Components: Z - S-S VPN IPSec/IKE Session Keys: Z - SNMPv3 Authentication Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SNMPv3 Authentication Secret: Z - SNMPv3 Privacy Secret: Z - SNMPv3 Session Key: Z - SSH Client Public Key: Z - SSH DHE/ECDHE Private Components: Z - SSH DHE/ECDHE Public Components: Z - SSH Host Public Key: Z - SSH Session Authentication Keys: Z - SSH Session Encryption Keys: Z - TLS DHE/ECDHE Private Components: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS DHE/ECDHE Public Components: Z - TLS Encryption Keys: Z - TLS HMAC Keys: Z - TLS Master 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 software load test by using RSA 2048 bits with SHA2-256 (RSA Cert. #A2907) for the new validated software to be uploaded into the module. A Software Load Test Key was preloaded to the module's binary at the factory and used for software load test. In order to load new software, the Crypto Officer must authenticate into the module before loading any software. 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 performs the Software Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A2907) during the Pre-Operational Self-Test. The module's executable code is in the form of the compiled software image loaded onto the module.

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 software integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

N/A for this module.

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature			
HighTemperature			
LowVoltage			
HighVoltage			

Table 15: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	
HighTemperature	

Table 16: Hardness Testing Temperatures

8 Non-Invasive Security

N/A

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 17: 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 Module's Boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of 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 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 Module's Boundary)	HDD	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)

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

Table 18: 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. The module's zeroization method is to overwrite the SSPs with either a random pattern or a constant pattern.	Powering off the module or terminating the session will erase all SSPs stored in the RAM of the module. 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.	Command via CLI or WebUI or by unplugging module
Zeroization Command	CO issues zeroization service. The module's zeroization method is to overwrite the SSPs with either a random pattern or a constant pattern.	The zeroization command will erase all SSPs stored in the RAM or in the Flash of the module. 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.	Entering into maintenance mode and selecting Factory Reset

Table 19: 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.

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 - 4096 bits - 128 - 256 bits	Public Key - PSP	Counter DRBG (A2907)		TLS RSA SigGen TLS RSA SigVer TLS ECDSA SigGen TLS ECDSA SigVer
CO, User, RA VPN Password	Authentication string with a minimum length of eight (8) characters.	8 characters minimum - N/A	Authentication Data - CSP - CSP			
DHE/ECDHE Shared Secret Z	Used to derive encryption keys	2048 bits, 3072 bits, 4096 bits; 256 bits, 384 bits, 521 bits - 112 bits,128 bits, 150 bits;	Key Agreement shared secret - CSP	KDF IKEv2 (A2907) KDF SSH (A2907)		KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128 bits,192 bits, 256 bits				
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		Counter DRBG (A2907)
DRBG Seed	DRBG seed coming from the entropy source Seed length = 384 bits	384 bits - 256 bits	DRBG Seed - CSP - CSP	Entropy as per SP 800-90B		Counter DRBG (A2907)
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		Counter DRBG (A2907)
ECDSA Private Keys	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)	256 - 521 bits - 128 - 256 bits	Private Key - CSP	Counter DRBG (A2907)		TLS ECDSA SigGen
ECDSA Public Keys	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer	128 - 256 bits - 128 bits minimum	Public Key - PSP	Counter DRBG (A2907)		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	384 bits - 256 bits	DRBG CSP - CSP	Entropy as per SP 800-90B		Counter DRBG (A2907)
IKEv2 SKEYSEED	Used to derive encryption keys	160 bits, 256 bits, 384 bits, or 512 bits - 160 bits, 256 bits, 384 bits, or 512 bits	Key Agreement seed - CSP	KDF IKEv2 (A2907)		KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)
Protocol Secrets	Secrets used by RADIUS or TACACS+ (8 characters minimum)	8 characters minimum - N/A	Authentication Data - CSP - CSP			
Public key for software content load test	Used to authenticate software and content to be installed on the firewall (RSA 2048 with SHA-256)	112 bits - 112 bits	Public Key - PSP - PSP			Software Load Test

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RA VPN IPSec Authentication	(HMAC-SHA-1, 160 bits) Used in authentication of remote access IPSec data.	160 bits - 160 bits	Session Key - CSP - CSP	CKG		Session Authentication (IPSec/IKE)
RA VPN IPSec Session Keys	Used to encrypt remote access sessions utilizing IPSec. (AES 128-CBC, 128/256-GCM)	128 or 256 bits - 128 or 256 bits	Session Key - CSP - CSP	CKG		Session Encryption/Decryption (IPSec/IKE)
RSA Private Keys	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)	2048 - 4096 bits - 112 - 152 bits	Private Key - CSP	Counter DRBG (A2907)		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 - 152 bits	Public Key - PSP	Counter DRBG (A2907)		TLS RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
S-S VPN IPSec Pre-Shared Keys	PSK used in conjunction with HMAC listed above for authentication. Entered into the module by the Crypto Officer once authenticated	N/A - N/A	Shared Secret - CSP - CSP			IPSec/IKE Keying Materials Development
S-S VPN IPSec/IKE Authentication Keys	(HMAC-SHA-1, SHA-256, SHA-384 or SHA-512) Used to authenticate the peer in an IKE/IPSec tunnel connection. (160, 256, 384, 512 bits)	160 - 512 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF IKEv2 (A2907)	KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)	Session Authentication (IPSec/IKE)
S-S VPN IPSec/IKE DHE or ECDHE Private Components	Diffie-Hellman or EC Diffie-Hellman private component used in key establishment (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521)	2048 - 4096 bits - 128 - 256 bits	Private Key - CSP - CSP	Counter DRBG (A2907)		IPSec/IKE Keying Materials Development
S-S VPN IPSec/IKE DHE or ECDHE Public	Diffie-Hellman or EC Diffie-Hellman public component	2048 - 4096 bits - 128 - 256 bits	Public Key - PSP - PSP	Counter DRBG (A2907)		IPSec/IKE Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Components	used in key agreement (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521)					
S-S VPN IPSec/IKE Session Keys	Used to encrypt IKE/IPSec data. These are AES (128, 192, or 256 CBC) IKE keys and (128, 192 or 256 CBC, , 128 or 256 GCM) IPSec keys	128 - 256 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF IKEv2 (A2907)	KAS-ECC (IPSec/IKE) KAS-FFC (IPSec/IKE)	Session Encryption/Decryption (IPSec/IKE)
SNMPv3 Authentication Key	HMAC-SHA-1/224/256/384/512 Authentication protocol key (160 bits)	160 - 512 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF SNMP (A2907)		Session Authentication (SNMPv3)
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
SNMPv3 Session Key	Privacy protocol encryption key (AES	128 - 256 bits - 128 -	Session Key - CSP - CSP	KDF SNMP (A2907)		Session Encryption/Decryption (SNMPv3)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	128/192/256 CFB)	256 bits				
SSH Client Public Key	Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits)	2048 - 4096 bits - 112 - 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 - 128 - 256 bits	Private Key - CSP - CSP	Counter DRBG (A2907)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development
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 - 128 - 256 bits	Public Key - PSP - PSP	Counter DRBG (A2907)	KAS-ECC (SSH) KAS-FFC (SSH)	SSHv2 Keying Materials Development
SSH Host Public Key	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)	2048 - 4096 bits - 128 - 256 bits	Public Key - PSP - PSP	Counter DRBG (A2907)		SSH ECDSA SigVer SSH RSA SigVer
SSH Session Authentication Keys	Authentication keys used in all SSH connections to the security module's command line	160, 256, or 512 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF SSH (A2907)	KAS-ECC (SSH) KAS-FFC (SSH)	Session Authentication (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)					
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 (A2907)	KAS-ECC (SSH) KAS-FFC (SSH)	Session Encryption/Decryption (SSH)
TLS DHE/ECDHE Private Components	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)	2048 bits - 4096 bits - 128 - 256 bits	Private Key - CSP	Counter DRBG (A2907)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS DHE/ECDHE Public Components	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-	2048 bits - 4096 bits - 128 - 256 bits	Public Key - PSP	Counter DRBG (A2907)	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)					
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	KDF TLS (A2907)	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 - 384 bits - 128 - 256 bits	Session Key - CSP - CSP	KDF TLS (A2907)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	Session Authentication (TLSv1.2)
TLS Master Secret	Secret value used to derive the TLS session keys	48 bytes - N/A	Master Secret - CSP - CSP	KDF TLS (A2907)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS Pre-Master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces	48 bytes - N/A	Shared Secret - CSP	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)	TLSv1.2 Keying Materials Development

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CA Certificates	Peer Public Key Input Password/Secret Input via	HDD:Plaintext RAM:Plaintext	Duration of use (Plaintext)	Zeroization Command Power	RSA Public Keys:Encrypts RSA Private Keys:Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	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			Cycle / Session Termination	ECDSA Public Keys:Encrypts ECDSA Private Keys :Encrypts
CO, User, RA VPN 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	N/A	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DHE/ECDHE Shared Secret Z		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Private Components:Paired With SSH DHE/ECDHE Public Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
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 / Session Termination	Entropy Input String:Paired With DRBG Seed :Paired With DRBG Key:Paired With
ECDSA Private Keys	Password/Secret Input via TLSv1.2 encrypted by AES and HMAC Password/Secr	HDD:Plaintext RAM:Plaintext	Duration of use (Plaintext)	Zeroization Command Power Cycle / Session	ECDSA Public Keys:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	et 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			Termination	
ECDSA Public Keys	Peer Public Key Input 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	ECDSA Private Keys :Paired With
Entropy Input String		RAM:Plaintext	Duration of use	Power Cycle /	DRBG Seed :Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	DRBG Key:Paired With DRBG V:Paired With
IKEv2 SKEYSEED		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Public Components: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 content load test		HDD:Plaintext	N/A	N/A	
RA VPN IPSec		RAM:Plaintext	Duration of use	Power Cycle / Session	

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

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	AES-GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM				
S-S VPN IPSec Pre-Shared 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	
S-S VPN IPSec/IKE Authentication Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Derived From S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paire

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					d With S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
S-S VPN IPSec/IKE DHE or ECDHE Private Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
S-S VPN IPSec/IKE DHE or ECDHE Public Components		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With
S-S VPN IPSec/IKE Session Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	S-S VPN IPSec/IKE DHE or ECDHE Private Components:Derived From S-S VPN IPSec/IKE DHE or ECDHE Private Components:Paired With S-S VPN IPSec/IKE DHE or ECDHE Public Components:Paired With
SNMPv3 Authentication 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	HDD:Plaintext	Duration of use	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	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	RAM:Plaintext	(plaintext)		
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 encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by AES-GCM	HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SNMPv3 Session Key		HDD:Plaintext RAM:Plaintext	Duration of use (plaintext)	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Privacy Secret:Derived From
SSH Client Public Key	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 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 Termination	SSH DHE/ECDHE Private Components:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH Host Public Key		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 Private Components:Derived From SSH DHE/ECDHE Public Components:Derived From
SSH Session Encryption Keys		RAM:Plaintext	Duration of use	Power Cycle / Session Termination	SSH DHE/ECDHE Private Components:Derived From SSH DHE/ECDHE Public 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
TLS Master Secret		RAM:Plaintext	Duration of use	Power Cycle / Session	TLS Pre-Master Secret:Derived From

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

Table 21: 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) (A2907)	P-256	KAT	SW/FW Integrity	Self-Test successful	Signature Verification
HMAC-SHA2-256 (A2907)	SHA2-256	KAT	SW/FW Integrity	Self-Test successful	Keyed Checksum

Table 22: Pre-Operational Self-Tests

The CASTs for the underlying ECDSA Signature Verification and HMAC-SHA2-256 algorithms are performed prior to the execution of the software integrity test listed in this section.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES GCM (A2907) Decrypt	256 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
AES GCM (A2907) Encrypt	256 Bits	KAT	CAST	Self-test output message	Encrypt	After each power-on or via self-test command

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A2907)	128 Bits	KAT	CAST	Self-test output message	Decrypt	After each power-on or via self-test command
Counter DRBG (A2907)	N/A	KAT / Health Tests	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) (A2907)	256 Bits	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
ECDSA SigVer (FIPS186-4) (A2907)	256 Bits	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
HMAC-SHA-1 (A2907)	160 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-224 (A2907)	224 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-256 (A2907)	256 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
HMAC-SHA2-384 (A2907)	384 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						self-test command
HMAC-SHA2-512 (A2907)	512 Bits	KAT	CAST	Self-test output message	Keyed Hash	After each power-on or via self-test command
KAS-ECC-SSC Sp800-56Ar3 (A2907)	256 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KAS-FFC	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
KAS-FFC-SSC Sp800-56Ar3 (A2907)	2048 Bits	KAT	CAST	Self-test output message	KAS Computation	After each power-on or via self-test command
KDF IKEv2 (A2907)	N/A	KAT	CAST	Self-test output message	IKEv2 with SHA-256	After each power-on or via self-test command
KDF SSH (A2907)	N/A	KAT	CAST	Self-test output message	SSHv2 with SHA-256	After each power-on or via self-test command
KDF TLS (A2907)	N/A	KAT	CAST	Self-test output message	TLSv1.2 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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A2907)	2048	KAT	CAST	Self-test output message	Sign	After each power-on or via self-test command
RSA SigVer (FIPS186-4) (A2907)	2048	KAT	CAST	Self-test output message	Verify	After each power-on or via self-test command
Safe Primes Key Generation (A2907)	2048 Bit Minimum	PCT	PCT	System log messages	KAS-FCC pairwise consistency test	On session
SHA-1 (A2907)	160 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-256 (A2907)	256 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-384 (A2907)	384 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
SHA2-512 (A2907)	512 Bits	KAT	CAST	Self-test output message	Hash	After each power-on or via self-test command
Software Load Test	2048 Bits	SW Load Test	SW/FW Load	System log messages	Software load test on content load	On session
SP 800-90B RCT/AP	N/A	Fault-Detection Test	CAST	Self-test output message	Health tests done on entropy source	After each power-on or via

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
T Health Tests on Entropy Source						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 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A2907)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A2907)	KAT	SW/FW Integrity	On Demand	Manually or Scheduled

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES GCM (A2907) Decrypt	KAT	CAST	On Demand	Manually or Scheduled
AES GCM (A2907) Encrypt	KAT	CAST	On Demand	Manually or Scheduled
AES-ECB (A2907)	KAT	CAST	On Demand	Manually or Scheduled
Counter DRBG (A2907)	KAT / Health Tests	CAST	On Demand	Manually or Scheduled
ECDSA / KAS-ECC	PCT	PCT	On session	On session
ECDSA SigGen (FIPS186-4) (A2907)	KAT	CAST	On Demand	Manually or Scheduled
ECDSA SigVer (FIPS186-4) (A2907)	KAT	CAST	On Demand	Manually or Scheduled

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-224 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-256 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-384 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
HMAC-SHA2-512 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
KAS-ECC-SSC Sp800-56Ar3 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
KAS-FFC	PCT	PCT	On session	On session
KAS-FFC-SSC Sp800-56Ar3 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
KDF IKEv2 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
KDF SSH (A2907)	KAT	CAST	On Demand	Manually or Scheduled
KDF TLS (A2907)	KAT	CAST	On Demand	Manually or Scheduled
RSA	PCT	PCT	On session	On session
RSA SigGen (FIPS186-4) (A2907)	KAT	CAST	On Demand	Manually or Scheduled
RSA SigVer (FIPS186-4) (A2907)	KAT	CAST	On Demand	Manually or Scheduled
Safe Primes Key Generation (A2907)	PCT	PCT	On session	On session
SHA-1 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-256 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-384 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
SHA2-512 (A2907)	KAT	CAST	On Demand	Manually or Scheduled
Software Load Test	SW 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

Table 25: 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 26: Error States

10.5 Operator Initiation of Self-Tests

Perform a power-cycle to initiate the Self-Tests.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The following procedure will put 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 enter the Approved mode.

- Select “Enable FIPS-CC Mode”.
- When prompted, select “Reboot” and the module will re-initialize and continue into “FIPS-CC” mode (Approved mode).
- The module will reboot.
- In “FIPS-CC” mode, the console port is available 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.

Should one or more power-up self-tests fail, the Approved mode of operation will not be achieved. Feedback will consist of:

- The module will output “FIPS-CC failure”
- The module will reboot and enter a state in which the reason for the reboot can be determined.
- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

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

11.2 Administrator Guidance

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

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-2/pan-os-admin/pan-os-admin.pdf

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

In FIPS-CC mode, the following rules shall apply:
The operator should not enable TLSv1.0 or use RSA for key wrapping; it is disabled by default.
Checked via CLI using “show shared” command
The operator should not enable TLSv1.3, it is disabled by default.
Checked via CLI using “show profiles” command
If using RADIUS, it must be configured using TLS.
Checked via CLI using “show shared” command
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.
Checked via CLI using “show deviceconfig” command

11.6 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

N/A