PAN-OS 11.0 VM-Series

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.1

Revision Date: June 13, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. General

The PAN-OS 11.0 VM-Series module is available in multiple capacity options. All models can be deployed as guest virtual machines on VMware ESXi, Hyper-V, and Linux server that is running the KVM (Kernel-based Virtual Machine) using a common base image distributed in a compatible hypervisor format.

The PAN-OS VM-Series is the virtualized form factor of the Palo Alto Networks next-generation firewall. The VM-Series is used to protect applications/data from cyber threats using Palo Alto Networks' next-generation firewall and advanced threat prevention features.

For purposes of this validation, the exact software version of the module tested was 11.0.3-h12. The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-3.

Table 1 - Security Levels

ISO/IEC 24759 Section 6.	FIPS 140-3 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

2. Cryptographic Module Specification

The tested operational environments are highlighted in Table 2.

Table 2 - Tested Operational Environments

Operating System	Hardware Platform	Processor	PAA/Acceleration
VMware ESXi v7.0	Dell PowerEdge R740	Intel Xeon Gold 6248	N/A
KVM 4 on Ubuntu 20.04	Dell PowerEdge R740	Intel Xeon Gold 6248	N/A
Hyper-V 2019 on Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Xeon Gold 6248	N/A

Table 3 - Vendor Affirmed Operational Environments

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

Operator Porting Rules

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

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

Approved Mode of Operation

The following procedure will put the module into the Approved mode of operation:

- During initial boot up, break the boot sequence via the console port connection (by entering "maint") 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 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.

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 reboot and enter a state in which the reason for the reboot can be determined.
- The module will output "FIPS-CC failure."
- 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.

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.

Zeroization

To perform the zeroization service, follow the procedure below:

- 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"

Approved and Allowed Algorithms

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

Table 4 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A1791	Conditioning Component AES-CBC-MAC SP 800-90B	AES-CBC-MAC	128 bits	Vetted conditioning component for ESV Cert. #E69
A3454	AES-CBC [SP 800-38A]	CBC	128, 192 and 256 bits	Encryption Decryption
A3454	AES-CFB128 [SP 800-38A]	CFB128	128 bits	Encryption Decryption
A3454	AES-CTR [SP 800-38A]	CTR	128, 192 and 256 bits	Encryption Decryption
A3454	AES-GCM [SP 800-38D]	GCM**	128 and 256 bits	Encryption Decryption
A3454	Counter DRBG [SP 800-90Arev1]	CTR DRBG	AES 256 bits with Derivation Function Enabled	Random Bit Generator
A3454	ECDSA KeyGen (FIPS 186-4)	ECDSA KeyGen	P-256, P-384, P-521	Key Generation
A3454	ECDSA KeyVer (FIPS 186-4)	ECDSA KeyVer	P-256, P-384, P-521	Public Key Validation
A3454	ECDSA SigGen (FIPS 186-4)	ECDSA SigGen	P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Generation
A3454	ECDSA SigVer (FIPS 186-4)	ECDSA SigVer	P-256, P-384, P-521 with SHA-1, SHA2-224,	Signature Verification

			SHA2-256, SHA2-384, and SHA2-512	
A3454	HMAC-SHA-1 [FIPS 198-1]	HMAC	HMAC-SHA-1 with λ=96, 160	Authentication for protocols
A3454	HMAC-SHA2-224 [FIPS 198-1]	HMAC	HMAC-SHA2-224 with λ=224	Authentication for protocols
A3454	HMAC-SHA2-256 [FIPS 198-1]	HMAC	HMAC-SHA2-256 with λ=256	Authentication for protocols
A3454	HMAC-SHA2-384 [FIPS 198-1]	HMAC	HMAC-SHA2-384 with λ=384	Authentication for protocols
A3454	HMAC-SHA2-512 [FIPS 198-1]	HMAC	HMAC-SHA2-512 with λ=512	Authentication for protocols
A3454	KAS-ECC-SSC Sp800-56Ar3	KAS	P-256/P-384/P-521	Key Exchange
A3454	KAS-FFC-SSC SP 800-56Ar3	KAS	MODP-2048/3072/4096	Key Exchange
A3454	KDF IKEv2 [SP 800-135rev1] (CVL)	IKEv2 KDF	SHA2-256, SHA2-384, SHA2-512	IKEv2
A3454	KDF SNMP [SP 800-135rev1] (CVL)	SNMPv3 KDF	Engine ID: 80001F88043030303030343935323630	SNMPv3
A3454	KDF SSH [SP 800-135rev1] (CVL)	SSHv2 KDF	SHA-1, SHA2-256, SHA2-512	SSH
A3454	TLS v1.2 KDF RFC7627 (CVL)	TLS1.2 KDF	TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384	TLS
A3454	RSA KeyGen (FIPS 186-4)	RSA KeyGen (FIPS 186-4)	2048, 3072, and 4096 bits	Key Pair Generation
A3454	RSA SigGen (FIPS 186-4)	RSA SigGen (FIPS 186-4)	2048, 3072, and 4096-bit with hashes 256/384/512	Signature Generation
A3454	RSA SigVer (FIPS 186-4)	RSA SigVer (FIPS 186-4)	2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1/224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not supported for ANSI X9.31	Signature Verification
A3454	SHA-1 [FIPS 180-4]	SHA	SHA-1	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A3454	SHA2-224 [FIPS 180-4]	SHA2	SHA-224	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A3454	SHA2-256 [FIPS 180-4]	SHA2	SHA-256	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A3454	SHA2-384 [FIPS 180-4]	SHA2	SHA-384	Digital Signature Generation/Verification

				Non-Digital Signature Applications (e.g. component of HMAC)
A3454	SHA2-512 [FIPS 180-4]	SHA2	SHA-512	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A3454	Safe Primes Key Generation [RFC 3526]	Safe Primes Key Generation	MODP-2048, MODP-3072, MODP-4096	Safe Primes Key Generation
A3454	Safe Primes Key Verification [RFC 3526]	Safe Primes Key Verification	MODP-2048, MODP-3072, MODP-4096	Safe Primes Key Verification
AES Cert. #A3454 and HMAC Cert. #A3454	KTS [SP 800-38F]	SP 800-38A and FIPS 198-1. KTS (key wrapping and unwrapping) per IG D.G.	AES-CBC or AES-CTR plus HMAC 128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping
AES-GCM Cert. A3454	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	AES-GCM 128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping
ESV Cert. #E69	SP 800-90B	ESV	Palo Alto Networks DRNG Entropy Source	Entropy
KAS-ECC-SSC Cert. #A3454, KDF IKEv2 Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256 and P-384 curves providing 128 or 192 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A3454, KDF SSH Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-ECC-SSC Cert. #A3454, TLS v1.2 KDF RFC7627 Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A3454, KDF IKEv2 Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048, 3072, and 4096-bit keys providing 112, 128, or 150 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A3454, KDF SSH Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
KAS-FFC-SSC Cert. #A3454, TLS v1.2 KDF RFC7627 Cert. #A3454	KAS [SP 800-56Arev3]	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	Key Exchange with protocol KDF
Vendor Affirmed	CKG (SP 800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-133 and IG D.H.	Key Generation Note: Symmetric keys and the seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment, and ensures when the nonce_explicit

part of the IV exhausts all possible values for a given session key, that a new TLS handshake is initiated per sections 7.4.1.1 and 7.4.1.2 of RFC 5246. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

    - From this RFC 5288, the GCM cipher suites in use are TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- 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), and ensures when the module exhausts all possible values for a given session key that this triggers a rekey condition. 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 2^{64} is exhausted, which can take hundreds of years. (In FIPS-CC Mode, SSH rekey is automatically configured at 1 GB of data or 1 hour, whichever comes first.)

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

The module is compliant to IG C.F:

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

The module does not have any algorithms that fall under:

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

Table 5 - Supported Protocols in the Approved Mode

Supported Protocols*
TLS 1.2
SSHv2
SNMPv3
IPsec and IKEv2

*Note: These protocols have not been tested or reviewed by the CMVP or the CAVP.

Cryptographic Boundary

The PAN-OS 11.0 VM-Series 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 is included in the file name in Section 11 (PanOS_vm-11.0.3-h12) 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.

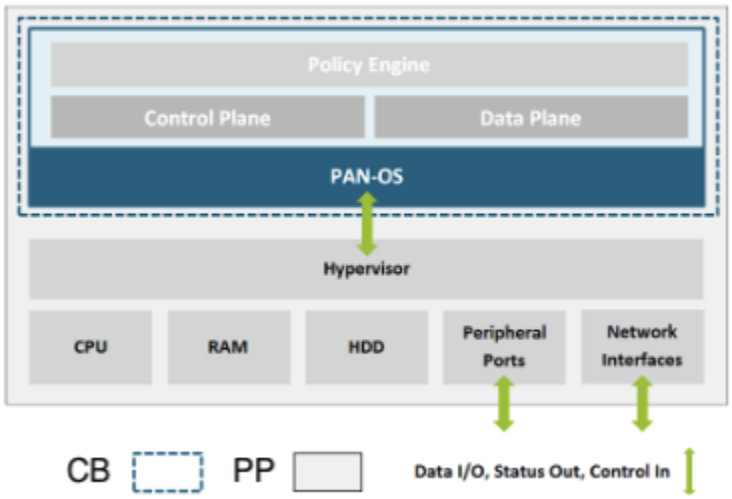

Figure 1 - Cryptographic Boundary

3. Cryptographic Module Interfaces

The module is a software only module that operates on a general purpose computing (GPC) platform. The physical ports and logical interfaces are consistent with a GPC operating environment. The module supports the following FIPS 140-3 logical interfaces:

Table 6 - Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
Power	Power In	Power supplies
Console, GPC I/O	Status Output	Self-test status output
Ethernet	Data input, control input, data output, status output	HTTPS, TLS, SNMP, IPsec, and SSH traffic data.

The module does not support a Control Output interface.

The module's physical and electrical characteristics, manual controls, and physical indicators are provided by the host GPC; the hypervisors provide virtualized ports and interfaces which map to the GPCs' physical ports and interfaces (i.e., network interfaces and GPC inputs/outputs).

4. Roles, Services, and Authentication

Roles and Services

While in the Approved mode of operation, all CO and User services are accessed via SSH or TLS sessions. Approved and allowed algorithms, relevant CSPs and public keys related to these protocols are accessed to support the following services. CSP access by services is further described in the following tables.

Table 7 - Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer	Show Version	Query module for version	Module provides version
Crypto Officer, User	Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts via CLI or WebUI	Confirmation of service via Configuration Logs
Crypto Officer	Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration via CLI or WebUI	Confirmation of service via Configuration Logs
Crypto Officer, User	View Other Configuration	Query module for current non-security relevant configuration via WebUI or CLI	Confirmation of service via Configuration Logs
Crypto Officer, User, RA VPN, S-S VPN	Show Status	Query status and version of the module via WebUI or CLI	Module status information via CLI or System Logs
RA VPN, S-S VPN	VPN	Initialize VPN connection	Confirmation of service via System Logs
Crypto Officer	Software Update	Loading new image	Message output noting version updated successfully
Unauthenticated	Zeroize	Initiate zeroization command	The device will overwrite all CSPs and provide status of completion
Unauthenticated	Self-Tests	Power cycling the module	Self-test status output via system logs
Unauthenticated	Show Status (Hypervisor)	View status of the module via hypervisor.	Module status via the hypervisor

The zeroization procedure is invoked when the operator initiates the service. The operator must be in control of the module during the entire procedure to ensure that it has successfully completed. During the zeroization procedure, no other services are available.

Note: Additional information on the configuration options the module provides can be found at https://docs.paloaltonetworks.com/

Assumption of Roles

The modules support four distinct operator roles, User and Cryptographic Officer (CO), Remote Access VPN, and Site-to-site VPN. The cryptographic modules enforce the separation of roles using unique authentication credentials associated with operator accounts.

The modules do not provide a maintenance role or bypass capability.

The modules all support the use of a password (i.e. Memorized Secret as per SP 800-140E). Upon first boot, the module requires that the Cryptographic Officer change the password from the default one to a custom one. The module automatically enforces a minimum password length of at least 8 characters. In "FIPS-CC" mode, the module automatically enforces a maximum of 10 failed attempts. Passwords stored in the module are hashed using SHA-256, and any passwords that are transported into/out of the module are protected via TLS 1.2.

Table 8 – Roles and Authentication

Role	Authentication Method	Authentication Strength
Cryptographic Officer	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication)	Password-based The minimum length is eight (8) characters[1] (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^8)$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is $10/(95^8)$, which is less than 1/100,000. The firewall's configuration supports at most ten failed attempts to authenticate in a one-minute period. Certificate/Public key-based The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is $1/(2^{112})$ which is less than 1/1,000,000. The probability of
User	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication	
Remote Access VPN (RA VPN)	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication	

[1] In FIPS-CC Mode, the module checks and enforces the minimum password length of eight (8) as specified in SP 800-63B. Passwords are securely stored hashed with salt value, with very restricted access control, and rate limiting mechanism for authentication attempts.

		successfully authenticating to the module within a one minute period is 60,000,000/(2^{112}), which is less than 1/100,000. The firewall supports at most 60,000,000 new sessions per second to authenticate in a one-minute period.
Site-to-Site VPN (S-S VPN)	IKE/IPSec Pre-shared keys - Identification with the IP Address and authentication with the Pre-Shared Key or certificate based authentication	The pre-shared key authentication method has a minimum security strength[2] of 95^6. The probability of successfully authenticating to the module is 1/(95^6), which is less than 1/1,000,000. The number of authentication attempts is limited by the number of new connections per second supported (120,000) on the fastest platform of the Palo Alto Networks firewalls. The probability of successfully authenticating to the module within a one minute period is 7,200,000/(95^6), which is less than 1/100,000. The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 60,000,000/(2^{112}), which is less than 1/100,000. The firewall supports at most 60,000,000 new sessions per second to authenticate in a one-minute period.

Definition of CSPs Modes of Access

The following table defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

[2] Note: The security strength (95^6) is based on the use of ASCII characters that are utilized, which surpasses the 6 character random number password allowance that sets a baseline minimum acceptable strength of 10^6.

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

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

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

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

Z = Zeroise: The module zeroises the SSP.

Table 9 - Approved Services

Service	Description	Approved Security Functions		Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Version	Query the module to display the version	N/A		N/A	CO	N/A	Version displayed via System Logs / CLI / UI
Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	Configuration/System Logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	Configuration/System Logs
		KAS	TLS v1.2 KDF RFC7627	TLS Pre-Master Secret	CO	G/E/Z	Configuration/System Logs
			TLS v1.2 KDF RFC7627	TLS Master Secret	CO	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components	CO	G/E/Z	Configuration/System Logs
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys	CO	G/E/Z	Configuration/System Logs
			AES-CBC	TLS Encryption Keys	CO	G/E/Z	Configuration/System Logs
		KTS	AES-GCM				
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys	CO	G/E/Z	Configuration/System Logs
			AES-CBC, AES-CTR	SSH Session Encryption Keys	CO	G/E/Z	Configuration/System Logs
		KTS	AES-GCM				
		KAS	KDF SSH	SSH DHE/ECDHE Private Components	CO	G/E/Z	Configuration/System Logs
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	
		N/A		CO, User, RA VPN Password	CO	G/E/W	Configuration/System Logs
		Counter DRBG, ESV		Entropy Input String	CO	G/E	Configuration/System Logs
				DRBG Seed			
				DRBG V			

				DRBG Key			
		KDF SNMP		SNMPv3 Authentication Secret	CO	W/E	Configuration/System Logs
		KDF SNMP		SNMPv3 Privacy Secret	CO	W/E	Configuration/System Logs
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		Authentication Key	CO	G/E/Z	Configuration/System Logs
		AES-CFB128		Session Key	CO	G/E/Z	Configuration/System Logs
		N/A		Protocol Secrets	CO	W/E	Configuration/System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		CA Certificates	CO	G/R/E/W	Configuration/System Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		RSA Public Keys	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		SSH Host Public Key	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		SSH Client Public Key	CO	W/E	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		Public key for software load test	CO	W/E	Configuration/System Logs
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration	RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	Configuration/System Logs
		ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO	G/W/E	Configuration/System Logs
		KAS	TLS v1.2 KDF RFC7627	TLS Pre-Master Secret	CO	G/E/Z	Configuration/System Logs
			TLS v1.2 KDF RFC7627	TLS Master Secret	CO	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components	CO	G/E/Z	Configuration/System Logs
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		HMAC-SHA2-256 HMAC-SHA2-384		TLS HMAC Keys	CO	G/E/Z	Configuration/System Logs
		AES-CBC or AES-GCM		TLS Encryption Keys	CO	G/E/Z	Configuration/System Logs
		HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512		SSH Session Authentication Keys	CO	G/Z	Configuration/System Logs
		AES-CBC, AES-CTR, or AES-GCM		SSH Session Encryption Keys	CO	G/E/Z	Configuration/System Logs
		KAS	KDF SSH	SSH DHE/ECDHE Private Components	CO	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification			G/E/R/W/Z	
				SSH DHE/ECDHE Public Components			

		N/A		CO, User, RA VPN Password	CO	G/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		CA Certificates	CO	G/R/E/W	Configuration/System Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		RSA Public Keys	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		SSH Host Public Key	CO	G/R/E/W	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		SSH Client Public Key	CO	W/E	Configuration/System Logs
		Counter DRBG, ESV		DRBG Seed	CO	G/E	Configuration/System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
View Other Configuration	Read-only of non-security relevant configuration	N/A		CO, User, RA VPN Password Note: includes all items in "Other Configuration"	CO, User	W/E	Configuration/System Logs
Show Status	Provides status information of the module	RSA SigGen (FIPS 186-4)		RSA Private Keys	CO, User	E	Configuration/System Logs
		ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	CO, User	E	Configuration/System Logs
		KAS	TLS v1.2 KDF RFC7627	TLS Pre-Master Secret	CO, User	G/E/Z	Configuration/System Logs
			TLS v1.2 KDF RFC7627	TLS Master Secret	CO, User	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Private Components	CO, User	G/E/Z	Configuration/System Logs
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		HMAC-SHA2-256 HMAC-SHA2-384		TLS HMAC Keys	CO, User	G/E/Z	Configuration/System Logs
		AES-CBC or AES-GCM		TLS Encryption Keys	CO, User	G/E/Z	Configuration/System Logs
		HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512		SSH Session Authentication Keys	CO, User	G/E/Z	Configuration/System Logs
		AES-CBC, AES-CTR, or AES-GCM		SSH Session Encryption Keys	CO, User	G/E/Z	Configuration/System Logs
		KAS	KDF SSH	SSH DHE Public/Private Components	CO, User	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	SSH ECDHE Public/Private Components		G/E/R/W/Z	

		Counter DRBG, ESV		DRBG Seed DRBG V DRBG Key Entropy Input String	CO	G/E	Configuration/System Logs
VPN	Provide network access for remote users or site-to-site connection	KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	S-S VPN IPSec/IKE Authentication Keys	S-S VPN	G/E/Z	Configuration/System Logs
			AES-CBC	S-S VPN IPSec/IKE Session Keys	S-S VPN	G/E/Z	Configuration/System Logs
		KTS	AES-GCM				
		KAS	KDF IKEv2	S-S VPN IPSec/IKE DHE/ECDHE Private Components	S-S VPN	G/E/Z	Configuration/System Logs
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	S-S VPN IPSec/IKE DHE/ECDHE Public Components		G/E/R/W/Z	
		N/A		S-S VPN IPSec Pre-Shared Keys	S-S VPN	W/E	Configuration/System Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys	S-S VPN	W/E	Configuration/System Logs
		RSA SigVer (FIPS 186-4)		RSA Public Keys	S-S VPN	W/E	Configuration/System Logs
		Counter DRBG, ESV		DRBG Seed DRBG V DRBG Key Entropy Input String	CO	G/E	Configuration/System Logs
VPN	Provide network access for remote users or site-to-site connection	RSA SigGen (FIPS 186-4)		RSA Private Keys	RA VPN	E	Configuration/System Logs
		ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys	RA VPN	E	Configuration/System Logs
		KAS	TLS v1.2 KDF RFC7627	TLS Pre-Master Secret	RA VPN	G/E/Z	Configuration/System Logs
			TLS v1.2 KDF RFC7627	TLS Master Secret		G/E/Z	
			CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification	TLS DHE/ECDHE Public Components	RA VPN	G/E/R/W/Z	Configuration/System Logs
				TLS DHE/ECDHE Private Components	RA VPN	G/E/Z	Configuration/System Logs
		KTS	HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys	RA VPN	G/E/Z	Configuration/System Logs
			AES-CBC	TLS Encryption Keys	RA VPN	G/E/Z	Configuration/System Logs
		KTS	AES-GCM				
		CKG, AES-CBC or AES-GCM		RA VPN IPSec Session Keys	RA VPN	G/E/Z	Configuration/System Logs
		CKG, HMAC-SHA-1		RA VPN IPSec Authentication	RA VPN	G/E/Z	Configuration/System Logs

		Counter DRBG, ESV	Entropy Input String DRBG Seed DRBG V DRBG Key	RA VPN	G/E	Configuration/System Logs
		RSA SigVer (FIPS 186-4)) ECDSA SigVer (FIPS 186-4)	CA Certificates	RA VPN	W/E	Configuration/System Logs
		ECDSA SigVer (FIPS 186-4)	ECDSA Public Keys	RA VPN	W/E	Configuration/System Logs
		RSA SigVer (FIPS 186-4)	RSA Public Keys	RA VPN	W/E	Configuration/System Logs
Software Update	Provides a method to update the software of the module	RSA SigVer (FIPS 186-4)	Public key for software content load test Note: Includes all keys from Other Configuration	CO	E	Configuration/System Logs
Zeroize	Destroys all keys in the module	N/A	All keys and SSPs	CO	Z	Zeroization indicator
Self-Test	Initiates self-tests and integrity test	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4)	Software integrity verification key	CO	E	System Logs
Show Status (Hypervisor)	Provides status of the module	N/A	N/A	All	R	LEDs

Note: Configuration/System Logs for Approved services above will indicate FIPS-CC mode is enabled, configuration requirements from Section 11 are followed, and that the service succeeded.

5. Software/Firmware Security

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 the Public Verification Key (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.

6. Operational Environment

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.

7. Physical Security

There are no applicable FIPS 140-3 physical security requirements.

8. Non-Invasive Security

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

9. Sensitive Security Parameters

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

Table 10 - SSPs

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[1]	Use & Related Keys
CA Certificates	112 bits minimum	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)
RSA Public Keys	112 bits minimum	RSA SigVer (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096-bit)
RSA Private Keys	112 bits minimum	RSA SigGen (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit)
ECDSA Public Keys	128 bits minimum	ECDSA SigVer (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted or Plaintext TLS handshake	N/A	HDD/RAM – plaintext	Zeroize Service	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)
ECDSA Private Keys	128 bits minimum	ECDSA SigGen (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	HDD – Zeroize Service RAM - Zeroize at session termination	ECDSA Private key for generation of signatures and authentication (P-256, P-384, or P-521)
TLS DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)
TLS DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DRBG, SP 800-56A Rev. 3	Plaintext - TLS handshake	N/A	N/A	Zeroize at session termination	Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement

								(DHE 2048, ECDHE P-256, P-384, P-521)
TLS Pre-Master Secret	N/A	TLS v1.2 KDF RFC7627 Cert. #A3454	KAS SP 800-56A Rev. 3	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS Master Secret along with client and server random nonces
TLS Master Secret	N/A	TLS v1.2 KDF RFC7627 Cert. #A3454	TLS v1.2 KDF RFC7627	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS session keys
TLS Encryption Keys	128 bits minimum	AES-CBC or AES-GCM Cert. #A3454	TLS v1.2 KDF RFC7627	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)
TLS HMAC Keys	256 bits minimum	HMAC-SHA2-256 HMAC-SHA2-384 Cert. #A3454	TLS v1.2 KDF RFC7627	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	HMAC keys used in TLS connections (SHA2- 256/384) (256, 384 bits)
SSH DHE/ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
SSH DHE/ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DRBG, SP 800-56A Rev. 3	Plaintext SSH handshake	N/A	RAM - plaintext	Zeroize at session termination	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
SSH Host Public Key	112 bits minimum	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A3454	DRBG, FIPS 186-4	N/A	N/A	HDD/RAM – plaintext	Zeroize Service	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521)
SSH Client Public Key	112 bits minimum	RSA SigVer (FIPS 186-4) Cert. #A3454	N/A	Encrypted via SSH or TLS	N/A	HDD/RAM – plaintext	Zeroize Service	Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits)
SSH Session Encryption Keys	128 bits minimum	AES-CBC, AES-CTR, or AES-GCM Cert. #A3454	KDF SSH	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	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)
SSH Session Authentication Keys	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 Cert. #A3454	KDF SSH	N/A	SSH, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	Authentication keys used in all SSH connections to the security module's command line interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits)
S-S VPN IPSec/IKE DHE or ECDHE Private Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DBRG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Power cycle	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)
S-S VPN IPSec/IKE DHE or ECDHE Public Components	112 bits minimum	KAS-ECC-SSC KAS-FFC-SSC Cert. #A3454	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Power cycle	Diffie-Hellman or EC Diffie-Hellman public component used in key agreement (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521)

S-S VPN IPSec/IKE Session Keys	128 bits minimum	AES-CBC, AES-GCM Cert. #A3454	KDF IKEv2	N/A	IPSec/IKE, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	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
S-S VPN IPSec/IKE Authentication Keys	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A3454	KDF IKEv2	N/A	IPSec/IKE, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	(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)
S-S VPN IPSec Pre-Shared Keys	N/A	N/A	N/A	Encrypted via SSH or TLS	N/A	HDD/RAM – plaintext	Zeroize Service	PSK used in conjunction with HMAC listed above for authentication. Entered into the module by the Crypto Officer once authenticated
RA VPN IPSec Session Keys	128 bits minimum	AES-CBC or AES-GCM Cert. #A3454	CKG, DRBG	N/A	N/A	RAM - plaintext	Zeroize at session termination	Used to encrypt remote access sessions utilizing IPSec. (AES 128-CBC, 128/256-GCM)
RA VPN IPSec Authentication	160 bits	HMAC-SHA-1 Cert. #A3454	CKG, DRBG	N/A	N/A	RAM - plaintext	Zeroize at session termination	(HMAC-SHA-1, 160 bits) Used in authentication of remote access IPSec data.
Software integrity verification key	128 bits	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4) Cert. #A3454	N/A	N/A	N/A	HDD - plaintext	N/A	Used to check the integrity of all software code (HMAC-SHA-256 and ECDSA P-256) *(Note: This is not considered an SSP)*
Public key for software content load test	112 bits	RSA SigVer (FIPS 186-4) Cert. #A3454	N/A	N/A	N/A	HDD - plaintext	N/A	Used to authenticate software/firmware and content to be installed on the firewall (RSA 2048 with SHA-256)
CO, User, RA VPN Password	N/A	SHA2-256 Cert. #A3454	External	Encrypted via SSH or TLS	N/A	HDD - a password hash (SHA2-256)	Zeroize Service	Authentication string with a minimum length of eight (8) characters.
Protocol Secrets	N/A	N/A	N/A	Encrypted via IPsec, SSH or TLS	N/A	HDD/RAM – plaintext	Zeroize Service	Secrets used by RADIUS or TACACS+ (8 characters minimum)
Entropy Input String	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A3454	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	Entropy input string coming from the entropy source Input length = 384 bits
DRBG Seed	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A3454	Entropy as per SP 800-90B	N/A	N/A	RAM - Plaintext	Power cycle	DRBG seed coming from the entropy source Seed length = 384 bits
DRBG Key	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A3454	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state Key used in the generation of a random values
DRBG V	128 bits	CKG (vendor affirmed), Counter DRBG	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state V used in the

		Cert. #A3454						generation of a random values
SNMPv3 Authentication Secret	N/A	KDF SNMP Cert. #A3454	N/A	Encrypted via TLS/SSH	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
SNMPv3 Privacy Secret	N/A	KDF SNMP Cert. #A3454	N/A	Encrypted via TLS/SSH	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
Authentication Key	160 bits minimum	HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A3454	KDF SNMP	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	HMAC–SHA-1/224/256/384/512 Authentication protocol key (160 bits)
Session Key	128 bits minimum	AES-CFB Cert. #A3454	KDF SNMP	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	Privacy protocol encryption key (AES 128/192/256 CFB)

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

Table 11 - Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
Palo Alto Networks DRNG Entropy Source	256 bits	ESV Cert. #E69 Entropy source provides full entropy, which is provided in the 384 bit seed.

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; these tests do not require any additional operator action.

Pre-operational Self-Tests

Pre-operational Software Integrity Test

- 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

Conditional self-tests

Cryptographic algorithm self-tests

- AES 128-bit ECB Encrypt Known Answer Test*
- AES 128-bit ECB Decrypt Known Answer Test*
  *Note: Supported by the module cryptographic implementation, but only utilized for CAST
- AES 128-bit CMAC Known Answer Test*
  **Note: Supported by the module cryptographic implementation, but only utilized for CAST*
- AES 256-bit GCM Encrypt Known Answer Test
- AES 256-bit GCM Decrypt Known Answer Test

- AES 192-bit CCM Encrypt Known Answer Test*
- AES 192-bit CCM Decrypt Known Answer Test*
  *Note: Supported by the module cryptographic implementation, but only utilized for CAST
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Sign Known Answer Test
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Verify Known Answer Test
- RSA 2048-bit Encrypt Known Answer Test
- RSA 2048-bit Decrypt Known Answer Test
  Note: RSA Encrypt/Decrypt are only used for self-tests
- ECDSA P-256 with SHA-512 Sign Known Answer Test
- ECDSA P-256 with SHA-512 Verify Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- DRBG SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests
- SP 800-90Arev1 Instantiate/Generate/Reseed Section 11.3 Health Tests
- SP 800-56Ar3 KAS-FFC-SSC 2048-bit Known Answer Test
- SP 800-56Ar3 KAS-ECC-SSC P-256 Known Answer Test
- SP 800-135rev1 TLS 1.2 with SHA-256 KDF Known Answer Test
- SP 800-135rev1 SSH KDF with SHA-256 Known Answer Test
- SP 800-135rev1 IKEv2 KDF with SHA-256 Known Answer Test
- SP 800-90B RCT/APT Health Tests on Entropy Source
  Note: The SP 800-90B Health Tests are implemented by the entropy source.

Conditional Pairwise Consistency Self-Tests

- RSA Pairwise Consistency Test
- ECDSA/KAS-ECC Pairwise Consistency Test
- KAS-FFC Pairwise Consistency Test

Conditional Software Load test

- Software Load Test – Verify RSA 2048 with SHA-256 signature on software at time of load

Conditional Critical Functions Tests

- SP 800-56A Rev. 3 Assurance Tests (Based on Sections 5.5.2, 5.6.2, and 5.6.3)

Error Handling

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

Table 12 - Errors and Indicators

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

11. Life-Cycle Assurance

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 PanOS_vm-11.0.3-h12 from the support site: https://support.paloaltonetworks.com/Support/Index, and a checksum (SHA-256) is available to ensure the module is correct:

PanOS_vm-11.0.3-h12: 6c3522db244bdd200075038d4eb5fff580c1d49610fab75e7e9f28f65b451017

Alternatively, the VM-Series 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 11.0.3-h12**
3. **request system software install version 11.0.3-h12**
4. **request restart system**

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

The module design corresponds to the module security rules noted in the section below.

Module Enforced Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-3 Level 1 module.

1. The cryptographic module provides four distinct operator roles. These are the User role, Remote Access VPN role, Site-to-site VPN role, and the Cryptographic Officer role.
2. The cryptographic module provides identity-based authentication.
3. The cryptographic module clears previous authentications when a power cycle is performed.
4. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module will automatically log out the operator. The CO will configure the period of inactivity.
5. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
6. The operator can command the module to perform the power-up self-test by cycling power of the module.
7. Power-up self-tests do not require any operator action.
8. Data output is inhibited during power-up self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module does not support a maintenance interface or role.
12. The module does not have any external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.

14. The module does not output intermediate key generation values.
15. Pre-shared keys used for IKE/IPsec must be at least 6 bytes in length, but no more than 255 bytes.

Vendor Imposed Security Rules

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

1. The operator should not enable TLSv1.0 or use RSA for key wrapping; it is disabled by default.
    a. Checked via CLI using “show shared” command
2. The operator should not enable TLSv1.3, it is disabled by default.
    a. Checked via CLI using “show profiles” command
3. If using RADIUS, it must be configured using TLS.
    a. Checked via CLI using “show shared” command
4. 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.
    a. Checked via CLI using “show deviceconfig” command

Failure to follow these Security Rules will cause the module to operate in a non-compliant state.

Key to Entity

The cryptographic module associates all keys (secret, private, or public) stored within, entered into or output from the module with authenticated operators of the module. Keys stored within the module are only made available to authenticated operators via TLS or SSH. Keys are only input or output from the module by the authenticated operator via a SSH/TLS/IPsec protected communication. Any attempt to intervene in the key to entity relationship would require defeating the module TLS/SSH/IPsec encryption and authentication/integrity mechanism.

12. Mitigation of Other Attacks

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

13. References

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

Palo Alto Networks Administrator’s Guide:
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/pan-os-admin/pan-os-admin.pdf

14. Definitions and Acronyms

AES – Advanced Encryption Standard
CA – Certificate Authority
CLI – Command Line Interface

CO – Crypto-Officer
CSP – Critical Security Parameter
CVL – Component Validation List
DB9 – D-sub series, E size, 9 pins
DES – Data Encryption Standard
DH – Diffie-Hellman
DRBG – Deterministic Random Bit Generator
EDC – Error Detection Code
ECDH – Elliptical Curve Diffie-Hellman
ECDSA – Elliptical Curve Digital Signature Algorithm
FIPS – Federal Information Processing Standard
HMAC – (Keyed) Hashed Message Authentication Code
KDF – Key Derivation Function
LED – Light Emitting Diode
RJ45 – Networking Connector
RNG –Random number generator
RSA – Algorithm developed by Rivest, Shamir and Adleman
SHA – Secure Hash Algorithm
SNMP – Simple Network Management Protocol
SSH – Secure Shell
TLS – Transport Layer Security
USB – Universal Serial Bus
VGA – Video Graphics Array