Panorama Virtual Appliance 10.1

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.1

Revision Date: August 28, 2024

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. General

The Panorama Virtual Appliance 10.1 from Palo Alto Networks Inc., hereafter referred to as "Panorama VM" or the "cryptographic module" are multi-chip standalone cryptographic modules designed to fulfill FIPS 140-3 level 1 requirements. The Panorama VM provides a centralized monitoring and management of multiple Palo Alto Networks next-generation (NG) firewalls and Wildfire appliances.

For purposes of this validation, the exact software version of the module tested was 10.1.5. 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	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
1	VMware ESXi v7.0	Dell PowerEdge R740	Intel Gold 6248	N/A
2	KVM on Ubuntu 20.04	Dell PowerEdge R740	Intel Gold 6248	N/A
3	Hyper-V 2019 on Microsoft Hyper-V Server 2019	Dell PowerEdge R740	Intel Gold 6248	N/A

Table 3 – Vendor Affirmed Operational Environments

#	Operating System	Hardware Platform
1	Amazon Web Services (AWS)	x86 Architecture *(Note: Specific processor/hardware is dependent on Instance/Machine Type selected for operation system)*
2	Microsoft Azure	
3	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 this module on any general purpose computer (GPC) or platform using the specified hypervisor and operating system on the validation certificate or other compatible operating and/or hypervisor system and affirm the module's 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 initialize the modules into the Approved mode of operation:

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

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

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

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.

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.

Selecting Panorama, Management-Only, and Log Collector System Modes

The Panorama VM supports multiple configurations that provide varying services. The Cryptographic Officer can initialize the module into different System Mode. The module supports the following System Modes:

- Panorama
- Management-Only
- Log Collector

The default and primary mode of operation is Panorama mode. An additional mode, Log Collector mode, focuses primarily on log gathering instead of management. The final mode supported by the module is Management-Only, which focuses primarily on management functions without logging capabilities.
To convert the module from the default mode, Panorama mode, to Log Collector or Management-Only mode, follow the steps below:

Convert the Panorama VM from Panorama mode to Log Collector or Management-Only mode:

- Log into the CLI via SSH, CO is authenticated with username/password
- Enter "request system system-mode logger" or "request system system-mode management-only"
- Enter "Y" to confirm the change to the selected mode.
- The system will reboot and perform the required power on self-tests.

Convert the Panorama VM from Log Collector or Management-Only mode to Panorama mode:

- Log into the CLI via SSH, CO is authenticated with username/password
- Enter "request system system-mode panorama"
- Enter "Y" to confirm the change to the selected mode.
- The system will reboot and perform the required power on self-tests

Note*: Changing the System Mode does not change FIPS-CC Mode.*

Zeroization

The following procedure will zeroize the module:

- Access the module's CLI via SSH, and command the module to enter maintenance mode ("debug system 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.

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. #E129
A2244	AES-CBC [SP 800-38A]	CBC	128, 192 and 256 bits	Encryption Decryption
A2244	AES-CFB128 [SP 800-38A]	CFB128	128 bits	Encryption Decryption
A2244	AES-CTR [SP 800-38A]	CTR	128, 192 and 256 bits	Encryption Decryption
A2244	AES-GCM [SP 800-38D]	GCM**	128 and 256 bits	Encryption Decryption
A2244	Counter DRBG [SP 800-90Arev1]	Counter DRBG	AES 256 bits with Derivation Function Enabled	Random Bit Generator
A2244	ECDSA KeyGen (FIPS 186-4)	ECDSA KeyGen (FIPS 186-4)	P-256, P-384, P-521	Key Generation
A2244	ECDSA KeyVer (FIPS 186-4)	ECDSA KeyVer (FIPS 186-4)	P-256, P-384, P-521	Public Key Validation
A2244	ECDSA SigGen (FIPS 186-4)	ECDSA SigGen (FIPS 186-4)	P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Generation
A2244	ECDSA SigVer (FIPS 186-4)	ECDSA SigVer (FIPS 186-4)	P-256, P-384, P-521 with SHA-1, SHA2-224, SHA2-256, SHA2-384, and SHA2-512	Signature Verification
A2244	HMAC-SHA-1 [FIPS 198-1]	HMAC	HMAC-SHA-1 with λ=160	Authentication for protocols
A2244	HMAC-SHA2-224 [FIPS 198-1]	HMAC	HMAC-SHA2-224 with λ=224	Authentication for protocols
A2244	HMAC-SHA2-256 [FIPS 198-1]	HMAC	HMAC-SHA2-256 with λ=256	Authentication for protocols
A2244	HMAC-SHA2-384 [FIPS 198-1]	HMAC	HMAC-SHA2-384 with λ=384	Authentication for protocols
A2244	HMAC-SHA2-512 [FIPS 198-1]	HMAC	HMAC-SHA2-512 with λ=512	Authentication for protocols
A2244	KAS-ECC-SSC Sp800-56Ar3	KAS	Ephemeral Unified Model: P-256/P-384/P-521	Key Exchange
A2244	KAS-FFC-SSC SP 800-56Ar3	KAS	dhEphem: MODP-2048	Key Exchange
A2244	KDF SNMP [SP 800-135rev1] (CVL)	SNMPv3 KDF	Engine ID: 80001F8804303030303030343935323630	SNMPv3
A2244	KDF SSH [SP 800-135rev1] (CVL)	SSHv2 KDF	SHA-1, SHA2-256, SHA2-512	SSH
A2244	KDF TLS	TLS 1.0/1.1 KDF, TLS1.2 KDF	TLS v1.0/1.1 TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384	TLS

	[SP 800-135rev1] (CVL)			
A2244	RSA KeyGen (FIPS 186-4)	RSA KeyGen (FIPS 186-4)	2048, 3072, and 4096 bits	Key Pair Generation
A2244	RSA SigGen (FIPS 186-4)	RSA SigGen (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes SHA2-256/384/512	Signature Generation
A2244	RSA SigVer (FIPS 186-4)	RSA SigVer (FIPS 186-4)	(ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1 and SHA2-224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not supported for ANSI X9.31	Signature Verification
A2244	SHA-1 [FIPS 180-4]	SHA	SHA-1	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2244	SHA2-224 [FIPS 180-4]	SHA2	SHA-224	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2244	SHA2-256 [FIPS 180-4]	SHA2	SHA-256	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2244	SHA2-384 [FIPS 180-4]	SHA2	SHA-384	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2244	SHA2-512 [FIPS 180-4]	SHA2	SHA-512	Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC)
A2244	Safe Primes Key Generation [RFC 3526]	Safe Primes Key Generation	MODP-2048	Safe Primes Key Generation
A2244	Safe Primes Key Verification [RFC 3526]	Safe Primes Key Verification	MODP-2048	Safe Primes Key Verification
AES Cert. #A2244 and HMAC Cert. #A2244	KTS [SP 800-38F]	SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping. AES-CBC or AES-CTR with HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512
AES-GCM Cert. #A2244	KTS [SP 800-38F]	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128 and 256-bit keys providing 128 or 256 bits of encryption strength	Key Wrapping. AES-GCM.
ESV Cert. #E129	SP 800-90B	ESV	Palo Alto Networks DRNG RDSEED Entropy Source	Entropy

KAS-ECC-SSC Cert. #A2244, KDF SSH Cert. #A2244	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. #A2244, KDF TLS Cert. #A2244	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. #A2244, KDF SSH Cert. #A2244	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. #A2244, KDF TLS Cert. #A2244	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 800-133rev2 and IG D.I (asymmetric seeds).	Key Generation Note:The seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG

** The module is compliant to IG C.H: GCM is used in the context of TLS and SSH:

- 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 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. Also, 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 Not Allowed in the Approved Mode of Operation

The cryptographic module supports the following non-Approved algorithms that are allowed for use in the Approved mode of operation:

Table 5A - Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
MD5	Only allowed as the PRF in TLSv1.1 per IG 2.4.AOnly allowed as the PRF in TLSv1.0 and v1.1 per IG 2.4.A	Message digest used in TLSv1.0 / v1.1 KDF only

Table 6 - Supported Protocols in the Approved Mode

Supported Protocols*
TLS v1.1, v1.2
SSHv2
SNMPv3

*Note: No parts of these protocols, other than the approved cryptographic algorithms and the KDFs, have been tested or reviewed by the CAVP and CMVP.

Cryptographic Boundary

The Panorama Virtual Appliance is a software cryptographic module and requires an underlying general purpose computer (GPC) environment. The module consists of a GPC (multi-chip standalone embodiment) with the cryptographic boundary defined below. The cryptographic boundary (CB) includes all of the software components of the module, which is included in the file name in Section 11 (Panorama_pc-10.1.5) 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.

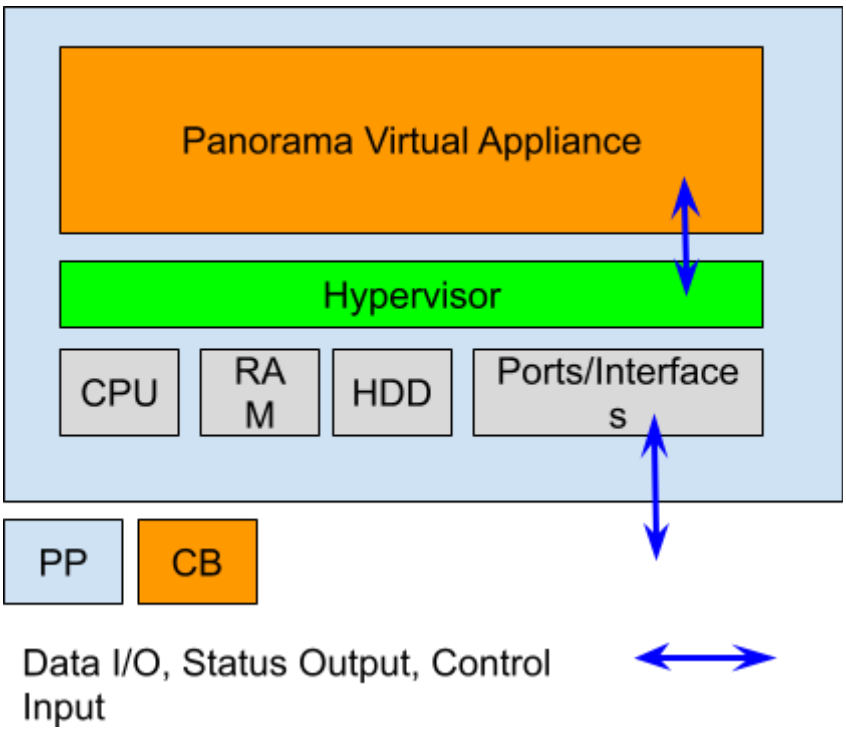

Figure 1 – Cryptographic Boundary

3. Cryptographic Module Interfaces

The Panorama VM is designed to operate on a general-purpose computer (GPC) platform. The module supports the following FIPS 140-3 interfaces, which have physical and logical ports consistent with a GPC operating environment. The module does not implement a control output interface.

Table 7 –Ports and Interfaces

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

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 8 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Version	Query module for version	Module provides version
CO, User	Access web portal	Connect to web portal from TLS client.	Confirmation of service via Configuration Logs
CO, User	Access CLI	Connect to SSH server from SSH client	Confirmation of service via Configuration Logs
CO	System Provisioning	Configuring and managing system configurations (e.g., IP address, system time, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Software Update	Loading new image	Message output noting version updated successfully via System Logs
CO	Panorama Manager Setup	Configuring and managing Manager configurations (e.g., HTTPS, NTP, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Manage Panorama Administrative Access	Configuring and managing Administrative configurations (e.g., creating user accounts, setting authentication method, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Configure High Availability	Configuring and managing High Availability (HA) configuration via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Certificate Management	Configuring and managing certificates via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Log Setting	Configuring and managing log settings via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Panorama Server Profiles	Configuring and managing Server configurations (e.g. SNMP, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs
CO	Setup Managed Devices and Deployment	Configuring and managing Managed Devices configurations (e.g., Versions, Licenses, etc.) via CLI or WebUI	Confirmation of service via Configuration Logs

CO	Configure Managed Log Collectors	Configuring and managing Managed Log Collectors configurations via CLI or WebUI	Confirmation of service via Configuration Logs
CO, Unauthenticated	Zeroize	Zeroize from CLI	Zeroization Indicator
CO, User, Unauthenticated	Self-Test	Run self-test via CLI or WebUI	Output results via System Logs
CO, User	Show Status	Show status via CLI or WebUI	FIPS-CC Mode Indicator
CO, User	System Audit	View system audit records via CLI or WebUI	Audit records via System Logs
CO, User	Monitor System Status and Logs	View system status records via CLI or WebUI	System status via System Logs
CO	Panorama Log Collector Setup	Configuring and managing Log Collectors configurations via CLI or WebUI	Confirmation of service via Configuration Logs.

Assumption of Roles

The module supports distinct operator roles. The cryptographic module in Panorama or Management-Only mode enforces the separation of roles using unique authentication credentials associated with operator accounts. The Log Collector mode only supports one role, the Crypto-Officer (CO) role.

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

Table 9 - Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	Memorized Secret (Unique Username/password) and/or Single-Factor Cryptographic Software (certificate common name / public key-based authentication)	Password-based Minimum length is eight[1] (8) characters (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 module'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.
User	Memorized Secret (Unique Username/password) and/or	

[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.

	Single-Factor Cryptographic Software (certificate common name / public key-based authentication)	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 $10/(2^{112})$, which is less than 1/100,000. The module supports at most 10 failed attempts and locks out afterwards.

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:

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

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

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

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

Z = Zeroise: The module zeroises the SSP.

Note: Unless otherwise specified, all services are available in all system modes. If there is a service that is specific to a certain system mode, it is noted in the Description column.

Table 10 – 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
Access web portal	Connect to module's web portal to invoke services. (Panorama or Management-Only Mode)	RSA SigVer (186-4)		CA Certificates	CO, User	G/R/E/W	System Logs
		RSA SigVer (186-4)		RSA Public Keys		G/R/E/W	
		ECDSA SigVer (186-4)		ECDSA Public Keys		G/R/E/W	
		KAS	KDF TLS (CVL), MD5 (No security claimed)	TLS Pre-Master Secret		G/E/Z	
				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 Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	
				DRBG V			
				DRBG Key			
				Entropy Input String			
Access CLI	Connect to module's CLI via SSH	KTS	HMAC-SHA-1 HMAC-SHA2-256	SSH Session Authentication Keys	CO, User	G/E/Z	System Logs

			HMAC-SHA2-512				
			AES-CBC AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM			G/E/Z	
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
		KAS	KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation Safe Primes Key Verification	SSH DHE/ECDHE Public Components		G/E/R/W/Z	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Management-only, and Logger modes. (Panorama or Management-Only Mode)	N/A		N/A	CO	N/A	System and Configuration logs
Panorama Software Update	Download and install software updates	RSA SigVer (FIPS 186-4)		Public Key for Software Content Load Test	CO	W/E	System and Configuration logs
Panorama Manager Setup	Presents configuration options for management interfaces and communication for peer services (e.g., SNMP, RADIUS). Import, Export, Save, Load, revert and validate Panorama configurations and state role (Panorama or Management-Only Mode)	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys	CO	G/W/E	System and Configuration logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)		ECDSA Private Keys		G/W/E	
		RSA SigVer (FIPS 186-4)		RSA Public Keys		G/R/E/W	
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Keys		G/R/E/W	
		KDF SNMP (CVL)		SNMPv3 Authentication Secret		W/E	
				SNMPv3 Privacy Secret		W/E	
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		Authentication Key		G/E/Z	
		AES-CFB128		Session Key		G/E/Z	
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		CA Certificates		G/R/E/W	
		KAS	KDF TLS (CVL), MD5 (No security claimed)	TLS Pre-Master Secret		G/E/Z	
				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 Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	

		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys		G/E/Z	
			AES-CBC, AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM				
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
			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		Protocol Secrets	CO	W/E	
		Counter DRBG, ESV		DRBG Seed	CO	G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Manage Panorama Administrative Access	Define access control methods via admin profiles, configure administrators and password profiles Configure local user database, authentication profiles, sequence of methods and access domains	N/A		CO, User Password	CO	G/E/W	System and Configuration logs
		RSA SigVer (FIPS 186-4)		SSH Client Public Key		W/E	
		RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4)		SSH Host Public Key		G/R/E/W	
Configure High Availability	Configure High Availability communication settings (Panorama or Management-Only Mode)	RSA SigVer (FIPS 186-4)		RSA Public Key	CO	G/R/E/W	Configuration Logs
		ECDSA SigVer (FIPS 186-4)		ECDSA Public Key		G/R/E/W	
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status.	ECDSA SigGen (FIPS 186-4) RSA SigGen (FIPS 186-4)		RSA Private Keys ECDSA Private Keys	CO	G/R/W/E	Configuration Logs
		ECDSA SigVer (FIPS 186-4) RSA SigVer (FIPS 186-4)		RSA Public Keys ECDSA Public Keys		G/R/W/E	Configuration Logs
		Counter DRBG, ESV		DRBG Seed		G/E	System Logs
				DRBG V			
				DRBG Key			
				Entropy Input String			
Panorama Log Setting	Configure log forwarding (Panorama or Management-Only Mode)	N/A		N/A	CO	N/A	Configuration Logs
Panorama Server Profiles	Configure communication parameters and information for peer servers (Panorama or Management-Only Mode)	KDF SNMP (CVL)		SNMPv3 Authentication Secret	CO	W/E	System Logs
				SNMPv3 Privacy Secret		W/E	
		HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512		Authentication Key		G/E/Z	
		AES-CFB128		Session Key		G/E/Z	
Setup Managed Devices and Deployment	Set-up and define managed devices, device groups for firewalls	N/A		N/A	CO	N/A	Configuration Logs

	Configure device deployment applications and licenses View current deployment information on the managed firewalls. It also allows you to manage software/firmware versions and schedule updates on the managed firewalls and managed log collectors. (Panorama or Management-Only Mode)					
Configure Managed Log Collectors	Setup and manage other Log Collector management, communication and storage settings View current deployment information on the managed Log Collectors. It also allows you to manage software/firmware versions and schedule updates on managed log collectors. (Panorama or Management-Only Mode)	N/A	CO, User Password	CO	G/E/W	System and Configuration logs
Zeroize	Overwrite all CSPs	N/A	All keys and SSPs	CO, Unauthenticated	Z	Zeroization Indicator
Self-Test	Run power up self-tests on demand by power cycling the module.	N/A	Software Integrity Verification Key	CO, User, Unauthenticated	E	System Logs
Show Status	View status of the module	N/A	N/A	CO, User	N/A	FIPS-CC Mode Indicator
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens. CO Only: Provides configuration commit capability. (Panorama or Management-Only Mode)	N/A	N/A	CO, User	N/A	System Logs
Monitor System Status and Logs	Review system status via the panorama system CLI, dashboard and logs; show status. (Panorama or Management-Only Mode)	N/A	N/A	CO, User	N/A	System Logs
Panorama Log Collector Setup	Presents configuration options for management interfaces and communication for peer services Import, Export, Save, Load, revert and validate Panorama configurations and state (Log Collector mode)	CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4)	RSA Private Keys	CO	G/W/E	System and Configuration logs
		CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen (FIPS 186-4)	ECDSA Private Keys		G/W/E	
		RSA SigVer (FIPS 186-4)	RSA Public Keys		G/R/E/W	
		ECDSA SigVer (FIPS 186-4)	ECDSA Public Keys		G/R/E/W	
		KAS KDF TLS (CVL),	TLS Pre-Master Secret		G/E/Z	

			MD5 (No security claimed)	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 Private Components		G/E/Z	
				TLS DHE/ECDHE Public Components		G/E/R/W/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	TLS HMAC Keys		G/E/Z	
			AES-CBC	TLS Encryption Keys		G/E/Z	
		KTS	AES-GCM	TLS Encryption Keys		G/E/Z	
		KTS	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512	SSH Session Authentication Keys		G/E/Z	
			AES-CBC, AES-CTR	SSH Session Encryption Keys		G/E/Z	
		KTS	AES-GCM				
		KAS	KDF SSH (CVL)	SSH DHE/ECDHE Private Components		G/E/Z	
			KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification				
		Counter DRBG, ESV		DRBG Seed		G/E	
				DRBG V			
				DRBG Key			
				Entropy Input String			

Note: Configuration/System Logs for Approved services above will indicate FIPS-CC mode is enabled and that the service succeeded.

5. Software/Firmware Security

The module performs the Software Integrity test by using HMAC-SHA-256 (HMAC Cert. #A2244) during the Pre-Operational Self-Test. In addition, the module also conducts a software load test by using RSA 2048 with SHA-256 (Cert. #A2244) for the new validated software to be uploaded into the module via the Panorama Software Update service. The Software Integrity Verification key and Public key for Software Content Load Test used for the Software Integrity and Software Load test, respectively, are generated externally and delivered as part of the module software image.

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.

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

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

8. Non-Invasive Security

There are currently no defined Approved non-invasive attack mitigation test metrics in SP 800-140F.

9. Sensitive Security Parameters Management

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

"TLS or SSH Session Key Encrypted" corresponds to the following KTS entries listed in the Approved Algorithms table:

- AES Cert. #A2244, HMAC Cert. #A2244
- AES-GCM Cert. #A2244

"SSH, KAS SP 800-56A Rev. 3" corresponds to the following KAS entries listed in the Approved Algorithms table:

- KAS-ECC-SSC Cert. #A2244, KDF SSH Cert. #A2244
- KAS-FFC-SSC Cert. #A2244, KDF SSH Cert. #A2244

"TLS, KAS SP 800-56A Rev. 3" corresponds to the following KAS entries listed in the Approved Algorithms table:

- KAS-ECC-SSC Cert. #A2244, KDF TLS Cert. #A2244
- KAS-FFC-SSC Cert. #A2244, KDF TLS Cert. #A2244

Table 11 – SSPs

Key/SSP/Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization[1]	Use & Related Keys
CA Certificates	112 - 256 bits	RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2244	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 - 150 bits	RSA SigVer (FIPS 186-4) Cert. #A2244	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 - 150 bits	RSA SigGen (FIPS 186-4) Cert. #A2244	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 - 256 bits	ECDSA SigVer (FIPS 186-4) Cert. #A2244	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 - 256 bits	ECDSA SigGen (FIPS 186-4) Cert. #A2244	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 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2244	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC Ephemeral values used in key agreement (KAS-FFC MODP-2048, KAS-ECC P-256, P-384, P-521)
TLS DHE/ECDHE Public Components	112 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2244	DRBG, SP 800-56A Rev. 3	Plaintext - TLS handshake	N/A	N/A	Zeroize at session termination	KAS-FFC or KAS-ECC Ephemeral values used in key agreement (KAS-FFC MODP-2048, KAS-ECC P-256, P-384, P-521)
TLS Pre-Master Secret	112 bits minimum	KDF TLS (CVL) Cert. #A2244, MD5 (No Security Claimed)	KAS-ECC-SSC or KAS-FFC-SSC, 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	384 bits	KDF TLS (CVL) Cert. #A2244, MD5 (No Security Claimed)	KDF TLS (CVL)	N/A	N/A	RAM – plaintext	Zeroize at session termination	Secret value used to derive the TLS session keys
TLS Encryption Keys	128 or 256 bits	AES-CBC or AES-GCM Cert. #A2244	KDF TLS (CVL)	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	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 Cert. #A2244	KDF TLS (CVL)	N/A	TLS, KAS SP 800-56A Rev. 3	RAM - plaintext	Zeroize at session termination	HMAC keys used in TLS connections (SHA-1, 256, 384) (160, 256, 384 bits)
SSH DHE/ECDHE Private Components	112 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2244	DRBG, SP 800-56A Rev. 3	N/A	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC public component (KAS-FFC MODP-2048, KAS-ECC P-256, KAS-ECC P-384, KAS-ECC P-521)
SSH DHE/ECDHE Public Components	112 - 256 bits	KAS-ECC-SSC KAS-FFC-SSC Cert. #A2244	DRBG, SP 800-56A Rev. 3	Plaintext SSH handshake	N/A	RAM - plaintext	Zeroize at session termination	KAS-FFC or KAS-ECC public component (KAS-FFC Group 14, KAS-ECC P-256, KAS-ECC P-384, KAS-ECC P-521)
SSH Host Public Key	112 - 256 bits	RSA SigVer (FIPS 186-4)	DRBG, FIPS 186-4	N/A	N/A	HDD/RAM – plaintext	Zeroize Service	SSH Host Public Key (RSA 2048, RSA 3072,

		ECDSA SigVer (FIPS 186-4) Cert. #A2244						RSA 4096, ECDSA P-256, P-384, or P-521)
SSH Client Public Key	112 - 150 bits	RSA SigVer (FIPS 186-4) Cert. #A2244	N/A	TLS or SSH Session Key Encrypted	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 - 256 bits	AES-CBC, AES-CTR, or AES-GCM Cert. #A2244	KDF SSH (CVL)	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: CBC or CTR) (128 or 256 bits: GCM)
SSH Session Authentication Keys	160 - 256 bits	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512 Cert. #A2244	KDF SSH (CVL)	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)
Software integrity verification key	128 bits	HMAC-SHA2-256, ECDSA SigVer (FIPS 186-4) Cert. #A2244	Factory preload	Import only, TLS or SSH Session Key Encrypted	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. #A2244	Factory preload	Import only, TLS or SSH Session Key Encrypted	N/A	HDD - plaintext	N/A	Used to authenticate software and content to be installed on the module (RSA 2048 with SHA-256)
CO, User Password	N/A	SHA2-256 Cert. #A2244	External	TLS or SSH Session Key Encrypted	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	External	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Secrets used by RADIUS (8 characters minimum)
Entropy Input String	256 bits	CKG (vendor affirmed), Counter DRBG Cert. #A2244	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. #A2244	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. #A2244	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 Cert. #A2244	Entropy as per SP 800-90B	N/A	N/A	RAM - plaintext	Power cycle	AES 256 CTR DRBG state V used in the generation of a random values
SNMPv3 Authentication Secret	N/A	KDF SNMP (CVL) Cert. #A2244	N/A	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)

SNMPv3 Privacy Secret	N/A	KDF SNMP (CVL) Cert. #A2244	N/A	TLS or SSH Session Key Encrypted	N/A	HDD/RAM – plaintext	Zeroize Service	Used to support SNMPv3 services (Minimum 8 characters)
SNMPv3 Authentication Key	160 - 256 bits	HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 Cert. #A2244	KDF SNMP (CVL)	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	HMAC–SHA-1/224/256 /384/512 Authentication protocol key (160 bits)
SNMPv3 Session Key	128 - 256 bits	AES-CFB128 Cert. #A2244	KDF SNMP (CVL)	N/A	N/A	HDD/RAM - Plaintext	Zeroize Service	Privacy protocol encryption key (AES 128/192/256 CFB128)

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.

The module utilizes the following entropy source, which is internal to the physical perimeter of the host GPC.

Table 12 - Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum number of bits of entropy	Details
Palo Alto Networks DRNG RDSEED Entropy Source	256 bits	ESV Cert. #E129 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy.

10. Self-Tests

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

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*
- AES 128-bit CMAC Known Answer Test*
- 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 *
- 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*
- 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 SP800-90Arev1 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 1.0/1.1 KDF Known Answer Test
- SP 800-135rev1 TLS 1.2 KDF with SHA-256 Known Answer Test
- SP 800-135rev1 SSH KDF with SHA-256 Known Answer Test
- SP 800-135rev1 IKEv2 KDF 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.

**Note: Supported by the module cryptographic implementation, but only utilized for CAST*

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 13 - 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 Panorama_pc-10.1.5 from the support site: https://support.paloaltonetworks.com/Support/Index, and a checksum (SHA-256) is available to ensure the module is correct:

Panorama_pc-10.1.5: 018fd6b322d1d65023751496ac3f9a7c4890fdd523f9d5a9145c752447b492cb

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

1. **request system software check**
2. **request system software download version 10.1.5**
3. **request system software install version 10.1.5**
4. **request restart system**

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

The module design corresponds to the module security rules.

Module Enforced Security Rules

When FIPS-CC mode is enabled, the module runs all the required items noted in Section 10 Self-Tests. 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 shall provide distinct operator roles. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
2. The cryptographic module shall clear previous authentications on power cycle.
3. The module shall support the generation of key material with the approved DRBG. The entropy provided must be greater than or equal to the strength of the key being generated.
4. Data output shall be inhibited during power-up self-tests and error states.
5. Processes performing key generation and zeroization processes shall be logically isolated from the logical data output paths.
6. The module does not output intermediate key generation values.
7. Status information output from the module shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module maintains separation between concurrent operators.
10. The module does not support a maintenance interface or role.

11. The module does not have any external input/output devices used for entry/output of data.
12. The module does not enter or output plaintext CSPs.

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. When FIPS-CC mode is enabled, the operator shall not install plugins.
    a. Checked via CLI using "show plugins installed"
3. When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by TLS protocol.
    a. Checked via CLI using "show deviceconfig" command
4. Once boot-up is complete, the module requires a minimum system uptime of 1 hour shall pass before the module can be used to ensure proper instantiation of the DRBG.
    a. Verify uptime via the following command: "show system info | match uptime"
    b. After this time, the server certificate (i.e. CA Certificate with Public/Private keys) and SSH Host Keys shall be regenerated using the following procedure:
        i. Login via CLI and issue the following commands:
            1. set deviceconfig system ssh profiles mgmt-profiles server-profiles <Name> default-hostkey key-type <RSA/ECDSA> <Key Size>
            2. set deviceconfig system ssh regenerate-hostkeys mgmt key-type <RSA/ECDSA> key-length <Key Size>
            3. set deviceconfig system ssh mgmt server-profile <Name>
            4. commit (Once complete, exit configure state)
            5. set ssh service-restart mgmt
        ii. Login via WebUI and create a new certificate chain
            1. Create new certificates via Device > Certificate Management > Certificates
            2. Navigate to Device > Setup > Management > General Settings > Click the gear icon
                a. Select "SSL/TLS Service Profile" and create a new profile with the certificates generated in previous step
                b. Click OK and commit the configuration

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 or TLS protected communication. Any attempt to intervene in the key to entity relationship would require defeating the module TLS or SSH encryption and authentication/integrity mechanism.

12. Mitigation of Other Attacks

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

13. References

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

[AGD] Panorama Administrator's Guide Version 10.1:
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/panorama/10-1/panorama-admin/panorama-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