Panorama Virtual Appliance 8.1

FIPS 140-2 Non-Proprietary Security Policy

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Revision Date: 7/18/2019

Change Record

Table 1 - Change Record

Date	Author	Description of Change
09/25/2018	Quang Trinh	Initial Authoring
10/22/2018	Quang Trinh	Add the CAVP algorithm certificates
11/16/2018	Quang Trinh	Update based on operational testing
4/17/2019	Quang Trinh	Update based on CMVP comments
5/30/2019	Quang Trinh	Update based on CMVP comments
6/24/2019	Quang Trinh	Update based on CMVP comments
7/18/2019	Quang Trinh	Update based on CMVP comments

Contents

Tables

1 Module Overview

The Panorama Virtual Appliance 8.1 module (also known as Panorama VM) is available in the following models:

Table 2 - Release Versions

Operational Environment	Panorama VM Release Version
VMware ESXi 5.5	8.1.6
Hyper-V	8.1.6
KVM	8.1.6
AWS*	8.1.6
Azure*	8.1.6
Google Cloud*	8.1.6

*Note: These operational environments are Vendor Affirmed. See Section 8 in this Security Policy for operator porting rules.

The Panorama VM is a multi-chip standalone software cryptographic module that runs on an underlying General Purpose Computer (GPC) environment. The figure below demonstrates the module's logical cryptographic boundary, and the physical cryptographic boundary as per the GPC's physical enclosure.

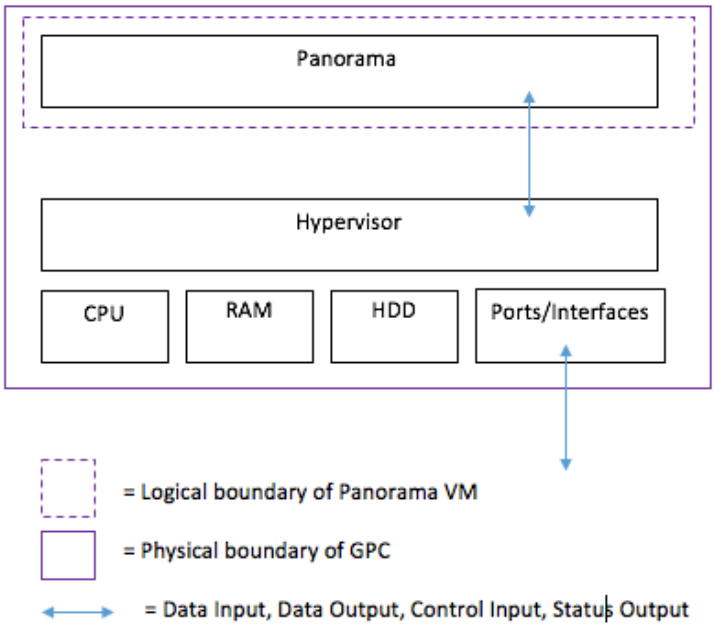

Figure 1 – Cryptographic Boundary

2 Mode of Operation

2.1 FIPS 140-2 Approved Mode of Operation

The module provides both FIPS 140-2 Approved and non-Approved modes of operation.

The following procedure will configure the Approved mode of operation:

- During initial boot up, break the boot sequence via the console port connection (by entering 'maint' when instructed to do so) to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter the Approved mode.
- Select "Enable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into the Approved mode.
- The module will reboot.
- In the Approved mode, the console port is available only as a status output port.

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.

2.2 Selecting Approved modes of operation

The Panorama VM supports multiple configurations that provide varying services. The Cryptographic Officer can initialize the module into different Approved modes of operation. The module supports the following Approved modes of operation:

- 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

2.3 Security Levels for Panorama and Management-Only Mode

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 3 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	N/A

Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Note: When initialized in Panorama or Management-Only mode, the module supports Level 3, identity based authentication.	

2.4 Security Level for Panorama Log Collector Mode

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 4 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
When initialized in Panorama Log Collector mode, the module supports Level 2 role based authentication.	

2.5 Non-Approved Mode of Operation

The following procedure will put the modules into the non-Approved mode of operation:

- During initial boot up, break the boot sequence via the console port connection (by entering 'maint' when instructed to do so) to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter the Approved mode.
- Select "Disable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into the Approved mode.
- The module will reboot.

2.6 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 5 - FIPS Approved Algorithms Used in Module

FIPS Approved Algorithm	CAVP Cert. #
AES [FIPS 197, SP800-38A]: - ECB, CBC, CTR modes; Encrypt/Decrypt; 128, 192 and 256 bits - CFB128 mode; Encrypt/Decrypt: 128 bits Note: AES-OFB, AES-CFB1, AES-CFB8, and AES-CFB128 (192, 256 bits) were also tested but are not available for use	5902
AES-CCM [SP800-38C]: Encrypt and Decrypt, 128-bit Note: AES-CCM was tested but is not used by the module except for the self-test.	5902
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128 and 256-bit Note 1: GCM IV handling is compliant with FIPS IG A.5 and SP800-38D.** Note 2: GCM 192-bit was tested but is not used by the module.	5902
CKG [SP800-133]: Function: Key Generation Method 1: Asymmetric Key Generation; SP800-133 §6, seed results from an unmodified DRBG output Method 2: Symmetric Key Generation; SP800-133 §7.1 (symmetric key results from an unmodified DRBG output), §7.2, and §7.3	Vendor Affirmed
CVL: ECDSA Signature Generation • P-256 SHA: SHA-224, SHA-256, SHA-384, SHA-512 • P-384 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Note: P-521 was tested, but not used by the module	2129
CVL: Elliptical Curve Diffie-Hellman Exchange [SP800-56A] -ECC CDH Primitive (Section 5.7.1.2) - P-256, P-384, P-521 -KAS-ECC all except KDF	2128
CVL: Diffie-Hellman Exchange [SP800-56A]	2128

FIPS Approved Algorithm	CAVP Cert. #
KAS-FFC all except KDF - Parameter sets: FB and FC	
CVL: KDF, Application Specific [SP800-135] -TLSv1.0/1.1/1.2 KDF -SNMPv3 KDF -SSHv2 KDF Note: IKE v1/v2 KDF were tested but are not used by the module.	2130
CVL: RSA [SP800-56B] -RSADP	2131
DRBG [SP800-90A] -CTR DRBG with AES-256 Derivation function enabled	2464
DSA [FIPS 186-4] -Key Generation: 2048 bits -Prerequisite to CVL #2128	1497
ECDSA [FIPS 186-4] - Key Pair Generation P-256, P-384 and P-521 - PKV P-256, P-384, and P-521 - Signature Generation P-256, P-384 and P-521; with all SHA-2 sizes* - Signature Verification P-256, P-384 and P-521; with SHA-1 and all SHA-2 sizes* Note: P-224 was tested, but not used by the module *Does not include the "short SHA-512" sizes SHA-512/224 or SHA-512/256	1575
HMAC [FIPS 198] - HMAC-SHA-1 with λ=96, 160 - HMAC-SHA-256 with λ=256 - HMAC-SHA-384 with λ=384 - HMAC-SHA-512 with λ=512	3882
SP 800-56A Rev.2 Elliptic Curve Diffie-Hellman Exchange (CVL Certs. #2128 and #2130, vendor affirmed; key agreement; key establishment methodology provides 128 bits, 192 bits or 256 bits of encryption strength); (Scenario 1 of IG D.8)	Vendor Affirmed IG D.1-rev2
SP 800-56A Rev.2 Diffie-Hellman Exchange (CVL Certs. #2128 and #2130, vendor affirmed; key agreement; key establishment methodology provides 112 bits or 128 bits of encryption strength); (Scenario 1 of IG D.8)	Vendor Affirmed IG D.1-rev2

FIPS Approved Algorithm	CAVP Cert. #
KTS [SP800-38F §3.1]: AES-CBC (128/192/256 bits) plus HMAC AES-CTR (128/192/256 bit) plus HMAC (Key wrapping; key establishment methodology provides between 128 bits and 256 bits of encryption strength)	AES 5902 HMAC 3882
KTS [SP800-38F §3.1]: AES-GCM (128 or 256 bits) (Key wrapping; key establishment methodology provides 128 bits or 256 bits of encryption strength)	AES 5902
RSA [FIPS 186-4] - Key Pair Generation: 2048 and 3072 bits - Signature Generation (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 2048, 3072, and 4096-bit with hashes (SHA-1^{+}/256/384/512) - Signature Verification (ANSI X9.31, RSASSA-PKCS1_v1-5, RSASSA-PSS): 1024^{++}, 2048, 3072, 4096-bit (per IG A.14) with hashes (SHA-1/224^{+++}/256/384/512) $^{+}$: Only used for signature generation in SSH in the Approved Mode $^{++}$: This size is not supported for RSASSA-PKCS1_v1-5 $^{+++}$: This Hash algorithm is not supported for ANSI X9.31	3090
SHA-1 and SHA-2 [FIPS 180-4]: - Hashes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 - Usage: Digital Signature Generation & Verification, Non-Digital Signature Applications (e.g., component of HMAC)	4658

** The module is compliant to IG A.5: GCM is used in the context of TLS and SSH:

- For TLS, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. (From this RFC, the GCM cipher suites in use are TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, 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.) During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
- For SSH, the module meets Option 4 of IG A.5. The fixed field is 32 bits in length and is derived using the SSH KDF; the fixed field is generated during the SSH session establishment and 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. (It would take hundreds of years for this to occur.)

In all of 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 cryptographic module supports the following non-FIPS Approved algorithms that are allowed for use in FIPS-CC mode.

Table 6 - FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
Diffie-Hellman, non-compliant to SP800-56A [safe primes: L=2048, N=2047] (key agreement; key establishment methodology provides 112 bits of encryption strength); the Diffie-Hellman key generation is not tested; (Scenario 4 of IG D.8)
CMAC - A self-test is performed for this algorithm, but it is not used by the module.
RSA wrap and unwrap, non-compliant to SP800-56B RSA (CVL Cert. #2131, key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
MD5 (within TLS)
Non-Approved NDRNG (seeding source) This provides a minimum of 128 bits of entropy depending on the operational environment.

Table 7 - Supported Protocols in FIPS Approved Mode

Supported Protocols*
TLS v1.0[1], v1.1 and 1.2
SSHv2
SNMPv3

**Note: these protocols were not reviewed or tested by the CMVP or CAVP.*

2.7 Non-Approved, Non-Allowed Algorithms in Non-Approved Mode

The cryptographic module supports the following non-Approved algorithms. No security claim is made in the current module for any of the following non-Approved algorithms.

Table 8 - Non-Approved, Non-Allowed Algorithms Used in Current Module

Non-FIPS Allowed Algorithms in Non-Approved Mode
Digital Signatures (non-Approved strengths, non-compliant):

[1] See vendor imposed security rule #4 in section 8

Non-FIPS Allowed Algorithms in Non-Approved Mode
RSA Key Generation: 512, 1024, 4096 RSA signature generation: Modulus bit length less than 2048 or greater than 4096 bits; up to 16384 bits RSA signature verification: Modulus bit length less than 1024 or greater than 4096 bits; up to 16384 bits ECDSA: B, K, P curves not equal to P-256, P-384 or P-521 DSA: 768 to 4096 bits
Encrypt/Decrypt: Camellia, SEED, Triple-DES (non-compliant), Blowfish, CAST, RC4, DES
Hashing: RIPEMD, MD5
Software Integrity Check: HMAC-SHA-256
Key Exchange (non-Approved strengths): Elliptic Curve Diffie-Hellman: B, K, P curves not equal to P-256, P-384 or P-521 Diffie-Hellman: 768, 1024 and 1536 bit modulus RSA: Less than 2048 bit modulus
Message Authentication: UMAC, HMAC-MD5, HMAC-RIPEMD

3 Ports and Interfaces

The Panorama VM is designed to operate on a general-purpose computer (GPC) platform. The module supports the following FIPS 140-2 interfaces, which have physical and logical ports consistent with a GPC operating environment.

Table 9 – Panorama VM FIPS 140-2 Ports and Interfaces

Type	GPC Peripheral Ports and Network Interfaces	FIPS 140-2 Designation
Power	Power	Power
Console	Ethernet, GPC I/O	Status Output
Management/Ethernet	Ethernet	Data input, control input, data output, status output

4 Identification and Authentication Policy

4.1 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 role.

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

Table 10 – Panorama Mode - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for Panorama services. The CO has the ability to create other CO and User accounts that have limited service access.	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.
User	This User role has read-only access defined for a set of configuration and status information	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.

Table 11 – Management-only Mode - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for Management-Only services. The CO has the ability to create other CO and User accounts that have limited service access.	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.

User	This User role has read-only access defined for a set of configuration and status information	Identity-based operator authentication	Username and password and/or certificate/public key based authentication.

Table 12 - Log Collector Mode- Role and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Crypto-Officer (CO)	This role has administrative capabilities for Log Collector services.	Role-based operator authentication	Username and Password and/or public key based authentication.

Table 13 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The minimum password length is six (6) characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is $1/(95^6)$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is $10/(95^6)$, which is less than 1/100,000. The Panorama's configuration supports at most ten attempts to authenticate in a one-minute period.
Certificate/public key based authentication	The security modules support certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, ECDSA P-384, or ECDSA 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 $3,600,000/(2^{112})$, which is less than 1/100,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period.

5 Security Parameters

Table 14 - Private Keys and CSPs

Key/CSP	Description
ECDSA Private Keys	Supports establishment of TLS session keys, user private keys and certificate signing keys (ECDSA P-256, P-384, P-521)
RSA Private Keys	Supports establishment of TLS session keys, SSH host authentication, user private keys and certificate signing keys (RSA 2048, 3072 or 4096 bits)
TLS DHE private Components	Diffie-Hellman private component used in TLS connections (DH Group 14, L = 2048, N >=224)
TLS ECDHE Private Components	EC Diffie-Hellman private component used in TLS connections (ECDHE P-256, P-384, P-521)
TLS Pre-master Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces

Key/CSP	Description
TLS Master Secret	Secret value used to derive the TLS session keys
TLS Encryption Keys	AES session keys used in TLS connections (128 or 256 bits; CBC or GCM)
TLS HMAC Keys	HMAC-SHA-1/256/384 session keys used in TLS connections
SSH DH Private Components	Diffie-Hellman private component (DH Group 14)
SSH ECDH Private Components	ECDH private component (P-256, P-384, P-521)
SSH Session Encryption Key	AES session key used in SSH connections (128, 192, 256 bits: CBC or CTR) (128 or 256 bits: GCM)
SSH Session Authentication Key	Session key used in SSH connections (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512)
Operator Passwords	Password for operator authentication
DRBG seed and state	DRBG seed coming from the NDRNG and AES 256 CTR DRBG state used in the generation of random values
SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
SNMPv3 Keys	AES CFB Privacy key and HMAC- SHA-1 Authentication keys
RADIUS Secret	Authentication key for RADIUS server (must be minimum of 6 characters)
Note: All CSP and keys defined may be accessed by the Panorama, Log-Collector, and Management-Only modes. For details regarding what CSPs are supported in each mode, please see Tables 17 – 18 below. The CSPs and keys may be shared between the Approved modes of operation.	

Table 15 - Public Keys

Key Name	Description
CA Certificates	RSA and/or ECDSA keys used to extend trust for certificates.
RSA Public Keys / Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096 bits)
ECDSA Public Keys / Certificates	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication (ECDSA P-256, P-384, P-521)
Client Authentication Public Key	Used to authenticate the end user (ECDSA P-256, P-384, P-521; RSA 2048, 3072, 4096 bits)
TLS DHE Public Components	Used in key agreement (DH Group 14)
TLS ECDHE Public Components	Used in key agreement (ECDHE P-256 , P-384, P-521)
SSH DH Public Components	Used in key agreement (DH Group 14)
SSH ECDH Public Components	Used in key agreement (P-256, P-384, P-521)
SSH Host RSA Public Key	Used in SSH public key authentication process (RSA 2048, 3072, or 4096 bits)
SSH Host ECDSA Public Key	Used in SSH public key authentication process (ECDSA P-256, P-384, or P-521)
SSH Client RSA Public Key	Used in SSH public key authentication process (RSA 2048, 3072, or 4096 bits)
Software Authentication Key	RSA key used to authenticate software (2048 bits)
Software Integrity Check Key	Used to check the integrity of crypto-related code (HMAC-SHA-256* and ECDSA P-256) *Keys used to perform power-up self-tests are not CSPs as per IG 7.4
Note: All keys defined may be accessed by the Panorama, Management-Only and Log-Collector modes. For details regarding what CSPs are supported in each mode, please see Tables 17 – 18 below. The keys may be shared between the Approved modes of operation.	

6 Access Control Policy

6.1 Roles and Services

The Approved and non-Approved modes of operation provide identical services. While in the Approved mode of operation all authenticated services and CSPs are accessed via authenticated SSH or TLS sessions. SNMPv3 authentication is supported but is not a method of module administration and does not allow read/write access of CSPs. Approved and allowed algorithms, relevant CSP and public keys related to these protocols are used to access the following services. CSP access by services is further described in the following tables. Additional service information and administrator guidance for Panorama can be found at https://www.paloaltonetworks.com/documentation.html

The Crypto-Officer may access all services, and through the "management of administrative access" service may define multiple Crypto-Officer roles with limited services. The User role provides read-only access to the System Audit service. When configured in Panorama or Management-Only mode, the module provides services via web-browser based interface and a command line interface (CLI). For the Panorama Log Collector mode, only the CLI is available for management.

The services listed below are also available in the non-Approved mode. In the non-Approved mode, non-Approved algorithms and non-Approved algorithm strengths are used to access these services.

Table 16 - Authenticated Services – Panorama VM Panorama or Management-Only

Service	Description	CSP Access
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama mode and Log Collector mode.	N/A
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens. Provides no configuration commit capability.	N/A
Panorama Software Update	Download and install software updates	Signature verification with RSA public key
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	Import or Export RSA/ECDSA Private Keys Import SNMPv3 Secrets Creation RADIUS Secret

Service	Description	CSP Access
Manage Panorama Administrative Access	Define access control methods via admin role profiles, configure administrators and password profiles Configure local user database, authentication profiles, sequence of methods and access domains	Import, modify, or delete operator passwords Import, modify, or delete SSH public keys Modify, read, or delete TLS Pre-master Secret, TLS Master Secret and TLS public keys Execute/Read/Write DRBG seed and state
Configure High Availability	Configure High Availability communication settings	N/A
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status.	Import or export RSA /ECDSA private keys Generate RSA/ECDSA private keys Sign RSA/ECDSA private keys Execute/Read/Write DRBG seed and state
Panorama Log Settings	Configure log forwarding	N/A
Panorama Server Profiles	Configure communication parameters and information for peer servers such as Syslog, SNMP trap servers, email servers and authentication servers	Import SNMPv3 Secrets Execute/Read SNMPv3 keys
Setup Managed Devices and Deployment	Set-up and define managed devices, device groups for firewalls Configure device deployment applications and licenses View current deployment information on the managed firewalls. It also allows you to manage software versions and schedule updates on the managed firewalls and managed log collectors.	N/A

Service	Description	CSP Access
Configure Managed Device Templates	Define and manage common base configuration templates for managed firewalls. Template configurations define settings that are required for the management of the firewalls on the network.	Import or export RSA/ECDSA private keys Signature generation with RSA/ECDSA private keys Generate RSA/ECDSA private keys Execute/Read/Write DRBG seed and state
Configure Managed Device Groups	Define and manage common base of policies and data objects for managed firewalls in configured device groups	N/A
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 versions and schedule updates on managed log collectors.	Modify operator passwords
Monitor System Status and Logs	Review system status via the panorama system CLI, dashboard and logs; show status.	N/A
Monitor Network Activity	Review aggregated information across all managed firewalls and show status. The aggregated view provides actionable information on trends in user activity, traffic patterns, and potential threats across your entire network.	N/A
Switch Context	Browses a managed firewall's web based user interface.	N/A

Table 17 - Authenticated Services – Panorama VM Log Collector

Service	Description	CSP Access
Panorama Log Collector Setup	Presents configuration options for management interfaces and communication for peer services	Import or Export RSA/ECDSA Private Keys

Service	Description	CSP Access
	Import, Export, Save, Load, revert and validate Panorama configurations and state	
Panorama Software Update	Download and install software updates.	Signature verification with RSA public key
Manage Panorama Administrative Access	Update Administrator password	Import or modify operator passwords
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status and usage.	Import or export RSA/ECDSA private keys Generate RSA/ECDSA private keys Sign with RSA/ECDSA private keys Execute/Read/Write DRBG seed and state

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 18 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs. The zeroization procedure is invoked when the operator performs a factory reset. The operator must be present to observe the method has completed successfully or in control via a remote management session. During the zeroization procedure, no other services are available. Procedures to perform zeroization: • During initial boot up, break the boot sequence via the console port connection (by entering 'maint' when instructed to do so) to access the main menu. • Select "Continue." • Select the "Factory Reset" option to enter the Approved mode.

	• Select “Factory Reset”. • When prompted, select “Reboot” and the module will re-initialize and continue into the Approved mode. • The module will reboot.
Self-Tests	Run power up self-tests on demand by power cycling the module.
Show Status	View status of the module via hypervisor.

7 Operational Environment

The hypervisor environment provides the isolated operating environment, and is the single operator of the virtual machine. The module was tested on the following modifiable operating environments on a GPC:

1. Vmware ESXi v5.5 running on a Dell PowerEdge R730 with Intel Xeon E5-2640 CPU
2. Vmware ESXi v5.5 running on a PacStar 451 with Intel Xeon E3-1258 CPU
3. KVM on CentOS 7.2 running on a Dell PowerEdge R730 with Intel Xeon E5-2630 CPU
4. Microsoft Hyper-V 2012 R2 running on a Dell PowerEdge R730 with Intel Xeon E5-2640 CPU
5. Amazon Web Services (AWS) instance m4.2xlarge*
6. Microsoft Azure instance standard D8s v3*
7. Google Cloud Platform (GCP) machine type 8 vCPUs, 32 GB*

Note that:

- Operational environments indexed with * are Vendor Affirmed.
- The processors tested and listed above are part of the Intel Multi Core Xeon (or Intel Xeon 64 bits) processor family.

To install, download the Panorama_pc-8.1.6 file from the support site (https://support.paloaltonetworks.com/Support/Index) and ensure the checksum SHA256: fb7efa8a47ea041480456aaf46314e204e30ff5a5c626a7bb0126535268a0619

The software module provides a Panorama Software Update service. The module’s validation to FIPS 140-2 is no longer valid once a non-validated software is loaded.

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 Panorama VM module on any general purpose computer (GPC) or platform using the specified hypervisor and operating system on the validation certificate or other compatible operating and/or hypervisor system and affirm the modules continued FIPS 140-2 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.

Reference: FIPS 140-2 Implementation Guidance G.5

8 Security Rules

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 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 provide identity-based authentication when in the Panorama or Management- Only mode, and role-based authentication when in the Log Collector mode
3. The cryptographic module shall clear previous authentications on power cycle.
4. 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.
5. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests
        1. Cryptographic algorithm tests
            a. AES Encrypt Known Answer Test
            b. AES Decrypt Known Answer Test
            c. AES CMAC Known Answer Test
            d. AES GCM Encrypt Known Answer Test
            e. AES GCM Decrypt Known Answer Test
            f. AES CCM Encrypt Known Answer Test
            g. AES CCM Decrypt Known Answer Test
            h. ECDSA Sign Known Answer Test
            i. ECDSA Verify Known Answer Test
            j. RSA Sign Known Answer Test
            k. RSA Verify Known Answer Test
            l. RSA Encrypt Known Answer Test
            m. RSA Decrypt Known Answer Test
            n. HMAC-SHA-1 Known Answer Test

o. HMAC-SHA-256 Known Answer Test
p. HMAC-SHA-384 Known Answer Test
q. SHA-1 Known Answer Test
r. SHA-256 Known Answer Test
s. SHA-384 Known Answer Test
t. SHA-512 Known Answer Test
u. DRBG Known Answer Test
v. ECDH Known Answer Test
w. DH Known Answer Test
x. SP800-90A Section 11.3 Health Tests

2. Software Integrity Test – HMAC SHA-256 and ECDSA P-256.

B. Conditional Self-Tests
1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG
2. ECDSA Pairwise Consistency Test Sign/Verify
3. RSA Pairwise Consistency Test Sign/Verify and Encrypt/Decrypt
4. Software Load Test – Verify RSA 2048 signature on software at time of load

C. If any conditional test fails, the module will output description of the error.

6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power of the module.
7. Upon re-configuration to/from the Log Collector or Management-Only mode of operation from/to Panorama mode, the cryptographic module shall reboot and perform all power-up self-tests.
8. Power-up self-tests shall not require any operator action.
9. Data output shall be inhibited during power-up self-tests and error states.
10. Processes performing key generation and zeroization processes shall be logically isolated from the logical data output paths.
11. The module does not output intermediate key generation values.
12. Status information output from the module shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
13. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
14. The module maintains separation between concurrent operators.
15. The module does not support a maintenance interface or role.
16. The module does not have any external input/output devices used for entry/output of data.
17. The module does not enter or output plaintext CSPs.

Vendor imposed security rules:

1. When configured, the module automatically logs out the operator when the cryptographic module remains inactive in any valid role for the administrator specified time interval.
2. When configured, the module enforces a timed access protection mechanism that supports at most ten authentication attempts per minute. After the administrator specified number of

consecutive unsuccessful password validation attempts has occurred, the cryptographic module shall enforce a wait period of at least one (1) minute before any more login attempts can be attempted. This wait period shall be enforced even if the module power is momentarily removed.

3. When FIPS-CC mode is enabled, the operator shall not install plugins. If a plugin is installed, the module shall be configured in a non-Approved mode of operation.
4. When FIPS-CC mode is enabled, TLSv1.0 is disabled. The operator should not re-enable TLSv1.0. TLSv1.0 can be used in an Approved mode of operation (Approved TLS KDF algorithm); however, TLSv1.0 protocol is no longer considered as secure in regards to Cipher Block Chaining IV attacks.
5. When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by a TLS protocol. If TACAS+ or RADIUS without a TLS protocol are set, the module shall be configured in a non-Approved mode of operation.
6. The operator shall not generate 4096-bit RSA key in FIPS-CC mode. If the operator wants to generate 4096-bit RSA key, the module shall be configured in a non-Approved mode of operation.

9 Physical Security Policy

The module is a software only module; FIPS 140-2 physical security requirements are not applicable.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside of the scope of FIPS 140-2, so these requirements are not applicable.

11 References

[FIPS 140-2] FIPS Publication 140-2 Security Requirements for Cryptographic Modules

12 Definitions and Acronyms

AES – Advanced Encryption Standard

CA – Certificate Authority

CLI – Command Line Interface

CO – Cryptographic Officer

DB9 – D-sub series, E size, 9 pins.

DH – Diffie-Hellman

DRBG – Deterministic Random Bit Generator

FIPS – Federal Information Processing Standard

HA – High Availability

HMAC – (Keyed) Hashed Message Authentication Code

LED – Light Emitting Diode

NDRNG – Non-deterministic random number generator

RJ45 – Networking Connector

RSA – Algorithm developed by Rivest, Shamir and Adleman

SHA – Secure Hash Algorithm

TLS – Transport Layer Security

USB – Universal Serial Bus