Palo Alto Networks

Panorama Virtual Appliance 9.0

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.0

Revision Date: September 29, 2020

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

List of Figures

1. Module Overview

The Panorama Virtual Appliance 9.0 module (also known as Panorama VM) is available in the following models:

Table 1 – Release Versions

Operational Environment	Panorama VM Release Version
VMware ESXi 6.5	9.0.9
Microsoft Hyper-V 2012 r2	9.0.9
CentOS 7 - KVM	9.0.9
AWS EC2*	9.0.9
Azure*	9.0.9
Google Cloud Platform*	9.0.9

*Note: These operational environments are Vendor Affirmed[1].

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.

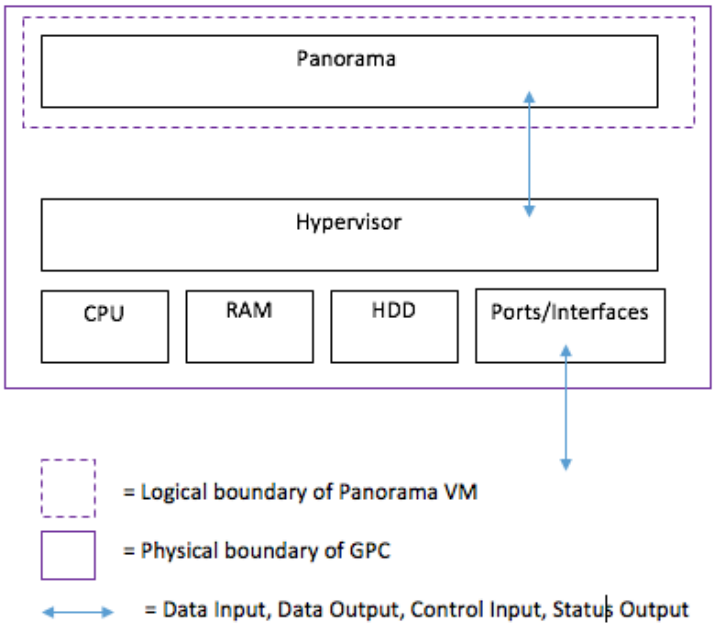

Figure 1 – Cryptographic Boundary

[1] See "Security Rules" section in this Security Policy for operator porting rules.

2. Security Levels

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

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services, 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
When initialized in Panorama or Management-Only mode, the module supports Level 3, identity-based authentication.	

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services, 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 system mode, the module supports Level 2 role-based authentication.	

3. Modes of Operation

The module provides both a FIPS 140-2 Approved (FIPS-CC Mode) and non-Approved (Normal Mode) mode of operation. This module is configured during initialization to operate only in an Approved or non-Approved mode of operation when in the operational state. The module cannot alternate service by service between Approved and non-Approved modes of operation.

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.

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 the FIPS-CC Mode. To change the FIPS-CC Mode back to Normal Mode, follow the instructions below.

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 non-Approved mode.

The module will reboot.

Approved and Allowed Algorithms

The cryptographic module has the following CAVP certificates:

Table 3 - CAVP Certificates for FIPS Approved Algorithms

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: Note: AES-OFB (128, 192, 256 bit), AES-CFB1 (128, 192, 256 bit), AES-CFB8 (128, 192, 256 bit) and AES-CFB128 (192, 256 bit) were also tested but are not available for use.	C999
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.	C999
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. Note 3: GMAC was tested but not used by the module.	C999
CKG [SP800-133]: Function: Key Generation Method 1: Asymmetric Key Generation; SP800-133 §6, seed results from an unmodified DRBG output	Vendor Affirmed

Method 2: Symmetric Key Generation; SP800-133 §7.1 (symmetric key results from an unmodified DRBG output), §7.2, and §7.3	
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 • P-521 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Note: Tested, but not used by the module.	C999
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	C999
CVL: Diffie-Hellman Exchange [SP800-56A] KAS-FFC Ephemeral Unified except KDF - Parameter sets: FB and FC	C999
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.	C999
CVL: RSA [SP800-56B] -RSADP Note: Tested but not used.	C999
DRBG [SP800-90A] -CTR DRBG with AES-256 Derivation function enabled is supported. No derivation function enabled is also supported.	C999
DSA [FIPS 186-4] -Key Generation: 2048 bits -Prerequisite to CVL #C999	C999
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-521 was tested, but the module does not generate this keypair. *Does not include the “short SHA-512” sizes SHA-512/224 or SHA-512/256	C999
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	C999
KAS-SSC: SP 800-56A Rev.3 Elliptic Curve Diffie-Hellman Exchange (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	Vendor Affirmed

and Diffie-Hellman Exchange (key agreement; key establishment methodology provides 112 bits of encryption strength)	
KTS [SP800-38F §3.1]: AES-CBC (128/192/256 bits) plus HMAC AES-CTR (128/192/256 bits) plus HMAC (Key wrapping; key establishment methodology provides between 128 bits and 256 bits of encryption strength)	C999
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)	C999
RSA [FIPS 186-4] - Key Pair Generation: 2048 and 3072 - 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 Note: RSA SigGen [FIPS186-2] tested but not used.	C999
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)	C999

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

- For TLS, The GCM implementation meets Scenario 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, 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. (From this RFC 5288, 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 Scenario 4 of IG A.5. 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 keys is established.

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

Table 4 - FIPS Allowed Algorithms Used in the Approved Mode

FIPS Allowed Algorithms
CMAC - A self-test is performed for this algorithm, but it is not used by the module.
RSA wrap, non-compliant to SP800-56B RSA (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 256 bits of entropy.

Table 5 - Supported Protocols in the Approved Mode

Supported Protocols
TLS v1.0[2], v1.1 and 1.2
SSHv2
SNMPv3

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

Non-Approved, Non-Allowed Algorithms

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 6 – Non-Approved, Non-Allowed Algorithms

Non-FIPS Algorithms in Non-Approved Mode
Digital Signatures (non-Approved strengths, non-compliant): RSA Key Generation: 512, 1024, and 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
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

[2] See vendor imposed security rule #4 in the “Security Rules” section.

4. 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 7 – Panorama VM FIPS 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

5. Roles, Services, and Authentication

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 8 – Panorama and Management-Only modes - Roles and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has administrative capabilities for Panorama Manager 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 9 – Log Collector mode - Roles and Authentication

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

Table 10 - Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Username and Password	The minimum password length is six (6) characters[3] (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 $3,600,000/(2^{112})$,

[3] In FIPS-CC Mode, the module checks and enforces the minimum password length of six (6) characters.

	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.

Security Parameters

The module contains the following keys and critical security parameters (CSP):

Table 11 - 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 Ephemeral private component used in TLS connections (DH Group 14, L = 2048, N >=224)
TLS ECDHE Private Components	EC Diffie-Hellman Ephemeral 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
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 (ECDH P-256, ECDH P-384, ECDH 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)
CO, User Passwords	Password for operator authentication
DRBG seed/state/input string	DRBG seed and input string coming from the NDRNG and AES 256 CTR DRBG state used in the generation of a random values

SNMPv3 Authentication Secret	SNMPv3 Authentication Secret
SNMPv3 Privacy Secret	SNMPv3 Privacy Secret
SNMPv3 Authentication Key	HMAC- SHA-1 Authentication key
SNMPv3 Session Key	AES CFB Privacy Encryption key
RADIUS Secret	Authentication key for RADIUS server (must be minimum of 6 characters)
Master Key	AES-256 CBC key used to protect private keys and CSPs
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 10 – 13. The CSPs and keys may be shared between the Approved modes of operation.	

Table 12 - Public Keys

Key Name	Description
CA Certificates	RSA and/or ECDSA keys used to extend trust for certificates.
RSA Public Keys	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096 bits)
ECDSA Public Keys	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, 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 10 – 13. The keys may be shared between the Approved modes of operation.	

Access Control Policy

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 13 - Authenticated Services – Panorama or Management-Only Mode

CO Services	Description	CSP/Key Access
System Provisioning	Perform panorama licensing, diagnostics, debug functions, manage Panorama support information and switch between Panorama Management-only, and Logger modes.	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 role	Import or Export RSA/ECDSA Private/Public Keys Import SNMPv3 Authentication and Privacy Secrets Execute/Read SNMPv3 keys Creation RADIUS Secret Execute/Read/Write Master key
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	Import, modify, or delete operator passwords Import, modify, or delete SSH Client RSA public keys

		Modify SSH Host RSA public key and SSH Host ECDSA public key
Configure High Availability	Configure High Availability communication settings	Import or export SSH RSA/ECDSA public keys
Panorama Certificate Management	Manage RSA/ECDSA certificates and private keys, certificate profiles, revocation status, and usage; show status.	Import or export RSA /ECDSA private/public keys Generate RSA/ECDSA private/public keys Sign RSA/ECDSA private keys Execute/Read/Write DRBG seed and state Execute/Read/Write Master key
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 Execute/Read Master key
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
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/public keys Signature generation with RSA/ECDSA private keys Generate RSA/ECDSA private/public keys Execute/Read/Write DRBG seed and state Execute/Read/Write Master key
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	Modify operator passwords

	View current deployment information on the managed Log Collectors. It also allows you to manage software versions and schedule updates on managed log collectors.	
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
System Audit	Allows review of limited configuration and system status via SNMPv3, logs, dashboard, show status, and configuration screens.	N/A
User Services	**Description**	
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
Monitor system status and logs	Review system status via the panorama system CLI, dashboard and logs; show status.	N/A

Table 14 - Authenticated Services – Log Collector Mode

CO Services	Description	CSP/Key Access
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	Import or Export RSA/ECDSA Private/Public Keys Execute/Read Master key
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; show status.	Import or export RSA/ECDSA private/public keys Generate RSA/ECDSA private/public keys Sign with RSA/ECDSA private keys

		Execute/Read/Write DRBG seed and state Execute/Read/Write Master key

Table 15 - 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. • Select "Factory Reset". • When prompted, select "Reboot" and the module will re-initialize and continue. 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.

6. 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 v6.5 running on a Dell PowerEdge R730 with Intel Xeon E5-2640 CPU
2. KVM on CentOS 7 running on a Dell PowerEdge R730 with Intel Xeon E5-2630 CPU
3. Microsoft Hyper-V 2012 R2 running on a Dell PowerEdge R730 with Intel Xeon E5-2640 CPU

Vendor Affirmed

4. Amazon Web Services (AWS) EC2 instance m4.2xlarge*
5. Microsoft Azure instance standard D8s v3*
6. 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-9.0.9 file from the support site (https://support.paloaltonetworks.com/Support/Index) and ensure the checksum SHA256: ab05e6fbf337ea348eca8b151822f370bfdabc8e493c8c5e2906aab096aba64b

Enter the following commands:

1. request system software check
2. request system software install version 9.0.9

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

7. Self-Tests / 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 ECB Encrypt Known Answer Test
            b. AES ECB 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. HMAC-SHA-512 Known Answer Test
            r. SHA-1 Known Answer Test
            s. SHA-256 Known Answer Test
            t. SHA-384 Known Answer Test
            u. SHA-512 Known Answer Test
            v. DRBG Known Answer Test
            w. ECDH Known Answer Test
            x. DH Known Answer Test
            y. 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 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 because of the Cipher Block Chaining IV attack, a client of the module could use a vulnerable implementation.
5. When FIPS-CC mode is enabled, the operator shall not use TACACS+. RADIUS may be used but must be protected by TLS protocol. If TACACS+ or RADIUS without TLS protocol are set, the module shall be configured in 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 non-Approved mode of operation

8. Physical Security

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

9. Mitigation of Other Attacks

The module is not designed to mitigate any specific attacks outside the scope of FIPS 140-2. These requirements are not applicable.

10. References

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

11. 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
NDRNG – Non-Deterministic Random Number Generator
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