Palo Alto Networks, Inc.

PAN-OS 9.0 VM-Series

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.4

Revision Date: June 29, 2022

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

1. Module Overview

The PAN-OS 9.0 VM-Series module is available in multiple capacity options (e.g., VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, and VM-1000-HV; note that these are sets of configuration options rather than actual module variants). All models can be deployed as guest virtual machines on VMware ESXi, Hyper-V 2012 r2 and Linux server that is running the KVM (Kernel-based Virtual Machine) using a common base image distributed in a compatible hypervisor format.

Table 1 - Validated Version Information

Operational Environment	PA-VM Release Software Version
VMware ESXi v6.5	9.0.9-h1
KVM on CentOS 7.5	9.0.9-h1
Microsoft Hyper-V 2012 r2	9.0.9-h1
Amazon AWS*	9.0.9-h1
Microsoft Azure*	9.0.9-h1
Google Cloud*	9.0.9-h1

See the Operational Environment section of this document for this listing of tested configurations of these module files.

The PAN-OS 9.0 VM-Series is a software cryptographic module and requires an underlying general purpose computer (GPC) environment. The module is comprised of a GPC (multi-chip standalone embodiment) and the Logical Cryptographic Module (LCM) boundary. The LCM boundary includes all of the logical software components of the module. The physical cryptographic module (PCM) boundary is defined by the enclosure around the host GPC on which it runs. Figure 1 depicts the logical diagram for the LCM boundary and illustrates the hardware components of a GPC.

*Note: These operational environments are Vendor Affirmed. See the Security Rules section in this Security Policy for operator porting rules.

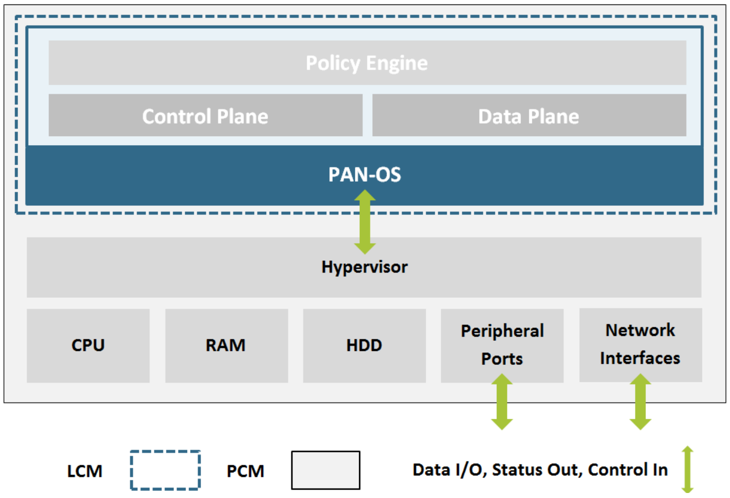

Figure 1 - Cryptographic Boundary

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

3. Modes of Operation

The module provides both a FIPS 140-2 Approved and non-Approved 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 modules support both a FIPS-CC mode and a non-FIPS-CC mode. The following procedure will put the modules into the FIPS-approved mode of operation:

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

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

- Status output interface will indicate "**** FIPS-CC MODE ENABLED ****" via the CLI session.
- Status output interface will indicate "FIPS-CC mode enabled successfully" via the console port.
- The module will display "FIPS-CC" at all times in the status bar at the bottom of the web interface.

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

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

Non-Approved Mode of Operation

The following procedure will put the modules into the FIPS-approved mode of operation:

- Access the module's CLI via SSH, and command the module to enter maintenance mode; the module will reboot
  - o Note: Establish a serial connection to the console port
- After reboot, select "Continue."
- Select the "Set FIPS-CC" option, and press enter.
- Select "Disable FIPS-CC Mode", and press enter.
- The module will disable FIPS-CC mode, and perform a factory reset (zeroization)
- Once complete, the module will provide the following status output:
  - o "Set FIPS-CC Mode Status: Success"

Approved and Allowed Algorithms

The cryptographic modules support the following FIPS Approved algorithms.

Table 3 – FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES [FIPS 197, SP800-38A]: - ECB, CBC, CTR modes; Encrypt/Decrypt; 128, 192 and 256-bit - CFB128 mode; Encrypt/Decrypt; 128-bit 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	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 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 P-521 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Note: P-256, P-384, and P-521 were tested, but not used by the module.	C999
CVL: KDF, Application Specific [SP800-135] - TLSv1.0/1.1/1.2 KDF - SNMPv3 KDF - SSHv2 KDF - IKE v1/v2 KDF	C999
CVL: RSA [SP800-56B] - RSADP Note: Tested but not used.	C999
DRBG [SP800-90A]: CTR DRBG with AES-256, one instantiation per plane Derivation function enabled	C999
DSA [FIPS 186-4] -Key Generation: 2048 bits	C999
ECDSA [FIPS 186-4] - Key Pair Generation P-256, P-384 and P-521 - Public Key Validation P-256, P-384, P-521 - Signature Generation P-256, P-384, and P-521; with all SHA-2 sizes+ - Signature Verification P-224, P-256, P-384, and P-521; with SHA-1 and all SHA-2 sizes+ +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) and Diffie-Hellman Exchange (key agreement; key establishment methodology provides 112 bits of encryption strength)	A2669
KAS (KAS-SSC Cert. #A2699, CVL Cert. #C999): SP 800-56A Rev3 compliant key agreement scheme, where testing was performed separately for the shared secret computation and for a TLS, SSH, and IKE KDF compliant with SP 800-135 Rev1	KAS-SSC Cert. #A2669 CVL Cert. #C999
KTS [SP800-38F §3.1]: AES-CBC (128/192/256 bit) plus HMAC AES-CTR (128/192/256 bit) plus HMAC (Key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES C999 HMAC C999
KTS [SP800-38F §3.1]: AES-GCM (Key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)* * The module is compliant to IG A.5: GCM is used in the context of TLS,	AES C999
FIPS 186-4 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 (per IG A.14) 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; Mod 4096 does not support SHA-1 [++]: This size is not supported for RSASSA-PKCS1_v1-5 [+++]: This Hash algorithm is not supported for ANSI X9.31 Note: FIPS 186-2 SigGen was tested, but not used by the module.	C999
Safe Primes Key Generation and Verification using MODP-2048	A2669
SHS (SHA-1 and SHA-2) [FIPS 180-4]: - Hashes: SHA-1, SHA-256, SHA-384, SHA-512 - Usage: Digital Signature Generation & Verification, Non-Digital Signature Applications (e.g., component of HMAC) (Note: SHA-224 was tested, but not used in the module)	C999

IPsec/IKEv2, SSH, and IPsec/IKEv1:

- 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 IPsec/IKEv2, The GCM implementation meets Scenario 1 of IG A.5: it is used in a manner compliant with RFCs 4106 and 7296 (RFC 5282 is not applicable, as the module does not use GCM within IKEv2 itself), and ensures when the module exhausts all possible values for a given session key that this triggers a rekey condition. During operational testing, the module was tested against an independent version of IPsec with IKEv2 and found to behave correctly.

- For SSH, the module meets Scenario 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.)

- For IPsec/IKEv1, the module meets Scenario 4 of IG A.5. The behavior is the same as the above description for SSH, except the fixed field is derived using the IKEv1 KDF instead of the SSH KDF. 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 all the above cases, the nonce_explicit is always generated deterministically. AES GCM keys are zeroized when the module is power-cycled. For each new TLS or SSH session, a new AES GCM 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
MD5 (within TLS)
NDRNGs (used to seed SP800-90A DRBG): one NDRNG per plane. This provides a minimum of 256 bits of entropy.
RSA wrap, non-compliant to SP800-56B RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

Table 5 - Supported Protocols in the Approved Mode

Supported Protocols*
TLS 1.0**, 1.1, 1.2
SSHv2
SNMPv3
IPsec and IKEv1/2

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

**Note: See vendor imposed rules in Self-Tests/Security Rules section below

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-FIPS Algorithms in Non-Approved Mode

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

4. Ports and Interfaces

The module is a software only module that operates on a general purpose computing (GPC) platform. The physical ports and logical interfaces are consistent with a GPC operating environment. The module supports the following FIPS 140-2 logical interfaces:

Table 7 - Ports and Interfaces

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

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

5. Roles, Services, and Authentication

Assumption of Roles

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

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

Table 8 – Roles and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to all configurations, show status and update services offered by the module. Within the PAN-OS software, this role maps to the "Superuser" administrator role.	Identity-based operator authentication	Username/password and/or public-key/certificate based authentication
User	This role has limited access to services offered by the modules. This role does not have access to modify or view the passwords associated with other administrator accounts The User may not view or alter CSPs of any type stored on the module. The User may change their own password. Within the PAN-OS software, this role maps to the "Superuser (read-only)" administrator role (also referred to as "Superreader").	Identity-based operator authentication	Username/password and/or public-key/certificate based authentication
Remote Access VPN (RA VPN)	Remote user accessing the network via VPN.	Identity-based operator authentication	Username/password and/or certificate based authentication
Site-to-site VPN (S-S VPN)	Remote VPN device establishing a VPN session to facilitate access to the network.	Identity-based operator authentication	IKE/IPSec Pre-shared keys - Identification with the IP Address and authentication with the Pre-Shared Key or certificate based authentication

Table 9 - Strength of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Username and Password	Minimum length is six (6) characters[1] (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 (1) minute is 10/(95^6), which is less than 1/100,000. The firewall's configuration supports at most ten attempts to authenticate in a one-minute period.
Public-Key/Certificate based authentication	The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521. The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 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.
IKE/IPSec pre-shared keys	The pre-shared key authentication method has a minimum security strength of 2^{112}. The probability of successfully authenticating to the module is 1/(2^{112}), which is less than 1/1,000,000. The number of authentication attempts is limited by the number of new connections per second supported (120,000) on the fastest platform of the Palo Alto Networks firewalls. The probability of successfully authenticating to the module within a one minute period is 7,200,000/(2^{112}), which is less than 1/100,000.

Roles and Services

The Approved and non-Approved mode of operation provide identical 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.

The services listed below are also available in the non-Approved mode. In the Non-Approved mode SSH, TLS and VPN processes will use non-Approved Algorithms and Approved algorithms with non-Approved strength.

Table 10 - Authenticated Services

Services	Description
Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts.
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration.
View Other Configuration	Read-only of non-security relevant configuration (see above).

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

Check Status	View status via the web interface, command line interface or VPN session
VPN	Provide network access for remote users or site-to-site connections.
Software Update	Provides a method to update the software on the firewall.

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

Table 11 - Authenticated Service Access

Service	Crypto Officer	User	RA VPN	S-S VPN
Security Configuration Management	Y	Y*	N	N
Other Configuration	Y	N	N	N
View Other Configuration	Y	Y	N	N
Check Status	Y	Y	Y	Y
VPN	N	N	Y	Y
Software Update	Y	N	N	N
*Note: The user role has use of this service only to change their own password.				

Table 12 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs.
Self-Tests	Run power up self-tests on demand by power cycling the module.
Show Status (Hypervisor)	View status of the module via hypervisor.

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

Security Parameters

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

Table 13 - Private Keys and CSPs

CSP #	Key Name	Type	Description
1	RSA Private Keys	RSA	RSA Private key for generation of signatures, authentication and key establishment (RSA 2048, 3072, or 4096 bits)
2	ECDSA Private Keys	ECDSA	ECDSA Private key for generation of signatures and authentication (P-256, P-384 or P-521)
3	TLS Pre-Master Secret	TLS Secret	Secret value used to derive the TLS Master Secret along with client and server random nonces
4	TLS Master Secret	TLS Secret	Secret value used to derive the TLS session keys
5	TLS DHE/ECDHE Private Components	DH, ECDH	Ephemeral Diffie-Hellman ephemeral private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521)
6	TLS HMAC Keys	HMAC	HMAC keys used in TLS connections (SHA-1, 256, 384) (160, 256, 384 bits)
7	TLS Encryption Keys	AES	AES (128 or 256 bit) keys used in TLS connections (GCM; CBC)
8	SSH Session Authentication Keys	HMAC	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)
9	SSH Session Encryption Keys	AES	Used in all SSH connections to the security module's command line interface. (128, 192, and 256 bits: CBC or CTR) (128 or 256 bits: GCM)
10	SSH DH Private Components	DH, ECDH	Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
11	S-S VPN IPSec/IKE Authentication Keys	HMAC	(HMAC-SHA-1, SHA-256, SHA-384 or SHA-512) Used to authenticate the peer in an IKE/IPSec tunnel connection. (160, 256, 384, 512 bits)
12	S-S VPN IPSec/IKE Session Keys	AES	Used to encrypt IKE/IPSec data. These are AES (128, 192, or 256 CBC) IKE keys and (128, 192 or 256 CBC, 128 CCM, 128 or 256 GCM) IPSec keys

13	S-S VPN IPSec/IKE DHE or ECDHE Private Components	DH, ECDH	Diffie Hellman or EC Diffie-Hellman private component used in key establishment (DHE 2048, ECDHE P-256, P-384)
14	S-S VPN IPSec Pre-Shared Keys	Part of HMAC	PSK used in conjunction with HMAC listed above for authentication. Entered into the module by the Crypto Officer once authenticated
15	RA VPN IPSec Session Keys	AES	Used to encrypt remote access sessions utilizing IPSec. (128-CBC, 128/256-GCM)
16	RA VPN IPSec Authentication	HMAC	(HMAC-SHA-1, 160 bits) Used in authentication of remote access IPSec data.
17	CO, User, RA VPN Password	Password	Authentication string with a minimum length of six (6) characters.
18	DRBG seed/state/input string	DRBG	DRBG seed and input string coming from the NDRNG and AES 256 CTR DRBG state (V and Key) used in the generation of a random values
19	SNMPv3 Authentication Secret	SNMPv3 Secrets	SNMPv3 secret used for localization (Minimum 8 characters)
20	SNMPv3 Privacy Secret	SNMPv3 Secrets	SNMPv3 secret used for localization (Minimum 8 characters)
21	Authentication Key	HMAC	HMAC–SHA1 Authentication protocol key (160 bits)
22	Session Key	AES	Privacy protocol encryption key (AES 128 CFB)
23	Protocol Secrets	Password	Secret used by RADIUS or TACACS+ (minimum length of six (6) characters)
24	Master Key	AES-256 CBC	Used to protect private keys and CSPs

Note: Transient CSPs are zeroized by an overwrite with a pseudo random pattern followed by read-verify. Intermediate plaintext key material (CSP) is zeroized when it is copied from one to another memory location. All keys (CSPs) are zeroized when they expire. Session keys (CSPs) are zeroized as soon as the associated session has ended/timed out/ or been closed. Private keys (CSPs) are zeroized when their corresponding public keys (certificates) expire.

Table 14 - Public Keys

	Key Name	Description
A	CA Certificates	ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521)
B	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, or P-521)

C	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)
D	TLS DH/ECDHE Public Components	Diffie-Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-256, P-384 and P-521)
E	SSH DH Public Components	Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521)
F	SSH Host Public Key	SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521) (The matching private key is among the RSA Private Keys or ECDSA Private Keys, in Table 13.)
G	SSH Client Public Key	Public RSA key used to authenticate client (RSA 2048, 3072 or 4096 bits)
H	S-S VPN IPSec/IKE DHE or ECDHE Public Component	Diffie-Hellman or EC Diffie-Hellman public component used in key agreement (DHE 2048, ECDHE P-256, P-384)
I	Public key for software content load test	Used to authenticate software and content to be installed on the firewall (RSA 2048 with SHA-256)
J	Software integrity verification key	Used to check the integrity of crypto-related code. (HMAC-SHA-256 and ECDSA P-256)

Access Control Policy

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:

- **R** = Read: The module reads the CSP. The read access is performed when a CSP is either exported from the module or executed by a security function.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 15 - CSP and Public Key Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
CO	Security Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9,10, 17, 18, 19, 20, 21, 22, 23, 24, A, B, C, D, E, F, G, I
CO	Other Configuration	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F, G
User, CO	View Other Configurations	R	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 18, A, B, C, D, E, F, G (operator's own password)

User	Security Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 17, A, B, C, D, E, F, G (operator's own password)
User, CO	Check Status	R	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F, G
S-S VPN	VPN	R	11, 12, 13, 14, 24, B, C, H
RA VPN	VPN	R	1, 2, 3, 4, 5, 6, 7, 15, 16, 18, 24, A, B, C, D
CO	Software Update	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 17, A, B, C, D, E, F, G
Unauthenticated	Self-Tests	R	J
Unauthenticated	Show Status	N/A	N/A
Unauthenticated	Zeroize	Z	All CSPs are zeroized.

6. Operational Environment

The hypervisor environment provides an isolated operating environment and is the single operator of the virtual machine. The module was tested on the following environments operating on a general-purpose computing platform.

Tested Configurations:

1. Vmware ESXi v6.5 running on a Dell PowerEdge R730 with Intel Xeon E5-2640 CPU
2. KVM on CentOS 7.5 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

The following operating environments are vendor affirmed:

4. Amazon AWS M4.Xlarge EC2 instance*
5. Microsoft Azure Standard D4 v2*
6. Google Cloud n1-standard-4*

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 140-2 requirement that only one (1) entity at a time can use the cryptographic module.

To install[2], download either PanOS_vm-9.0.9-h1 file from the support site (https://support.paloaltonetworks.com/Support/Index) and ensure the checksum (SHA-256) is correct:

- **9.0.9-h1**: 66699898b696b9c78d528c87e132a2d940ac31149847c5a74f61e33fcfce5d2c

On Vmware ESXi,

1. Download the OVA file.
2. Set up the virtual standard switch(es) you need for the VM-Series firewall.
3. Deploy the OVA
   a. Right-click on host and select **Deploy OVF Template**.
   b. Browse to the OVA file you downloaded. Click **Next**.
   c. Name the VM-Series firewall instance. Click **Next**.
   d. Select the ESXi host for the VM-Series firewall. Click **Next**.
   e. Select the datastore to use. Click **Next**.
   f. Select the networks to use for the two initial vNICs.
   g. Review the details, select **Power on after deployment**, and click **Next**.
   h. When the deployment is complete, click the **Summary** tab to review.

On KVM,

1. On the Virt-manager, select **Create a new virtual machine**.

[2] Installation steps are different based on the environment. Please use this Deployment Guide https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment.html

2. Add a descriptive **Name** for the VM-Series firewall.
3. Select **Import existing disk image**, browse to the image, and set the **OS Type**: Linux.
4. Add network adaptors, and configure the **Memory** and **CPU**.
5. Configure the virtual disk settings.
6. Configure the network adapters based on your environment.
7. Click **Begin Installation**.

On Microsoft Hyper-V,

1. Login to Hyper-V Manager and select your VM.
2. Select **Settings > Hardware > Network Adaptor > Hardware Acceleration**.
3. Under Virtual machine queue, uncheck **Enable virtual machine queue**.
4. Click **Apply** save your changes and **OK** to exit the VM settings.
5. Download the VHDX file.
6. Set up any vSwitch(es) that you will need.
7. Install the firewall.
    a. Choose a **Name** and **Location** for the VM-Series firewall.
    b. Choose **Generation 1**.
    c. Choose the Memory.
    d. Configure networking. Select an external vSwitch to connect the management interface of the firewall.
    e. To connect the **Virtual Hard Disk**, select **Use an existing virtual hard disk** and browse to the VHDX file you downloaded earlier.
    f. Review the summary and click **Finish**.
8. Assign virtual CPUs to the firewall.
9. Connect at least one network adaptor for the dataplane interface on the firewall.
10. Power on the firewall.

After the VM-Series firewall has been deployed on the hypervisor, update the software version to 9.0.9-h1 using the following commands (as authorized administrator):

1. **request system software check**
2. **request system software download version 9.0.9-h1**
3. **request system software install version 9.0.9-h1**
4. **request restart system**

Note that Operational environments indexed with * are Vendor Affirmed.

The software module provides a 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 VM-series firewall on any general purpose computer (GPC) or platform using the specified hypervisor and operating system on the validation certificate or other compatible operating and/or hypervisor system and affirm the modules continued FIPS 140-2 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 provides four distinct operator roles. These are the User role, Remote Access VPN role, Site-to-site VPN role, and the Cryptographic Officer role.
2. The cryptographic module provides identity-based authentication.
3. The cryptographic module clears previous authentications on power cycle.
4. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module will automatically log out the operator. The CO will configure the period of inactivity.
5. When 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 have 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.
6. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
7. The module supports the generation of key material with the approved DRBG. The entropy provided must be equal to or greater than the security strength of the key being generated. The approved DRBG requests a minimum of 256 bits of entropy per every 384 bits of seed input.

8. The cryptographic module performs 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. RSA Sign Known Answer Test
            i. RSA Verify Known Answer Test
            j. RSA Encrypt Known Answer Test
            k. RSA Decrypt Known Answer Test
            l. ECDSA Sign Known Answer Test
            m. ECDSA Verify 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 SP800-90A Known Answer Tests
            w. SP 800-90A Section 11.3 Health Tests
            x. DH Known Answer Test
            y. ECDH Known Answer Test Per IG 9.6
    B. Software Integrity Test –verified with HMAC-SHA-256 and ECDSA P-256.
    C. Critical Functions Tests
        1. N/A
    D. Conditional Self-Tests
        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG
        2. RSA Pairwise Consistency Test
        3. ECDSA Pairwise Consistency Test
        4. Software Load Test – Verify RSA 2048 with SHA-256 signature on software at time of load
        5. If any conditional test fails, the module will output description of the error.
2. The operator can command the module to perform the power-up self-test by cycling power of the module.
3. Power-up self-tests do not require any operator action.
4. Data output is inhibited during power-up self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not have any external input/output devices used for entry/output of data.
9. The module does not enter or output plaintext CSPs.

10. The module does not output intermediate key generation values.

Vendor imposed security rules:

1. In FIPS-CC mode, the following rules shall apply:
    a. The operator should not enable TLSv1.0; it is disabled by default.
    Note that 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.
    b. Pre-shared keys used for IKE/IPsec must be at least 14 bytes in length.
    c. If using RADIUS, it must be configured using TLS. In all other cases, the module shall be configured in non-Approved mode of operation.
    d. If using TACACS+, configure the service route via an IPSec tunnel, and ensure the TACACS+ server is configured for a minimum password length of six (6) characters (to match Table 17 of this document), or greater. In all other cases, the module shall be configured in non-Approved mode of operation.
    e. 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

There are no applicable FIPS 140-2 physical security requirements.

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