

PAN-OS 10.2 running on PA-220, PA-220R, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, and PA-7000 Series NGFWs

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.2

Revision Date: August 9, 2024

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <u>https://www.paloaltonetworks.com/company/trademarks.html</u>. All other marks mentioned herein may be trademarks of their respective companies. This document may be freely reproduced and distributed whole and intact including this copyright notice.

| 1. General | 3 |
|--|----|
| 2. Cryptographic Module Specification | 3 |
| 3. Cryptographic Module Interfaces | 21 |
| 4. Roles, Services, and Authentication | 23 |
| 5. Software/Firmware Security | 29 |
| 6. Operational Environment | 29 |
| 7. Physical Security | 29 |
| 8. Non-Invasive Security | 30 |
| 9. Sensitive Security Parameter Management | 30 |
| 10. Self-Tests | 33 |
| 11. Life-Cycle Assurance | 35 |
| 12. Mitigation of Other Attacks | 36 |
| 13. Definitions and Acronyms | 36 |
| 14. Reference Documents | 37 |
| Appendix A - PA-220 - FIPS Accessories/Tamper Seal Installation (6 Seals) | 37 |
| Appendix B - PA-220R- FIPS Accessories/Tamper Seal Installation (5 Seals) | 40 |
| Appendix C - PA-800 series - FIPS Accessories/Tamper Seal Installation (11 Seals) | 40 |
| Appendix D - PA-3200 Series - FIPS Accessories/Tamper Seal Installation (19 Seals) | 43 |
| Appendix E - PA-5200- FIPS Accessories/Tamper Seal Installation (28 Seals) | 45 |
| Appendix F - PA-7050 - FIPS Accessories/Tamper Seal Installation (24 Seals) | 48 |
| Appendix G - PA-7080 - FIPS Accessories/Tamper Seal Installation (10 Seals) | 56 |
| Appendix H - PA-5450 FIPS Accessories/Tamper Seal Installation (12 Seals) | 62 |
| Appendix I - PA-410 FIPS Accessories/Tamper Seal Installation (4 Seals) | 63 |
| Appendix J - PA-440/450/460 FIPS Accessories/Tamper Seal Installation (4 Seals) | 64 |
| Appendix K - PA-3400 Series FIPS Accessories/Tamper Seal Installation (11 Seals) | 65 |
| Appendix L - PA-5400 Series FIPS Accessories/Tamper Seal Installation (11 Seals) | 66 |

1. General

Palo Alto Networks offers a full line of next-generation security appliances. Our platform architecture is based on our single-pass engine, PAN-OS, for networking, security, threat prevention, and management functionality that is consistent across all platforms. The devices differ only in capacities, performance, and physical configuration.

| ISO/IEC 24759 Section 6. [Number Below] | FIPS 140-3 Section Title | Security Level |
|--|---|----------------|
| 1 | General | 2 |
| 2 | Cryptographic Module Specification | 2 |
| 3 | Cryptographic Module Interfaces | 2 |
| 4 | Roles, Services, and Authentication | 3 |
| 5 | Software/Firmware Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Physical Security | 2 |
| 8 | Non-Invasive Security | N/A |
| 9 | Sensitive Security Parameter Management | 2 |
| 10 | Self-Tests | 2 |
| 11 | Life-Cycle Assurance | 3 |
| 12 | Mitigation of Other Attacks | N/A |
| | Overall Security Level | 2 |

The cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-3.

2. Cryptographic Module Specification

Purpose

Palo Alto Networks offers a full line of next-generation security appliances that range from the PA-220, designed for enterprise remote offices, to the PA-7080, which is a modular chassis designed for high-speed datacenters. Our platform architecture is based on our single-pass engine, PAN-OS, for networking, security, threat prevention, and management functionality that is consistent across all platforms. The devices differ only in capacities, performance, and physical configuration.

The Palo Alto Networks PA-220, PA-220R, PA-400 Series, PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, and PA-7000 Series NGFWs (hereafter referred to as the modules) are multi-chip standalone modules that provide network security by enabling enterprises to see and control applications, users, and content – not just ports, IP addresses, and packets – using three unique identification technologies: App-ID, User-ID, and Content-ID. These identification technologies, found in Palo Alto Networks' enterprise firewalls, enable enterprises to create business-relevant security policies – safely enabling organizations to adopt new applications, instead of the traditional "all-or-nothing" approach offered by traditional port-blocking firewalls used in many security infrastructures.

Features and Benefits

- **Application visibility and control:** Accurate identification of the applications traversing the network enables policy-based control over application usage at the firewall, the strategic center of the security infrastructure.
- **Visualization tools:** Graphical visibility tools, customizable reporting and logging enables administrators to make a more informed decision on how to treat the applications traversing the network.

- **Application browser:** Helps administrators quickly research what the application is, its behavioral characteristics and underlying technology resulting in a more informed decision making process on how to treat the application.
- User-based visibility and control: Seamless integration with enterprise directory services (Active Directory, LDAP, eDirectory) facilitates application visibility and policy creation based on user and group information, not just IP address. In Citrix and terminal services environments, the identity of users sitting behind Citrix or terminal services can be used to enable policy-based visibility and control over applications, users and content. An XML API enables integration with other, 3rd party user repositories.
- **Real-time threat prevention:** Detects and blocks application vulnerabilities, viruses, spyware, and worms; controls web activity; all in real-time, dramatically improving performance and accuracy.
- **File and data filtering:** Taking full advantage of the in-depth application inspection being performed by App-ID, administrators can implement several different types of policies that reduce the risk associated with unauthorized file and data transfer.
- Legacy firewall support: Support for traditional inbound and outbound port-based firewall rules mixed with application-based rules smooth the transition to a Palo Alto Networks next generation firewall.
- Networking architecture: Support for dynamic routing (OSPF, RIP, BGP), virtual wire mode and layer 2/layer 3 modes facilitates deployment in nearly any networking environment.
- **Policy-based Forwarding**: Forward traffic based on policy defined by application, source zone/interface, source/destination address, source user/group, and service.
- **Virtual Systems**: Create multiple virtual "firewalls" within a single device as a means of supporting specific departments or customers. Each virtual system can include dedicated administrative accounts, interfaces, networking configuration, security zones, and policies for the associated network traffic.
- VPN connectivity: Secure site-to-site connectivity is enabled through standards-based IPSec VPN support while remote user access is delivered via SSL VPN connectivity.
- Quality of Service (QoS): Deploy traffic shaping policies (guaranteed, maximum and priority) to enable positive policy controls over bandwidth intensive, non-work related applications such as streaming media while preserving the performance of business applications.
- **Real-time bandwidth monitor:** View real-time bandwidth and session consumption for applications and users within a selected QoS class.
- **Purpose-built platform:** combines single pass engine with parallel processing hardware to deliver the multi-Gbps performance necessary to protect today's high-speed networks.

Tested Configurations

The configurations for this validation are highlighted in Table 2.

| Model | Hardware [Part Number and Version] | Firmware Version | Distinguishing Features |
|---------|---------------------------------------|------------------|---|
| PA-220 | 910-000128, Physical Kit: 920-000084 | 10.2.8-h4 | RJ45 Ports, Micro-USB, LEDs, USB, Power Supply |
| PA-220R | 910-000147, Physical Kit: 920-000226 | 10.2.8-h4 | RJ-45 Ports, SFP, USBs, Micro-USB, LEDs, Power Supply |
| PA-410 | 910-000231, Physical Kit: 920-000454 | 10.2.8-h4 | RJ45 interfaces, USB, LED, Power supply, Ground stud |
| PA-440 | 910-000212, Physical Kit: 920-000454 | 10.2.8-h4 | RJ 45 interfaces, USB, LEDs, Micro USB |
| PA-450 | 910-000232, Physical Kit: 920-000454 | 10.2.8-h4 | RJ 45 interfaces, USB, LEDs, Micro USB |
| PA-460 | 910-000230, Physical Kit: 920-000454 | 10.2.8-h4 | RJ 45 interfaces, USB, LEDs, 1 Micro USB |
| PA-820 | 910-000120, Physical Kit: 920-000185 | 10.2.8-h4 | RJ45 Ports, Micro-USB, SFP, SFP/SFP+, Power, LEDs, USB |
| PA-850 | 910-000119, Physical Kit: 920-000185 | 10.2.8-h4 | RJ45 Ports, Micro-USB, SFP, SFP/SFP+, Power, LEDs, USB |

Table 2 - Cryptographic Module Tested Configuration

| PA-3220 | 910-000162, Physical Kit: 920-000212 | 10.2.8-h4 | RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power |
|---------|--------------------------------------|-----------|--|
| PA-3250 | 910-000163, Physical Kit: 920-000212 | 10.2.8-h4 | RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power |
| PA-3260 | 910-000164, Physical Kit: 920-000212 | 10.2.8-h4 | RJ45 ports, SFP/SFP+ ports, QSFP+ ports, HSCI ports, USB ports, Micro-USB, LED, Power |
| PA-3410 | 910-000241, Physical Kit: 920-000333 | 10.2.8-h4 | 1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28 |
| PA-3420 | 910-000242, Physical Kit: 920-000333 | 10.2.8-h4 | 1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28 |
| PA-3430 | 910-000243, Physical Kit: 920-000333 | 10.2.8-h4 | 1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28 |
| PA-3440 | 910-000244, Physical Kit: 920-000333 | 10.2.8-h4 | 1 x 1000Base-T (management) - RJ-45, 1 x 10Gb Ethernet (HA) - SFP+, 1 x console - RJ-45, 1 x management (USB) - micro-USB, 10 x 1Gb Ethernet/10Gb Ethernet - SFP/SFP+, 12 x 1/2.5/5/10GBase-T - RJ-45, 2 x 1000Base-T (HA) - RJ-45, 4 x 25Gb Ethernet - SFP28 |
| PA-5220 | 910-000132, Physical Kit: 920-000186 | 10.2.8-h4 | RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB |
| PA-5250 | 910-000131, Physical Kit: 920-000186 | 10.2.8-h4 | RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB |
| PA-5260 | 910-000125, Physical Kit: 920-000186 | 10.2.8-h4 | RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB |
| PA-5280 | 910-000157, Physical Kit: 920-000186 | 10.2.8-h4 | RJ45 ports, SFP/SFP+, QSFP28 port, QSFP+ ports, HSCI ports, SFTP+ ports, Power supply, LEDs, USB |
| PA-5410 | 910-000252, Physical Kit: 920-000320 | 10.2.8-h4 | 1 x 1000Base-X (management) – |

| | | | SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45 |
|---------------------------------------|---|--------------------------------|--|
| PA-5420 | 910-000253, Physical Kit: 920-000320 | 10.2.8-h4 | 1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45 |
| PA-5430 | 910-000254, Physical Kit: 920-000320 | 10.2.8-h4 | 1 x 1000Base-X (management) – SFP, 1 x 40Gb Ethernet (management) - QSFP+, 1 x console - RJ-45, 1 x micro-USB, 12 x 10Gb Ethernet - SFP+, 2 x 1 Gigabit Ethernet (High Availability) – SFP, 4 x 25Gb Ethernet - SFP28, 4 x 40Gb Ethernet/100Gb Ethernet - QSFP28, 8 x 1/2.5/5/10GBase-T - RJ-45 |
| PA-5450* | 910-000223, Physical Kit: 920-000309, PA-5400 BC-A: 920-000293, PA-5400 MPC-A: 910-000195, PA-5400 NC-A: 910-000194, PA-5400 DPC-A: 910-000204 | 10.2.8-h4 | Networking cards, Data processing cards, Base cards, Management processor cards, Electrostatic Discharge, LEDs, Logging Drive Corner, USB, Console port, HSCI-A/B, Logging ports, Management Ports, HA ports, Ejector Tabs, RJ45, QSFP28, SFP/SFP+, Ground Studs, Fans, Power |
| PA-7050** | 910-000102, Physical Kit: 920-000112, PAN-PA-7050-SMC-B: 910-000185, PAN-PA-7000-DPC-A: 910-000169, PAN-PA-7000-LFC-A: 910-000183, PAN-PA-7000-100G-NPC-A: 910-000156 | 10.2.8-h4 | Networking cards, Log/Data processing cards, Log forwarding cards, Management processor cards, RJ45 ports, SFP ports, SFP+ ports, HSCI ports, QSFP+ ports, Power supply, Power Switch, LEDs, USB |
| PA-7080** | 910-000122, Physical Kit: 920-000119, PAN-PA-7080-SMC-B: 910-000186, PAN-PA-7000-DPC-A: 910-000169, PAN-PA-7000-LFC-A: 910-000183, PAN-PA-7000-100G-NPC-A: 910-000156 | 10.2.8-h4 | Networking cards, Log/Data processing cards, Log forwarding cards, Management processor cards, RJ45 ports, SFP+, HSCI, QSFP+, Power Switch, LEDs, USB |
| * Palo Alto Networks PA-5450 Cards | PA-5450 firewalls are tested with the following cards that ca | an be configured for use in th | e Approved mode of operation |

• Base Card (BC): PA-5400 BC-A P/N: 920-000293

• Management Processor Card (MPC): PA-5400 MPC-A P/N: 910-000195

• Networking Card (NC): PA-5400 NC-A P/N: 910-000194

• Data Processor Card (DPC): PA-5400 DPC-A P/N: 910-000204

**PA-7050/7080 uses the following cards below. The required cards include the SMC (must use either the 7050 or 7080 to match the chassis), LFC, and at least one NPC. A DPC can be optionally utilized as well, but must be accompanied by at least one NPC.

Network Processing Cards:

```
    PAN-PA-7000-100G-NPC-A: P/N: 910-000156
    Log Forwarding Card:

            PAN-PA-7000-LFC-A: P/N: 910-000183

    Log/Data Processing Card:

            PAN-PA-7000-DPC-A: P/N: 910-000169

    Switch Management Cards:

            PAN-PA-7080-SMC-B: P/N: 910-000186
```

• PAN-PA-7050-SMC-B: P/N: 910-000185

Approved Mode of Operation

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

- Install physical kit opacity shields and tamper evidence seals according to the Physical Security Policy section. Physical kits must be correctly installed to operate in the Approved mode of operation. The tamper evidence seals and opacity shields shall be installed for the module to operate in the Approved mode of operation.
- During initial boot up, break the boot sequence via the console port connection (by pressing the maint button when instructed to do so) to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter the Approved mode.
- Select "Enable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into "FIPS-CC" mode (Approved mode).
- The module will reboot.
- In "FIPS-CC" mode, the console port is available as a status output port.
- Once the module has finished booting, the Crypto Officer can authenticate using the default credentials that come with the module
 - o Once authenticated, the module will automatically require the operator to change their password; and the default credential is overwritten

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

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

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

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

Note: Disabling FIPS-CC mode causes a complete factory reset, which is described in the Zeroization section below.

Non-Compliant State

Failure to follow the directions in the Approved Mode of Operation above and Section 11 will result in the module operating in a non-compliant state.

Zeroization

The following procedure will zeroize the module:

- Access the module's CLI via SSH, and command the module to enter maintenance mode; the module will reboot
 Note: Establish a serial connection to the console port
- After reboot, select "Continue."
- Select "Factory Reset"
- The module will perform a zeroization, and provide the following message once complete:

• "Factory Reset Status: Success"

Approved and Allowed Algorithms

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

| | Table 3 - Approved Algorithms | | | |
|--------------|--|--------------|--|---|
| CAVP Cert | Algorithm and Standard | Mode/Method | Description / Key Size(s) / Key Strength(s) | Use / Function |
| A2138 | | | | Vetted conditioner component for ESV Cert. #E70 |
| A2153 | Conditioning | | | Vetted conditioner component for ESV Cert. #E68 |
| A2165 | AES-CBC-MAC SP 800-90B | AES-CBC-MAC | 128 bits | Vetted conditioner component for ESV Cert. #E72, E73 |
| A2541 | | | | Vetted conditioner component for ESV Cert. #E71 |
| A2906 | AES-CBC [SP 800-38A] | СВС | 128, 192 and 256 bits | Encryption Decryption |
| A2906 | AES-CCM [SP 800-38C] | ССМ | 128 bits | Encryption Decryption |
| A2906 | AES-CFB128 [SP 800-38A] | CFB128 | 128 bits | Encryption Decryption |
| A2906 | AES-CTR [SP 800-38A] | CTR | 128, 192 and 256 bits | Encryption Decryption |
| A2906 | AES-GCM [SP 800-38D] | GCM** | 128 and 256 bits | Encryption Decryption |
| A2906 | Counter DRBG [SP 800-90Arev1] | CTR DRBG | AES 256 bits with Derivation Function Enabled | Random Bit Generator |
| A2906 | ECDSA KeyGen (FIPS 186-4) | ECDSA KeyGen | P-256, P-384, P-521 | Key Generation |
| A2906 | ECDSA KeyVer (FIPS 186-4) | ECDSA KeyVer | P-256, P-384, P-521 | Public Key Validation |
| A2906 | ECDSA SigGen (FIPS 186-4) | ECDSA SigGen | P-256, P-384, P-521 with SHA2-224, SHA2-256, SHA2-384, and SHA2-512 | Signature Generation |
| A2906 | ECDSA SigVer (FIPS 186-4) | ECDSA SigVer | P-256, P-384, P-521 with SHA-1, SHA2-224, SHA2-256, SHA2-384, and SHA2-512 | Signature Verification |
| A2906 | HMAC-SHA-1 [FIPS 198-1] | НМАС | HMAC-SHA-1 with λ=96, 160 | Authentication for protocols |
| A2906 | HMAC-SHA2-224 [FIPS 198-1] | НМАС | HMAC-SHA2-224 with λ=224 | Authentication for protocols |
| A2906 | HMAC-SHA2-256 [FIPS 198-1] | НМАС | HMAC-SHA2-256 with λ=256 | Authentication for protocols |
| A2906 | HMAC-SHA2-384 [FIPS 198-1] | НМАС | HMAC-SHA2-384 with λ=384 | Authentication for protocols |
| A2906 | HMAC-SHA2-512 [FIPS 198-1] | НМАС | HMAC-SHA2-512 with λ=512 | Authentication for protocols |
| A2906 | KAS-ECC-SSC Sp800-56Ar3 | KAS | P-256/P-384/P-521 | Key Exchange |
| A2906 | KAS-FFC-SSC SP 800-56Ar3 | KAS | MODP-2048/3072/4096 | Key Exchange |
| A2906 | KDF IKEv2 [SP 800-135rev1] (CVL) | IKEv2 KDF | SHA2-256, SHA2-384, SHA2-512 | IKEv2 |

| A2906 | KDF SNMP [SP 800-135rev1] (CVL) | SNMPv3 KDF | Engine ID: 80001F88043030303030 343935323630 | SNMPv3 |
|--|---|--|---|---|
| A2906 | KDF SSH [SP 800-135rev1] (CVL) | SSHv2 KDF | SHA-1, SHA2-256, SHA2-512 | SSH |
| A2906 | KDF TLS [SP 800-135rev1] (CVL) | TLS1.2 KDF | TLS v1.2 Hash Algorithm: SHA2-256, SHA2-384 | TLS |
| A2906 | RSA KeyGen (FIPS 186-4) | RSA KeyGen (FIPS 186-4) | 2048, 3072, and 4096 bits | Key Pair Generation |
| A2906 | RSA SigGen (FIPS 186-4) | RSA SigGen (FIPS 186-4) | 2048, 3072, and 4096-bit with hashes 256/384/512 | Signature Generation |
| A2906 | RSA SigVer (FIPS 186-4) | RSA SigVer (FIPS 186-4) | 2048, 3072, 4096-bit (per IG C.F) with hashes SHA-1/224+++/256/384/512 (Signature Verification) +++ This Hash algorithm is not | Signature Verification |
| | | | | Digital Signature Generation/Verification |
| A2906 | SHA-1 [FIPS 180-4] | SHA | SHA-1 | Non-Digital Signature Applications (e.g. component of HMAC) |
| | SH 42-224 [EIDS | | | Digital Signature Generation/Verification |
| A2906 | 180-4] | SHA2 | SHA-224 | Non-Digital Signature Applications (e.g. component of HMAC) |
| | SHA2-256 [EIPS | | | Digital Signature Generation/Verification |
| A2906 [180-4] | SHA2 | SHA-256 | Non-Digital Signature Applications (e.g. component of HMAC) | |
| A2906 | SHA2-384 [FIPS 180-4] | SHA2 | SHA-384 | Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC) |
| A2906 | SHA2-512 [FIPS 180-4] | SHA2 | SHA-512 | Digital Signature Generation/Verification Non-Digital Signature Applications (e.g. component of HMAC) |
| A2906 | Safe Primes Key Generation [RFC 3526] | Safe Primes Key Generation | MODP-2048, MODP-3072, MODP-4096 | Safe Primes Key Generation |
| A2906 | Safe Primes Key Verification [RFC 3526] | Safe Primes Key Verification | MODP-2048, MODP-3072, MODP-4096 | Safe Primes Key Verification |
| AES Cert. #A2906 and HMAC Cert. #A2906 | KTS [SP 800-38F] | SP 800-38A, FIPS 198-1, and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G. | AES-CBC or AES-CTR plus HMAC 128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength | Key Wrapping |
| AES-CCM Cert. #A2906 | KTS [SP 800-38F] | SP 800-38C and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G. | AES-CCM 128-bit keys providing 128 bits of encryption strength | Key Wrapping |
| AES-GCM Cert. #A2906 | KTS [SP 800-38F] | SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G. | AES-GCM 128 and 256-bit keys providing 128 or 256 bits of encryption strength | Key Wrapping |
| ESV Cert. #E27 | SP 800-90B | ESV | AMD Random Number Generator | Entropy |
| ESV Cert. #E68, E70, | SP 800-90B | ESV | Palo Alto Networks DRNG Entropy Source | Entropy |

| E71, E72, E73 | | | | |
|--|-------------------------|---|--|---|
| ESV Cert. #E128 | SP 800-90B | ESV | Octeon III Entropy Source | Entropy |
| KAS-ECC-S SC Cert. #A2906, KDF IKEv2 Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2). | P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength | Key Exchange with protocol KDF |
| KAS-ECC-S SC Cert. #A2906, KDF SSH Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2). | P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength | Key Exchange with protocol KDF |
| KAS-ECC-S SC Cert. #A2906, KDF TLS Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2). | P-256, P-384, and P-521 curves providing 128, 192, or 256 bits of encryption strength | Key Exchange with protocol KDF |
| KAS-FFC-S SC Cert. #A2906, KDF IKEv2 Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2). | 2048, 3072, and 4096-bit keys providing 112, 128, or 150 bits of encryption strength | Key Exchange with protocol KDF |
| KAS-FFC-S SC Cert. #A2906, KDF SSH Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2). | 2048-bit key providing 112 bits of encryption strength | Key Exchange with protocol KDF |
| KAS-FFC-S SC Cert. #A2906, KDF TLS Cert. #A2906 | KAS [SP 800-56Arev3] | SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2). | 2048-bit key providing 112 bits of encryption strength | Key Exchange with protocol KDF |
| Vendor Affirmed | CKG (SP 800-133rev2) | Section 5.1, Section 5.2, and Section 6.1 | Cryptographic Key Generation; SP 800- 133 and IG D.H (symmetric keys and asymmetric seeds). | Key Generation Note: The symmetric keys and seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG |

**The module is compliant to IG C.H: GCM is used in the context of TLS, IPsec/IKEv2, SSH:

- For TLS, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.
 - From this RFC, the GCM cipher suites in use are TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.
- For IPsec/IKEv2, The GCM implementation meets Scenario 1 of IG C.H: it is used in a manner compliant with RFCs 4106 and 7296 (RFC 5282 is not applicable, as the module does not use GCM within IKEv2 itself). 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 C.H. 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. (It would take hundreds of years for this to occur.)

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

The module is compliant to IG C.F:

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

The module does not have any algorithms that fall under:

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

The following table documents the module's algorithms that are non-approved and not allowed for use in the approved mode of operation.

Table 4 - Supported Protocols in Approved Mode

| TLSv1.2 |
|-----------------|
| SSHv2 |
| IPSec and IKEv2 |
| SNMPv3 |

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

Module Diagrams

Figure 1 depicts the logical block diagram for the modules. The cryptographic physical perimeter includes all of the logical components of the modules and the boundary is the physical enclosure of the firewall.



Figure 1 - Logical Diagram

Figures 2 - 29 depict the modules and their interfaces. Please refer to the appendices for depictions of the modules with the physical kits installed.





Figure 3 - PA-220 Rear Interfaces



Figure 4 - PA-220R Front Interfaces



Figure 5 - PA-220R Rear Interfaces



Figure 6 - PA-820 / PA-850 Front Interfaces



Figure 8 - PA-850 Rear Interfaces



Figure 9 - PA-3200 Series Front Interfaces



Figure 10 - PA-3200 Series Rear Interfaces



Figure 9 - PA-3200 Series Front Interfaces



Figure 10 - PA-3200 Series Rear Interfaces



Figure 11 - PA-3410/3420 Front Interfaces



Figure 12 - PA-3430/3440 Front Interfaces



Figure 13 - PA-3400 Rear Interfaces



Figure 14 - PA-5200 Series Front Interfaces



Figure 15 - PA-5200 Rear Interfaces



Figure 16 - PA-7050 Front Interfaces



Figure 17 - PA-7050 Back Interfaces



Figure 18 - PA-7080 Front (on Left) and Back (on Right) Interfaces



Figure 19 - PA-410 Front Interfaces







Figure 21 - PA-400 Front Interfaces (PA-440/450/460 front panels are identical)



Figure 22 - PA-400 Rear Interfaces (PA-440/450/460 rear panels are identical)



Figure 23 - PA-5410/5420/5430 Front Interfaces (Note: All modules are identical)



Figure 24 - PA-5410/5420/5430 Rear Interfaces (Note: All modules are identical)



Figure 25 - PA-5450 Front Interfaces



Figure 26 - PA-5450 Management Processor Card



Figure 27 - PA-5450 Networking Card



Figure 28 - PA-5450 Data Processing Card



Figure 29 - PA-5450 Rear Interfaces

3. Cryptographic Module Interfaces

The modules are multi-chip standalone modules with ports and interfaces as shown below. The modules do not implement a control output interface.

| Physical Interface | Logical Interface | Data that passes over port/interface |
|--|--|--------------------------------------|
| HSCI (PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5450, PA-7000 Series) | Data input, control input, data output, status output | SSH |
| LED | Status output | Module status via LED indicators |
| Micro USB Console (PA-220, PA-220R, PA-800 Series, PA-3200 Series, PA-3400 Series,, PA-440/PA-450/PA-460, PA-5400 Series, PA-5450, PA-7050, PA-7080) | Status output | Self-test output |
| Power | Power | N/A |
| Power switch (PA-7000 Series) | Control input | Power input switch |

| QSFP+ (PA-3260, PA-3430/PA-3440, PA-5250, PA-5260, PA-5280, PA-5400 Series, PA-7000 Series) | Data input, control input, data output, status output | TLS, IPsec, or SSH |
|--|--|--------------------|
| QSFP28 (PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7000 Series) | Data input, control input, data output, status output | TLS, IPsec, or SSH |
| RJ45 Console | Status output | Self-test output |
| RJ45 Ethernet | Data input, control input, data output, status output | TLS, IPSec |
| RJ45 HA (PA-3200 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7050, PA-7080) | Data input, control input, data output, status output | SSH |
| RJ45 Log (PA-5450) | Data input, control input, data output, status output | TLS, IPsec |
| RJ45 MGT (PA-400 Series, PA-3200 Series, PA-3400 Series, PA-440/PA-450/PA-460, PA-5400 Series, PA-5450, PA-7000 Series) | Data input, control input, data output, status output | TLS, SSH |
| SFP (PA-220R,PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-7000 Series) | Data input, control input, data output, status output | TLS, IPSec, or SSH |
| SFP+ (PA-800 Series, PA-3200 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, PA-5450, PA-7050, PA-7080) | Data input, control input, data output, status output | TLS, IPSec, or SSH |
| SFP28 (PA-3400 Series, PA-5400 Series) | Data input, control input, data output, status output | TLS, IPSec |

4. Roles, Services, and Authentication

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.

| Role | Service | Input | Output |
|---|--------------------------------------|--|--|
| Crypto Officer | Show Version | Query module for version | Module provides version |
| Crypto Officer, User | Security Configuration Management | Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts via CLI or WebUI | Confirmation of service via Configuration Logs |
| Crypto Officer | Other Configuration | Networking parameter configuration, logging configuration, and other non-security relevant configuration via CLI or WebUI | Confirmation of service via Configuration Logs |
| Crypto Officer, User | View Other Configuration | Query module for current non-security relevant configuration via WebUI or CLI | Confirmation of service via Configuration Logs |
| Crypto Officer, User, RA VPN, S-S VPN | Show Status | Query status of the module via WebUI or CLI | Module status information via CLI or System Logs |
| RA VPN, S-S VPN | VPN | Initialize VPN connection | Confirmation of service via System Logs |
| Crypto Officer | Firmware Update | Loading new image | Message output noting version updated successfully |
| Unauthenticated | Zeroize | Initialize Factory Reset via Maintenance Mode | Console Output |
| Unauthenticated | Self-Tests | Power removal | Console Output |
| Unauthenticated | Show Status (LEDs) | N/A | LEDs |

Table 6 - Roles, Service Commands, Input and Output

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 support concurrent operators.

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

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

The passwords for the RA VPN and S-S VPN roles are created as part of the Security Configuration Management service allocated to the Cryptographic Officer.

| Role | Authentication Method | Authentication Strength | | | | | |
|----------------------------------|--|--|--|--|--|--|--|
| Cryptographic Officer | Memorized Secret (Username/password) and/or Single-Factor Cryptographic Software (certificate/public key-based authentication) | Password-basedThe minimum length is eight (8) characters1 (95 possible characters).The probability that a random attempt will succeed or a falseacceptance will occur is $1/(95^8)$ which is less than $1/1,000,000$. Theprobability of successfully authenticating to the module within oneminute is $10/(95^8)$, which is less than $1/100,000$. The firewall's | | | | | |
| User | Memorized Secret (Username/password) and/or Single-Factor Cryptographic Software (certificate/public key-based authentication) | configuration supports at most ten failed attempts to authenticate in a one-minute period. <u>Certificate/Public key-based</u> The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072 RSA 4086 ECDSA P-256 P-384 or P-521 | | | | | |
| Remote Access VPN (RA VPN) | Memorized Secret (Username/password) and/or Single-Factor Cryptographic Software (certificate-based authentication) | The minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is $1/(2^{112})$ which is less than $1/1,000,000$. The probability of successfully authenticating to the module within a one minute period is $3,600,000/(2^{112})$, 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. | | | | | |
| Site-to-Site VPN (S-S VPN) | IKE/IPSec Pre-shared keys - Identification with the IP Address and authentication with the Pre-Shared Key (Memorized Secret) or Single-Factor Cryptographic Software (certificate based authentication) | 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. 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 1/2,000,000/(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 1/1,000,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period. | | | | | |

Table 7 - Roles and Authentication

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

CSP Access Rights

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

- *G* = Generate: The module generates or derives the SSP.
- *R* = Read: The SSP is read from the module (e.g. the SSP is output).
- *W* = Write: The SSP is updated, imported, or written to the module.
- *E* = Execute: The module uses the SSP in performing a cryptographic operation.
- *Z* = Zeroise: The module zeroises the SSP.

| Service | Description | Approved Security Functions | | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|--|--|---|-------------------------------------|-----------|--------------------------------------|---|
| Show Version | Query the module to display the version | N/A | | N/A | СО | N/A | Version displayed via System Logs / CLI / UI |
| Security Configuration Management | Configuring and managing cryptographic | CKG RSA KeyGen (FIPS 186-4) RSA SigGen (FIPS 186-4) | | RSA Private Keys | CO | G/W/E | Configuration/System Logs |
| parameters and setting/modifying security policy, including creating | | CKG ECDSA KeyGen (FIPS 186-4) ECDSA SigGen | | ECDSA Private Keys | со | G/W/E | |
| | additional CO accounts | KAS | KDF TLS (CVL) | TLS Pre-Master Secret | СО | G/E/Z | |
| | | | KDF TLS (CVL) | TLS Master Secret | СО | G/E/Z | |
| | | | CKG, ECDSA | TLS DHE/ECDHE Private Components | со | G/E/Z | |
| | | KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification | TLS DHE/ECDHE Public Components | | G/E/R/W/Z | | |
| | | KTS | HMAC-SHA2- 256 HMAC-SHA2- 284 | TLS HMAC Keys | СО | G/E/Z | |
| | | KTC . | AES-CBC | TLS Encryption Keys | СО | G/E/Z | |
| | | KTS KTS | HMAC-SHA-1 HMAC-SHA-1 256 HMAC-SHA2- 512 | SSH Session Authentication Keys | со | G/E/Z | |
| | | ₩TS | AES-CBC, AES-CTR | SSH Session Encryption Keys | СО | G/E/Z | |
| | | KAS | KDF SSH (CVL) | SSH DHE/ECDHE Private Components | СО | G/E/Z | |
| | | | KAS-ECC-SSC KAS-FFC-SSC Safe Primes Key Generation, Safe Primes Key Verification | SSH DHE/ECDHE Public Components | | G/E/R/W/Z | |
| | | N/A | | CO, User, RA VPN Password | со | G/E/W | |
| | | Counter DRBG, ESV | | DRBG Seed DRBG V DRBG Key | СО | G/E | |

Table 8 - Approved Services

| | | | | Entropy Input String | | | | |
|---------------|------------------------|--------------------------------|---------------------|-------------------------|----------|--------------|---------------------------|--|
| | | | 1P (CVL) | SNMPv3 Authentication | со | W/E | 1 | |
| | | | | Secret | | | | |
| | | KDF SNN | 1P (CVL) | SNMPv3 Privacy Secret | CO | W/E | 1 | |
| | | HMAC-S | HA-1 | Authentication Key | CO | G/E/Z | 1 | |
| | | HMAC-SHA2-224 HMAC-SHA2-256 | | | | | | |
| | | | | | | | | |
| | | HMAC-SI | HA2-384 | | | | | |
| | | | HA2-512 | | | 0 (5 (7 | 4 | |
| | | AES-CFB | 128 | Session Key | 0 | G/E/Z | 4 | |
| | | N/A | | Protocol Secrets | <u> </u> | W/E | 4 | |
| | | RSA SigV | er (FIPS 186-4) | CA Certificates | 0 | G/R/E/W | | |
| | | ECDSA S | igver S-4) | | | | | |
| | | FCDSA S | igVer | FCDSA Public Keys | 0 | G/R/F/W | 1 | |
| | | (FIPS 186 | 5-4) | Eebb, (Tublic Reys | | 0,11,2,11 | | |
| | | RSA SigV | er | RSA Public Keys | со | G/R/E/W | 1 | |
| | | (FIPS 186 | 5-4) | - | | | | |
| | | RSA SigV | er (FIPS 186-4) | SSH Host Public Key | CO | G/R/E/W | | |
| | | ECDSA S | igVer | | | | | |
| | | (FIPS 186 | 5-4) | | | | 4 | |
| | | RSA SigV | er (FIPS 186-4) | SSH Client Public Key | CO | W/E | 4 | |
| | | RSA SigV | er (FIPS 186-4) | Public key for firmware | 0 | VV/E | | |
| Other | Networking | Rev ciac | en | RSA Privata Kava | <u> </u> | G/W/F | Configuration/System Loss | |
| Configuration | parameter | (FIPS 184 | 5-4) | NOT I IVALE NEVS | | 0/ VV/L | Computation/System Logs | |
| | configuration, logging | ECDSA S | igGen | ECDSA Private Kevs | со | G/W/E | 1 | |
| | configuration, and | (FIPS 186-4) | | | | |] | |
| | other non-security | KAS | KDF TLS | TLS Pre-Master Secret | CO | G/E/Z |] | |
| | relevant configuration | | (CVL) | | | | | |
| | | | KDF TLS | TLS Master Secret | CO | G/E/Z | | |
| | | | (CVL) | | | | 4 | |
| | | | CKG, | TLS DHE/ECDHE Private | со | G/E/Z | | |
| | | | ECDSA | | 4 | C/F/DA4//7 | 4 | |
| | | | 186-4) | TLS DHE/ECDHE Public | | G/E/R/W/Z | | |
| | | | FCDSA | Components | | | | |
| | | | KeyVer (FIPS | | | | | |
| | | | 186-4), | | | | | |
| | | | KAS-ECC-SSC, | | | | | |
| | | | KAS-FFC-SSC, | | | | | |
| | | | Safe Primes | | | | | |
| | | | Generation | | | | | |
| | | | Safe Primes | | | | | |
| | | | Kev | | | | | |
| | | | Verification | | | | | |
| | | HMAC-S | HA2-256 | TLS HMAC Keys | CO | G/E/Z | 1 | |
| | | HMAC-S | HA2-384 | | | | 1 | |
| | | AES-CBC | or AES-GCM | TLS Encryption Keys | CO | G/E/Z | | |
| | | HMAC-SI | HA-1 | SSH Session | со | G/Z | | |
| | | HMAC-S | HAZ-256 | Authentication Keys | | | | |
| | | AFS-CBC AFS-CTR or | | SSH Session Encryption | <u> </u> | G/E/7 | 1 | |
| | | ALS-CBC | /, πεστοικ, υι Λ | Kevs | | U/L/Z | | |
| | | KAS | KDF SSH | SSH DHE/ECDHF | со | G/E/Z | 1 | |
| | | | | Private Components | | | 1 | |
| | | | CKG, | | | C/E/D/M//7 | 4 | |
| | | | ECDSA | SSH DHE/ECDHE Public | 1 | G/E/R/W/Z | 1 | |
| | | | KeyGen (FIPS | Components | | | 1 | |
| | | | FCDSA | | | | | |
| | | | KevVer (FIPS | | | | 1 | |
| | | | 186-4), | | | | 1 | |
| | | | KAS-ECC-SSC, | | | | | |
| | | | KAS-FFC-SSC, | | | | 1 | |
| | | | Safe Primes | | | | 1 | |
| | | | Key | | | | | |
| | | | Safe Primes | | | | 1 | |
| | | | Kev | | | | | |
| | | | Verification | | | | | |
| | | | | | | | 4 | |
| | | N/A | | CO, User, RA VPN | со | G/E/W | | |
| | | Comi | | Password | 60 | С/Г | 4 | |
| | | Counter | UKBG, ESV | DRBC V | | G/E | 1 | |
| | | | | | 1 | | | |
| | | | | Entropy Input String | 1 | | 1 | |
| | | RCA Cial | er (FIDS 184-4) | SSH Host Public Kov | <u> </u> | G/R/E/M/ | 1 | |
| | | ECDSA S | igVer | SSITTIOSLE UDIIC NEY | | G/ IV/ L/ VV | | |
| | | | | | | | | |

| | | (FIPS 186-4) | | | | | |
|-----------------------------|---|--|---|---|----------|-----------|---------------------------|
| | | | | | | | |
| | | | | | | | |
| | | RSA SigV | er (FIPS 186-4) | SSH Client Public Key | CO | W/F | - |
| View Other Configuration | Read-only of non-security relevant | N/A | | CO, User, RA VPN Password | CO, User | W/E | Configuration/System Logs |
| | computation | | | Note: includes all items in "Other Configuration" | | | |
| Show Status | Provides status information of the | RSA SigG | ien (FIPS 186-4) | RSA Private Keys | CO, User | E | Configuration/System Logs |
| | module | ECDSA S (FIPS 186 | igGen 5-4) | ECDSA Private Keys | CO, User | E | |
| | | KAS | KDF TLS (CVL) | TLS Pre-Master Secret | CO, User | G/E/Z | |
| | | | KDF TLS (CVL) | TLS Master Secret | CO, User | G/E/Z | |
| | | | CKG, ECDSA | TLS DHE/ECDHE Private Components | CO, User | G/E/Z | |
| | | | KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, Safe Primes Key Generation, Safe Primes Key | Components | | G/E/R/W/Z | |
| | | HMAC-SHA2-256 | | TLS HMAC Keys | CO, User | G/E/Z | - |
| | | | Cor AES-GCM | TLS Encryption Keys | CO, User | G/E/Z | |
| | | | HA-1 HA2-256 HA2-512 | SSH Session Authentication Keys | CO, User | G/E/Z | |
| | | AES-CBC, AES-CTR, or AES-GCM Counter DRBG, ESV | | SSH Session Encryption Keys | CO, User | G/E/Z | |
| | | | | DRBG Seed DRBG V DRBG Key Entropy Input String | RA VPN | G/E | |
| | | KAS | KDF SSH (CVL) | SSH DHE/ECDHE Private Components | СО | G/E/Z | |
| | Durida d | | CKG, ECDSA KeyGen (FIPS 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification | SSH DHE/ECDHE Public Components | | G/E/R/W/Z | |
| VPN | Provide network access for remote users or site-to-site connection | KTS | HMAC-SHA-1 HMAC-SHA2- 256 HMAC-SHA2- 384 HMAC-SHA2- 512 | S-S VPN IPSec/IKE Authentication Keys | S-S VPN | G/E/Z | Configuration/System Logs |
| | | KTS | AES-CBC AES-CCM | S-S VPN IPSec/IKE Session Keys | S-S VPN | G/E/Z | |
| | | KTS KAS | AES-GCM KDF IKEv2 (CVL) | S-S VPN IPSec/IKE DHE/ECDHE Private Components | S-S VPN | G/E/Z | |
| | | | ECDSA KeyGen (FIPS | | | G/E/R/W/Z | 4 |

| | | N/A ECDSA Si (FIPS 186 RSA SigVi | 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification | S-S VPN IPSec/IKE DHE/ECDHE Public Components S-S VPN IPSec Pre-Shared Keys ECDSA Public Keys RSA Public Keys | S-S VPN S-S VPN S-S VPN | W/E W/E | |
|-----------------------|--|---|---|---|-------------------------------|------------|---------------------------|
| | | (FIPS 186 RSA SigG | 6-4) en | RSA Private Keys | RA VPN | E | |
| | | ECDSA Si (FIPS 186 | -4) igGen 5-4) | ECDSA Private Keys | RA VPN | E | |
| | | KAS | KDF TLS (CVL) | TLS Pre-Master Secret | RA VPN | G/E/Z | |
| | | | KDF TLS (CVL) | TLS Master Secret | | G/E/Z | |
| | | | CKG, ECDSA | TLS DHE/ECDHE Public Components | RAVPN | G/E/R/W/Z | |
| | | | KeyGen(FIP3 186-4), ECDSA KeyVer (FIPS 186-4), KAS-ECC-SSC, KAS-FFC-SSC, Safe Primes Key Generation, Safe Primes Key Verification | Components | KA VPN | G/E/Z | |
| | | KTS | HMAC-SHA2- 256 HMAC-SHA2- 384 | TLS HMAC Keys | RA VPN | G/E/Z | |
| | | ктѕ | AES-CBC AES-GCM | TLS Encryption Keys | RA VPN | G/E/Z | |
| | | CKG, AES-CBC | or AES-GCM | RA VPN IPSec Session Keys | RA VPN | G/E/Z | |
| | | CKG, HMAC-Sł | HA-1 | RA VPN IPSec Authentication | RA VPN | G/E/Z | |
| | | Counter I | DRBG, ESV | DRBG Seed DRBG V DRBG Key Entropy Input String | RA VPN | G/E | |
| | | RSA SigV ECDSA SigV (FIPS 186 | er (FIPS 186-4)) igVer 5-4) | CA Certificates | RAVPN | W/E | |
| | | ECDSA S | igVer 5-4) | ECDSA Public Keys | RAVPN | W/E | |
| F | | KSA SigV | er 5-4) | RSA Public Keys | RA VPN | W/E | |
| Firmware Update | Provides a method to update the firmware of the module | RSA SigVer (FIPS 186-4) | | Public key for firmware content load test Note: Includes all keys from Other Configuration | co | | Configuration/System Logs |
| Zeroize | Destroys all keys in the module | N/A | | All keys and SSPs | CO | Z | Zeroization indicator |
| Self-Test | Initiates self-tests and integrity test | HMAC-SH ECDSA SI (FIPS 186 | HA2-256, igVer 5-4) | FIrmware integrity verification key | со | E | System Logs |
| Show Status (LEDs) | Provides status of the module | N/A | | N/A | All | R | LEDs |

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

5. Software/Firmware Security

The module performs the Firmware Integrity test by using HMAC-SHA-256 and ECDSA signature verification (HMAC and ECDSA Cert. #A2906) during the Pre-Operational Self-Test. In addition, the module also conducts the firmware load test by using RSA 2048 with SHA-256 (Cert. #A2906) for the new validated firmware to be uploaded into the module.

The pre-operational self-tests can be initiated by power cycling the module. When this is performed, the module automatically runs the cryptographic algorithm self-tests in addition to the pre-operational firmware integrity test.

6. Operational Environment

The FIPS 140-3 Operational Environment requirements are not applicable because the Firewalls do not contain modifiable operational environments. The operational environment is limited since the modules include a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into these modules is out of the scope of this validation and requires a separate FIPS 140-3 validation.

7. Physical Security

The multi-chip standalone modules are production quality containing standard passivation. Chip components are protected by an opaque enclosure. There are tamper evident seals that are applied on the modules by the Crypto-Officer. All unused seals are to be controlled by the Crypto-Officer. The seals prevent removal of the opaque enclosure without evidence. The Crypto-Officer must ensure that the module surface is clean and dry. Tamper evident seals must be pressed firmly onto the adhering surfaces during installation and once applied the Crypto-Officer shall permit 24 hours of cure time for all tamper-evident seals. The Crypto-Officer should inspect the seals and shields for evidence of tamper every 30 days. If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact Customer Support.

Note: For ordering information, see Table 2 for physical kit part numbers and versions. Opacity shields and Tamper Seals are included for the physical kits.

Refer to the Appendix for instructions on installation of the tamper seals and opacity shields.

| Taur | Table 7 - Thysical Security hispection duidennes | | | | | | | | | | |
|--|--|---|--|--|--|--|--|--|--|--|--|
| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details | | | | | | | | | |
| Tamper-Evident Seals (PA-7080, PA-7050, PA-5220, PA-5250, PA-5260, PA-5280, PA-3220, PA-3250, PA-3260, PA-820, PA-850, PA-220R, PA-220, PA-410/440/450/460, PA-5450, PA-5410/5420/5430, and PA-3410/3420/3430/3440) | 30 days | Verify integrity of tamper-evident seals in the locations identified in the physical Kit Installation Guide. Seal integrity to be verified within the modules operating temperature range. | | | | | | | | | |

Table 9 - Physical Security Inspection Guidelines

| Top, Bottom, Front and Rear Opacity Shields (PA-7050 PA-5450) | 30 days | Verify that the plenums and opacity shields have not been deformed from their original shape, thereby reducing their effectiveness |
|---|---------|--|
| Front and Rear Covers (PA-3220, PA-3250, PA-3260) | 30 days | Verify that front and rear covers have not been deformed from their original shape, thereby reducing their effectiveness |
| Front Cover (PA-7080, PA-5450, PA-5410/5420/5430, and PA-3410/3420/3430/3440) | 30 days | Verify that front cover has not been deformed from its original shape thereby reducing its effectiveness |
| Front cover and Cage Enclosure (PA-220) | 30 days | Verify that front cover and cage enclosure have not been deformed from their original shape, thereby reducing their effectiveness |

8. Non-Invasive Security

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

9. Sensitive Security Parameter Management

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

| Table 10 - SSPs | | | | | | | | | | |
|-----------------------|---------------------|--|------------------------|---|---------------|------------------------|---|--|--|--|
| Key/SSP/Name/Ty pe | Strength | Security Function and Cert. Number | Generatio n | Import/Export | Establishment | Storage | Zeroization | Use & Related Keys | | |
| CA Certificates | 112 bits minimum | RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | TLS or SSH Session Key Encrypted | N/A | HDD/RAM – plaintext | HDD – Zeroize Service RAM - Zeroize at session termination | ECDSA/RSA Public key - Used to trust a root CA intermediate CA and leaf /end entity certificates (RSA 2048, 3072, and 4096 bits) (ECDSA P-256, P-384, and P-521) | | |
| RSA Public Keys | 112 bits minimum | RSA SigVer (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | TLS or SSH Session Key Encrypted or Plaintext TLS handshake | N/A | HDD/RAM – plaintext | Zeroize Service | RSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048, 3072, or 4096-bit) | | |
| RSA Private Keys | 112 bits minimum | RSA SigGen (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | TLS or SSH Session Key Encrypted | N/A | HDD/RAM – plaintext | HDD – Zeroize Service RAM - Zeroize at session termination | RSA Private keys for generation of signatures, authentication or key establishment. (RSA 2048, 3072, or 4096-bit) | | |
| ECDSA Public Keys | 128 bits minimum | ECDSA SigVer (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | TLS or SSH Session Key Encrypted or Plaintext TLS handshake | N/A | HDD/RAM – plaintext | Zeroize Service | ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521) | | |
| ECDSA Private Keys | 128 bits minimum | ECDSA SigGen (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | TLS or SSH Session Key Encrypted | N/A | HDD/RAM – plaintext | HDD - Zeroize Service | ECDSA Private key for generation of | | |

| | | | | | | | RAM - Zeroize at session termination | signatures and authentication (P-256, P-384, or P-521) |
|--|---------------------|--|-------------------------------|------------------------------|-------------------------------|------------------------|--------------------------------------|--|
| TLS DHE/ECDHE Private Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906 | DRBG, SP 800-56A Rev. 3 | N/A | N/A | RAM - plaintext | Zeroize at session termination | Ephemeral Diffie-Hellman private FFC or EC component used in TLS (DHE 2048, ECDHE P-256, P-384, P-521) |
| TLS DHE/ECDHE Public Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906 | DRBG, SP 800-56A Rev. 3 | Plaintext - TLS handshake | N/A | N/A | Zeroize at session termination | Diffie_Hellman or EC Diffie-Hellman Ephemeral values used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521) |
| TLS Pre-Master Secret | N/A | KDF TLS Cert. #A2906 | KAS SP 800-56A Rev. 3 | N/A | N/A | RAM – plaintext | Zeroize at session termination | Secret value used to derive the TLS Master Secret along with client and server random nonces |
| TLS Master Secret | N/A | KDF TLS Cert. #A2906 | KDF TLS | N/A | N/A | RAM – plaintext | Zeroize at session termination | Secret value used to derive the TLS session keys |
| TLS Encryption Keys | 128 bits minimum | AES-CBC or AES-GCM Cert. #A2906 | KDF TLS | N/A | TLS, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | AES (128 or 256 bit) keys used in TLS connections (GCM; CBC) |
| TLS HMAC Keys | 256 bits minimum | HMAC-SHA2- 256 HMAC-SHA2- 384 Cert. #A2906 | KDF TLS | N/A | TLS, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | HMAC keys used in TLS connections (HMAC-SHA2-256 /384) (256, 384 bits) |
| SSH DHE/ECDHE Private Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert.#A2906 | DRBG, SP 800-56A Rev. 3 | N/A | N/A | RAM - plaintext | Zeroize at session termination | Diffie Hellman or EC Diffie-Hellman private (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521) |
| SSH DHE/ECDHE Public Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906 | DRBG, SP 800-56A Rev. 3 | Plaintext SSH handshake | N/A | RAM - plaintext | Zeroize at session termination | Diffie Hellman or EC Diffie-Hellman public component (DH Group 14, ECDH P-256, ECDH P-384, ECDH P-521) |
| SSH Host Public Key | 112 bits minimum | RSA SigVer (FIPS 186-4) ECDSA SigVer (FIPS 186-4) Cert. #A2906 | DRBG, FIPS 186-4 | N/A | N/A | HDD/RAM – plaintext | Zeroize Service | SSH Host Public Key (RSA 2048, RSA 3072, RSA 4096, ECDSA P-256, P-384, or P-521) |
| SSH Client Public Key | 112 bits minimum | RSA SigVer (FIPS 186-4) Cert. #A2906 | N/A | Encrypted via SSH or TLS | N/A | HDD/RAM – plaintext | Zeroize Service | Public RSA key used to authenticate client. (RSA 2048, 3072, and 4096 bits) |
| SSH Session Encryption Keys | 128 bits minimum | AES-CBC, AES-CTR, or AES-GCM Cert. #A2906 | KDF SSH | N/A | SSH, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | Used in all SSH connections to the security module's command line interface. (128, 192, or 256 bits: AES CBC or CTR) (128 or 256 bits: AES GCM) |
| SSH Session Authentication Keys | 160 bits minimum | HMAC-SHA-1 HMAC-SHA2- 256 HMAC-SHA2- 512 Cert. #A2906 | KDF SSH | N/A | SSH, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | Authentication keys used in all SSH connections to the security module's command line interface (HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512) (160, 256, 512 bits) |

| S-S VPN IPSec/IKE DHE or ECDHE Private Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert. #A2906 | DBRG, SP 800-56A Rev. 3 | N/A | N/A | RAM - plaintext | Power cycle | Diffie-Hellman or EC Diffie-Hellman private component used in key establishment (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521) |
|--|---------------------|--|-------------------------------|---------------------------------------|--|--|-----------------------------------|---|
| S-S VPN IPSec/IKE DHE or ECDHE Public Components | 112 bits minimum | KAS-ECC-SSC KAS-FFC-SSC Cert.#A2906 | DRBG, SP 800-56A Rev. 3 | N/A | N/A | RAM - plaintext | Power cycle | Diffie-Hellman or EC Diffie-Hellman public component used in key agreement (DHE 2048, DHE 3072, DHE 4096, ECDHE P-256, P-384, P-521) |
| S-S VPN IPSec/IKE Session Keys | 128 bits minimum | AES-CBC, AES-CCM, AES-GCM Cert. #A2906 | KDF IKEv2 | N/A | IPSec/IKE, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | Used to encrypt IKE/IPSec data. These are AES (128, 192, or 256 CBC) IKE keys and (128, 192 or 256 CBC, 128 CCM, 128 or 256 GCM) IPSec keys |
| S-S VPN IPSec/IKE Authentication Keys | 160 bits minimum | HMAC-SHA-1 HMAC-SHA2- 256 HMAC-SHA2- 384 HMAC-SHA2- 512 Cert.#A2906 | KDF IKEv2 | N/A | IPSec/IKE, KAS SP 800-56A Rev. 3 | RAM - plaintext | Zeroize at session termination | (HMAC-SHA-1, SHA-256, SHA-384 or SHA-512) Used to authenticate the peer in an IKE/IPSec tunnel connection. (160, 256, 384, 512 bits) |
| S-S VPN IPSec Pre-Shared Keys | N/A | N/A | N/A | Encrypted via SSH or TLS | N/A | HDD/RAM – plaintext | Zeroize Service | PSK used in conjunction with HMAC listed above for authentication. Entered into the module by the Crypto Officer once authenticated |
| RA VPN IPSec Session Keys | 128 bits minimum | AES-CBC or AES-GCM Cert. #A2906 | CKG, DRBG | N/A | N/A | RAM - plaintext | Zeroize at session termination | Used to encrypt remote access sessions utilizing IPSec. (AES 128-CBC, 128/256-GCM) |
| RA VPN IPSec Authentication | 160 bits | HMAC-SHA-1 Cert.#A2906 | CKG, DRBG | N/A | N/A | RAM - plaintext | Zeroize at session termination | (HMAC-SHA-1, 160 bits) Used in authentication of remote access IPSec data. |
| Firmware integrity verification key | 128 bits | HMAC-SHA2- 256, ECDSA SigVer (FIPS 186-4) Cert. #A2906 | N/A | N/A | N/A | HDD - plaintext | N/A | Used to check the integrity of all firmware code (HMAC-SHA-256 and ECDSA P-256) (Note: This is not considered an SSP) |
| Public key for firmware content load test | 112 bits | RSA SigVer (FIPS 186-4) Cert. #A2906 | N/A | N/A | N/A | HDD - plaintext | N/A | Used to authenticate firmware and content to be installed on the firewall (RSA 2048 with SHA-256) |
| CO, User, RA VPN Password | N/A | SHA2-256 Cert.#A2906 | External | Encrypted via SSH or TLS | N/A | HDD - a password hash (SHA2-256) | Zeroize Service | Authentication string with a minimum length of eight (8) characters. |
| Protocol Secrets | N/A | N/A | N/A | Encrypted via IPSEC, SSH or TLS | N/A | HDD/RAM – plaintext | Zeroize Service | Secrets used by RADIUS or TACACS+ (8 characters minimum) |
| Entropy Input String | 256 bits | CKG (vendor affirmed), Counter DRBG | Entropy as per | N/A | N/A | RAM - plaintext | Power cycle | Entropy input string coming from the entropy source |

| | | Cert. #A2906 | SP 800-90B | | | | | Input length = 384 bits |
|------------------------------------|---------------------|---|------------------------------------|--------------------------|-----|------------------------|-----------------|--|
| DRBG Seed | 256 bits | CKG (vendor affirmed), Counter DRBG Cert. #A2906 | Entropy as per SP 800-90B | N/A | N/A | RAM - Plaintext | Power cycle | DRBG seed coming from the entropy source Seed length = 384 bits |
| DRBG Key | 256 bits | CKG (vendor affirmed), Counter DRBG Cert. #A2906 | Entropy as per SP 800-90B | N/A | N/A | RAM - plaintext | Power cycle | AES 256 CTR DRBG state Key used in the generation of a random values |
| DRBG V | 128 bits | CKG (vendor affirmed), Counter DRBG Cert. #A2906 | Entropy as per SP 800-90B | N/A | N/A | RAM - plaintext | Power cycle | AES 256 CTR DRBG state V used in the generation of a random values |
| SNMPv3 Authentication Secret | N/A | KDF SNMP Cert. #A2906 | N/A | Encrypted via TLS/SSH | N/A | HDD/RAM – plaintext | Zeroize Service | Used to support SNMPv3 services (Minimum 8 characters) |
| SNMPv3 Privacy Secret | N/A | KDF SNMP Cert. #A2906 | N/A | Encrypted via TLS/SSH | N/A | HDD/RAM – plaintext | Zeroize Service | Used to support SNMPv3 services (Minimum 8 characters) |
| Authentication Key | 160 bits minimum | HMAC-SHA-1 HMAC-SHA2- 224 HMAC-SHA2- 256 HMAC-SHA2- 384 HMAC-SHA2- 512 Cert.#A2906 | KDF SNMP | N/A | N/A | HDD/RAM - Plaintext | Zeroize Service | HMAC-SHA-1/224 /256/384/512 Authentication protocol key (160 bits) |
| Session Key | 128 bits minimum | AES-CFB128 Cert. #A2906 | KDF SNMP | N/A | N/A | HDD/RAM - Plaintext | Zeroize Service | Privacy protocol encryption key (AES 128 CFB) |

Note: SSPs are implicitly zeroized when power cycling and explicitly zeroized when using the zeroize service.

Table 11 - Non-Deterministic Random Number Generation Specification

| Entropy Source | Minimum number of bits of entropy | Details | | | | | |
|--|--------------------------------------|---|--|--|--|--|--|
| Palo Alto Networks DRNG Entropy Source | 256 bits | ESV Cert. #E68, E70, E71, E72, E73 Entropy source provides full entropy, which is provided in the 384 bit seed. | | | | | |
| AMD Random Number Generator | 256 bits | ESV Cert. #E27 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy. | | | | | |
| Octeon III Entropy Source | 256 bits | ESV Cert. #E128 When initialized per Section 11, the DRBG is seeded with 256 bits of entropy. | | | | | |

10. Self-Tests

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

Pre-operational Self-Tests

Pre-operational Firmware Integrity Test

• Verified with HMAC-SHA-256 and ECDSA P-256

Note: the ECDSA and HMAC-SHA-256 KATs are performed prior to the Firmware integrity test

Conditional self-tests

Cryptographic algorithm self-tests

- AES 128-bit ECB Encrypt Known Answer Test*
- AES 128-bit ECB Decrypt Known Answer Test *
- AES 128-bit CMAC Known Answer Test*
 *Note: Supported by the module cryptographic implementation, but only utilized for CAST
- AES 256-bit GCM Encrypt Known Answer Test
- AES 256-bit GCM Decrypt Known Answer Test
- AES 192-bit CCM Encrypt Known Answer Test
- AES 192-bit CCM Decrypt Known Answer Test
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Sign Known Answer Test
- RSA 2048-bit PKCS#1 v1.5 with SHA-256 Verify Known Answer Test
- RSA 2048-bit Encrypt Known Answer Test
- RSA 2048-bit Decrypt Known Answer Test Note: RSA Encrypt/Decrypt are only used for self-tests
- ECDSA P-256 with SHA-512 Sign Known Answer Test
- ECDSA P-256 with SHA-512 Verify Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- DRBG SP 800-90Arev1 Instantiate/Generate/Reseed Known Answer Tests
- SP 800-90Arev1 Instantiate/Generate/Reseed Section 11.3 Health Tests
- SP 800-56Ar3 KAS-FFC-SSC 2048-bit Known Answer Test
- SP 800-56Ar3 KAS-ECC-SSC P-256 Known Answer Test
- SP 800-135rev1 TLS 1.2 with SHA-256 KDF Known Answer Test
- SP 800-135rev1 SSH KDF with SHA-256 Known Answer Test
- SP 800-135rev1 IKEv2 KDF with SHA-256 Known Answer Test
- SP 800-90B RCT/APT Health Tests on Entropy Source Note: The SP 800-90B Health Tests are implemented by the entropy source.

Conditional Pairwise Consistency Self-Tests

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

Conditional Firmware Load test

• Firmware Load Test - Verify RSA 2048 with SHA-256 signature on firmware at time of load

Conditional Critical Functions Tests

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

Error Handling

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

Table 12 - Errors and Indicators

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

11. Life-Cycle Assurance

The module does not have any specific maintenance requirements. For details regarding the secure installation, initialization, startup, and operation of the module, see section "Modes of Operation".

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

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-3 Level 2 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 each power cycle.
- 4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
- 5. Data output is inhibited during power-up self-tests, zeroization and error states.
- 6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- 7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- 8. The module maintains separation between concurrent operators.
- 9. The module does not support a maintenance interface or role.
- 10. The module does not have any external input/output devices used for entry/output of data.
- 11. The module does not enter or output plaintext CSPs.
- 12. The module does not output intermediate key generation values.

Vendor imposed security rules

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

- The operator shall not enable TLSv1.0 or use RSA for key wrapping; it is disabled by default

 Checked via CLI using "show shared" command
- 2. The operator should not enable TLSv1.3, it is disabled by default.
 - a. Checked via CLI using "show profiles" command
- 3. For devices supporting AMD entropy (PA-5410/5420/5430), a minimum system uptime of 273 hours shall pass before the module can be used to ensure proper instantiation of the DRBG.
 - a. Verify uptime via the following command: "show system info | match uptime"
 - b. After this time, the server certificate (i.e. CA Certificate with Public/Private keys) and SSH Host Keys shall be regenerated using the following procedure:
 - i. Login via CLI and issue the following commands:
 - 1. set deviceconfig system ssh profiles mgmt-profiles server-profiles <Name> default-hostkey

key-type <RSA/ECDSA> <Key Size>

- 2. set deviceconfig system ssh regenerate-hostkeys mgmt key-type <RSA/ECDSA> key-length <Key Size>
- 3. set deviceconfig system ssh mgmt server-profile <Name>
- 4. commit (Once complete, exit configure state)
- 5. set ssh service-restart mgmt
- ii. Login via WebUI and create a new certificate chain
 - 1. Create new certificates via Device > Certificate Management > Certificates
 - 2. Navigate to Device > Setup > Management > General Settings > Click the gear icon
 - a. Select "SSL/TLS Service Profile" and create a new profile with the certificates generated in previous step
 - b. Click OK and commit the configuration
- 4. For devices with Octeon III entropy used/present (e.g. PA-220/PA-220R/PA-3200/PA-5200/PA-7000 series), a minimum system uptime of 1 hour shall pass before the module can be used to ensure proper instantiation of the DRBG.
 - a. Verify uptime via the following command: "show system info | match uptime"
 - b. After this time, the server certificate (i.e. CA Certificate with Public/Private keys) and SSH Host Keys shall be regenerated. See Rule 3b above for procedure required
- 5. If using RADIUS, it must be configured using TLS.
 - a. Checked via CLI using "show shared" command
- 6. If using TACACS+, configure the service route via an IPSec tunnel, and ensure the TACACS+ server is configured for a minimum password length of eight (8) characters or greater.
 - a. Checked via CLI using "show deviceconfig" command

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

b.

12. Mitigation of Other Attacks

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

13. Definitions and Acronyms

API – Application Programming Interface App-ID – Application Identification - Palo Alto Networks' ability to identify applications and apply security policy based on the ID rather than the typical port and protocol-based classification. BGP - Border Gateway protocol - Dynamic routing protocol CA – Certificate authority Content-ID - Content Identification - Palo Alto Networks' threat prevention features including Antivirus, Antispyware, and Intrusion Prevention. CO - Cryptographic Officer DLP - Data loss prevention Gbps - Gigabits per second HA – High Availability HSCI - High Speed Chassis Interconnect IKE - Internet Key Exchange IP – Internet Protocol **IPSec - Internet Protocol Security** LDAP - Lightweight Directory Access Protocol LED - Light Emitting DiodeOCSP - Online Certificate Status Protocol OSPF – Open Shortest Path First – Dynamic routing protocol

PAN-OS - Palo Alto Networks' Operating System QoS - Quality of Service QSFP - Quad Small Form-factor Pluggable RA VPN - Remote Access Virtual Private Network RIP - Routing Information Protocol - Dynamic routing protocol RJ45 - Networking Connector RNG -Random number generator S-S VPN - Site to site Virtual Private Network SFP - Small Form-factor Pluggable Transceiver SSL - Secure Sockets Layer TLS - Transport Layer Security USB - Universal Serial Bus User-ID – User Identification – Palo Alto Networks' ability to apply security policy based on who initiates the traffic rather than the typical IP-based approach. VPN - Virtual Private Network XML - Extensible Markup Language

14. Reference Documents

FIPS 140-3 - FIPS Publication 140-3 Security Requirements for Cryptographic Modules Palo Alto Networks Administrator's Guide : https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-2/pan-os-admin/pan-os-admin.pdf

Appendix A - PA-220 - FIPS Accessories/Tamper Seal Installation (6 Seals)

- 1. Place the firewall upside down on a flat Electrostatic Discharge (ESD) protected surface and ground yourself by touching a metal surface on the firewall.
- 2. Slide the firewall into the physical chassis cover and attach it to the cover using a Phillips-head screwdriver to tighten four (4) captive screws (two (2) screws on each side of the cover).



- 3. Install the front (network, management, and console) cables (you cannot access the front ports after you complete the front-cover install described in the following steps).
- 4. Place the physical front cover onto the physical chassis cover and attach it using four (4) #4-40 x .25" screws (two (2) screws on each side of the cover).



5. Route the front-port cables through the front-cover cable-guide openings.



6. Attach the physical front-cover panel to the FIPS front cover by sliding the two (2) panel tabs under the physical chassis cover and then attach the panel using two (2) #4-40 x .25" screws.



7. Apply a tamper-evident seal to each location shown in the following illustration (six (6) seals total). After all seals are applied, place the firewall right-side up.



Appendix B - PA-220R- FIPS Accessories/Tamper Seal Installation (5 Seals)

1. Place three tamper-evident seals on the top of the module.



2. Place two tamper-evident seals on the bottom of the module.



Appendix C - PA-800 series - FIPS Accessories/Tamper Seal Installation (11 Seals)

1. Place the firewall on a flat Electrostatic Discharge (ESD) protected surface and ground yourself by touching a metal surface on the firewall.

2. Place the physical back cover onto the back of the firewall and attach it using four #4-40 x 5/16 screws (two screws on each side of the back cover).



- 3. Insert the front (network, management, and console) cables in to the front ports.
- 4. Place the physical front cover onto the front of the firewall and place the rack-mount brackets over the holes on the front cover. Attach the front cover and rack-mount brackets to the firewall using eight (8) #6-32 x 5/16" rack-mount bracket screws (shipped with the firewall)—use four (4) screws on each side. Route the front cables through the front-cover cable-guide opening.



5. Apply a tamper-evident seal to each location shown in the following illustrations (eleven (11) seals total). The seal placement over the power supply of the PA-820 firewall and PA-850 firewall is slightly different as shown.







Appendix D – PA-3200 Series – FIPS Accessories/Tamper Seal Installation (19 Seals)

1. Install the back cover to the back of the firewall



2. Attach the bracket to the firewall that will be used. Note: The firewall can use a mid-mount, front-mount or four-post mount. All seal placement is the same for the various use cases.



Front-Mount Install

Four-Post Rack Kit Install



3. Place 19 tamper seals on the module. Note: Tamper seal placement is the same for all mount types. Seal #16 is required only for the front-mount of four-post rack installations. It is not required for the mid-mount installation



Appendix E - PA-5200- FIPS Accessories/Tamper Seal Installation (28 Seals)

- 1. Place the firewall upside down on a flat Electrostatic Discharge (ESD) protected surface and ground yourself by touching a metal surface on the firewall.
- 2. Install power cables: plug the power cords into the power inlets located on the back of the firewall and connect the ground lug and ground cable to the ground lug bolts (you cannot access these back ports after you attach the FIPS back cover).
- **3.** Place the physical back cover onto the back of the firewall and attach it to the firewall using four (4) #8-32 x 1/4" screws (two (2) screws on each side of the cover). Route the power cables through the back-cover cable-guide openings.



4. Attach the physical back-cover panel to the physical back cover using four (4) #4-40 x 1/4" screws (one (1) screw on each side of the cover and two (2) screws on the back of the cover).



 Place the physical front cover onto the front of the firewall and place the rack-mount brackets over the holes on the front cover. Attach the front cover and rack-mount brackets to the firewall using eighteen (18) #8-32 x 5/16" screws (shipped with the firewall)—use nine (9) screws on each side.



6. Apply a tamper-evident seal to each location shown in the illustrations (28 seals).





Appendix F - PA-7050 - FIPS Accessories/Tamper Seal Installation (24 Seals)

1. Attach front right rack mount brackets in 4-post rack position. Do not attach rear rack mount brackets. Note that brackets are rotated 180 degrees, so the screw holes line up and the rack mount holes are now on the front of the chassis.



2. Align the right plenum bracket with five (5) open screw holes. Attach air plenum brackets using five (5) of the remaining bracket screws as shown. Repeat for the left side.

3. Attach bottom plenum to the front right rack mount bracket. Place only the middle two (2) screws.

4. Attach the bottom plenum to the rearward right plenum bracket.

5. Rotate PA-7050 chassis clockwise 90 degrees onto the bottom plenum.

6. Assemble top plenum and cable guide hardware.

7. Attach top plenum to the front left rack mount bracket

8. Attach front opacity shield using the four (4) captive screws

9. Attach top plenum to the rearward left plenum bracket along with plenum's rear opacity shield as shown

10. Loosen four (4) screws on the panel containing the power supply vent. Insert the power supply vent opacity shield and tighten screws.

11. Facing the front of the module, affix two (2) seals to top of the front opacity shield, one (1) near left edge and one (1) near the right edge. Ensure the seals, when placed, overlap onto the top of the plenum, as shown. (2 total)

12. Facing the front of the module affix one (1) seal centered to the bottom of the front opacity shield to the bottom air plenum, as shown. (1 total)

13. Facing the rear of the module, affix two (2) seals to top of the rear opacity shield, one (1) near left edge and one (1) near the right edge. Ensure the seals, when placed, overlap onto the top of the plenum, as shown.(2 total)

- 14. Facing the rear of the module;
 - A. Affix one (1) seal to the top plenum/opacity shield, covering the left and right outermost screws, as shown.
 - B. Affix one (1) seal to the left and right edge of the top plenum bracket folding over the outer edge of the module, as shown.
 - C. Affix one (1) seal to the top of each rear panel (three (3). Ensure that the seals lap onto the top rear plenum brackets, as shown.

(7 total)

- 15. Facing the rear of the module,
 - A. Affix one (1) seal to the bottom of each rear panel (three (3). Ensure that the seals laps onto the bottom rear plenum brackets, as shown.

- B. Affix one (1) seal to the left and right edge of the bottom plenum bracket folding over the outer edge of the module, as shown.
- C. Affix one (1) seal to the bottom plenum's rear side and the bottom plenum rear bracket.

(6 total)

16. Facing the rear of the module;

- Affix one (1) seal to cover one (1) screw for each power switch, as shown.
- Affix one (1) seal to the top and bottom of the vent opacity shield, as shown. Please ensure that the captive screw is covered.

(6 total)

Appendix G - PA-7080 - FIPS Accessories/Tamper Seal Installation (10 Seals)

1. Using the supplied screws attach the Cable Manager Kit with upper opacity lip to the front of the PA-7080, as shown.

2. Using the supplied screws, attach the Left and Right Front Cover brackets to the sides of the PA-7080, as shown.

3. Using the supplied screws attach front opacity shield to the PA-7080 as shown.

4. The final assembly for the PA-7080 with the physical kit is as shown.

- 5. Facing the front of the PA-7080:
 - A. Affix one (1) seal to the front and center of the exhaust fan tray. Ensure the seal overlaps the seam with the front PA-7080 branding panel as shown. (1 total)
 - Affix one (1) seal to the left and right outer edge of mounting flanges for the front opacity shield. Seals should fold over the edge of the cover flange and mounting bracket onto the side of the PA-7080. (2 total)
 - C. Affix one (1) seal to the front and center of the air intake fan tray. Ensure the seal overlaps the seam with the PA-7080 electrostatic discharge port panel as shown. (1 total)

- 6. Facing the rear of the PA-7080;
 - D. Affix one (1) seal to the left and right outer edge of the upper back panel. Seals should be placed just below the rear exhaust vent as shown. Seals should wrap around onto the sides of the PA-7080 (2 total).
 - E. Affix one (1) seal to the left and right outer edges of each power entry module as shown. Seals should wrap around onto the sides of the PA-7080 (4 total).

Appendix H - PA-5450 FIPS Accessories/Tamper Seal Installation (12 Seals)

The PA-5450 requires twelve tamper seals. Follow the directions below to install the physical kit. Affix 7 seals at the locations on the rear of the device:

On the top cover of the module, place one seal at the following location:

Affix the front opacity shield to the front of the device and screw into the locations as below:

Finalize the process by adding four seals at the following locations to secure the screws:

| | 0 | | palor Pates as a 0000 | Palosito Pauso na Base anc | * | A paloatro Vice m O O O O m | | PA-5400 | 0 0 | |
|----------------|---|---|-----------------------------|----------------------------------|----------|--|--|---------|-----|---------------|
| → 11 | | _ | | _ | | _ | | _ | | ↓ 9 |
| | | | | | | | | | | |
| → 12 | C | | | | | | | | 1 | ← |

Appendix I - PA-410 FIPS Accessories/Tamper Seal Installation (4 Seals)

The PA-410 requires four tamper labels. The placement of these seals are needed in the following areas. Affix one seal to the front of the module that connects to the top/bottom.

The left and right side of the module requires one seal each in the same location, as noted in the following area. This wraps to the top and bottom of the module. The last seal is placed on the rear side of the module, and wraps to the top and bottom of the module.

Appendix J - PA-440/450/460 FIPS Accessories/Tamper Seal Installation (4 Seals)

The PA-440/450/460 require four tamper labels that are placed at the same location as the modules have the same enclosure. Affix four seals on the rear of the module as shown below:

Appendix K - PA-3400 Series FIPS Accessories/Tamper Seal Installation (11 Seals)

The PA-3400 series require 12 tamper labels that are placed at the same location on all devices in the series. Affix 12 seals on the module as shown below in the diagrams:

Appendix L - PA-5400 Series FIPS Accessories/Tamper Seal Installation (11 Seals)

The PA-5400 series requires 11 tamper labels. The location of the tamper labels placement is the same for all models in the series. Affix 11 seals on the module as shown below in the diagrams:

