Palo Alto Networks

GlobalProtect App

FIPS 140-2 Non-Proprietary Security Policy

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: March 10, 2021

Table of Contents

Module Overview

The GlobalProtect App is a software multi-chip standalone cryptographic module that runs on a commercially available operating system and provides security for mobile users. The module is capable of running on the following platforms with the following version.

Table 1 - Module Version

Operating Environment	Tested Configuration	GlobalProtect App Version
Microsoft Windows 10 Enterprise with Intel i7 CPU with and without PAA	Dell Precision 5520	5.1.4
macOS Mojave 10.14 with Intel i5 CPU with and without PAA	Apple Macbook Pro	5.1.4

Figure 1 demonstrates the logical boundary of the cryptographic module.

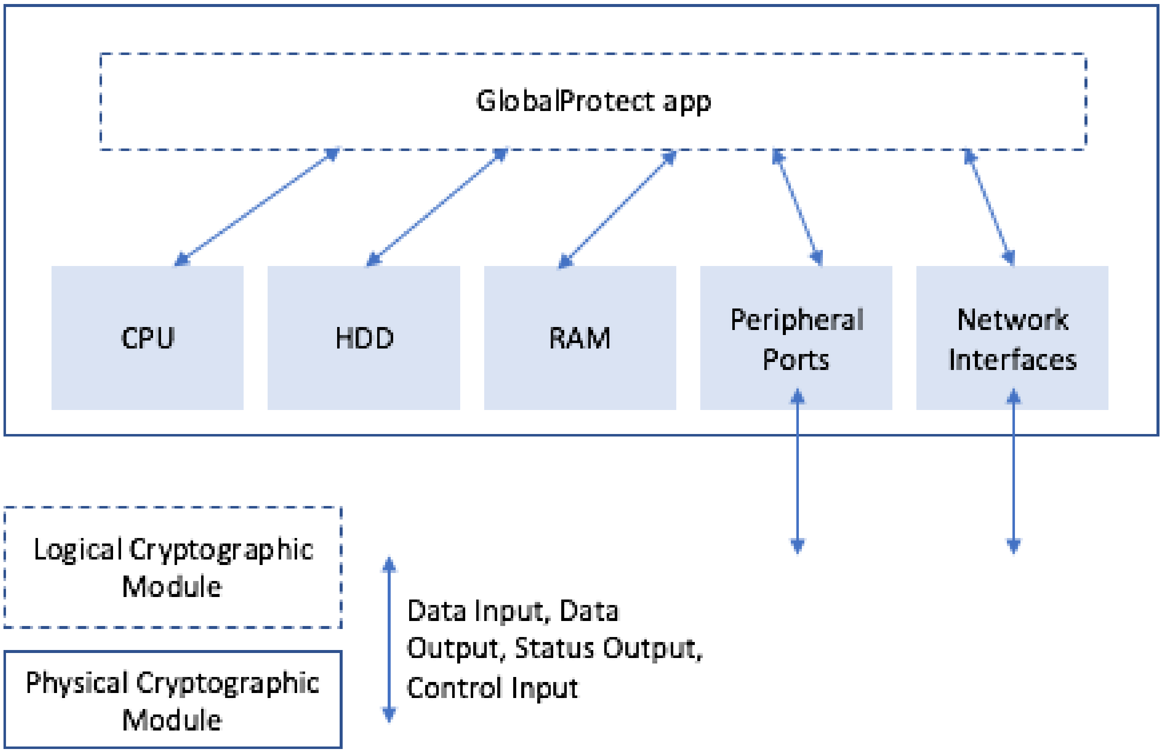
GlobalProtect app
CPU
HDD
RAM
Peripheral Ports
Network Interfaces
Logical Cryptographic Module
Physical Cryptographic Module
Data Input, Data Output, Status Output, Control Input

Figure 1 - Cryptographic Boundary

Security Levels

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services, Authentication	1
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
Overall Module Security Level	**1**

Modes of Operation

Approved Mode of Operation

The module supports an Approved mode of operation (FIPS-CC mode) and non-Approved mode (non-FIPS-CC mode). When the module is first installed, it must be placed in FIPS-CC mode as the first action and shall not be disabled. If the module is to be taken out of FIPS-CC mode, it must first be uninstalled and then reinstalled without following the procedures below. The following procedures provide detail on how to complete the module's setup into FIPS-CC mode for Windows or macOS. For details regarding downloading the software, see the Operational Environment section below. After it has been downloaded, use the GlobalProtect Installer (macOS) or GlobalProtect Setup Wizard (Windows 10) to complete installation.

Windows 10

For the GlobalProtect App running on Windows, you must first enable FIPS mode on the Windows device using the following steps:

- Launch Command Prompt
- Enter regedit to open the Windows Registry
- In the Windows Registry, go to: HKEY_LOCAL_MACHINES\System\ConcurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\
- Right-click the Enabled registry value and then select Modify…
- To enable FIPS mode, set the Value Data to 1. The default value of 0 indicates that FIPS mode is disabled
- Click OK, and then restart the endpoint

Once Windows has been placed into FIPS mode, complete the process by performing the following steps:

- launch the Command Prompt
- Enter regedit to open the Windows Registry
- In the Windows Registry, go to: HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
- Click Edit and then select New > String Value
- When prompted, set the Name of the new registry value to enable-fips-cc-mode
- Right-click the new registry and then select Modify…
- To enable FIPS-CC mode, set the Value Data to yes
- Click OK
- Restart the GlobalProtect App service
    - Launch the Command Prompt
    - Enter services.msc to open the Windows Services manager
    - From the Services list, select PanGPS
    - Restart the service

The module will display the following message in the About section following the service restart: "FIPS-CC Mode Enabled".

macOS

For the GlobalProtect App running on macOS, complete the steps below. To enable FIPS-CC mode for the GlobalProtect App, your macOS endpoint must be FIPS 140-2 compliant. By default, FIPS mode for the Mac operating system is automatically enabled on endpoints running macOS 10.8 and later releases.

- Launch a plist editor, such as Xcode.
- In the plist editor, open the following plist file: /Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist
- Locate the GlobalProtect App Settings dictionary: /Palo Alto Networks/GlobalProtect/Settings
    - Note: If the Settings dictionary does not exist, create it. You can add each key to the Settings dictionary as a string

- Enable FIPS-CC mode for the GlobalProtect App by adding the following key-value pair in the Settings dictionary:

  ```
  <key>enable-fips-cc-mode</key>
  <string>yes</string>
  ```

- Restart the GlobalProtect App service by one of the following methods:
  - Reboot your endpoint
    - Launch Finder
    - From the Finder sidebar, select Applications
    - Open the Utilities folder
    - Open Activity Monitor
    - Stop the PanGPS service
  - Restart the GlobalProtect App application and GlobalProtect App service (PanGPS)
    - Launch Terminal
    - Execute the following commands:

```
username>$ launchctl unload -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl unload -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist
```

Approved and Allowed Algorithms

The module supports the following algorithms FIPS approved algorithms.

Table 3 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES [FIPS 197, SP 800-38A]: Functions: Encryption, Decryption ECB, CBC, *GMAC, CTR modes; Encrypt/Decrypt; 128, *192 and 256-bit	C1544
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128, *192, and 256-bit Note: GCM IV handling is compliant with FIPS IG A.5 and SP 800-38D.	C1544
CVL: KDF, Application Specific [SP 800-135] -TLS 1.2 with hashes SHA-256, SHA-384, and SHA-512	C1544
DRBG [SP 800-90A]: Prediction resistance enabled CTR DRBG (AES): Derivation function enabled *HMAC DRBG, no reseed with hashes SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 *HASH DRBG with hashes SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	C1544
*Diffie-Hellman Exchange [SP 800-56A] - KAS-FFC Component with hashes SHA-224 and SHA-256	C1544

*DSA [FIPS 186-4] - Key Generation: 2048 bits	C1544
ECDSA [FIPS 186-4] - Key Pair Generation P-224, P-256, P-384, and P-521 - PKV P-224, P-256, P-384, and P-521 - *Signature Generation Component P-224, P-256, P-384 and P-521 - Signature Generation P-224, 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	C1544
Elliptic Curve Diffie-Hellman Exchange [SP 800-56A] -ECC CDH primitive (5.7.1.2) Curves: P-224, P-256, P-384, P-521	C1544
Elliptic Curve Diffie-Hellman Exchange [SP 800-56A] -KAS-ECC Curves: P-224, P-256, P-384, P-521 with hashes SHA-224, SHA-256, SHA-384, and SHA-512	C1544
HMAC [FIPS 198] - HMAC-SHA-1 with λ=160 - *HMAC-SHA-224 with λ=224 - HMAC-SHA-256 with λ=256 - HMAC-SHA-384 with λ=384 - *HMAC-SHA-512 with λ=512	C1544
KTS [SP 800-38F Section 3.1]: Option 1: AES-CBC (128 or 256 bit) plus HMAC Option 2: AES-GCM (128 or 256 bit) (Key establishment; for both listed options, key establishment methodology provides 128 or 256 bits of encryption strength)	C1544
RSA [FIPS 186-4]: - Signature Generation (ANSI X9.31): 2048, 3072, 4096 bits with hashes SHA-256, SHA-384, and SHA-512 - Signature Generation (PKCS1_v1.5): 2048, 3072, 4096 bits with hashes *SHA-224, SHA-256, SHA-384, and SHA-512 - Signature Generation (RSASSA-PSS): 2048, 3072, 4096 bits with hashes *SHA-224, SHA-256, SHA-384, and SHA-512 - Signature Verification (ANSI X9.31): *1024, 2048, 3072, 4096 bits with hashes SHA-1, SHA-256, SHA-384, and SHA-512 - Signature Verification (PKCS1_v1.5): *1024, 2048, 3072, 4096 bits with hashes SHA-1, *SHA-224, SHA-256, SHA-384, and SHA-512 - Signature Verification (RSASSA-PSS): *1024, 2048, 3072, 4096 bits with hashes SHA-1, *SHA-224, SHA-256, SHA-384, and SHA-512 *Note: The use of 4096 bit keys in FIPS-CC mode is vendor affirmed*	C1544
SHS [FIPS 180-4] - Hashes: SHA-1, *SHA-224, SHA-256, SHA-384, SHA-512 - Usage: Digital Signature Generation & Verification, Non-Digital Signature Applications (e.g., component of DRBG and HMAC)	C1544

*Denotes algorithms that were CAVS tested, but are not used.

The module is compliant to IG A.5: GCM is used in the context of TLS, IPsec:

- For TLS, the GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 3.2 of RFC 5289 for TLS key establishment.
  (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, the GCM implementation meets Option 2 of IG A.5: Approved DRBG is used to generate at least 96-bit IVs for each and every encryption operation.

During operational testing, the module was tested against independent versions of TLS and IPsec and found to behave correctly (i.e., connection establishes successfully).

Table 4 - Supported Protocols in the Approved Mode

Supported Protocols
TLS 1.2*
IPSec**

(*) No parts of this protocol, other than the KDF, have been tested by the CMVP and CAVP
(**) The module includes IPsec, but IKE and the IKE KDF are not supported

Non-Approved, Non-Allowed Algorithms

The GlobalProtect App supports the following non-Approved algorithms in the non-Approved mode.

Table 5 – Non-Approved, Non-Allowed Algorithms

Non-FIPS Algorithms in Non-Approved Mode
Encrypt/Decrypt: Camellia, CHACHA, Triple-DES (non-compliant), SEED, RC4, IDEA
Hashing: MD5
Message Authentication: HMAC-MD5
Diffie-Hellman

Ports and Interfaces

The module's physical ports and interfaces are described in the table below:

Table 6 - Module Ports and Interfaces

Interface	Logical Interface
Data Input	API Input Parameters
Data Output	API Output Parameters
Power Input	None
Control Input	API Function Calls
Status Output	API Return Calls

Roles, Services, and Authentication

The module supports a single instance of the two authorized roles: The Crypto-Officer and User.
The module does not provide a maintenance role or bypass capability. The module does not implement any authentication.

Table 7 - Roles and Required Identification and Authentication

Role	Description
Crypto-Officer	This role has access to all services as noted in Table 10.
User	This role has access to all services as noted in Table 10.

The module contains the following CSPs and Public Keys:

Table 8 - Private Keys and CSPs

CSP #	Key Name	Type	Description
1	RSA Private Keys	RSA	RSA Private key used for authentication, and signature generation (RSA 2048, 3072, or 4096 bits)
2	ECDSA Private Keys	ECDSA	ECDSA Private key used for authentication, and signature generation (P-224, P-256, P-384 or P-521)
3	TLS ECDHE Private Components	ECDH	ECDHE private component used in key agreement (P-256, P-384, P-521)
4	TLS Pre-Master Secret	N/A	Value used during TLS handshake for session negotiation
5	TLS HMAC Keys	HMAC	HMAC keys used in TLS connections (SHA-1, SHA-256 and SHA-384) (key size >= block size)

6	TLS Encryption Keys	AES	AES keys used in TLS connections (AES 128/256 bits GCM or CBC)
7	IPSec Authentication Keys	HMAC	HMAC-SHA-1 used for authentication (key size >= block size)
8	IPSec Session Keys	AES	Used to encrypt IPSec data AES CBC (128 bits) AES GCM (128 or 256 bits)
9	DRBG Seed, State, Input String	DRBG	Values used in the generation of a random value. V (128 bits) and Key (128/192/256 bits)

Table 9 - Public Keys

	Key Name	Description
A	CA Certificates	Used to extend trust for certificates (ECDSA – P-256/384/521) (RSA – 2048/3072/4096 bits)
B	ECDSA Public Keys	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, and peer authentication. (ECDSA P-224, 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, and peer authentication. (RSA 2048, 3072, or 4096 bits)
D	TLS ECDHE Public Components	ECDHE public component used in key agreement (P-256, P-384 and P-521)
E	Software Integrity Verification Key	HMAC-SHA-1 used to verify the integrity of the module during power-up

Table 10 - Services

Service	Description	Crypto-Officer Access	User Access
Show Status	Provides information regarding the system status	Y	Y
Self-Test	Perform on-demand self-tests.	Y	Y
Security Configuration Management	Configure the module with necessary setup details to support VPN tunnel establishment.	Y	Y
VPN Tunnel	Creates an SSL/IPsec VPN tunnel.	Y	Y
Zeroize (Uninstall)	All CSPs are zeroized.	Y	Y

CSP Access Table

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 the following:

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g., the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module (persistent storage)
Z = Zeroize: The module zeroizes the CSP.

Table 11 - CSP/Public Key Access Rights

Service \ CSP	RSA Private Keys	ECDSA Private Keys	TLS ECDHE Private Components	TLS Pre-Master Secret	TLS HMAC Keys	TLS Encryption Keys	IPSec Authentication Keys	IPSec Session Keys	DRBG Seed, State, Input String	CA Certificates	ECDSA Public Keys	RSA Public Keys	TLS ECDHE Public Components	Software Integrity Verification Key
Show Status	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Self-Test	-	-	-	-	-	-	-	-	-	-	-	-	-	R
Security Configuration Management	W	W	WE	WE	WE	GWE	-	-	E	RW	RW	RW	-	-
VPN Tunnel	E	E	WE	WE	WE	GWE	GWE	GWE	E	R	R	R	R	-
Zeroize (Uninstall)	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

Operational Environment

The module has a modifiable operational environment, and was tested on the following environments operating on a general-purpose computing platform.

Microsoft Windows 10 Enterprise with Intel Core i7 (Dell Precision 5520)

MacOS Mojave 10.14 with Intel Core i5 (Apple Macbook Pro)

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 entity at a time can use the cryptographic module.

To install, download the following from the Palo Alto Networks Support site (https://support.paloaltonetworks.com/), and ensure the checksum (SHA-256) is correct:

macOS: GlobalProtect-5.1.4.pkg

C5D79D8BF11077F569032569DC41D5C5DE1D14697A98E3AE3F831189785CBB1D

Windows: GlobalProtect64-5.1.4.msi

44E305B6B350FC25A80B3E97EAC50238EF7D2E2C412B01730A85CFB98A50DEA0

The module may be ported and used on other Operational Environments per IG G.5, such as (but not limited to): Windows 10 Education, Windows 10 Mobile, Windows 10 Home, and Windows 10 Pro. The module was not formally tested on other Operational Environments and the CMVP makes no statement as to the correct operation of the module or the security strength of the generated keys when ported and executed in an operational environment not listed on the validation certificate.

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 two distinct operator roles: The Crypto-Officer and User role.
2. The module supports the generation of key material using an Approved DRBG.
3. The cryptographic module performs the following tests
    A. Power up Self-Tests
        1. Cryptographic algorithm tests
            a. HMAC-SHA-1/224/256/384/512 Known Answer Test
            b. AES-128 ECB Encrypt/Decrypt Known Answer Test
            c. AES-256 GCM Encrypt/Decrypt Known Answer Test
            d. RSA 2048-bit PKCS#1 Sign/Verify Known Answer Test
            e. DRBG (CTR_DRBG) Known Answer Test

f. ECCDH (Shared secret per SP 800-56A Section 5.7.1.2, IG 9.6) Primitive “Z” Computation Known Answer Test

g. ECDSA P-224 Sign/Verify Pairwise Consistency Test

B. Software Integrity Test –verified with HMAC-SHA-1

C. Critical Functions Tests

1. N/A

D. Conditional Self-Tests

1. SP 800-90A Section 11 DRBG Health Tests
2. Continuous Random Number Generator (RNG) test
3. ECDSA Pairwise Consistency Test
4. 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 power cycling the platform.
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 (uninstall) 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 other than the ports and interfaces of the GPC on which the module operates.
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. CSPs must not be shared between Approved and non-Approved modes. When the administrator first downloads the GlobalProtect App software, they must immediately place it into FIPS-CC mode. They cannot use the GlobalProtect App in non-Approved mode and then switch it to FIPS-CC mode.
2. If the administrator wants to switch from FIPS-CC mode to non-FIPS-CC mode, they must perform a complete uninstall of the module first, and then re-install the module
3. TLS_DHE_* cipher suites shall not be used by the operator; use of this cipher suite is a violation of this Security Policy.
4. TDES shall not be used by the operator; use of this cipher in any cipher suite is a violation of this Security Policy.
5. CHACHA shall not be used by the operator; use of this cipher in any cipher suite is a violation of this Security Policy.

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 the GlobalProtect App module on any general purpose computer (GPC) or platform using the specified 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.

Physical Security

There are no physical security requirements as this is a software module.

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.