Palo Alto Networks GlobalProtect App 6 Security Target

Version: 1.0
Date: July 26, 2023

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the GlobalProtect client (GlobalProtect App 6).

The Palo Alto Networks GlobalProtect App provides users with the ability to securely communicate with their internal networks.

The focus on this evaluation is on the TOE functionality supporting the claims in the Protection Profile for Application Software.

The Security Target contains the following additional sections:

- Product Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Palo Alto Networks GlobalProtect App 6 Security Target

ST Version – Version 1.0

ST Date – July 26, 2023

TOE Identification – GlobalProtect App 6, which is available in five images (four downloadable from the Palo Alto Networks Support site), include the following:

- Windows 11
    - GlobalProtect64-6.0.7.msi
- macOS 12
    - GlobalProtect-6.0.7.pkg
- Android 12

    - global-protect-6.0.7-signed.apk
- iOS 16
    - GlobalProtect App downloaded from iTunes Store
- Linux Ubuntu 20.04
    - PanGPLinux-6.0.7.tgz

TOE Developer – Palo Alto Networks, Inc.

Evaluation Sponsor – Palo Alto Networks, Inc.

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017*

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications: This ST is conformant to:

- Protection Profile for Application Software, Version 1.4, October 7, 2021 [APPSW].
- Functional Package for Transport Layer Security (TLS), Version 1.1, March 1, 2019 [PKGTLS]

This TOE and ST are conformant to Parts 2 (extended) and 3 (extended) of Common Criteria Version 3.1, Revision 5.

The following NIAP Technical Decisions[1] apply to this APPSW, and have been accounted for in the ST development:

- TD0624 – Addition of DataStore for Storing and Setting Configuration Options
- TD0628 – Addition of Container Image to Package Format
- TD0664 – Testing activity for FPT_TUD_EXT.2.2
- TD0669 – FIA_X509_EXT.1 Test 4 Interpretation
- TD0717 – Format Changes for PP_APP_V1.4
- TD0719 – ECD for PP APP V1.3 and 1.4
- TD0743 – FTP_DIT_EXT.1.1 Selection Exclusivity
- TD0756 – Update for Platform-provided Full Disk Encryption

The TOE and ST is package-name conformant to [PKGTLS].

The following NIAP Technical Decisions apply to this PKGTLS, and have been accounted for in the ST development:

- 0442 – Updated TLS Ciphersuites for TLS package
- 0469 – Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1
    - Not Applicable: TLS server is not supported by the TOE.
- 0499 – Testing with pinned certificates
- 0513 – CA Certificate loading
- 0588 – Session Resumption Support in TLS Package
    - Not Applicable: SFRs for this are not supported by the TOE.

[1] TD0736 (HTTPS server is not supported by the TOE), TD0650 (VPN Client PP-Module is not claimed), TD0726 and TD0770 (TLS server is not supported by the TOE) are not applicable for the reasons stated.

- 0739 – PKG_TLS_V1.1 has 2 different publication dates

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example, FDP_ACC.1 (1) and FDP_ACC.1 (2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using italicized and are surrounded by brackets (e.g., [*assignment*]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold and are surrounded by brackets (e.g., [**selection**]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… some **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- The ST does not highlight operations that have been completed by the PP and EP authors.

1.3.1 Terminology

The following terms and abbreviations are used in this ST:

Remote Access VPN	Provides secure access to internal and cloud-based business applications

1.3.2 Acronyms

AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
FIA	Identification and Authentication CC Class
FIPS	Federal Information Processing Standard

FMT	Security Management CC Class
FSP	Functional Specification
HMAC	Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol (Secure)
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Security Management
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
VPN	Virtual Private Network
VPNGW	VPN Gateway

2. Product Description

The TOE is the Palo Alto Networks GlobalProtect App that provides users with the ability to access their company network resources via the Palo Alto Networks GlobalProtect Portals and Gateways that have been deployed. The TOE also provides several management functions that include, for example, allowing the endpoint user to select their desired gateway, and to collect troubleshooting logs from the TOE. Additional components that interact with the TOE are noted in the TOE Overview.

2.1 TOE Overview

The GlobalProtect App is a software program that runs on the endpoint (desktop/laptop computer) to protect users by using the same security policies that protect the sensitive resources in corporate networks. The GlobalProtect App secures the traffic using TLS and allows users to connect to corporate networks to access company's resources from anywhere in the world (e.g., when users are remote). The TOE runs on platforms identified in section 1.1.

The TOE is a software program as specified in the APPSW, which uses TLS to protect communication as defined in PKGTLS. The TOE interacts with other GlobalProtect components, which include the Palo Alto Networks GlobalProtect Portal and Gateway.

The Palo Alto Next Generation Firewall provides the GlobalProtect Portal, which provides details for the GlobalProtect infrastructure. Every client system that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the Palo Alto Next Generation Firewall GlobalProtect Gateways. The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps.

Once connected, user and host information are sent to the GlobalProtect gateway, which identifies the identity of the operator that is connecting along with details of the host via the host profile (e.g., antivirus definitions installed, security patches, etc.).

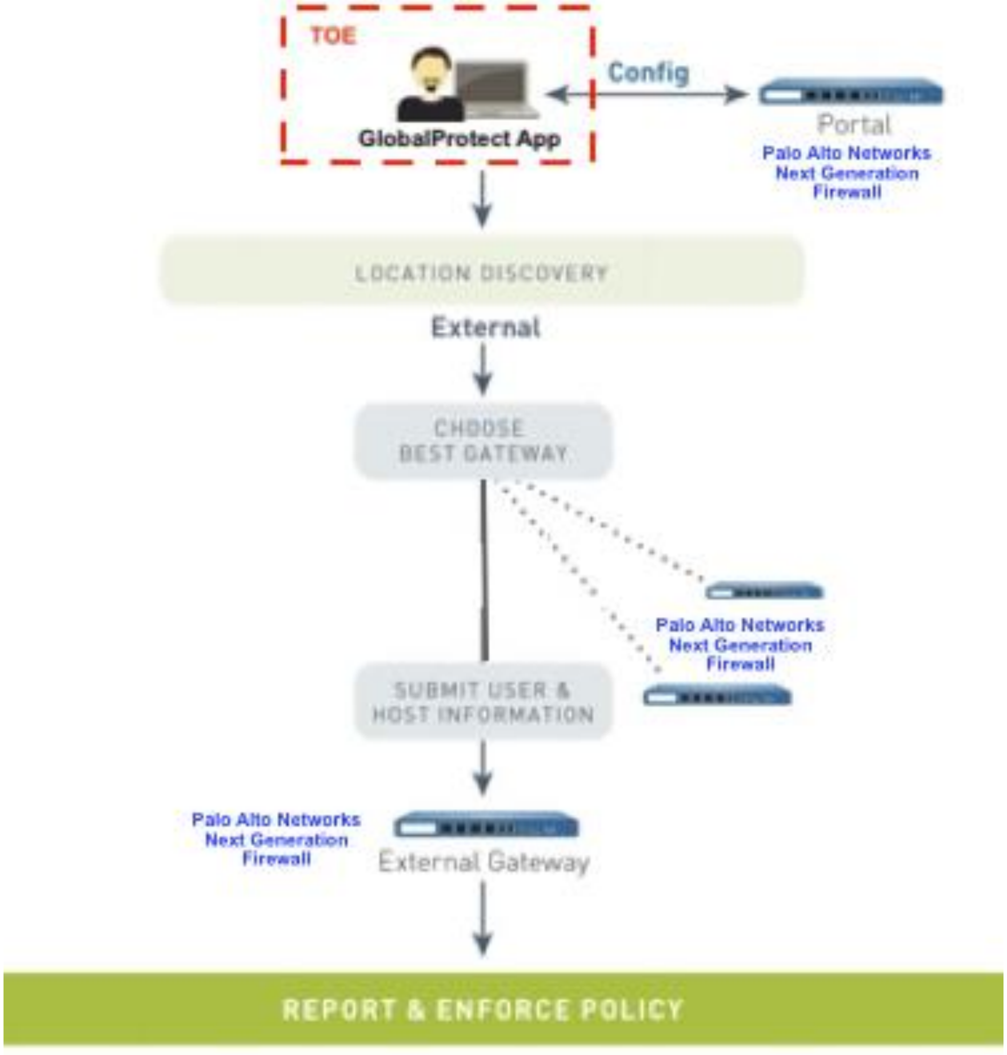
TOE
GlobalProtect App
Config
Portal
Palo Alto Networks Next Generation Firewall
LOCATION DISCOVERY
External
CHOOSE BEST GATEWAY
Palo Alto Networks Next Generation Firewall
SUBMIT USER & HOST INFORMATION
Palo Alto Networks Next Generation Firewall
External Gateway
REPORT & ENFORCE POLICY

Figure 1: TOE Deployment

.

2.2 TOE Architecture

The TOE is a software solution that is composed of items listed in Section 2.2.1 and 2.2.2. The software is available for download from the Palo Alto Networks support site.

The following diagram depicts the software architecture of the TOE.

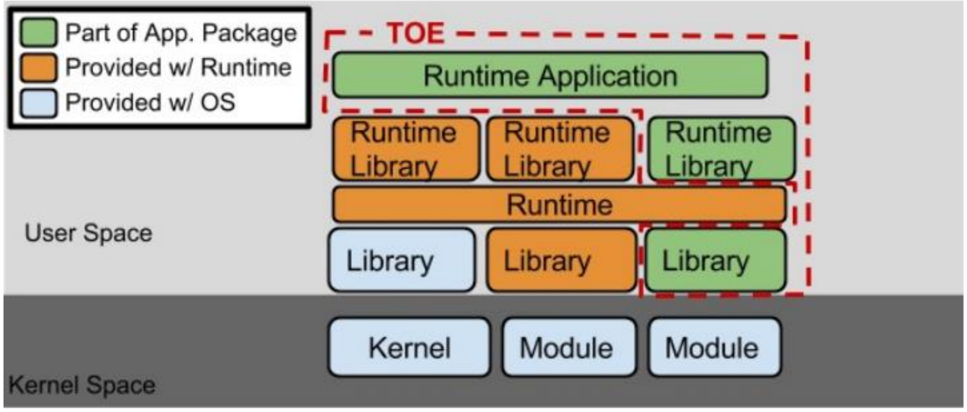

Figure 2: TOE Architecture

2.2.1 Physical Boundaries

The physical boundary of the TOE is the GlobalProtect App installed and running on a supported platform (see below).

2.2.1.1 Software Requirements

The TOE runs on desktop or mobile operating system that includes macOS 12 or later, Android 12 or later, iOS 16 or later, Linux Ubuntu 20.04 or later, or Windows 11 that communicates with a Palo Alto Networks Next Generation Firewall that utilizes PAN-OS 10.1 or later.

2.2.1.2 Hardware Requirements

The TOE must be installed on desktop/laptop/phone with operating systems identified above. The GlobalProtect Portal and Gateway reside on a Palo Alto Networks Next Generation Firewall. The Palo Alto Networks Next Generation Firewall is covered in a separate evaluation and is in the operational environment.

The TOE was installed and tested on the following platforms[2].

- HP Envy running Windows 11 – Processor: Intel Core i7-1250U (Alder Lake microarchitecture)
- MacBook Air running macOS 12 - Processor: Apple M-Series M1
- Samsung S21 Ultra running Android 12 - Processor: Qualcomm Snapdragon 888
- iPhone 12 Mini running iOS 16 – Processor: Apple A-Series A14 (Bionic)
- HP Envy running Ubuntu 20.04 – Processor: Intel Core i7-1250U (Alder Lake microarchitecture)

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels

[2] While the TOE was tested on these operating systems, the TOE will function and behave the same on later versions of the operating systems identified here. This is vendor affirmed.

2.2.2.1 Cryptographic Support

The TOE implements NIST validated cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of cryptographic protocols such as TLS. In order to utilize these features, the TOE must be configured in FIPS-CC mode.

GlobalProtect App includes algorithms that are covered by CAVP certificates that are noted in this document. In addition, the TOE also relies on the underlying platforms. **Table 3** contains information regarding all the keys included and utilized by the TOE.

2.2.2.2 User Data Protection

The TOE restricts its access to only using network connectivity when it is needed to communicate to the Palo Alto Networks Gateway or Portal. Other functionality on the host platform such as its camera, Bluetooth, USB, or microphone are not needed. The TOE does not store any sensitive data in non-volatile memory.

2.2.2.3 Identification and Authentication

The TOE authenticates the X.509 certificate of the Palo Alto Networks GlobalProtect Gateway/Portal as part of establishing a TLS connection.

2.2.2.4 Security Management

The TOE provides access to the security management features using an interface on a general-purpose computer. Security management operations are provided to the user of the TOE. A user is able to perform security management by configuring necessary items such as assigning the Palo Alto Networks GlobalProtect Portal and Gateway that the TOE will use for its connections. It also provides the user with the ability to collect troubleshooting logs, configure gateway and portal, check the current version, check for updates, and to enable/disable the transmission of information regarding the system's hardware/software or configuration. The TOE relies on the OS' network ports (i.e. ethernet ports) for communication and management capabilities.

In order to install or uninstall the TOE, the user is required to have platform administrator privileges.

2.2.2.5 Privacy

The TOE does not transmit PII over the network.

2.2.2.6 Protection of the TSF

The TOE implements a variety of functions to ensure that it is protected against corruption. These include utilizing platform APIs, memory mapping, and stack-based buffer overflow protection. Palo Alto Networks provides customers with a means of updating their TOE using trusted updates. These trusted updates are securely delivered and installed using protection mechanisms such as TLS, and by using approved digital signature methods. All these updates are properly signed using RSA 2048 with SHA-256. The trusted update site also provides a checksum of the updates that can be used for additional verification before it is utilized.

2.2.2.7 Trusted Path/Channels

The TOE protects communication between itself as the endpoint and other networks using TLS. TLS 1.2 is utilized to encrypt all data that is passed from the TOE to other components (i.e., Palo Alto Networks GlobalProtect Portals and Gateways).

2.3 TOE Documentation

Palo Alto Networks Inc. offers a series of documents that describe the installation of Palo Alto Networks GlobalProtect App as well as guidance for subsequent use and administration of the applicable security features.

For GlobalProtect App 6, these documents include the following:

- Palo Alto Networks GlobalProtect App 6 Security Target, [This document]
- Palo Alto Networks GlobalProtect App User Guide Version 6, January 24, 2023 (Last Updated)
- Palo Alto Networks GlobalProtect Administrator's Guide Version 10.1 or Later, February 22, 2023 (Last Updated)
- Palo Alto Networks Common Criteria Evaluation Configuration Guide (CCECG) GlobalProtect App 6, June 28, 2023

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumption) from [APPSW].

In general, the [APPSW] has presented a Security Problem Definition appropriate for software applications, and as such, is applicable to the TOE.

The following threats are directly from the [APPSW]:

T. NETWORK_ATTACK An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.

T.NETWORK_EAVESDROP An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

T.PHYSICAL_ACCESS An attacker may try to access sensitive data at rest.

The following assumptions are made as drawn directly from the [APPSW]:

A. PLATFORM The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

A. PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

A. PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

4. Security Objectives

The sections below identify the security objectives for the TOE and for the operational environment. These security objectives identify the responsibilities of the TOE and the operational environment in meeting security needs.

4.1 Security Objectives for the TOE

O.INTEGRITY

Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.

O.QUALITY

To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

O.MANAGEMENT

To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

O.PROTECTED_STORAGE

To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Security Objectives for the Operational Environment

OE.PLATFORM Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the following Protection Profiles (PP):

- *Protection Profile for Application Software, Version 1.4, 7 October 2021* [APPSW],
- *Functional Package for Transport Layer Security (TLS), Version 1.1 [PKGTLS]*

The SARs are the set of SARs specified in [APPSW].

5.1 Extended Requirements

All extended requirements in this ST have been drawn from the [APPSW] and [PKGTLS]. The [APPSW] and [PKGTLS] define all the extended SFRs (*_EXT.1) and since they are not redefined in this ST, the [APPSW] and [PKGSTLS] should be consulted for more information in regard to those CC extensions.

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Palo Alto TOE.

Table 1 TOE Security Functional Components

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_CKM_EXT.1 Cryptographic Key Generation Services
	FCS_CKM.1/AK Cryptographic Asymmetric Key Generation
	FCS_CKM.2 Cryptographic Key Establishment
	FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption
	FCS_COP.1/Hash Cryptographic Operation – Hashing
	FCS_COP.1/KeyedHash Cryptographic Operation – Keyed-Hash Message Authentication
	FCS_COP.1/Sig Cryptographic Operation -- Signing
	FCS_RBG_EXT.1 Random Bit Generation Services
	FCS_RBG_EXT.2 Random Bit Generation from Application
	FCS_STO_EXT.1 Storage of Credentials
	FCS_TLS_EXT.1 TLS Protocol
	FCS_TLSC_EXT.1 TLS Client Protocol
	FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication
	FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension
FDP: User Data Protection	FDP_DEC_EXT.1 Access to Platform Resources
	FDP_NET_EXT.1 Network Communications
	FDP_DAR_EXT.1 Encryption of Sensitive Application Data

Requirement Class	Requirement Component
FIA: Identification and Authentication	FIA_X509_EXT.1 X.509 Certificate Validation
	FIA_X509_EXT.2 X.509 Certificate Authentication
FMT: Security Management	FMT_MEC_EXT.1 Supported Configuration Mechanism
	FMT_CFG_EXT.1 Secure by Default Configuration
	FMT_SMF.1 Specification of Management Functions
FPR: Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	FPT_API_EXT.1 Use of Supported Services and APIs
	FPT_AEX_EXT.1 Anti-Exploitation Capabilities
	FPT_TUD_EXT.1 Integrity for Installation and Update
	FPT_TUD_EXT.2 Integrity for Installation and Update
	FPT_IDV_EXT.1 Software Identification and Versions
	FPT_LIB_EXT.1 Use of Third Party Libraries
FTP: Trusted Path/Channel	FTP_DIT_EXT.1 Protection of Data in Transit

5.2.1 Cryptographic Support (FCS)

FCS_CKM_EXT.1 – Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [

- ***implement asymmetric key generation***

].

FCS_CKM.1/AK – Cryptographic Asymmetric Key Generation

FCS_CKM.1.1/AK The **application** shall **[**

- ***implement functionality***

] to generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **[**

- ***[ECC schemes]*** *using* ***[“NIST curves” P-384 and [P-256, P-521]]*** *that meet the following:* ***[FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4]***

].

FCS_CKM.2 – Cryptographic Key Establishment

FCS_CKM.2.1 The application shall [***implement functionality***] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

[

- ***[Elliptic curve-based key establishment schemes****] that meets the following:* ***[NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]***

].

FCS_COP.1/SKC – Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC The **application** shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm **[**

- ***AES-CBC (as defined in NIST SP 800-38A) mode,***
- ***AES-GCM (as defined in NIST SP 800-38D) mode***

] and cryptographic key sizes [***128-bit, 256-bit***].

FCS_COP.1/Hash – Cryptographic Operation – Hashing

FCS_COP.1.1/Hash The **application** shall perform [*cryptographic hashing* services] in accordance with a specified cryptographic algorithm [

- ***SHA-1,***
- ***SHA-256,***
- ***SHA-384***

] and message digest sizes [

- ***160***
- ***256,***
- ***384***

] bits that meet the following: [FIPS Pub 180-4].

FCS_COP.1/KeyedHash – Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash The **application** shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [

- ***HMAC-SHA-256,***
- ***HMAC-SHA-384***]

and [

- ***HMAC-SHA-1***

] with key sizes [*160, 256, 384*] and message digest sizes [***256, 384***] and [***160***] bits that meet the following [FIPS Pub 198-1, '*The Keyed-Hash Message Authentication Code'* and FIPS Pub 180-4 '*Secure Hash Standard'*]**.**

FCS_COP.1/Sig – Cryptographic Operation – Signing

FCS_COP.1.1/Sig The **application** shall perform [*cryptographic signature services (generation and verification)*] in accordance with a specified cryptographic algorithm [

- ***RSA schemes*** *using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5],*
- ***ECDSA schemes*** *using ["NIST curves" P-256, P-384 and [**P-521**]] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6*

].

FCS_RBG_EXT.1 – Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [

- ***implement DRBG functionality***

] for its cryptographic operations.

FCS_RBG_EXT.2 – Random Bit Generation from Application

FCS_RBG_EXT.2.1 The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [***CTR_DRBG(AES)***]

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [

- ***no other noise source***

] with a minimum of [

- ***256 bits***

] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_STO_EXT.1 – Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- ***not store any credentials***

] to non-volatile memory.

FCS_TLS_EXT.1 – TLS Protocol

FCS_TLS_EXT.1 The product shall implement [

- ***TLS as a client***

].

FCS_TLSC_EXT.1 - TLS Client Protocol

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a client that supports the cipher suites [

- ***TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***

] and also supports functionality for [

- ***mutual authentication***

].

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [

- ***with no exceptions***

].

FCS_TLSC_EXT.2 - TLS Client Protocol with Mutual Authentication

FCS_TLSC_EXT.2.1 The product shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.5 - TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups [

- ***secp256r1,***
- ***secp384r1,***

].

5.2.2 User Data Protection (FDP)

FDP_DEC_EXT.1 – Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- ***network connectivity***

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- ***no sensitive information repositories***

].

FDP_NET_EXT.1 – Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- ***user-initiated communication for [connections to Palo Alto Networks Next Generation Firewall Gateways and Portals].***

].

FDP_DAR_EXT.1 – Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- ***not store any sensitive data***

] in non-volatile memory.

5.2.3 Identification and Authentication (FIA)

FIA_X509_EXT.1– X.509 Certificate Validation

FIA_X509_EXT.1.1 The application shall [***implement functionality***] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [***OCSP as specified in RFC 6960, CRL as specified in RFC 5280 Section 6.3***].
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
  - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
  - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 – X.509 Certificate Authentication

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***TLS***].

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall [***allow the administrator to choose whether to accept the certificate in these cases***].

5.2.4 Security Management (FMT)

FMT_MEC_EXT.1 – Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall [

- ***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.***

].

FMT_CFG_EXT.1 – Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [

- ***enable/disable the transmission of any information describing the system's hardware, software, or configuration***
- ***[setting gateway and portal addresses***
- ***collecting troubleshooting logs***
- ***check for updates***
- ***querying the current version of the TOE]***

]

5.2.5 Privacy (FPR)

FPR_ANO_EXT.1 – User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [

- ***not transmit PII over a network***

].

5.2.6 Protection of the TSF (FPT)

FPT_API_EXT.1 – Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_AEX_EXT.1 – Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address expect for [*no exceptions*].

FPT_AEX_EXT.1.2 The application shall [

- ***not allocate any memory region with both write and execute permissions***

].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be compiled with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 – Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [***provide the ability***] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [***provide the ability***] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [***with the platform OS, as an additional software package to the platform OS***].

FPT_TUD_EXT.2 – Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the [***format of the platform-supported package manager***].

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_IDV_EXT.1 – Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with **[*[GlobalProtect software version]*].**

FPT_LIB_EXT.1 – Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [*OpenSSL*, *OESIS*]

5.2.7 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 – Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [

- ***encrypt all transmitted [data] with [TLS as a client as defined in the Functional Package for TLS for [traffic to VPN gateway]]***

] between itself and another trusted IT product.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference to [APPSW].

Table 2 Assurance Components

Requirement Class	Requirement Component
ASE: Security Target	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives
	ASE_REQ.1 Security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance Documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
	ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability Assessment	AVA_VAN.1 Vulnerability survey

6. TOE Summary Specification

This chapter describes the security functions:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channel

6.1 Cryptographic Support

<table>
<tr>
<td>FCS_CKM_EXT.1
FCS_CKM.1/AK</td>
<td>
The GlobalProtect App itself does not generate certificates or keypairs[3]. Platform Administrators are able to set/load client or server certificates into the certificate store of the platform (i.e., keypair generated by the platform) it is running on. During a TLS handshake, the TOE utilizes ECDHE for the key establishment with NIST curves that include P-256, P-384, and P-521 that adhere to the NIST Special Publication 800-56A Revision 3.

The TOE uses the functionality provided by the platform in order to securely store X.509 certificates that are used for connections to the Palo Alto Networks GlobalProtect Gateway/Portal. The platform provides the necessary security to protect these items.

For Windows, certificates are stored within the Windows Certificate Store.
For macOS, certificates are stored within the Keychain.
For Android, certificates are stored on Keystore
For iOS, certificates are stored within the Keychain.
For Linux, certificates are stored in Linux keyrings.

The TOE's keys/credentials are noted in Table 3.

<b>Table 3 - Keys and Credentials</b>
<table>
<tr><th>Key</th><th>Description/Usage</th><th>Storage</th></tr>
<tr><td>CA Certificates</td><td>Used to extend trust for certificates
(ECDSA – P-256/384/521)
(RSA – 2048/3072/4096 bits)</td><td>OS' key store</td></tr>
<tr><td>RSA Public Keys</td><td>RSA public keys managed as certificates for the verification of signatures, establishment of TLS, and peer authentication.
(RSA 2048/3072/4096 bits)</td><td>OS' key store</td></tr>
</table>
</td>
</tr>
</table>

[3] NOTE: EC key pairs are generated by the TOE as part of the ECDHE key establishment scheme, but these ephemeral keys are not stored.

	RSA Private Keys	RSA Private key used for authentication, and signature generation (RSA 2048, 3072, or 4096 bits)	OS' key store
	ECDSA Public Keys	ECDSA public keys managed as certificates for the verification of signatures, establishment of TLS, and peer authentication. (P-256/384/521)	OS' key store
	ECDSA Private Keys	ECDSA Private key used for authentication, and signature generation (P-256, P-384 or P-521)	OS' key store
FCS_CKM.2	The TOE implements key establishment methods using elliptical curve key establishment scheme (ECDHE). The curves utilized by the TOE include P-256, P-384, and P-521 as defined in NIST SP 800-56A Revision 3. For details regarding the algorithms supported and their CAVP certificates, see **Table 4**.		
FCS_COP.1/SKC	The TOE is able to encrypt/decrypt using AES-CBC mode (as defined in NIST SP 800-38A) and AES-GCM mode (as defined in NIST SP 800-38D) with key sizes 128-bits and 256-bits. Corresponding CAVP certificates for these algorithms are present in **Table 4**.		
FCS_COP.1/Hash	The TOE uses hash functions that include SHA-1, SHA-256 and SHA-384 as defined in FIPS 180-4. The digest sizes include 160-bits, 256-bits, and 384-bits that are compliant with FIPS 180-4. The hashing capabilities are utilized for digital signature verification and generation and data integrity checks. SHA-1 is not used for generating digital signatures as noted in SP 800-131A but is only used for verification for legacy purposes. The TOE uses SHA-256 and SHA-384 hashing as part of generating digital signatures. SHA-1 is used as part of the software integrity power-up test. Corresponding CAVP certificates for these algorithms are present in **Table 4**.		
FCS_COP.1/KeyedHash	The TOE supports the use of Keyed-Hash Message Authentication algorithms that include HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384. They include key sizes of 160 bits, 256-bits, and 384-bits respectively. The HMAC-SHA functions are used as part of the TOE's integrity check (HMAC-SHA-1) to ensure that it has not been tampered and is additionally used as part of the TLS handshake (HMAC-SHA-256 and HMAC-SHA-384). Corresponding CAVP certificates for these algorithms are present in **Table 4**.		
FCS_COP.1/Sig	Both RSA and ECDSA schemes are used for TLS functions with approved key sizes. These include RSA 2048-bits, 3072-bits, and 4096-bits. For ECDSA, they include the curves P-256, P-384, and P-521. During TLS handshakes, these certificates are used for peer authentication to verify the server's identity. These certificates are also used by the TOE to present its identity as a client when connecting to a Palo Alto Networks Gateway. Corresponding CAVP certificates and the relevant schemes for these algorithms are present in **Table 4**.		
FCS_RBG_EXT.1 FCS_RBG_EXT.2	The TOE implements DRBG functionality using the CTR_DRBG in AES mode by default. The DRBG is seeded using the Intel RDSEED or source identified below, which provides a minimum of 256 bits of entropy. A description of the noise sources for the operating systems are noted below. Windows – Intel RDSEED macOS – Secure Enclave (TRNG)		

	Android – /dev/random iOS – Secure Enclave (TRNG) Linux – Intel RDSEED
FCS_STO_EXT.1	The TOE does not generate or store any credentials. All certificates and private keys are generated externally and are stored externally on the platforms.
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2 FCS_TLSC_EXT.5 FTP_DIT_EXT.1	All data that is transmitted between the GlobalProtect App and the Palo Alto Networks VPN Gateway and Portal are encrypted using TLS. When the TOE is establishing a TLS session, it checks the reference identifier that has been specified by the user via the GlobalProtect App. These reference identifiers include IP addresses and are checked when looking at the Common Name or in the Subject Alternative Name. The TOE supports the handling of wildcards if a certificate is presented with one in it. Certificate pinning is not supported. The TOE shall not establish a trusted channel if the server certificate is invalid – no exceptions. During the TLS handshake with connections to the Palo Alto Networks VPN Gateway and Portal (both acting as the server), the TOE presents the following cipher suites in its Client Hello. The TOE is only a client and does not act as a server in any connection. TLS 1.2 is the only version of TLS supported by the TOE. *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289* *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289* *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289* *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289* *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289* *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289* *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289* *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289* During the negotiation of the TLS handshake, X.509v3 certificates are used to verify the server's identity. Additionally, client certificates can be set on the GlobalProtect App to support mutual authentication. For the cipher suites noted above, the client hello extension supports secp256r1 and secp384r1 curves.

Table 4 Cryptographic Functions and CAVP Certificates

Function(s)	Standards	Certificates
Asymmetric key generation (FCS_CKM_EXT.1 and FCS_CKM.1/AK)		
ECDSA (P-256, P-384, P-521 curves)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	A2999
Cryptographic key establishment (FCS_CKM.2)		

Elliptic curve-based scheme	NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”	A2999
Symmetric encryption/decryption (FCS_COP.1/SKC)		
AES CBC, GCM (128, 256 bits)	FIPS PUB 197 CBC as defined in NIST SP 800-38A GCM as defined in NIST SP 800-38D	A2999
Cryptographic hashing (FCS_COP.1/Hash)		
SHA-1, SHA-256, SHA-384	FIPS PUB 180-4	A2999
Cryptographic signature services (FCS_COP.1/Sig)		
RSA with 2048-bit, 3072-bit, 4096-bit	FIPS PUB 186-4	A2999
ECDSA with NIST Curves P-256, P-384, P-521	FIPS PUB 186-4	A2999
Keyed-hash message authentication (FCS_COP.1/KeyedHash)		
HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	FIPS Pub 198-1 FIPS Pub 180-4	A2999
Deterministic random bit generation (FCS_RBG_EXT.2)		
CTR_DRBG (AES)	NIST SP 800-90A	A2999

6.2 User Data Protection

FDP_DEC_EXT.1	The GlobalProtect App does not store any sensitive data in non-volatile memory. During the configuration of the TOE, the user is not able to enter any sensitive data. When a user is initiating connections to the Palo Alto Networks Gateway or Portal, they are required to enter their authentication data for each new session that includes the username and password that is defined from the Palo Alto Networks Next Generation Firewall Gateway/Portal for the connection to succeed. These credentials are not stored or managed by GP. The application restricts its access to only using network connectivity when it is needed to communicate to the Palo Alto Networks Gateway or Portal. Other functionality on the host platform such as its camera, Bluetooth, USB, or microphone are not needed. The TOE does not require access to sensitive information repositories.
FDP_NET_EXT.1	
FDP_DAR_EXT.1	

6.3 Identification and Authentication

FIA_X509_EXT.1	The GlobalProtect App implements the ability to perform certificate path validation on the certificate chain that is presented to it by the Palo Alto Networks GlobalProtect Gateway or Portal. The certificate path validation begins with the identity certificate presented by the Gateway or Portal, and then proceeds in checking the intermediate CA certificate(s) until it reaches the trusted root certificate issued in the platform OS trust store. Only root certificates stored here are used and trusted by the TOE. On Windows platform, use the Certificates Snap-In (from the MMC). On Android/Linux platforms, use the keyring or Keystore to store the certificate. On MacOS/iOS platforms, use the Keychain to install the certificate. The following steps are performed for each certificate in the path: ● The public key algorithm/parameters are checked (i.e., RSA/ECDSA key sizes meet FIPS-CC requirements) ● The certificate is checked to make sure it is not expired (i.e. validity period of the certificate must be proper) ● The CA certificate includes caSigning purpose in the key usage field ● The certificate is checked to make sure it is not revoked using either CRL/OCSP ● The issuer name is checked to ensure that it matches the subject name of the previous certificate in the chain ● The certificate is checked that it terminates with a trusted CA certificate and that all CA certificates have the basicConstraints extension present (and set to TRUE) ● The extendedKeyUsage field is checked such that OCSP certificates and server certificates contain the correct OID (e.g., OCSP Signing purpose and Server Authentication purpose) ● The key usage extension of the certificate is checked to make sure that it is allowed to sign certificates ● Path lengths are checked to ensure it does not exceed any maximum path length inserted Certificates that are presented to the TOE must meet the x509v3 requirements as defined in RFC 5280 for TLS. If there are any issues with the certificate presented (as noted above), the application will not accept the certificate and reject the connection. A log message will be generated, and an administrator will be required to address the problem noted in order for the connection to succeed. The TOE will also display an error window with the failure reason and the option to continue is greyed out (i.e. unable to be selected). In FIPS-CC mode, the option to continue or override based on the administrator discretion is disabled. The TOE also supports the revocation checking of the certificate presented using either OCSP or CRL (as specified in RFC 6960 and RFC 5280 Section 6.3). In the event that the certificate is revoked following a check of its status, the TOE will reject the connection, and not allow the connection to continue. In the event that OCSP/CRL can't be reached, the administrator is provided with a warning message that the revocation status cannot be checked or determined along with the option to proceed with the connection as permitted by FIA_X509_EXT.2.2. Certificates are not used for email encryption, or server certificates presented for EST.
FIA_X509_EXT.2	

6.4 Security Management

FMT_MEC_EXT.1	When the TOE is configured, it is required that the platform administrator follow the rules defined in the administrator guide to properly set the correct configuration. If they are not followed, the GlobalProtect App will be active in non-FIPS-CC mode. The installation of the TOE must be completed by a platform administrator that is present at the endpoint/device on which the TOE resides as it will need administrator privileges to perform the installation of the software. There are no default credentials that are used or included with the TOE during its configuration. The TOE stores configuration data using mechanisms recommended by the OS. If the TOE is installed on a Windows 11 or Ubuntu 20.04 environment, it is required that the platform OS' FIPS mode be enabled. FIPS mode is also required for the macOS and iOS platform, but this is enabled by default. As noted in the Common Criteria Evaluated Configuration Guide, a platform administrator setting the TOE on a Windows 11 environment is required to launch the Windows Registry and make the proper edits there to set FIPS-CC mode. For the macOS configuration, a platform administrator is required to edit the relevant plist file to set the FIPS-CC mode of the TOE. This file is located in the platform's Library folder. Detailed instructions on how to set the required settings for enabling FIPS-CC mode for the GlobalProtect App on macOS is included in the CCECG. If the TOE is installed on Android or iOS mobile managed device, please use the MDM to enable FIPS-CC mode. Detailed instructions on how to set the required settings for enabling FIPS-CC mode for the GlobalProtect App on mobile platform is included in the CCECG. For the Linux configuration, a platform administrator is required to edit the relevant pangps.xml file to set the FIPS-CC mode of the TOE. Detailed instructions on how to set the required settings for enabling FIPS-CC mode for the GlobalProtect App on Linux is included in the CCECG. Once the TOE has been properly initialized into FIPS-CC mode, the TOE will have the ability to connect to the Palo Alto Networks Gateways provided by the Palo Alto Networks Next Generation Firewalls. The TOE provides several management functions that include the following that can be performed by the user: ▪ Enable/disable the transmission of any information describing the system's hardware, software, or configuration ▪ Setting gateway and portal addresses ▪ Check for updates ▪ Collecting troubleshooting logs (i.e. GlobalProtect App system logs for the application, self-test results, connection details) ▪ Querying the current version of the TOE
FMT_CFG_EXT.1	
FMT_SMF.1	

	By default, the TOE includes file permissions that protect the TOE's binary and data files from modification from normal unprivileged users. The TOE also includes an integrity check for itself to ensure that no malicious activity occurs.

6.5 Privacy

FPR_ANO_EXT.1	The GlobalProtect App does not transmit personally identifiable information about an individual. While the TOE may use client certificates to identify itself to the Palo Alto Networks GlobalProtect Gateway, it does not include sensitive information such as financial records, medical history, or social security numbers that could be used to identify an individual.

6.6 Protection of the TSF

FPT_API_EXT.1	The TOE includes the use of documented, platform APIs for underlying platforms.
FPT_AEX_EXT.1	The TOE automatically enables ASLR (Address Space Layout Randomization) when the application is compiled on Windows 11 (/DYNAMICBASE link flag) or macOS/Android/iOS/Linux (-pie link flag), and stack-based buffer overflow protection is enabled by default (compiled with /GS flag). There is no administrator intervention required to set this item. The GlobalProtect App does not request any memory mapping at an explicit address. The TOE does not allocate any memory region with both write and execute permissions; users shall also not write user-modifiable files to directories that contain executable files unless they are explicitly told to do so. The GlobalProtect App is designed to be compatible with the security features that are provided by the platform vendors that it is installed on.
FPT_TUD_EXT.1 FPT_TUD_EXT.2	The TOE has specific versions, which can be queried by the user via the TOE's interface. New versions of the TOE are created by Palo Alto Networks, which an administrator can retrieve to update the current version of the TOE. During the installation process, a digital signature verification check is automatically performed to verify that the update has not been modified. All new versions of the GlobalProtect App are digitally signed by Palo Alto Networks using RSA 2048 with SHA-256. The following package formats are used for the GlobalProtect installation file: • Windows: GlobalProtect64-6.0.7.msi • macOS: GlobalProtect-6.0.7.pkg • Android: global-protect-6.0.7-signed.apk • iOS: Download from iTunes Store • Linux: PanGPLinux-6.0.7.tgz

	The TOE is packaged such that the uninstall of the software results in complete zeroization of the TOE automatically. All files are removed from the platform when this uninstall process is initiated. Before files are uninstalled, they are overwritten with a random pattern, and then zeroized.
FPT_IDV_EXT.1	Palo Alto Networks provides a version control system for its software components. The TOE has a unique software versioning that identifies major versions and their subsequent maintenance releases in the following form: <major>.<minor>.<maintenance release>. Major and minor releases introduce new major and minor features for the product, and additional maintenance releases (e.g. 6.0.1, 6.0.2[4]) are released on a regular cadence to fix issues identified with the major release.
FPT_LIB_EXT.1	The TOE utilizes OpenSSL for its crypto functions and OESIS to provide endpoint security detection service in the underlying platforms. This library is checked for its integrity during the installation/initialization period to ensure that it has not been tampered with, and that the necessary procedures are followed to place this library in its required FIPS-CC mode.
ALC_TSU_EXT.1	The TOE is regularly updated with maintenance releases once a major release is made available to the public. These maintenance releases include various bug fixes to improve product features and to address any security vulnerabilities that may have come up in previous versions. When a new version is available, users are notified via an email from Palo Alto Networks with the specific version published. These versions are also displayed on Palo Alto Networks' Customer Support page (https://support.paloaltonetworks.com). Palo Alto Networks provides an updated version of the product on a regular basis to customers. The support portal provides users the ability to download new versions of the software. This portal also includes links to the Palo Alto Networks Release Notes that highlight all the changes included in the published release. These release notes detail all the bug fixes and security advisories/vulnerabilities that have been addressed. When a user downloads the new version from the support portal there is an option to display the SHA-256 checksum of the file that can be verified again once the file is downloaded. Palo Alto Networks provides customers with a Security Advisory page for any security vulnerabilities that have been identified in Palo Alto Networks products (https://securityadvisories.paloaltonetworks.com/). Each vulnerability is given a criticality rating and an updated status on any updates or mitigations regarding each discovered vulnerability. Each vulnerability listing also provides a list of the versions of the product that the vulnerability is known to affect. In the event that a vulnerability has been discovered, Palo Alto Networks provides users with the ability to report them via the Product Security Incident Response Team (PSIRT) via a trusted channel for a website: (https://securityadvisories.paloaltonetworks.com/Report) Palo Alto Networks provides timely security updates to our customers. Depending on the CVSS (Common Vulnerability Scoring System), the security updates can be provided as quickly as 2 weeks via a security hotfix release.

[4] There is also an internal build number which may be displayed. This is used by the vendor for internal tracking only.

6.7 Trusted Path/Channel

FTP_DIT_EXT.1	All data that is transmitted between the GlobalProtect App and the Palo Alto Networks Gateway and Portal are encrypted using TLS.

7. Protection Profile Claims

This ST is conformant to the [APPSW] and TLS Functional Package.

8. Rationale

This Security Target includes by reference the [APPSW] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [APPSW] assumptions. Security functional requirements have been reproduced verbatim with the protection profile operations completed. Operations on the security requirements follow [APPSW] application notes and assurance activities. The security target did not add or remove any security requirements. Consequently, [APPSW] rationale applies and is complete.