National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Palo Alto Networks GlobalProtect App 6

Report Number:	**CCEVS-VR-VID11402-2023**
Dated:	**October 20, 2023**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

The Aerospace Corporation

Farid Ahmed

Anne Gugel

Richard Toren

Robert Wojcik

Johns Hopkins University - Applied Physics Laboratory

Common Criteria Testing Laboratory

Anthony Apted

Armin Najafabadi

Pascal Patin

Leidos Inc.

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Palo Alto Networks GlobalProtect App 6 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant and meets the assurance requirements defined in the following documents:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([6])

The TOE is Palo Alto Networks GlobalProtect App 6.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5) as interpreted by the Assurance Activities contained in the Protection Profile (PP). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([7]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluation in accordance with National Voluntary Laboratory Assessment Program NVLAP accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Palo Alto Networks GlobalProtect App 6
Security Target	Palo Alto Networks GlobalProtect App 6 Security Target, Version 1.0, 26 July 2023
Sponsor & Developer	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
Completion Date	September 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
CCTL Evaluation Personnel	Anthony Apted Armin Najafabadi Pascal Patin
CCEVS Validators	Jim Donndelinger Farid Ahmed Anne Gugel Richard Toren Robert Wojcik

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is a software application supported and tested on the following operating system platforms:

- Windows 11
- macOS 12
- Android 12
- iOS 16
- Linux Ubuntu 20.04

The TOE runs on the endpoint (desktop/laptop computer or mobile device) to protect users by using the same security policies that protect the sensitive resources in corporate networks. The TOE secures the traffic using TLS and allows users to connect to corporate networks to access the company's resources from anywhere in the world. The TOE interacts with other GlobalProtect components, which include the Palo Alto Networks GlobalProtect Portal and Gateway.

The Palo Alto Next Generation Firewall operates the GlobalProtect Portal, which provides details for the GlobalProtect infrastructure, and the GlobalProtect Gateway. Every client system that participates in the GlobalProtect network receives configuration information from the Portal, including information about available GlobalProtect Gateways and any client certificates that may be required to connect to a gateway. The GlobalProtect Gateway provides security enforcement for traffic from the GlobalProtect App.

The following figure provides adepiction of the TOE deployment.

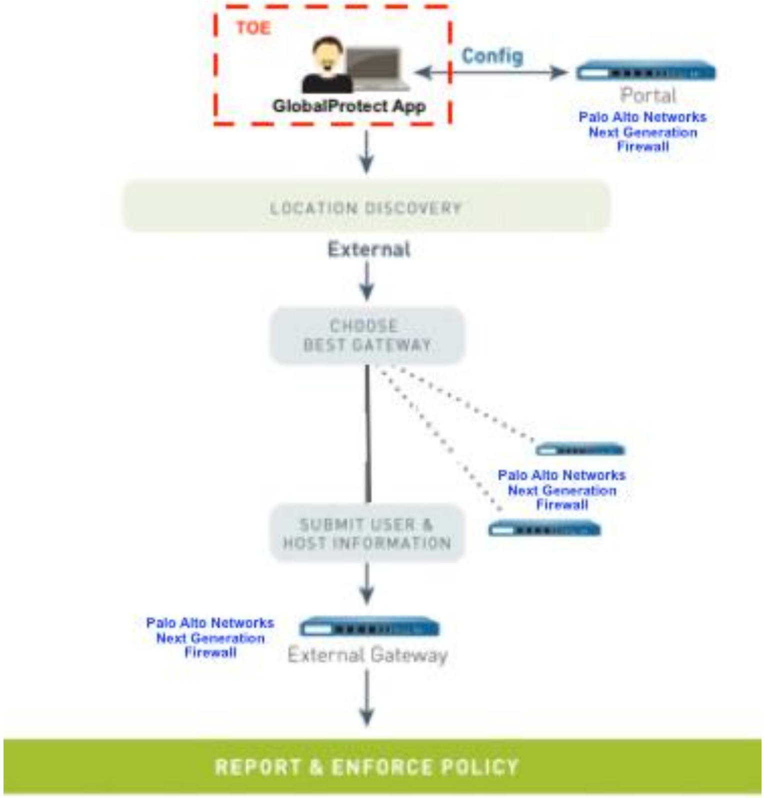
TOE
GlobalProtect App
Config
Portal
Palo Alto Networks Next Generation Firewall
LOCATION DISCOVERY
External
CHOOSE BEST GATEWAY
Palo Alto Networks Next Generation Firewall
SUBMIT USER & HOST INFORMATION
Palo Alto Networks Next Generation Firewall
External Gateway
REPORT & ENFORCE POLICY

Figure 1: TOE Deployment

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 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. The algorithm certificate references are listed in Table 2 below.

Table 2: CAVP Certificate References

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

4.2 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.

4.3 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.

4.4 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.

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

4.5 Privacy

The TOE does not transmit personally identifiable information (PII) over the network.

4.6 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 the 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. Palo Alto Networks signs all updates 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.

4.7 Trusted Path/Channels

The TOE protects communication between itself as the endpoint and other networks using TLS. The TOE uses TLS 1.2 to encrypt all data that it transmits to external IT entities (i.e., Palo Alto Networks GlobalProtect Portals and Gateways).

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST reproduces the assumptions about the use of the TOE directly from the Protection Profile for Application Software, Version 1.4, 7 October 2021 to which it claims conformance. Those assumptions are as follows:

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

5.2 Threats

The following threats are directly from the Protection Profile for Application Software, Version 1.4, 7 October 2021.

- 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.
- 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.
- 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.
- An attacker may try to access sensitive data at rest.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following documents:
    - *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
    - *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([6])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.

- The evaluation of security functionality of the product was limited to the functionality specified in Palo Alto Networks GlobalProtect App 6 Security Target, Version 1.0, 26 July 2023 ([7]). Any additional security-related functional capabilities included in the product were not covered by this evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- Palo Alto Networks GlobalProtect App User Guide Version 6, January 24, 2023 ([8])
- Palo Alto Networks GlobalProtect Administrator's Guide Version 10.1 or Later, Feb 22, 2022([9])
- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) GlobalProtect 6 App, June 28, 2023 ([10]).

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Evaluation Technical Report for Palo Alto Networks GlobalProtect App 6* Version 1.0, 28 August 2023 ([11).

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Palo Alto Networks GlobalProtect App 6*, Version 1.0, 28 August 2023 ([12])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specifications:

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

The evaluation team devised a test plan based on the test activities specified in the above specifications. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

The TOE was tested at Leidos's Columbia, MD location from May 2023 to July 2023. The procedures and results of this testing are available in the test report referenced above.

8 TOE Evaluated Configuration

The TOE is Palo Alto Networks GlobalProtect App 6, supported and tested on the following operating systems[1]:

- Windows 11
- macOS 12
- Android 12
- iOS 16
- Linux Ubuntu 20.04

The following figure depicts the test configuration used by the evaluation team to test the TOE on each of its supported platforms.

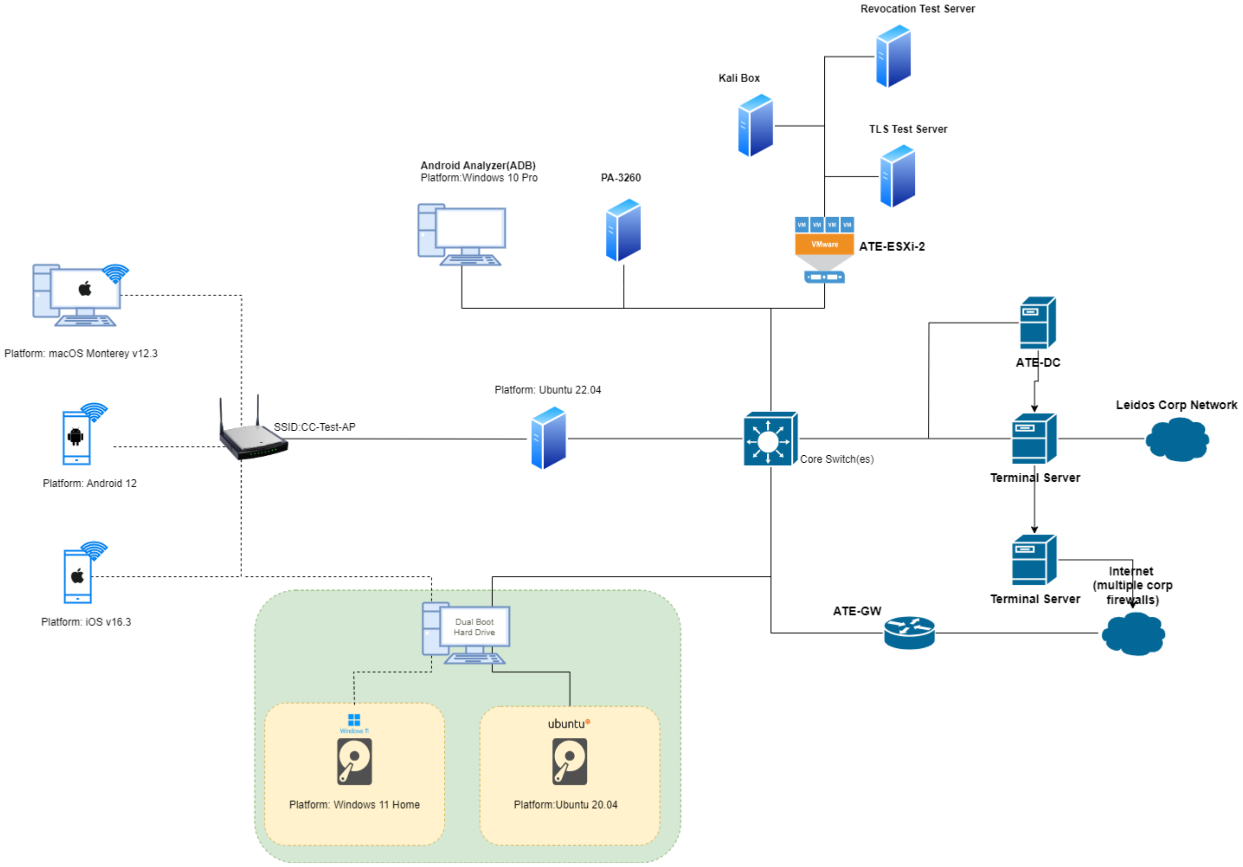

Figure 2: Test Configuration

The following components were used to create the test configuration:

TOE Platforms

- HP Envy x360 2-in-1 Laptop, configured for Dual Boot

[1] While the TOE was tested on these operating systems, the TOE is compatible with later versions of the operating systems identified here. This is vendor affirmed.

    - Windows 11
    - Ubuntu 20.04
- iPhone 12 mini
    - iOS v16.3
- MacBook Pro (14-inch, 2021)
    - macOS Monterey v12.3
- Galaxy S21 Ultra 5G
    - Android v12.3, Hostname: Galaxy S21 Ultra 5G

Test Configuration Components

- Palo Alto Networks PA-3260 Firewall—hosts GlobalProtect Portal and Gateway
- Router—connects between wireless and wired networks
    - OpenSSL 3.0.2
- Wireless AP—allows wireless mobile devices to connect to test network
- Android Analyzer (ADB)
    - Android Studio (Electric Eel 2022.1.1)
- ATE-GW—Main router/gateway
- ATE-DC—Main Domain Controller (DC) for Test environment/DNS server
- ATE-ESXi-2—Virtualization server hosting:
    - Revocation Test Server--hosts TLS/OCSP test tools
        - OpenSSL 1.1.1
        - Wireshark 2.6.10
    - TLS Test Server—hosts TLS test tools
        - Proprietary Python TLS test tools
        - OpenSSL 1.1.1
        - Wireshark 2.6.10
    - Kali Box—hosts testing tools
        - SSLyze v2.0.6
        - OpenSSL 1.1.1
- Terminal Server—provides tester access to the Test Environment from corporate network

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the team test plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for Application Software*, Version 1.4, 7 October 2021, the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 were fulfilled.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Palo Alto Networks GlobalProtect App 6 ([11]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([6])

The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the PP listed above.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the following public vulnerability databases:

- National Vulnerability Database (NVD) (https://nvd.nist.gov/vuln/search)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/)

The evaluation team performed searches on 29 September 2023 using the following search terms:

- “Palo Alto Networks” – TOE vendor
- “GlobalProtect” – TOE name
- “VPN Client” – TOE application type
- “OpenSSL 1.1.1” – Third-party library included with TOE
- “OESIS” – third-party library included with TOE.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. In addition, the evaluation team’s testing demonstrated the accuracy of the claims in the ST.

- The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, performed the Assurance Activities in the *Protection Profile for Application Software*, Version 1.4, 7 October 2021, the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All of the validators concerns are adequately captured in Section 5, Assumptions and Clarification of Scope. Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

11 Security Target

The ST for this product's evaluation is *Palo Alto Networks GlobalProtect App 6 Security Target*, Version 1.0, 26 July 2023 ([7]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activity Report
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019

[7] Palo Alto Networks GlobalProtect App 6 Security Target, Version 1.0, 26 July 2023

[8] Palo Alto Networks GlobalProtect App User Guide Version 6, January 24, 2023

[9] Palo Alto Networks GlobalProtect Administrator's Guide Version 10.1 or Later, February 22, 2022

[10] Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) GlobalProtect 6 App, June 28, 2023

[11] Evaluation Technical Report for Palo Alto Networks GlobalProtect App 6, Version 1.0, 28 August 2023.

[12] Assurance Activities Report for Palo Alto Networks GlobalProtect App 6, Version 1.0, 28 August 2023.

[13] Palo Alto Networks GlobalProtect App 6 Common Criteria Test Report and Procedures, Version 1.0, 28 July 2023.