National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Palo Alto Networks GlobalProtect App Version 5.1.5

Report Number: CCEVS-VR-VID11085-2020
Dated: August 17, 2020
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements

Validation Team

Randy Heimann

Lisa Mitchell

Clare Olin

Jean Petty

Chris Thorpe

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report 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 Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Palo Alto Networks GlobalProtect App Version 5.1.5 (the Target of Evaluation, or TOE). The TOE versions run on either Windows 10 or macOS (minimum version 10.14). 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 applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Palo Alto Networks GlobalProtect App Version 5.1.5 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2020.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following documents:

- Protection Profile for Application Software, Version 1.3 [5]
- Functional Package for Transport Layer Security (TLS), Version 1.1 [6]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The security functions specified in these Protection Profiles include protection of communications between the TOE and external IT entities, cryptographic support, user data protection, identification and authentication via X509 certificates, security management, privacy, protection of the TSF, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profiles and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([9]) and the associated test report produced by the Leidos evaluation team ([11]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [5], [6] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

Protection Profile for Application Software, Version 1.3, March 1, 2019

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

- 0416 – Correction to FCS_RBG_EXT.1 Test Activity
- 0427 – Reliable Time Source
- 0437 – Supported Configuration Mechanism
- 0434 – Windows Desktop Application Test
- 0444 – IPsec Selections
- 0445 – User Modifiable File Definition
- 0465 – Configuration Storage for .NET Apps
- 0486 – Removal of PP-Module for VPN Clients from allowed with list
- 0495 – FIA_X509_EXT.1.2 Test Clarification
- 0498 – Application Software PP Security Objectives and Requirement Rationale
- 0505 – Clarification of revocation testing under RFC6066
- 0510 – Obtaining random bytes from for iOS/macOS

Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019

- 0442 – Updated TLS Ciphersuites for TLS package
- 0469 – Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1

  Note: This Technical Decision is not applicable to the TOE as the TOE does not claim FCS_TLSS_EXT.1.1
- 0499 – Testing with pinned certificates
- 0513 – CA Certificate loading

There were no Observation Reports submitted during this evaluation.

All other Technical Decisions were found to be not applicable to the TOE, either because they were not related to the claimed Protection Profile or because they related to optional or selection-based functionality that was not claimed in the TOE's Security Target [7].

1.2 Threats

The ST references the PPs to which it claims conformance for statements of threats that the TOE and its operational environment are intended to counter. Those threats, drawn from the claimed PP, are as follows:

- 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.

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 and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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).

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Palo Alto Networks GlobalProtect App Version 5.1.5
	The TOE is available in two versions:
	• Windows 10
	  • GlobalProtect64-5.1.5.msi
	  • SHA-256 checksum: 530C35A1390EEBCFF2F9B8D0781C914561468401D3DE135BADA44D9FB869AE38
	• macOS 10.14 (and newer)
	  • GlobalProtect-5.1.5.pkg
	  • SHA-256 checksum: 102D2EDE71F818FC2F225C6BB1A57D46B806C865A12B9EE333065856E0E2532F

Sponsor & Developer:	Palo Alto Networks, Inc. 3000 Tannery Way Santa Clara, CA 95054
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	August 2020
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	Protection Profile for Application Software, Version 1.3, 1 March 2019 Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019

Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Greg Beaver
Validation Personnel:	Randy Heimann Lisa Mitchell Clare Olin Jean Petty Chris Thorpe

3 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 ETR.

3.1 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. In addition, the TOE also relies on the underlying platforms Windows 10 and macOS.

3.2 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.

3.3 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.

3.4 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.

3.5 Privacy

The TOE does not transmit PII over a network.

3.6 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 of 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.

3.7 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).

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- 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).
- 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.

4.2 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 only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in
    - *Protection Profile for Application Software*, Version 1.3 [5]
    - *Functional Package for Transport Layer Security (TLS)*, Version 1.1 [6]

  and performed by the evaluation team).
- This evaluation covers only the specific software 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 Version 5.1.5 Target*, Version 1.0, May 8, 2020 [7].
- 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 Validation Report.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

The TOE is the Palo Alto Networks GlobalProtect App Version 5.1.5, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report.

The TOE includes a "FIPS-CC" mode of operation. This mode must be enabled for the TOE to meet the claimed requirements.

5.2 Excluded Functionality

All product functionality that is not claimed by the Security Target as part of achieving exact conformance to the *Protection Profile for Application Software* [5] and *Functional Package for Transport Layer Security (TLS*) [6] is excluded from the evaluation scope.

6 Documentation

Palo Alto 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 each TOE model is as follows:

- Palo Alto Networks GlobalProtect App User Guide Version 5.0, July 12, 2019 [8]
- Palo Alto Networks Common Criteria Evaluation Configuration Guide (CCECG), GlobalProtect App 5.1.5 May 8, 2020 [10]

This is also provided for initial setup purposes. To use the product in the evaluated configuration, the product must be configured as specified in these guides.

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 device as evaluated. Consumers are encouraged to download this CC configuration guide (CCECG above) from the NIAP website.

7 Independent Testing

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

- *Palo Alto Global Protect v 5.1.5 Common Criteria Test Report and Procedures Protection Profile for Application Software v1.3 with Functional Package for TLS v1.1, Version 1.0, June 12, 2020* [11]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Palo Alto GlobalProtect [9]

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 *Protection Profile for Application Software* [5] and the *Functional Package for Transport Layer Security (TLS),* Version 1.1 [6].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in *Protection Profile for Application Software* [5] and the *Functional Package for Transport Layer Security (TLS)* [6]. 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.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal 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 *Protection Profile for Application Software* [5] and the *Functional Package for Transport Layer Security (TLS),* Version 1.1 [6] were fulfilled.

7.1 Test Configuration

The evaluated version of the TOE consists of Palo Alto GlobalProtect App 5.1.5 running on the following physical appliances:

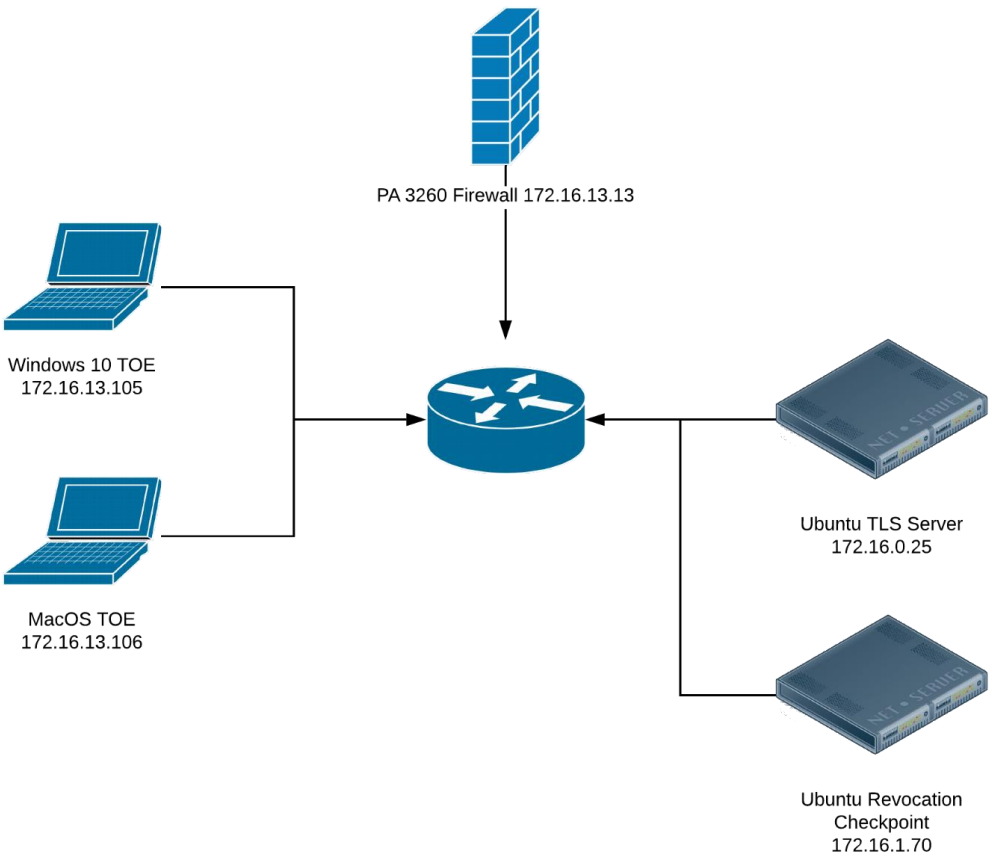
TOE Devices:

- Windows 10 Pro 1909
  - IP: 172.16.13.105
  - MAC: F0:92:1C:58:E3:C1
  - Software
    - Wireshark 2.6.10
- MacMini MacOS version 10.14.6
  - IP: 172.16.13.106
  - MAC: F0:18:98:EA:DC:B5

Support Devices:

- PA 3260 Firewall
  - IP 172.16.13.13
  - MAC: 08-66-1F-01-E4-D2

  - PAN OS: 9.0.6
  - Purpose: Hosts valid Portal and Gateway services.
  - 3260-vpn.paloaltocc.com
    - 172.16.14.13
    - MAC: C4-24-56-AB-D4-4A
- Ubuntu TLS server
  - IP: 172.16.0.25
  - MAC: AA-6C-3A-6F-8D-FF
  - Ubuntu 18.0.4
  - Purpose: provides a configurable TLS server.
  - Software
    - Python 2.7
    - Wireshark 2.6.10
    - OpenSSL 1.1.1
- Ubuntu Revocation checkpoint
  - IP 172.16.1.70
  - MAC: 02-23-72-FE-F4-F2
  - Ubuntu 18.0.4
  - Purpose: provides Revocation checkpoint services.
  - Software
    - OpenSSL 1.1.1



The TOE must be deployed as described in section 4.1 of this Validation Report and be configured in accordance with the *Palo Alto Networks GlobalProtect App User Guide Version 5.0* [8], and *Palo Alto Networks Common Criteria Evaluation Configuration Guide (CCECG), GlobalProtect App 5.1.5* [10].

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

7.2 Vulnerability Analysis

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration. Both the MacOS and Windows installer files were scanned using McAfee Endpoint Security. Security definitions were up to date as of June 11, 2020. No vulnerabilities were found in either file.

The evaluation team searched the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) and the Palo Alto Security Advisories (https://securityadvisories.paloaltonetworks.com) vulnerability repositories. Searches were performed on 7/13/2020.

The keyword searches included the following terms:

- Palo Alto
- GlobalProtect
- Management Software
- TCP
- TLS
- Microarchitectural
- GlobalProtect– The latest vulnerabilities at the vendor website: https://securityadvisories.paloaltonetworks.com

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.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Protection Profile for Application Software*, Version 1.3 [5]
- F*unctional Package for Transport Layer Security (TLS),* Version 1.1 [6]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECC) GlobalProtect App 5.1.5, May 8, 2020.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *Palo Alto Networks GlobalProtect App Version 5.1.5 Target, Version* 1.0, May 8, 2020 [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

[5] Protection Profile for Application Software, Version 1.3, Version 1.3, 1 March 2019

[6] Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019

[7] Palo Alto Networks GlobalProtect App Version 5.1.5 Target, Version 1.0, May 8, 2020

[8] Palo Alto Networks GlobalProtect App User Guide Version 5.0, July 12, 2019

[9] Assurance Activities Report for Palo Alto Networks GlobalProtect App Version 5.1.5, Version 1.0, 2020-06-02

[10] Palo Alto Networks Common Criteria Evaluation Configuration Guide (CCECG), GlobalProtect App 5.1.5, May 8, 2020

[11] Palo Alto Global Protect v 5.1.5 Common Criteria Test Report and Procedures Protection Profile for Application Software v1.3 with Functional Package for TLS v1.1, Version 1.0, June 12, 2020