Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Appgate SDP v5.4

Version 1.0, 4 April 2022

Report Identifier: AISEP-CC-CR-2022-EFT-T023

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Appgate SDP v5.4 against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is Appgate SDP v5.4. The nominal version 5.4 incorporates:

- Appgate SDP v5.4.4 Appliance
- Appgate SDP Windows Client v5.4.4, macOS Client v5.4.3, Ubuntu Client v5.4.3, Fedora Client v5.4.3 and Android Client v5.4.3.

The TOE enables network administrators to establish a Software Defined Perimeter (SDP) to control access by network-based users to network resources in physical, cloud-based and hybrid environments.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP).

Common Criteria Supplementary Guidance is available from Appgate's SDP Admin guide v5.4 website under *Appendix* and then select the *Common Criteria* page [6].

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program. The evaluation was performed by Teron Labs and was completed on 28 January 2022.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends that:

- the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to Appgate's product administrator guidance
- users configure and operate the TOE according to Appgate's Common Criteria Supplementary Guidance
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- the passwords for all identities should be handled securely
- multi-factor authentication should be considered for all admin users for additional security
- the system auditor should review the audit trail generated and exported by the TOE periodically
- the use of SSH for administration of the TOE was out of the scope this evaluation and should be disabled by the administrator after initial configuration and not be used
- users should verify the integrity of the TOE software prior to installation by comparing the fingerprint of the downloaded software against the value available from Appgate's Common Criteria Supplementary Guidance.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [7] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [7] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Appgate SDP v5.4.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Appgate SDP
TOE Type	Network and Network-Related Devices and Systems
Software version	v5.4 (Appgate SDP v5.4.4 Appliance and Appgate SDP Windows Client v5.4.4, macOS Client v5.4.3, Ubuntu Client v5.4.3, Fedora Client v5.4.3 and Android Client v5.4.3)
Security Target	*Appgate SDP v5.4 Security Target Version 1.0 dated 2022-03-16*
Evaluation Technical Report	*Evaluation Technical Report 1.0 dated 22 March 2022* Document reference EFT-T023-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, Version 3.1 Rev 5, April 2017
Methodology	Common Methodology for Information Technology Security, Version 3.1 Rev 5, April 2017
Conformance	EAL 2 augmented with ALC_FLR.1 (Basic flaw remediation)

Developer	Appgate Kungsgatan 34 411 19 Gothenburg Sweden
Evaluation facility	Teron Labs Pty Ltd Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Appgate SDP v5.4.

Appgate SDP provides capabilities to control access of network-based users to network resources in physical, cloud-based and hybrid environments, using the approach to computer security known as the Software Defined Perimeter (SDP).

The principle of operation is that Gateways are deployed in front of networked resource (application and server) infrastructure, effectively making those resources invisible to the outer network. A Controller defines access rights for users and devices (collectively, the Clients) on an individual basis. A Client establishes a secure TLS tunnel to the Controller, which authenticates the user. This process is based on verifying user claims within each session—including device posture and identity—before issuing Entitlement tokens to the user. The Client passes the issued Entitlement tokens on to the Gateways, which provision a firewall instance just for that user. The Gateway then translates the Entitlements into a set of individualized firewall rules. For each packet received from the Client, the correct rules allow, conditionally allow or block access to the network resources protected by the Gateway.

In the language of NIST SP800-207 [5] the Appgate Gateways are Policy Enforcement Points (PEPs) with the ability to enforce fine-grained many-to-many access policies. Acting like a Policy Decision Point (PDP) the Appgate Controller controls the operation of the Appgate Gateways. The TOE also maintains a separation between the control plane and the data plane. The Appgate Client to Controller communications and Controller to Gateway communications are separate to the payload communications between the Client and the Gateways.

TOE Functionality

The TOE functionality that was evaluated is described in section 2 of the Security Target [7].

TOE physical boundary

The TOE physical boundary is described in section 2.3 of the Security Target [7].

TOE Architecture

Appgate SDP comprises an appliance component and a client software component installed on a user's device, such as a workstation, laptop, or mobile platform.

The Appgate SDP appliance is a stateless, configurable component that can operate in the following roles:

- Controller—the central point of administration for the Appgate SDP deployment. It includes an internal database for the storage of system configuration data and provides the following capabilities:
  - Certificate Authority (CA) for the deployment
  - Creation and signing of tokens used for authentication, authorization, and Policy distribution

- Authentication of administrators logging in via the Admin User Interface (UI) and REST API, and users logging in via the Client
- Assignment of Policies to users and creation of the list of Entitlements for each user
- Assignment of roles to administrators and enforcement of privileges.

- Gateway—the policy enforcement point, responsible for controlling user access to network resources. The Gateway uses Claims and Entitlement information from each user to manage firewall rules and provide real-time access control.
- LogServer—collects logs from the Controllers and Gateways to provide an audit trail of actions and user access. A LogServer is typically configured on an existing Controller appliance but can also be stand-alone where Controller performance is critical. Alternatively, log files can be exported using `rsyslog` to an external log server. Note, the LogServer role is excluded from the evaluated configuration.

The Appgate Client software component is installed on a user's device, such as a workstation, laptop, or mobile platform. An Appgate Client establishes a secure TLS tunnel to the Controller, which authenticates the user. The Controller verifies user claims and issues Entitlement tokens to the Client. On behalf of the user, the Appgate Client submits the Entitlement tokens to relevant Appgate Gateways, which control the user's subsequent access to network resources.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [7].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [7] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per operational guidance documentation [6].

Secure delivery

Software delivery procedures

The appliance (Controller, Gateway) software image (ISO) is available from Appgate's Admin Guide web site:

https://sdphelp.appgate.com/adminguide/v5.4/introduction.html

Navigate to the "Appendix" folder containing the "Common Criteria" document. An account is required to access the ISO image file.

For the appliance software image there is a SHA256 hash which can be found for each release. Beside the hash method for ensuring the authenticity of the software, there is a digital signature as well, using GPG. The signature and the hash are checked during the upgrade process to guarantee the integrity of the Appgate SDP downloaded software.

When a new release is published, Product Management sends an e-mail out to customers to notify them of the new release and the corresponding release notes, together with highlighted features or critical fixes. The update images are downloadable from the Appgate web site.

Software for the clients (Windows, macOS, Ubuntu, Fedora and Android Mobile) is available from the Appgate Common Criteria Supplementary Guidance web page [6]. The web page also provides SHA256 hash values and GPG digital signatures for each client installer file.

Installation of the TOE

The operational guidance documentation [6] contains all relevant information for the secure configuration of the TOE.

Version verification

Appgate SDP is distributed software, and it is assumed all Controllers and Gateways are running the same version, that is, v 5.4.4. The only exception would be in the middle of a planned upgrade process where appliances are updated in a sequenced manner.

An overview of the Appgate SDP appliance software versions can be found in the Appgate SDP admin UI, which runs on any of the controller nodes. The dashboard appliance widget will show a list of all registered appliances and reports their corresponding version number. Also via console or SSH the command *cz-config status* (run as sudo user) will show the version number of the appliance.

The version of the Appgate Client software can be found by clicking on the Appgate SDP icon in the tray menu and click the 3 dots in the upper right corner to open up the menu. *About* will indicate the client version of the software.

Documentation and guidance

The guidance documentation included in the TOE is available on-line at the following URL:

https://sdphelp.appgate.com/adminguide/v5.4/index.html [6]

The guidance documentation includes CC Supplementary Guidance available on-line at the following URL:

https://sdphelp.appgate.com/adminguide/v5.4/common-criteria.html [6]

The user guide for Clients can be found here:

https://sdphelp.appgate.com/userguide/v5.4/index.html [6]

All Common Criteria material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4]

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

- there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains
- the TOE components critical to security policy enforcement will be protected from unauthorized physical modification
- the operational environment must ensure that security measures are in place to protect DNS hostname resolution if DNS is used.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [9].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These developer tests are designed in such a way as to exercise the TOE security functional requirements and the TOE interfaces identified in the TOE design documentation.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that security target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [7] and **has met** the requirements of Common Criteria EAL2+ALC_FLR.1.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australian Certification Authority **certifies** the evaluation of Appgate SDP Version 5.4 performed by the Australian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed. In addition to the objectives involving competent administrators and physical security there is an objective involving the protection of any DNS used by the software. If hostnames are used then the name to address mapping system used is clearly important even in simple setups and should be carefully designed. In modern cloud, multi-cloud and hybrid-cloud environments the TOE allows for various naming system configurations that must be thoughtfully designed by people with specific domain knowledge so that the name to address mapping process is reliable and can be trusted.

The Australian Certification Authority also recommends:

- that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to Appgate's product administrator guidance
- users configure and operate the TOE in accordance with Appgate's CC Supplementary Guidance [6] available as an appendix page in the product administrator guidance
- users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- passwords for all identities should be handled securely
- multi-factor authentication should be considered for all admin users for additional security
- the system auditor should review the audit trail generated and exported by the TOE periodically
- the use of SSH for administration of the TOE was out of the scope of this evaluation and should be disabled by the administrator after initial configuration and not be used
- users should verify the integrity of the TOE software prior to installation by comparing the fingerprint of the downloaded software against the value available in Appgate's CC Supplementary Guidance [6].

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 5, April 2017*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 5, April 2017*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 5, April 2017*
4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
5. NIST Special Publication 800-207 Zero Trust Architecture dated August 2020
6. Guidance documentation:
   - *Admin Guide* – https://sdphelp.appgate.com/adminguide/v5.4/introduction.html
   - *CC Supplementary Guidance* – https://sdphelp.appgate.com/adminguide/v5.4/common-criteria.html
   - *User Guide* - https://sdphelp.appgate.com/userguide/v5.4/index.html
7. *Appgate SDP v5.4 Security Target Version 1.0 dated 2022-03-16*
8. Evaluation Technical Report - *EFT-T023 ETR 1.0 dated 22 March 2022*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*
10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

Abbreviations

AISEP	Australian Information Security Evaluation Program
API	Application Programming Interface
ASD	Australian Signals Directorate
CA	Certificate Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
DNS	Domain Name System
EAL	Evaluation Assurance Level
GPG	GNU Privacy Guard
HTTPS	Hypertext Transfer Protocol Secure
ISO	Disc image format – often contains a complete file system
PDP	Policy Decision Point
PEP	Policy Enforcement Point
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer (stateless)
SDP	Software Defined Perimeter
SHA256	Secure Hash Algorithm 256 bit digest
SPA	Single Packet Authorization
SSHv2	Secure Shell version 2
TLS 1.2	Transport Layer Security version 1.2
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface