Australian Information Security Evaluation Program

Maintenance Report for
Appgate SDP v6.0

Version 1.0, 17 March 2023

Report Identifier: AISEP-CC-MR-2023-AAC092

Table of contents

Introduction

Overview

This document is an Assurance Continuity Maintenance Report describing the findings of the Australian Information Security Evaluation Program (AISEP) concerning the certification of Appgate SDP v5.4.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Appgate against the requirements contained in *Assurance Continuity: CCRA Requirements v2.2, 30-September-2021* (Ref [1]).

In the course of the last four years, Appgate SDP has been evaluated and certified in the AISEP three times. The versions certified were Cyxtera Technologies Appgate v4.3 in August 2019, Appgate v5.2 in January 2021 and Appgate v5.4 in April 2022. The Certification Report identifier for the Appgate v5.4 evaluation and certification is AISEP-CC-CR-2022-EFT-T023 (Ref [5]).

Teron Labs submitted *Appgate SDP v6.0 Impact Analysis Report Version 1.0* to the Australian Certification Authority (ACA) on 30 January 2023. The Impact Analysis Report (IAR) describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Document / TOE Identification for the maintained TOE

IAR - *Appgate SDP v6.0 Impact Analysis Report Version 1.0, January 25, 2023*

ST - *Appgate SDP v6.0 Security Target Version 1.0, 2023-1-25*

Guidance – a) https://sdphelp.appgate.com/adminguide/v6.0/common-criteria.html

b) https://sdphelp.Appgate.com/userguide/v6.0/

Maintained TOE - Appgate SDP v6.0 consisting of:

- Appgate SDP v6.0.1 Appliance
- Appgate SDP Windows Client v6.0.2
- Appgate SDP macOS Client v6.0.2
- Appgate SDP Ubuntu Client v6.0.2
- Appgate SDP Fedora Client v6.0.2
- Appgate SDP Android Client v6.0.1

IAR introduction summary

The Appgate SDP v6.0 TOE 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 Appgate SDP is built on three core principles:

1. Identity-centric - It is designed around the user, addressing the perimeter-less enterprise. Users are authenticated before they are allowed to connect to a network.
2. Zero-Trust - It enforces the “Zero Trust” model so that anyone attempting to access a resource must authenticate first. All unauthorized resources are invisible. Zero Trust ensures that once proper access criteria are met, a dynamic one-to-one connection is generated from the user’s machine to the specific resource needed. Everything else is completely invisible. This applies the principle of least privilege to the network and reduces the attack surface.
3. Cloud-centric - The Software-Defined Perimeter (SDP) is built for the cloud and has no centralized network chokepoint. It is completely distributed and as scalable as the internet itself. An SDP is engineered to operate natively in cloud networks.

The principle of operation is that Gateways are deployed in front of networked resource (application and server) infrastructure, effectively making it invisible on the 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.

The 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 Client runs on each user’s device and makes access requests to the Controller.

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

1. 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 assignment of policies to users and creation of the list of entitlements for each user.
2. Gateway—The Gateway is the enforcement point, responsible for controlling user access to protected resources. After seeding it registers with the Controller and will then be listed as available to receive Client connections. Once registered it runs as a stateless appliance only needing to receive the token revocation list from the Controller. The Gateway uses the Claims and Entitlement tokens from each user to manage firewall rules and provide real-time access control.

Description of changes

The material in this section is a condensed version of the information in the IAR.

Appgate version changes

Certified TOE (v5.4) →	Maintained TOE (v6.0)
• Appgate SDP v5.4.4 Appliance • Appgate SDP Windows Client v5.4.4 • Appgate SDP macOS Client v5.4.3 • Appgate SDP Ubuntu Client v5.4.3 • Appgate SDP Fedora Client v5.4.3 • Appgate SDP Android Client v5.4.3	• Appgate SDP v6.0.1 Appliance • Appgate SDP Windows Client v6.0.2 • Appgate SDP macOS Client v6.0.2 • Appgate SDP Ubuntu Client v6.0.2 • Appgate SDP Fedora Client v6.0.2 • Appgate SDP Android Client v6.0.1

Library and other dependency version changes

Certified TOE (v5.4) →	Maintained TOE (v6.0)
• Bouncy Castle Java API v1.68 • WolfSSL 4.6.0-fips uses Wolfcrypt 4.0 • PostgreSQL 9.4 / BDR • Appliance base Ubuntu 18.04	• Bouncy Castle Java API v1.70 • WolfSSL 5.2.0-fips with Wolfcrypt 4.0 • PostgreSQL 12 / BDR 3.7 • Appliance base Ubuntu 20.04
• Windows 7 SP1 and later, .NET 4.5 and later • Apple OSX/macOS 10.14.6 or newer • Ubuntu 16.04 • Fedora 33+ gnome-keyring • Android 6 or later	• Windows 10 and 11, .NET 4.5 and later • Apple OSX/macOS 10.15.7 or newer • Ubuntu 16.04 or later • Fedora 35+ gnome-keyring • Android 7 or later

Feature changes (brief subset summary)

- Port 444 not used for peer communications
- DNS Forwarder now supports the use of the appliance's hosts file.
- CRL support for appliance to Controller connections
- Improved Azure API calls with rate limiting and result caching.
- macOS smartcard certificate authentication added
- Added support for OIDC as a new type of IdP. Can be used for user and admin UI authentication.
- Added support for an additional appliance remote command - netcat

- Admin UI - Introduced an updated information architecture and menu system to better match the product's evolving use cases.
- The concept of Conditional Entitlements has been superseded by three Access Control options.
- Configurable connection rate limiter to throttle new Client connections to Gateways
- Expiring appliance certificates will be automatically renewed in the 24 hours preceding expiration. Only applies to certificates managed by the Collective.

Affected developer evidence

Certified TOE (v5.4) →	Maintained TOE (v6.0)
Security Target: Appgate SDP v5.4 Security Target Version 1.0, March 16, 2022	**Maintained Security Target:** Appgate SDP v6.0 Security Target Version 1.0, January 25, 2023
Guidance Documentation: https://sdphelp.appgate.com/adminguide/v5.4/common-criteria.html The user guide for Clients is available on-line at the following URL: https://sdphelp.Appgate.com/userguide/v5.4/	**Maintained Guidance Documentation:** https://sdphelp.appgate.com/adminguide/v6.0/common-criteria.html The user guide for Clients is available on-line at the following URL: https://sdphelp.Appgate.com/userguide/v6.0/
Design Documentation Appgate SDP v5.4 Design Documentation Version 1.0, 2022-03-16	**Maintained Design Documentation** Appgate SDP v6.0 Design Documentation Version 1.0, 2023-1-25
Common Criteria ALC Life Cycle Support Guidance Appgate SDP v5.4 EAL2+ Life-Cycle Support Documentation Plus ALC_FLR.1 Version 1.0, 2022-03-16	**Maintained Common Criteria ALC Life Cycle Support Guidance** Appgate SDP v6.0 EAL2+ Life-Cycle Support Documentation Plus ALC_FLR.1 Version 1.0, 2023-1-25
Test Plan Appgate SDP v5.4 Test Plan, Version 1.0, 23 November 2021	**Maintained Test Plan** Appgate SDP v6.0 Test Plan, Version 1.0, 9 November 2022

Regression testing

The IAR (Ref [1]) describes the Appgate regression testing effort. Regression testing was performed on the following Appgate versions: 5.5, 5.5.1, 5.5.2, 5.5.3 5.5.4, 5.5.5 (client), 5.5.6 (appliance), 6.0.0 and 6.0.1. The testing includes automated unit testing, system testing and end to end testing. Manual testing has also been performed against all 5.5.x and 6.0.x images.

Vulnerability analysis

The IAR details vulnerability searches against two relevant databases in November 2022.

- http://web.nvd.nist.gov/view/vuln/search
- https://www.appgate.com/support/software-defined-perimeter-support/sdp-security-advisories

The search focussed on the subset of the product that was evaluated as part of the certified TOE. One CVE (Common Vulnerability and Exposure) and seven Appgate security advisories were analysed and found to apply to versions of the TOE prior to v6.0.1.

Conclusion

After consideration of the Impact Analysis Report (IAR) provided by Teron Labs the Australian Certification Authority (ACA) has determined that the described changes are minor. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is acceptable for the maintained TOE, Appgate v6.0.

References and abbreviations

References

1. *Assurance Continuity: CCRA Requirements, version 2.2. 30-September-2021*

2. *Appgate SDP v6.0 Impact Analysis Report Version 1.0, January 25, 2023*

3. *Appgate SDP v6.0 Security Target Version 1.0, 2023-1-25*

4. *Guidance documentation:*

    a) *https://sdphelp.appgate.com/adminguide/v6.0/common-criteria.html*
    b) *https://sdphelp.Appgate.com/userguide/v6.0/*

5. *Certification Report Appgate SDP v5.4 Version 1.0, 4 April 2022 Report Identifier: AISEP-CC-CR-2022-EFT-T023*

6. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

7. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

Abbreviations

ACA	Australian Certification Authority
AISEP	Australian Information Security Evaluation Program
API	Application Programming Interface
BDR	Bi-Directional Replication
CCRA	Common Criteria Recognition Arrangement
CRL	Certificate Revocation List
CVE	Common Vulnerability and Exposure
DNS	Domain Name System
IAR	Impact Analysis Report
IdP	Identity Provider
OIDC	OpenID Connect
SDP	Software Defined Perimeter
ST	Security Target
UI	User Interface