



# Certificate Report

## Version 1.0

## 16 May 2023

## CSA_CC_22007

## For

## Waterfall WF-500 version 2

## From

## Waterfall Security Solutions Ltd.

This page is left blank intentionally

# Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

## Amendment Record

| Version | Date | Changes |
|---|---|---|
| 1.0 | 16 May 2023 | Released |

**NOTICE**

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

# Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Waterfall WF-500 version 2 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

| TOE Components | Appliance Part Number |
|---|---|
| TX Module | WF-500TX |
| RX Module | WF-500RX |

Table 1 – TOE Components

The TOE enables online transmission of data (e.g. information, alerts, files, video streams, etc.) from a designated sending network to a designated receiving network in a unidirectional mode only. No information can be transmitted in the reverse direction through the TOE. The TOE does not provide any management or auditing functionality.

The TOE can operate in four evaluated configurations (WF-500-Compact (CC), WF-500-Standard (CC), WF-500-Standard SPLIT (CC) and WF-500-Standard HOST (CC). These differing hardware configurations don't affect the functionality and the security of WF-500 version 2.

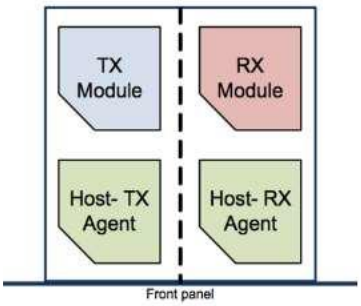
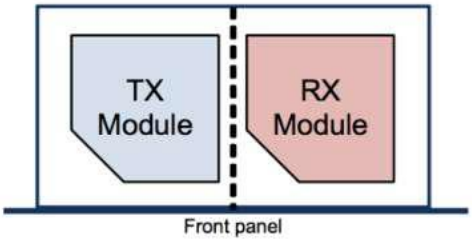
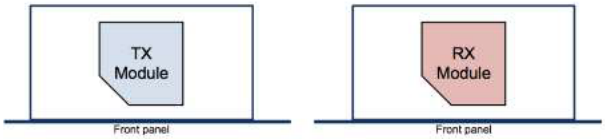
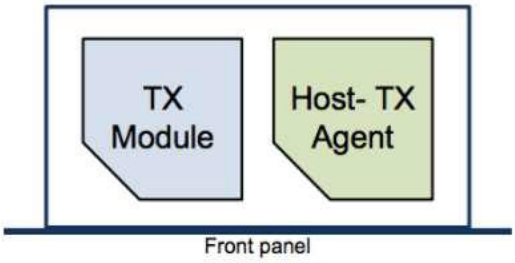
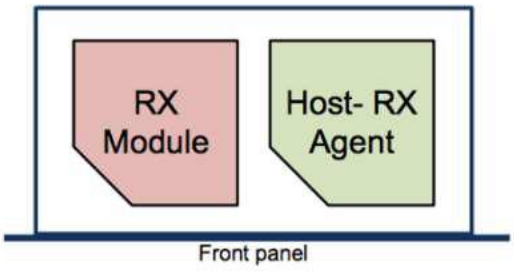
| TOE Configuration | |
|---|---|
| 1 |  <br>WF-500-Compact (CC) |
| 2 |  <br>WF-500-Standard (CC) |
| 3 |  <br>WF-500-Standard-Split (CC) |
| 4 |  <br>WF-500-Standard-Host-TX (CC) |
| |  <br>WF-500 Standard-Host-RX configuration |

Table 2 - TOE Configurations

The list of guidance documents to use with the product in its certified configuration is as follows.

| Name | Date | Method of Delivery |
|---|---|---|
| WF-500 Unidirectional Security Gateway Hardware User Guide | March 2023 | PDF by Secure-FTP or digital media secured shipment |

Table 3 - List of guidance document

The Waterfall Unidirectional Security Gateway Version 2 (i.e., the TOE) is a network gateway that enforces unidirectional information flow control policy on network traffic flowing through the gateway and does not require nor provide any management capabilities. The TOE consists of two components, the TX Module and the RX Module that is connected via a single standard fibre-optic cable.

The Agent Host function is to organise, encode, and filter data per customer specifications, and is outside the scope of evaluation.

The evaluation of the TOE has been carried out by SGS Brightsight, an approved CC test laboratory, at the assurance level CC EAL 4 augmented with ALC_DVS.2, ALC_FLR.2, AVA_VAN.5 (Advanced Methodical Vulnerability Analysis) and completed on 6 April 2023.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

| TOE Security Functionality |
| --- |
| The TOE enables online transmission of data (e.g., information, alerts, files, video streams, etc.) from a designated sending network to a designated receiving network in a unidirectional mode only. No information can be transmitted in the reverse direction through the TOE.<br><br>The TOE does not provide any management or auditing functionality |

Table 4: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

## Table of Contents

# 1 Certification

## 1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

## 1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is partially covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

# 2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **15 May 2028**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

# 3 Identification

The Target of Evaluation (TOE) is the Waterfall WF-500 version 2, and comprises of the following components and configurations:

| TOE Components | Appliance Part Number |
|---|---|
| TX Module | WF-500TX |
| RX Module | WF-500RX |

Table 5 – TOE Components

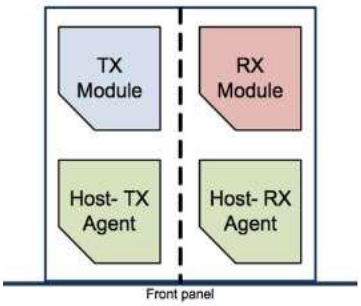
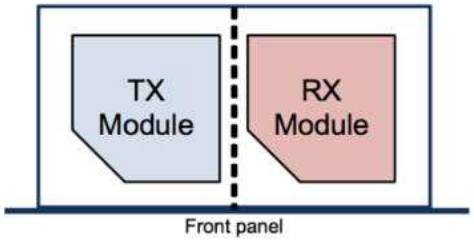
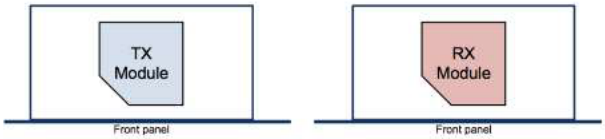
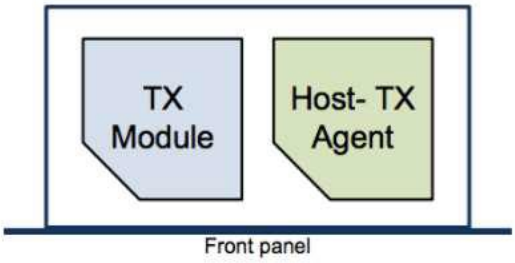
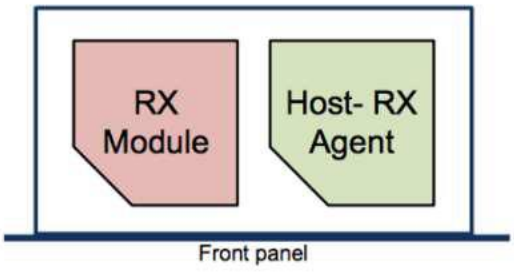
| TOE Configuration | |
|---|---|
| 1 |  <br>WF-500-Compact (CC) |
| 2 |  <br>WF-500-Standard (CC) |
| 3 |  <br>WF-500-Standard-Split (CC) |
| 4 |  <br>WF-500-Standard-Host-TX (CC) |
| |  <br>WF-500 Standard-Host-RX configuration |

Table 6 - TOE Configurations

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

| Name | Date | Method of Delivery |
|---|---|---|
| WF-500 Unidirectional Security Gateway Hardware User Guide | March 2023 | PDF by Secure-FTP or digital media secured shipment |

Table 7 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

| | |
|---|---|
| TOE | Waterfall WF-500 version 2 |
| Security Target | Waterfall Unidirectional Security Gateway WF-500 Ver 2, Security Target Version 3.0 |
| Developer | Waterfall Security Solutions Ltd |
| Sponsor | Waterfall Security Solutions Ltd |
| Evaluation Facility | SGS Brightsight |
| Completion Date of Evaluation | 6 April 2023 |
| Certification Body | Cyber Security Agency of Singapore (CSA) |
| Certificate ID | CSA_CC_22007 |
| Certificate Validity | 5 years from date of issuance |

Table 8: Additional Identification Information

# 4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- User Data Protection

Specific details concerning the above mentioned security policy can be found in Chapter 5 of the Security Target [1].

# 5 Assumptions and Scope of Evaluation

## 5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

| Environmental Assumptions | Description |
|---|---|
| OE.FILTER_LOW | The IT environment shall filter or transform the information transmitted through the TOE to the receiving network such that it cannot result in compromise of the integrity of hosts or processes on the receiving network. |
| NOE.PHYSICAL | The intended operation environment shall prevent unauthorized physical access to the TOE and to the fibre optic cable connecting its separate parts. |
| NOE.ADMIN | Physical access to the TOE shall be authorised only to personnel that will not attempt to circumvent the TOE's security functionality. |

Table 9: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

## 5.2 Clarification of Scope

Waterfall software configurations are performed on Agent Host Modules to organise, encode, and filter data per user specifications. The Agent Host Modules are outside the scope of evaluation.

The scope of evaluation is limited to the claims made in the Security Target [1].

Users are reminded to set up the TOE as per guidance Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

## 5.3 Evaluated Configuration

The TOE consists of two parts of the network gateway that enforces a unidirectional information flow through the gateway. The TX module picks up network frames from a sending network (A), and forwards them to the receiver module (RX) for transmission to a receiving network (B). The TOE hardware ensures that no information can flow from the receiving network to the sending network.

## 5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

## 5.5 Non-TOE Components

The TOE does not require additional components for its operation.

# 6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

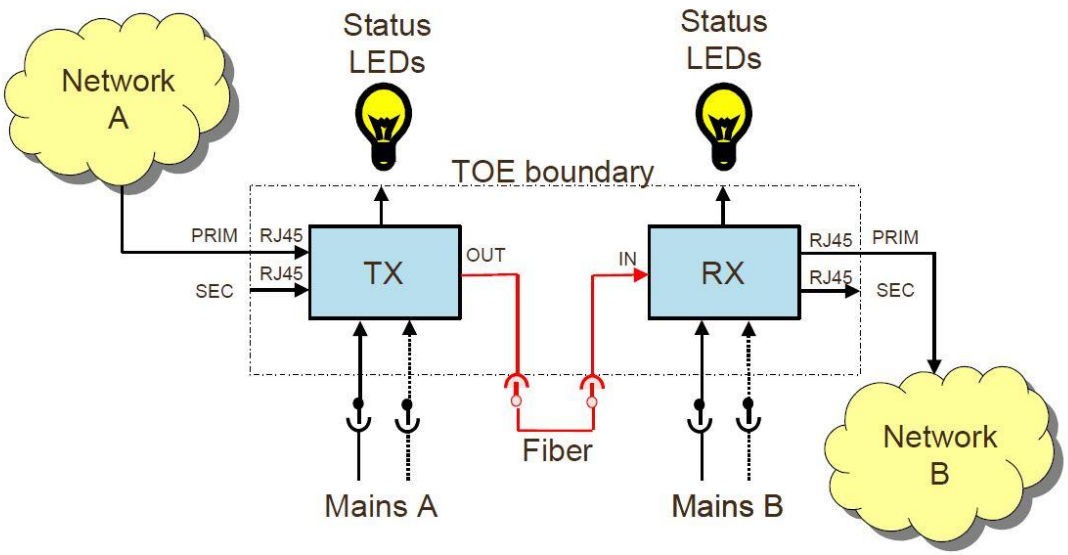



Figure 1 - Logical Architecture of the TOE

The subsystem TX contains a laser LED that converts electronic signals to light. The subsystem RX contains a photoelectric cell that can sense light and convert it to electronic signals. The fibre optic cable (outside the scope of evaluation) allows light to move from the TX to the RX.

The TX and RX subsystem share a common design. The main components include power supplies, PCB and a Small Form-factor Pluggable (SFP). The PCB contains a module that forward network frames to the SFP or receives them from the SFP. This module initialises other modules on the PCB. These modules do not contribute to the unidirectionality of the information flow. The SFP is essential for providing unidirectionality. The SFP is based on a standard optical network transceiver/receiver component. It is custom-made for Waterfall. For the TX subsystem the receiver part is removed. For the RX subsystem the transceiver part is removed. The two SFPs in combination with the design of the PCB make the unidirectionality of the TOE.

# 7 Documentation

The evaluated documentation as listed in

| *Name* | Date | Method of Delivery |
|---|---|---|
| WF-500 Unidirectional Security Gateway Hardware User Guide | March 2023 | PDF by Secure-FTP or digital media secured shipment |

Table 7 - Guidance Document (part of TOE deliverables) is being provided

with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

# 8 IT Product Testing

## 8.1 Developer Testing (ATE_FUN)

### 8.1.1 Test Approach and Depth

The developer performed functional testing covering all TSFIs and module-to-module interactions to demonstrate standard unidirectional operation, inactivity of unused RJ45 port, and performance testing.

### 8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9].

### 8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

## 8.2 Evaluator Testing (ATE_IND)

### 8.2.1 Test Approach and Depth

Evaluation results from previous CC Certification (2017) were considered, with new assessments and verdicts updated for current TOE. A fresh Vulnerability Assessment was performed for the current CC evaluation.

Developer’s tests were repeated with no findings.

The evaluator analysed the design and developer testing, and based on this analysis concentrated the tests in the areas that were not completely clear from the design.

### 8.2.2 Test Configuration

A detailed test description was provided in the ATE document. The Waterfall WF-500 version 2 (Standard Configuration) was configured for the evaluator test environment. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

### 8.2.3 Test Results

The developer’s test reproduced were verified by the evaluator to conform to the expected results from the test plan.

## 8.3 Penetration Testing (AVA_VAN)

### 8.3.1 Test Approach and Depth

The AVA_VAN.5 assurance class requires the evaluator to conduct a methodical vulnerability analysis based on publicly available source of information and based on structured examination of the evidence while performing previous evaluation activities (ASE, ADV, AGD, ATE).

The evaluator's strategy for performing vulnerability analysis was based on the following:

1. Identification of areas of concern using the generic weaknesses enumeration database Common Weakness Enumeration, version 3.1 as inspiration and the CEM.
2. Collecting possible vulnerabilities from the design assessment by asking security questions inspired by generic weaknesses separately for all security implementations of the TOE.
3. Collecting possible vulnerabilities from applicable attack lists and public vulnerability search
4. These security relevant questions are then translated into TOE-specific possible vulnerabilities (uniquely identified with POS_VUL_xxx)
5. The evaluator argues whether a possible vulnerability is removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. If yes, the possible vulnerability is considered as solved, otherwise it is uniquely labelled as potential vulnerability POT_VUL_xxx. Potential vulnerabilities are then addressed in the context of penetration tests and/or further code review.

   No potential vulnerabilities were found. The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.5) treating the resistance of the TOE to an attack with the High attack potential.

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

# 9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 augmented by ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

# 10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 3 - List of guidance document contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

No additional recommendation was provided by the evaluators.

# 11 Acronyms

| | |
|---|---|
| CCRA | Common Criteria Recognition Arrangement |
| CC | Common Criteria for IT Security Evaluation |
| CCTL | Common Criteria Test Laboratory |
| CSA | Cyber Security Agency of Singapore |
| CEM | Common Methodology for Information Technology Security Evaluation |
| cPP | Collaborative Protection Profile |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IT | Information Technology |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SCCS | Singapore Common Criteria Scheme |
| SFR | Security Functional Requirement |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |

# 12 Bibliography


[1] Waterfall Security Solutions Ltd, “Waterfall Unidirectional Secuirty Gateway WF-500 V2, Security Target Version 3.0,” 13 March 2023.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Waterfall Security Solutions Ltd, “WF-500 Unidirectional Security Gateway Hardware User Guide,” March 2023.

[10] SGS Brightsight, “Evaluation Technical Report Version 3.0 - Waterfall WF-500 version 2,” 6 April 2023.


----------End of Report ----------