CSA SINGAPORE

Singapore Common Criteria Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE

Certificate Report

Version 1.0

8 August 2025

CSA_CC_25005

For

Waterfall Unidirectional Security Gateway WF-600 Version F

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), CC:2022 Revision 1 (ISO/IEC 15408:2022) and Common Methodology for Information Technology Security Evaluation (CEM), CEM:2022 Revision 1 (ISO/IEC 18045:2022) in Singapore.

The SCCS is owned and managed by the Evaluation Authority 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.

Version	Date	Changes
1.0	8 August 2025	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 Unidirectional Security Gateway WF-600 Version F and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Hardware Identifier	Version
TX Traffic Controller, PN: WF-EBA000001	F
RX Traffic Controller, PN: WF-EBA000002	F

Table 1 - TOE components identifier

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

Name	Version	Method of Delivery
WF-600 Unidirectional Security Gateway Hardware Guide	1.5	Secure FTP or Secured Shipment

Table 2 - List of guidance documents

The TOE (network gateway) serves as the primary security mechanism that enforces unidirectional data flow between networks. It functions through a transmitting (TX) component that reads data from the sending network and a receiving (RX) component that writes this data to the receiving network. The hardware architecture ensures that reverse data flow is physically impossible. The TOE is installed within a WF-600 chassis and operates in conjunction with TX and RX Host Agent[1], however these components are beyond the scope of the TOE.

This system is frequently deployed in industrial environments, such as power plants, where it enables secure transmission of operational data to corporate networks while maintaining complete isolation of critical infrastructure from external networks.

[1] The Host Agents provide product management and monitoring capabilities and support for standard network protocols, including FTP (file transfer), SMTP (email), SNMP traps, Syslog, PI, Modbus, WMQ, ICCP, OPC-DA, and others.

Figure *1* depicts the typical usage scenario of the TOE.

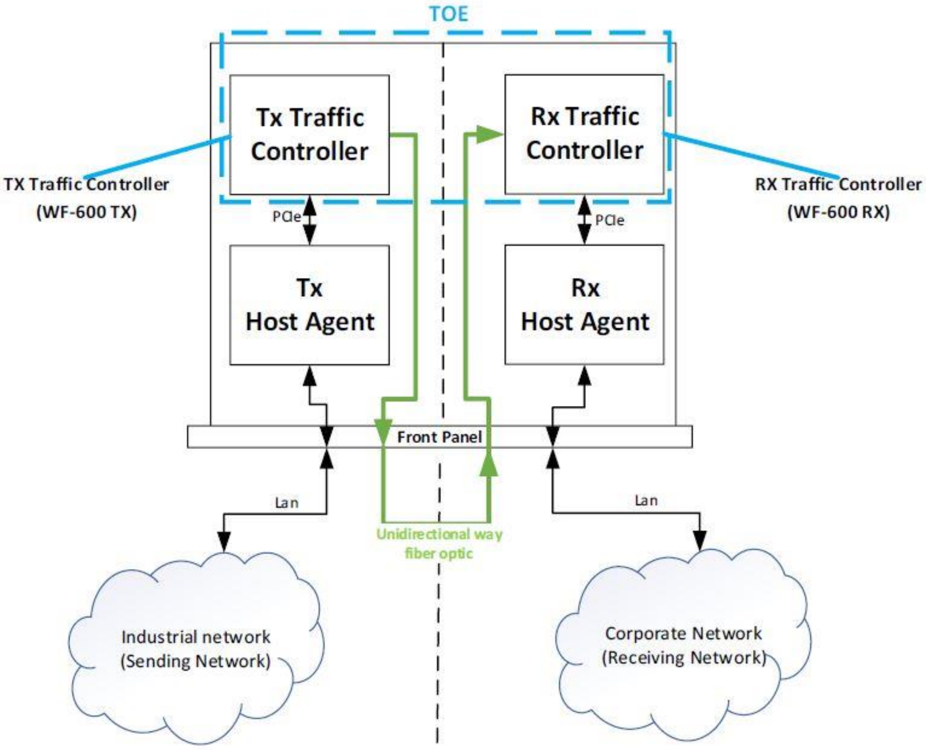
TOE
Tx Traffic Controller
Rx Traffic Controller
TX Traffic Controller (WF-600 TX)
RX Traffic Controller (WF-600 RX)
PCIe
PCIe
Tx Host Agent
Rx Host Agent
Front Panel
Lan
Lan
Unidirectional way fiber optic
Industrial network (Sending Network)
Corporate Network (Receiving Network)

Figure 1 - Typical Usage Scenario

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 AVA_VAN.5 , ALC_DVS.2, and ALC_FLR.2 and completed on 24 July 2025.

The Evaluation Authority 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 information (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.

Table 3: 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 4 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 Evaluation Authority conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, November 2022 CC:2022 Revision 1 [2] [3] [4] [5] [6];
- Common Methodology for IT Security Evaluation (CEM), November 2022 CEM:2022 Revision 1 [7]; and
- SCCS scheme publications**Invalid source specified.Invalid source specified.Invalid source specified.**

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 **7 August 2029**[2].

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.

[2] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in CCC SP-101-3 Publication #3 [11]. 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: Waterfall Unidirectional Security Gateway WF-600, Revision F.

The following table identifies the TOE deliverables.

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

Table 4 - TOE Deliverables

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

Name	Version	Method of Delivery
WF-600 Unidirectional Security Gateway Hardware Guide	1.5	PDF by Secure-FTP or digital media secured shipment

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	Waterfall Unidirectional Security Gateway WF-600 Version F
Security Target	WF-600 Waterfall-Security Unidirectional Security Gateway Security Target Version 2.0," April 2025
Developer	Waterfall Security Solutions, Ltd
Address of Developer	14 Hamelacha St., Afek Industrial Park, Rosh Ha'ayin, Israel 4809133
Sponsor	Waterfall Security Solutions, Ltd
Address of Sponsor	14 Hamelacha St., Afek Industrial Park, Rosh Ha'ayin, Israel 4809133
Evaluation Facility	SGS Brightsight BV
Completion Date of Evaluation	24 July 2025
Evaluation Authority	Cyber Security Agency of Singapore (CSA)
Address of Evaluation Authority	5 Maxwell Road Level 3, Tower Block, MND Complex, 069110
Certificate ID	CSA_CC_25005
Certificate Validity	5 years from date of issuance

Table 6: 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 a compromise of the integrity of hosts or processes on the receiving network. Note: The Waterfall TX and RX Host Agent Modules (considered to be in the IT environment) proxy the information transmitted through the TOE to the receiving network, thereby implementing a restrictive traffic filter that allows only a specific unidirectional protocol stream into the receiving network. This filtering functionality is not being evaluated in the context of this Security Target
OE.PHYSICAL	The intended operation environment shall prevent unauthorized physical access to the TOE and to the unidirectional fiber-optic cable connecting its separate parts.
OE.ADMIN	Physical access to the TOE shall be authorized only to personnel who will not attempt to circumvent the TOE's security functionality.
OE.NETWORK	The TOE is the only interconnection between the sending and receiving networks.

Table 7: Environmental Assumptions

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

5.2 Clarification of Scope

The TOE is installed within a WF-600 chassis and operates in conjunction with TX and RX Host Agent[3], however these components are beyond the scope of the TOE.

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 documents to correctly deploy and use the TOE in the evaluated configuration.

[3] The Host Agents provide product management and monitoring capabilities and support for standard network protocols, including FTP (file transfer), SMTP (email), SNMP traps, Syslog, PI, Modbus, WMQ, ICCP, OPC-DA, and others.

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 component picks up network frames from a sending network and forwards them to the receiver component (RX) for transmission to a receiving network. The TOE 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

As clarified in section 5.2 the TOE is required to be installed within the WF-600 chassis, and works in conjunction with the TX and RX Host Agent.

6 Architecture Design Information

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

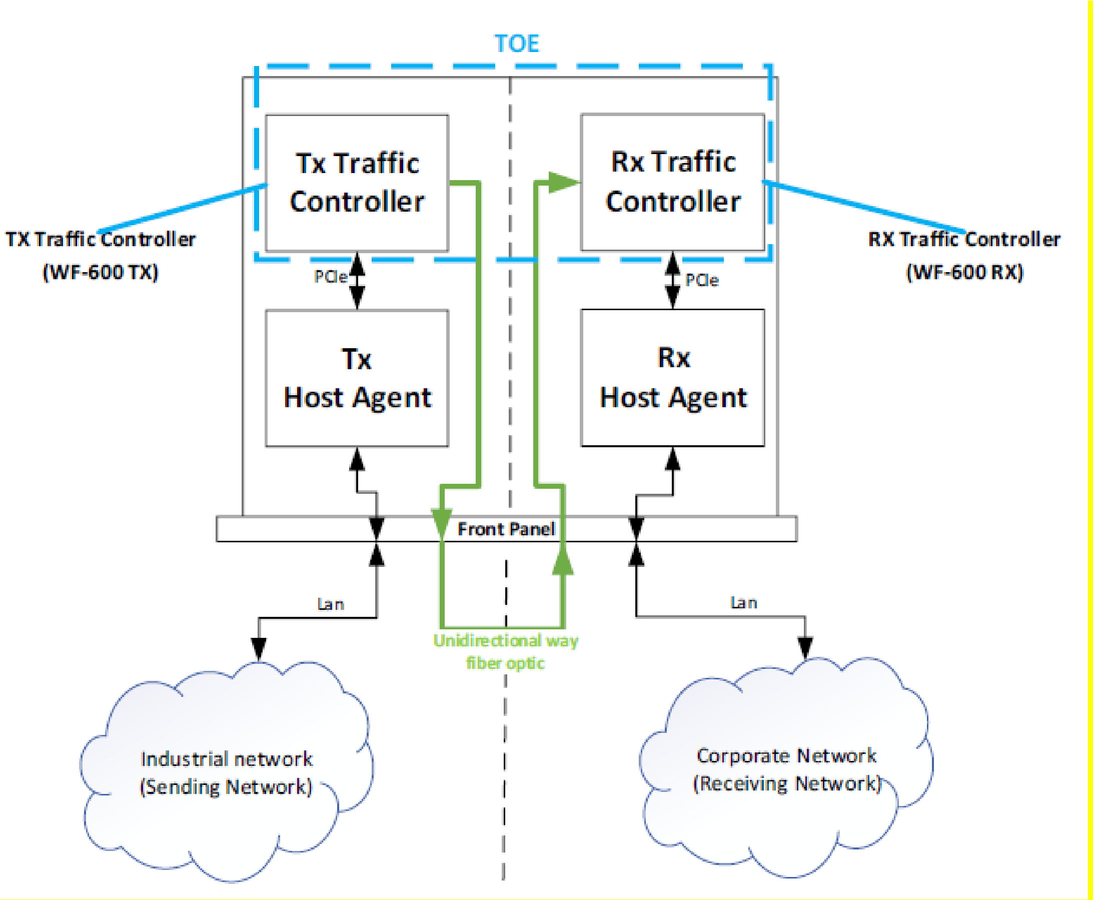
TOE
Tx Traffic Controller
Rx Traffic Controller
TX Traffic Controller (WF-600 TX)
RX Traffic Controller (WF-600 RX)
PCIe
PCIe
Tx Host Agent
Rx Host Agent
Front Panel
Lan
Lan
Unidirectional way fiber optic
Industrial network (Sending Network)
Corporate Network (Receiving Network)

Figure 2 - Logical Architecture of the TOE (From [ST])

WF-600 Waterfall-Security TOE consists of the following components:

1. TX Traffic Controller
2. RX Traffic Controller
3. TOE Guidance

Each of the Traffic Controllers performs a specific function:

1. The Waterfall TX Traffic Controller receives information from a Host Agent software and transmits information via a unidirectional fiber optic cable to the RX Traffic Controller.
2. The Waterfall RX Traffic Controller receives information from the TX Traffic Controller via a single unidirectional fibre optic cable and sends the information to an RX Host Agent.

The TX Host Agent transmits information from the TX network to the TX Traffic Controller, and the TX Traffic Controller sends the data to the RX Traffic Controller. The RX Traffic Controller received information from the TX Traffic Controller. The received information is sent to the RX Host Agent, and the RX Host Agent sends the information to the corporate network. The Host Agent's function is to organize, encode, and filter information per customer specifications. All Waterfall-Security software configurations are performed on the Host Agent. The TX and RX Host Agent is not included in the TOE.

The TX Traffic Controller uses an SFP that contains a laser diode that only transmits the light, that converts electronic signals to light. The RX Traffic Controller contains a photoelectric cell that can sense light and convert it to electronic signals. The TX and RX Traffic Controllers are connected via a single standard unidirectional fibre-optic cable, allowing light to be transmitted from the TX laser diode to the RX photoelectric cell.

The TOE has the following features:

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

7 Documentation

The evaluated documentation as listed in

Name	Version	Method of Delivery
WF-600 Unidirectional Security Gateway Hardware Guide	1.5	PDF by Secure-FTP or digital media secured shipment

Table 5 - 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.

Testing (1) demonstrating uni-directionality and direction of information flow, (2) demonstrating that the SFPs of the TX and RX module enforce uni-directionality and (3) tests on TX and RX controller voltage were performed.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [8]

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

The evaluator selected tests from the developer tests to be repeated. The selection includes tests which focus on:

- Verifying the claimed security functionality – unidirectional data transfer
- Verifying implemented security mechanism – modified SFPs
- Verifying the TOE operation in High Availability setup

8.2.2 Test Configuration

The developer provided the test environment for the testing, where the evaluator (1) witnessed the repeated tests performed by the developer and (2) performed additional testing.

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 and additional testing performed by the evaluation attained expected results.

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 open source publicly maintained weakness enumeration database. Areas of concerns includes Accessibility, Cryptography, Secure Channel etc.
2. Collecting possible vulnerabilities from the design assessment by asking security questions
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
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 labelled as potential vulnerability. Potential vulnerabilities are then addressed in the context of penetration tests and/or further code review.

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.

Penetration Test	Description
PEN_1: Indication LED	Verify if LED output from the TX board contains relevant network data
PEN_2: Leakage through TX power interfaces	Verify if power interfaces contain relevant network data
PEN_3: Leakage through RX power interfaces	
PEN_4: Leakage through EM interfaces inside the metal chassis	Verify if data is leaked via EM radiation
PEN_5: Leakage of EM signals near TX power input	
PEN_6: Force TX optical transmitter port	Verify the absence of useful information inside TX and RX module when data is forced in via the opposite direction
PEN_7: Force TX optical receiver port	

Table 8 - Penetration Test Case

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 2 - List of guidance documents 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.

Please refer to https://waterfall-security.com for information pertaining to the product security support duration.

- No additional recommendation was provided by the evaluators.
- The Evaluation Authority provided the additional comments:
    - As clarified in section 5.2 the TOE is required to be installed within the following non-TOE components - WF-600 chassis, TX and RX Host Agent which are outside the scope of the evaluation.

List of Applicable SCCS Publications

Developers and CCTLs are required to comply with the latest SCCS Publications at the time of application.

Please list the up-to-date SCCS Publications along with their version numbers that are being complied with at the time of application:

- SCCS Publication #1, #2 and #3 v9.0
- Certification Application Form v4.0
- Preliminary Assessment Report Version 1.0

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 Solution Ltd, “WF-600 Waterfall-Security Unidirectional Security Gateway Security Target Version 2.0,” April 2025.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model. [Document Number CCMB-2022-11-001], CC:2022 Revision 1,” November 2022.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components. [Document Number CCMB-2022-11-002], CC:2022 Revision 1,” November 2022.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components. [Document Number CCMB-2022-11-003], CC:2022 Revision 1,” November 2022.

[5] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation – Part 4: Framework for the specification of evaluation methods and activities. [Document Number CCMB-2022-11-004], CC:2022 Revision 1,” November 2022.

[6] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation – Part 5: Pre-defined packages of security requirements. [Document Number CCMB-2022-11-005], CC:2022 Revision 1,” November 2022.

[7] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2022-11-006], CC:2022 Revision 1,” November 2022.

[8] Waterfall Security Solutions Ltd, “WF-600 Unidirectional Security Gateway Hardware Guide Version 1.5,” August 2024.

[9] Brightsight B.V., “Evaluation Technical Report “Waterfall Unidirectional Security Gateway WF-600”,” 24 July 2025.

[10] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 9.0,” 2025.

[11] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 9.0,” 2025.

[12] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 9.0,” 2025.

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