Certification Report

Waterfall Unidirectional Security Gateway WF-500, Version 2.0

Sponsor and developer: ***Waterfall Security Solutions, Ltd.***
14 Hamelacha St., Afek Industrial Park
Rosh Ha'ayin, 4809133
Israel

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0618820-CR**

Report version: **1**

Project number: **0618820**

Author(s): **Denise Cater**

Date: **24 March 2023**

Number of pages: **11**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Waterfall Unidirectional Security Gateway WF-500, Version 2.0. The developer of the Waterfall Unidirectional Security Gateway WF-500, Version 2.0 is Waterfall Security Solutions, Ltd. located in Rosh Ha'ayin, Israel and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a network gateway that enforces a unidirectional information flow policy on network traffic flowing through the gateway. The TOE consists of two modules. The transceiver model (TX) picks up network frames from a sending network (A), and forwards them to the receiver model (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. The two models are connected via a single standard fiber-optic cable. This cable is not part of the TOE. There are four different hardware configurations for WF-500, for WF-500-Compact and WF-500-Standard-Split, and the host agents exist in the same cabinet. However, those agents are out of scope of the TOE as well.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 24 March with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Waterfall Unidirectional Security Gateway WF-500, Version 2.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Waterfall Unidirectional Security Gateway WF-500, Version 2.0 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.2 (Flaw reporting procedures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Waterfall Unidirectional Security Gateway WF-500, Version 2.0 from Waterfall Security Solutions, Ltd. located in Rosh Ha'ayin, Israel.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	WF-500 The evaluated hardware configurations of the TOE are: • WF-500-Compact (CC) • WF-500-Standard (CC) • WF-500-Standard SPLIT (CC) • WF-500-Standard HOST (CC)	Version 2
Firmware	Embedded in hardware	n/a

To ensure secure usage a set of guidance documents is provided, together with the Waterfall Unidirectional Security Gateway WF-500, Version 2.0. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

The TOE is a network gateway that enforces a unidirectional information flow policy on network traffic flowing through the gateway. The TOE consists of two modules. The transceiver module (TX) reads network frames from the sending network, and transmits them to the receiver module (RX) for writing to the receiving network. The TOE hardware ensures that no information can flow from the receiving network to the sending network. The two modules are connected via a single standard fiber-optic cable.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

Only the following cabinet configurations are part of the certification:

- WF-500-Compact (CC)
- WF-500-Standard (CC)
- WF-500-Standard SPLIT (CC)
- WF-500-Standard HOST (CC)

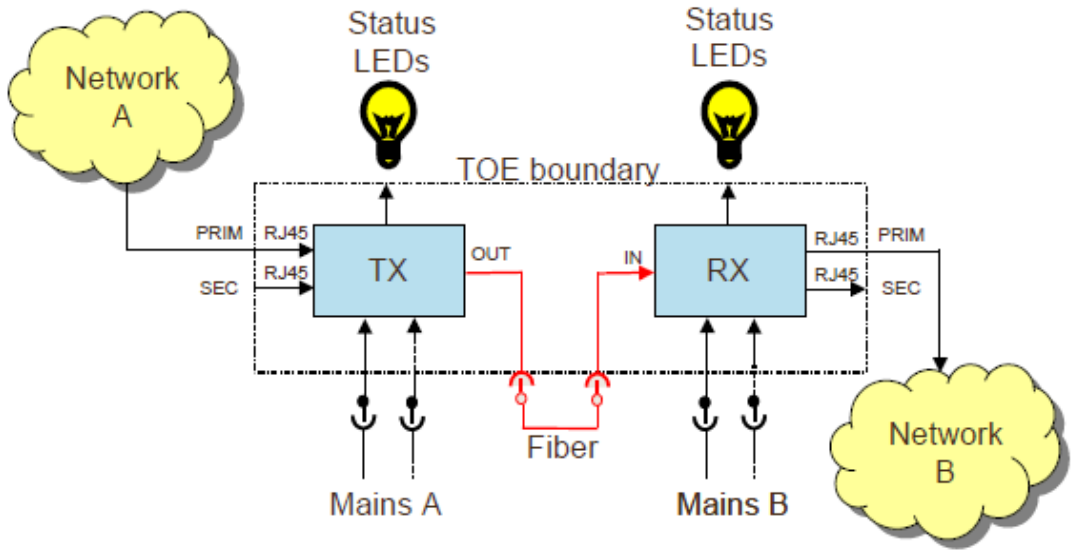
2.4 Architectural Information

The general architecture consists of two subsystems:

- The TX subsystem providing:
  - Read information from the sending network A
  - Transmit information to the RX (over fiber-optic cable)

- The RX subsystem providing:
  - Receive information from the TX subsystem
  - Write information to the receiving network B

In the figure below, the TOE is depicted in its operational environment. The TOE operates in a will be located within controlled access facility. The information flows through the primary RJ45 port (PRIM). The secondary RJ45 port (SEC) for TX is disabled, and the secondary RJ45 port (SEC) for RX is also not to be used. The TOE contains LED to on the front panel to indicate the status 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 fiber-optic cable allows light to move from the TX to the RX.

The TOE Security Functionality is implemented entirely in hardware. The TOE also contains firmware that implements functionality such as control of the front-panel display LEDs.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	**Version**
Waterfall WF-500 Unidirectional Security Gateway Hardware User Guide	Publication Date March 2023

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed testing on functional specification and subsystem level, and included test categories to:

- Demonstrate standard unidirectional operation
  - Demonstrate uni-directionality
  - Demonstrate uni-directionality when in Power Off state. Test LEDs interface
- Show that secondary RJ45 port is inactive

- Test individual TX and RX unidirectional functions by host with optical link
- Test galvanic properties by replacing dedicated SFP's for standard types
- Performance testing (changing transmission rates, changing bandwidths, file transfer, availability)

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests.

The evaluator created and executed additional functional test cases test to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

The evaluator conducted an advanced 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 first step of this type of vulnerability analysis is the identification of areas of concern (as defined in [CEM] and the [CWE]). The areas of concern are identified by the evaluator using the generic weaknesses enumeration database [CWE] version 3.1 as inspiration and the [CEM, Appendix B].
- The evaluator then collected possible vulnerabilities from the design assessment by asking security questions inspired by generic weaknesses separately for all security implementations of the TOE, and collected possible vulnerabilities from applicable attack lists and public vulnerability search.
- These security relevant questions were then translated into TOE-specific possible vulnerabilities. From this analysis the evaluator determined whether a possible vulnerability was removed or sufficiently mitigated by the TOE implementation/environment/functional testing evidence. If yes, the possible vulnerability was considered as resolved, otherwise it was labelled as a potential vulnerability. Potential vulnerabilities were then addressed in the context of penetration tests and/or further code review.

The total test effort expended by the evaluators was 4 weeks. During that test campaign, 75% of the total time was spent on side-channel testing and 25% on physical tests.

2.6.3 Test configuration

The Waterfall WF-500 Version 2 Compact Configuration was used for developer testing.

Final evaluator testing was performed the Waterfall WF-500 Version 2 Standard Configuration. Some earlier evaluator testing was performed using configuration WF-500 Version 1 Compact Configuration. The evaluator analysed the differences between Version 1 and Version 2 of the hardware (and embedded firmware) and provided a justification that the test results obtained on the WF-500 Version 1 Compact Configuration were equally applicable to the WF-500 Version 2 Compact Configuration.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

In this security evaluation direct re-use has been made of previous evaluation results on the previous product certified on 10 April 2017 under NSCIB-CC-17-119023. Verification of the similarity of the newer hardware platforms with the older hardware platforms has been performed using the developers Impact Analysis Report (IAR). The original evaluator evidence has been updated to address all changes and full independent and penetration testing has been repeated on the newer hardware platforms. A new site audit was performed as part of this evaluation activity.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Waterfall Unidirectional Security Gateway WF-500, Version 2.0. Details of how to verify the TOE version are provided in the Hardware User Guide section 4.2.1

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Waterfall Unidirectional Security Gateway WF-500, Version 2.0, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

Details of the TOE hardware configurations is given in the Hardware User Guide sections 3.3.1, 3.3.4, 3.3.5, and 3.3.7 Other hardware configurations as mentioned in [AGD] sections 3.3.2, 3.3.3, 3.3.6, and 3.3.8 are not claimed in the [ST] and are not covered by this certification. In addition, only the Tx A and Rx A network ports can be used to operate in accordance with the evaluated configuration. The Tx B and Rx B network ports must not be used.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

3 Security Target

The Waterfall Unidirectional Security Gateway WF-500 V2, Security Target Version 3, 13 March 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
Rx	Receive
TOE	Target of Evaluation
Tx	Transmit

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “Waterfall WF-500 version 2” – EAL4+, 22-RPT-1027, v4.0, 23 March 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Waterfall Unidirectional Security Gateway WF-500 V2, Security Target Version 3, 13 March 2023

(This is the end of this report.)