

Certification Report

Waterfall Unidirectional Security Gateway, WF-500, Version 1

Sponsor and developer: **Waterfall Security Solutions Ltd.**
16 Hamelacha St., Afek Industrial Park
48091 Rosh Ha'ayin
Israel

Evaluation facility: **Brightsight**
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-119023-CR**

Report version: **1**

Project number: **NSCIB-CC-119023**

Author(s): **NLNCSA**

Date: **10 April 2017**

Number of pages: **12**

Number of appendices: **0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Certificate

Standard Common Criteria for Information Technology Security Evaluation (CC),
Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number **CC-17-119023**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder
and developer

Waterfall Security Solutions Ltd.

**16 Hamelacha St., Afek Industrial Park, 48091 Rosh
Ha'ayin, Israel**

Product and
assurance level

**Waterfall Unidirectional Security Gateway, WF-500,
Version 1.**

Assurance Package:

- EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5

Project number

NSCIB-CC-119023

Evaluation facility

Brightsight BV located in Delft, the Netherlands



Common Criteria Recognition
Arrangement for components
up to EAL2

Applying the Common Methodology for Information Technology Security
Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.



SOGIS Mutual Recognition
Agreement for components up
to EAL4

Validity

Date of issue : **10-04-2017**

Certificate expiry : **10-04-2022**



PRODUCTS
RvA C 078
Accredited by the Dutch
Council for Accreditation

A handwritten signature in blue ink, appearing to be 'G. J. van der...'.

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

CONTENTS:

| | |
|--|-----------|
| Foreword | 4 |
| Recognition of the certificate | 5 |
| International recognition | 5 |
| European recognition | 5 |
| 1 Executive Summary | 6 |
| 2 Certification Results | 7 |
| 2.1 Identification of Target of Evaluation | 7 |
| 2.2 Security Policy | 7 |
| 2.3 Assumptions and Clarification of Scope | 7 |
| 2.4 Architectural Information | 8 |
| 2.5 Documentation | 8 |
| 2.6 IT Product Testing | 9 |
| 2.7 Re-used evaluation results | 10 |
| 2.8 Evaluated Configuration | 10 |
| 2.9 Results of the Evaluation | 10 |
| 2.10 Comments/Recommendations | 10 |
| 3 Security Target | 11 |
| 4 Definitions | 11 |
| 5 Bibliography | 12 |

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 license 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, in order 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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: <http://www.commoncriteriaportal.org>.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: <http://www.sogisportal.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 1. The developer of the Waterfall Unidirectional Security Gateway 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 Target of Evaluation – TOE (i.e., the Waterfall Unidirectional Security Gateway, WF-500, Version 1) 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. This cable is not part of the TOE.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 April 2017 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, 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 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 it 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 4 [CEM], for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 [CC].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Waterfall Unidirectional Security Gateway, WF-500, Version 1 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. It should be noted that the certification results only apply 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 releasable 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 1 from Waterfall Security Solutions Ltd. located in Rosh Ha'ayin, Israel.

The TOE is comprised of TX Modules (WF-500TX) and RX Modules (WF-500RX) organised in the following product configurations:

| Delivery item type | Identifier | Version | Medium |
|--------------------|--|---------|--|
| Hardware | WF-500 (includes a number of pre-configured arrangements) <ul style="list-style-type: none"> ⌵ WF-500 Compact ⌵ WF-500 Standard ⌵ WF-500 Standard split ⌵ WF-500 Standard Host TX or Standard Host RX | 1 | 19" rack cabinet |
| Firmware | Internal, part of WF-500 | V60.3 | Preloaded on an appliance during manufacturing |

To ensure secure usage a set of guidance documents is provided together with the Waterfall Unidirectional Security Gateway. Details can be found in section 0 of this report.

2.2 Security Policy

The Target of Evaluation – TOE (i.e., the Waterfall Unidirectional Security Gateway, WF-500, Version 1) 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. Assumptions and Clarification of Scope

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the [ST].

- ∅ The intended operation environment shall prevent unauthorized physical access to the TOE and to the fiber-optic cable connecting its separate parts.
- ∅ Physical access to the TOE shall be authorized only to personnel that will not attempt to circumvent the TOE's security functionality.
- ∅ The TOE is the only interconnection between the sending and receiving networks.

2.3.2 Clarification of scope

The Security Target [ST] assumes an operational environment such that threats could come only from the attached networks. From these threats T.HACK_LOW as defined in the Security Target [ST] requires the IT environment to 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.

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

2.4 Architectural Information

There are four different hardware configurations for the Waterfall Unidirectional Security Gateway, WF-500, Version 1. The general architecture consists of two subsystems:

- ∅ the transceiver (TX) subsystem providing
 - Read information from the sending network A
 - Transmit information to the RX (via fiber-optic cable)
- ∅ the receiver (RX) subsystem providing
 - Receive information from the TX subsystem
 - Write information to the receiving network B

The TX subsystem contains a laser LED that converts electronic signals to light. The RX subsystem contains a photoelectric cell that can sense light and convert it to electronic signals. The TX subsystem and RX subsystem are connected via a single standard fiber-optic cable, allowing light to move from the TX LED to the RX photoelectric cell. The cable is not included in the TOE.

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.

In Figure 1 the TOE is depicted in its operational environment. The TOE will be located within a controlled access facility. The information flows through the primary RJ45 port (PRIM). The secondary RJ45 port (SEC) is disabled. The TOE contains LEDs on the front panel to indicate the status of the TOE.

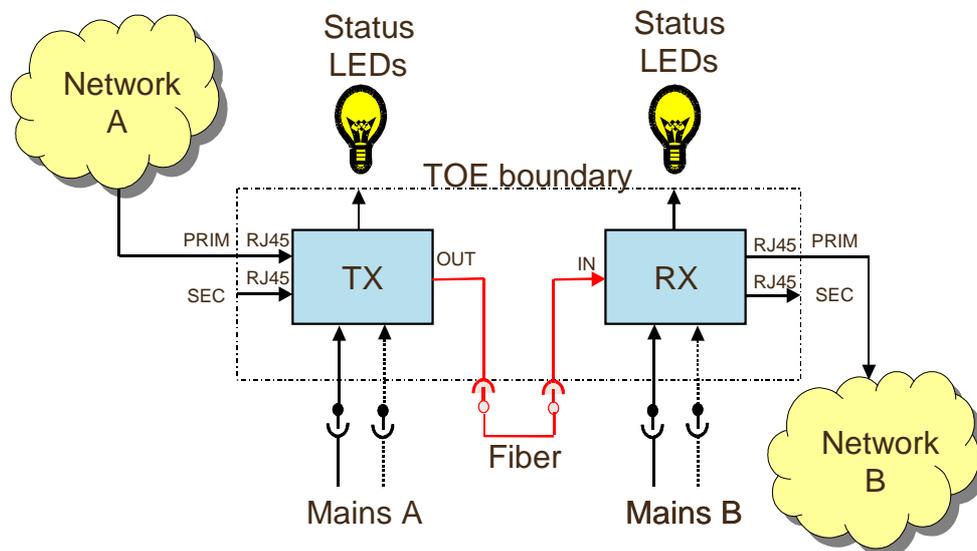


Figure 1: The TOE in its environment

2.5 Documentation

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

| Identifier | Version | Medium |
|---|------------------|-------------|
| Waterfall Unidirectional Security Gateway WF-500 Common Criteria Evaluated Configuration Guide, version 1.0.9 | November 2016 | Paper / pdf |

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 has performed testing on FSP and subsystem level including all TSFI with four defined tests.

The independent testing performed by the evaluator comprised of:

- ∅ Sample testing (4:ATE_IND.2-4) to validate the developer testing by repeating all four developer tests, as the number is small.
- ∅ Independent testing (4:ATE_IND.2-6) was performed based on 6 new tests defined by the evaluator for the validation of the correct information flow.

Before these tests were conducted it was verified that the TOE was suitable for testing and has a unique reference number as identified in the ST introduction.

2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following testing approach:

- ∅ The evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a shortlist with a number of possible vulnerabilities to be tested;
- ∅ The evaluators used CEM Annex B.2 as an additional source for possible vulnerabilities and penetration tests;
- ∅ These were presented, under NSP#6, to the certifier.

The combination of all these sources led to 6 separate penetration tests that cover the following:

- ∅ Possible side channels that allow bystanders to eavesdrop information passing through the TOE;
- ∅ Trying to cause a TOE failure such that the TOE comes in a state that it passes information through from the receiving network to the sending network.

2.6.3 Test Configuration

The tests are performed on configuration WF-500 Compact. The following figure indicates the components used in the tests.

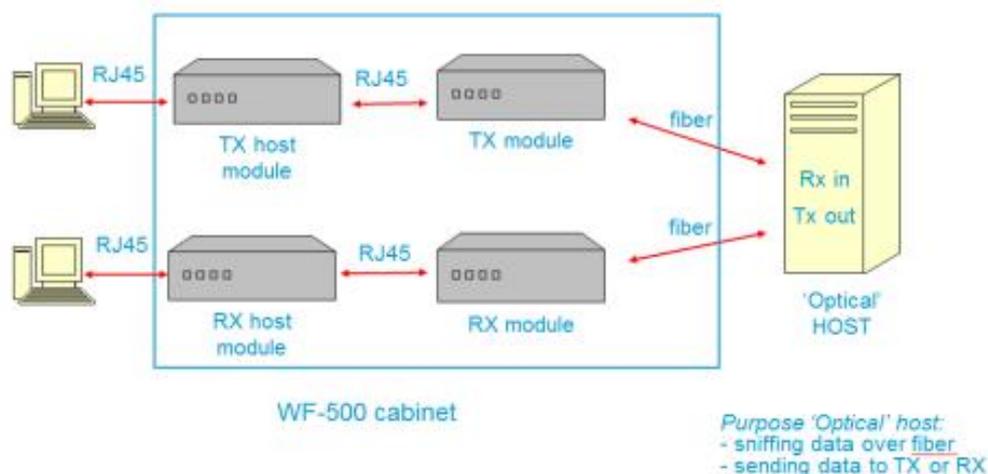


Figure 2: TOE test set-up

The penetration test set-up also included an oscilloscope to measure internal signals and an EMA coil to measure EMA signals.

2.6.4 Testing 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 Re-used evaluation results

In this security evaluation direct re-use has been made of previous evaluation results on the previous product certified on 12-07-2012 under NSCIB-CC-11-34146. 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.

There has also been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE. No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Waterfall Unidirectional Security Gateway, WF-500, Version 1 and can be identified by its identification at the backside of the appliances.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the [ETR]² which references a 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 1, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target [ST]. The Security Target does not claim conformance to any Protection Profile.

2.10 Comments/Recommendations

The customer should be aware that:

- Ø The TOE and the fiber optic link should be located within a controlled access facility that prevents any possible physical access by unauthorized personnel. Authorized personnel must not attempt to circumvent security functionality or tamper with the modules, or rewire network connections to bypass the TOE;
- Ø Use separate power and network infrastructure for the sending and receiving networks, connected to the TX and RX, respectively.
- Ø Ensure that, besides through the TOE, there are no information paths between the sending and the receiving networks that might bypass the gateway, allowing information to flow in the other direction. In particular, it is recommended to use physically separate network infrastructures for the separate networks. Relying on virtual separation mechanisms (e.g. VLANs on a shared switch) is not considered to be best practice.

² The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The Waterfall Unidirectional Security Gateway WF-500 Security Target, version 1.2, December 01, 2016 [ST] is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

| | |
|-------|---|
| EMA | Electromagnetic Analysis |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| LED | Light Emitting Diode |
| NSCIB | Netherlands scheme for certification in the area of IT security |
| NSP | NSCIB Scheme Procedure |
| PP | Protection Profile |
| TOE | Target of Evaluation |
| VLAN | Virtual LAN |

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 4, September 2012.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
- [ETR] Evaluation Technical Report Waterfall Unidirectional Security Gateway WF-500 EAL4+, 16-RPT-574, v2.0, 4 April 2017.
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
- [ST] Waterfall Unidirectional Security Gateway WF-500 Security Target, version 1.2, December 01, 2016.

(This is the end of this report).