Certification Report

Sponsor and developer:	***Waterfall Security Solutions Ltd.,*** **16 Hamelacha St., Afek Industrial Park** **Rosh Ha'ayin, 48091** **Israel**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-11-34146-CR**
Report version:	**1**
Project number:	**NSCIB-CC-11-34146**
Authors(s):	**NLNCSA**
Date:	**July 10, 2012**
Number of pages:	**17**
Number of appendices:	**0**

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

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Eindhoven:
De Rondom 1
P.O. Box 6235
5600 HE Eindhoven
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)40 265 0 302

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a
registered company with the
Amsterdam Chamber of Commerce
under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)

Certificate number **PC 4603306**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
Waterfall Security Solutions Ltd.
Located in Hamelacha 16 Afek Ind. Part,
48091 ROSH HA'AYIN ISRAEL

Product and assurance level
Waterfall Unidirectional Security Gateway model WF-400, version 1,

Assurance Package:

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

Project number **NSCIB-CC-11-34146-CR**

Evaluation facility **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. 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.

Validity
Date of issue : **12-07-2012**
Certificate expiry : **12-07-2022**

Registration number
Notified Body 0336

PRODUCTS
RvA C 078
Accredited by the Dutch
Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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.

A part of the procedure is the technical examination (evaluation) of the product 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 complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, 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 satisfies the security requirements.

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

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

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 in the technical domain of Smart cards and similar Devices. 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 and approved certification schemes can be found on: http://www.sogisportal.eu.

This evaluation contains assurance components beyond EAL4 and the product type does not fall in a technical domain for which a higher recognition level applies. Therefore the mutual recognition under the terms of the CCRA and SOGIS-MRA by the nations listed above is limited to the EAL 4 components of these assurance families.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Waterfall Unidirectional Security Gateway model WF-400, version 1. The developer of the WF-400 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 model WF-400, 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 appliances. The transceiver appliance (TX) picks up network frames from a sending network, and forwards them to the receiver appliance (RX) for transmission to a receiving network. The TOE hardware ensures that no information can flow from the receiving network to the sending network. The two appliances 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 and was completed on July 4th 2012 with the final delivery 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 certification was completed on July 10th 2012 with the preparation of this Certification Report.

The scope of the evaluation is defined by the Security Target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the 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 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 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Waterfall Unidirectional Security Gateway model WF-400, 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 model WF-400, version 1 from Waterfall Security Solutions Ltd. located in Rosh Ha'ayin, Israel. It is comprised of a pair of WF-400 appliances, including one TX appliance and one RX appliance. For each appliance type (TX or RX), two variants are supported: a single power supply variant, and a dual power-supply variant (for redundancy).

This report pertains to the TOE which is comprised of the following main components:

Delivery item type	Identifier	Version	Medium
Hardware	WF-400 (containing a pair of WF-400 appliances, including one TX appliance and one RX appliance) Appliance Part Number ¡ WF-400TX ¡ WF-400RX ¡ WF-400TX- 2PS (Dual Power) ¡ WF-400RX- 2PS (Dual Power)	1	19" rack
Firmware	Internal, part of WF-400	40	Preloaded on an appliance during manufacturing

After delivery of the TOE the packing list must be checked for the product labels (S/N on rear side).

To ensure secure usage a set of guidance documents is provided together with the Unidirectional Security Gateway. Details can be found in section 2.5 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 appliances. The transceiver appliance (TX) picks up network frames from a sending network, and forwards them to the receiver appliance (RX) for transmission to a receiving network. The TOE hardware ensures that no information can flow from the receiving network to the sending network.

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. The following topics are of relevance:

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

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled “TOE design (ADV_TDS)”. The intent of this chapter is to characterise the degree of architectural separation of the major components.

The Waterfall Unidirectional Security gateway is comprised of a pair of WF-400 appliances, including one transceiver appliance (TX) appliance and one receiver appliance (RX). For each appliance type (TX or RX), two variants are supported: a single power supply variant, and a dual power-supply variant (for redundancy).

The TX appliance contains a laser LED that converts electronic signals to light. The RX appliance contains a photoelectric cell that can sense light and convert it to electronic signals. The TX appliance and RX appliance 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 LED to on the front panel to indicate the status of the TOE.

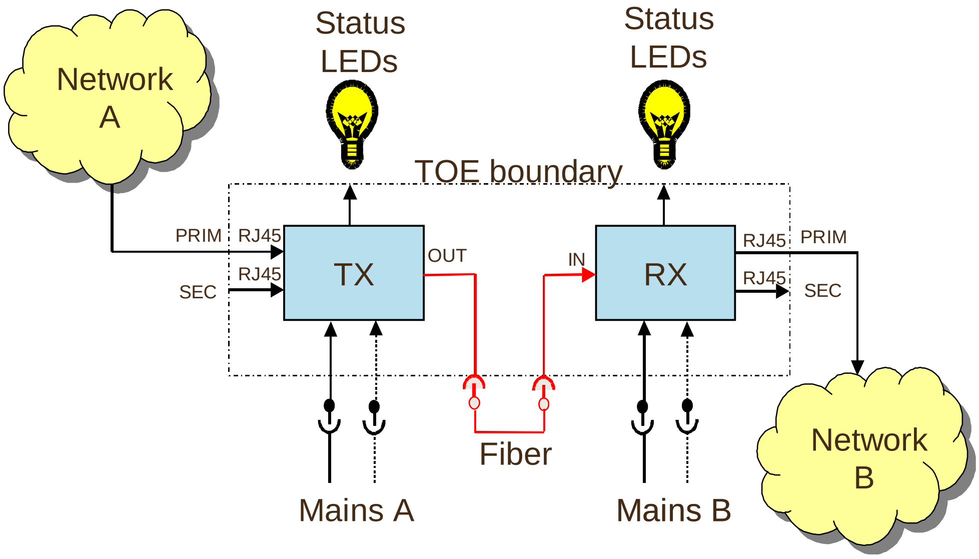

Figure 1: The TOE in its environment

2.5 Documentation

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

Identifier	Version	Medium
Waterfall Unidirectional Security Gateway Common Criteria Evaluated Configuration Guide	June 2012	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 Scheme, and in discussion with the Scheme more penetration tests emerged.

The combination of all these sources led to 5 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 a pair of appliances: WF-400-RX-2PS and WF-400-TX-2PS, that is with dual power supply.

The following figure indicates the components used in the tests.

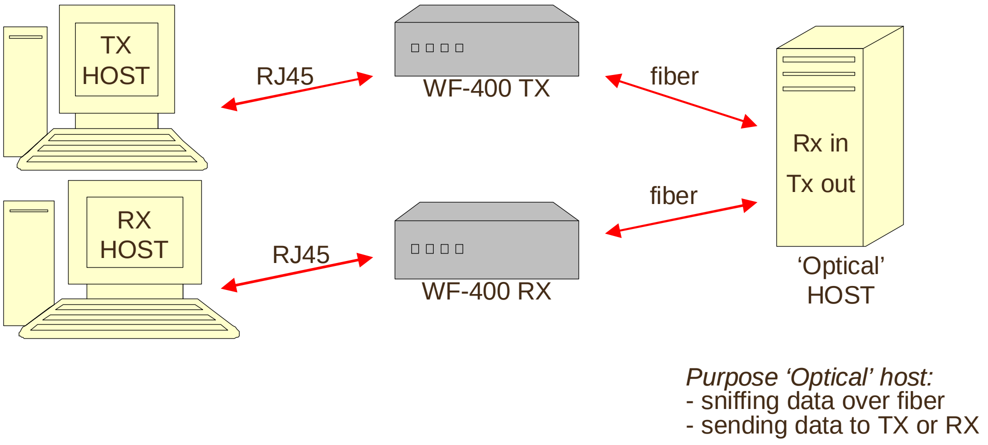
TX
HOST
RJ45
WF-400 TX
fiber
Rx in
Tx out
RX
HOST
RJ45
WF-400 RX
fiber
'Optical'
HOST
Purpose 'Optical' host:
- sniffing data over fiber
- sending data to TX or RX

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 Evaluated Configuration

The TOE is defined uniquely by its name and version number Waterfall Unidirectional Security Gateway model WF-400, version 1 and can be identified by its identification at the backside of the appliances.

The TOE needs no specific configuration settings because there is only one configuration defined.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references a ASE Intermediate Report and several other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Implementation representation	ADV_IMP.1	Pass
TOE design	ADV_TDS.3	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

Life-cycle support		**Pass**
Configuration Management capabilities	ALC_CMC.4	Pass
Configuration Management scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development security	ALC_DVS.2	Pass
Flaw remediation	ALC_FLR.2	Pass
Life-cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.1	Pass

Security Target		**Pass**
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass

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

Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass

Tests		**Pass**
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Waterfall Unidirectional Security Gateway model WF-400, version 1 to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5**. This implies that the product satisfies the security technical requirements specified in Waterfall Unidirectional Security Gateway WF-400 Security Target, version 0.72, June 29, 2012. The Security Target does not claim conformance to any Protection Profile.

2.9 Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

- The two appliances 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 appliances, or rewire network connections to bypass the TOE.
- Use separate power and network infrastructure for the sending and receiving networks, connected to the TX and RX, respectively.
- 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 infrastructure for the separate networks. Relying on virtual separation mechanisms (e.g. VLANs on a shared switch) is not considered to be best practice.
- The TOE is normally delivered together with TX and RX agent software running on servers in the sending and receiving networks, respectively. These servers cannot affect the enforcement of unidirectional information flow by the TOE and are not considered during the evaluation.

3 Security Target

The Waterfall Unidirectional Security Gateway WF-400 Security Target, version 0.72, June 29, 2012 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:

CC	Common Criteria
EMA	Electromagnetic Analysis
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LED	Light Emitting Diode
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
NSP	NSCIB Scheme Procedure
PP	Protection Profile
RX	Receiver appliance
TX	Transceiver appliance
TOE	Target of Evaluation

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 version 3.1 revision 1, and Part II and III, version 3.1 revision 3.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.

[ETR] Brightsight, Evaluation Technical Report Waterfall Unidirectional Security Gateway WF-400 – EAL4+, Version 1.0, July 4, 2012.

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[ST] Waterfall Unidirectional Security Gateway WF-400 Security Target, version 0.72, June 29, 2012.

(This is the end of this report).