Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	07/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/04/2023/RC, v1.0
Decorrenza *(Date of 1st Issue)*	22 agosto 2024
Nome e Versione del Prodotto *(Product Name and Version)*	OPSWAT NetWall Optical Diode OD-101 v1.0.1
Sviluppatore *(Developer)*	OPSWAT Inc.
Tipo di Prodotto *(Type of Product)*	Dispositivi e sistemi di protezione perimetrale (Boundary Protection Devices and Systems)
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 22 agosto 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. 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 National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) 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 Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

OPSWAT NetWall Optical Diode OD-101 v1.0.1

OCSI/CERT/CCL/04/2023/RC

Version 1.0

22 August 2024

Organismo di Certificazione della Sicurezza Informatica

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	22/08/2024

2 Table of contents

Organismo di Certificazione della Sicurezza Informatica

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

API	Application Programming Interface
CLI	Command Line Interface

Organismo di Certificazione della Sicurezza Informatica

CM	Cryptographic Module
GUI	Graphical User Interface
REST	Representational State Transfer
RX	Reception
SFP	Small Form-Factor Pluggable
SKU	Stock Keeping Unit
SSL	Secure Socket Layer
SQL	Structured Language Query
TX	Transmission
UI	User Interface
WebUI	Web User Interface

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

[AGD] AGD Documentation OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.5, 04 April 2024

[INST_GUIDE] OPSWAT NetWall OD-101 Common Criteria Evaluated Configuration Guide v1.3, Version: 1.3, 18 January 2024

[ETR2] Evaluation Technical Report OPSWAT NetWall Optical Diode OD-101 v1.0.1, OPSWATEVOD-038_ETR_v2, CCLab Software Laboratory, 09 April 2024

[ETR5] Evaluation Technical Report OPSWAT NetWall Optical Diode OD-101 v1.0.1, OPSWATEVOD-038_ETR_v5, CCLab Software Laboratory, 11 July 2024

[ST] Security Target OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.7, 22 May 2024

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT -Products. A higher recognition level for evaluations beyond EAL4 is provided for IT -Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA up to EAL4.

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**OPSWAT NetWall Optical Diode OD-101 v1.0.1**", developed by OPSWAT Inc.

The Target of Evaluation (TOE) consists of a TX Module that connects with a sending - or trusted network - and a RX Module that connects to a receiving - or untrusted - network. Both modules enforce in hardware a one-way information flow control policy on network traffic flowing through the TOE. These modules are running on a Linux based system on both the TX and RX devices.

The connection between the TX Module and RX Module consists of an optical link cable.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL4, augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2 according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "NetWall Optical Diode OD-101 v1.0.1" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	OPSWAT NetWall Optical Diode OD-101 v1.0.1
Security Target	Security Target OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.7, 22 May 2024
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5
Developer	OPSWAT Inc.
Sponsor	OPSWAT Inc.
LVS	CCLab – The Agile Cybersecurity Laboratory (Budapest site)
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	June 1, 2023
Evaluation ending date	April 10, 2024

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description it is possible to refer to the Security Target [ST].

The Target of Evaluation (TOE) is a unidirectional security gateway software using optical diodes for data transfer containing a TX Module and a RX Module services that enforce in software and hardware a one-way data flow. TX Module connects to the sending or trusted network and a RX Module connects to the receiving or untrusted Network.

The connection between the TX Module and RX Module consists of an optical link cable.

The TOE allows information such as real time process control data, syslog event records, or files to be transferred from the industrial control network to the corporate network over a dedicated and protected connection. The TOE prevents any data from flowing back to the industrial network and prevents source network identifying information such as IP address and MAC address of systems in the industrial networks from being transferred to the destination network. Only the data payload is transferred. The sending Network is fully protected against any network based cyber-attacks initiated at the receiving network, since no data can be sent from the receiving network to the sending network.

A typical usage scenario consists of a source network that represents an industrial control network, and a receiving network that represents the corporate network. Information can be shared from the industrial network to the corporate network without have corporate network connect directly to the industrial control network, preventing an attack from the external network that might impact its integrity or result in a denial of service. The TOE allows information to flow from the industrial network to the corporate network, while preventing any information from flowing back through the data diode to the industrial network. This serves to prevent a wide range of online attacks.

A second typical usage is to securely move information from an untrusted network into a secured or trusted network. For example, classified Intelligence Community or DoD networks that must receive information from a lower classified network such as the internet, while maintaining network isolation from the lower classified network. In this scenario, the TOE is configured such that the Destination Server connects to the higher security network.

Bundled with the TOE is a Web Application which allows a user (TOE Administrator – admin - only) to configure the TOE to connect to systems in the source and destination networks and configure the data type that is being transferred by the TOE. Web Application can be accessed through a browser displaying the Web App GUI.

In addition to the Web Application, there is a Command Line Interface (CLI) that can also be used to configure the system. The configuration Web Application and CLI are not included in the TOE boundary and their use is recommended for the configuration phase only and with a local, direct connection with the appliance.

The Web App allows the configuration of Industry Control protocol connector software such as Modbus, OPC DA & UA connectors that are typically provided with the TOE but reside outside the TOE boundary.

In particular, OPSWAT TX Connector (outside of the TOE) is a software that can run on the same appliance as the OPSWAT TX Module or on a server in the sending domain. The OPSWAT TX Connector forwards protocol specific data between the sending network servers and forwards this information to the OPSWAT TX Module for delivery to the other domain. The currently supported protocols are:

- Modbus
- OPC UA
- SMTP
- IEC 104
- DNP3
- MQTT
- OSI-PI

On the receiving side, OPSWAT RX Connector (outside of the TOE) is software that can run on the same appliance as the OPSWAT RX Module or on a server in the receiving domain. The OPSWAT RX Connector forwards protocol specific data between the OPSWAT RX Module and forwards to a server on the same appliance or to a server on the receiving domain.

For a detailed description of the TOE, refer to sections 1.3 and 1.4 of the Security Target [ST].

7.3.1 TOE architecture

OPSWAT NetWall OD-101 follows the hardware philosophy shown in the following Figure 1. It uses Unidirectional TX only transceiver at the sending server and RX only transceiver at the receiving server with an optical cable to connect the TX side to the RX side. These optic transceivers have been modified to allow only transmission on the TX side and reception on the RX side. Other transmission paths are physically disabled.

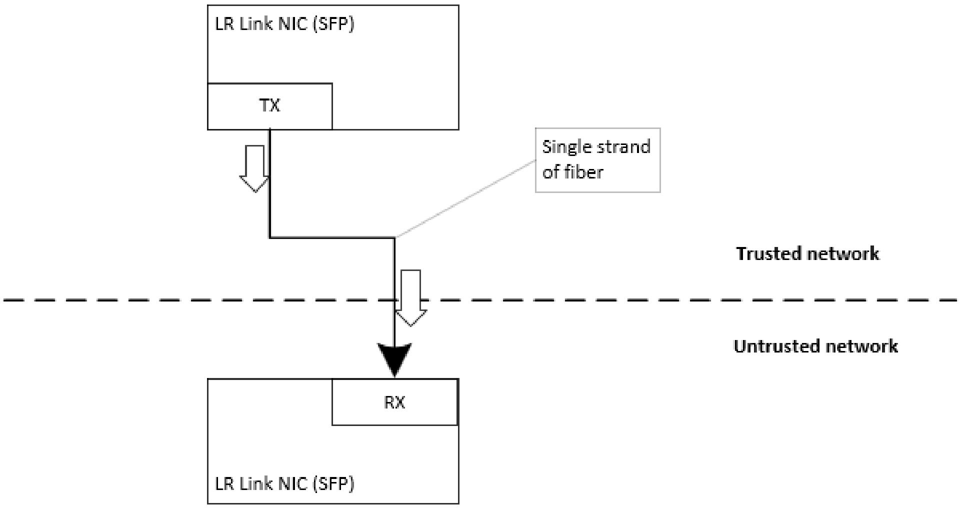

Figure 1 – Schematic description of the TOE

This creates a physical layer enforced one-way transfer of data with no back channel. OPSWAT NetWall OD-101 supports redundant optical connection providing a higher level of data delivery assurance. The TOE is divided into two different modules, OPSWAT TX Module and OPSWAT RX Module (Figure 2).

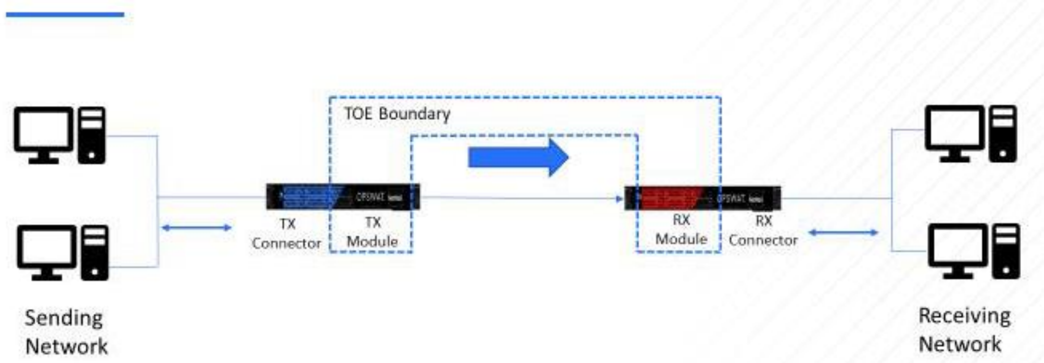

Figure 2 – TOE physical boundaries

Figure 3 shows the TOE architecture also indicating non-TOE components. The blue and red brackets are indicating the TOE itself. The TSFIs can be found in the green (inside DiodeSend or DiodeReceive) and white boxes in the blue and red brackets.

DiodeSend, SFPTX1 and SFPTX2 in the TX module and DiodeReceive, SFPRX1 and SFPRX2 constitute the TOE boundary. The OPSWAT TX Module and OPSWAT RX Module modules are placed in the BLUE and RED appliances.

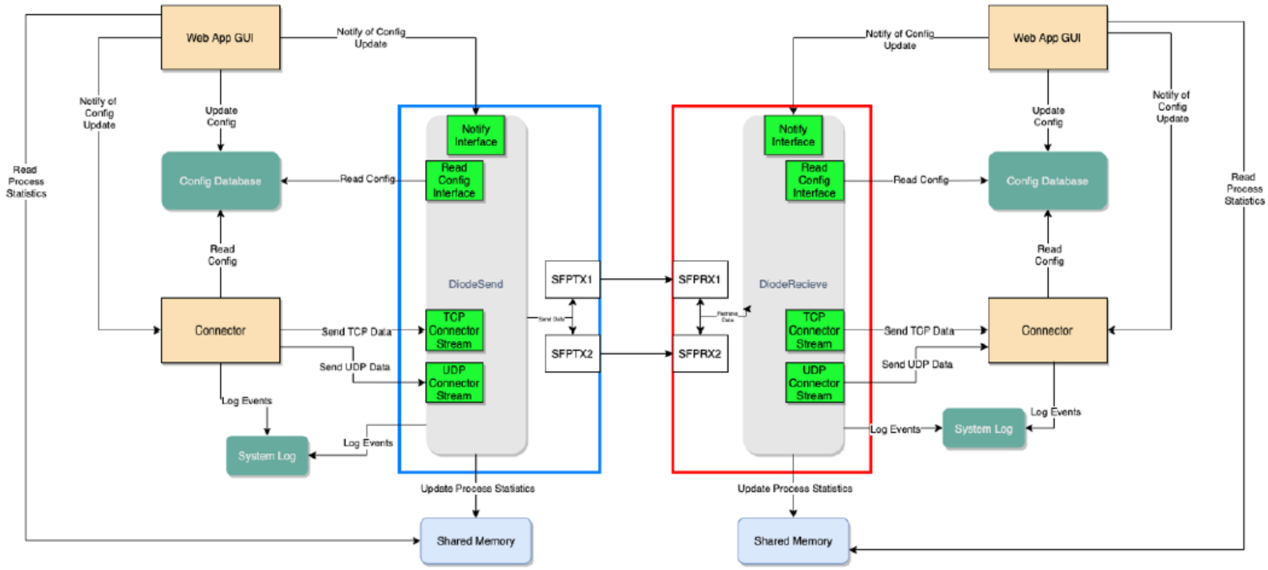

Figure 3 – TOE architecture

The TOE is a software component which is part of the whole OPSWAT NetWall Optical Diode product. The BLUE and RED appliances are running a Linux based operating system and the following services:

TOE components:

- TX Module
- RX Module

NON-TOE components:

- Web App GUI
- Config Database
- Connector

- System Log
- Shared Memory

7.3.2 TOE security features

Assumptions, threats, and security objectives are defined in section 3 and 4 of the Security Target [ST].

The major security features of the TOE are summarised in the following:

1) User data protection

TOE is implemented in two independent modules (they have independent power sources and independent optic interfaces) OPSWAT TX Module and OPSWAT RX Module. The Hardware doesn't permit more ways to transmit electronic or optic signals other than the described interfaces.

OPSWAT TX Module is connected only to the sending network through OPSWAT TX Connector (outside the TOE) and the TX Module is not connected to the receiving network. OPSWAT RX Module is only connected to the receiving network through OPSWAT RX Connector (outside the TOE).

TCP/UDP Stream

The OPSWAT TX Connector interfaces to protocol specific data between the sending network servers and forwards this information to the OPSWAT TX Module. OPSWAT TX Module will remove all routable information from the data received from OPSWAT TX Connector before sending it to the OPSWAT RX Module, performing an effective protocol break.

A fiber-optic cable connects TX and RX Modules. The fiber optic cable can be made redundant, providing a higher level of data delivery assurance. The transceivers within the TOE (SFPTX1, SFPTX2, SFPRX1 and SFPRX2) have been physically modified to support only the communication in one single direction, from TX Module to RX Module. SFPTX1 and SFPTX2 lack optics and circuitry required to receive data. SFPRX1 and SFPRX2 lack optics and circuity required to send data. This guarantees that all the information flowing through the TOE is transferred over a physically enforced one-way connection between the TX and RX Modules and therefore covered by the Unidirectional SFP.

TX Module is connected with the sending network through OPSWAT TX Connector using standard RJ45 interfaces. The TX Module cannot read information from the receiving network because its network interfaces are connected only to the sending network. The TX Module converts the incoming communication into an optic-based data transmission using a fiber-optic transceiver. This transceiver has been physically modified to support only data transmission, implementing galvanic isolation.

A fiber-optic cable connects the BLUE module to the RED module and constitutes the only connection between these two components. The fiber optic cable can be made redundant, providing a higher level of data delivery assurance. This fiber-optic cable connects to the RX Module's optic port. OPSWAT RX Module converts the incoming optical data into electronic signals using a fiber-optic transceiver. This transceiver has been physically modified to support only data reception, implementing galvanic isolation.

RX module is connected with the receiving network through OPSWAT RX Connector using standard RJ45 interfaces. OPSWAT RX Module transmits the data received from the TX Module to the OPSWAT RX Connector and, from there to the stations and servers in the receiving network. The RX Module cannot transmit information back to the sending network because its network interfaces are connected only to the receiving network and, as commented the optical transceiver in the RX Module has been physically modified to support only data reception.

Security management

Only an admin with valid credentials and a security dongle (see section 10.1) can change the configuration data and the secure attributes within the database in both sides, Sending and Receiving. The configuration data and secure attributes of the TOE cannot be modified from the TOE.

Read Config

Once the admin performs changes on the configuration data and/or secure attributes within the database using the Web App GUI and/or the CLI, the TOE will be notified about the change using the Notify of Config Update function. Once notified, the TOE will read the new configuration data using Read Config function.

A detailed description of the TOE security functionality is provided in sections 1.4 and 6 of the Security Target [ST].

7.4 Documentation

The guidance documentation specified in "Annex A – Guidelines for the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 8.2 of this report.

7.5 Protection Profile conformance claims

The TOE does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 4 assurance package, augmented with the CC part 3 components ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5.

All the SFRs have been selected from CC Part 2 [CC2].

It is possible to refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab – The Agile Cybersecurity Laboratory (Budapest site).

The evaluation was completed on April 10, 2024, with the issuance by the LVS of the approved Evaluation Technical Report [ETR2]. Following some clarifications requested by the Certification Body during the editing of the certification report the ETR was further revised with the issuance of a final version ([ETR5]).

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The Certification Body recommends reviewing the assumptions in the [ST], section 3.3, which are necessary conditions to be implemented for the TOE security:

- *A.ADMIN - Personnel with authorized physical access to the appliances where the TOE is placed, will not attempt to circumvent the TOE's security functionality or perform any malicious action.*
- *A.PHYSICAL - Appliances (including TOE, Fiber cable and Web App GUI console) will be located within secure and controlled access facilities, preventing unauthorized access.*
- *A.NETWORK - TOE will be the only communications channel between sending and receiving networks*.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR2] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "OPSWAT NetWall Optical Diode OD-101 v1.0.1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with ALC_DVS.2, ALC_FLR.2 and AVA_VAN.5 (augmentation in *italics* in Table 1).

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	*ALC_DVS.2*	*Pass*
Developer defined life-cycle model	ALC_LCD.1	Pass

Assurance classes and components		Verdict
Well-defined development tools	ALC_TAT.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential customers of the product “NetWall Optical Diode OD-101 v1.0.1” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “Security Objectives for the Operational Environment” specified in section 4 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

As mentioned in section 7.8, the Certification Body recommends reviewing the assumptions in the [ST], section 3.3, which are necessary conditions to be implemented for the TOE security:

- *A.ADMIN - Personnel with authorized physical access to the appliances where the TOE is placed, will not attempt to circumvent the TOE's security functionality or perform any malicious action.*
- *A.PHYSICAL - Appliances (including TOE, Fiber cable and Web App GUI console) will be located within secure and controlled access facilities, preventing unauthorized access.*
- *A.NETWORK - TOE will be the only communications channel between sending and receiving networks.*

This Certification Report is valid for the TOE in its evaluated configuration; in particular, “Annex A – Guidelines for the secure usage of the product” includes a number of recommendations relating to delivery, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([INST_GUIDE], [AGD]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE delivery

The following is the procedural steps that define how the TOE is configured and delivered to the customer:

1. Receive P.O. – The purchase order (P.O.) is received within OPSWAT's order fulfilment department.
2. Review P.O. - Verify item SKUs within PO are correct.
3. Address any concerns and errors with PO if needed.
4. OPSWAT retrieve and assemble necessary hardware to complete the purchase order.
5. Check and Report stock level for inventory management.
6. Pass Serial Number information for recording.
7. Check and verify parts list.
8. Verify software tools are up to date and software archives are correct.
9. Perform inspections on hardware.
10. Complete hardware configurations.
11. Complete Software build out per the required steps for each SKU.
12. Boot check software versions.
13. Power down.
14. Apply markings.
15. Wipe down unit.
16. Prepare for packaging in OPSWAT shipping material.
17. Component and miscellaneous items checked for each product as packed.
18. Insert OPSWAT material into packed boxes.
19. Move to staging for Shipping/return labels Security seal.

The Customer can check in the invoice the Serial Number of the appliances sent to them. This Serial Number is also indicated in a label added to the appliances. In the same way, Small Form-Factor Pluggable (SFP) slots have a label indicating the Serial Number. This Serial Number can be compared with the Serial Number indicated in the invoice. Regarding software, OPSWAT will inform the users about the Software reference that needs to be installed to be compliant with the current certification in OPSWAT NetWall Data Diode OD-101 Common Criteria Evaluated Configuration Guide [INST_GUIDE]. The document, together with [AGD] document and User Manual, will be available at https://docs.opswat.com/netwalldiode/netwall-diode with the corresponding hash values for integrity protection.

The customers will be able to check the different hashes of the update packages OPSWAT provides to them by comparing it with the recommended version. In that way, the customer can check if the installed software is the correct one.

Every product related documentation is available through the OPSWAT's Technical Documentation for OPSWAT Products page (https://docs.opswat.com/netwalldiode), where always the latest documentation is published. The page is managed using DeveloperHub, and since the tool is available only for people with proper access rights and credentials the integrity of the documentation is protected.

9.2 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the documents [INST_GUIDE] and [AGD] contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [INST_GUIDE] and [AGD] documents for the TOE being in the evaluated configuration.

The TOE is identified in the Security Target [ST] with the version number 1.0.1. The evaluation of the TOE was conducted on configuration 1.5.0. The name, version and configuration number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The TOE is just the TX and RX module loaded into the hardware element. These are responsible for one-way dataflow communication. TX and RX are abbreviations for Transmit and Receive. Therefore, TOE is just the two packages responsible for these not a hardware specification. These two packages are:

- NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE
- NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED

The TOE is delivered with all the necessary software components already installed, but the customer can download the evaluated version of the TOE from the https://my.opswat.com/portal/products page and the integrity of the downloaded files can be validated using the HASH values available for every version. The downloaded package can be installed using the Software Update product function.

Table 2 provides a list of possible hardware appliances where the TOE can be installed. TOE component is the same for both appliances which differ only for performance granted.

Target Hardware	Serial number	Software version	Installation package	HASH
NetWall BLUE 1U	NW202300019	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE	SHA256: d2d2d225832486f85358e3fefe84b97b05401321a9bc0896879448f4055fc28c
NetWall RED 1U	NW202300020	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED	SHA256: e1be95643a2c6c8548ce4096c1bacfd3aa43d8ec6621b1ac96b49b2e826b826a
NetWall BLUE DIN rail	LR202207015043	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE	SHA256: d2d2d225832486f85358e3fefe84b97b05401321a9bc0896879448f4055fc28c
NetWall RED DIN rail	LR202207015044	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED	SHA256: e1be95643a2c6c8548ce4096c1bacfd3aa43d8ec6621b1ac96b49b2e826b826a

Table 2 – NetWall Optical Diode OD-101 v1.0.1 evaluated version identification

The items described in section 10.1 “TOE operational environment” must be available before performing the installation.

10.1 TOE operational environment

Bundled with the TOE is a Web Application which allows a user to configure the TOE to connect to systems in the source and destination networks and configure the data type that is being transferred by the TOE. The Web Application can be accessed by TOE administrators using a browser connected locally to the appliances to display the Web App GUI.

In addition to the Web Application, there is a Command Line Interface (CLI) that can also be used to configure the system. The configuration Web Application and CLI are not included in the TOE boundary.

The Web App allows the configuration of Industry Control protocol connector software such as Modbus, OPC DA & UA connectors that are typically provided with the TOE but reside outside the TOE boundary.

Two USB devices (security dongles) are provided by OPSWAT, which encrypts each dongle with information unique to customer's site. The dongles are encrypted and configured so they cannot be accessed from a computer by normal means. Each dongle contains the following information that is unique for each customer:

- A Site Key identifies the organization's site. This Key is the same on all dongles in the organization.
- A security key unique to each dongle.

These two dongles are preregistered. If the organization needs extra dongles these need to be registered via the CLI to work properly. The user needs admin credentials to access the CLI. So, these dongles act as a second factor for authentication.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The evaluator conducted the tests locally. The test configuration was installed by the evaluator who followed the steps described in [AGD] and the [INST_GUIDE] document.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The tests were performed by using three networks. A sender network (BLUE) and a Receiving Network (RED) and an Access Network. The Sender and Receiving networks were not able to communicate with each other. The Access Network did have access to Sender and Receiving Networks for configuration and test. An Ubuntu Server (sender) was setup on the sender network and an Ubuntu Server (destination) was setup on the receiving network. The servers were equipped with the netcat-openbsd package installed.

11.2.2 Test coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Due to the relatively small sample size, all Developer's tests were repeated by the Evaluators to confirm the validity of expected results. These are:

- Test Case 1 - TX Module UDP Stream Config
- Test Case 2 - RX Module UDP Stream Config
- Test Case 3 - UDP Data Send
- Test Case 4 - TX Module TCP Stream Config
- Test Case 5 - RX Module TCP Stream Config
- Test Case 6 - TCP Data Send
- Test Case 7 - DiodeSend Initialization
- Test Case 8 - DiodeReceive Initialization

The Evaluator also created five additional test cases to test specifically one-way functionality provided by the TOE.

11.3.2 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

The Evaluators designed the following attack scenarios:

- Injection attacks (Cross-Site Scripting and SQL injection).
- Information leak over OSI layers in network packets.
- SSL vulnerability
- Password brute-force authentication attack
- Manipulation of cron jobs scripts.
- Buffer overflow.
- File upload
- Man-in-the-middle attack.
- Escape from restricted CLI.
- Unauthorised modification of TOE parameters.
- Information leak on REST API when unauthenticated.
- Illicit information flow (over one-way transmission).

The Evaluators has concluded that the TOE is resistant to High attack potential in its intended operating environment.