OPSWAT

Security Target

OPSWAT NetWall Unidirectional Security Gateway
Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5

TOE Reference:	OPSWAT NetWall USG-100
Version	v1.7
Date	2025-04-16
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2023-09-14	Miguel Ángel Fernández Otero	The first version of the Security Target.
v1.1	2023-11-27	Miguel Ángel Fernández Otero	Partial amendments based on the 1st analysis cycle
v1.2	2024-02-23	Miguel Ángel Fernández Otero	Amendments based on the 1st analysis cycle (finished)
v1.3	2024-04-18	Miguel Ángel Fernández Otero	Amendments based on the 2nd analysis cycle
v1.4	2024-09-04	Miguel Ángel Fernández Otero	Amendments based on the 3rd analysis cycle
v1.5	2024-09-12	Miguel Ángel Fernández Otero	Typo corrected
v1.6	2025-02-03	Miguel Ángel Fernández Otero	NOC 30/10/2024
v1.7	2025-04-16	Miguel Ángel Fernández Otero	Delivery of Draft Certification Report

Table of Contents

1 Introduction

1.1 ST Reference

Table 1 - ST Reference

ST Title	OPSWAT NetWall Unidirectional Security Gateway Security Target
ST Version	1.7
ST Creation Date	2025-04-16

1.2 TOE Reference

Table 2 - TOE Reference

TOE Name	OPSWAT NetWall Unidirectional Security Gateway
TOE Reference	OPSWAT NetWall USG-100
TOE Version	1.0.0
Short Name	USG-100

1.3 TOE Overview

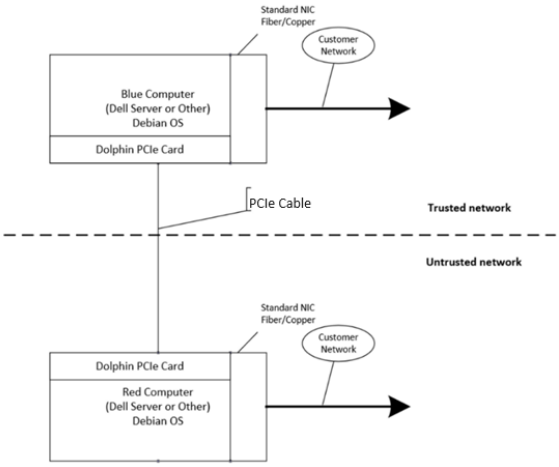
The Target of Evaluation (TOE) is a Unidirectional Gateway that enforces a one-way information flow control policy on network traffic flowing through it. Referring to the figure below, the TOE consists of a software TX Module (placed inside the BLUE Computer indicated in the Figure) that connects to the sending or trusted network and a software RX Module (placed in the Red Computer indicated in the Figure) that connects to the receiving or untrusted Network. These modules are running on a Linux based system on both the BLUE and RED devices. The modules are not directly indicated in Figure 1, but as they are software components running on the mentioned Debian OS they are included. Each of the modules is connected with a specialized PCIe card installed.

A cable connects the PCIe interface cards, and the data is transferred across the cable.

The PCIe link (via the PCIe cable) between the two appliances is not a network connection: an OPSWAT-developed non-routable communications topology is used instead.

The following figure shows the system architecture using a high-level description. Blue and Red computers are the appliances containing TX and RX modules in sending and receiving sides. The detailed description of the system can be found in Figure 3 with the internal components visible.

Figure 1 - System architecture schematics



1.3.1 TOE Boundary

The figure below illustrates the USG-100 architecture and defines the TOE boundary.

TOE is divided into two different software modules, OPSWAT TX Module and OPSWAT RX Module. These modules are composed of different components as indicated in the picture. PciXfrSnd, in the TX module and PciXfrRcv, in the RX module constitute the TOE boundary. The OPSWAT TX Module and OPSWAT RX Module modules are placed in the BLUE and RED appliances. The different configurations of these appliances are described in section 1.4.1 Physical scope of the TOE.

Figure 2 - Operational environment

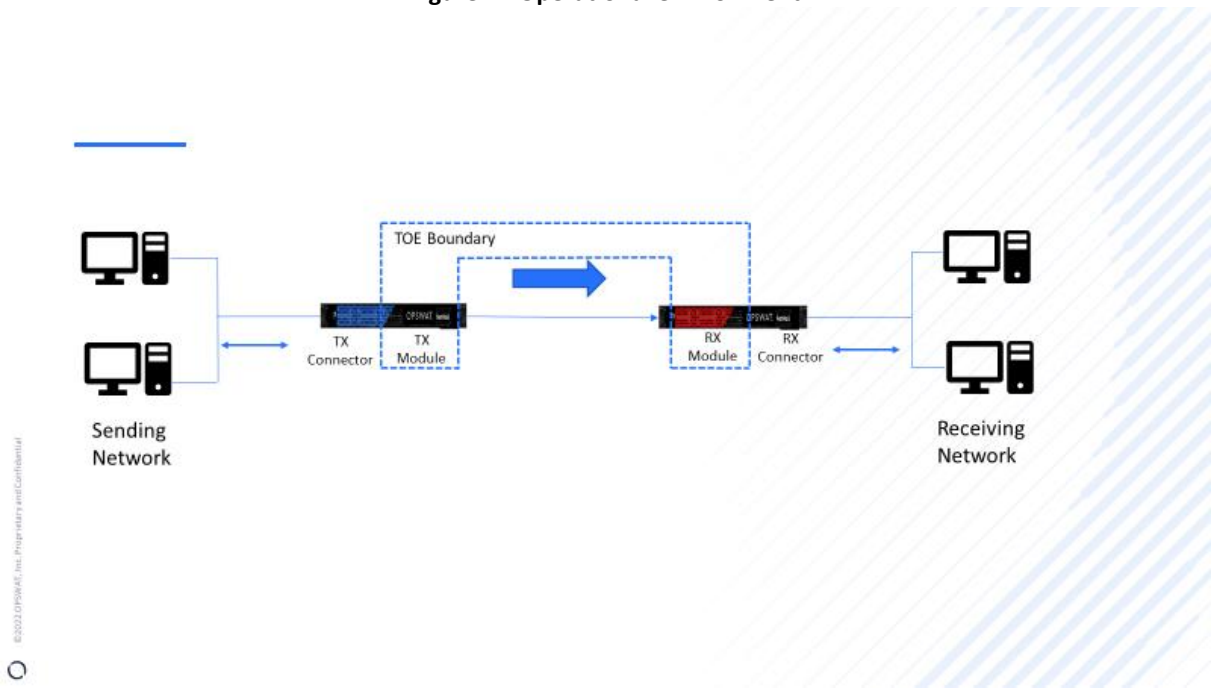
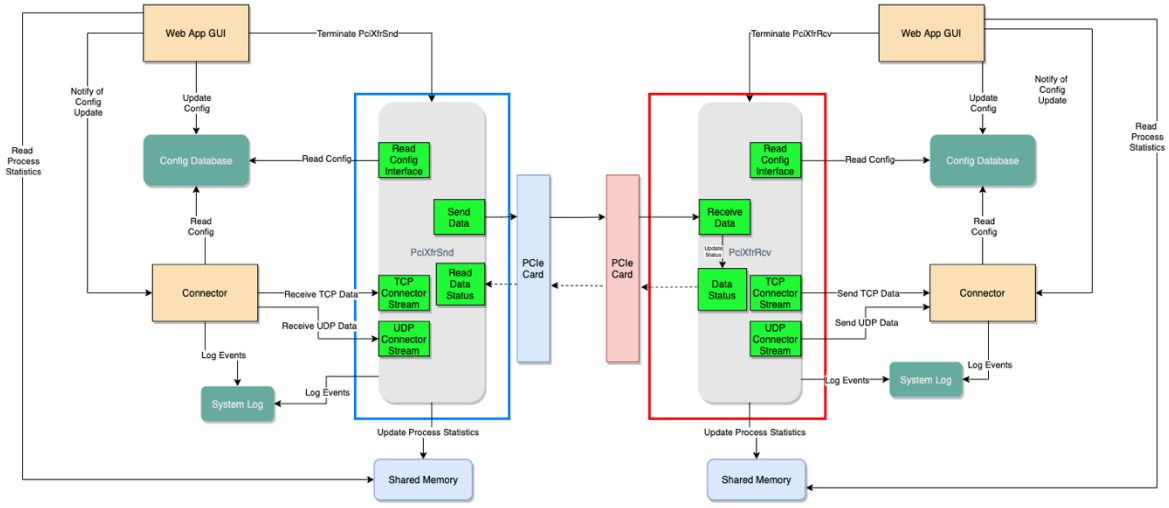


Figure 3 shows the TOE architecture containing the TOE and non-TOE components. The blue and red brackets indicate the TOE itself.

Figure 3 - System architecture



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

- **TOE components:**
  - TX Module Subsystem
    - PciXfrSnd
  - RX Module Subsystem
    - PciXfrRcv
- **NON-TOE components:**
  - Web App GUI
  - Config Database
  - Connector
  - System Log
  - Shared Memory

1.3.2 TOE Type

The Target of Evaluation (TOE) is a Unidirectional Security Gateway that enforces a one-way data flow. TOE consists of a TX Module that connects to the sending or trusted network and a RX Module that connects to the receiving or untrusted Network.

1.3.3 TOE Usage and Major Security Features

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 non-networked connection guaranteeing the delivery of the data. The TOE prevents any network 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, and a status message is read when the data has been successfully delivered. The sending Network is fully protected against any network based cyber-attacks initiated at the receiving network, since no network data can be sent from the receiving network to the sending network.

A typical usage scenario consists of a sending 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 network information from flowing back through the TOE 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.

1.3.4 Non-TOE Software/Firmware/Hardware

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. 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. OPSWAT 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. 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 (Figure 4). The user needs admin credentials to access the CLI. So, these dongles act as a second factor for authentication. To register the dongles the user needs to plug in the dongles in the corresponding NetWall appliance and follow the steps indicated in the picture below.

Figure 4 - Security dongle registration

```
netwall> dongle
netwall (dongle)> register

Dongle Number: 1080
Dongle Site ID: e5d4877b-5923-421c-848c-bfbcc3366dfd
Do you want to register this dongle ?
Continue? [y/N] y

netwall (dongle)> list

You can delete any dongle by its ID
ID: 1042 Site ID: e5d4877b-5923-421c-848c-bfbcc3366dfd
ID: 1080 Site ID: e5d4877b-5923-421c-848c-bfbcc3366dfd

netwall (dongle)>
```

- OPSWAT TX Connector (outside of the TOE) is 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 proxies 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 & DA
    - SMTP
    - IEC 104
    - DNP3
    - MQTT
    - OSI-PI
- 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 proxies 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.
- Configuration parameters for TX Connectors and RX Connectors are comprised of IP Address, Ports and other variables depending on the protocol used. The TX Connectors and RX Connectors do not modify the TX module or the RX module configuration parameters specified in section 3.5.1 of the [AGD]. In the very unlikely case that an attacker injects malicious configuration parameters, it is not possible to modify the Information Flow Control. The Flow control depends on memory segments in the PCIeRX card. The memory segments are statically set in PCIXfrSnd and PciXfrRcv during the boot process and are immutable after. The memory segments cannot be created, deleted or altered by any configuration. As the memory segment does not depend on any configuration, even if the configuration database is corrupted, the memory segments will function.

- PCIeTX card Description: PCIeTX card pass binary data from the sending network to the receiving network. This non-routable binary data has no network information, such as IP or MAC address.
- PCIeRX card Description: PCIeRX uses memory segments that receive this binary data sent by PCIeTX over a PCIe channel. A memory segment is a block of memory allocated to the PCIe card in the appliance placed in the receiving network. The computer that creates a memory segment must explicitly allow access to that segment for the PCIe card installed in the other computer. A PCIe card can only create local memory segments: it cannot create a memory segment in the other computer. The PCIe card in the Receiving Network computer creates two memory segments: a Data Segment and a Status Segment. Each of these segments are readable and writable from the Sending Network computer as well. There are no memory segments on the Sending Network computer: the Receiving Network computer has no mechanism to write data to the Sending Network computer. Therefore, even if the Receiving Network computer is compromised, it cannot directly pass any data to the Sending Network because there is no path to do so. In addition, the hardware-enforced protocol of the PCIe cards prevents the remote creation and authorization of memory segments. The memory segment allocation configuration is statically set in the code and cannot be changed by a configuration.
- Configuration Database
    - Standard SQLITE3 database – single file.
    - The configuration database is used by PciXfrSnd and PciXfrRcv to read configuration via Read Config Interface (SQLITE3 C++ API, libsqlite3 3.34.1-3)
    - PciXfrSnd and PciXfrRcv only read configuration from streams file table.

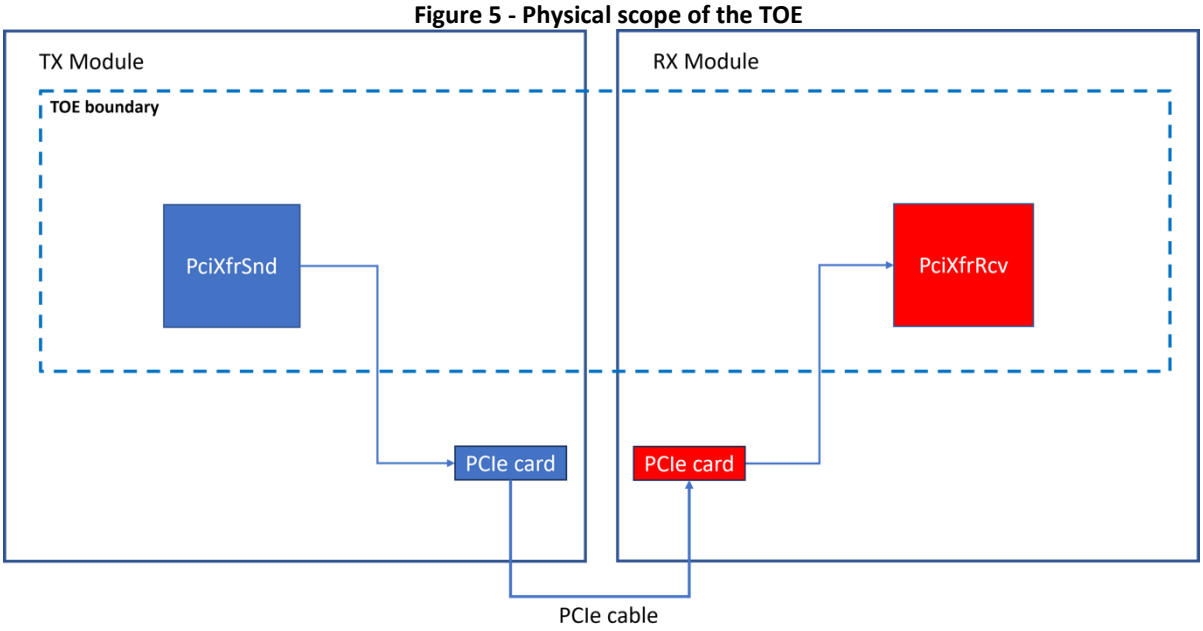
1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.4.1 Physical Scope of the TOE

The different components conforming TX and RX Modules are indicated in the figure below. In this section a description of the components will be provided together with a detail of the different configurations to be evaluated. Figure 5 shows the physical scope of the TOE with the TOE boundary highlighted with blue dotted line.

Figure 5 - Physical scope of the TOE



- PciXfrSnd Description: PciXfrSnd module reads network data from the sending network, transforms that data into internal data representation and sends that to the PciXfrRcv module over a PCIe card and the PCIe cable, which are not in the TOE boundary and have no security functions implemented regarding the SFRs.
- PciXfrRcv Description: PciXfrRcv module receives the internal data sent by PciXfrSnd module over a PCIe card and the PCIe cable, which are not in the TOE boundary and have no security functions implemented regarding the SFRs , extracts the network data from the internal data representation, ensuring data integrity is intact and recreates the network payload into the receiving network by injecting that data into the newly created network connections.

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 versions. The downloaded package can be installed using the Software Update product function.

Table 3 - OPSWAT NetWall evaluated version identification

Name	Serial number	Software version	Installation package	HASH
NetWall BLUE 1U	NW202400101	USG-100: 1.0.0 Config: 5.5.0	NetWall_USG-100_1.0.0_Config_5.5.0.1958_BLUE.pkg	7be8dd374b19633207e561fe1597822f06c81b39ccbf7e0aebb5290263d2e87a
NetWall RED 1U	NW202400102	USG-100: 1.0.0	NetWall_USG-100_1.0.0_Config_5.5.	b8ca6a1841dcff6f0e40c0845f1fcfa54814fb4192742a57897a

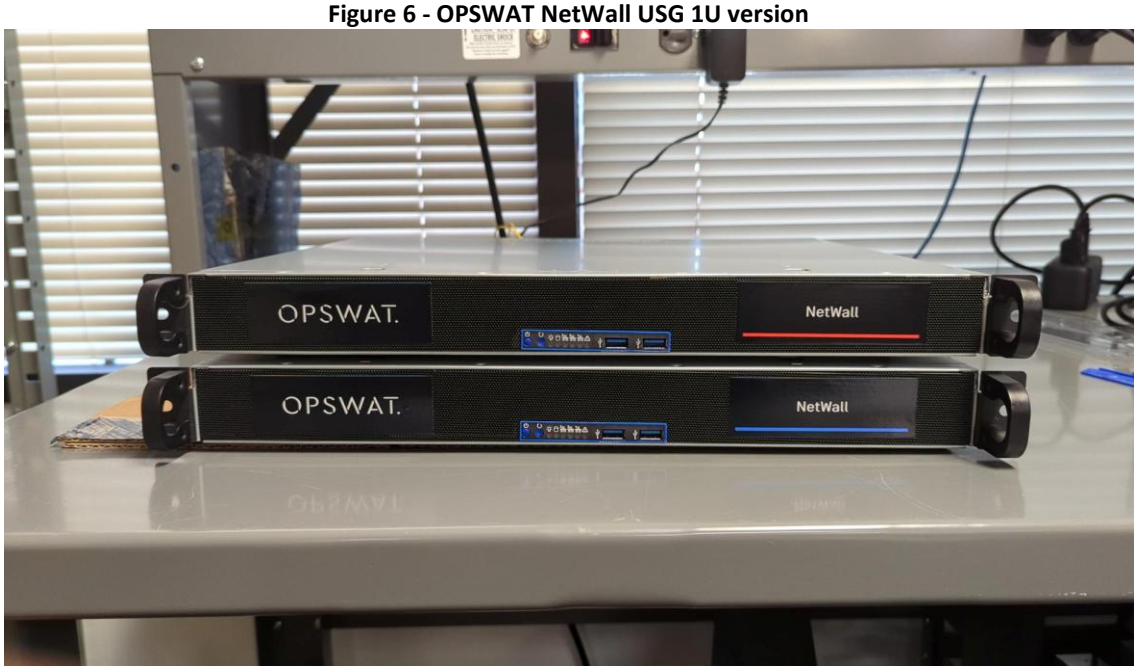
		Config: 5.5.0	0.1959_RED.pkg	9278e100781b

Once the development work has finished for a given version, the candidate version is built using Jenkins and sent to the QA team who will perform regression and new features testing. Once the software is accepted by both QA Team and the Engineering leader the software is officially released together with the documentation corresponding to the new version. The installation packages are uploaded and stored in Amazon S3 Bucket to make them available for the users via my.opswat.com where they can download it.

The TOE can operate in the following evaluated configurations. These different configurations don't affect the functionality and the security of TOE (Figure 6 illustrates the TOE hardware):

- 1U version with IXH610 PCIe card: Two 1U half-depth appliances (NetWall BLUE and NetWall RED) running respectively:
  - OPSWAT TX Module and OPSWAT TX Connector in NetWall BLUE.
  - OPSWAT RX Module and OPSWAT RX Connector in NetWall RED.
- 1U version with PXH810 PCIe card: Two 1U half-depth appliances (NetWall BLUE and NetWall RED) running respectively:
  - OPSWAT TX Module and OPSWAT TX Connector in NetWall BLUE.
  - OPSWAT RX Module and OPSWAT RX Connector in NetWall RED.
- 1U version with PXH830 PCIe card: Two 1U half-depth appliances (NetWall BLUE and NetWall RED) running respectively:
  - OPSWAT TX Module and OPSWAT TX Connector in NetWall BLUE.
  - OPSWAT RX Module and OPSWAT RX Connector in NetWall RED.
- 1U version with MXH914 PCIe card: Two 1U half-depth appliances (NetWall BLUE and NetWall RED) running respectively:
  - OPSWAT TX Module and OPSWAT TX Connector in NetWall BLUE.
  - OPSWAT RX Module and OPSWAT RX Connector in NetWall RED.
- 1U version with MXH930 PCIe card: Two 1U half-depth appliances (NetWall BLUE and NetWall RED) running respectively:
  - OPSWAT TX Module and OPSWAT TX Connector in NetWall BLUE.
    OPSWAT RX Module and OPSWAT RX Connector in NetWall RED.

Figure 6 - OPSWAT NetWall USG 1U version



1.4.2 TOE Guidance

The following guidance is considered part of the TOE:

- OPSWAT NetWall Unidirectional Security Gateway AGD Documentation v1.4 [AGD]
- OPSWAT NetWall Unidirectional Security Gateway USG-100 Common Criteria Evaluated Configuration Guide v1.2 [USG-UM]
- NetWall v5.5.0 [P-UM]

OPSWAT customers can request a copy of the guidance by contacting OPSWAT support.

1.4.3 Logical Scope of the TOE

The following sequence describes the information flow through the TOE:

1. OPSWAT TX Connector (outside the TOE) on TX side receives a protocol-specific data stream from the industrial network servers or stations.

2. OPSWAT TX Connector sends the information to OPSWAT TX Module.

3. OPSWAT TX Module reads the information, extracts the data payload by removing any routable information like protocol-specific headers, performing a protocol break and transmits the information to OPSWAT RX over a PCIe cable (the cable is outside the TOE but maintained within a physically secure environment). OPSWAT TX Module will wait for OPSWAT RX to communicate status using the Status Segment.

4. OPSWAT RX Module receives the information, reconstruct the headers and sends it to OPSWAT RX Connector on the RX server (outside the TOE).

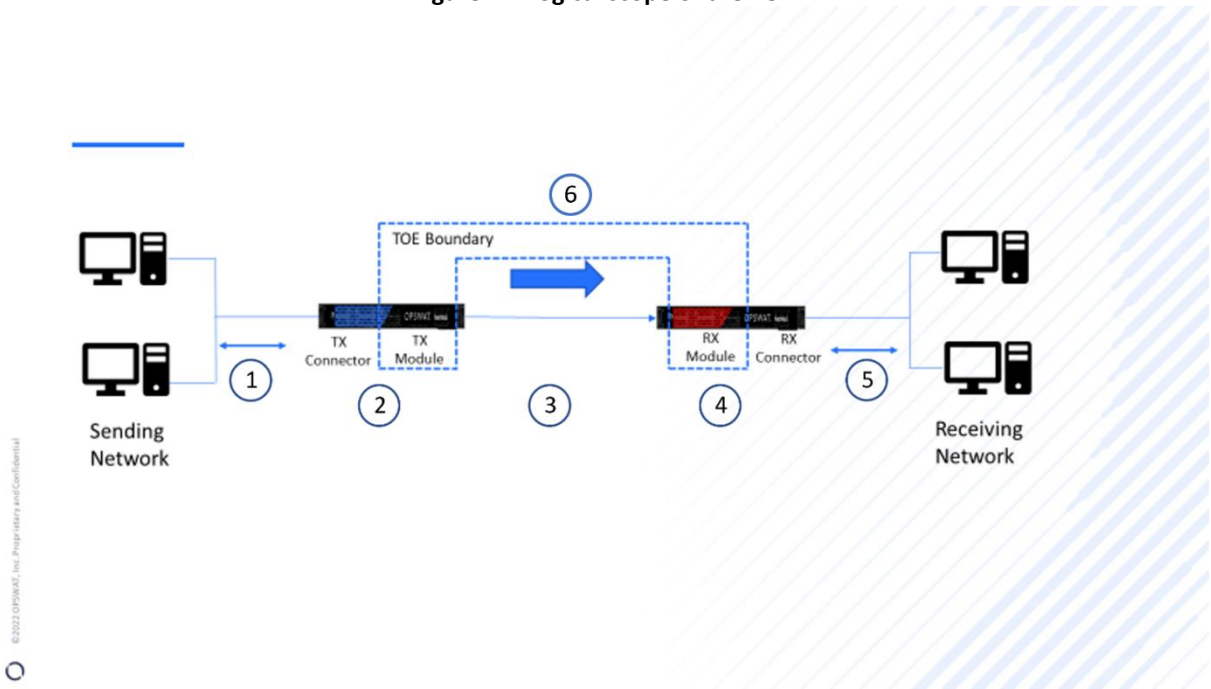
5. OPSWAT RX Connector communicates the data stream to the corporate network servers or stations.

6. OPSWAT RX module write on the Status Segment indicating the result of the operation:

- If the write Failed:
    - NetWall Red will close the connection with the Server in the Receiving network.
    - If the Server in the Receiving network closed its connection, NetWall Red will close its side of the connection and mark the status of the Write as failed in the Status Segment.
- If the Write succeeded, NetWall Red waits for the next Command/Data from NetWall Blue.

When a change of configuration is done, the PciXfrSnd/PciXfrRcv processes are terminated by the Web App GUI. The PciXfrSnd/PciXfrRcv processes will start automatically, and the Read Config function is used to query the modified configuration. Terminate PciXfrSnd/PciXfrRcv is done via SIGKILL. SIGKILL is specifically chosen as it is indiscriminate process termination (e.g. there's no possibility to block/catch/handle SIGKILL).

Figure 7 – Logical scope of the TOE



2 Conformance Claims

Table 4 – Conformance Claims

Common Criteria Conformance	Common Criteria for Information Technology Security Evaluation, CC Part 2 conformant, CC Part 3 conformant
Common Criteria version	Version 3.1 Revision 5, April 2017
PP Conformance	The TOE does not claim conformance with any Protection Profile.
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5

3 Security Problem Definition

This section defines the security problem to be addressed by the TOE and its operational environment and includes the following:

- Organizational Security Policies (OSPs),
- Assets,
- Secure Usage Assumptions, and
- Threats.

3.1 Organizational Security Policies

This Security Target does not identify any rules or guidelines that must be followed by the TOE and/or its operational environment, phrased as Organizational Security Policies.

All defined security objectives are derived from assumptions and threats only.

3.2 Assets

The IT assets requiring protection are the following:

- Transferred data: All the information transferred from sending to receiving network, including files and streams from different protocols.
- Configuration of the TOE: RX and TX Modules and Connectors require to be configured. This configuration is performed in the Web UI and stored in independent Data Bases for RX and TX.

The TOE is part of the OPSWAT NetWall Unidirectional Security Gateway product, and it is running under the same underlying operating system as the non-TOE components, which means that the same physical security measures apply to them as to the TOE itself. Also, the configuration of the TOE is stored inside the PciXfrSnd and PciXfrRcv modules as well as in the secure Config Database since the configuration is read and stored during Read Config. A.ADMIN and A.PHYSICAL will assure the security of all components inside the product, since only the administrator has access to the configuration, and changing it require local access to both RED and BLUE sides. The related operational environment security objectives (OE.ADMIN, OE.PHYSICAL) are covered by the abovementioned assumptions. The Config Database cannot be accessed directly, and the Web APP GUI is secured by the access control system, valid credentials for the Web App GUI and a valid security dongle are required to modify the configuration.

3.3 Assumptions

Table 5 – Assumptions

Assumption	Description
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 and PCIe cable) 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.

3.4 Threats

Table 6 – Threats

Threat	Threat agent	Asset	Adverse action
T.LEAKAGE	Attacker	Transferred data	Information residing in the receiving network is accidentally or maliciously transmitted to the sending network.
T.BLUECOMP	Attacker	Configuration of the TOE	A host or process integrity in the sending network is accidentally or maliciously compromised by the action of an actor in the receiving network.
T.TOPOLEAK	Attacker	Transferred data	OSI Layer 3 data from the sending network is passively detected on the receiving network.
T.REDCOMP	Attacker	Configuration of the TOE	A host or process integrity in the receiving network is accidentally or maliciously compromised by the action of an actor in the sending network.

4 Security Objectives

The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

Table 7 – Security Objectives for the TOE

Objective	Description
O.DATAFLOW	TOE will only allow data information to flow only from sending network to receiving network, except the status information written by RED in the corresponding memory segment, that BLUE can read.
O.PROTOBREAK	TOE will filter OSI Layer 3 information transmitted from the sending to the receiving network such that the receiving network cannot infer Network layer (OSI Layer 3) information of the sending network.
O.SECUREINIT	The TOE will only use the new configuration read from the Config Database if the initialization was successful, otherwise the TOE restarts and loads the previous configuration.

Table 8 – Security Objectives for the Operational Environment

Objective	Description
OE.PHYSICAL	Appliances where the TOE is placed and the PCIe cable connecting sending and receiving sides will be physically protected, within secure and controlled access facilities.
OE.ADMIN	Administrators with physical access to the appliances where the TOE is placed, will properly follow the TOE guidance and will not try to perform any malicious action or circumvent the TOE's security functionality.
OE.NETWORK	TOE is the only interconnection between sending and receiving networks

4.1 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, enforce policies, and uphold assumptions.

The following tables provide a mapping of security objectives for the TOE and security objectives for the operational environment of the TOE to the defined threats, policies, and assumptions, illustrating that each security objective covers at least one threat, enforces a policy or upholds an assumption and that each threat, policy or assumption is covered by at least one security objective.

The tables below provide information regarding:

- the identified security objectives providing effective countermeasures for the threats;

- the identified security objectives providing complete coverage of each organizational security policy;
- the identified security objectives upholding each assumption.

4.1.1 Security Objectives Rationale related to Threats

The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

Table 9 – Security Objectives Rationale – Threats

Threats	Objectives	Rationale
T.LEAKAGE	O.DATAFLOW	O.DATAFLOW ensures that protocol data flowing through the TOE will only be allowed from sending network to receiving network.
T.BLUECOMP	O.DATAFLOW O.SECUREINIT	O.DATAFLOW ensures that data flowing through the TOE will only be allowed from sending network to receiving network. A user with access to receiving network cannot transmit any information to any host or process on sending network. O.SECUREINIT ensures that the TOE will not get compromised during initialization.
T.REDCOMP	O.DATAFLOW O.SECUREINIT	O.DATAFLOW ensures that data flowing through the TOE will only be allowed from sending network to receiving network. This mitigates most attacks as most of them requires feedback from the attacked host or process. O.SECUREINIT ensures that the TOE will not get compromised during initialization.
T.TOPOLOEAK	O.PROTOBREAK	O.PROTOBREAK ensures that data flowing through the TOE does not disclose sending network topology.

4.1.2 Security Objectives Rationale relating to Assumptions

The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

Table 10 – Security Objectives Rationale – Assumptions

Assumptions	Objectives	Rationale
A.ADMIN	OE.ADMIN	OE.ADMIN directly upholds A.ADMIN
A.PHYSICAL	OE.PHYSICAL	OE.PHYSICAL directly upholds A.PHYSICAL
A.NETWORK	OE.NETWORK	OE.NETWORK directly upholds A.NETWORK

5 Security Requirements

This section defines the SFRs, and SARs met by the TOE.

This section defines whether the SFRs and SARs are clear, unambiguous, and well-defined, whether they are internally consistent, and whether the SFRs meet the security objectives of the TOE.

5.1 Conventions

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using bold text. (Example: **TSF Data**) Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

5.2 TOE Security Functional Requirements

List of the SFRs along with their description and the operations performed on them.

Table 11 – SFRs

Name	Description	S	A	R	I
FDP_IFC.2	Complete Information Flow Control		X		
FDP_IFF.1	Simple Security Attributes		X		
FMT_MSA.3	Static attribute initialisation	X	X		

Note: S = Selection, A = Assignment, R = Refinement, I = Iteration

5.2.1 Complete Information Flow Control (FDP_IFC.2)

FDP_IFC.2	*Complete information flow control*

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [*Unidirectional SFP*][1] on [*the TX, the RX, and all information flowing through the TOE*][2] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

[1] [assignment: *information flow control SFP*]
[2] [assignment: *list of subjects and information*]

5.2.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1	*Simple security attributes*

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*Unidirectional SFP*][3] based on the following types of subject and information security attributes: [*None*][4].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*no security attribute-based rules*][5].

FDP_IFF.1.3 The TSF shall enforce the [following additional information flow control SFP rules:

(1) the TSF shall permit the TX to read information from the sending network,

(2) the TSF shall permit the TX to transmit information to the RX,

(3) the TSF shall permit the RX to receive information from the TX,

(4) the TSF shall permit the RX to write information to the receiving network,

(5) the TSF shall permit the TX to read information from status data segment in RX module][6].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no rules that explicitly authorise information flows*][7].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

(1) the TSF shall deny the RX to transmit information to the TX; and

(2) the TSF shall deny the TX to receive information sent by the RX][8].

Application Note 1: The Unidirectional SFP permits information flow from the sending network to the receiving network via TOE TX and RX Modules and denies information flow in

[3] [assignment: *information flow control SFP*]
[4] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[5] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[6] [assignment: *additional information flow control SFP rules*]
[7] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[8] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

the reverse direction except the status flag that the TX module reads from PCIeRX. Enforcement of this SFR guarantees the delivery of information between sending and receiving networks by using the status flag. The TX Connector Module could verify if the data sent is received and provides the capability for retransmitting data.

5.2.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3	*Static attribute initialisation*

Hierarchical to: No other components.

Dependency: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Unidirectional SFP*][9] to provide [configurational][10] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*None*][11] to specify alternative initial values to override the default values when an object or information is created.

Application Note 2: The TOE configuration data and security attributes cannot be modified on the TOE, so the FMT_MSA.1 Management of security attributes SFR is not applicable.

Application Note 3: The security roles, the identification, and the authentication are done by a non-TOE component, by the Web App GUI or by the CLI. Since the TOE itself does not manage roles the FMT_SMR.1 Security roles SFR is not applicable.

Application Note 4 (FMT_MSA.3.2): The TOE itself does not manage users or roles. The identification and authentication, and the access control is covered by its operational environment.

5.3 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL 4, augmented with the CC part 3 components ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5.

Table 12 – Assurance Requirements

Assurance Requirements		
Class ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification

[9] [assignment: *access control SFP, information flow control SFP*]
[10] [selection, choose one of: restrictive, permissive, [assignment: *other property*]]
[11] [assignment: *the authorised identified roles*]

Class ALC: Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_FLR.2	Flaw reporting procedures
	ALC_CMS.4	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Class ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_TDS.3	Basic modular design
	ADV_IMP.1	Implementation representation of the TSF
Class AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

5.4 Security Requirements Rationale

This section provides the rationale for necessity and sufficiency of security requirements, demonstrating that each of the security objectives is addressed by at least one security requirement, and that every security functional requirement is directed toward solving at least one objective.

5.4.1 Security Requirements Coverage

The table in section 5.4.1.1 provides a mapping between the Security Functional Requirements and the Security Objectives, illustrating that each Security Functional Requirement covers at least one Objective and that each Objective is covered by at least one Security Functional Requirement.

5.4.1.1 Security Functional Requirements Related to Security Objectives

The following table should give a rationale that all Security Objectives are covered by at least one SFR and to show that there is no Security Objective not covered and no SFR used that is not required.

Table 13 – Security Functional Requirements Related to Security Objectives

Functional Requirement	Rationale	Objective
FDP_IFC.2	The TSF must enforce a unidirectional information flow SFP on all requests to move data through the TOE.	O.DATAFLOW
FDP_IFF.1	The TSF ensures that interfaces designed to receive information can only receive information (and never send it) and interfaces designed to send information can only send information (and not receive it), with	O.DATAFLOW

	the exception of the status flag placed in the PCIe card in the RED side being read by the BLUE side. This mechanism has been implemented as a solution to guarantee delivery of the data.	
FMT_MSA.3	The configuration data and secure attributes of the TOE cannot be modified from the TOE, only admins with physical access, appropriate credentials (username, password), and a security dongle can modify those data through the Web App GUI or through the CLI.	O.SECUREINIT OE.PHYSICAL OE.ADMIN

5.4.1.2 Security Assurance Requirements Rationale

The level of assurance for this ST is Evaluation Assurance Level (EAL) 4, as defined in CC Part 3, augmented with the CC Part 3 components AVA_VAN.5, ALC_DVS.2, and ALC_FLR.2.

EAL 4 ensures that the product has been designed, tested, and reviewed with maximum assurance from positive security engineering based on good development practices. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security.

AVA_VAN.5, Advanced Methodical Vulnerability Analysis augments EAL4 by ensuring that the TOE has undergone advanced methodical vulnerability analysis to confirm that the product is resilient to attacks with High attack potential. EAL 4 augmented by AVA_VAN.5 is appropriate for a TOE designed to protect industrial networks from cyber-attacks and to prevent leakage of information from classified networks.

ALC_DVS.2, Sufficiency of Security Measures augmentation provides justification that the security measures assure the necessary level of protection to keep confidentiality and integrity of the TOE in its development environment.

ALC_FLR.2, Flaw reporting procedures provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE, and providing guidance to TOE users for how to submit security flaw reports to the developer.

5.5 Requirements Dependency Rationale

5.5.1 Rationale Showing that Dependencies are Satisfied

The SFRs in this ST satisfy all the required dependencies listed in the Common Criteria. The table in this section lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As it is indicated by the table, all dependencies are fulfilled.

5.5.1.1 Security Functional Requirements Dependencies

The following table provides a summary of the SFRs and their dependencies

Table 14 – Summary of Security Functional Requirements Dependencies

Component	Dependency	Which is:
FDP_IFC.2	FDP_IFF.1	Included
FDP_IFF.1	FDP_IFC.1,	FDP_IFC.1 is included as it is covered by

	FMT_MSA.3	FDP_IFC.2. FMT_MSA.3 included.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 not applicable as the security attributes cannot be managed on the TOE. FMT_SMR.1 not applicable as there are no roles managed on the TOE.

5.5.1.2 Security Assurance Requirements Dependencies

The following table provides a summary of the SARs and their dependencies.

Table 15 – SAR Dependencies

Component	Depends On:	Which is:
ADV_ARC.1	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included.
	ADV_TDS.1	hierarchically higher component ADV_TDS.3 is included
ADV_FSP.4	ADV_TDS.1	hierarchically higher component ADV_TDS.3 is included.
ADV_IMP.1	ADV_TDS.3	included
	ALC_TAT.1	included
ADV_TDS.3	ADV_FSP.4	included
AGD_OPE.1	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included.
AGD_PRE.1	no dependencies	not applicable
ALC_CMC.4	ALC_CMS.1	hierarchically higher component ALC_CMS.4 is included.
	ALC_DVS.1	Hierarchically higher component ALC_DVS.2 is included
	ALC_LCD.1	included
ALC_CMS.4	no dependencies	not applicable
ALC_DEL.1	no dependencies	not applicable
ALC_DVS.2	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
ALC_TAT.1	ADV_IMP.1	included
ASE_INT.1	no dependencies	not applicable
ASE_CCL.1	ASE_INT.1	included
	ASE_ECD.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
ASE_SPD.1	no dependencies	not applicable
ASE_OBJ.2	ASE_SPD.1	included
ASE_ECD.1	no dependencies	not applicable
ASE_REQ.2	ASE_OBJ.2	included
	ASE_ECD.1	included
ASE_TSS.1	ASE_INT.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
	ADV_FSP.1	hierarchically higher component ADV_FSP.4 is included
ATE_COV.2	ADV_FSP.2	hierarchically higher component ADV_FSP.4 is included
	ATE_FUN.1	included
ATE_FUN.1	ATE_COV.1	hierarchically higher component ATE_COV.2 is included
ATE_IND.2	ADV_FSP.2	hierarchically higher component ADV_FSP.4 is included
	AGD_OPE.1	included
	AGD_PRE.1	included
	ATE_COV.1	hierarchically higher component ATE_COV.2 is included
	ATE_FUN.1	included
ATE_DPT.1	ADV_ARC.1	included
	ADV_TDS.2	hierarchically higher component ADV_TDS.3 is included

	ATE_FUN.1	included
AVA_VAN.5	ADV_ARC.1	included
	ADV_FSP.4	included
	ADV_IMP.1	included
	ADV_TDS.3	included
	AGD_OPE.1	included
	AGD_PRE.1	included
	ATE_DPT.1	included

6 TOE Summary Specification

The following table provides a description of the mechanisms that the TOE implements to cover each SFR defined in section 5, providing description of security functionality given in each of the SFRs and a high-level perspective of their implementation in the TOE.

Table 16 – TOE Summary Specification

Component	Description
User Data Protection (FDP)	
FDP_IFC.2	TOE is implemented in two independent modules (they have independent power sources and independent PCIe cards) OPSWAT TX Module and OPSWAT RX Module. The Hardware doesn't permit more ways to transmit electronic signals other than the described interfaces. OPSWAT TX Module is connected only to the sending network through OPSWAT TX Connector (outside the TOE as indicated) 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 as indicated). 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 PCIe cable connects the PCIe cards within TX and RX Modules. The internal memory of these cards has been modified so communications between the two of them are only possible in one single direction, from TX Module to RX Modules. In the PCIe card placed in the receiving network, a Data Segment is created (where the sending appliance can write the data being transfer). Other Data Segment is created also in the receiving PCIe card named Status Segment. TX Module can read this status segment to check if the data has been successfully transferred. There are no Data Segments created in sending PCIe, that guarantees that RX Module can't read or write sending PCIe memory so the communication can only happen from TX Module to RX Module and therefore covered by the Unidirectional SFP.
FDP_IFF.1	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 send the information to the PCIe cable though PCIeTX. The PCIe cable between PCIeTX and PCIeRX constitutes the only connection between these two components. 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 PCIe card memory segments in the RX Module has been modified to support only data reception.

Security Management (FMT)	
FMT_MSA.3	Only an admin with valid credentials and a security dongle 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. Once the admin performs changes on the configuration data and/or secure attributes within the database using the Web App GUI, the TOE will be terminated by the GUI. After termination, the TOE will automatically start and the new configuration data will be retrieved using the Read Config function.

7 Acronyms

Table 17 – Acronyms

Acronym	Meaning
IT	Information Technology
CC	Common Criteria
OSP	Organizational Security Policy
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
SA	Security Association
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
DoD	Department of Defense
TX	Transmission
RX	Reception
CLI	Command Line Interface

8 Bibliography

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

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

[AGD] OPSWAT NetWall Unidirectional Security Gateway AGD Documentation, version: v1.4, date: 2024-08-29 (OPSWAT NetWall USG-100 AGD documentation v1.4.pdf)

[P-UM] NetWall v5.5.0 (NetWall – v5.5.0.pdf)

[USG-UM] OPSWAT NetWall Unidirectional Security Gateway USG-100 Common Criteria Evaluated Configuration Guide v1.2, version: v1.2, date: 2024-05-08 (OPSWAT NetWall Unidirectional Security Gateway USG-100 Common Criteria Evaluated Configuration Guide v1.2.pdf)

