Unidirectional Gateway - Data Diode

Security Target

Version 1.0

August 2021

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	5 Aug 2021	L Turner	Release for certification.

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 5
2 TOE Description 6
2.1 Type 6
2.2 Usage 6
2.3 Logical Scope 6
2.4 Physical Scope 7
3 Security Problem Definition 8
3.1 Threats 8
3.2 Assumptions 8
3.3 Organizational Security Policies 8
4 Security Objectives 9
4.1 Objectives for the Operational Environment 9
4.2 Objectives for the TOE 9
5 Security Requirements 10
5.1 Conventions 10
5.2 Extended Components Definition 10
5.3 Functional Requirements 10
5.4 Assurance Requirements 12
6 TOE Summary Specification 14
6.1 Unidirectional Data Transfer 14
6.2 Fail Secure 15
7 Rationale 16
7.1 Security Objectives Rationale 16
7.2 Security Requirements Rationale 17
7.3 TOE Summary Specification Rationale 19

List of Tables

Table 1: Evaluation identifiers 5
Table 2: Terminology 5
Table 3: Threats 8
Table 4: Assumptions 8
Table 5: Organizational Security Policies 8
Table 6: Security Objectives for the Operational Environment 9
Table 7: Security Objectives 9
Table 8: Summary of SFRs 10
Table 9: Assurance Requirements 12
Table 10: Security Objectives Mapping 16
Table 11: Suitability of Security Objectives 16
Table 12: Security Requirements Mapping 17
Table 13: Suitability of SFRs 18
Table 14: Dependency Analysis 18
Table 15: Map of SFRs to TSS Security Functions 19

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Sphyrna Security Unidirectional Gateway - Data Diode Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Unidirectional Gateway is used to provide a one-way connection between two networks of different security levels. The Unidirectional Gateway - Data Diode is the security enforcing subsystem that ensures that data can only be transmitted in one direction and that no data can be passed, either explicitly or covertly, in the reverse direction.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Sphyrna Security Unidirectional Gateway - Data Diode Identifier: 2010-UG100-SSI
Security Target	Sphyrna Security Unidirectional Gateway - Data Diode Security Target, v1.0

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

d) EAL4 augmented with ADV_INT.2, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_FLR.3, ATE_DPT.2 and AVA_VAN.4

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
TUI	Text-based User Interface

2 TOE Description

2.1 Type

4 The TOE is a one-way data transfer subsystem.

2.2 Usage

5 The Sphyrna Security Unidirectional Gateway, shown in Figure 1 is a self-contained, tamper resistant, 1U rack mounted device capable of securely transferring data in one direction only between two security domains (the black and red networks depicted) via the data diode (the TOE). No configuration is required for enforcement of unidirectional data transfer.

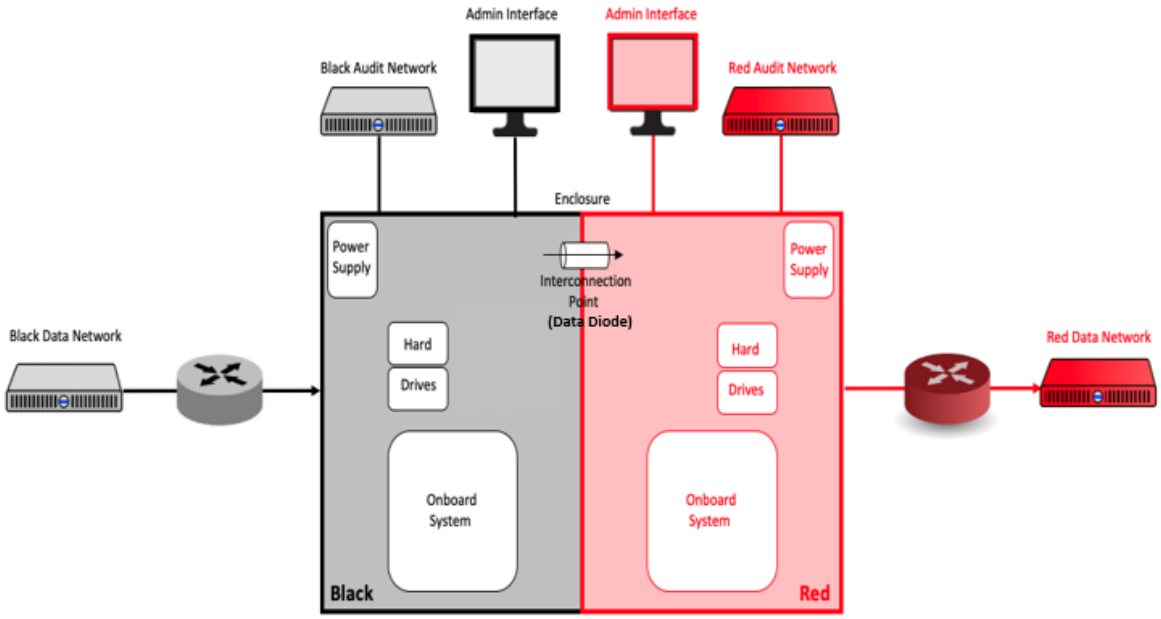

Figure 1: Example TOE deployment

6 The Unidirectional Gateway is intended for deployment in a physically secure environment.

2.3 Logical Scope

7 The TOE logical scope comprises the following security functions:

a) **Unidirectional Data Transfer.** The TOE ensures that data can only be transmitted in one direction and that no data can be passed, either explicitly or covertly, in the reverse direction.

b) **Failure with Preservation of Secure State.** The TOE will not allow data to be transmitted from high side to low side in the event power or hardware failures.

2.4 Physical Scope

8 The physical boundary of the TOE is limited to the hardware components that enforce unidirectional data transfer, which consists of two physical data diode components, each housed in a tamper resistant case. Together these components comprise the overall logical data diode (the TOE).

9 The TOE is delivered to customers via commercial carrier.

2.4.1 Guidance Documents

10 The TOE includes the following guidance documents (PDF):

a) Sphyrna Security Unidirectional Gateway (Data Diode) User Guide, v1.0.3

2.4.2 Non-TOE Components

11 The TOE operates with the following components in the environment:

a) **Connecting equipment.** The low side and high side connected network equipment.

b) **Unidirectional Gateway.** The TOE is a subsystem of the Unidirectional Gateway devices, which consists of a custom 1U tamper-resistant enclosure that houses two single board computers, two power supplies, and four hard drives (two per computer in a RAID configuration).

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
T.TRANSFER	A user or process on the output network accidentally or deliberately transmits data through the TOE to the input network resulting in the unauthorized disclosure of information from the high-side to the low-side.
T.TAMPER	An adversary tampers with the contents of the TOE during delivery, and/or after installation resulting in the unauthorized disclosure of information from the high-side to the low-side.
T.FAILURE	The TOE fails in some manner resulting in the unauthorized disclosure of information from the high-side to the low-side.

3.2 Assumptions

Table 4: Assumptions

Identifier	Description
A.PHYSICAL	The TOE will be stored and deployed in accordance with the physical security requirements of the high side.
A.CONNECT	The TOE is the only method of interconnecting the high-side and low-side networks.
A.NO_EVIL	Authorised users of the TOE are non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.
A.ENCLOSURE	The TOE enclosure is constructed to resist tampering efforts and employs mechanisms to detect and respond to tamper attempts.

3.3 Organizational Security Policies

Table 5: Organizational Security Policies

Identifier	Description
OSP.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access high side network equipment.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	The TOE will be stored and deployed in accordance with the physical security requirements of the high side.
OE.CONNECT	The TOE shall be the only method of interconnecting the only two on-board systems, the high-side and the low-side.
OE.NO_EVIL	Authorised users of the TOE shall be non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.
OE.ENCLOSURE	The TOE enclosure shall resist, detect and respond to tamper attempts.
OE.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access high side network equipment.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.ONE_WAY	The TOE shall ensure that data can only be transmitted from the low-side to the high-side.
O.FAIL_SECURE	The TOE shall maintain a secure state in the event of a power or hardware failure ensuring that no data can be transferred from the high-side to the low-side, even in the event of such failures.

5 Security Requirements

5.1 Conventions

12 This document uses the following font conventions to identify SFR operations:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

13 None defined.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.5	No illicit information flows
FPT_FLS.1	Failure with preservation of secure state

5.3.1 User Data Protection (FDP)

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 Flow Policy*] on [

- *Subjects: Input Port, Output Port*
- *Information: All Data Transiting the TOE*]

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.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1 The TSF shall enforce the [*Unidirectional Flow Policy*] based on the following types of subject and information security attributes: [

- *Subjects: Input Port, Output Port*
- *Information: All Data Transiting the TOE*
- *Attributes: Inherent attributes*].

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: [*data may flow from the Input Port to the Output Port*].

FDP_IFF.1.3 The TSF shall enforce the [*none*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

FDP_IFF.5 No illicit information flows

Hierarchical to: FDP_IFF.4 Partial elimination of illicit information flows

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [*Unidirectional Flow Policy*].

5.3.2 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- *Power failure*
- *Hardware failure*]

5.4 Assurance Requirements

14 The TOE security assurance requirements (EAL4+) are summarized in Table 9. Augmented components are shown in bold text.

Table 9: Assurance Requirements

Assurance Class	Components	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	**Well-structured internals**
	ADV_TDS.3	Basic modular design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
ALC: Life-cycle Support	**ALC_CMC.5**	**Advanced support**
	ALC_CMS.5	**Development tools CM coverage**
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_FLR.3	**Systematic flaw remediation**
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
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
ATE: Tests	ATE_COV.2	Analysis of coverage

Assurance Class	Components	Description
	ATE_DPT.2	**Testing: security enforcing modules**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability Assessment	**AVA_VAN.4**	**Methodical vulnerability analysis**

6 TOE Summary Specification

6.1 Unidirectional Data Transfer

15 Each of the two physical data diodes is housed in a tamper resistant case and sealed with the same tamper resistant tape used on the enclosure. The data diodes have a 10Gbps fibre optic port for receiving data from the black side and a 10Gbps fibre port for transmitting data to the red side. Optical splitters are used to connect the receive ports on the data diodes to the optical ports on the black onboard system. The optical splitter is used to provide an optical carrier (OC) signal to the fibre optic emitter so that it will send data. This is shown in Figure 2 and Figure 3.

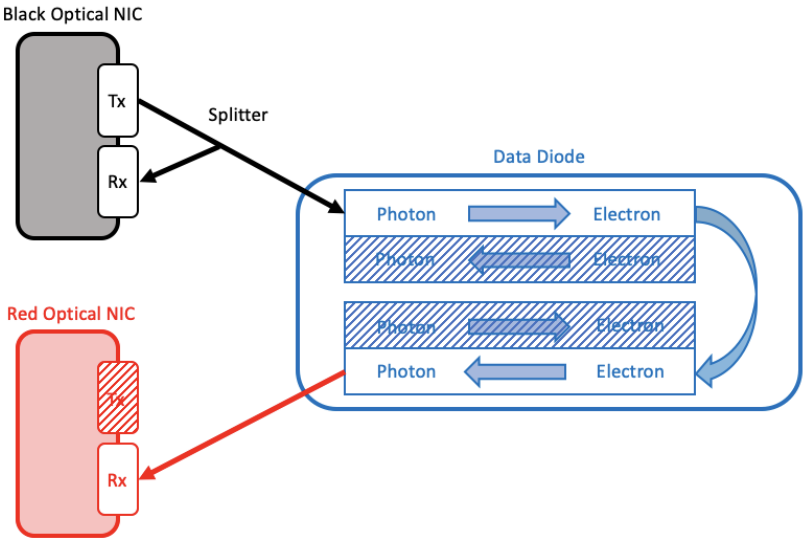

Figure 2: Data Diode Connectivity

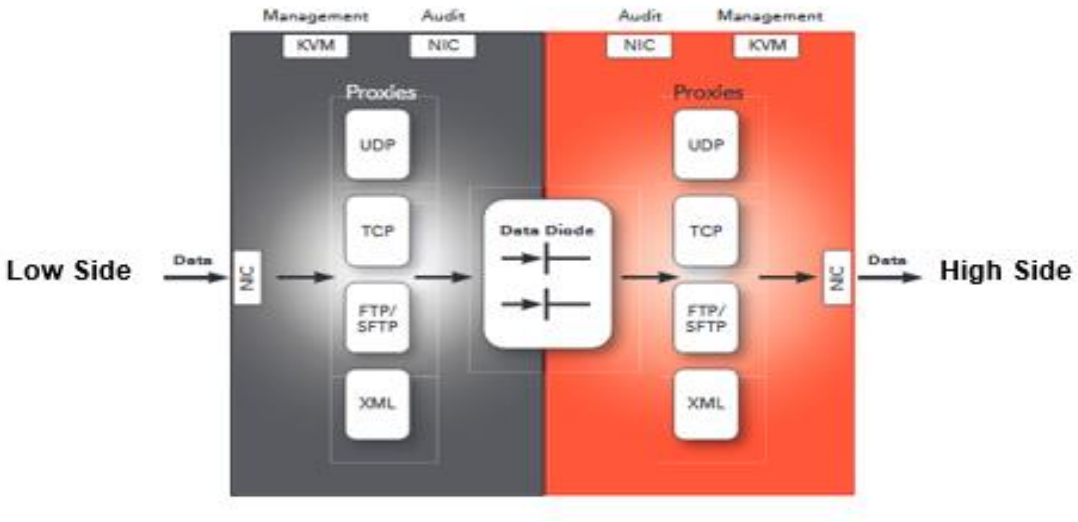

Figure 3: Unidirectional Gateway (Data Diode) Logical Architecture

16 The data diodes themselves are comprised of two Small Form-factor Pluggable (SFP+) transceivers that are powered using power isolator circuitry. The power isolator circuitry ensures that at no time is there a direct electrical path between the black power supply rails input and the SFP power rails output. The first SFP+ transceiver converts the optical signal to an electrical signal. The second SFP+ transceiver converts the electrical signal back to an optical signal so that it can be sent to the red side.

17 Unidirectional data transfer is assured in the following ways:

a) **Connectivity.** The optical network interfaces on the onboard systems have separate transmit and receive ports. This allows single strand optical cables to be used to connect with each optical interface (i.e., one for transmit and one for receive). Single strand optical cable is inherently capable of transferring data in only one direction: there is no return path from the red system to the black system over which to transmit data. The transmit port on the red side is permanently disabled using epoxy while the receive port on the black side only receives the optical carrier signal from the optical splitter. In addition, there is no reverse path through the data diode itself;

b) **Signal Conversion.** The optical signal coming from the black system is converted to electrical and back to optical prior to being transmitted to the red system. This signal conversion mitigates any attempts to leverage the transmission mechanism in an attempt to transfer data in the reverse direction; and

c) **Power Isolation.** The power isolator circuit ensures that the power cannot be used as a low bandwidth mechanism through which to covertly transfer data.

6.2 Fail Secure

18 The absence of a reverse signal path ensures that no data can be transferred from high side (red) to low side (black) regardless of hardware or power failure. Security policy enforcement does not rely on power or active components.

7 Rationale

7.1 Security Objectives Rationale

19 Table 10 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 10: Security Objectives Mapping

	T.TRANSFER	T.TAMPER	T.FAILURE	A.PHYSICAL	A.CONNECT	A.NO_EVIL	A.ENCLOSURE	OSP.PERSONNEL
O.ONE_WAY	X							
O.FAIL_SECURE			X					
OE.PHYSICAL		X		X				
OE.CONNECT	X				X			
OE.NO_EVIL						X		
OE.ENCLOSURE		X					X	
OE.PERSONNEL						X		X

20 Table 11 provides the justification to show that the security objectives are suitable to address the security problem.

Table 11: Suitability of Security Objectives

Element	Justification
T.TRANSFER	**O.ONE_WAY.** Enforcing one-way data transmission prevents the disclosure of information from high-side to low-side. **OE.CONNECT.** The operational environment ensures that the TOE is the only interconnection point between the high-side and the low-side.
T.TAMPER	**OE.PHYSICAL.** The operational environment ensure that delivery, storage and operation occur in a secure manner, commensurate with the security requirements of the high-side – thereby reducing the risk of tampering to acceptable levels.

Element	Justification
	OE.ENCLOSURE. The 1U enclosure surrounding the TOE is resistant to tampering due to its construction and incorporates tamper detection and response mechanisms.
T.FAILURE	**O.FAIL_SECURE.** Ensures that a failure of the TOE does not result in a violation of one-way data transmission.
A.PHYSICAL	**OE.PHYSICAL.** Upholds the assumption by restating it as an objective for the operational environment.
A.CONNECT	**OE.CONNECT.** Upholds the assumption by restating it as an objective for the operational environment.
A.NO_EVIL	**OE.NO_EVIL.** Upholds the assumption by restating it as an objective for the operational environment. **OE.PERSONNEL.** Also contributes to upholding this assumption as high-side security requirements will likely include personnel vetting measures commensurate with the information being protected.
A.ENCLOSURE	**OE.ENCLOSURE.** Upholds the assumption by restating it as an objective for the operational environment.
OSP.PERSONNEL	**OE.PERSONNEL.** Upholds the policy by restating it as an objective for the operational environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

21 EAL4+ has been selected at the direction of the evaluation sponsor.

7.2.2 SFR Rationale

Table 12: Security Requirements Mapping

	O.ONE_WAY	O.FAIL_SECURE
FDP_IFC.2	X	
FDP_IFF.1	X	

	O.ONE_WAY	O.FAIL_SECURE
FDP_IFF.5	X	
FPT_FLS.1		X

Table 13: Suitability of SFRs

Objectives	SFRs
O.ONE_WAY	**FDP_IFC.2.** Defines the scope of the Unidirectional Flow Policy (i.e. input, output, data). **FDP_IFF.1.** Defines the Unidirectional Flow Policy requiring that data only flow from input to output. **FDP_IFF.5.** Requires that there be no illicit information flows from output to input.
O.FAIL_SECURE	**FPT_FLS.1.** Requires the TOE to maintain a secure state in the event of a failure covering power and hardware components.

Table 14: Dependency Analysis

SFR	Dependencies	Rationale
FDP_IFC.2	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met
	FMT_MSA.3	Not met – the security attributes used to define the Unidirectional Flow SFP are inherent (i.e. they are not data objects) and therefore do not need to be initialized.
FDP_IFF.5	FDP_IFC.1	Met
FPT_FLS.1	None	n/a

7.3 TOE Summary Specification Rationale

22 Table 15 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 15: Map of SFRs to TSS Security Functions

	Unidirectional Data Transfer	Fail Secure
FDP_IFC.2	X	
FDP_IFF.1	X	
FDP_IFF.5	X	
FPT_FLS.1		X

--END OF DOCUMENT--