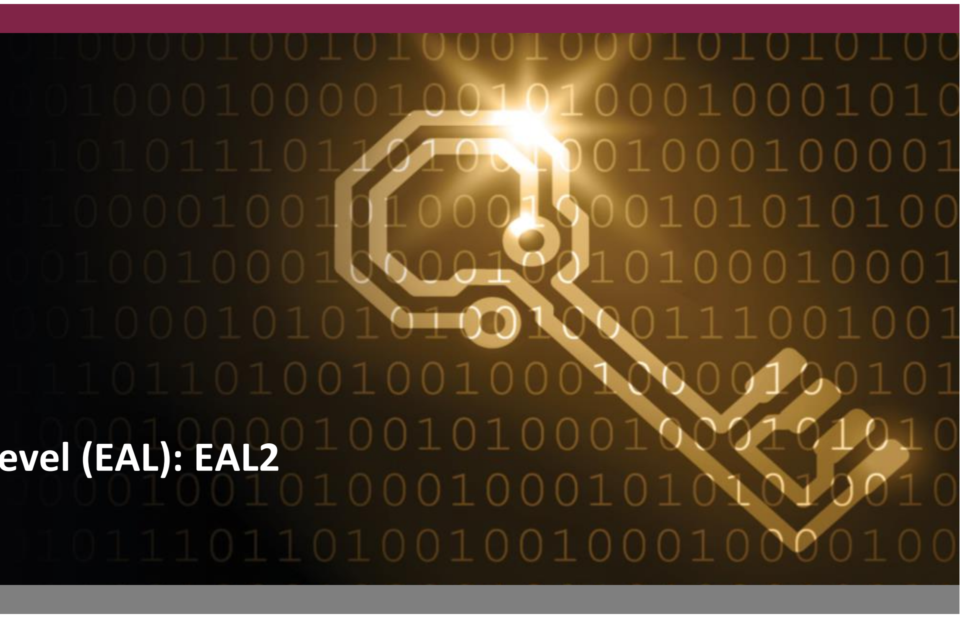
SENTRY

Secured RX and Secured TX

v1.0



Security Target

Evaluation Assurance Level (EAL): EAL2
Document Version: 0.5

Prepared for:

Prepared by:

SENTRY - Paris
14, rue du Zéphyr
Bat A1
91140 Villejust
France

Phone: +33 607 539 513
www.sentryvideowalls.com

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the SENTRY Secured RX and Secured TX v1.0 and will hereafter be referred to as the TOE throughout this document. The TOE is a hardware one-way video and audio encoder and decoder.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*SENTRY Secured RX and Secured TX v1.0 Security Target*
ST Version	Version 0.5
ST Author	Corsec Security, Inc.
ST Publication Date	February 27, 2025
TOE Reference	SENTRY Secured RX and Secured TX v1.0

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. This section provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is a hardware TOE comprised of two devices, the SENTRY Secured RX and Secured TX v1.0, that act as a data diode for audio/video signals between a source device and output device. The TOE is a subset of the SENTRY Secure Video Wall solution, which provides the capability to remove data channels from the video signal, enforcing a one-way video and audio channel to the Video Wall.

The TOE major security feature is protection of data through enforcement of a one-way data stream at the hardware level, by physically removing all unessential data streams, and emulating a clean signal in order to ensure compatibility.

1.3.1 TOE Components

The TOE is comprised of two hardware devices: The Sentry Secured TX (STX) - a video/audio encoder device, and the Sentry Secured RX (SRX) – a video/audio decoder device. The STX and SRX are configured in sequence between the source device and a secure display output. The following paragraphs provide a brief description of the product components.

1.3.1.1 Secured TX Device

The SENTRY SRX & STX is a display adapter with an HDMI-in port, HDMI-out loopout port, one-way optical fiber port, and a 12V power connector. The STX device is the main device transforming HDMI digital signals into optical signals transferred via optical fiber. It includes an HDMI loopout port (to provide a local copy of the video source displayed), an EDID emulator that forces signal resolution to avoid communication errors with the final display, and a HDMI to Optical Fiber transceiver.

1.3.1.2 Secured RX Device

The SENTRY SRX is a display adapter with an optical fiber-in port, an HDMI-out port, and a 12v power connector. The SRX transforms optical signal back into HDMI digital signals.

1.4 Non-TOE Hardware/Software/Firmware

The following environmental components are required for operation of the TOE:

- Video/audio source device meeting the minimum requirements outlined in Table 2
- HDMI display (for local display loopout)
- HDMI display (for secure output)
- 3x HDMI cables
- 1x LC Optical Fiber cable

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – TOE Minimum Requirements

Category	Requirement
Image Source Device	Resolution 1920x1080p@30hz

No additional software or firmware is required to operate the TOE.

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a hardware platform compliant to the minimum requirements as listed in Table 2. The TOE is installed as depicted in Figure 1. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Video/audio source device
- HDMI display (for local display loopout)
- HDMI display (for secure output)
- 3x HDMI cables
- 1x LC Optical Fiber cable

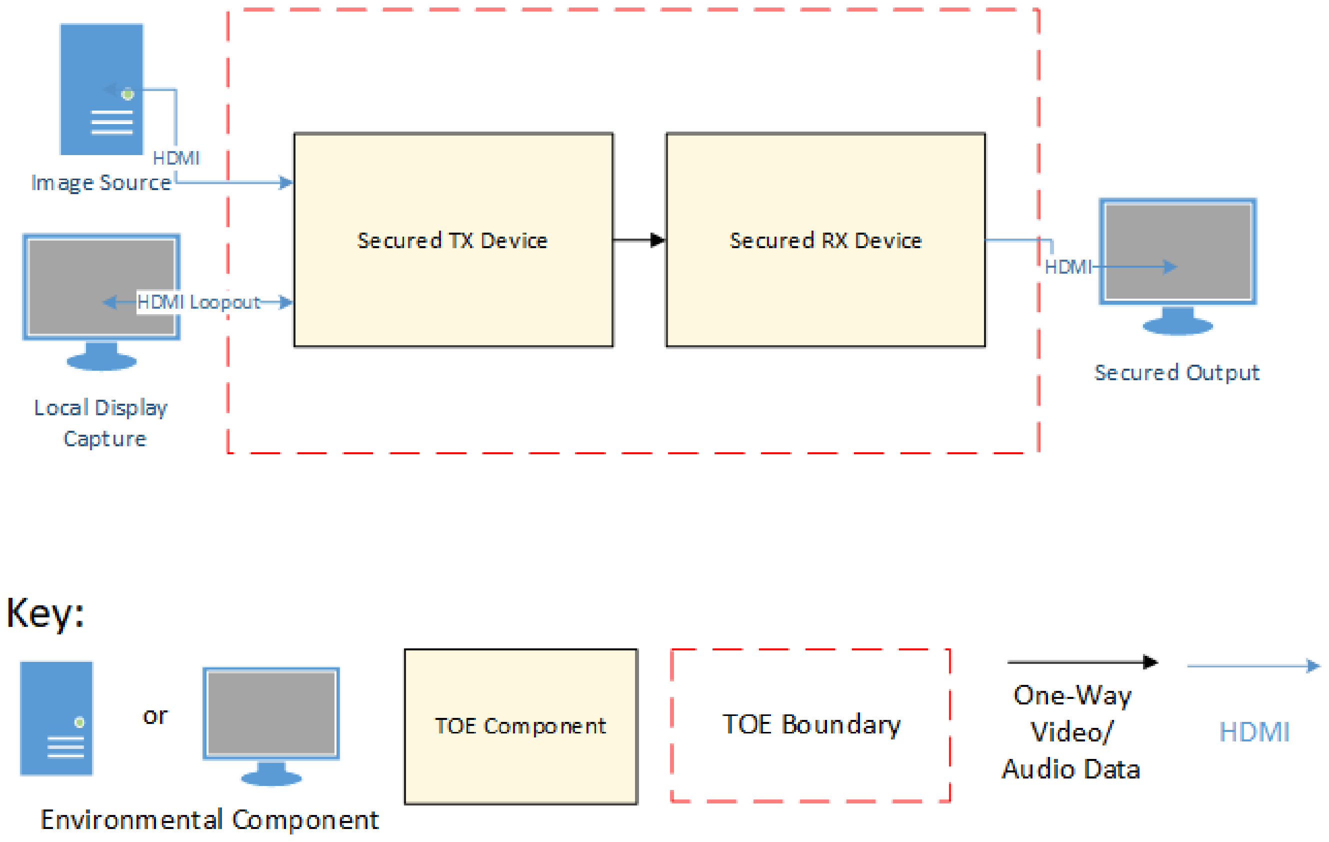


Figure 1 – Physical TOE Boundary

1.5.1.1 TOE Hardware

The TOE is a hardware-only TOE and is comprised of the SRX & STX v1.0

Customers can verify that the TOE hardware they receive is from SENTRY rather than an imposter by confirming that the package is being delivered either through MOD[1] agreed transport companies or in-person by SENTRY employees. SENTRY employees are identified by their company-issued badges.

With either delivery method, the TOE hardware is provided with tamper-evident labels. In the event the label appears to have been tampered with, SENTRY will declare the device unusable.

1.5.1.2 Guidance Documentation

The following PDF-formatted guide, which is available for SENTRY customers with an active account to download through the SENTRY website, are required reading and part of the TOE:

Table 3 – Guidance Documentation

Name	Format	SHA-256 Hash	Download
SENTRY Secured RX and Secured TX Devices Guidance Supplement v0.5	PDF	43972d97a46a131fb8ba574ff1b66f4e539a0e36a66 3f437941a0ff886269746	https://www.sentryvideowalls .com/en/partner-zone/secured-rx-tx-devices

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

- User Data Protection

1.5.2.1 User Data Protection

The TOE enforces a one-way video and audio data stream from the source device to a secure output display device, ensuring that only the video and audio channels are passed through, and no data can be passed back to the source device through the TOE, therefore protecting all other connected devices from unwanted communications.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

There are no features and/or functionality that are not part of the evaluated configuration of the TOE.

[1] Ministry of Defense

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, CC:22, Revision 1, November 2022; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) v1.1 as of July 22, 2024 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- Remote processes: Rogue processes inserted to the host system connected to the TOE which have the potential to communicate with other devices connected to the TOE via the HDMI EDID channel.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[2] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 lists the applicable threats.

Table 5 – Threats

Name	Description
T.TAMPERING	A user or process on the SRX device that either (a) accidentally or deliberately breaches the confidentiality of SRX information by transmitting data through the TOE to the STX device or, (b) accidentally or deliberately breaches the integrity of the STX device by transmitting data through the TOE to the STX device.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 6 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 6 – Organizational Security Policies

Name	Description
P.TRAFFIC_FLOW	The TOE must route data in accordance with the implemented information flow control policy.

[2] TSF – TOE Security Functionality

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 7 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 7 – Assumptions

Name	Description
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE will be protected from unauthorized modification.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 8.

Table 8 – Security Objectives for the TOE

Name	Description
O.TRAFFIC	The TOE must route traffic only as defined by the information flow control SFP.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 9 lists the IT security objectives that are to be satisfied by the environment.

Table 9 – IT Security Objectives

Name	Description
OE.PROTECT_TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 10 lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 10 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_IFC.2	Complete information flow control		X		
FDP_IFF.1	Simple security attributes		X		

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

6.2.1 Class FDP: User Data Protection

FDP_IFC.2 Complete information flow control

FDP_IFC.2.1

The TSF shall enforce the [*information flow control SFP*] on [*the following:*

- *Subjects: Source devices*
- *Information: Audio data, video data*]

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

FDP_IFF.1.1

The TSF shall enforce the [*information flow control SFP*] based on the following types of subject and information security attributes: [*Only the following components of the HDMI signal are passed through:*

- *Video data*
- *Audio data*].

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: [*Only a minimum standard HDMI signal will be accepted*].

FDP_IFF.1.3

The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules*].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC:2022 Part 3 and are an EAL2 assurance level as defined in CC:2022 Part 5. Table 12 summarizes these requirements.

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
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 13 lists the security functionality and their associated SFRs.

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR	Description
User Data Protection	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes

7.1.1 User Data Protection

The Information Flow Control SFP is used to enforce one-way communication from video/audio source devices to the secure output display device. Only the video and audio channels are passed through. The SFP is strictly enforced by way of physically negating connections for additional data streams supported by the HDMI protocol, while emulating the additional data streams so as not to disrupt the HDMI signal.

TOE Security Functional Requirements Satisfied: FDP_IFC.2, FDP_IFF.1.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, 2022 Revision 1.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 14 provides a mapping of the objectives to the threats they counter.

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.TAMPERING A user or process on the SRX device that either (a) accidentally or deliberately breaches the confidentiality of SRX information by transmitting data through the TOE to the STX device or, (b) accidentally or deliberately breaches the integrity of the STX device by transmitting data through the TOE to the STX device.	OE.PROTECT_TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to protect itself and the TOE from external interference or tampering.	OE.PROTECT_TRAFFIC ensures that the TOE is protected from external interference or tampering.

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 15 gives a mapping of policies and the objectives that support them.

Table 15 – Policies: Objectives Mapping

Policies	Objectives	Rationale
P.TRAFFIC_FLOW The TOE must route data in accordance with the implemented security policy.	O.TRAFFIC The TOE must route or switch traffic only as defined by the information flow control SFP.	O.TRAFFIC ensures that traffic is routed only as dictated by the information flow control SFP, meeting the P.TRAFFIC_FLOW policy.

Every policy is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT_TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.NOEVIL The users who manage the TOE are nonhostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are nonhostile, appropriately trained and follow all guidance.

Every assumption is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 shows a mapping of the objectives and the SFRs that support them.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.TRAFFIC The TOE must route or switch traffic only as defined by the information flow control SFP.	FDP_IFC.2 Complete information flow control	The requirement meets the objective by enforcing an information flow control policy that ensures that access to data is granted in a controlled manner to prevent data anomalies.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFF.1 Simple security attributes	The requirement meets the objective by providing information flow control functionality to manage data flows within the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR	Dependencies	Dependency Met	Rationale
FDP_IFC.2	FDP_IFF.1	Yes	
FDP_IFF.1	FDP_IFC.1	Yes	Although FDP_IFC.1 is not included, FDP_IFC.2, which is hierarchical to FDP_IFC.1 is included. This satisfies this dependency.
	FMT_MSA.3	N/A	FMT_MSA.3 is not included because the TOE does not provide any management functions.
FMT_MSA.3	FMT_MSA.1	N/A	FMT_MSA.1 is not included because the TOE does not provide any management functions
	FMT_SMR.1	N/A	FMT_SMR is not included because the TOE does not maintain any user roles
FMT_MSA.1	FDP_IFC.1	Yes	Although FDP_IFC.1 is not included, FDP_IFC.2, which is hierarchical to FDP_IFC.1 is included. This satisfies this dependency.
	FMT_SMR.1	N/A	FMT_SMR.1 is not included because the TOE does not maintain any user roles
	FMT_SMF.1	N/A	FMT_SMF.1 is not included because the TOE does not provide any management functions
FMT_SMR.1	FIA_UID.1	N/A	FIA_UID.1 is not included because the TOE is a hardware device with no user interface. It does not support any authentication or identification functions.
FMT_SMF.1	No dependencies		
FIA_UID.1	No dependencies		

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms and Terms

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IT	Information Technology
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com