13 MARCH 2020
Document Version 1.0

INVISIRON CYBER DEFENCE PLATFORM SECURITY TARGET

invisiron®

For more information visit us at

https://invisiron.com

Document management

Document identification

Document Title	Invisiron Cyber Defence Platform Security Target
Document Version	1.0
Document Date	13-MAR-2020
Release Authority	Invisiron Pte Ltd

Document history

Version	Date	Description
0.1	31-OCT-2019	Initial Released
0.2	06-NOV-2019	Updated Section 1
0.3	07-NOV-2019	Minor corrections in Section 1 and Section 5
0.4	08-NOV-2019	Minor correction in Figure 1
0.5	12-DEC-2019	Added one security feature in Section 1, Section 5 and Section 6
0.6	17-FEB-2020	Updated the TOE name from Solida to Invisiron Updated Section 1, Section 5 and Section 6 based on evaluator's findings
1.0	13-MAR-2020	Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1) 5

1.1 ST Reference 5

1.2 TOE Reference 5

1.3 Document Organization 5

1.4 Defined Terms 6

1.5 TOE Overview 7

1.5.1 TOE Usage and Major Security Functions 7

1.5.2 TOE Type 7

1.5.3 Supporting Hardware, Software and/or Firmware 8

1.6 TOE Description 8

1.6.1 Physical Scope of the TOE 8

1.6.2 Logical Scope of the TOE 12

2 Conformance Claim (ASE_CCL.1) 14

3 Security Problem Definition (ASE_SPD.1) 15

3.1 Overview 15

3.2 Threats 15

3.3 Organisational Security Policies 16

3.4 Assumptions 16

4 Security Objectives (ASE_OBJ.2) 17

4.1 Overview 17

4.2 Security Objectives for the TOE 17

4.3 Security Objectives for the Environment 18

4.4 Security objectives rationale 18

4.4.1 TOE security objectives rationale 19

4.4.2 Environment security objectives rationale 21

5 Security Requirements (ASE_REQ.2) 23

5.1 Overview 23

5.2 Extended Components Definition 23

5.2.1 Intrusion and Packet Content Detection System (IDS) 23

5.3 Security Functional Requirements 27

5.3.1 Overview 27

5.3.2 IDS_SDC_EXT.1 IDS data collection 28

5.3.3 IDS_ANL_EXT.1 Analyzer analysis and Packet Filtering 29

5.3.4 IDS_RCT_EXT.1 Analyzer reaction 29
5.3.5 IDS_RDR_EXT.1 Restricted data review 29
5.3.6 IDS_STG_EXT.1 Guarantee of IDS data availability 30
5.3.7 IDS_STG_EXT.2: Prevention of IDS data loss 30
5.3.8 FAU_GEN.1 Audit data generation 30
5.3.9 FAU_SAR.1 Audit Review 31
5.3.10 FDP_ACC.1 Subset access control 31
5.3.11 FDP_ACF.1 Security attribute based access control 33
5.3.12 FIA_ATD.1 User attribute definition 33
5.3.13 FIA_AFL.1 Authentication failure handling 33
5.3.14 FIA_UAU.2 User authentication before any action 34
5.3.15 FIA_UID.2 User identification before any action 34
5.3.16 FIA_SOS.1 Verification of secrets 34
5.3.17 FMT_MSA.1 Management of security attributes 34
5.3.18 FMT_MSA.3 Static attribute initialisation 35
5.3.19 FMT_MTD.1 Management of TSF data 35
5.3.20 FMT_MOF.1 Management of security functions behaviour 35
5.3.21 FMT_SMF.1 Specification of Management Functions 36
5.3.22 FMT_SMR.1 Security Roles 36
5.3.23 FTP_TRP.1 Trusted Path 37
5.3.24 FPT_STM.1 Reliable Time Stamps 37

5.4 TOE Security Assurance Requirements 37
5.4.1 Explanation for Selecting the SARs 38

5.5 Security Requirements Rationale 39
5.5.1 Dependency Rationale 39
5.5.2 Mapping of SFRs to Security Objectives for the TOE 40

6 TOE Summary Specification (ASE_TSS.1) 43

6.1 Overview 43
6.2 Intrusion Detection and Prevention 43
6.3 Security Audit 44
6.4 Identification and Authentication 44
6.5 Security Management 44
6.6 Secure Communication 45

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	Invisiron Cyber Defence Platform Security Target
ST Version	1.0
ST Date	13-MAR-2020

1.2 TOE Reference

TOE Title	Invisiron Cyber Defence Platform 3.1.0 executing on S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances
TOE Software Version	Invisiron Cyber Defence Platform 3.1.0
TOE Hardware Models	S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
Authentication Data	It is information used to verify the claimed identity of a user.
Admin	Users that are allowed to perform both TOE configuration and monitoring application
Authorised User	Authorised user is a user that has the privilege (assigned by Admin) to perform either TOE monitoring only or both TOE configuration and monitoring
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
SSH	Secure Shell
SIEM	Security information and event management
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TOE	Target of Evaluation
User data	Data created by and for the user, which does not affect the operation of the TSF.

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The TOE is Invisiron Cyber Defence Platform 3.1.0 executing on S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender appliances. The TOE is a software and hardware appliance. Each appliance model operate using an identical software image with identical functionality. The TOE is used as a network monitoring and incident management platform. They implement an intrusion and prevention system and reputation based detection. The intrusion detection and prevention engine implements a full deep packet inspection capability (DPI). This engine is controlled by rules that are similar to the industry standard SNORT rules. These rules allow for performing deep packet inspection of the network traffic at full line rate. The reputation based detection engine is built around blacklists. These blacklists contain malicious IP addresses, domain names, DGA domains, Tor exit nodes, URLs and SSL certificates. In addition to the security engines the TOE also provides security event logging and packet capture. This data is stored in files which can be exported out from the platforms. The TOE physical boundary defines all hardware and software that is required to support the TOE's logical boundary as well as the TOE's security functionality.

The following table highlights the range of security functions implemented by the TOE:

Security Feature	Description
Intrusion and Packet Content Detection System	The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured security filters. If the analysis of collected network traffic indicates a potential intrusion attempt or the presence of malicious content in a packet, an action set associated with the detecting filter is triggered.
Security Audit	The TOE generates audit records for security events. Admin and Authorised User has the ability to view and export the audit and transaction logs.
Identification and Authentication	Admin and Authorised user are required to identify and authenticate with the TOE prior to any user action or information flow being permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
Secure Communication	The TOE can protect the user data from disclosure and modification by using HTTPS (TLS v1.2) and SSH as a secure communication

1.5.2 TOE Type

The TOE is a software and hardware and is used as an network monitoring and incident management platform. The TOE provides security functionality such as Intrusion and Packet Content Detection

system, Security Audit, Identification and Authentication, Security Management and Secure Communication. The TOE can be categorised as *Network and Network-Related Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Supporting Hardware, Software and/or Firmware

Minimum System Requirements	
Appliance	
Software	Invisiron Cyber Defence Platform 3.1.0
Hardware	S-1000, S-2000, S-4000, S-6000, S-6000DNS, S-6000DDoS and microDefender
Web-based GUI User	
Web Browser	Microsoft Edge 44 and later Mozilla Firefox 64 and later Google Chrome 71 and later

1.6 TOE Description

1.6.1 Physical Scope of the TOE

The TOE implements an advanced cyber threat defence mechanism. It is designed to be installed in line between an Internet router and the main network switch or firewall. Network packets are inspected in real-time as they pass through the platform in both directions (inbound and outbound protection). Malicious network packets can be dropped instantly before they have a chance to reach inside the protected network.

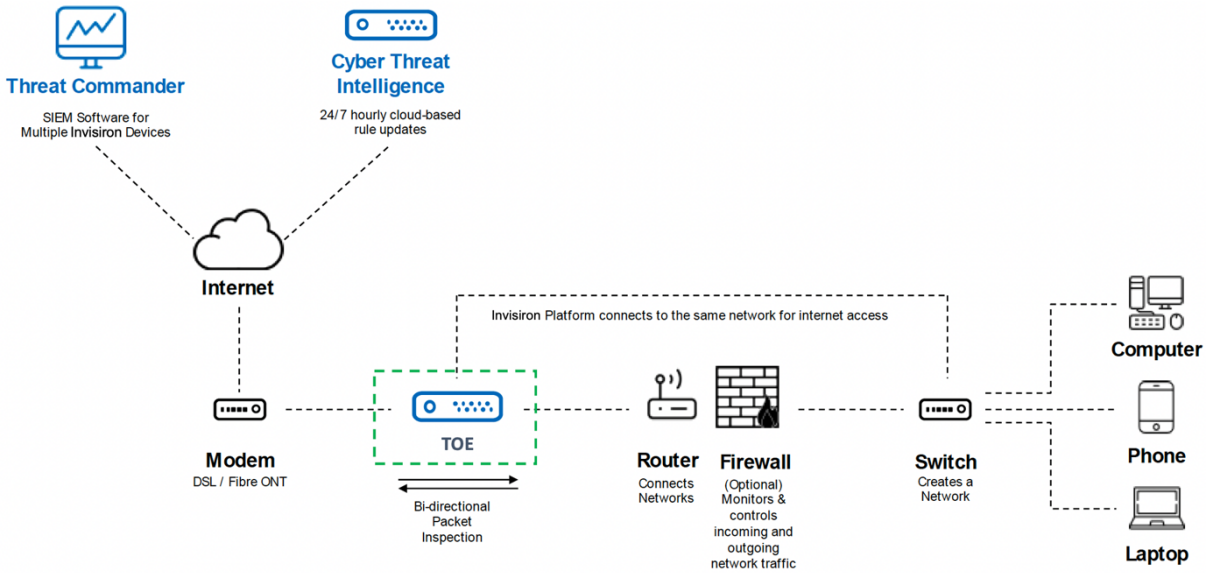

Figure 1 - TOE Physical Scope

The TOE is divided up into two sections. One section performs the security operations on the network packets and the other section handles the management and configuration of the platform. The section that handles the security operations for the protected network is implemented without the use of a traditional operation system. Instead it is implemented using a technology that allows for direct ownership of the hardware of the server. The section that handles management and configuration is implemented using a Linux kernel and a limited set of support functions.

The platforms presence on the network is transparent to other IT equipment in the protected network. No IP addresses or MAC addresses are required or exposed on the Ethernet ports used for network protection. Network packets travel through the platform in stealth mode and the security operations are performed on the packets as they reside temporarily in memory buffers in the platform. There are no TCP/IP stacks being used and there is no operating system involved in the security operations. The configuration and management is handled through a separate dedicated management Ethernet port only accessible from inside the protected network. The platforms are configured and managed through a web GIU application accessed from this management Ethernet connection. One part of this GUI web application handles device configuration and the second part allows for monitoring the device. This communication goes over HTTPS through the use of a standard web browser inside the platform.

An external cloud located server is used to transfer up-to-date Cyber Threat Intelligence (CTI) to the TOE containing lists of malicious IP addresses, domain names, URL's, SSL certificates, TOR exit nodes, DGA domain names and DPI rules. The TOE use this intelligence to make decisions about what network packets to allow into the protected network and which ones to block and drop. The TOE performs automatic hourly updates of this CTI over a SSH or HTTPS connection. In addition to CTI updates the TOE also pull software updates from this server. The TOE support remote monitoring through either a third party monitoring tool or by Invisiron's own developed remote monitoring tool called Threat

Commander SIEM. The TOE send security events over a SSH to an external server running the remote monitoring software.

The table below identifies the difference between each TOE hardware models. The table only shows the features that vary between platforms. Other features are supported in an identical way between all platforms.

Functions / TOE Hardware Models	HA Mode	Dual WAN	DDoS	DNS filter	10GbE
S-1000	N/A	N/A	N/A	N/A	N/A
S-2000	X	N/A	N/A	N/A	N/A
S-4000	X	X	N/A	N/A	N/A
S-6000	X	N/A	N/A	N/A	X
S-6000DNS	N/A	N/A	N/A	X	X
S-6000DDoS	X	N/A	X	N/A	X
microDefender	N/A	N/A	N/A	N/A	N/A

- **HA Mode**

  Supports running a pair of two platforms together in an active passive configuration mode.

- **Dual WAN**

  Support for connecting the platform with two independent Internet connections and using them in an active/passive mode for failure protection.

- **DDoS**

  Support for mitigating denial-of-service and distributed denial-of-service attacks.

- **DNS filter**

  Packet filtering with rules and logic tailored for DNS packets.

- **10 GbE**

Support for 10 Gigabit Ethernet connections through copper or optical SFP modules.

The Ethernet ports on the NIC card are fully transparent to the traffic that flows through them. This means there are no visible MAC addresses or IP addresses associated with these ports. There is also no traditional networking stack attached to these ports. Instead, packets are flowing freely in and out through the ports at the highest speed allowed by the NIC card. The microDefender Cyber Defense Platform is based on an Arm processor and Ethernet ports included on the motherboard. Its security functionality is identical to that of the other platforms.

The table below describes the ports and interfaces implemented by the TOE and if they are used in the TOE or not.

Port/Interfaces	Management	Internet/ Network Data	External threat data collection	Remote Monitoring and Control	Same on all devices
Local Management Ethernet port	X	N/A	X	X	Yes
WAN Ethernet ports	N/A	X	N/A	N/A	Yes
LAN Ethernet ports	N/A	X	N/A	N/A	Yes
Additional Ethernet ports	N/A	N/A	N/A	N/A	Yes
USB ports	N/A	N/A	N/A	N/A	Yes
HDMI/VGA port	N/A	N/A	N/A	N/A	Yes

The physical boundary includes the following guidance documentation:

- Invisiron User Manual S-1000 Cyber Defence Platform
- Invisiron User Manual S-2000 Cyber Defence Platform
- Invisiron User Manual S-4000 and S-6000 Cyber Defence Platforms
- Invisiron User Manual S-6000DDoS Denial of Service Mitigation
- Invisiron User Manual S-6000DNS DNS Threat Mitigation
- Invisiron User Manual microDefender Cyber Defence Platform

The TOE is delivered by Invisiron's authorized representative to the customer. The TOE is wrapped in a plastic bag to provide resistance against moisture. Each TOE is then enclosed in cardboard shipping boxes and sealed with tape that contains Invisiron logo. A shipping label identifying the exact product (including the serial number for the included device) and the customer name is provided on the outside of the box. If any issues occur during the delivery process, the customer or appointed account

manager can communicate via a phone call or face-to-face to resolve the issue via contact information provided below.

Invisiron maintain one product support center which is located in Singapore

The contact information for the support center is:

- Invisiron Pte Ltd
  1 Pemimpin Drive #08-03, One Pemimpin
  Singapore 576151
  Phone: +65 6692 6760

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

- **Intrusion and Packet Content Detection System**. The TOE collects network traffic and subjects it to statistical and signature-based analysis, depending on configured security filters. If the analysis of collected network traffic indicates a potential intrusion attempt or the presence of malicious content in a packet, an action set associated with the detecting filter is triggered. The action set determines if the traffic is permitted or blocked. If traffic is permitted, an alert will be written to a TOE data log (specifically, the Event log). If traffic is blocked, an alert will also be written to the TOE Event log. Writing an alert to the TOE data log (specifically, the Event log) is always performed—in the evaluated configuration, action sets that block traffic always generate an alert. In addition to writing to the TOE data log files, the TOE can generate alerts in the form of a notification to a syslog server or through an email to an email address. The TOE provides capabilities for the admin and authorised users to review the TOE data logs. The TOE protects the TOE data logs from modification and deletion. When the space available for TOE data storage is exhausted, the oldest of the TOE log data files is deleted and an audit record to this effect is generated. The TOE can be configured to block or permit network traffic based on protocol, packet contents or IP address and port. Network traffic that is permitted based on traffic management filtering is still subject to IPS filtering, unless the traffic management filter is configured to allow traffic through the device without IPS filtering

- **Security Audit.** The TOE generates audit records for security events. Types of audit logs are:

  - Low severity security incidents
  - Medium severity security incidents
  - Critical severity security incidents

  Only Admin and Authorised user have the capability to view and export these audit and transaction logs via the web-based GUI interface

- **Identification & Authentication.** All users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to key in a valid username and password in order to access the TOE. The acceptable minimum password length is 6-characters and maximum is 30-characters. The TOE checks the credentials presented by the user against the authentication information stored in the database. There are two types of users; Admin and Authorised User. Admin is a user that is allowed to perform both TOE configuration and monitoring. Authorised user is a user that has the privilege (assigned by Admin) to perform either TOE monitoring only or both TOE configuration and monitoring

- **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The TOE provides web-based GUI interface that permit the admin to configure and manage the TOE.

- **Secure Communication.** The TOE provides a secure HTTPS (TLS v1.2) and SSH channel between the TOE and remote users/IT Systems. It also provides assured identification of its end points and protection of the communicated data from modification or disclosure

2 Conformance Claim (ASE_CCL.1)

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2

3 Security Problem Definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The following are threats identified for the TOE and the IT System the TOE monitors:

Identifier	Threat statement
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to modify the behaviour of TSF data without being detected.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.REPLAY	An unauthorized person may replay valid identification and authentication data obtained while monitoring the TOE's network interface to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.

Identifier	Threat statement
T.TOECOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between distributed components of the TOE.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.MALICE	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organisational Security Policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE:

Identifier	Assumption statement
A.NOEVIL	Authorized admins are non-hostile and follow all administrator guidance.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

4 Security Objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

The following are the TOE security objectives:

Identifier	Objective statements
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized admin use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.MEDIAT	The TOE must mediate the flow of all information from users on an external network to resources on an internal network and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized admin to use the TOE security functions and must ensure that only authorized admins are able to access such functionality.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components.
O.SENSOR	The TOE shall collect IDS data in the form of network packets flowing between network segments to which it is connected.

O.ANALYZER	The TOE shall analyse collected IDS data in order to identify intrusion attempts and shall be able to record the results of its analysis.
O.RESPONSE	The TOE shall respond to intrusion attempts it identifies based on its configuration.
O.REVIEW	The TOE shall provide capabilities for effective review of stored IDS data.
O.STORAGE	The TOE shall provide capabilities to automatically manage stored audit records and IDS data in the event that available storage space is exhausted.

4.3 Security Objectives for the Environment

The following are the security objectives for the operational environment of the TOE:

Identifier	Objective statements
OE.ADMTRA	Authorized admins are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

4.4 Security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

THREATS/ ASSUMPTIONS / OBJECTIVES	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAUTH	T.OLDINF	T.PROCOM	T.REPLAY	T.SELPRO	T.TUSAGE	T.TOECOM	T.MISUSE	T.INFLUX	T.MALICE	A.NOEVIL	A.PHYSEC	A.SINGEN
O.ACCOUN	✓															
O.AUDREC	✓															
O.IDAUTH				✓												
O.MEDIAT			✓		✓											
O.SECFUN		✓														
O.SECSTA								✓								
O.SINUSE							✓									
O.TOECOM										✓						
O.SENSOR											✓		✓			
O.ANALYZER											✓		✓			
O.RESPONSE											✓		✓			
O.REVIEW											✓		✓			
O.STORAGE												✓				
OE.ADMTRA									✓					✓		
OE.GUIDAN									✓							
OE.PHYSEC															✓	
OE.SINGEN																✓

4.4.1 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats in the security problem definition.

Threats	Rationale
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that admin is accountable for the use of security functions related to audit.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search the information contained in the audit trail.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.
O.SECFUN	This security objective is necessary to counter the threat T.AUDFUL by requiring that the TOE provides functionality that ensures that only the admin and authorized user has access to the TOE security functions.
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threat T.SELPRO.
O.SINUSE	This security objective is necessary to counter the threats: T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
O.TOECOM	This security objective is necessary to counter the threat T.TOECOM by requiring the TOE to protect the confidentiality of communications between distributed TOE components.
O.SENSOR	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to collect all network packets flowing between network segments to which it is connected
	This security objective is necessary to counter the threat T.MALICE by ensuring the TOE is able to collect all network packets flowing between network segments to which it is connected in order to capture malicious packet
O.ANALYZER	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to analyse those network packets and network flows in order to identify intrusion attempts such as misuse of an IT System

Threats	Rationale
	This security objective is necessary to counter the threat T.MALICE by ensuring the TOE is able to analyse those network packets and network flows in order to identify intrusion attempts such as malicious packet
O.RESPONSE	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to respond in order to identified intrusion attempts such as misuse of an IT System
	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to respond in order to identified intrusion attempts such as malicious packet
O.REVIEW	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to provide capabilities to review the results of the TOE's analysis and response of the identified intrusion attempts such as misuse of an IT System
	This security objective is necessary to counter the threat T.MISUSE by ensuring the TOE is able to provide capabilities to review the results of the TOE's analysis and response of the identified intrusion attempts such as malicious packet
O.STORAGE	This security objective is necessary to counter the threat T.INFLUX by ensuring the TOE is able to automatically manage storage of audit records and IDS data in the event that available storage is exhausted.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions in the security problem definition.

Assumptions	Rationale
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that authorized admins receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).

Assumptions	Rationale
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE (A.SINGEN)

5 Security Requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Extended Components Definition

5.2.1 Intrusion and Packet Content Detection System (IDS)

This ST defines a new functional class for use within this ST: Intrusion and Packet Content Detection System (IDS). This family of IDS requirements was created to specifically address the data collected and analysed by the TOE. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of security data and specify requirements for collecting, analysing and reviewing malicious data.

5.2.1.1 IDS Data Collection (IDS_SDC_EXT)

This family defines requirements for being able to collect IDS data from targeted IT resources.

Management: IDS_SDC_EXT.1
The following actions could be considered for the management functions in FMT:
a) maintenance of the parameters that control IDS data collection.

Audit: IDS_SDC_EXT.1

There are no auditable events foreseen.

IDS_SDC_EXT.1 IDS data collection

Hierarchical to: No other components.

Dependencies: None

IDS_SDC_EXT.1.1 The TSF shall be able to collect the following information from targeted IT System resource(s):
a) **[*selection: network traffic*]**; and
b) **[assignment: no additional events]**.

IDS_SDC_EXT.1.2 At a minimum, the TSF shall collect and record the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the *Details* column of the following table.

Event	**Details**
Network traffic	Protocol, source address, destination address

5.2.1.2 IDS Analyzer and Packet Filtering (IDS_ANL_EXT)

This family defines requirements for being able to analyse collected IDS data.

Management: IDS_ANL_EXT.1
The following actions could be considered for the management functions in FMT:
a) maintenance of the parameters that control IDS data analysis.

Audit: IDS_ANL_EXT.1
There are no auditable events foreseen.

IDS_ANL_EXT.1 Analyzer analysis and Packet Filtering

Hierarchical to: No other components.

Dependencies: IDS_SDC_EXT.1

IDS_ANL_EXT.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:
a) **[*selection: packet filtering, statistical, signature*]**; and
b) **[assignment: no other function]**.

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information:
a) Date and time of the result, type of result, identification of data source; and
b) **[assignment: data destination, protocol and severity]**.

5.2.1.3 Intrusion Reaction (IDS_RCT_EXT)

This family defines requirements for being able to react to the results of IDS data analysis.

Management: IDS_RCT_EXT.1
The following actions could be considered for the management functions in FMT:
a) maintenance of the parameters that control IDS reaction.

Audit: IDS_RCT_EXT.1
There are no auditable events foreseen.

IDS_RCT_EXT.1 Analyzer reaction

Hierarchical to: No other components.

Dependencies: IDS_ANL_EXT.1

IDS_RCT_EXT.1.1 The TSF shall send an alarm to **[assignment: the IDS data log and the notification contacts configured for the filter triggered by the network traffic]** and take **[assignment: the action configured for the filter triggered by the network traffic, which can be to:**

- **Block the network traffic**

- **Permit the network traffic**

] when an intrusion is detected.

5.2.1.4 IDS Data Review (IDS_RDR_EXT)

This family defines requirements for reviewing IDS data and restricting access to IDS data.

Management: IDS_RDR_EXT.1
The following actions could be considered for the management functions in FMT:
a) maintenance of the group of users with read access rights to the IDS data.

Audit: IDS_RDR_EXT.1
There are no auditable events foreseen.

IDS_RDR_EXT.1 Restricted data review

Hierarchical to: No other components.
Dependencies: IDS_SDC_EXT.1, IDS_ANL_EXT.1

IDS_RDR_EXT.1.1	The TSF shall provide **[assignment: authorised users and admin]** with the capability to read **[assignment: list of IDS data]** from the IDS data.
IDS_RDR_EXT.1.2	The TSF shall provide the IDS data in a manner suitable for the user to interpret the information.
IDS_RDR_EXT.1.3	The TSF shall prohibit all users read access to the IDS data, except those users that have been granted explicit read access.

5.2.1.5 IDS Data Storage (IDS_STG_EXT)

This family defines requirements for securely storing IDS data.

Management: IDS_STG_EXT.1, IDS_STG_EXT.2
There are no management actions foreseen.
Audit: IDS_STG_EXT.1, IDS_STG_EXT.2
There are no auditable events foreseen.

IDS_STG_EXT.1 Guarantee of IDS data availability

Hierarchical to: No other components.

Dependencies: IDS_SDC_EXT.1, IDS_ANL_EXT.1

IDS_STG_EXT.1.1	The TSF shall protect the stored IDS data from unauthorized deletion.
IDS_ STG_EXT.1.2	The TSF shall protect the stored IDS data from modification.
IDS_ STG_EXT.1.3	The TSF shall ensure that **[assignment: metric for saving IDS data]** IDS data will be maintained when the following conditions occur: **[*selection: IDS data storage exhaustion*]**.

IDS_STG_EXT.2: Prevention of IDS data loss

Hierarchical to: No other components.

Dependencies: IDS_STG_EXT.1

IDS_STG_EXT.2.1 The TSF shall **[*selection: overwrite the oldest stored IDS data*]** and send an alarm if the storage capacity has been reached.

5.3 Security Functional Requirements

5.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Identifier	Title
Intrusion and Packet Content Detection System (IDS)	
IDS_SDC_EXT.1	IDS data collection
IDS_ANL_EXT.1	Analyzer analysis and Packet Filtering
IDS_RCT_EXT.1	Analyzer reaction
IDS_RDR_EXT.1	Restricted data review
IDS_STG_EXT.1	Guarantee of IDS data availability
IDS_STG_EXT.2	Prevention of IDS data loss
Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
Access Control	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute-based access control
Identification and Authentication	
FIA_ATD.1	User Attribute Definition

Identifier	Title
FIA_AFL.1	Authentication failure
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_SOS.1	Verification of secrets
Security Management	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data (Password)
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
Trusted Path	
FTP_TRP.1	Trusted Path
Time Stamps	
FPT_STM.1	Reliable time stamps

5.3.2 IDS_SDC_EXT.1 IDS data collection

<table>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td>IDS_SDC_EXT.1.1</td><td>The TSF shall be able to collect the following information from targeted IT System resource(s):
a) [network traffic]; and
b) [no additional events]</td></tr>
<tr><td>IDS_SDC_EXT.1.2</td><td>At a minimum, the TSF shall collect and record the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of the following table.

<table><tr><th>Event</th><th>Details</th></tr><tr><td>Network traffic</td><td>Protocol, source address, destination address</td></tr></table></td></tr>
</table>

Dependencies:	No dependencies
Notes:	None

5.3.3 IDS_ANL_EXT.1 Analyzer analysis and Packet Filtering

Hierarchical to:	No other components.
IDS_ANL_EXT.1.1	The TSF shall perform the following analysis function(s) on all IDS data received: a) **[*packet filtering, statistical, signature*]**; and b) **[no other function].**
IDS_ANL_EXT.1.2	The TSF shall record within each analytical result at least the following information: a) Date and time of the result, type of result, identification of data source; and b) **[data destination, protocol and severity].**
Dependencies:	IDS_SDC_EXT.1
Notes:	None

5.3.4 IDS_RCT_EXT.1 Analyzer reaction

Hierarchical to:	No other components.
IDS_RCT_EXT.1.1	The TSF shall send an alarm to **[the IDS data log and the notification contacts configured for the filter triggered by the network traffic]** and take **[assignment: the action configured for the filter triggered by the network traffic, which can be to:** • **Block the network traffic** • **Permit the network traffic** **]** when an intrusion is detected.
Dependencies:	IDS_ANL_EXT.1
Notes:	No dependencies

5.3.5 IDS_RDR_EXT.1 Restricted data review

Hierarchical to:	No other components.
IDS_RDR_EXT.1.1	The TSF shall provide **[authorised users and admin]** with the capability to read **[list of IDS data]** from the IDS data.
IDS_RDR_EXT.1.2	The TSF shall provide the IDS data in a manner suitable for the user to interpret the information.
IDS_RDR_EXT.1.3	The TSF shall ensure that **[metric for saving IDS data]** IDS data will be maintained when the following conditions occur: **[*IDS data storage exhaustion*]**.

Dependencies:	IDS_SDC_EXT.1, IDS_ANL_EXT.1
Notes:	None

5.3.6 IDS_STG_EXT.1 Guarantee of IDS data availability

Hierarchical to:	No other components.
IDS_STG_EXT.1.1	The TSF shall protect the stored IDS data from unauthorized deletion.
IDS_STG_EXT.1.2	The TSF shall protect the stored IDS data from modification.
IDS_STG_EXT.1.3	The TSF shall ensure that **[metric for saving IDS data]** IDS data will be maintained when the following conditions occur: **[*IDS data storage exhaustion*]**.
Dependencies:	IDS_SDC_EXT.1, IDS_ANL_EXT.1
Notes:	None

5.3.7 IDS_STG_EXT.2: Prevention of IDS data loss

Hierarchical to:	No other components.
IDS_STG_EXT.2.1	The TSF shall **[*overwrite the oldest stored IDS data*]** and send an alarm if the storage capacity has been reached.
Dependencies:	IDS_STG_EXT.1
Notes:	None

5.3.8 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit report of the following auditable events: c) Start-up and shutdown of the audit functions; d) All auditable events for the [***not specified***] level of audit; and e) [***Specifically defined auditable events listed in the Notes section below***].
FAU_GEN1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

Dependencies:	FPT.STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • Low severity security incidents • Medium severity security incidents • Critical severity security incidents

5.3.9 FAU_SAR.1 Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**Admin and Authorised User**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.3.10FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table 1 below**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	**Table 1 - Subject, Object and Operations for FDP_ACC.1**

Subject	Object	Operation
Admin / Authorised User	Configuration	Dashboard (View)
		Rule Management: • Rule Set (View / Edit / Delete) • Rule List (view, edit, delete)
		Threat Intelligence: • Threat Lists (view, edit, delete) • External Threat Lists (view, edit, delete)

			• Threat Intel Server (view, edit, delete)
			Data Logging: • Logging Control (view, edit, delete) • Log File management (view, rename, download, delete)
			Remote Monitoring (view, edit, delete)
			High Availability (view, edit, delete)
			Port Statistics (view)
			Admin (Settings): • Configuration (view, edit, delete) • User Management (view, edit, delete) • System Management (view, edit, delete)
		Monitoring	Dashboard (View)
			Traffic Patterns: • Overall (view) • DNS (view) • ICMP (view)
			Data Logging • Log File Management (view, download, rename, delete)
			Threat Lists (view)
			Threat Analytics: • Detected Threats (view, export) • IP Threats (view, export) • Domain Threats (view, export) • Rule Blocked Threats (view, export)

5.3.11FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Table 1**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**a) If the Admin is successfully authenticated accordingly, then access is granted based on privilege allocated;** **b) If the Admin is not authenticated successfully, therefore, access permission is denied**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.3.12FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password**]
Dependencies:	No dependencies.
Notes:	None.

5.3.13 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [***an admin configurable positive integer*** [**2 to 5**]] unsuccessful authentication attempts occur related to [**user entering their password for authentication to the TOE**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**block usage of the TOE**].

Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.3.14FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.15FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Notes:	None.

5.3.16 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [• **number of characters equal to or greater than 6 and less than or equal to 30** • **any combination of upper- and lower-case letters, numbers**]
Dependencies:	No dependencies.
Notes:	None.

5.3.17 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify, delete]*** the security attributes [**Admin Account, TOE Configuration, Users Account**] to [**Admin and Authorised User**].
Dependencies:	[FDP_ACC.1 Subset access control, or

	FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.18 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

5.3.19 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [***modify***] the [**User Accounts**] to [**Admin and Authorised User]**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.20 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***disable, enable and modify the behaviour of***] the functions [**TOE Configurations**] to [**Admin and Authorised User**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.21 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [
	• **Rule Management:**
	  ○ **Rule Set (view, edit, delete)**
	  ○ **Rule List (view, edit, delete)**
	• **Threat Intelligence:**
	  ○ **Threat Lists (view, edit, delete)**
	  ○ **External Threat Lists (view, edit, delete)**
	  ○ **Threat Intel Server (view, edit, delete)**
	• **Data Logging:**
	  ○ **Logging Control (view, edit, delete)**
	  ○ **Log File management (view, rename, download, delete)**
	• **Remote Monitoring (view, edit, delete)**
	• **High Availability (view, edit, delete)**
	• **Port Statistics (view)**
	• **Admin (Settings):**
	  ○ **Configuration (view, edit, delete)**
	  ○ **User Management (view, edit, delete)**
	• **System Management (view, edit, delete)**]

Dependencies:	No dependencies.
Notes:	None.

5.3.22 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Admin, Authorised User**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.23 FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] users **or IT Systems** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].
FTP_TRP.1.2	The TSF shall permit [***remote users***] to initiate communication via the trusted path
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial user authentication***, [**and all further communication after authentication**]].
Dependencies:	No dependencies
Notes:	None.

5.3.24 FPT_STM.1 Reliable Time Stamps

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Dependencies:	No dependencies
Notes:	None.

5.4 TOE Security Assurance Requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
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_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4.1 Explanation for Selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

5.5 Security Requirements Rationale

5.5.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
IDS_SDC_EXT.1	No dependencies	N/A
IDS_ANL_EXT.1	IDS_SDC_EXT.1	IDS_SDC_EXT.1
IDS_RCT_EXT.1	IDS_ANL_EXT.1	IDS_ANL_EXT.1
IDS_RDR_EXT.1	IDS_SDC_EXT.1, IDS_ANL_EXT.1	IDS_SDC_EXT.1, IDS_ANL_EXT.1
IDS_STG_EXT.1	IDS_SDC_EXT.1, IDS_ANL_EXT.1	IDS_SDC_EXT.1, IDS_ANL_EXT.1
IDS_STG_EXT.2	IDS_STG_EXT.1	IDS_STG_EXT.1
FAU_GEN.1	FPT.STM.1	FPT_STM.1
FAU_SAR.1	FAU.GEN.1	FAU.GEN.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	FIA_UID.1	FIA_UID.2
FIA_UAU.2	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1

SFR	Dependency	Inclusion
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_SMR.1 FMT_MSA.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTP_TRP.1	No dependencies	N/A
FPT_STM.1	No dependencies	N/A

5.5.2 Mapping of SFRs to Security Objectives for the TOE

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by: • FAU_GEN.1 which outlines what events must be audited • FIA_UID.2 ensures that users are identified to the TOE
O.AUDREC	This objective is completely satisfied by: • FAU_GEN.1 which outlines what events must be audited • FAU_SAR.1 which requires that the audit trail can be read • FPT_STM.1 ensures that reliable time stamps are provided for audit records
O.IDAUTH	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE • FIA_UID.2 which ensures that users are identified to the TOE • FMT_MTD.1 which restricts the ability to modify the user accounts to Admin

OBJECTIVE	RATIONALE
O.MEDIAT	This objective is completely satisfied by • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes such as Admin Account, TOE Configuration, Users Account to Admin. • FMT_MSA.3 which ensures that there are permissive default values for security attributes that are used to enforce the SFP. • FMT_MTD.1 which restricts the ability to modify the user accounts to Admin
O.SECFUN	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to disable, enable and modify the behaviour of the TOE Configurations are restricted to an Admin and Authorised User • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes such as Admin Account, TOE Configuration, Users Account to Admin. • FMT_MSA.3 which ensures that there are permissive default values for security attributes that are used to enforce the SFP. • FMT_MTD.1 which restricts the ability to modify the user accounts to Admin • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.SECSTA	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to disable, enable and modify the behaviour of the TOE Configurations are restricted to an Admin and Authorised User • FMT_MSA.1 which restricts the ability to change default, modify and delete the security attributes such as Admin Account, TOE Configuration, Users Account to Admin. • FMT_MSA.3 which ensures that there are permissive default values for security attributes that are used to enforce the SFP. • FMT_MTD.1 which restricts the ability to modify the user accounts to Admin
O.SINUSE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users

OBJECTIVE	RATIONALE
O.TOECOM	This objective is completely satisfied by • FTP_TRP.1 which ensures that traffic transmitted between TOE components (client and appliance) is protected from disclosure and modification
O.SENSOR	This objective is completely satisfied by: • IDS_SDC_EXT.1 which ensures that the network traffic (consist of date and time of the event, type of event, subject identity, the outcome (success or failure) of the event, protocol, source address and destination address) is collected and recorded
O.ANALYZER	This objective is completely satisfied by: • IDS_ANL_EXT.1 which performed packet filtering, statistical, signature analysis functions and recorded date and time of the result, type of result, identification of data source, data destination, protocol and severity within each analytical result
O.RESPONSE	This objective is completely satisfied by: • IDS_RCT_EXT.1 which ensures that specify the capability to respond to identified intrusion attempts by generating an alarm and taking action (Block or Permit) based on the configuration of the IDS filter that was triggered.
O.REVIEW	This objective is completely satisfied by: • IDS_RDR_EXT.1 which specifies the capabilities for authorized users to review the results generated by the TOE's analysis functions.
O.STORAGE	This objective is completely satisfied by: • IDS_STG_EXT.1 and IDS_STG_EXT.2 which specifies the TOE behaviour in the event the storage available for audit records and IDS data is exhausted and mechanisms for ensuring a specified amount of audit records and IDS data will still be available when this occurs.

6 TOE Summary Specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Intrusion Detection and Prevention
- Security Audit
- Identification and Authentication
- Security Management
- Secure Communication

6.2 Intrusion Detection and Prevention

The TOE collects and records network traffic and subjects it to statistical and signature-based analysis, depending on configured security filters (**IDS_SDC_EXT.1**). It also performed packet filtering, statistical, signature analysis functions and recorded date and time of the result, type of result, identification of data source, data destination, protocol and severity within each analytical result (**IDS_ANL_EXT.1**). If the analysis of collected network traffic indicates a potential intrusion attempt or the presence of malicious content in a packet, an action set associated with the detecting filter is triggered. It has the capability to respond to identified intrusion attempts by generating an alarm and taking action based on the configuration of the IDS filter that was triggered (**IDS_RCT_EXT.1**). The action set determines if the traffic is permitted or blocked. If traffic is permitted, an alert will be written to a TOE data log (specifically, the Event log). If traffic is blocked, an alert will also be written to the TOE Event log. Writing an alert to the TOE data log (specifically, the Event log) is always performed—in the evaluated configuration, action sets that block traffic always generate an alert. In addition to writing to the TOE data log files, the TOE can generate alerts in the form of a notification to a syslog server or through an email to an email address. The TOE provides capabilities for the admin and authorised users to review the TOE data logs (**IDS_RDR_EXT.1**). The TOE protects the TOE data logs from modification and deletion. When the space available for TOE data storage is exhausted, the oldest of the TOE log data files is deleted and an audit record to this effect is generated (**IDS_STG_EXT.1 and IDS_STG_EXT.2**)**.** The TOE can be configured to block or permit network traffic based on protocol, packet contents or IP address and port. Network traffic that is permitted based on traffic management filtering is still subject to IPS filtering, unless the traffic management filter is configured to allow traffic through the device without IPS filtering

6.3 Security Audit

The TOE generates a fine-grained set of audit log. These logs are stored locally, and the TOE can also send them to an external SYSLOG server for alternative storage. The TOE will generate audit logs (which contain the date and time of the event, type of event, subject identity and outcome of the transaction event) for the following auditable events (**FAU_GEN.1**):

- Low severity security incidents
- Medium severity security incidents
- Critical severity security incidents

The TOE's Admin and Authorized User have the capability to view and export these audit records via a web-based GUI interface (**FAU_SAR.1**). Timestamps are generated by TOE for audit logs. It is s generated from the clock provided in the TOE hardware (**FPT_STM.1**)

6.4 Identification and Authentication

The TOE maintains two types of user roles which are the roles Admin and Authorised User (**FMT_SMR.1**). Admin is a user that is allowed to perform configuration and monitoring application. Admin can modify the access control list and mapping of users (Authorised users) to roles either Monitoring or Configuration application (**FMT_MSA.1**). These users (Admin and Authorised User) able to interact with the TOE via a web-based GUI interface (connected to the Management Port). When a user issues a request to the TOE to access protected resources, the TOE requires that the user to identify and authenticate themselves before performing any TSF mediated action (**FIA_UAU.2, FIA_UID.2**). In order for the users to access the TOE, users have to enter the MGNT port IP address in the browser. At the login page, users need to key in a valid user name and password in order to access the TOE (**FIA_ATD.1**). The acceptable minimum password length is greater than or equal to 8 characters and combination of upper- and lower-case letters, numbers (**FIA_SOS.1**). The TOE has the ability to detect unsuccessful authentication attempts by the user (2 to 5 attempts depending on admin settings) and when the defined number of unsuccessful authentication attempts has been met, the TOE will block the usage of the TOE (**FIA_AFL.1**). The TOE checks the credentials presented by the user against the authentication information stored in the database and grant access if they are match.

6.5 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE. TOE provides a suite of management functions to Admin and Authorised User under the Configuration application privilege. These functions allow for the configuration of the TOE to suit the organization in which it is deployed. The following tasks are the management functions (**FMT_SMF.1, FMT_MSA.3, FMT_MTD.1, FMT_MOF.1**):

- Rule Management:

    - Rule Set (view, edit, delete)
    - Rule List (view, edit, delete)
- Threat Intelligence:
    - Threat Lists (view, edit, delete)
    - External Threat Lists (view, edit, delete)
    - Threat Intel Server (view, edit, delete)
- Data Logging:
    - Logging Control (view, edit, delete)
    - Log File management (view, rename, download, delete)
- Remote Monitoring (view, edit, delete)
- High Availability (view, edit, delete)
- Port Statistics (view)
- Admin (Settings):
    - Configuration (view, edit, delete)
    - User Management (view, edit, delete)
- System Management (view, edit, delete)

6.6 Secure Communication

The TOE provides trusted paths for communication with external IT entities that is logically distinct from other communication channels. These trusted paths protect transmitted data from disclosure and undetected modification. All remote communications take place over a secure encrypted session, either through an HTTPS (TLS v1.2) connection or over an SSH connection (**FTP_TRP.1**). The TOE initiates these trusted channels when:

- Users accessing the TOE via the web browser
- The TOE communicates with external Cyber Threat Intelligence and notification server.
- The TOE communicates with external remote monitoring server
- The TOE communicates with external syslog server