iDeras Security Target

Document Version: v1.3
Document Date:18 October 2013

Company
Infosys Gateway SdnBhd
Unit 808, 8th Floor, Block E,
PusatDaganganPhileo,
Damansara 1, No. 9, Jalan 16/11, Off JalanDamansara
46350 Petaling Jaya, Selangor.
MALAYSIA.

Document Revision History

Version	Date	Prepared By	Description
d1	03 Oct 2012	Infosys	Initial draft.
d2	09 January 2013	Infosys	Updating info based on EOR
d3	14 August 2013	Infosys	Updating info based on EOR
v1	06 September 2013	Infosys	Final
v1.1	06 September 2013	Infosys	Updated based upon Peer Review
v1.2	20 September 2013	Infosys	Updated based upon Peer Review
v1.3	18 October 2013	Infosys	Update based upon Peer Review and comments from MyCB

Table of Contents

1 Document Overview

This document is the Security Target (ST) for the iDeras Unified Threat Management (UTM). The ST is designed to meet the requirements of the CC ASE Class for EAL2, and provides a baseline for the subsequent phases of Target of Evaluation (TOE) evaluation works. This ST contains the following sections:

- *Security Target Introduction*: Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE;
- *Conformance Claims*: provides the ST claims of conformance to CC packages;
- *TOE Security Problem Definition*: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment;
- *Security Objectives*: Identifies the security objectives that are satisfied by the TOE and the TOE environment;
- *Security Requirements*: Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE; and
- *TOE Summary Specification*: Describes the security functions provided by the TOE to satisfy the security requirements and objectives; and
- *Rationale*: Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

2 Security Target Introduction

2.1 Security Target Reference

Security Target Title	:	iDeras Security Target
Security Target Version	:	v1.3
Security Target Date	:	18 October 2013

2.2 TOE Reference

TOE Name	:	iDeras Unified Threat Management (UTM)
Hardware Appliance version	:	ID-1208 (Type: 2U), ID-2016 (Type: 4U)
Software Version	:	5.02
TOE Initial	:	iDeras

2.3 Terminology and Acronyms

TOE	Target of Evaluation
TSF	TOE Security Functionality
CLI	Command Line Interface
LAN	Local Area Network
TLS	Transport Layer Security
SSH	Secure Shell
Webconfig	Web interface for TOE administration purpose
IP	Internet Protocol
NTP	Network Time Protocol
OSP	Organizational Security Policy

2.4 Reference

CCPart1 Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

CCPart2 Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

CCPart3 Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

CEM Common Methodology for Information Technology Security Evaluation (CEM): Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

2.5 TOE Overview

2.5.1 Usage and major security features of the TOE

The iDeras product is a Unified Threat Management (UTM) or hybrid solution consists of firewall packet filtering technology, offering server hosting services, network security with management features and gateway security management inside a single appliance. IDeras developed in Series of boxes comes in two models, which is ID-1208 (Type: 2U) and ID-2016 (Type: 4U), developed by Malaysian Local Company, Infosys Sdn Bhd. iDeras can be uses as hosting server, where iDeras pre-equipped with MySQL database feature, web server hosting and RAID support features. The network management features has the capabilities of recognizing hardware and software network configuration within the existing enterprise network, managing domains, directories, files, remote printing services and messaging (email hosting) services. The gateway features are to manage enterprise network traffic flow with supporting security features of Intrusion Detection/Prevention, Firewall packet filtering, Anti-Malware, Content-Filtration and many more.

However, for this evaluation, only parts of gateway function will be the TOE. Refer to Section TOE Description for more details.

The major security features of the TOE included in the evaluation are Identification and Authentication, User Data Protection, Security Audit, Security Management and Protection of the TSF.

2.5.2 TOE Type

The TOE is an application-level firewall that performed network packets filtering, network packets inspection, network load controls, and content filtering within network packets that are flows in the enterprise network traffics that travels in (incoming network packets) and out (outgoing network packets) of the organization’s internal networks. Application-level firewall with pre-equipped additional features as per described in TOE Overview, are known as Unified Threat Management (UTM).

2.5.3 Non-TOE hardware/software/firmware required by the TOE

The TOE comes with a hardware appliance and operating system that is required to run the TOE as following:

Table 1: Non-TOE Hardware and Software Specification

Model	Specification	Details
ID-2016	CPU Speed	Dual Intel Xeon E5645 2.4Ghx 6 Core
	Memory	32GB Triple-Channel DDR3 1333 MHz ECC
	Storage	5x3.5' removable HDD Trays Max capacity 8TB RAID 0,1,5 Support 1x8GB CompactFlash
	Interface	16x1 GbE Ports (Copper) 2x1 GbE Ports (Fiber) 2xUSB 2.0 ports
	Power supply	500W/each redundant power supply
	Form Factor	2U Rack mount
	Operating System	CentOS5
	Appliance Type:	4U
ID-1208	CPU Speed	2.0GHz~3GHz, Intel i3 ~i7, 2~8 Core
	Memory	Dual Channel DDR3 (2GB~16GB) 8GB Compact Flash For OS Restore & Redundancy
	Storage	Standard: Dual 500GB ~ 2TB SATA Raid: 250GB ~ 1TB Mirrored
	Interface	6x1 GbE Ports (Copper) 2xUSB 2.0 ports
	Power supply	~90W
	Form Factor	1U Rack mount
	Operating System	CentOS5
	Appliance Type:	2U

2.6 TOE Description

2.6.1 Physical Scope of TOE

The TOE is installed inside the model hardware appliances as stated below, is consists of the following components:

- ID-1208 (Type: 2U) and ID-2016 (Type: 4U): Hardware appliance includes the physical port connections on the outside of the appliance rack. Refer Table 1 for more details. Refer Figure 1 and Figure 2 for the physical presentation of hardware appliance.
- CentOS5
- iDERAS User Guide

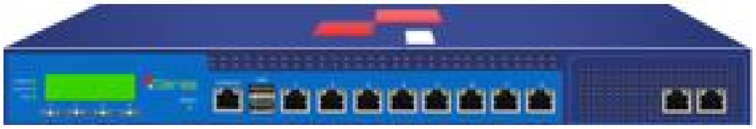

Figure 1: ID-1208 Model

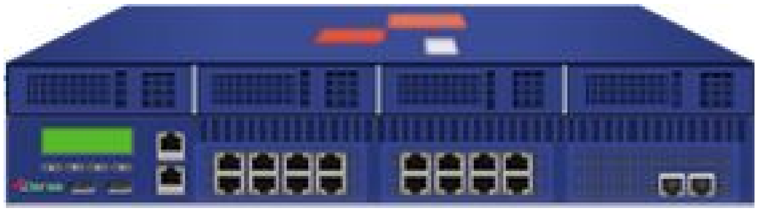

Figure 2: ID-2016 Model

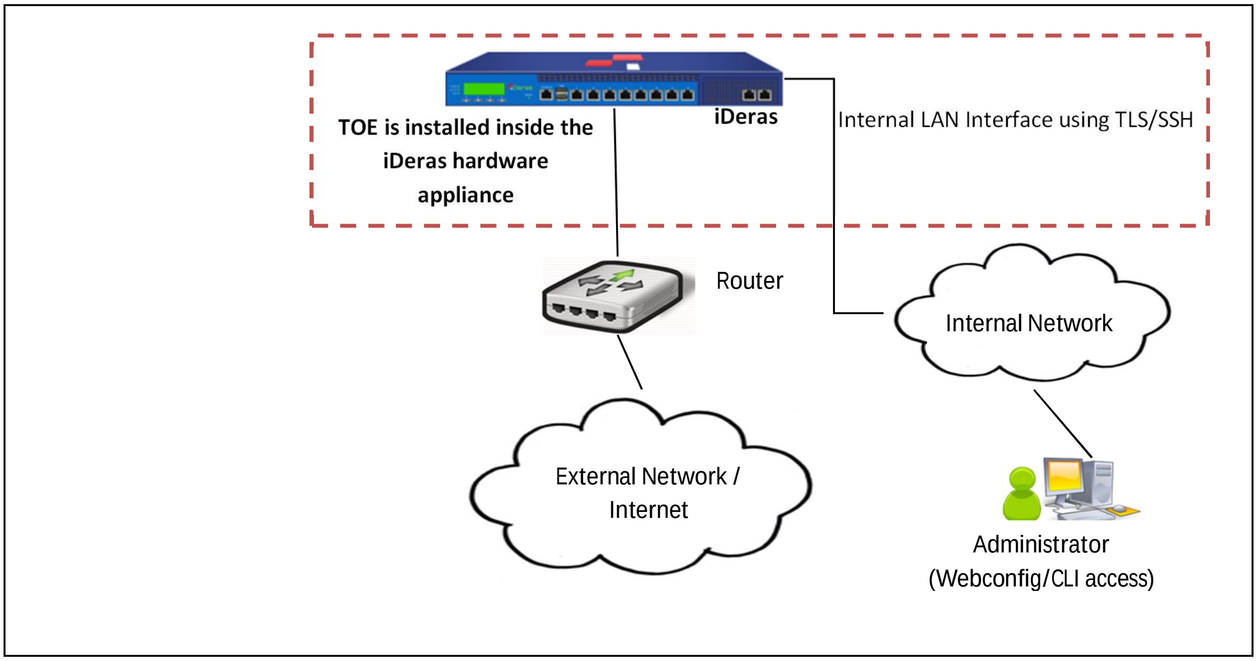
TOE is installed inside the iDeras hardware appliance
iDeras
Internal LAN Interface using TLS/SSH
Router
Internal Network
External Network / Internet
Administrator (Webconfig/CLI access)

Figure 3: Typical TOE deployment

All hardware appliance and operating system are not part of the scope of evaluation.

The TOE is deployed with objectives of providing network perimeter security, in which controls of data/information transfer between two networks, one considered to be “external” to the assets that are to be protected by the TOE and the second considered to be “internal”. The TOE must be placed in a secure physical area where only authorized administrators are granted physical access to the TOE.

External interface are consider to external network to the LAN network (Internal), normally known as Internet Gateway provided through ISP (Internet Service Provider) network router configurations.

Whereas for Internal Network are known as Local Area Network (LAN) that shall be segregated based on organization security policies enforced and implemented by TOE Administrator, authorized to applied to the TOE, accordingly.

TOE administrator could administer TOE through 2 interfaces. Refer following Figure 3 for illustration of typical TOE deployment:

a) Console Interface – Access through Command Line Interface (CLI) over SSH using RJ-45 cable.

b) Internal LAN Interface –Access through Web Interface (Webconfig) over TLS/HTTPS in an internal network located in the same physical secure location.

2.6.2 Logical Scope of TOE

The logical scope of TOE is described based on several security functional requirements.

2.6.2.1 Identification and Authentication

TOE administrator can access TOE by providing username and password in the Webconfig interface and CLI interface. By default, administrator can use a built-in administrative account known as “admin” used for authenticating through Webconfig. TOE Administrator will be granted role based on built-in Groups, access to services (UTM/Firewall) and pages within Webconfig. Password for each administrator account is governed by password policy. TOE Administrator are able to modify the existing configurable settings as per required by the organizational security policies implemented/enforced. However, several built-in features could not be modified by TOE Administrator. For more details, refer to Section TOE Summary Specification and Guidance Documentation.

2.6.2.2 User Data Protection

TOE has the capabilities of protecting the internal network (organization network, enterprise network or etc) from external network intrusions using information flow controls between internal and external network. The TOE will check the inbound and outbound IP network protocols, contents and ports; before allowing or rejecting the IP network and packets. TOE Administrator can configure packet filter rules and policies based on the subject and information security attributes. By default, all external (Internet) traffic will be blocked. TOE Administrator can configure any services, ports and protocols that are accessible between Internet and Internal networks. For more details, refer to Section TOE Summary Specification and Guidance Documentation.

2.6.2.3 Security Management

TOE features can be managed through Webconfig and CLI by TOE Administrator. User of TOE, whom are assigned with TOE Administrator roles is configurable using built-in feature by assigning to administrator account “admin”. TOE Administrator could enable, disable and modify the behaviour of services controlled by TOE, packet filtering rules, user attribute values, network settings, time-of-day web access, NTP Time Server, backup and restore configurations setting, restart and shutdown functions, password policies and related functions of TOE. For more details, refer to Section TOE Summary Specification and Guidance Documentation.

2.6.2.4 Security Audit

The TOE will generate audit records for selected security events in several log files and categories. Each audited event will be recorded along with date and time of event, account user who performed the event, event name, system filename related to event and other event details. Audit records can be viewed by TOE Administrator and cannot be edited. TOE Administrator could select and filter the logs for easy viewing. TOE will create a new log file to store the audit records if the size limit is reached for a single log file. Limitation of the log storage is based on the internal hard disk equipped within the TOE appliance. Kindly refer to Section 2.5.3 on the information about TOE storage capacity. For more details, refer to Section TOE Summary Specification and Guidance Documentation.

2.6.2.5 Protection of the TSF

The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. TOE prevents modification of date and time manually. For more details, refer to Section TOE Summary Specification.

2.6.3 Product features not included in scope

Product features that are not part of the evaluation scope as following:

- Domain &LDAP and its related functionalities
- SSL Certificates, encryption and digital signatures
- Multi-WAN
- DHCP Server
- Local DNS Server
- OpenVPN
- PPTP Server
- Proxy Server
- IPsec VPN
- OpenVPN
- PPTP VPN
- Antimalware
- Bandwidth and QoS
- Intrusion Protection
- Content Filter
- Web Proxy
- Windows Networking including Windows domain group and user
- File and Print
- Mail
- Mail Scanning
- Web Server
- Database
- Language
- Mail Notification
- Disk Usage
- Processes
- Certificate Manager
- Reports (excepts Logs)

3 Conformance Claims

The following conformance claims are made for the TOE and ST:

CCv3.1 conformant The ST and the TOE are Common Criteria conformant to Common Criteria version 3.1 Revision 4.

Part 2 conformant The ST is Common Criteria Part 2 extended

Part 3 conformant The ST is Common Criteria Part 3 conformant

Package conformant The ST is package conformant to the package Evaluation Assurance Level EAL2.

Protection Profile conformance None

4 TOE Security Problem Definition

4.1 Assumption

The assumptions are made to ensure the security of the TOE and its deployed environment.

Table 2: Assumptions

A.PHY	The TOE and its environment are physically secure and managed by authorized TOE Administrator.
A.FLOW	Data and information could not flows through between internal and external networks and vice versa, unless it passes through the TOE.
A.ADMIN	Authorized TOE Administrators is non-hostile and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
A.TIMEBACK	The TOE environment will provide reliable time stamps and backup storage enough for TOE supporting operational environments.
A.MGMT	The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that secure and trusted connections can be established to the management network (i.e. through a trusted VPN or trusted Virtual LAN).
A.CONN	Authorized TOE Administrators will access the TOE using a secure connection.
A.USER	Unauthorized user who is not authorized TOE Administrators cannot access the TOE remotely from the internal or external networks or trusted networks.

4.2 Threats

Assets that are protected by the TOE are sensitive data, stored in the TOE and internal network including critical TOE configuration data (configuration files, packet filtering rule-base and others), audit records, administrator credentials, TOE data and TOE security functions.

Threat agents are entities that can adversely act on the assets. The threat agents identified are an unauthorized person and an authorized administrator (a person that has been successfully authenticated and authorized as an administrator).

Threats may be addressed either by the TOE or by its intended environment.

Table 3: Threats

T.ACCESSLOG	An unauthorized person successfully accesses the TOE data or security functions without being detected.
T.AUDIT	An unauthorized person or authorized administrator may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.

T.EXPLOIT	An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.
T.REMOTE	An unauthorized person or unauthorized external IT entities may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized TOE Administrator desktop and the TOE.
T.CONFIG	An unauthorized person may read, modify, or destroy TOE configuration data.
T.NOAUTH	An unauthorized person may attempt to bypass the TOE access controls, in accordance to modify current existing security configurations, provided by the TOE.
T.SPOOF	An unauthorized person may carry out network spoofing activities, in which, information flows through the TOE into a connected network by using a spoofed source address.

4.3 Organizational Security Policies

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

Table 4: Organizational Security Policy

P.ROLE	Only authorized individuals are assigned by the organization have access to the TOE.
P.PASSWORD	Authorized TOE Administrator shall use/create password with combination of special character, number and alphabet with minimum lengths of 12in mitigating password guessing activities.

5 Security Objectives

Security objectives are formed to address the security problem definition defined in earlier section. The security implementation in TOE and its environment will meet these objectives.

5.1 Security Objectives for the TOE

The security objectives for the TOE as following:

Table 5: Security Objectives for the TOE

O.ACCESSLOG	TOE shall record a readable log of security events.
O.AUDIT	TOE shall prevent an unauthorized person or authorized TOE Administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.EXPLOIT	TOE shall mediate the information flow in internal network and between internal and external network.
O.CONFIG	TOE shall prevent unauthorized person to access TOE functions and configuration data. Only authorized TOE Administrator shall have access to TOE management interface.
O.NOAUTH	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.

5.2 Security Objectives for the Operational Environment

The security objectives for the TOE operational environment as following:

Table 6: Security Objectives for the Operational Environment

OE.PHY	The TOE and its environment shall be physically secure.
OE.FLOW	The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
OE.ADMIN	Authorized TOE Administrators shall be non-hostile and follow guidance; however, TOE Administrators is not free from human error or mistakes.
OE.TIMEBACK	The TOE environment shall provide reliable time stamps and backup storage.
OE.MGMT	The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, enforced with HTTPS).

OE.CONN	Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.
OE.USER	Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.

6 Extended Components

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) applicable for the TOE. These requirements are presented following the conventions identified in Section 9.1 Conventions.

6.1 Extended Security Functional Requirement (SFR)

Table 7: Extended SFR Component

Extended Component	Extended Component Name	Rationale
Class FAU : Security Audit		
FAU_GEN.3	Simplified Audit Data Generation	FAU class contains families of functional requirements that are related to monitor security-relevant events, and act as a deterrent against security violations. This component is a member of FAU_GEN, an existing CC Part 2 family. This extended requirement for the FAU class has been included in this ST because TSF audit function does not log start and stop of auditing function; hence FAU_GEN.1.1 (a) is not applicable. This component is also created to simplify the requirement of FAU_GEN.1.
Class FPT : Protection of the TSF		
FPT_STM.2	Reliable time stamps by operational environment	FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. This component is a member of FPT_STM, an existing CC Part 2 family. This extended requirement for the FPT class has been included in this ST because the operational environment is providing reliable time stamps for TSF functions that is not covered in FPT_STM.1 .

6.1.1 Class FAU: Security Audit

FAU_GEN.3 Simplified Audit Data Generation

Hierarchical No other component

Dependencies FPT_STM.2 Reliable time stamps by operational environment

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:

[**assignment: defined auditable events**].

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event

b) [**assignment: other information about the event**].

6.1.2 Class FPT: Protection of the TSF

FPT_STM.2 Reliable time stamps by operational environment

Hierarchical No other component

Dependencies No other dependencies

FPT_STM.2.1 The operational environment shall be able to provide reliable time stamps for the TSF functions.

6.2 Extended Security Assurance Requirement (SAR)

There are no extended SAR components defined for this evaluation.

7 TOE Security Functional Requirements

This section provides the security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

7.1 Conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to the statement of security functional requirements. Following are the operations and the document conventions as 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 an acronym at the end of the component identifier as follows: FCS_COP.1 (SWP).

7.2 Security Functional Requirements

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Table 8: Security Functional Requirements

Component	Component Name
Class FAU : Security Audit	
FAU_GEN.3	Simplified Audit Data Generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
Class FDP : User Data Protection	
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes
Class FIA : Identification and Authentication	
FIA_ATD.1	User attributes definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_SOS.1	Verification of secrets
Class FMT : Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation

Class FPT : Protection of the TSF	
FPT_STM.2	Reliable time stamps by operational environment

7.2.1 Class FAU: Security Audit

FAU_GEN.3Simplified Audit Data Generation

Hierarchical No other components.

Dependencies FPT_STM.2 Reliable time stamps by operational environment

FAU_GEN.3.1 The TSF shall be able to generate an audit record of the following auditable events:[

a) **Successful/failure authentication to iDeras web portal;**

b) **Web portal page accessed by user;**

c) **Reset user password**]

FAU_GEN.3.2 The TSF shall record within each audit record at least the following information:

a)Date and time of the event;

b)[Username;

c) Event;

d) Filename;

e) Event details]

Application notes None

FAU_SAR.1 Audit review

Hierarchical No other components.

Dependencies FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**administrator**] with the capability to read [**all audit trail data**] 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.

Application notes None

FAU_SAR.3 Selectable audit review

Hierarchical No other components.

Dependencies FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**select log file and/or filter**] of audit data based on [

a) **log file related to event**

b) **filter log using any key words inserted in filter field**]

Application notes None

FAU_STG.1 Protected audit trail storage

Hierarchical No other components.

Dependencies FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

Application notes None

FAU_STG.4Prevention of audit data loss

Hierarchical FAU_STG.3 Action in case of possible audit data loss

Dependencies FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [**create a new log file to store the audit records if the size limit is reached for a log file**] if the audit trail is full.

Application notes None

7.2.2 Class FDP: User Data Protection

FDP_IFC.1 Subset Information Flow Control

Hierarchical	No other components.
Dependencies	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1	The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] on **[a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;** **b) information: traffic sent through the TOE from one subject to another;** **c) operation: allow/reject information].**
Application notes	None

FDP_IFF.1 Simple Security Attributes

Hierarchical No other components.

Dependencies FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] based on the following types of subject and information security attributes: [

a) subject security attributes:

- **Presumed address**

b) information security attributes:

- **Presumed address of source subject;**
- **Presumed address of destination subject;**
- **Presumed port of source subject;**
- **Presumed port of destination subject;**
- **TOE interface on which traffic arrives and departs;**
- **Transport layer protocol information;**
- **Service**].

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: [

a**) Subject on an internal network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the administrator;**
- **the presumed address of the source subject, in the information, translates to an internal network address; and**
- **the presumed address of the destination subject, in the information, translates to an address on the other connected network.**

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- **all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the administrator;**
- **the presumed address of the source subject, in the information, translates to an external network address; and**
- **the presumed address of the destination subject, in the information, translates to an address on the other connected network**].

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

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

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

a) Reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) Reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) Reject requests for access of services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) Reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;

e) **Reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and**

f) **For application protocols supported by the TOE (e.g., DNS24, HTTP25, SMTP26, and POP327), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC28). This shall be accomplished through protocol filtering that are designed for that purpose**].

Application notes None

7.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 Subset Information Flow Control

Hierarchical No other components.

Dependencies No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) **Username**

b) **Password**

c) **Role based on Built-in Groups**

d) **Services**

e) **Access page**].

Application notes None

FIA_UAU.2 User authentication before any action

Hierarchical FIA_UAU.1 Timing of authentication

Dependencies FIA_UID.1 Timing of identification

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.

Application notes None

FIA_UID.2 User identification before any action

Hierarchical FIA_UID.1 Timing of identification

Dependencies No dependencies.

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.

Application notes None

FIA_SOS.1 Verification of secrets

Hierarchical No other components.

Dependencies No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

a) **Minimum Password length configurable value**

b) **Minimum Password age configurable value**

c) **Maximum Password age configurable value**

d) **Password history size configurable value**

e) **Starts with a letter or number**

f) **Must not contain characters |** ;].

Application notes (a) until (c) value are configurable by administrator. (d) and (e) value are build-in value and not configurable by administrator.

7.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical No other components.

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [***enable, disable, modify the behaviour of***] the functions [

a) **start-up and shutdown services in System.Resources.Services Module;**

b) **create, delete, modify, and view information flow security policy rules that permit or deny information flows in Network.Firewall Module;**

c) **create, delete, modify and view user attribute values defined in FIA_ATD.1 in Directory.Accounts.User Module, Directory.Accounts.Group Module, System.Settings.Administrators**

Module and System.Resources.Services Module;

d) create, delete, modify, and view network settings in Network.Settings Module;

e) Modify the protocol filter to block unwanted traffic in Gateway.Protocol_Filter.Protocol_Configuration Module;

f) enable and disable the NTP Time Server inSystem.Settings.Date Module;

g) backup and restore configuration settings manually in System.Backup.Backup_Settings Module;

h) restart and shutdown manually TOE in System.Settings.Shutdown-Restart Module;

i) Configure password policies in Directory.Setup.Password_Policies Module.

] to [**administrator**].

Application Note None

FMT_MTD.1 Management of TSF data

Hierarchical No other components.

Dependencies FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [***change_default, modify, delete,***[**and add**]] the [**user attributes defined in FIA_ATD.1.1**] to [**administrator**].

Application Note None

FMT_SMF.1 Specification of Management Functions

Hierarchical No other components.

Dependencies No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**functions as in FMT_MOF.1.1**].

Application Note None

FMT_SMR.1 Security roles

Hierarchical No other components.

Dependencies No dependencies.

FMT_SMR.1.1 The TSF shall maintain the roles [**administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note By default, administrator account that is newly created will have limited access to the TOE. It is up to the default administrator account (username: admin) to give access to specific pages in the web-based administration portal and access to core applications on TOE. By default, administrator account can only access page to change their password and download security certificates (not part of scope).

FMT_MSA.1 Management of security attributes

Hierarchical No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] to restrict the ability to [***change_default, modify, delete,***[**and add**]] the security attributes [**as in FDP_IFF.1.1**] to [**administrator**].

Application Note None

FMT_MSA.3 Static attribute initialisation

Hierarchical No other components.

Dependencies FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

Application Note By default, all external (Internet) traffic will be block. Administrator can configure any services and ports that can be accessible from the Internet.

7.2.5 Class FPT: Protection of the TSF

FPT_STM.2 Reliable time stamps by operational environment

Hierarchical No other components.

Dependencies No other dependencies

FPT_STM.2.1 The operational environment shall be able to provide reliable time stamps for the TSF functions.

Application Note Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.3 and FMT_SAE.1 security functions. The TOE does not have a feature to generate time stamps independently. The date and time stamp is provided by NTP server.

7.3 Security Assurance Requirements

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

Table 9: Security Assurance Requirements for EAL2

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_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	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_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

8 TOE Summary Specifications

TOE addressed the security functional requirements as following:

8.1 Identification and Authentication

TOE administrator can access and manage the TOE by providing username and password in the Webconfig login interface and CLI interface. By default, administrator can use a default built-in administrative account "admin" with password "admin" to be authenticated to Webconfig for first time. Administrator can modify the default password to a strong password according to P.PASSWORD.

TOE Administrator will be granted role based on Built-in Groups, access to services and pages in Webconfig. There are 3 built-in groups: *allusers, domain_admins and domain_users*. Following are group definition:

- *allusers* – Containing all users in TOE
- *domain_admins* – Windows domain administrators
- *domain_users* – Windows domain users

By default, TOE Administrator will be in group *allusers.domain_admins and domain_users* groups are not part of the scope.

By default, account "admin" has access to all services except Windows Networking. However, Windows Networking service can be enabled by administrator after successfully login to Webconfig. A new account created by TOE Administrator will have limited access to Webconfig pages and services. By default, a new account can only access account User Profile page to modify password and profiles. A new account user can also download security certificates in Security and Keys page (not in scope). A new account user can obtained administrator role if configured to access administrative page in Webconfig.

Password for each TOE Administrator account is governed by a password policy. The policies that are configurable by administrator are:

- Minimum Password Length
- Minimum Password Age
- Maximum Password Age
- History Size

Password must also starts with a letter or number and must not contain characters **|;** which are build-in values that are not configurable by TOE Administrator.

TOE Security Functional Requirements Satisfied
FIA_ATD.1
FIA_UAU.2
FIA_UID.2
FIA_SOS.1

8.2 User Data Protection

TOE protects the internal network (organization network) from external network intrusions by using information flow control between internal and external network. The TOE will check the inbound and outbound IP packets from unauthenticated external IT entities before allowing or rejecting the network traffic in forms of IP packets. The decision to allow or reject/drop traffic will be based on packet filter rules created by administrator.

Administrator could configure packet filter rules and policies based on the subject and information security attributes or criteria. The criteria are as following:

- Source address of information (i.e IP address, MAC address)
- Destination address of information (i.e IP address, MAC address)
- Source port of information
- Destination port of information
- Interface that the traffic arrives and departs
- Transport layer protocol information
- Service used by information

By default, all external (Internet) traffic will be blocked. TOE Administrator can configure any services, protocols and ports that can be accessible from the Internet. Pre-configured network traffic protocol listings are made available in TOE. TOE Administrator can block any unwanted network traffic using the ready-made protocol listings.

TOE Security Functional Requirements Satisfied
FDP_IFC.1
FDP_IFF.1

8.3 Security Management

TOE functions can be managed through Webconfig and CLI by TOE Administrator. User of TOE has administrator roles, which can be configured by built-in administrator account “admin”.

By default, administrator account that is newly created will have limited access to the TOE. It is up to the default administrator account (username: admin) to give access to specific pages in Webconfig and access to core applications on TOE. By default, administrator account can only access page to change their password and download security certificates (not part of scope).

Administrator could enable, disable or modify the management functionalities of TOE as following:

- start-up and shutdown services in System.Resources.Services Module;
- create, delete, modify, and view information flow security policy rules that permit or deny information flows in Network.Firewall Module;
- create, delete, modify and view user attribute values defined in FIA_ATD.1 in Directory.Accounts.User Module, Directory.Accounts.Group Module, System.Settings.Administrators Module and System.Resources.Services Module;

- create, delete, modify, and view network settings in Network.Settings Module;
- Modify the protocol filter to block unwanted traffic in Gateway.Protocol_Filter.Protocol_Configuration Module;
- enable and disable the NTP Time Server in System.Settings.Date Module;
- backup and restore configuration settings manually in System.Backup.Backup_Settings Module;
- restart and shutdown manually TOE in System.Settings.Shutdown-Restart Module;
- Configure password policies in Directory.Setup.Password_Policies Module.

By default, all external (Internet) traffic will be blocked. TOE Administrator can configure any services, protocols and ports that can be accessible from the Internet. Pre-configured network traffic protocol listings are made available in TOE. TOE Administrator can block any unwanted network traffic using the ready-made protocol listings.

TOE Security Functional Requirements Satisfied
FMT_MOF.1
FMT_MTD.1
FMT_SMF.1
FMT_SMR.1
FMT_MSA.1
FMT_MSA.3

8.4 Security Audit

The TOE will generate audit records for selected security events in several log files. The security events that will be audited are as following:

- Successful/failure authentication to iDeras web portal
- Web portal page accessed by user
- Reset user password

Each audited events will be recorded along with date and time of event, account user who performed the event, event name, system filename related to event and other event details. Audit records can be viewed by administrator and cannot be modified.

Administrator could read all audit trail data. Administrator could select and filter the logs for suitable interpretation. Administrator needs to select a log file related to the event and/or filter the content of the log. Log filtering is executed by inserting the related key words in the filter field to search the log records in log file.

TOE will create a new log file to store the audit records if the size limit is reached for a log file.

TOE Security Functional Requirements Satisfied
FAU_GEN.3
FAU_SAR.1
FAU_SAR.3
FAU_STG.4
FAU_STG.1

8.5 Protection of the TSF

The security audit functions will generate audit records of events along with date and time of event. To ensure a reliable date and time, TOE enforce the time stamps to be taken from a reliable source from the environment. NTP server is used as a reliable source of environment. However, NTP server itself is not part of the scope. TOE prevents manual modification of date and time to preserve integrity of date and time from NTP server.

TOE Security Functional Requirements Satisfied
FPT_STM.2

9 Rationale

9.1 Protection Profile Conformance Claim Rationale

ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

9.2 Security Objectives Rationale

This section explains how threat, assumptions and OSP are related to each other. The following tables show threat, assumptions and organizational policy being mapped to security objectives.

9.2.1 Rationale for Security Objectives Mapped to Threats

Table 10: Rationale Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.ACCESSLOG An unauthorized person successfully accesses the TOE data or security functions without being detected.	**O.ACCESSLOG** TOE shall record a readable log of security events.	This security objectives counter threat because any success or failure of authentication events will be recorded in a readable log of security events. Each security events will be logged along with the username presented by unauthorized person.
T.AUDIT An unauthorized person or authorized administrator may intentionally or unintentionally delete audit records to destroy evidence of adverse events executed.	**O.AUDIT** TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	This security objective counter threat because it will prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The objective also ensures the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
T.EXPLOIT An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.	**O.EXPLOIT** TOE shall mediate the information flow in internal network and between internal and external network.	This security objective counters threat because TOE will mediate the information flow in internal network and between internal and external network to decide whether to allow or drop information send by unauthorized person.
T.REMOTE An unauthorized person or	**OE.MGMT** The TOE shall be managed from	This security objective counters threat because the deployment environment will secure the

unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).	remote connection by administrator when remotely access the TOE. It also specifies that the TOE will be deployed in a separate network from the internal and external networks.
	OE.CONN Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent eavesdropping.	This security objective counters threat because the environment will provide a secure and encrypted connection to prevent unauthorized person or external IT entity sniff the data and modify it.
T.CONFIG An unauthorized person may read, modify, or destroy security critical TOE configuration data.	**O.CONFIG** TOE shall prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.	This security objective counters threat because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.
T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non-security functions provided by the TOE.	**O.NOAUTH** The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective counters threat because security events are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. The audit records cannot be modified by administrator to preserve its integrity. It will also not be overwritten in the case of audit trail is full.
T.SPOOF An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.	**O.EXPLOIT** TOE shall mediate the information flow in internal network and between internal and external network.	This security objective counters threat because TOE will mediate the information flow in internal network and between internal and external network to decide whether to allow or drop information send by unauthorized person.

9.2.2 Rationale Security Objectives Mapped to OSP Rationale

Table 11: Rationale Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE Only authorized persons assigned by the organization have access to the TOE.	**OE.USER** Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	This security objective counters OSP because unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.
	O.CONFIG TOE shall prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.	This security objective counters OSP because TOE will prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.
P.PASSWORD Authorized administrator shall use password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective counters OSP because authorized administrator shall be non-hostile and follow guidance on creating a good password.
	O.NOAUTH The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	This security objective counters threat through functions of TOE that is able to enforce password protection based upon the implementation of organizational security policy, through the usage of password with combination of special character, number and alphabet with minimum lengths of 12 to make it hard to guess; whilst protecting the TOE from the attempt of unauthorized users to bypass, deactivate, or tamper with TOE security functionality.

9.2.3 Rationale Security Objectives Mapped to Assumptions

Table 12: Rationale Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY The TOE and its environment are physically secure.	**OE.PHY** The TOE and its environment shall be physically secure.	This security objective counters assumption because the TOE and its environment shall be physically secure.
A.FLOW Information cannot flow through internal and external networks unless it passes through the TOE.	**OE.FLOW** The TOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.	This security objective counters assumption becauseTOE shall be deployed so that information cannot flow through internal and external networks unless it passes through the TOE.
A.ADMIN Authorized administrators are non-hostile and follow guidance; however, they are not free from error.	**OE.ADMIN** Authorized administrators shall be non-hostile and follow guidance; however, they are not free from error.	This security objective counters assumption becauseauthorized administrators shall be non-hostile and follow guidance; however, they are not free from error.
A.TIMEBACK The TOE environment will provide reliable time stamps and backup space.	**OE.TIMEBACK** The TOE environment shall provide reliable time stamps and backup space.	This security objective counters assumption becauseTOE environment shall provide reliable time stamps and backup space.
A.MGMT The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN).	**OE.MGMT** The TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).	This security objective counters assumption because TOE shall be managed from a network that is physically separated from the internal and external networks. Remote management of the TOE is only permitted in the event that a secure and trusted connection can be established to the management network (i.e. through a trusted VPN, HTTPS).
A.CONN Authorized administrators will access the TOE using a secure connection.	**OE.CONN** Authorized administrators shall access the TOE using a secure connection provided by the environment to prevent	This security objective counters assumption because authorized administrators shall access the TOE using a secure connection provided by the environment to

	eavesdropping.	prevent eavesdropping.
A.USER Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	**OE.USER** Unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.	This security objective counters assumption because unauthorized user who is not authorized administrators cannot access the TOE remotely from the internal or external networks.

9.3 Extended Security Functional Requirement Rationale

Refer Section Extended Security Functional Requirement (SFR) for the rationale.

9.4 Extended Security Assurance Requirement Rationale

Not applicable since there is no extended Security Assurance Requirement declared in ST.

9.5 Security Functional Requirements Rationale

This section provides the rationale of using SFRs to meet the security objectives for the TOE and justify the SFRs dependencies that have been satisfied or not satisfied.

9.5.1 Rationale for SFR Mapped to Security Objectives for TOE

Table 13: Rationale for SFR Mapped to Security Objectives for TOE

Security Objectives	SFRs	Rationale
O.ACCESSLOG TOE shall record a readable log of security events.	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_SAR.1	This SFR specify that administrator will have the capability to view the audit trail data in log form. It traces back to this objective.
	FAU_SAR.3	This SFR specify that administrator will have the ability to select log file related to the security event. Administrator is able to filter the log for a better view. It traces back to this objective.
O.AUDIT TOE shall prevent an unauthorized person or authorized administrator to modify or deletes audit records of security events executed. The TOE shall ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by administrator or unauthorized person. It traces back to this objective.
	FAU_STG.4	This SFR specify that if the log file reach the size limit, TOE will create a new log file to ensure that the integrity of audit records are preserved. Audit records will not be overwritten. It traces back to this objective.
	FPT_STM.2	This SFR specify that the environment (NTP server) will provide a reliable time stamps for TOE, thus preserving the integrity of the security event date and time that is being audited. It traces back to this objective.
O.EXPLOIT TOE shall mediate the information flow in internal network and between internal and external	FDP_IFC.1	This SFR identify the external IT entities in the Unauthenticated Information Flow Control SFP that send information to other entity. The SFP will either reject or allow the information flow. It traces back to this objective.

network.	FDP_IFF.1	This SFR identify the external IT entity and its security attributes as part of the information flow control SFP. TOE will permit or deny the information flow based on network packet rules configured by administrator. It traces back to this objective.
O.CONFIG TOE shall prevent unauthorized person to access TOE functions and configuration data. Only TOE authorized administrator shall have access to TOE management interface.	FIA_ATD.1	This SFR provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_SOS.1	This SFR enforce a password policy in order to ensure that all account passwords are hard to guess. Therefore, unauthorized person will require longer duration and higher processing speed to guess/brute force the password in order to be authenticated. It traces back to this objective.
	FMT_MOF.1	This SFR restrict the ability to enable, disable and modify TOE functions to administrator. It traces back to this objective.
	FMT_MTD.1	This SFR restrict the ability to change default value, modify, delete and add user attributes in FIA_ATD.1.1 to administrator. It traces back to this objective.
	FMT_SMF.1	This SFR identify management functions that are available in TOE as in FMT_MOF.1.1, that are managed by administrator. It traces back to this objective.

	FMT_SMR.1	This SFR identify the roles exist in TOE, which is administrator. Each user account created must be associated to administrator role that have access to TOE management interface. It traces back to this objective.
	FMT_MSA.1	This SFR restrict the ability to change default value, modify, delete and add subject and information security attributes in packet filter rules, as in FDP_IFF.1.1 to administrator. It traces back to this objective.
	FMT_MSA.3	This SFR enforce a restrictive packet filter rules by default (during the initial start of TOE). Administrator will have access to management interface to modify the default value in packet filter rules. It traces back to this objective.
O.NOAUTH The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functionality.	FAU_GEN.3	This SFR specify security events that are being audited and recorded in log file. Each security event will be recorded along with date and time of event, user who execute the event, filename and other event details. It traces back to this objective.
	FAU_STG.1	This SFR specify that audit records cannot be modified or deleted by administrator or unauthorized person. It traces back to this objective.
	FAU_STG.4	This SFR specify that if the log file reach the size limit, TOE will create a new log file to ensure that the integrity of audit records are preserved. Audit records will not be overwritten. It traces back to this objective.
	FIA_UAU.2	This SFR require each person to be successfully authenticated before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.
	FIA_UID.2	This SFR require each person to be successfully identified before being allowed to perform any actions on TOE functions and configuration data at the TOE management interface. It traces back to this objective.

9.5.2 SFR Dependency Rationale

The following table provides a demonstration that all SFRs dependencies included in the ST have been satisfied.

Table 14: SFR Dependencies

SFR	Dependency	Dependency Met?	Justification
FAU_GEN.3	FPT_STM.2	Yes	-
FAU_SAR.1	FAU_GEN.1	No	Met with FAU_GEN.3. Refer Section 8.1 for more details.
FAU_SAR.3	FAU_SAR.1	Yes	-
FAU_STG.1	FAU_GEN.1	No	Met with FAU_GEN.3. Refer Section 8.1 for more details.
FAU_STG.4	FAU_STG.1	Yes	-
FDP_IFC.1	FDP_IFF.1	Yes	-
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes	-
FIA_ATD.1	-	-	-
FIA_UAU.2	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1. Dependency is fulfilled with FIA_UID.2.
FIA_UID.2	-	-	-
FIA_SOS.1	-	-	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_SMF.1	-	-	-
FMT_SMR.1	FIA_UID.1	No	FIA_UID.2 is hierarchical to FIA_UID.1.

			Dependency is fulfilled with FIA_UID.2.
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes	-
FPT_STM.2	-	-	-

9.6 Security Assurance Requirements Rationale

EAL2 was chosen to provide a basic assurance. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2, the TOE will have undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of basic.