FIBERHOME Optical Transport Equipment

Security Target

Version:1.5

FiberHome Telecommunication Technologies Co., Ltd.

April 2016

LEGAL INFORMATION

Version

Table 1 - History of FIBERHOME Optical Transport Equipment Security Target

Version	Date	Description
0.1	2015/09/01	Initial version
1.0	2015/09/18	Refined Traffic Policy, completed all sections
1.1	2015/10/30	Update version information
1.2	2015/11/02	Addressed internal review comments
1.3	2016/01/19	Update section 1.3.1 “Usage and major features of the TOE” Update section 8.1 “Rationale for Security Objectives” Update section 4.2 ” Security Objectives for the Environment"
1.4	2016/02/05	Update section 7 and figure 1
1.5	2016/04/12	Update section 1.3.1 , section 3.3 and section 4.2 to remove all references to NMS server

Contents

Figures

Tables

1 ST Introduction

1.1 ST and TOE Identification

ST title:	FIBERHOME Optical Transport Equipment Security Target
ST developer:	FiberHome Telecommunication Technologies Co., Ltd.
ST version number:	1.5
ST publication Date:	2016-02-05
CC version used:	CC Version 3.1, Revision 4
CC conformance:	CC V3.1 part 2 extended and conformant to CC V3.1 part 3 augmented (EAL 2 augmented by ALC_FLR.2)
TOE name:	FONST1000/FONST1000 U5/FONST 5000/ FONST 5000 U Series OTN Equipment

1.2 Overview

This chapter presents a general overview of FIBERHOME Optical Transport Equipment, FIBERHOME Optical Transport Equipment is an optical Network Terminal (ONT) equipment used to terminate the optical fiberline, demultiplex the signal into its component parts (voice telephone, television, and Internet), and provide power to customer telephones. As well as, FIBERHOME Optical Transport Equipment helps to provide secure Internet connectivity.

1.3 TOE Overview

1.3.1 Usage and major features of the TOE

The TOE consists of

- One FIBERHOME Optical Transport Equipment(OTE), either:
  - FONST 1000/FONST 1000 U5/FONST 5000
  - FONST 5000 U Series (U10/U20/U30/U40/U60)
- One OTNM 2000 EMS(Element Management System) Server
- One EMS Client is intended to run on a workstation.

The TOE is depicted in Figure 1, together with relevant entities in its environment.

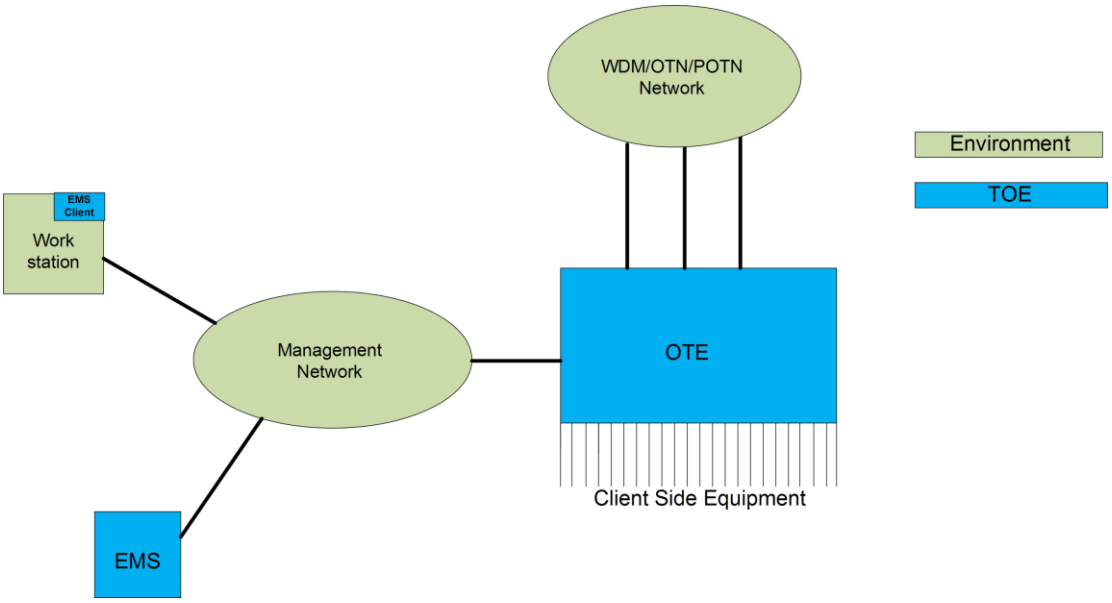


Figure 1 - TOE demarcation

These relevant entities in its environment are:

- A Management network, which is used to manage the OTE, This management network is considered to be trusted, and contains：
  - One or more management workstations with an EMS Client installed on them, which is used as a graphical user interface to the EMS Server.
  - Windows Server 2008 supply time sources.
- An WDM or OTN/POTN network, consisting of other OTEs, connected to the TOE. The WDM/OTN/POTN network is considered to be trusted.

The major security features of this TOE in this ST are as follows:

- Management network,
- Authorization,
- Access Control,
- Audit.

For the security features described above, the contents of each function are described in "1.4.2 Logical boundary".

1.3.2 TOE Type

The FONST1000/FONST1000 U5/FONST 5000/ FONST 5000 U Series OTN

Equipment series of products are packet optical transport equipment based on the unified switching system offered by FiberHome Telecommunication Technologies Co., Ltd. (referred to as FiberHome hereinafter).

1.3.3 Required non-TOE hardware/software/firmware

The EMS Server requires software as following table:

Table 2 - EMS Server required software

Type	Name and version
Server	A Server suitable to run the OS（The suggested hardware is: CPU 2x3.0GHz SPARC64 VII four-core Processors; Memory 32GB(8*4GB);Disks 1.5T）
OS	Windows Server 2008 (Supply time sources)

The EMS Client requires software as following table:

Table 3 - EMS Client required software

Type	Name and version
Workstation	A Workstation suitable to run the OS (see below)
OS	Windows Server 2008

1.4 TOE Description

1.4.1 Physical boundary

The TOE consists of:

- One FIBERHOME Optical Transport Equipment (FONST 1000/FONST 1000 U5/FONST 5000/FONST 5000 U Series)
- One EMS (Element Management System), consisting of a server plus software
- One EMS Client is intended to run on a workstation.

1.4.1.1 Physical Scope Optical Transport Equipment

Table 4 - Physical scope of optical transport equipment

FONST 1000	
Hardware	FONST 1000
Software	RP0201

Guidance	FONST 1000 intelligent OTN Equipment Configuration Guide FONST 1000 Intelligent OTN Equipment Hardware Description FONST 1000 Intelligent OTN Equipment Product Description
FONST 1000 U5	
Hardware	FONST 1000 U5
Software	RP0100
Guidance	FONST 1000 intelligent OTN Equipment Configuration Guide FONST 1000 Intelligent OTN Equipment Hardware Description FONST 1000 Intelligent OTN Equipment Product Description
FONST 5000	
Hardware	FONST 5000
Software	RP0201
Guidance	FONST 5000 intelligent OTN Equipment Configuration Guide FONST 5000 Intelligent OTN Equipment Hardware Description FONST 5000 Intelligent OTN Equipment Product Description
FONST 5000 U10	
Hardware	FONST 5000 U10
Software	RP0101
Guidance	FONST 5000 U Series Packet Enhanced OTN Equipment Alarm And Performance Reference FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description FONST 5000 U Series Packet Enhanced OTN Equipment Product Description FONST 5000 U Series Packet Enhanced OTN Equipment Routine Maintenance FONST 5000 U Series Packet Enhanced OTN EquipmentTroubleshooting Guide
FONST 5000 U20	
Hardware	FONST 5000 U20
Software	RP0101

Guidance	FONST 5000 U Series Packet Enhanced OTN Equipment Alarm And Performance Reference FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description FONST 5000 U Series Packet Enhanced OTN Equipment Product Description FONST 5000 U Series Packet Enhanced OTN Equipment Routine Maintenance FONST 5000 U Series Packet Enhanced OTN EquipmentTroubleshooting Guide
FONST 5000 U30	
Hardware	FONST 5000 U30
Software	RP0101
Guidance	FONST 5000 U Series Packet Enhanced OTN Equipment Alarm And Performance Reference FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description FONST 5000 U Series Packet Enhanced OTN Equipment Product Description FONST 5000 U Series Packet Enhanced OTN Equipment Routine Maintenance FONST 5000 U Series Packet Enhanced OTN EquipmentTroubleshooting Guide
FONST 5000 U40	
Hardware	FONST 5000 U40
Software	RP0101
Guidance	FONST 5000 U Series Packet Enhanced OTN Equipment Alarm And Performance Reference FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description FONST 5000 U Series Packet Enhanced OTN Equipment Product Description FONST 5000 U Series Packet Enhanced OTN Equipment Routine Maintenance FONST 5000 U Series Packet Enhanced OTN EquipmentTroubleshooting Guide
FONST 5000 U60	

Hardware	FONST 5000 U60
Software	RP0101
Guidance	FONST 5000 U Series Packet Enhanced OTN Equipment Alarm And Performance Reference FONST 5000 U Series Packet Enhanced OTN Equipment Hardware Description FONST 5000 U Series Packet Enhanced OTN Equipment Product Description FONST 5000 U Series Packet Enhanced OTN Equipment Routine Maintenance FONST 5000 U Series Packet Enhanced OTN EquipmentTroubleshooting Guide

1.4.1.2 Physical Scope EMS Server

Table 5 - Physical scope of EMS Server

e-FimOTNM 2000	
Software	mysql5.5.34 e-Fim OTNM2000 Element Management System V2.0R5
Guidance	e-Fim OTNM2000 Element Management SystemOperation Guide e-Fim OTNM2000Element Management System Product Description e-Fim OTNM2000Element Management SystemStandalone System InstallationGuide

1.4.1.3 Physical scope EMS client

Table 6 - Physical scope of EMS Client

EMS Client	**Name and version**
Software	e-Fim OTNM 2000 ClientV2.0R5(Build04.20.05.50BD4)

1.4.2 Logical boundary

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE. The TOE provides the following security features:

1.4.2.1 Access Control

- The TOE transport data to/from client-side equipment across the

WDM/OTN/POTN network in such a waythat:

- Only the intended recipients are able to read the signal.
- Nobody can modify the signals.

1.4.2.2 Authorization

- supports a flexible role-based authorization framework with predefined and customizable roles for management. These roles can use the TOE to manage the WDM/OTN/POTN network, and manage the TOE itself.

1.4.2.3 Authentication

- supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

1.4.2.4 Auditing

- supports flexible logging and auditing of events.

2 Conformance Claims

2.1 CC conformance claim

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012.

as follows

- CC Part 2 extended,
- CC Part 3 conformant.

2.2 PP claim

This security target does not claim to any protection profile.

2.3 Security requirement package claim

This security target claims to be conformant to the assurance package **EAL 2** augmented by **ALC_FLR.2** (Flaw reporting procedures).

3 Security Problem Definition

3.1 Threats

3.1.1 Assets and threat agents

The assets are:

1. The ability of administrators to manage various aspects of the TOE securely
2. Confidentiality and integrity of communication of client-side equipment over the WDM/OTN/POTN network

These assets are threatened by the following threat agents:

1. TA.CLIENT-SIDE An attacker with access to some client-side equipment.
2. TA.PHYSICAL An attacker with physical access to the TOE
3. TA.ROGUE_USER A TOE user seeking to act outside his/her authorization

3.1.2 Threats

Threats to the TOE are defined as below:

T.Confidentiality	TA.CLIENT-SIDE is able to read traffic that he is not allowed to read
T.Integrity	TA.CLIENT-SIDE is able to modify traffic that he is not allowed to modify
T.Physical_attack	TA.PHYSICAL gains physical access to the TOE (OTE, EMS or machine running the EMS Client) and is able to perform actions on the TOE.
T.Unauthorised	TA.ROGUE_USER performs actions on the TOE that he is not authorized to do
T.Authorised	TA.ROGUE_USER performs actions on the TOE that he is authorized to do, but these are undesirable and it cannot be shown that this user was responsible.

3.2 Organizational Security Policies

Security policies to be fulfilled by the TOE are defined as below:

P.FLEXIBLE_MANAGEMENT The TOE must be able to support:

- a flexible role-based authorization framework with predefined and customizable roles , to manage the TOE itself.
- a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of IP-address and time of login.
- flexible logging and auditing of events.

3.3 Assumptions

Assumptions for the IT and non-IT environment and intended usage are defined as below:

A.TRUSTED_NETWORK It is assumed that the Management Network and the WDM/OTN/POTN network are trusted. It is also assumed that Windows Server 2008(supply time sources) are trusted and will not be used to attack the TOE.

4 Security Objectives

These security objectives describe how the threats described in the previous section will be addressed. It is divided into:

- The Security Objectives for the TOE, describing what the TOE will do to address the threats
- The Security Objectives for the Operational Environment, describing what other entities must do to address the threats

A rationale that the combination of all of these security objectives indeed addresses the threats may be found in section 8.1 of this Security Target.

4.1 Security Objectives for the TOE

TOE security objectives are defined as below:

O. Access The TOE shall ensure that client-side equipment can:

- Only send data across the network to certain other client-side equipment
- Only receive data across the network from that client-side equipment
- Is not able to modify data that is not created by it or sent to it.

O.Authorise The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the WDM/OTN/POTN network, and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.

O.Authenticate The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC address and time of login.

O.Auditing The TOE shall support flexible logging and auditing of events.

4.2 Security Objectives for the Environment

Security objectives for the Environment (covers objectives for the IT environment and non IT-environment)are defined as below:

OE.SERVER_SECURITY The customer shall ensure that the EMS Server and the Optical Transport Equipment shall be protected from physical attacks.

OE.CLIENT_SECURITY The customer shall ensure that management workstations that host the EMS Client, are protected from physical and logical attacks that would allow attackers to subsequently:

- Disclose passwords or other sensitive information
- Hijack the client
- Execute man-in-the-middle attacks between client and EMS Server or similar attacks

OE.TRUST&TRAIN_USERS The customer shall ensure that roles are only assigned to users that are sufficiently trustworthy and sufficiently trained to fulfill those roles.

OE.TIME Windows Server 2008 supplies the TOE with time.

OE.TRUSTED_NETWORKS The customer shall ensure that:

- The Management Network and WDM/OTN/POTN Network are trusted, and will not be used to attack the TOE.
- Windows Server 2008(supply time sources) are trusted, so that they will not be used to attack the TOE.

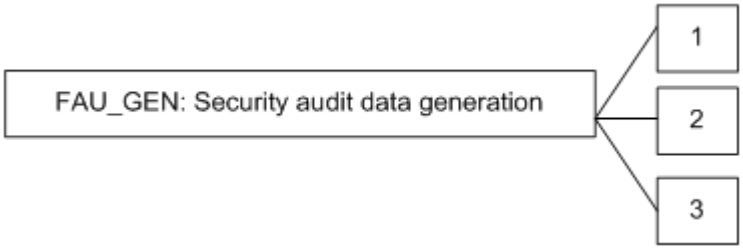
5 Extended Component Definition

FAU_GEN.3Simplified audit data generation

Family behaviour

This Security Target introduces one extended component: FAU_GEN.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

Component levelling



FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

FAU_GEN.3 Add or delete types of events to be logged in the security log.

Management: FAU_GEN.1, FAU_GEN.2, FAU_GEN.3

There are no management activities foreseen.

Audit: FAU_GEN.1, FAU_GEN.2, FAU_GEN.3

There are no auditable events foreseen.

FAU_GEN.3 Simplified audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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: Date and time of the event, **[assignment:** *other information about the event*].

5.1 Definitions

The following terms are used in the security requirements:

Roles:

- Administrator

Subjects/External Entities

- Services (on a Network)
- Ports (any physical Port to Client Equipment)

Objects:

- Traffic

Operations:

- Receive
- Send
- Modify

None of the subjects or objects have attributes

Subjects.

- Administrators: This user group has the management domain over assembly of objects and operation authorities over assembly of application operations.
- Security Administrator Group: This user group has the operation authorities related to the security management, including user management and online user management.
- Operator Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application operators by default.
- Maintainer Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application maintainers by default.
- Inspector Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application inspectors by default.
- Devcfg: This user group has the operation authorities of the Devcfg.
- Eot Group: This user group has the operation authority of the Eot group.
- NMS Group: This user group has the operation authority of the OTNMApi.

- Customized roles: these roles can be defined in the TOE by the Administrator (or by a configurable role who has the right to create roles) and have customizable rights.

None of the roles above has full “root” access to the TOE. This is reserved for FIBERHOME maintenance staff that regularly service the TOE using the systems console, but this is out of scope and not described further in this ST.

Operations

Operations in the TOE are divided into

- Topology Management
- Fault Management
- Performance Management
- Configuration Management
- Maintenance Management
- Security Management

A full list of operations is outside the scope of this ST, and can be found in the TOE Guidance.

6 IT Security Requirements

6.1 Security Functional Requirements

This chapter defines the TOE security functional requirements. A list of the security functional requirements is provided in Table 7. The full text of the security functional requirements is contained below.

The following notational conventions are used in the requirements. Operations are indicated in **bold**, except refinements, which are indicated in ***bold italic***. In general refinements were applied to clarify requirements and/or make them more readable. Iterations were indicated by adding three letters to the component name

Table 7 - TOE security functional requirements

Class	Functional requirement	Title
Access	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification & Authentication	FIA_UID.2	User identification before any action
	FIA_UAU.2	User authentication before any action
	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FTA_SSL.3	TSF-initiated termination
	FTA_MCS.1	Basic limitation on multiple concurrent sessions
Roles & Authorisation	FMT_SMR.1	Security roles
	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
Logging & Auditing	FAU_GEN.3	Audit data generation
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Management	FMT_SMF.1	Specification of Management Functions

6.1.1 Access

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Traffic Policy** on

- **Ports**
- **Traffic**
- **Receive, Send, Modify.**

FDP_IFF.1 Simple security attributes

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

- **Ports**
- **Traffic**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject andcontrolled information via a controlled operation if the following rules hold:

- **Ports can Receive Traffic from other Ports on the WDM/OTN/POTN Network, if soallowed by the Traffic Policy rules**
- **Ports cannot Receive Traffic not destined for that port**
- **Ports can Send Traffic to other Ports on the WDM/OTN/POTN Network, if so allowedby the Traffic Policy rules**
- **Portscannot Modify Traffic on other Ports**

FDP_IFF.1.3, FDP_IFF.1.4, FDP_IFF.1.5 ***(refined away)***

6.1.2 Identification & Authentication

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each ***EMS***user to be successfully identified

- ***by username (in all cases), and***
- ***by IP-address (if so configured for that user)***
- ***by MAC-address (if so configured for that user)***
- ***and ensure that the user is allowed to login at this time (if so configured for that EMSuser)***

before allowing any other TSF-mediated actions on behalf of that user

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each ***EMS***user to be successfully authenticatedbefore allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positiveinteger within 2-3** unsuccessful authentication attempts occur related to **the sameEMS user account**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **lock the EMS user account**

- **until unlocked by the administrator, or**
- **until an administrator configurable positive integer within [24-infinity] of hourshave passed, if the account has not been set to permanent locking.**

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ***passwords*** meet:

- **At least 8characters including three of the four types: number, small letter, capital letter, other characters**
- **cannot be the same as the user name, the user name twice, the username in reverse or a common dictionary word**
- **can be configured to expire after a configurable amount of time < 180 days**
- **can be configured to be different from the previous 5 or more passwords when changed**

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a

- **configurable period of inactivity more than 30 minutes**
- **when the allowed work time (if so configured for that user) expires, or**
- **when one of the user roles is being locked while he is logged in**

FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** session per user ***and a limit of 64sessions for all EMS users together.***

6.1.3 Roles &Authorisation

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **Administrators**
- **Security Administrator Group**
- **Operator Group**
- **Maintainer Group**
- **Inspector Group**
- **Devcfg**[1]
- **Eot Group**[2]
- **NMS Group**[3]
- **Customized roles**

FMT_SMR.1.2 The TSF shall be able to associate users with ***one or more*** roles.

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Role Policy** on **all roles and resources andthe TOE** and all operations among ***roles*** and ***resources and the TOE*****.**

FDP_ACC.2.2 The TSF shall ensure that all operations between any ***role*** and any ***resource and the TOE*** are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

[1]Configuration management module: a program used by the EMS to configure devices and the system operating environment

[2]Eot:Command line operation

[3]NMS Group: This user group has the operation authority of the OTNMApi. When the upper-level NMS system connects to the OTNM2000 through the northbound interface, you need to create a user for the NMS on the OTNM2000 and add the user into the NMS group. The NMS group is for managing the access authorities of the NMS

FDP_ACF.1.1 The TSF shall enforce the **Role Policy** to objects based on the following: **all roles, all resources and the TOE**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among ***roles*** and ***resources and the TOE*** is allowed:

- **for the roles Administrators, Security Administrator Group, Operator Group, Maintainer Group, Inspector Group, Devcfg, Eot Group and NMS Group, as defined in the guidance**
- **for the customized roles, as defined by their customization**
- **the Administrator and appropriately customized roles can perform the functions in FMT_SMF.1**
- **if a user has multiple roles, it is sufficient if only one role is allowed to do the operation**
- **if a role is locked no user has this role**

FDP_ACF.1.3, FDP_ACF.1.4 ***(refined away)***.

6.1.4 Logging & Auditing

The TOE maintains 3 separate logs:

- A security log for authentication events
- An operation log for operations performed by users
- A system log for EMS server tasks that are not directly related to users performing operations

FAU_GEN.3 Audit data generation

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

In the security log:

- **authentication success/failure**
- **user account is locked**
- **user account is unlocked**
- **user account is enabled**
- **user account is disabled**

FAU_GEN.3.2 The TSF shall record within each audit record:

- **Date and time of the event,**
- **User name**
- **Type of event**
- **Detailed Information**

FAU_SAR.1Audit review

FAU_SAR.1.1 The TSF shall provide **Administrator and suitably customized roles** with the capability to read **security log** 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.

FAU_STG.1 Protected audit trail storage

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.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records** if the audit trail is full.

6.1.5 Management

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

Table 8 - Management functions

Management function	Related to SFR
Manage the Traffic Policy Rules	**FDP_IFF.1**
Set whether a user can only login from certain IP addresses, and if so, which IP addresses	**FIA_UID.2**
Set whether a user can only login from certain MAC-addresses, and if so, which MAC-addresses	**FIA_UID.2**
Set the time that a user may remain logged in while inactive	**FTA_SSL.3**
Set whether a user is only allowed to work at certain times, and if so, at which times	**FTA_SSL.3**
Set the number of allowed unsuccessful authentication attempts	**FIA_AFL.1**

Management function	Related to SFR
Set the number of hours that an account remains locked	**FIA_AFL.1**
Set whether a user account should be: o **unlockable, or** o **locked (either permanently or temporarily)** **when it exceeds the number of allowed consecutive unsuccessful authentication attempts**	**FIA_AFL.1**
Unlock a user account	**FIA_AFL.1**
Set whether a user password expires after a certain time, and if so, after how long	**FIA_SOS.1**
Set whether the new password of a user must be different from the last n passwords when the password is changed by the user and configure n	**FIA_SOS.1**
Set the maximum number of concurrent sessions for the same user	**FTA_MCS.1**
Create, edit and delete customized roles	**FMT_SMR.1**
Add or remove roles to/from users	**FMT_SMR.1**
Add or delete types of events to be logged in the security log	**FAU_GEN.3.1**
Create, edit and delete user accounts	-
Disable/enable user accounts	-
Lock/unlock roles	-
Adding, deleting and modifying rules in the Communication Policy	**FDP_IFC.1, FDP_IFF.1**

6.2 Security Assurance Requirements

The security assurance requirements for the TOE are the assurance components of evaluation assurance level 2 (EAL 2)augmented ALC_FLR.2. They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 9.

Table 9 - Security assurance requirements of the EAL 2+ALC_FLR.2

Assurance class	Assurance component (Identifier & Name)	
Development(ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design

Assurance class	Assurance component (Identifier & Name)	
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw reporting procedures**
Security target evaluation (ASE)	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
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment (AVA)	AVA_VAN.2	Vulnerability analysis

6.3 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL2+ALC_FLR.2. The reasons for this choice are that:

- EAL 2 is deemed to provide a good balance between assurance and costs and is in line with FiberHome customer requirements.
- ALC_FLR.2 provides assurance that FiberHome has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with FiberHome customer requirements.
- The refinements are derived from FiberHome customer requirements as well.

7 TOE Summary Specification

Access control: Transport input to/from client-side equipment across the WDM/OTN/POTN network insuch a way that:

- Only the intended recipients are able to read the signal
- Nobody can modify the signals

FDP_IFC.1, FDP_IFF.1

The TOE uses several mechanisms to enforce the Traffic Policy:

- Ports are physically isolated from each other, and can only talk to each other through a switch in the TOE.

Authentication: The TOE supports a flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login.

General:

This functionality is implemented through a standard login screen.

FIA_UID.2, FIA_UAU.2, FIA_AFL.1

Whenever a user of the TOE wishes to use the TOE, the user needs to use either the graphical EMS-client or the CLI. The first action required by the user is then to log-in.

The TOE allows the Administrator to configure (for each user), how that user must log-in:

- The user must always provide a username and a password
- Whether the user can only login from a predefined IP-addresses and/or MAC-address
- Whether the user is only allowed to be logged in during a certain time interval (e.g. officehours)
- Whether an account is unlockable or not, and when an account is not unlockable:
  - how many times a user can fail consecutive authentication attempts before that account is locked
  - how the account is unlocked by the Administrator or until a

predefined time elapses

FTA_MCS.1

Even if all of the above is correct, the user can still be denied access when:

- the user is already logged in
- too many other users are already logged in

FTA_SSL.3

The TOE will log a user out when:

- The Administrator locks one of the roles that that user currently has. The user can subsequently log in again, but he will not have that role.
- The user is only allowed to be logged in during a certain time interval, and this interval expires.

FIA_SOS.1

Whenever the user has to provide a new password to the TSF (all passwords expire in 6 months or less), these passwords have to meet certain rules to ensure that the passwords cannot be easily guessed or broken by brute force. Passwords that do not meet these rules are rejected by the TOE.

Authorization: The TOE supports a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the TOE itself.

FMT_SMR.1, FDP_ACC.2, FDP_ACF.1, FMT_SMF.1

The TOE allows management of the telecommunications network by different users. The TOE can be configured to give each user precisely the access to the resources of the telecommunication network that user needs to do his job. To assist in this, the TOE has a number of pre-defined roles:

- Administrators: This user group has the management domain over assembly of objects and operation authorities over assembly of application operations.
- Security Administrator Group: This user group has the operation authorities related to the security management, including user management and online user management.
- Operator Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application operators by default.

- Maintainer Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application maintainers by default.
- Inspector Group: This user group has the management domain over assembly of objects and operation authorities over assembly of application inspectors by default.
- Devcfg: This user group has the operation authorities of the Devcfg.
- Eot Group: This user group has the operation authority of the Eot group.
- NMS Group: This user group has the operation authority of the OTNMApi.

and can assign these roles to specific users.

The role of Administrator is a global role: he has all rights for all resources. The other three roles are assigned per resource, that is: a user can have the Maintenance role for one resource, but Operator role for another, and no role at all for all other resources.

Finally, the Administrator can manage the TOE itself through a series of configuration and management screens.

Accounting: The TOE supports flexible logging and auditing of events.

FAU_GEN.3, FAU_SAR.1, FAU_STG.1, FAU_STG.4

The TOE maintains a security log for authentication events.

The log is only accessible to the Administrator, who is only able to read the log (not modify/delete them). Once the log becomes full, the oldest records are overwritten.

8 Rationale

8.1 Rationale for Security Objectives

Table 10 - Rationale for security objectives (1)

Security objectives / Threat/OSP/ Assumption	O.AUTHORISE	O.AUTHENTICATE	O. ACCESS	O.AUDITING	OE.SERVER_SECURITY	OE.CLIENT_SECURITY	OE.TRUST&TRAIN_USERS	OE.TIME	OE.TRUSTED_NETWORKS
T. Confidentiality			X						
T.Integrity			X						
T.Physical_attack			X		X	X			
T.Unauthorised	X	X				X	X		
T.Authorised				X			X		
P.FLEXIBLE_MANAGEMENT	X	X		X				X	
A.TRUSTED_NETWORK									X

Table 11 - Rationale for security objectives (2)

Assumptions/OSPs/Threats	Objectives
OSP.Flexible_Management The TOE must be able to support: • a flexible role-based authorization framework with predefined and customizable roles, both to manage the TOE itself. • a flexible authentication framework, allowing the TOE to accept/reject users based on username/password and a configurable subset of: IP/MAC-address, time of login.	This OSP is primarily implemented by the combination of three security objectives: • O.AUTHORISE that restates the first item of the OSP, • O.AUTHENTICATE that restates the second item of the OSP, and • O.AUDITING that restates the

Assumptions/OSPs/Threats	Objectives
• flexible logging and auditing of events.	third bullet of the OSP Additionally, to perform logging (part of the third item), the TOE must have a time source. OE.TIME states that this time source will be connected to the TOE
T.Confidentiality TA.CLIENT-SIDE is able to read traffic that he is not allowed to read	This threat is countered by the first two bullets of O.ACCESS, which directly prevent access to this traffic
T.Integrity TA.CLIENT-SIDE is able to modify traffic that he is not allowed to modify	This threat is countered by the third bullet of O.ACCESS, which directly prevents modification of this traffic
T.Physical_attack TA.PHYSICAL gains physical access to the TOE(OTE, EMS or EMS Client) and is able to perform actions on the TOE.	This threat is countered by: • OE.SERVER_SECURITY, preventing attackers physical access to the EMS and OTE, and • OE.CLIENT_SECURITY, preventing attackers physical access to the EMS Client
T.Unauthorised TA.ROGUE_USER performs actions on the TOE that he is not authorized to do.	This threat is countered by four security objectives: • OE.TRUST&TRAIN_USERS that ensures that only users that are properly trusted and trained will be able to gain access to certain roles • O.AUTHENTICATE that ensures users are properly authenticated so the TOE knows which roles they have • O.AUTHORISE that ensures that only users with certain roles can do certain actions. • OE.CLIENT_SECURITY, which prevents TA.ROGUE_USER from bypassing the client.

Assumptions/OSPs/Threats	Objectives
	So the only way that a user can perform a management action is when he has a role, and the only way he can get this role is if he is properly trained and trusted. Therefore this threat is countered.
T.Authorised TA.ROGUE_USER performs actions on the TOE thathe is authorized to do, but these are undesirable andit cannot be shown that this user was responsible.	This threat is countered by: • OE.TRUST&TRAIN_USERS that ensures that only users that are properly trusted and trained will be able to gain access to certain roles. This should go along way to prevent the threat from being realized. • Should this prove insufficient, O.AUDITING will ensure that the actions of the user can be traced back to him. Together these two security objectives counter the threat.
A.TRUSTED_NETWORK It is assumed that the Management Network and theWDM/OTN/POTN network are trusted. It is also assumed that Windows Server 2008(supply time sources) is trusted and will not be used to attack the TOE.	This assumption is upheld by OE.TRUSTED_NETWORK, which restates the assumption.

8.2 Security Functional Requirements Rationale

Table 12 - Rationale for security functional requirements (1)

Security objectives / Security functional requirements	O. ACCESS	O.AUTHORISE	O.AUTHENTICATE	O.AUDITING
FDP_IFC.1	X			
FDP_IFF.1	X			
FIA_UID.2			X	
FIA_UAU.2			X	
FIA_AFL.1			X	
FIA_SOS.1			X	
FTA_SSL.3			X	
FTA_MCS.1			X	
FMT_SMR.1		X		
FDP_ACC.2		X		
FDP_ACF.1		X		
FAU_GEN.3				X
FAU_SAR.1				X
FAU_STG.1				X
FAU_STG.4				X
FMT_SMF.1	X	X	X	X

Table 13 - Rationale for security functional requirements (2)

Security objectives	SFRs addressing the security objectives
O. Access The TOE shall ensure that client-side equipment can: • Only send data across the network to certainother client-side equipment • Only receive data across the network from thatclient-side equipment • Is not able to modify data that is not created by itor sent to it.	This objective is met by FDP_IFF.1 and FDP_IFC.1 specifying that there arerules regulating the access and FMT_SMF.1 allowing management of theserules.

Security objectives	SFRs addressing the security objectives
O.Authorise The TOE shall support a flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the WDM/OTN/POTN network and manage the TOE itself. Each role allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a role that allows this.	This objective is met by: FMT_SMR.1 stating the predefined and customizable roles. FDP_ACC.2 and FDP_ACF.1 defining a Role Policy, which states how the various roles manage the network and the TOE. These also state that only roles can perform actions(operations on resources) and therefore users can only do this when they have the correct role FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible, role-based authorization framework.
O.Authenticate The TOE shall support a flexible authentication framework, allowing the TOE to accept/reject users based on: Username/password and a configurable subset of IP/MAC-address and time of login.	This objective is met by: • FIA_UID.2 stating that identification will be done by username, password, IP/MAC-address, login time • FIA_UAU.2 stating that users must be authenticated • FIA_SOS.1 stating that passwords must have a minimum quality • FIA_AFL.1 stating what happens when authentication fails repeatedly • FTA_SSL.3 logging users off when they are no longer allowed to work or when their role is locked • FTA_MCS.1 preventing a user of having too many sessions or all users together having too many sessions • FMT_SMF.1 configuring all of the above. Together, these SFRs support a flexible authentication framework.

Security objectives	SFRs addressing the security objectives
O.Auditing The TOE shall support flexible logging and auditing of events.	This objective is met by: • FAU_GEN.3 showing which events are logged • FAU_SAR.1 showing that the logged events can be audited and by whom • FAU_STG.1 showing how the audit logs are protected • FAU_STG.4 stating what happens when the audit log becomes full • FMT_SMF.1 configuring all of the above Together, these SFRs support a flexible logging and auditing framework.

8.2.1 Dependencies Rationale

Table 14- Rationale for dependencies of security functional requirements

SFR	Dependencies
FAU_GEN.3	FPT_STM.1: met in the environment by OE.TIME
FAU_SAR.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FAU_STG.1	FAU_GEN.1: met by FAU_GEN.3, which is similar enough to meet the dependency
FAU_STG.4	FAU_STG.1: met
FDP_ACC.2	FDP_ACF.1: met
FDP_ACF.1	FDP_ACC.1: met by FDP_ACC.2 FMT_MSA.3: unnecessary, since there are no security attributes
FDP_IFC.1	FDP_IFF.1: met
FDP_IFF.1	FDP_IFC.1: met FMT_MSA.3: unnecessary, since there are no security attributes
FIA_AFL.1	FIA_UAU.1: met by FIA_UAU.2
FIA_SOS.1	_

SFR	Dependencies
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FIA_UID.2	_
FMT_SMF.1	_
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FTA_MCS.1	FIA_UID.1: met by FIA_UID.2
FTA_SSL.3	_

9 Appendix

9.1 Acronyms

EMS	Element Management System
NMS	Network Management System
NTP	Network Time Protocol
ONT	Optical Network Terminal
OTE	Optical Transport Equipment
OTNM	Optical Transport Network Management
POTN	Packet Enhanced Optical Transport Network
WDM	Wave Division Multiplexing

9.2 References

[CC] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, dated September 2012, Version 3.1, Revision 4, CCMB- 2012-09-001
Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated September 2012, Version 3.1, Revision 4, CCMB-2012-09-003

[CEM] *Common Evaluation Methodology for Information Technology Security Evaluation*, dated September 2012, Version 3.1, Revision 4, CCMB-2012-09-004