ZTE

ZTE OTN Solution

Security Target

LEGAL INFORMATION

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

Users may visit ZTE technical support website http://ensupport.zte.com.cn to inquire related information. The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Version	Date	Comment
0.1	20/05/2022	First draft
0.2	03/06/2022	Refine security features
0.3	17/06/2022	Minor description update
0.4	07/07/2022	Minor update after internal review
0.5	13/10/2022	Update according to evaluation results
0.6	26/10/2022	Minor update
0.7	04/11/2022	Minor update and correct guidance names/version
0.8	23/11/2022	Update according to evaluation results
0.9	10/01/2023	Update according to evaluation results
0.10	12/01/2023	Update according to evaluation results
0.11	14/02/2023	Update according to evaluation results
1.0	23/03/2023	Finalize and release
1.1	18/05/2023	Minor update

Contents

1 ST Introduction

1.1 ST References

Title	ZTE OTN Solution Security Target
Version	1.1
Date	18-05-2023
Author	ZTE Corporation

1.2 TOE reference

TOE Name	ZTE OTN Solution	
TOE version	V1.10	
TOE Components	Hardware Models	Software version
	ZXONE 9700 S3K ZXONE 9700 G2K ZXONE 9700 NX41 ZXONE 9700 OX42 ZXONE 9700 NXG0 ZXONE 9700 NXG1	ZXONE19700V1.10.010.002B500, including the following patches: ZXONE19700V1.10.010.002B500CP001 ZXONE19700V1.10.010.002B500CP002 ZXONE19700V1.10.010.002B500CP003
	ZXONE 7000 C2	ZXONE7000V2.00R5B111, including the following patches: ZXONE7000V2.00R5B111_C01 ZXONE7000V2.00R5B111_C02
	ZXMP M721 CX66A(E) ZXMP M721 CX63A(E) ZXMP M721 DX63(E)	ZXMPM721V5.10.070.001B100, including the following patches: ZXMPM721V5.10.070.001B100CP001 ZXMPM721V5.10.070.001B100CP002
Developer	ZTE Corporation	

1.3 TOE Overview and usage

The TOE is the ZTE OTN solution aimed to build broadband and intelligent full connection for the ICT field in the 5G era. Based on cloud datacenters (DCs), ZTE OTN solution establishes large-capacity interconnection pipes between DCs and between DCs and services, to implement unified transport of fixed/wireless networks and vertical industries.

The TOE is widely used in metro network (including core layer, aggregation layer, and access layer) and backbone network. They provide transmission solutions with various capacities, transmission distances, and intelligent service applications.

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

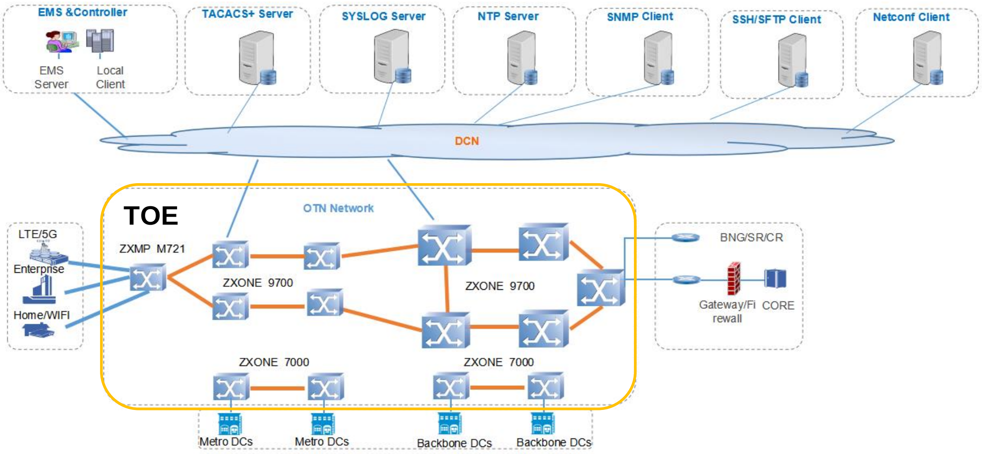


Figure 1: The TOE in its environment

These entities are:

- A DCN network to manage the TOE. This management network is considered to be trusted, and contains (apart from the TOE):
    - EMS client/server: This is a Network Management System[1] used by a network operator to monitor and configure its entire optical transmission network.
    - SSH client: a command line interface to manage the TOE.
    - SFTP client: a command line interface to upload TOE patches or download syslog files.
    - Netconf client: a proprietary XML-based command interface to manage the TOE.

[1] Some operators refer to an NMS as an OSS (Operations Support System).

  - TACACS+ server: a TACACS+ server as a remote authentication server.
  - Syslog server: an external syslog server to keep the audit log.
  - SNMP client: an external client for receiving the SNMP trap generated by the TOE.
  - NTP server: an external server that provides time source.
- An OTN/WDM network, consisting of other OTEs, connected to the TOE. The OTN/WDM network is considered to be trusted.

1.3.1 Major security features

The major security features of the TOE are:

1. Secure management and usage of the TOE, to ensure that only properly authorized staff can manage and/or use the TOE;
2. Secure interaction between various parts of the TOE and between the TOE and various machines in the environment, so that the management data and commands cannot be read or modified in-between;
3. Logging and auditing of user actions;
4. Information flow control for management traffic.

1.3.2 Non-TOE Hardware/Software/Firmware

The environment for TOE comprises the following software as shown in Figure 1:

- Management Clients:
  - EMS client/server
  - SSH client
  - SFTP client
  - Netconf client
- Supporting Servers:
  - TACACS+ server
  - Syslog server
  - SNMP client
  - NTP server

The environment for TOE comprises the following:

- Local PCs are used by administrators to connect to the TOE for accessing the services with a secure channel by a SSH/SFTP client, or local console. The TOE is accessed by using a command line terminal.
- Remote PCs/workstations used by administrators to connect to the TOE for access with a SSH/SFTP client, Netconf client or EMS client.
- Servers hosting the following servers:
  - EMS server, for TOE management through the EMS GUI client.
  - TACACS+ server is optional and may be used instead of local authentication.
  - Syslog server is optional and is used for receiving audit information from the TOE via SYSLOG protocol.
  - SNMP client is optional and is used for receiving alarm information from the TOE via SNMP protocol.
  - NTP server is used for synchronizing time to the TOE.
- Other OTEs

1.4 TOE Description

1.4.1 Physical scope

The TOE consists of both OTE hardware, software and guidance documents. The TOE software is provisioned in the TOE hardware. Both are delivered to the customer physically with a contracted shipping company. The customer needs to download the software package as ZIP file and the guidance documents as zed or pdf files from ZTE’s support website and the user has to verify the versions provided in the following table for all TOE parts for secure acceptance.

1.4.1.1 Physical Scope Optical Transmission Equipment

Type	Delivery Items	Version
ZXONE 9700 Series		
Hardware models	ZXONE 9700 S3K ZXONE 9700 G2K ZXONE 9700 NX41 ZXONE 9700 OX42 ZXONE 9700 NXG0 ZXONE 9700 NXG1	V4.20

Software packages[2]	Download software package name: ***IV202302030197.zip***, which contains the following files with their corresponding hash values: • ZXONE19700V1.10.010.002B500_@M4NCPM-REL-221124.set, e67fa89307d3f09ae34d21580de2aa4740cab793154c3d9c57ce705d7e041905 • ZXONE19700V1.10.010.002B500CP001_@NCPM-M4.set, 082c0b02e617fd9601977828d6b2348b8f28dfee2b54e589d2487048a246d687 • ZXONE19700V1.10.010.002B500CP002_@NCPM-M4.set, 4b802ee756c15cf863934801760a1a4cfce9e56500b08ee8c924e12edacdfc3f • ZXONE19700V1.10.010.002B500CP003_@NCPM-M4.set, a5b30d164093e04ca610e2713f191ffb3e92e763abb0876e20fcce558a56584d • ZXONE19700V1.10.010.002B500_@M2NCPQ-REL-221124.set, cfb4ea3c701d252a744c9561bec419e1f8c395fe8d28acee8faf76c9992154ae • ZXONE19700V1.10.010.002B500CP001_@NCPQ-M2.set, 791da8c91c30d7290f38b391e012928fa4929b2125951f1cebfa78fa2ddaabc6 • ZXONE19700V1.10.010.002B500CP002_@NCPQ-M2.set, e33a3059dbf7620db1eab71afc3f1b14936792364fd5f3598b05809f6c76bbd0 • ZXONE19700V1.10.010.002B500CP003_@NCPQ-M2.set, aa1d5e20e2c932decd6a129349e296f443bff9e4c816eae94bfd793c9b2849e9 • ZXONE19700V1.10.010.002B500_@SNPG-REL-221128.set, 4dc8e0dde7006ce109adc2da5e4087e7c714f7b67c65ace59a5a6d115813e929 • ZXONE19700V1.10.010.002B500CP001_@SNPG.set, 6d595ecf6454eeafd49f0811720d26fc0505b3fa3457611c36a4a327002adbfc • ZXONE19700V1.10.010.002B500CP002_@SNPG.set, c6563a0164d8ef451c9608fea7de575d74e92525cacc80f9af4e1f78ed48ac70	V1.10

[2] See appendix A for the correspondence between software packages and hardware models

Guidance documents	ZXONE 9700 Quick Installation Guide	R1.7, 2019-07-18
	Unitrans ZXONE 9700 Packet OTN Equipment Routine Maintenance(V4.20)	R1.1, 2022-02-28
	Unitrans ZXONE 9700 Packet OTN Equipment Alarm Handling(V4.20)	R1.0, 2021-06-15
	Unitrans ZXONE 9700 Packet OTN Equipment Performance Reference(V4.20)	R1.0, 2021-06-15
	Unitrans ZXONE 9700 Packet OTN Equipment Security Description(V4.20)	R1.0, 2021-06-25
	Unitrans ZXONE 9700 Packet OTN Equipment Hardware Description(V4.20)	R1.1, 2022-03-30
	OTN Product CLI User Manual.en-US	V1.5, 2023-01-04
	OTN Product QX Interface Specification.en-US	V1.2, 2022-10-19
	ZXONE 9700 ZXONE 7000 ZXMP M721 Interface Specification Return Value.en-US	V1.0
	ZXONE 9700 ZXONE 7000 ZXMP M721 Common Criteria Security Evaluation - Certified Configuration	V3.0, 2023-03-27
ZXONE 7000 Series		
Hardware model	ZXONE 7000 C2	V2.00
Software packages	Download software package name: ***IV202302030198.zip***, which contains the following files with their corresponding hash values: • ZXONE7000V2.00R5B111.set, 7eac0dbc526e16c89e066d91c79c4c84c5957e5956cf8e0f2bacaff705545cb6 • ZXONE7000V2.00R5B111_C01.set,	V2.00

	57a4881f2a56e936d78426e10635b6f9b7ed80ad663e73320140b9d259164304 • ZXONE7000V2.00R5B111_C02.set, 1f150e85d58eae95bd8ad1a2e192d1ae34c73ecaead41f9c796dafc7236407db	
Guidance documents	ZXONE 7000 Quick Installation Guide	R1.1, 2018-01-23
	Unitrans ZXONE 7000 Cloud OTN Equipment Routine Maintenance Guide(V2.00)	R1.0, 2019-07-03
	Unitrans ZXONE 7000 Cloud OTN Equipment Alarm Handling (V2.00)	R1.0, 2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Performance Reference (V2.00)	R1.0, 2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Security Description (V2.00)	R1.0, 2022-06-10
	Unitrans ZXONE 7000 Cloud OTN Equipment Hardware Description(V2.00)	R1.2, 2021-12-26
	OTN Product CLI User Manual.en-US	V1.5, 2023-01-04
	ZXONE 7000 NETCONF Interface Specification.en-US	V1.3, 2023-01-04
	ZXONE 9700 ZXONE 7000 ZXMP M721 Interface Specification Return Value.en-US	V1.0
	ZXONE 9700 ZXONE 7000 ZXMP M721 Common Criteria Security Evaluation - Certified Configuration	V3.0, 2023-03-27
ZXMP M721 Series		
Hardware models	ZXMP M721 CX66A(E) ZXMP M721 CX63A(E)	V5.10

	ZXMP M721 DX63(E)	
Software packages[3]	Download software package name: ***IV202302020153.zip***, which contains the following files with their corresponding hash values: • ZXMPM721V5.10.070.001B100_@NCPLC-REL-221128.set, b7354a5c50c103996649f57d07ae5a39622993d826b85de9393f709b4d9c1115 • ZXMPM721V5.10.070.001B100CP001_@NCPLC-REL.set, c337f703cb3a39c9c5db4d121efd6a2d654d0522ba5f0a8ebacb38b270d8a601 • ZXMPM721V5.10.070.001B100CP002_@NCPLC-REL.set, 5b98fde341ec45b3046f7bea2b4f5e835c3b6a556d075f5474e235065a41fa99 • ZXMPM721V5.10.070.001B100_@NCPLE-REL-221125.set, 7fd7268e79ad94cc87c305afaa40ee0203301bde8ee11753462abaa5ce708e1d • ZXMPM721V5.10.070.001B100CP001_@NCPLE-REL.set, 91e206f9c9f9a9d44eedc1afdb327ead3d4d4109fd4001fd932a5e0335cade03 • ZXMPM721V5.10.070.001B100CP002_@NCPLE-REL.set, 76d175381a623df93812ad9d7fd3c0ae5717ecbc4bb6e8319eaade08df946bc0 • ZXMPM721V5.10.070.001B100_@NCP(E)-REL-221125.set, 1e7837a566063c4dcb044bc1381a67e7e1ec020797cf34c6ffbc586329527598 • ZXMPM721V5.10.070.001B100CP001_@NCP(E)-REL.set, 808645b439d0b7a5710f8d85a33e7e4edd76e1b9cf4f271cca29a901bf953b92 • ZXMPM721V5.10.070.001B100CP002_@NCP(E)-REL.set, 8e9aa4d0472b997169b4251d2193464a2abfe6267cca71775b09999d3fe12617	V5.10
Guidance Documents	ZXMP M721 Quick Installation Guide	R2.0, 2022-04-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Routine Maintenance (V5.10)	R1.0, 2021-04-25

[3] See appendix A for the correspondence between software packages and hardware models

	Unitrans ZXMP M721 Metro-Edge OTN Equipment Alarm Handling (ZENIC ONE R22)(V5.10)	R1.0, 2021-06-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Performance Reference (ZENIC ONE R22)(V5.10)	R1.0, 2021-06-30
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Security Description(V5.10)	R1.0, 2021-06-10
	Unitrans ZXMP M721 Metro-Edge OTN Equipment Hardware Description(V5.10)	R1.4, 2022-08-27
	OTN Product CLI User Manual.en-US	V1.5, 2023-01-04
	OTN Product QX Interface Specification.en-US	V1.2, 2022-10-19
	ZXONE 9700 ZXONE 7000 ZXMP M721 Interface Specification Return Value.en-US	V1.0
	ZXONE 9700 ZXONE 7000 ZXMP M721 Common Criteria Security Evaluation - Certified Configuration	V3.0, 2023-03-27

1.4.2 Logical scope

Figure 2 shows the logical architecture of the TOE. All the software components are included in the TOE software bundle listed in section 1.4.1.

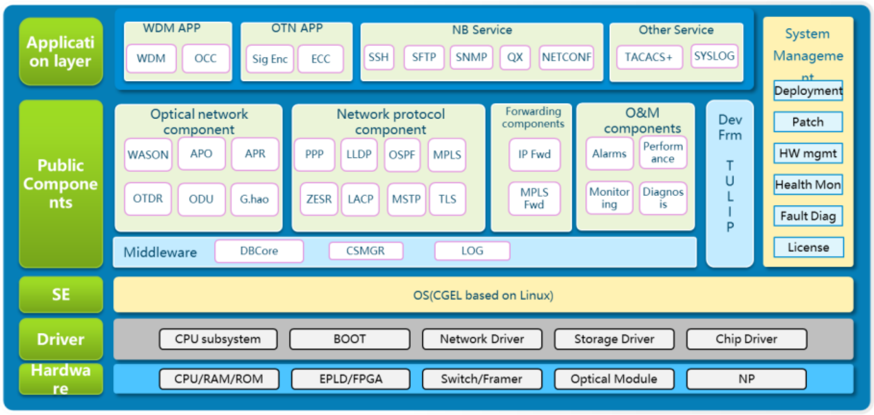


Figure 2 Logical Architecture of the TOE

The TOE provides the following security functionalities:

1. Users identification and authentication is enforced so users must be authenticated by password before using or managing the TOE. User sessions are monitored and passwords are verified to enforce secure authentication;
2. Access control is strictly enforced to TOE users based on their privilege level and the access control policy;
3. User management functionalities are provided to control the users and their attributes (privilege level, password, idle time, account lock, etc.);
4. TOE communications with the management client or EMS server are protected against modification or disclosure;
5. User actions are logged. The log trail is protected against unauthorized modification. The TOE provides administrators with log review capabilities.
6. Information flow control: The TOE accepts management traffic from the DCN network according to the ACL rules.

2 Conformance Claims

This ST conforms to Common Criteria, version 3.1R5, as defined by [CC] with

- ▢ CC Part 2 conformant
- ▢ CC Part 3 conformant

This ST claims conformance to EAL 3 augmented with ALC_FLR.2.

This ST conforms to no Protection Profile.

3 Security Problem Definition

This section describes the assets, threat agents and threats to the TOE.

3.1 Assets

USER_DATA User data from a user device that is transmitted by the TOE.

ADMIN_ACCESS Administrative access to the TOE.

TSF_DATA TSF data stored and managed by the Management Clients and that is used to enforce the security mechanism, such as the stored user passwords, the user attributes, or the encryption keys for the trusted channels. This data shall only be modified by users with **ADMIN_ACCESS.**

TSF_ACTIVITY_LOGS User and administrator log records generated by the TSF.

3.2 Threat agents

TA.REMOTE An attacker with access to the DCN Network that is connected to the TOE. This agent does not have authorized access to the TOE.

TA.USER An attacker with authorised access to the TOE, but without any administrative rights.

3.3 Threats

T.COMMUNICATION_CH **TA.REMOTE** may be able to disclose or modify **USER_DATA** or **TSF_DATA** data while being transmitted through unsecure networks.

T.UNAUTHENTICATED_USER **TA.REMOTE** may be able to bypass the user authentication and to access the TOE and perform administrative actions (**ADMIN_ACCESS**) on the TOE and modify **TSF_DATA**.

T.UNAUTHORIZED_ADMIN **TA.USER** may be able to bypass the access control policy or information flow control policy of the TOE and perform administrative actions (**ADMIN_ACCESS**) without administrative rights and modify **TSF_DATA**.

T.UNDETECTED_ACTIVITY **TA.REMOTE** or **TA.USER** may be able to attempt or perform abusive actions on the TOE without administrator awareness (**TSF_ACTIVITY_LOGS**).

T.UNKNOWN_SOURCE

TA.REMOTE may be able to bypass the information flow access control and to access the TOE and perform administrative actions (**ADMIN_ACCESS**) on the TOE and modify **TSF_DATA**.

3.4 Assumptions

A.TIME

The environment will provide a reliable timestamp for the TOE.

A.TRUSTED_NETWORK

The TOE, SYSLOG server, SNMP client, TACACS+ server and other OTEs are deployed in a controlled environment; at the operator's equipment room in trusted networks. The TOE and the TOE management clients/servers are segregated from the core network and IP management network so only authorized network traffic is allowed.

A.PHYSICAL_PROTECTION

TOE hardware equipment and the required clients/servers are placed in a safe and controllable space. These devices shall be maintained and operated only by authorized personnel.

A.ADMINISTRATORS

The personnel working as authorized administrators are trustworthy and trained for the TOE administration.

A.MANAGEMENT_DEVICE

The administrator uses a secure remote management terminal and server for remote access to the TOE. The client or server is up to date regarding security upgrades and cryptographic support.

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 7.1 of this Security Target.

4.1 Security objectives for the TOE

O.SECURE_COMMUNICATION The TOE shall provide the means to establish the secure communication channels between the TOE and the Management Clients.

O.USER_AUTHENTICATION The TOE shall enforce the user authentication on all user access to the TOE.

O.ACCESS_CONTROL The TOE shall implement a flexible privilege-based authorization framework. Each privilege allows a user to perform certain actions, and the TOE shall ensure that users can only perform actions when they have a privilege that allows them to perform such action.

O.AUDITING The TOE shall enforce logging of user actions and provide auditing capabilities to the audit review privilege.

O.INFORMATION_FLOW_CONTROL The TOE shall ensure that only accept the clients/servers from the accepted network sources to manage the TOE.

4.2 Security objectives for the Operational Environment

OE.TIME The TOE environment shall provide reliable time via trusted NTP service and protect the communication between the TOE and the NTP service.

OE. TRUSTED_NETWORK The TOE, SYSLOG server, SNMP client, TACACS+ server and other OTEs are deployed in controlled environments; at the operator's equipment room in a trusted network. The TOE and the TOE management clients/servers are segregated from the core network and IP management network so only authorized network traffic is allowed.

OE.PHYSICAL_PROTECTION TOE hardware equipment, and the required clients/servers shall be placed in a safe and controllable space. These devices shall be maintained and operated only by authorized personnel.

OE.ADMINISTRATORS The personnel working as authorized administrators shall be trustworthy and thoroughly trained for the TOE administration and will follow the TOE’s user guidance.

OE.MANAGEMENT_DEVICE The TOE administrator shall use a secure remote management terminal and server for remote access to the TOE. The client or server shall be up to date regarding security upgrades and cryptographic support.

5 Security Requirements

5.1 Extended components definition

There are no extended components defined.

5.2 Definitions

The following terms are used in the security requirements:

5.2.1 Subjects:

- **S.User:** the users with access to the TOE and that are responsible for the TOE management and that are connected through the DCN Management network.

5.2.2 Operations

5.2.2.1 User Management Operations

- **OP.lockUnlockUser**: to unlock or lock a user. A locked user is not able to log-in to the TOE;
- **OP.userManagement**: to perform user management functions, which include adding, removing users or modifying user attributes from TOE;
- **OP**.**logReview**: to review the logs generated by the TOE;
- **OP.RuleManagement**: to perform security rule management functions, which include adding, removing or modifying security rules;
- **OP.idleTimeout:** to set the amount of time that a user can remain idle before it is logged out from the TOE.

5.2.3 Objects

- **O.user**: this object includes all information of the user account. The specific fields can be seen in the following section as these are considered security attributes;
- **O.rule**: this object includes all information of the security rule. The specific fields can be seen in the following section as these are considered security attributes;
- **O.setting**: this object includes all information of the security common settings. The specific fields can be seen in the following section as these are considered security attributes.

5.2.4 Security attributes

- **User**
  - **User.username**: User unique identifier;
  - **User.password**: the user password;
  - **User.passwordHistory:** the user password change history;
  - **User.privilegeLevel**: the privilege level of this user (0 ~ 15);
  - **User.rule**: the security rule of the user;
  - **User.isLocked**: this indicates if the user account is locked or not. Only not locked users are allowed to login.
- **Rule**
  - **Rule.passwordExpirationDate**: is the expiration date of user password if used;
  - **Rule.passwordHistoryNumber**: is the history number of the last passwords. When set, the user cannot use the passwords in this password history for when changing the password;
  - **Rule.allowedIPs**: is the list of the allowed source IPs for the user to log-in. If the log-in is requested from other IPs, access is denied;
  - **Rule.allowedWorkSchedule**: is the accepted time schedule for the user to log-in. Outside this timeframe the user is not allowed to log-in to the TOE;
  - **Rule.authenticationAttempts**: is the maximum authentication attempts allowed for the user before locking its account;
  - **Rule.lockedPeriod**: is the period of time that the user account will remain locked.
- **Setting**
  - **Setting.idleTimeout**: is the amount of time that the user can remain idle before it is logged out from the TOE.

5.3 Security Functional Requirements

The following notational conventions are used in the requirements:

- Assignments are indicated in **bold text**;
- Selections are indicated in **bold underlined text**;
- Refinements are indicated with ***bold italic text*** and ~~strikethroughs~~. In general refinements were applied to clarify requirements and/or make them more readable;
- Iterations are indicated by adding three letters to the component name;
- References are indicated with [square brackets].

The SFRs have been divided into five major groups:

- Identification & Authentication
- Authorization & Security Management
- Logging & Auditing
- Trusted Path
- Secure Channel
- Information Flow Control

5.3.1 Identification & Authentication

5.3.1.1 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each ***S.User*** ~~user~~ to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.1.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each ***S.User*** ~~user~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.3.1.3 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within 0 and 16 (Rule.authenticationAttempts, default 5) for NETCONF and SSH interface; within 3 and 16 (default 5) for QX interface** unsuccessful authentication attempts occur related to **S.User authentication**.

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

- **Until is unlocked by the security administrator, or**
- **Until a security administrator configurable time (Rule.lockedPeriod) have passed, if the account has not been set to permanent locking.**

Application Note: The security administrator is an S.User with the privilege level containing the corresponding rights (OP.lockUnlockUser, OP.RuleManagement)

5.3.1.4 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that ~~secrets~~ ***User.password*** meet:

- **At least 8 characters including four types: number, upper case letter, lower case letter, special characters;**

- **Cannot be the same as the username, the username in reverse[4] or a common password dictionary word;**
- **The new password cannot be the same as one of the last (Rule.passwordHistoryNumber) passwords set in User.passwordHistory.**

5.3.1.5 FTA_SSL.3 TSF-initiated termination

- FTA_SSL.3.1 The TSF shall terminate an interactive session after a **period of inactivity that equals the configured time (Setting.idleTimeout).**

5.3.1.6 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~~ ***S.User***.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **3** sessions per ~~user~~ ***S.User***.

5.3.1.7 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ ***S.User***:

- **User.username;**
- **User.password;**
- **User.passwordHistory;**
- **User.privilegeLevel;**
- **User.rule;**
- **User.isLocked.**

[4] If the username is chang, “gnahc” is not allowed

5.3.2 Authorization & Security Management

5.3.2.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **For CLI Interface: Privilege level 0 to 15**
- **For QX interface: all users has privilege level 15**
- **For Netconf interface: User defined roles which can be assigned with different operations.**

Application note: For CLI interface, there are 16 privilege levels. Each privilege level is treated as a distinct role. However, a user can only belong to one privilege level (role). For QX interface, the role is managed by the EMS server.

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

Application note: For CLI interface, the role of a user is identified by his privilege level.

5.3.2.2 FMT_SMF.1 Specification of Management Functions

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

Management function	**Related to SFR**
OP.ruleManagement -> User.Rule.allowedIPs Set whether a user(assigned the rule) can only login from certain IP-addresses, and if so, which IP addresses	**FDP_ACF.1**
OP.idleTimeout -> Setting.idleTimeout Set the time that users may remain logged in while inactive	**FTA_SSL.3**
OP.ruleManagement -> User.Rule.allowedWorkSchedule Set whether a user (assigned the rule) is only allowed to work at certain times, and if so, at which times	**FDP_ACF.1**
OP.ruleManagement -> User.Rule.authenticationAttempts Set the number of allowed unsuccessful authentication attempts	**FIA_AFL.1**
OP.ruleManagement -> User.Rule.lockedPeriod Set the time that an account(assigned the rule) remains	**FIA_AFL.1**

locked	
OP.lockUnlockUser -> User.isLocked Unlock a user account	**FIA_AFL.1**
OP.ruleManagement -> User.Rule.passwordExpirationDate Set whether a user (assigned the rule) password expires after a certain time, and if so, after how long	**FDP_ACF.1**
OP.ruleManagement -> Rule.passwordHistoryNumber Set the length password history that it is maintained to prevent the users from using the same password. E.g. if set to 3, then the users cannot use the last 3 passwords	**FIA_SOS.1**
OP.userManagement -> User.privilegeLevel Assign the privilege level of a user	**FMT_SMR.1**
OP.ruleManagement -> Rule.allowedIPs Configure the accepted management traffic	**FDP_IFF.1**
OP.userManagement Create, edit and delete user accounts	**FIA_ATD.1** **FIA_SOS.1**
OP.logReview Log review	**FAU_SAR.1**

Application Note: Not all management functions are implemented in all TSFIs. Actual implemented functions are described in the guidance documents mentioned in chapter 1.4.1.

5.3.2.3 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the **Privilege-based Access Control Policy** on

- **Subjects:**
  - **S.User**
- **Objects:**
  - **O.user;**
  - **O.rule;**
  - **O.setting.**

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.3.2.4 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Privilege-based Access Control Policy** to objects based on the following:

- **Subjects:**
    - **S.User, with security attributes:**
        - **User.privilegeLevel;**
        - **User.rule;**
        - **User.isLocked;**
- **Objects:**
    - **O.user;**
    - **O.rule;**
    - **O.setting.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **S.User is allowed to perform all operations defined in FMT_SMF.1.1, if and only if the user is authenticated and his User.privilegeLevel has the corresponding operation right;**
- **S.User is allowed to perform OP.logReview, if the user is authenticated and his User.privilegeLevel includes the log view right.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **S.User is locked (User.isLocked is True);**
- **S.User’s User.privilegeLevel does not include the right to perform the operation;**

- **S.User password has expired (current time >= User.rule.passwordExpirationDate);**
- **S.User session has been terminated due to:**
    - **Inactivity (Setting.idleTimeout).**

5.3.2.5 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Access Control Policy** to restrict the ability to **change_default, modify, delete** the security attributes:

- **Rule.passwordExpirationDate**
- **Rule.passwordHistoryNumber**
- **Rule.allowedIPs**
- **Rule.authenticationAttempts**
- **Rule.lockedPeriod**
- **Setting.idleTimeout**
- **User.username**
- **User.password**
- **User.passwordHistory**
- **User.privilegeLevel**
- **User.rule**
- **User.isLocked**

to **S.User**.

5.3.2.6 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **S.User with privilege level 15** to specify alternative initial values to override the default values when an object or information is created.

5.3.3 Logging & Auditing

5.3.3.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TOE shall be able to generate an audit record of the following auditable events:

a) ~~Start-up and shutdown of the audit functions~~;

b) All auditable events for the **not specified** level of audit; and

c) **The following auditable events:**

- **S.User authentication (security log);**
- **OP.lockUnlockUser (security log);**
- **OP.enableDisableUser (operation log);**
- **OP.userManagement (operation log);**
- **OP.ruleManagement (operation log);**
- **OP.idleTimeout (operation log).**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none**.

Application note: Start-up and shutdown of the audit functions is not explicitly logged, however the logging functionality is enabled at start-up and cannot be disabled.

5.3.3.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **S.User with OP.logReview right** with the capability to read **all log records** 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.

5.3.3.3 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.

5.3.3.4 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall **overwrite the oldest stored audit records**[5] and **no other actions** if the audit trail is full.

Application note: Audit records can be exported to a backup server.

[5] The operation was completed to “take no other actions”, and this was subsequently refined away to make the sentence more readable.

5.3.4 Trusted Path

5.3.4.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure.**

FTP_TRP.1.2 The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication and all TOE management functions defined in FMT_SMF.1**.

Application note: This SFR addresses the SSH CLI secure communication where the TOE is acting as the SSH server.

5.3.5 Secure Channel

5.3.5.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **TOE management**.

5.3.6 Information Flow Control

5.3.6.1 FDP_IFC.1 Subset information flow control

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

- **Subjects: Management device;**
- **Information: IP packages;**
- **Operation: accept or deny the IP packages.**

5.3.6.2 FDP_IFF.1 Simple security attributes

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

- **Subject security attributes: IP address, Port number;**

- **Information security attributes: IP protocol, source IP address, source port number, destination IP address, destination port number.**

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:

- **The TOE uses the Access Control List to match the IP packets of the management traffic. If the IP packet match an ACL rule, the TOE discards or accepts the packets based on the action specified in the ACL rule;**
- **An ACL rule is constructed by one or more of the following attributes: IP protocol number, source IP address, source port number, destination IP address, destination port number.**

FDP_IFF.1.3 The TSF shall enforce the **no other information flow control SFP rules**.

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: **none**.

5.4 Security Assurance Requirements

The assurance requirements are EAL3+ALC_FLR.2 and have been summarized in the following table:

Assurance Class	Assurance Components	
	Identifier	Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage

	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.2	Flaw reporting 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.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.5 Security Assurance Requirements Rationale

The Security Assurance Requirements for this Security Target are EAL3+ ALC_FLR.2. The reasons for this choice are that:

- EAL 3 is deemed to provide a good balance between assurance and costs and is in line with ZTE customer requirements.
- ALC_FLR.2 provides assurance that ZTE has a clear and functioning process of accepting security flaws from users and updating the TOE when required. This is also in line with ZTE customer requirements.

6 TOE Summary Specification

This chapter describes how the TOE implements the security functional requirements defined in chapter 5.

6.1 User identification and authentication

The TOE users are required to identify and authenticate themselves before they can perform any action using the TOE. User authentication is based on the username and password provided by the users and has a limited number of attempts before the user account is locked. Users can be unlocked by the security administrator. Users can also wait to be automatically unlocked after a period of time that is configurable by the security administrator.

The TOE maintains user information in order to enforce authentication and access control. The following information is maintained for each user:

- User name and password;
- Password history;
- User privilege level;
- User rules, including expiration date, the length of password history, allowed IPs, allowed authentication time, number of authentication attempts and locked period;
- Locked and enabled status indicators.

User concurrent sessions are limited to:

a maximum 50 for each user in the TOE (with 3 as the default value). Furthermore, except the connections from the QX interface, the sessions are automatically terminated after period of inactivity that is configurable by the security administrator in the TOE.

The security administrator can also restrict the time when a user can be authenticated in the TOE by

1. setting the expiration time of the password of users,
2. managing the activation status of a user (e.g. automatically deactivate a user after N days of inactivity, re-activate a user) and
3. revoking the access right when the user is already logged in.

User passwords have to meet certain rules to ensure that the passwords cannot be easily guessed or broken by brute force:

- The range of the password minimum length is 6~128, and the default recommended value is 8, including four types: number, upper case letter, lower case letter, other characters;
- The password cannot be the same as the username, the username in reverse or a common password dictionary word;
- The new password cannot be the same as one of the last (Rule.passwordHistoryNumber) passwords set in User.passwordHistory.

Locally managed passwords that do not meet these rules are rejected by the TOE.

(FIA_UID.2, FIA_UAU.2, FIA_AFL.1, FIA_ATD.1, FTA_MCS.1, FIA_SOS.1 and FTA_SSL.3)

6.2 Authorization & Security Management

The TOE enforces access control on users based on user privileges and user roles. Each user privilege or role has an allowed set of allowed actions (including various management actions). For QX interface, the TOE does not implement access control. The users from QX interface have the highest privilege level.

Access control also verifies that user information is correct, such as that the user is enabled and not locked, user is not idle, user's password is not expired. The access control on the TOE also checks the user's allowed time interval.

(FMT_SMR.1, FDP_ACC.2, FDP_ACF.1, FMT_SMF.1, FMT_MSA.1 and FMT_MSA.3)

6.3 Logging & Auditing

The TOE generates audit logs to record the following events:

- User authentication;
- Locking or unlocking a user account;
- Enabling or disabling a user account;
- Add, remove or modify a user account;
- Add, remove or modify a user’s rule;

- When a user session is terminated by timeout;

The log records include date and time of event, subject identity (if applicable), and the outcome (success or failure) of the event.

The TOE provides the capability to review the logs to the security administrator of the TOE.

The audit store is protected against manipulation. Log records cannot be edited and can only be deleted by the administrator of the TOE.

The log records overwrite themselves when the log trail is full in the TOE. Nonetheless, the records can be automatically sent to a remote server set on the DCN management network.

(FAU_GEN.1, FAU_SAR.1, FAU_STG.1 and FAU_STG.4)

6.4 Trusted Path

The TOE provides secure interaction between its various parts and between itself and various machines in the environment, so that user data and/or management commands cannot be read or modified in between.

Communication between the TOE and the Management Client is protected by SSH. The supported cryptographic algorithms for each protocol are provided below:

Channel	Security Technology	Algorithms	Key Length
Management Client	SSH	Key exchange is performed using diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 The public key algorithm of the SSH transport	

		implementation are ssh-rsa ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 For data encryption are aes256-ctr aes192-ctr aes128-ctr aes128-gcm aes256-gcm For data integrity protection are hmac-sha2-256 hmac-sha2-512

The TOE can also acted as an SSH client to manage other network elements, as shown in Figure 1. However TOE acting as an SSH client is explicitly excluded from the evaluation scope. For the user who wants to use the TOE to manage other network elements, the communication between the TOE and the managed network element must be protected by the environment as per OE.TRUSTED_NETWORK describes.

(FTP_TRP.1)

6.5 Secure Channel

The TOE provides secure interaction between its various parts and between itself and various machines in the environment, so that user data and/or management commands cannot be read or modified in between.

Communication between the TOE and the Management Client and Server is protected by SSH or TLS. TLS supports mutual authentication.The supported cryptographic algorithms for each protocol are provided below:

Channel	Security Technology	Algorithms	Key Length
Management Client and Server	TLS	ecdhe-rsa-aes-128-gcm-sha256 ecdhe-rsa-aes-256-gcm-sha384	
	SSH	Key exchange is performed using	

		diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 The public key algorithm of the SSH transport implementation are ssh-rsa ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 For data encryption are aes256-ctr aes192-ctr aes128-ctr aes128-gcm aes256-gcm For data integrity protection are hmac-sha2-256 hmac-sha2-512

(FTP_ITC.1)

6.6 Information Flow Control

The TOE enforces the following Management Traffic Policy:

User authentication can be restricted based on the user’s IP address, port number and IP protocol. The administrator can set an allowed IP (or set of IPs) in the ACL rules so the user can only be successfully authenticated by connecting from the allowed IP.

(FDP_IFC.1, FDP_IFF.1)

7 Rationales

7.1 Security Objectives Rationale

Assumptions/Threats	**Objectives**
T.COMMUNICATION_CH	This threat is directly covered by **O.SECURE_COMMUNICATION** as it enforce to use secure communication channels on all communications between the TOE and the Management Clients.
T.UNAUTHENTICATED_USER	This threat is directly covered by **O.USER_AUTHENTICATION** as it enforces user authentication in the TOE.
T.UNAUTHORIZED_ADMIN	This threat is directly covered by **O.USER_AUTHENTICATION** and **O.ACCESS_CONTROL** as these enforce user authentication and authorization based on the user's privilege.
T.UNDETECTED_ACTIVITY	This threat is directly covered by **O.USER_AUTHENTICATION** and **O.AUDITING** as these enforce user authentication and logging of user actions on the TOE.
T.UNKNOWN_SOURCE	This threat is covered by **O.INFORMATION_FLOW_CONTROL** and **OE.TRUSTED_NETWORK** as only authorised users in the secure DCN network can manage the information flow control rules. And the TOE enforces correct management traffic according to the ACL rules.
A.TIME	This assumption is upheld by **OE.TIME**, which directly covers the assumption.
A. TRUSTED_NETWORK	This assumption is upheld by **OE.TRUSTED_NETWORK**, which directly covers the assumption.
A.PHYSICAL_PROTECTION	This assumption is upheld by **OE.PHYSICAL_PROTECTION**, which directly covers the assumption.
A.ADMINISTRATORS	This assumption is upheld by **OE.ADMINISTRATORS**, which directly covers the assumption.
A.MANAGEMENT_DEVICE	This assumption is upheld by **OE.MANAGEMENT_DEVICE**, which directly covers

	the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O.SECURE_COMMUNICATION	This objective is met by: • **FTP_TRP.1** for the secure communication between the TOE and the client; • **FTP_ITC.1** for the secure communication between the TOE and other trusted IT products.
O.USER_AUTHENTICATION	This objective is met by: • User identification and authentication before any action (**FIA_UID.2, FIA_UAU.2**); • Limited user authentication attempts (**FIA_AFL.1**); • Complex user password (**FIA_SOS.1**); • Limitation of user session (**FTA_SSL.3**, **FTA_MCS.1**); • Supporting user configuration (**FMT_SMF.1**).
O.ACCESS_CONTROL	This objective is met by: • User roles (privilege) and attributes implementation (**FIA_ATD.1**, **FMT_SMR.1**); • Enforcing access control based on user privilege and attributes (**FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3**); • Supporting access control configuration (**FMT_SMF.1**).
O.AUDITING	This objective is met by: • Audit data generation (**FAU_GEN.1**) • Audit data protection (**FAU_STG.1, FAU_STG.4**); • Supporting audit data review (**FAU_SAR.1, FMT_SMF.1**).
O.INFORMATION_FLOW_CONTROL.	This objective is met by: • Information flow control (**FDP_IFC.1, FDP_IFF.1**)

7.3 Dependencies

SFR	Dependency	Coverage
FIA_UID.2	None.	None.
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_AFL.1	FIA_UAU.2	FIA_UAU.2
FIA_SOS.1	None.	None.
FTA_SSL.3	None.	None.
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FAU_GEN.1	FPT_STM.1	N/A. See below
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FTP_TRP.1	None.	None.
FTP_ITC.1	None.	None.
FIA_ATD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1

	FMT_MSA.3	FMT_MSA.3

FPT_STM.1 cannot be implemented by the TOE because it does not have the capability to generate reliable time stamps, therefore the time information is provided by a NTP server in the TOE network (OE.TIME).

A Correspondence between hardware models and software packages

ZXONE 9700 Series	
Hardware models	**Software packages**
ZXONE 9700 S3K ZXONE 9700 NX41 ZXONE 9700 OX42	• ZXONE19700V1.10.010.002B500_@M4NCPM-REL-221124.set • ZXONE19700V1.10.010.002B500CP001_@NCPM-M4.set • ZXONE19700V1.10.010.002B500CP002_@NCPM-M4.set • ZXONE19700V1.10.010.002B500CP003_@NCPM-M4.set
ZXONE 9700 G2K	• ZXONE19700V1.10.010.002B500_@M2NCPQ-REL-221124.set • ZXONE19700V1.10.010.002B500CP001_@NCPQ-M2.set • ZXONE19700V1.10.010.002B500CP002_@NCPQ-M2.set • ZXONE19700V1.10.010.002B500CP003_@NCPQ-M2.set
ZXONE 9700 NXG0 ZXONE 9700 NXG1	• ZXONE19700V1.10.010.002B500_@SNPG-REL-221128.set • ZXONE19700V1.10.010.002B500CP001_@SNPG.set • ZXONE19700V1.10.010.002B500CP002_@SNPG.set

Table 1 ZXONE 9700 software packages and hardware models correspondence

ZXONE 7000 Series	
Hardware model	**Software packages**
ZXONE 7000 C2	• ZXONE7000V2.00R5B111.set, • ZXONE7000V2.00R5B111_C01.set, • ZXONE7000V2.00R5B111_C02.set

Table 2 ZXONE 7000 software packages and hardware models correspondence

ZXMP M721 Series	
Hardware models	**Software packages**
ZXMP M721 CX66A(E)	• ZXMPM721V5.10.070.001B100_@NCPLC-REL-221128.set • ZXMPM721V5.10.070.001B100CP001_@NCPLC-REL.set • ZXMPM721V5.10.070.001B100CP002_@NCPLC-REL.set

ZXMP M721 CX63A(E)	• ZXMPM721V5.10.070.001B100_@NCPLE-REL-221125.set • ZXMPM721V5.10.070.001B100CP001_@NCPLE-REL.set • ZXMPM721V5.10.070.001B100CP002_@NCPLE-REL.set
ZXMP M721 DX63(E)	• ZXMPM721V5.10.070.001B100_@NCP(E)-REL-221125.set • ZXMPM721V5.10.070.001B100CP001_@NCP(E)-REL.set • ZXMPM721V5.10.070.001B100CP002_@NCP(E)-REL.set,

Table 3 ZXMP M721 software packages and hardware models correspondence

B The different TOEs

The different TOEs can be distinguished by capacity (number of ports/cards) and by the protocols they support.

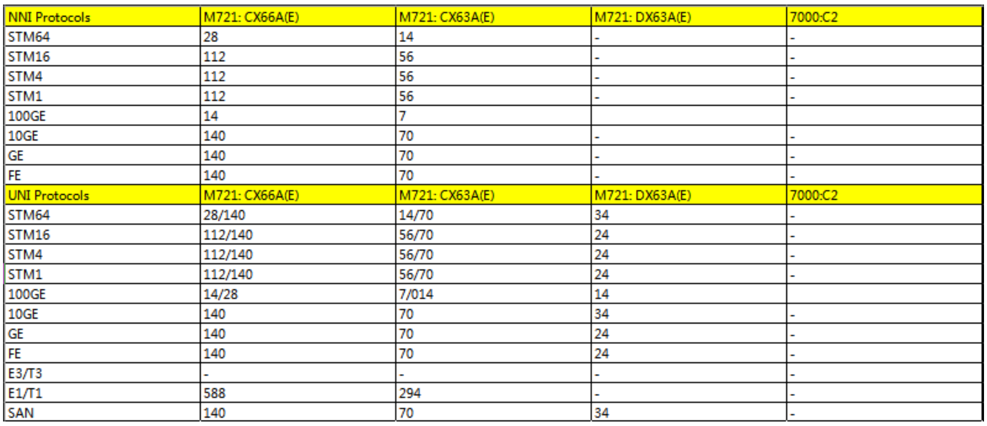
The management interfaces supported by the TOEs are listed in Table 3

Table 3: Supported interfaces

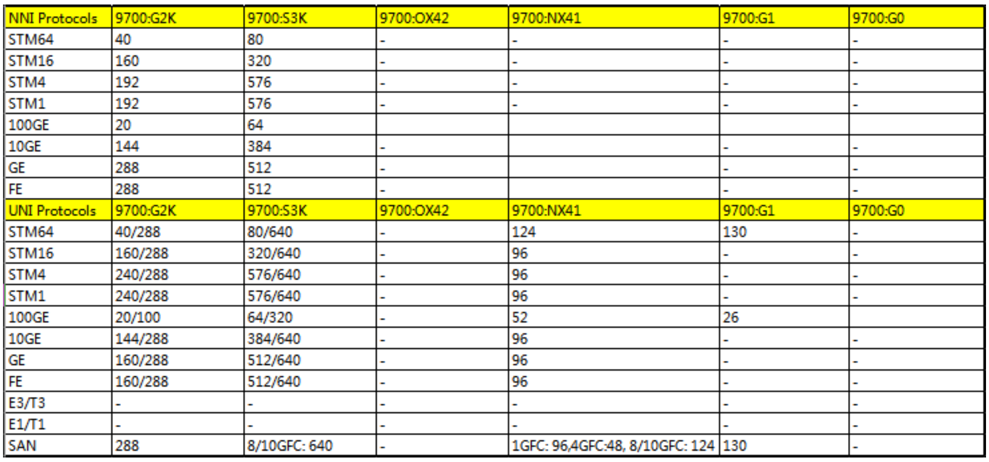
TOE Series	**TSFI**				
	NETCONF	QX	SSH	SFTP	TACACS+
ZXONE 9700 Series	Not Supported	Support	Support	Support	Support
ZXMP M721 Series	Not Supported	Support	Support	Support	Support
ZXONE 7000 Series	Support	Not Supported	Support	Support	Support

The protocols supported by the OTN TOEs are listed in Table 4. These are divided into NNI Protocols (to the OTN Network) and UNI protocols (to Client-Side Equipment.

Table 4: OTN Protocols



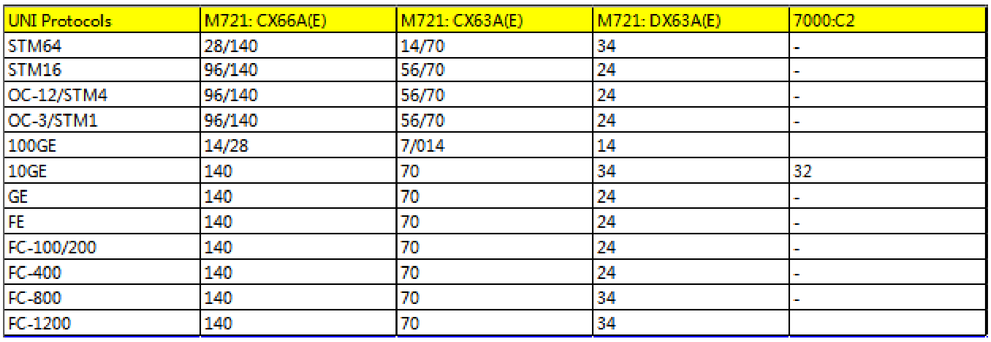
NNI Protocols	M721: CX66A(E)	M721: CX63A(E)	M721: DX63A(E)	7000:C2
STM64	28	14	-	-
STM16	112	56	-	-
STM4	112	56	-	-
STM1	112	56	-	-
100GE	14	7		
10GE	140	70	-	-
GE	140	70	-	-
FE	140	70	-	-
UNI Protocols	M721: CX66A(E)	M721: CX63A(E)	M721: DX63A(E)	7000:C2
STM64	28/140	14/70	34	-
STM16	112/140	56/70	24	-
STM4	112/140	56/70	24	-
STM1	112/140	56/70	24	-
100GE	14/28	7/014	14	
10GE	140	70	34	-
GE	140	70	24	-
FE	140	70	24	-
E3/T3	-	-	-	-
E1/T1	588	294	-	-
SAN	140	70	34	-



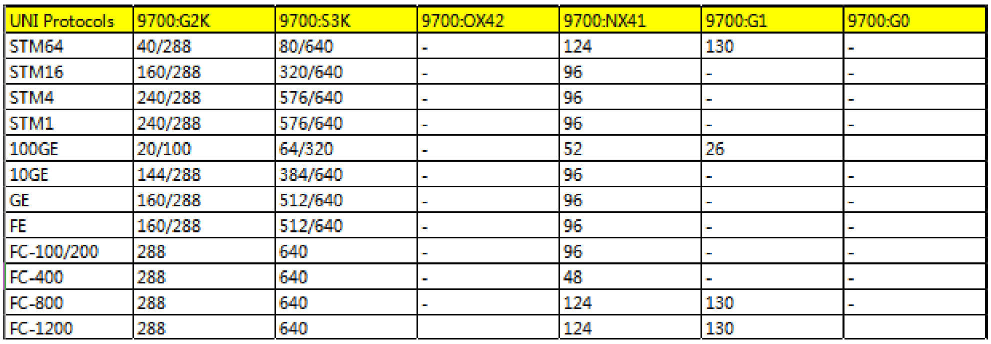
NNI Protocols	9700:G2K	9700:S3K	9700:OX42	9700:NX41	9700:G1	9700:G0
STM64	40	80	-	-	-	-
STM16	160	320	-	-	-	-
STM4	192	576	-	-	-	-
STM1	192	576	-	-	-	-
100GE	20	64				
10GE	144	384	-		-	-
GE	288	512	-		-	-
FE	288	512	-		-	-
UNI Protocols	9700:G2K	9700:S3K	9700:OX42	9700:NX41	9700:G1	9700:G0
STM64	40/288	80/640	-	124	130	-
STM16	160/288	320/640	-	96	-	-
STM4	240/288	576/640	-	96	-	-
STM1	240/288	576/640	-	96	-	-
100GE	20/100	64/320	-	52	26	
10GE	144/288	384/640	-	96	-	-
GE	160/288	512/640	-	96	-	-
FE	160/288	512/640	-	96	-	-
E3/T3	-	-	-	-	-	-
E1/T1	-	-	-	-	-	-
SAN	288	8/10GFC: 640	-	1GFC: 96,4GFC:48, 8/10GFC: 124	130	-

The protocols supported by the WDM TOEs are listed in Table 5. Each protocol can be used for connecting to Client-Side Equipment or WDM network equipment.

Table 5: WDM Protocols



UNI Protocols	M721: CX66A(E)	M721: CX63A(E)	M721: DX63A(E)	7000:C2
STM64	28/140	14/70	34	-
STM16	96/140	56/70	24	-
OC-12/STM4	96/140	56/70	24	-
OC-3/STM1	96/140	56/70	24	-
100GE	14/28	7/014	14	
10GE	140	70	34	32
GE	140	70	24	-
FE	140	70	24	-
FC-100/200	140	70	24	-
FC-400	140	70	24	-
FC-800	140	70	34	-
FC-1200	140	70	34	



UNI Protocols	9700:G2K	9700:S3K	9700:OX42	9700:NX41	9700:G1	9700:G0
STM64	40/288	80/640	-	124	130	-
STM16	160/288	320/640	-	96	-	-
STM4	240/288	576/640	-	96	-	-
STM1	240/288	576/640	-	96	-	-
100GE	20/100	64/320	-	52	26	
10GE	144/288	384/640	-	96	-	-
GE	160/288	512/640	-	96	-	-
FE	160/288	512/640	-	96	-	-
FC-100/200	288	640	-	96	-	-
FC-400	288	640	-	48	-	-
FC-800	288	640	-	124	130	-
FC-1200	288	640		124	130	

C List of Acronyms

ACL	Access Control Level
CC	Common Criteria
CM	Customer Management
DCN	Data Communications Network
DST	Daylight Saving Time
EMS	Equipment Management System
ICT	Information and Communications Technology
IP	Internet Protocol
MAC	Media Access Control
NMS	Network Management System
NNI	Network-to-network Interface
NTP	Network Time Protocol
OTE	Optical Transmission Equipment
OTN	Optical Transmission Network
PC	Personal Computer
PP	Protect Profile
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
UME	Unified Management Expert

UNI	User Network Interface
VLAN	Virtual Local Area Network
WDM	Wave Division Multiplexing
WDM	Wavelength Division Multiplexing

D References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017

[AIS20] Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Version 2.0, 2 December 1999

[FIPS 180-4] FIPS PUB 180-4 – Secure Hash Standard (SHS)

[FIPS 186-4] FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013

[FIPS 197] FIPS PUB 197 – Advanced Encryption Standard (AES), November 26, 2001

[FIPS 198-1] FIPS PUB 198-1 - The Keyed-Hash Message Authentication Code (HMAC), July 2008

[NIST SP800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001

[NIST SP800-38D] NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[NIST SP800-56A] NIST Special Publication 800-56A Rev. 3 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[NIST SP800-56B] NIST Special Publication 800-56B Rev. 2 – Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, July 2018

[NIST SP800-90A] NIST Special Publication 800-90A Rev. 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[PKCS#1 V2.1] PKCS #1 v2.1: RSA Cryptography Standard, April 2004

[PKCS#3] PKCS #3: Diffie-Hellman Key- Agreement Standard, version 1.4, November 1993

[RFC 1321] The MD5 Message-Digest Algorithm, R. Rivest, April 1992

[RFC 2104] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC 3268] *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*, P. Chown, June 2002

[RFC 3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, Version 2.1, J. Jonsson, B. Kaliski, 2003-02-01

[RFC 3526] RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), May 2003

[RFC 4251] RFC 4251 – The Secure Shell (SSH) Protocol Architecture, January 2006

[RFC 4252] RFC 4252 - The Secure Shell (SSH) Authentication Protocol, January 2006

[RFC 4253] RFC 4253 - The Secure Shell (SSH) Transport Layer Protocol, January 2006

[RFC 4254] RFC 4254 - The Secure Shell (SSH) Connection Protocol, January 2006

[RFC 4344] The Secure Shell (SSH) Transport Layer Encryption Modes, M. Bellare, T. Kohno, C. Namprempre, 2006-01-01

[RFC 4346] RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[RFC 5246] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

[RFC 5288] AES Galois Counter Mode (GCM) Cipher suited for TLS, J. Salowey, A. Choudhury, D. McGrew 2008-08-01

[RFC 5289] TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), August 2008

[RFC 8439] ChaCha20 and Poly1305 for IETF Protocols, June 2018

[RFC 6655] AES-500CCM Cipher Suites for Transport Layer Security (TLS), July 2012

[RFC 5116] An Interface and Algorithms for Authenticated Encryption, January 2008

[RFC 8018] PKCS #5: Password-Based Cryptography Specification Verion 2.1, B. Kaliski, 2017-01-01

[RFC 8446] RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3, August 2018