ZTE Access System Series
Security Target

ZXA10 C300M/C350M, ZXMSG 5200/5208,
FSAP 9800, ZXDSL 9806H/9816/9836

Date	April 25, 2012
Authors	She Zuoliang (ZTE) Dirk-Jan Out (Brightsight)
Version	1.0

ZTECORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

Document history

Version	Date	Comment
0.1	October 10, 2011	First version
0.2	November 15, 2011	Processed ZTE comments, added functionality.
0.3	November 16, 2011	Clarified where different systems are, added EMS
0.4	December 28, 2011	Confirmed TOE name and versions. Submitted to SERTIT.
0.5	January 25, 2012	• Corrected spelling mistakes in Physical Scope • Showed in FIA_UAU.2 that TACACS+/RADIUS is not available on all TOEs • Removed 9806H v3.0, as it will not be ready in time • Reformulated the section on xPON in 1.2.1 to make it more readable • Modified FIA_UAU.2 to clarify that TACACS+ and RADIUS server are not part of the TOE • Replaced Appendix A with a more readable version • Added List of Abbreviations in Appendix B • Changed the nuber of login options from “two” to “four” in 1.3.1, as it caused confusion • Removed sentence “Other options were not evaluated” from 1.3.1. as it duplicated the previous sentence. • Introduced Management network, to clarify the role of TA.NETWORK
0.6	February 13, 2012	• Modified the table in 1.1. to better reflect broadband/narrowband support. • Updated the table in 1.3.1 to remain consistent with table in 1.1. • Corrected “CC Security Manual” to “Security Issues”in the table in 1.3.1 • Corrected that all TOEs have RADIUS support, and some have TACACS+ support (instead of some have TACACS+ and RADIUS support) • Made a slight clarification of RADIUS/TACACS+ support in the TSS
0.7	February 23, 2012	• Adapted ST to reflect that FSAP 9800 V1.0.6P9 does not support SSH.
0.8	March 29, 2012	• Adapted ST to correct the TOE version • Adapted ST to reflect that FSAP 9800 v1.0.6P9 does not support RADIUS • Update table in Appendix A
0.9	April 2, 2012	• Update table in Appendix A • Fix misplacement of 9806H
1.0	April 25, 2012	• Final, change the format for the public release.

References

[CCp1] Common Criteria for IT Security Evaluation, Part 1, v3.1r3, July 2009

[CCp2] Common Criteria for IT Security Evaluation, Part 2, v3.1r3, July 2009
[CCp3] Common Criteria for IT Security Evaluation, Part 3, v3.1r3, July 2009
[CEMe] Common Methodology for IT Security Evaluation, v3.1r3, July 2009

Content

1 ST Introduction 5
1.1 ST and TOE References 5
1.2 TOE Overview and usage 6
1.2.1 Major security features 7
1.2.2 Non-TOE Hardware/Software/Firmware 7
1.3 TOE Description 8
1.3.1 Physical scope 8
1.3.2 Logical scope 11

2 Conformance Claims 12

3 Security Problem Definition 13
3.1 Organisational Security Policies 13
3.2 Threats 13
3.2.1 Assets and threat agents 13
3.2.2 Threats 14
3.3 Assumptions 14

4 Security Objectives 15
4.1 Security objectives for the TOE 15
4.2 Security objectives for the Operational Environment 16

5 Security Requirements 17
5.1 Extended components definition 17
5.2 Definitions 17
5.3 Security Functional Requirements 18
5.3.1 Management 18
5.3.2 Separation 19
5.4 Security Assurance Requirements 20
5.5 Security Assurance Requirements Rationale 21

6 TOE Summary Specification 22

7 Rationales 23
7.1 Security Objectives Rationale 23
7.2 Security Functional Requirements Rationale 25
7.3 Dependencies 26

A Supported Protocols 27

B List of Acronyms 28

1 ST Introduction

1.1 ST and TOE References

This is version 1.0 of the Security Target for the ZTE Access System Series.

The term ZTE Access System refers to the collective of:

Name	Type	SW Platform
ZXMSG 5208 V1.0.1	Narrowband and broadband	ZXMAP 2.0 Linux (2.6.21.7)
ZXDSL 9806H V1.2P20	Broadband only	
ZXDSL 9806H V2.1P5	Narrowband and broadband	
ZXDSL 9816 V2.0.0		
ZXDSL 9836 V1.0.0P1		
ZXA10 C300M V2.1T5		ZXIAP v1.2 ZXROS 04.08.01 Vxworks 5.5.1
ZXA10 C350M V2.1T5		
ZXMSG 5200 V3.2P03T2		
FSAP 9800 V3.2P3	Broadband only	
FSAP 9800 V1.0.6P9		Vxworks 5.4

Each of these is considered a TOE. The major differences between TOEs are the type, the physical interfaces (various types of broadband and narrowband), and the capacity. See Appendix A of this Security Target for details.

1.2 TOE Overview and usage

The TOE is an Access System, which regulates the access between:

- networks, like a provider IP network or the PSTN
- subscribers, who wish to access these networks.

The TOE is depicted in Figure 1:

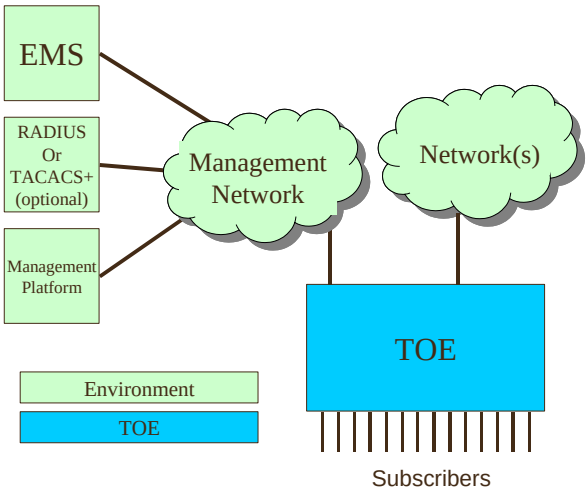

Figure 1: The TOE

The subscribers can access the TOE through a wide variety of technologies, like POTS, ISDN, xDSL, FE/GE and xPON. The exact technologies depend on the particular TOE. See Appendix A for details on the:

- specific network technologies
- specific subscriber access technologies

that are supported by each TOE.

The TOE has the following general functionalities[1]:

- Provide access of subscribers to networks (and vice versa)
- Convert the protocols used by the subscribers to protocols suitable for the networks (and vice versa)
- Allow management of itself through a Management Network

[1] Not all TOEs offer the same functionality. See Appendix A for details.

1.2.1 Major security features

The TOE:

- Provides secure management of itself, to ensure that only properly authorized staff can manage the TOE
- Ensures that subscribers have only access to the networks and functionalities/entities on those networks that they are entitled to
- Ensures that subscribers cannot read traffic from/to other subscribers
- Ensures that subscribers cannot modify traffic from/to other subscribers

Note that the TOE offers access to different subscribers through a set of physical ports. In many cases, there will be a 1:1 relation between subscribers and ports, but it is allowed to have multiple subscribers to a single port:

- If this port is based on xPON technology, the TOE will be able to protect subscribers from each other by:
  - Encrypting data downstream so that only a specific subscriber can read it
  - Using TDM upstream, so each subscriber has his own time-slice to send data
- If this port uses a different protocol (e.g. FE/GE), the TOE itself will not protect subscribers on that port against each other, and, if required, they should take care of this protection themselves (e.g. by using cryptography).

1.2.2 Non-TOE Hardware/Software/Firmware

The TOE requires:

- networking connectivity, both to the Management Network, its upstream networks and to its subscribers.
- A platform for management of the TOE (connected to the Management Network) running:
  - telnet (RFC 854-861) for the FSAP 9800 V1.0.6P9
  - SSH (RFC 4250-4256) for all other TOEs
- (Optional) An authentication server (connected to the Management Network), either:
  - A RADIUS Server that supports RFC 2865 (Authentication & Authorization) and RFC 2866 (Accounting) for RADIUS
  - A TACACS+ Server (connected to one of the Networks) that supports TACACS+ Version 1.78（DRAFT);
- An EMS (connected to the Management Network). The EMS can also be used to manage the TOE, but this option was not evaluated.

1.3 TOE Description

1.3.1 Physical scope

ZXMSG5200 V3.2P03T2	
Hardware	ZXMSG 5200
Software	MSG5200 V3.2P03T2 ZXIAP v1.2 ZXROS 04.08.01 Vxworks (5.5.1)
Guidance	ZXMSG 5200(V3.2) Configuration Manual (CLI) ZXMSG 5200(V3.2) Maintenance Manual ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume I ZXMSG 5200(V3.2) Configuration Manual (NetNumen) Volume II ZXMSG 5200 (V3.2) Security Issues
C300M V2.1T5	
Hardware	ZXA10 C300M
Software	MSG_6000 V2.1T5 ZXIAP v1.2 ZXROS 04.08.01 Vxworks (5.5.1)
Guidance	ZXA10 C300M(V2.1) Multi-service Access Equipment Configuration Manual (CLI) ZXA10 C300M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen) ZXA10 C300M(V2.1) Multi-service Access Equipment Maintenance Manual ZXA10 C300M(V2.1) Security Issues
C350M V2.1T5	
Hardware	ZXA10 C350M
Software	MSG_6000 V2.1T5 ZXIAP v1.2 ZXROS 04.08.01 Vxworks (5.5.1)
Guidance	ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (CLI) ZXA10 C350M(V2.1) Multi-Service Access Equipment Configuration Manual (NetNumen) ZXA10 C350M(V2.1) Multi-Service Access Equipment Routine Maintenance Manual ZXA10 C350M(V2.1) Security Issues
ZXMSG 5208 V1.0.1	
Hardware	ZXMSG 5208
Software	ZXMSG 5208 V1.0.1

	ZXMAP 2.0 Linux 2.6.21.7
Guidance	ZXMSG 5208(V1.0) Feature Guide ZXMSG 5208(V1.0) Configuration Manual (NetNumen) ZXMSG 5208(V1.0) Command Reference (Volume I) ZXMSG 5208(V1.0) Command Reference (Volume II) ZXMSG 5208(V1.0) Command Reference (Volume III) ZXMSG 5208(V1.0) Security Issues
FSAP 9800 V1.0.6P9	
Hardware	FSAP 9800
Software	9800 V1.0.6P9 Vxworks (V5.4)
Guidance	FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (CLI) FSAP 9800 (V1.0.6) Full Service Access Platform Operation Manual (NetNumen) FSAP 9800 (V1.06) Full Service Access Platform Maintenance Manual FSAP 9800 (V1.06) Security Issues
FSAP 9800 V3.2P3	
Hardware	FSAP 9800
Software	9800 V3.2P3 ZXIAP v1.2 ZXROS 04.08.01 Vxworks (5.5.1)
Guidance	FSAP 9800 (V3.2) Full Service Access Platform Maintenance Manual.pdf FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (CLI) FSAP 9800 (V3.2) Full Service Access Platform Operation Manual (NetNumen) FSAP 9800 (V3.2) Security Issues
ZXDSL 9806H V1.2P20	
Hardware	ZXDSL 9806H
Software	ZXDSL 9806H V1.2P20 ZXMAP 2.0 Linux 2.6.21.7
Guidance	ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume I) ZXDSL 9806H (V1.2) ZTE Broadband Universal Access System User Manual (Volume II) ZXDSL 9806H (V1.2) Security Issues
ZXDSL 9806H V2.1P5	
Hardware	ZXDSL 9806H
Software	ZXDSL 9806H V2.1P5 ZXMAP 2.0 Linux 2.6.21.7

Guidance	ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(CLI) ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Configuration Manual(NetNumen) ZXDSL 9806H (V2.1) ZTE Broadband Universal Access System Maintenance Manual ZXDSL 9806H (V2.1) Security Issues
ZXDSL 9816 V2.0.0	
Hardware	ZXDSL 9816
Software	ZXDSL 9816 v2.0.0 ZXMAP 2.0 Linux 2.6.21.7
Guidance	ZXDSL 9816(V2.0) Configuration Manual (CLI) ZXDSL 9816(V2.0) Configuration Manual (NetNumen) ZXDSL 9816(V2.0) Security Issues
ZXDSL 9836 V1.0.0P1	
Hardware	ZXDSL 9836
Software	ZXDSL 9836 v1.0.0P1 ZXMAP 2.0 Linux 2.6.21.7
Guidance	ZXDSL 9836(V1.0) Command Reference (Volume I).pdf ZXDSL 9836(V1.0) Command Reference (Volume II).pdf ZXDSL 9836(V1.0) Command Reference (Volume III).pdf ZXDSL 9836(V1.0) Hardware Description.pdf ZXDSL 9836(V1.0) Maintenance Manual.pdf ZXDSL 9836(V1.0) Product Description.pdf ZXDSL 9836(V1.0) Security Issues

1.3.2 Logical scope

The logical scope of the TOE consists of the following functionalities:

- Provides secure management of itself, to ensure that only properly authorized staff can manage the TOE
- Ensures that subscribers have only access to the services on the networks that they are entitled to
- Ensures that subscribers cannot read traffic from/to other subscribers
- Ensures that subscribers cannot modify traffic from/to other subscribers

Secure management of the TOE, to ensure that only properly authorized staff can manage the TOE.

There are four ways of managing the TOE:

- Graphically, through an EMS (over the Management network).
- Text-based:
  - Over telnet (over the Management Network)
  - Through a local connection (Hyper Terminal over RS-232)
  - Over SSH over the Management Network, possibly extended with RADIUS or TACACS+

Only the following options were evaluated:

- telnet, for the FSAP 9800 V1.0.6P9
- SSH, possibly extended with RADIUS or TACACS+) for all other TOEs.

Ensures that subscribers have only access to the services on the networks that they are entitled to

The TOE can be configured to provide fine-grained access control: ensuring that each subscriber has only access to the exact services that he is entitled to.

Ensures that subscribers cannot read traffic from/to other subscribers Ensures that subscribers cannot modify traffic from/to other subscribers

The TOE provides separation between the traffic streams of subscribers so that unauthorized disclosure/modification is prevented.

2 Conformance Claims

This ST conforms to:

- CC, version 3.1R3, as defined by [CCp1], [CCp2], [CCp3] and [CEMe].
- CC Part 2 as CC Part 2 extended
- CC Part 3 as CC Part 3 conformant

This ST conforms to no Protection Profile.
This ST conforms to EAL 2+ALC_FLR.2, and to no other packages.

3 Security Problem Definition

3.1 Organisational Security Policies

None

3.2 Threats

3.2.1 Assets and threat agents

The assets are:

1. The ability of administrators to manage various aspects of the TOE securely
2. Access to certain networks and/or entities/services on those networks
3. Confidentiality and integrity of communication between subscribers and networks

These assets are threatened by the following threat agents:

1. TA.SUBSCRIBER A Subscriber
2. TA.NETWORK An attacker with access to the Management Network[2]
3. TA.PHYSICAL An attacker with physical access to the TOE

[2] This attacker does not exist for FSAP 9800 V1.06P9. See A_TRUSTED_ NETWORK

3.2.2 Threats

The combination of assets and threats gives rise to the following threats:

T.UNAUTHORISED_ADMIN[3]
TA.NETWORK or TA.SUBSCRIBER gains access to the management functionality of the TOE.

T.UNAUTHORISED_ACCESS
TA.SUBSCRIBER gains access to a service on a Network that he is not authorized to access

T.PHYSICAL_ATTACK
TA.PHYSICAL gains physical access to the TOE and is able to perform actions on the TOE.

T.CONFIDENTIALITY
TA.SUBSCRIBER is able to read traffic from/to another subscriber

T.INTEGRITY
TA.SUBSCRIBER is able to modify traffic from/to another subscriber

3.3 Assumptions

This Security Target uses one assumption:

A.TRUSTED_NETWORK (for FSAP 9800 V1.0.6P9)
It is assumed that the Network(s) (including the Management Network) are trusted, such that they will not interfere with subscriber and/or management traffic. It is also assumed that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

A.TRUSTED_NETWORK (for all other TOEs)
It is assumed that the Network(s) (except the Management Network) are trusted, such that they will not interfere with subscriber traffic. It is also assumed that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

[3] As TA.NETWORK does not exist for the FSAP 9800 V1.06P9: for this TOE only TA.SUBSCRIBER is relevant.

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. ACCESS
The TOE shall ensure that subscribers have only access to the services on the networks that they are entitled to.

O.MANAGE_ACCESS
The TOE shall offer administrators the possibility to modify the access that subscribers have to networks.

O.AUTHENTICATE_ADMIN
The TOE shall identify and authenticate administrators before allowing them access to administrative functions.

O.ENCRYPTED_MANAGEMENT (not relevant for FSAP 9800 V1.0.6P9)
The TOE shall offer an encrypted channel for administrative actions, preventing disclosure, insertion and/or modification of administrative commands.

O. SEPARATION_OF_PORTS
The TOE shall offer physical ports, and be able to separate traffic between different ports, such that:

- It is not possible to listen in on traffic from one port on a different port
- It is not possible to modify traffic on one port from another port

O. xPON (only on TOEs offering xPON)
THE TOE shall offer physical xPON ports to subscribers, such that:

- It is not possible for one subscriber on a xPON port to listen in on traffic from/to other subscribers on that xPON port
- It is not possible for one subscriber on a XPON port to modify traffic from/to other subscribers on that xPON port

4.2 Security objectives for the Operational Environment

OE.PHYSICAL_SECURITY
The operator shall ensure that the TOE shall be protected from physical attacks.

OE.MULTIPLE_SUBSCRIBERS
Where multiple subscribers are connected to a single non-xPON port, and it is desired that the confidentiality and/or integrity of traffic from/to a subscriber shall be protected from other subscribers, this must be arranged by the environment.

OE.TRUSTED_NETWORK (for FSAP 9800 V1.0.6P9)
The environment shall ensure that the Network(s) are trusted (including the Management Network), such that they will not interfere with subscriber and./or management traffic and that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

OE.TRUSTED_NETWORK (for all other TOEs)
The environment shall ensure that the Network(s) are trusted (except the Management Network), such that they will not interfere with subscriber traffic and that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.

5 Security Requirements

5.1 Extended components definition

None.

5.2 Definitions

The following terms are used in the security requirements:

Roles:

- Administrator

Subjects/External Entities

- Services (on a Network)
- Ports (any physical Port to a subscriber)
- xPON Port (a virtual Port to an xPON subscriber)[4]

Objects:

- Traffic

Operations:

- Receive
- Send
- Modify

None of the subjects or objects have attributes.

[4] Note that a Port is a physical port, while an xPON port is a virtual port: one port supporting xPON can support many xPON ports. Ports are physically separated, while xPON ports are cryptographically and separated from each other by TDM.

5.3 Security Functional Requirements

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.

5.3.1 Management

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **Administrator**

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each ***Administrator*** to be successfully identified ***by username*** before allowing any other TSF-mediated ***Administrator*** actions on behalf of that ***Administrator***.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each ***Administrator*** to be successfully authenticated

- ***by password***
- ***through a non-TOE RADIUS server (when so configured)***
- ***through a non-TOE TACACS+ server (when so configured)*** [5]

before allowing any other TSF-mediated ***Administrator*** actions on behalf of that ***Administrator***.

FMT_SMF.1 Specification of Management Functions

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

OMM Management function	Related to SFR
Change Administrator username	FIA_UID.2
Change Administrator password	FIA_UAU.2
Manage the Traffic Policy Rules	FDP_IFF.1

FTP_ITC.1 Inter-TSF trusted channel (not relevant for FSAP 9800 V1.0.6P9)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and ***an SSH-client*** that is logically distinct from other communication channels and provides assured identification of its

[5] Not supported on MSG5208, ZXDSL 9806H, 9816 and 9836 TOEs

end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit the ***SSH-client*** to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall **not**[6] initiate communication via the trusted channel.

5.3.2 Separation

FDP_IFC.1 Subset information flow control
FDP_IFC.1.1 The TSF shall enforce the **Traffic Policy** on

- **Ports, xPON Ports**[7]
- **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, xPON Ports**[8]
- **Traffic**

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:

- **Ports and xPON Ports can Receive Traffic from a Service, if so allowed by the Traffic Policy rules**
- **Ports and xPON Ports cannot Receive Traffic not destined for that port**
- **Ports and xPON Ports can Send Traffic to a Service, if so allowed by the Traffic Policy rules**
- **Ports and xPON Ports cannot Modify Traffic on other Ports or xPON Ports**

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

[6] A refinement for readability.
[7] Only MSG5200, C300M and C350M support xPON Ports.
[8] Only MSG5200, C300M and C350M support xPON Ports.

5.4 Security Assurance Requirements

The assurance requirements are EAL2+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.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	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.1	Evidence of coverage
	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 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 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.
- The refinements are derived from ZTE customer requirements as well.

6 TOE Summary Specification

FMT_SMR.1, FIA_UID.2, FIA_UAU.2, FPT_ITC.1

Administrators can only login on the TOE by using a ssh-client[9]. They can then login through a standard username/password mechanism, and all the communication between TOE and ssh-client is encrypted through ssh.

Optionally, the login procedure can be handled through a TACACS+ or RADIUS server (where supported by the TOE). This will still result in an encrypted ssh-session.

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, which switches the communication from Subscribers to Networks and vice versa.
- The TOE supports VLANs, to ensure that certain ports can only talk to certain networks.
- The TOE supports L2 Isolation, preventing ports in the same VLAN from communicating with each other, thus preventing ports from talking to erach other directly (they can then only talk through each other via an entity in one of the Networks)
- The TOE supports ACL rules, both on Layer 2 (Ethernet) and Level 3 (IP), allowing fine-grained access control on MAC-address (source and destination), IP (source and destination) and ports.
- The TOE provides MAC Source Guard, IP/MAC binding, DHCP snooping and DHCP IP Source Guard to prevent subscribers from modifying their own MAC and or IP addresses to circumvent the ACL rules
- For xPON the TOE provides downstream encryption and upstream time-division multiplexing as per the EPON and GPON standards.

FMT_SMF.1

The TOE allows an administrator to manage:

- The usernames/passwords of administrators
- Manage the ACL-rules

through a command-line based interface.

[9] There are other ways, but these are not available in the evaluated configuration (see 1.3.2).

7 Rationales

7.1 Security Objectives Rationale

Assumptions/OSPs/Threats	Objectives
T.UNAUTHORISED_ADMIN TA.NETWORK or TA.SUBSCRIBER gains access to the management functionality of the TOE.	For FSAP 9800 V1.0.6P9 (which requires a secure management network), this threat is countered by: • O.AUTHENTICATE_ADMIN, ensuring that only authorized administrators shall gain access to the management functionality. •
	For all other TOEs (which do not require a secure management network), this threat is countered by: • O.AUTHENTICATE_ADMIN, ensuring that only authorized administrators shall gain access to the management functionality. • O.ENCRYPTED_MANAGEMENT, ensuring that the connection between administrator and TOE is secure
T.UNAUTHORISED_ACCESS TA.SUBSCRIBER gains access to a service on a network that he is not authorized to access	This threat is countered by: • O.ACCESS, regulating access to networks and\ • O.MANAGE_ACCESS, ensuring that administrators can regulate this access
T.PHYSICAL_ATTACK TA.PHYSICAL gains physical access to the TOE and is able to perform actions on the TOE.	This threat is countered by OE.PHYSICAL_SECURITY, preventing attackers physical access to the TOE.
T.CONFIDENTIALITY T.SUBSCRIBER is able to read traffic from/to another subscriber	This threat is countered by: • O.SEPARATION_OF_PORTS, where there is a 1:1 relation between ports and subscribers • O.xPON for xPON ports with multiple subscribers per port • OE.MULTIPLE_SUBSCRIBERS for other ports with multiple subscribers As these three cases cover all possibilities, these security objectives counter the threat.
T.INTEGRITY T.SUBSCRIBER is able to modify traffic from/to another subscriber	This threat is countered by: • O.SEPARATION_OF_PORTS, where there is a 1:1 relation between ports and subscribers • O.xPON for xPON ports with multiple subscribers per port • OE.MULTIPLE_SUBSCRIBERS for other ports with multiple subscribers

	As these three cases cover all possibilities, these security objectives counter the threat.
A.TRUSTED_NETWORK (for FSAP 9800 V1.0.6P9) It is assumed that the Network(s) are trusted (including the Management Network), such that they will not interfere with subscriber and/or management traffic. It is also assumed that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.	This assumption is upheld by OE.TRUSTED_NETWORK (for FSAP 9800 V1.0.6P9), which restates the assumption.
OE.TRUSTED_NETWORK (for all other TOEs) The environment shall ensure that the Network(s) are trusted (except the Management Network), such that they will not interfere with subscriber traffic and that the EMS, RADIUS and TACACS+ servers will not be used to attack the TOE.	This assumption is upheld by OE.TRUSTED_NETWORK (for all other TOEs), which restates the assumption.

7.2 Security Functional Requirements Rationale

Security objectives	SFRs addressing the security objectives
O. ACCESS The TOE shall ensure that subscribers have only access to the services on the networks that they are entitled to.	This objective is met by FDP_IFF.1 and FDP_IFC.1 specifying that there are Traffic Policy rules regulating the access.
O.MANAGE_ACCESS The TOE shall offer administrators the possibility to allow/deny subscribers access to services and/or entities on networks.	This objective is met by FMT_SMF.1 allowing administrators to manage the Traffic Policy rules
O. AUTHENTICATE_ADMIN The TOE shall identify and authenticate administrators before allowing them access to administrative functions.	This objective is met by: • FMT_SMR.1 defining the role of administrator • FIA_UID.2 stating that identification of administrators will be done by username • FIA_UAU.2 stating that administrators must be authenticated by password, RADIUS or TACACS+ • FMT_SMF listing what the administrative functions relevant to security are and that they can only be performed by an Administrator
O.ENCRYPTED_MANAGEMENT The TOE shall offer an encrypted channel for administrative actions, preventing discloser and/or modification of administrative commands.	For the FSAP 9800 V1.0.6P9, this objective is not relevant and therefore not met. As a result FPT_ITC.1 is not relevant for this TOE. For all other TOEs, this objective is met by FPT_ITC.1 providing a trusted channel between the SSH-client used by administrators and the TSF.
O. SEPARATION_OF_PORTS The TOE shall offer physical ports, and be able to separate traffic between different ports, such that: o It is not possible to listen in on traffic from one port on a different port o It is not possible to modify traffic on one port from another port	This objective is implemented by FDP_IFC.1 and FDP_IFF.1, where FDP_IFF.1 restates the objective.
O. xPON (only on TOEs offering xPON) THE TOE shall offer physical xPON ports to subscribers, such that: o It is not possible for one subscriber on a xPON port to listen in on traffic from/to other subscribers on that xPON port o It is not possible for one subscriber on a XPON port to modify traffic from/to other subscribers on that xPON port	This objective is implemented by FDP_IFC.1 and FDP_IFF.1, where FDP_IFF.1 restates the objective.

7.3 Dependencies

SFR	Dependencies
FIA_UID.2	-
FIA_UAU.2	FIA_UID.1: met by FIA_UID.2
FMT_SMR.1	FIA_UID.1: met by FIA_UID.2
FPT_SMF.1	-
FPT_ITC.1	-
FDP_IFC.1	FDP_IFF.1: met
FDP_IFF.1	FDP_IFC.1: met FMT_MSA.3: not met, as the policy does not use security attributes, management of these attributes is unnecessary.
SAR	**Dependencies**
EAL 2	All dependencies within an EAL are satisfied
ALC_FLR.2	-

A Supported Protocols

Upstream Protocol	Entity and goal	MSG5200	C300M	C350M	MSG5208	FSAP 9800V1	FSAP 9800V3	ZXDSL 9806HV1	ZXDSL 9806HV2	ZXDSL 9816	ZXDSL 9836
V5.1	LE in the PSTN										
V5.2	LE in the PSTN										
E1	To TDM Network										
GPNI	To GPON OLT										
EPNI	To EPON OLT										
ATM	To ATM network	Not evaluated				Not evaluated	Not evaluated				
PWE3	To IP network										
FE/GE	To IP network										
GE10	To IP network	Not evaluated			Not evaluated	Not evaluated	Not evaluated				
IUA/SCTP	For ISDN services										
H.248/Megaco(IPv4 only, IPv6 in future)	From one of: • Softswitch (in NGN) • AGCF (in IMS)										
SIP	To P-CSCF (in IMS) To common SIP server or Softswitch (in NGN)										
RTP/RTCP	To/from another media gateway										
PPP/PPPoE	Between end-user and BRAS. 5200 supports this with PPPoE+										
RADIUS	RADIUS Server										
TACACS+	TACACS+ Server										
RIP/OSPF	Routers	Not evaluated	Not evaluated	Not evaluated		Not evaluated	Not evaluated				
ISIS/BGP	Routers	Not evaluated	Not evaluated	Not evaluated		Not evaluated	Not evaluated				
PIM-SM/PIM-DM	Routers	Not evaluated	Not evaluated	Not evaluated		Not evaluated	Not evaluated				
IGMP	IPTV server										
DHCP Client	DHCP Server										
FTP	FTP-Server (for backup_										
TFTP	FTP-Server (for backup_	Do not use	Do not use	Do not use	Do not use	Do not use	Do not use				
RS-232	Hyperterminal connection for CLI	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated
Telnet Server	To CLI	Do not use	Do not use	Do not use	Do not use		Do not use	Do not use	Do not use	Do not use	Do not use
SSH	To CLI										
SNMP (v1, 2 or 3)	To EMS	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated
NTP	NTP Server. This could also be the Softswitch or EMS if these are configured as NTP Server										
Secure NTP	NTP Server. This could also be the Softswitch or EMS if these are configured as NTP Server									Not evaluated	Not evaluated
Downstream Protocol	**Entity and goal**	**MSG5200**	**C300M**	**C350M**	**MSG5208**	**FSAP 9800V1**	**FSAP 9800V3**	**ZXDSL 9806HV1**	**ZXDSL 9806HV2**	**ZXDSL 9816**	**ZXDSL 9836**
POTS	To end-user										
ISDN BRI and PRI	To end-user										
V.24	To end user										
V.35, G.703(SHDSL modem provide the interface)	To end user										
2/4 wire VF	To end user	Not evaluated									
E1	To end user										
T1	To end user										
E&M	To end user	Not evaluated									
SHDSL (TDM Mode)	To end user										
ADSL, ADSL2, ADSL2+	To end user										
VDSL2	To end user										
SHDSL (ATM mode)	To end user										
SHDSL.bis	To end user										
FE/GE	To end user										
EPON	To end user										
GPON	To end user										
Telnet Client/HTTP/SNMP	To end user modems	Not evaluated				Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated	Not evaluated

The cells in this table have the following meaning:

- Grey Cell: This feature does not exist in the TOE
- White Cell: This feature is supported in the evaluated configuration
- Not Evaluated: This feature exists in the TOE, but is not supported in the evaluated configuration. Enabling it may have consequences for the security of the TOE.
- Do not use: This feature exists in the TOE, but is not supported not in the evaluated configuration. Enabling it will likely have consequences for the security of the TOE.

B List of Acronyms

ADSL	Asymmetric DSL
AGCF	Access Gateway Control Function
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EMS	Element Management System
EPNI	EPON Network Interface
EPON	Ethernet PON
E&M	Earth & Magneto
FE	Fast Ethernet
FTP	File Transfer Protocol
GE	Gigabit Ethernet
GPNI	GPON Network Interface
GPON	Gigabit PON
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	IP Television
ISDN	Integrated Services Data Network
ISIS	Intermediate System to Intermediate System
IUA	ISDN User Adaptation
LE	Local Exchange
NGN	Next Generation Network
NTP	Network Time Protocol
OLT	Optical Line Terminal
OSPF	Open Shortest Path First
P-CSCF	Proxy Call Session Control Function
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Media
PIM-SM	PIM Sparse Media
PON	Passive Optical Network
POTS	Plain Old Telephony Service
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PWE3	Pseudo Wire Emulation Edge - Edge
RADIUS	Remote Authentication Dial In User Service

RCTP	Real Time Control Protocol
RIP	Routing Information Protocol
RTP	Real Time Protocol
SCP	Session Control Protocol
SHDSL	Single Rate High Speed DSL
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
TFTP	Trivial FTP
VDSL	Very High Bit Rate DSL
VF	Voice Frequency
xPON	EPON or GPON