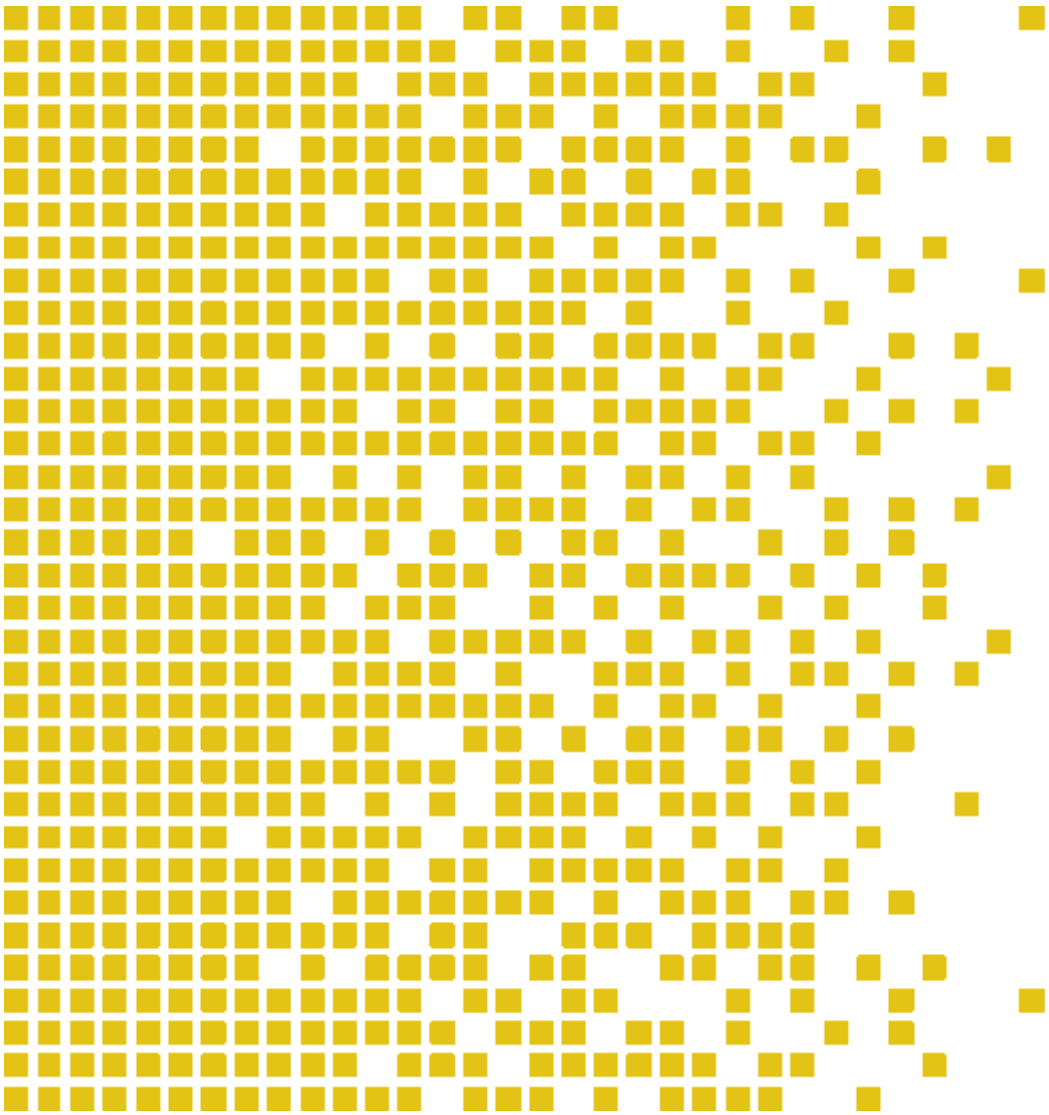
SERTIT-094 CR Certification Report

Issue 1.0 8 November 2017

ZXCTN 6000 Series of Access Router v3.10.10 Build 12



SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Sec urity, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

ZTE Coperation ZXCTN 6000 Series of Access Router is a router that enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/ MPLS-based networks.

ZXCTN 6000 Series of Access Router version v3.10.10 Build 12 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) augmented requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Jørn Arnesen Head of SERTIT
Date approved	8 November 2017

2 Abbreviations

ACL	Access Control List
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM Evaluation	Common Methodology for Information Technology Security
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
LAN	Local Area Network
MAC	Media Access Control
MPLS	Multi-Protocol Label
OSPF	Open Shortest Path First
POC	Point of Contact
QoS	Quality of Service
QP	Qualified Participant
RADIUS	Remote Authentication
RFC	Request for Comments
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol

TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
VPN	Virtual Private Network

3 References

[1] ZXCTN 6000 Series Access Router running ZXROSng Operating System Security Target, Version 3.3.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Preparative Procedures ZXCTN 6000 Series Access Router Running ZXROSng Operating System, v2.0, 10 August 2017

[8] Operational User Guidance ZXCTN 6000 Series Access Router Running the ZXROSng Operating System, v2.0, 14 August 2017

[9] Evaluation Technical Report Common Criteria EAL2+ Evaluation of ZXCTN 6000 Series Access Routers Running ZXROSng Operating System, v2.0, 6 September 2017.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZXCTN 6000 Series of Access Router version v3.10.10 Build 12 to the Sponsor, ZTE Coperation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was ZXCTN 6000 Series of Access Router and version v3.10.10 Build 12.

These products are also described in this report as the Target of Evaluation (TOE). The developer was ZTE Coperation.

The TOE is a ZXCTN 6000 Series of Access Router running v3.10.10 Build 12.

A ROUTER is a device with Layer-2 switch and offers Layer-3 capabilities. As a Layer 2 switch – it analyses incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. The layer-3 enabled switch supports routing of the traffic. Routers may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include BGPv4 and OSPFv2.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the Security Target [1] section 1.4.1 and 1.4.2.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2, augmented by ALC_FLR.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in Security Target*[1] section 3.3.*

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet, and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.AUDIT_REVIEW
  Actions performed by users may not be known to the administrators due to actions not being recorded or the audit records not being reviewed prior to the machine shutting down, or an unauthorized administrator modifies or destroys audit data.
- T.NO_PRIVILEGE
  An unauthorized user may gain access to inappropriately view, tamper, modify, or delete TOE Security Functionality data.
- T.MEDIATE
  An unauthorized entity may send impermissible information through the TOE which results in the exploitation of resources on the network.
- T.NO_AUTH _SESSION
  A user may gain unauthorized access to an unattended session and alter the TOE security configuration.
- T.NO_AUTH_ACCESS
  An unauthorized user gains management access to the TOE and alter the TOE security configuration.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- A.NO_EVIL&TRAIN
  The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error. The administrators are trained in the appropriate use of the TOE.

- A.CONNECTIVITY
  All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes:
  - RADIUS, TACACS+ server interface (optional)
  - SNMP/SYSLOG interface (required)
  - NTP interface (required)
  - SSH interface for remote client (at least one of the local or remote administration client is required)
- A.PHYSICAL
  The TOE will be located in an environment that provides physical security to prevent unauthorized physical access, commensurate with the value of the IT assets protected by the TOE and uninterruptible power, temperature control required for reliable operation.
- A.REMOTE_AUTH
  External authentication services will be available via either RADIUS/TACACS+, or both when the TOE is configured to use remote authentication.
- A.TIMES
  External NTP services will be available.

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- O.AUDIT_REVIEW
  The TOE will provide the privileged administrators and authentication administrators the capability to review Audit data and will restrict audit review to administrators who have been granted explicit read-access. The TOE will generate audit records which will include the time that the event occurred and the identity of the administrator performing the event.
- O.MANAGE
  The TOE must provide services that allow effective management of its functions and data and restrict access to the TOE Management functions to the privileged administrators and authentication administrators.
- O.IDAUTH
  The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
- O.MEDIATE
  The TOE shall control the flow of information among its network connections according to routing rules and BGPv4/OSPFv2 routing protocols which prevent the communication with trusted routers from modification, insertion and replay errors.
- O.TOE_ACCESS
  The TOE will provide mechanisms that control an administrator's logical access to the TOE and to deny access to unattended session to configure the TOE.

- O.ROUTE
  The TOE shall be able to accept routing data from trusted routers according to BGPv4/OSPFv2.

4.13 Non-IT Security Objectives

- OE.TIMES
  NTP server will be available to provide accurate/synchronized time services to the TOE.
- OE.CONNECTIVITY
  All TOE external interfaces except for the network traffic/data interface are attached to the internal (trusted) network. This includes:
  1. RADIUS, TACACS+ server interface (optional)
  2. SNMP, SYSLOG interface (required)
  3. NTP interface (required)
  4. SSH interface for remote client (at least one of the local or remote administration client is required)
- OE.NO_EVIL&TRAIN
  The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error. The administrators are trained in the appropriate use of the TOE.
- OE.PHYSICAL
  The operational environment provides the TOE with appropriate physical security to prevent unauthorized physical access, commensurate with the value of the IT assets protected by the TOE and uninterruptible power, temperature control required for reliable operation.
- OE.USERS
  All administrators are “vetted” to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FDP_IFC.1(1) Subset information flow control (unauthenticated)
- FDP_IFC.1(2) Subset information flow control (export policy)
- FDP_IFF.1(1) Simple security attributes (unauthenticated)
- FDP_IFF.1(2) Simple security attributes (export policy)
- FDP_UIT.1 Data exchange integrity
- FIA_AFL.1 Authentication failure handling

- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User authentication before any action
- FIA_UAU.5 Multiple authentication mechanisms
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_MTD.1(1) Management of TSF data
- FMT_MTD.1(2) Management of TSF data
- FMT_MTD.1(3) Management of TSF data
- FMT_MTD.1(4) Management of TSF data
- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_ITC.1(1) Inter-TSF trusted channel (SSH)
- FTP_ITC.1(2) Inter-TSF trusted channel (RADIUS/TACACS+)
- FTP_ITC.1(3) Inter-TSF trusted channel (NTP)

4.15 Security Function Policy

The TOE provides:

- Handling of packet flows using the OSPFv2, and BGPv4 protocols
- Local and remote administration
- Authentication, either in the TOE or through TACACS+ or RADIUS.
- Administrator Profiles to permit or deny access to a hierarchical branch or specific commands.
- Audit
- Management and configuration of the TOE
- Mitigate DoS attacks

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[9] to SERTIT in 6 September 2017. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification with complete summary
	ADV_TDS.1	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Production support, acceptance procedures and automation
	ALC_CMS.2	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[9] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.4.1 provided by the developer. The preparative Procedures [7] and Operational User Guidance [8] describe all necessary steps to configure the TOE in the certified configuration.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The TOE are substantially similar to other router/switches on the market. This technology is well-established. The technology and possible vulnerabilities are described in a series of public documents.

The evaluators assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found and three turned out to be possibly exploitable. All of them are related to short MD5 password for BGP and OSPF. Consequently the developer has updated the guidance to enhance the secure configuration of the TOE to request the user use strong password (longer than 10 characters which contains combination of alphanumeric and special characters) for

MD5 authentication for the BGP and OSPF, and as a result this issue has become moot.

5.6 Developer's Tests

The developer test plan consists of 6 different categories. In total there are 27 test cases defined by the developer. The categories are based on major grouping of security functionalities, and, in combination with all SFR and TSFIs. All the TSFIs are covered by at least 3 tests. The developer has performed testing on the ZXCTN 6120E-XF, 6150, and 6180.

5.7 Evaluators' Tests

The evaluator decided to sample at least 1 test per TSFI to repeat, except for the EXIF_L_CLI, where the evaluator sampled 2 tests as this interface provides important security feature to limit only authenticated and authorized user can access the management interface of the TOE. As a result there were 7 tests from the developer tests were repeated by the evaluator.

Furthermore the evaluator analysed the developer test plan to see whether additional ATE tests could be performed, and devised additional 11 tests.

During the test the evaluator noted:

- There are 4 types of NTP authentication scenario:

Client	Server	Synchronization
Incomplete	Incomplete	Y
Incomplete	Complete	Y
Complete	Incomplete	N
Complete	Complete	Passing authentication:Y;Otherwise N

  Therefore to prevent the NTP authentication falls back to "no-authentication", the administrator must make sure that both the client and server NTP attention configuration is complete, i.e., proper key value and proper key ID are both configured.
- The privilege escalation commend of the TOE, the "enable" command, does not enforce password strength check. Therefore the administrator must ensure that the default password of "enable" is changed and strong password rule must be applied, as per described in [AGD-PRE] section 2.3.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that ZXCTN 6000 Series of Access Router version v3.10.10 Build 12 running ZXROSng meet the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL 2 Augmented with ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of ZXCTN 6000 Series of Access Router version v3.10.10 Build 12 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE. The summary of the recommendations are:

- Section 5.5:
  To prevent OSPF and BGP MD5 password bruteforce, the administrator must configure these password with minimum 10 characters long using alphanumeric and special characters, as per described in [AGD-OPE] section 3.12 and 3.13.
- Section 5.7
  There are 4 types of NTP authentication scenario:

Client	Server	Synchronization
Incomplete	Incomplete	Y
Incomplete	Complete	Y
Complete	Incomplete	N
Complete	Complete	Passing authentication:Y;Otherwise N

  Therefore to prevent the NTP authentication falls back to “no-authentication”, the administrator must make sure that both the client and server NTP attention configuration is complete, i.e., proper key value and proper key ID are both configured.
- Section 5.7
  The privilege escalation commend of the TOE, the “enable” command, does not enforce password strength check. Therefore the administrator must

ensure that the default password of “enable” is changed and strong password rule must be applied, as per described in [AGD-PRE] section 2.3.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Hardware:

The list of hardware models is shown in **Table** *1*

Model	Interface Description	Type
ZXCTN 608-GF	Contains service interfaces and management & auxiliary interfaces Service interfaces: 2x 1 Gbps Optical Ethernet 2x 1 Gbps Electrical Ethernet 2x 1 Gbps Combo Ethernet Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Mini USB console interface	Access Router
ZXCTN 608-GE/GK	608-GE is fan free design whereas 608-GK contains a fan inside. Both routers contain service interfaces and management & auxiliary interfaces Service interfaces: 4x 1 Gbps Optical Ethernet 2x 1 Gbps Electrical Ethernet 2x E1 Interfaces Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Mini USB console interface	

ZXCTN 6120E-XK/XF	Both routers contains service interfaces and management & auxiliary interfaces Service interfaces: 2x 10 Gbps Optical Ethernet 4x 1 Gbps Optical Ethernet 4x 1 Gbps Electrical Ethernet 4x 1 Gbps Combo Ethernet Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Mini USB console interface 1x Fast Ethernet external alarm 1x Fast Ethernet BITS/GPS interface The 6120E-XK supports the additional interface of E1.	
ZXCTN 6120S	Contains 1 main control board slot that supports the following control boards: SMDE SMDE(BS61) Contains 2 available LIC card slots that support the following LIC cards: OIXG1 OIXG2 OIX6G OIGE8 EIGE8 OEIGE8 OEIGE OEIFE8	

	E1E16-75 E1E16-120 OIS4	
ZXCTN 6150	Contains 2 main control board slots for 1+1 redundancy the slots support the following control boards: SME SME(BS61) Contains 6 available LIC card slots that support the following LIC cards: OIXG1 OIXG2 OIX6G OIGE8 EIGE8 OEIGE8 OEIGE OEIFE8 E1E16-75 E1E16-120 OIS4	
ZXCTN 6180	Contains 2 main control board slots for 1+1 redundancy the slots support the following control boards: SMF Contains 10 available LIC card slots that support the following LIC cards: OIXG1 OIXG2 OIX6G OIGE8	

	EIGE8 OEIGE8 OEIGE OEIFE8 E1E16-75 E1E16-120 OIS4	

Table 1 List of Models

Main control boards:

Main control boards	**Ports supported**
SMDE SMDE(BS61)	Service interfaces: 2x 10 Gbps Optical Ethernet 4x 1 Gbps Optical Ethernet 2x 1 Gbps Electrical Ethernet 1x E1 16-pin Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Fast Ethernet Qx 1x Fast Ethernet external alarm 1x Fast Ethernet BITS Interface 2x Fast Ethernet GPS Interface
SME SME(BS61)	Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Fast Ethernet Qx 1x Fast Ethernet BITS Interface 2x Fast Ethernet GPS Interface
SMF	Management & Auxiliary interfaces: 1x Fast Ethernet LCT (Local craft terminal interface) 1x Fast Ethernet GPS Interface

Table 2 List of Main control boards

LIC cards:

LIC cards	Ports supported
OIXG1	1x 10 Gbps Ethernet optical interface
OIXG2	2x 10 Gbps Ethernet optical interface
OIX6G	1x 1Gbps Ethernet optical interface 6x 1 Gbps Electrical Ethernet
OIGE8	8x 1 Gbps Ethernet optical interface
EIGE8	8x 1 Gbps Electrical Ethernet
OEIGE8	4x 1 Gbps Electrical Ethernet and 4x 1 Gbps Ethernet optical interface
OEIGE	4x 1 Gbps Electrical Ethernet or 4x 1 Gbps Ethernet optical interface
OEIFE8	4x 100 Mbps Electrical Ethernet and 4x 100 M bps Ethernet optical interface
E1E16-75	4x 1 Gbps Electrical Ethernet 4x 1 Gbps Ethernet optical interface 1x SCSI 50-pin angle solder socket (female) used for E1 electrical signals
E1E16-120	1x SCSI 50-pin angle solder socket (female) used for E1 electrical signals
OIS4	4x 10 Gbps Ethernet optical interface

Table 3 List of line cards

Software:

TOE	Product Software	ZXROSng Operating system	ZTE Carrier Grade Embedded Linux	Linux Kernel
608-GF/GE/GK	V3.10.10B12	v4.00.30R3	CGEL_V5.0.1.30	3.10.55
6120S	V3.10.10B12	v4.00.30R3	CGEL_V_3.04.10.P6.F5	2.6.21
6150	V3.10.10B12	v4.00.30R3	CGEL_V_3.04.10.P6.F5	2.6.21
6180	V3.10.10B1	v4.00.30R3	CGEL_V_3.04.10.P6.F	2.6.21

	2		5	
6120E-XF/XK	V3.10.10B12	v4.00.30R3	CGEL_V4.03.20_P6B3	2.6.32

Guidance:

- Preparative Procedures ZXCTN 6000 Series Access Router Running ZXROSng Operating System, v2.0, 10 August 2017
- Operational User Guidance ZXCTN 6000 Series Access Router Running the ZXROSng Operating System, v2.0, 14 August 2017

TOE Documentation

The supporting guidance documents evaluated were:

[a] Preparative Procedures ZXCTN 6000 Series Access Router Running ZXROSng Operating System, v2.0, 10 August 2017

[b] Operational User Guidance ZXCTN 6000 Series Access Router Running the ZXROSng Operating System, v2.0, 14 August 2017

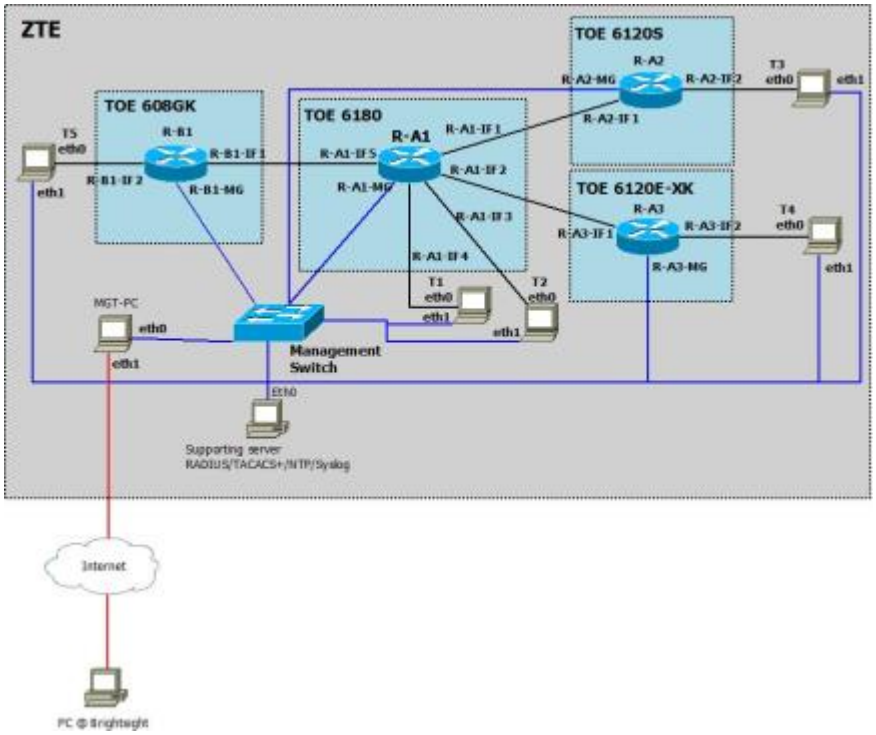
Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

The TOE was tested on the following models: ZXCTN 608GK, ZXCTN 6180, ZXCTN 6120S, and ZXCTN 6120E-XK; with software version 3.10.10 Build 12, configured according to [7] and [8].

Environmental Configuration

The TOE is tested in the following setup:


ZTE
TOE 61205
R-A2
R-A2-MG
R-A2-IF2
R-A2-IF1
T3
eth0
eth1
TOE 608GK
R-B1
T5
eth0
R-B1-IF1
R-B1-IF2
R-B1-MG
eth1
TOE 6180
R-A1
R-A1-IF1
R-A1-IF5
R-A1-IF2
R-A1-MG
R-A1-IF3
R-A1-IF4
TOE 6120E-XX
R-A3
R-A3-IF1
R-A3-IF2
R-A3-MG
T4
eth0
eth1
MGT-PC
eth0
eth1
T1
eth0
eth1
T2
eth0
eth1
Management
Switch
Eth0
Supporting server
RADIUS/TACACS+/NTP/Syslog
Internet
PC @ Brightsight