ZXR10 3900 Series Switches

Running the ZXROS Operating System

Security Target

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26771900
Fax: +86-755-26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn
Version: R1.5

LEGAL INFORMATION

Revision History

Date	Version	Remark
2011/03/01	0.8	Initial version
2011/03/08	0.9	Revised according to “110307 [Action ASE] EAL2 ZXROS ASE actionpoints+answer v0.2”
2011/04/13	1.0	Revised according to “EOR_TDS_03_03 ZXR10 3900 Series”
2011/05/25	1.1	Added “Revision History”
2011/05/26	1.2	Revised “5.1.2.21 FMT_MTD.1(3) Management of TSF data”
2011/06/07	1.3	Added “date of ST” to ST cover
2011/07/27	1.4	Fixed “version number of guidance documents”
2011/08/19	1.5	Minor refinement

Serial Number: SJ-20110815105844-031

Publishing Date: 2011/08/19 (R1.5)

Contents

Chapter 1
ST INTRODUCTION

Table of Contents

1.1 ST IDENTIFICATION

1.1.1 ST Title

V1.5 of the Security Target for the 3900 Series of ZXR10 Switches running the ZXROS Operating System.

1.1.2 References

The following documentation was used to prepare this ST.

[CCp1]

Common Criteria for Information Technology Security Evaluation – Part 1:

Introduction and general model, dated July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-001

[CCp2]

Common Criteria for Information Technology Security Evaluation – Part 2:

Security functional requirements, dated July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-002

[CCp3]

Common Criteria for Information Technology Security Evaluation – Part 3:

Security assurance requirements, dated July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003

[CEM]

Common Evaluation Methodology for Information Technology Security Evaluation, dated July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004

1.2 TOE IDENTIFICATION

This Security Target describes the 3900 Series of ESS (Ethernet Service Switches) running the ZXROS Operating System v4.08.

The 3900 series consists of the following ESSs:

Table 1-1 3900 Series Models

Series	Model	Interface Description	Type
39A Series	3928A	24 x 100Mbps Base-T 2 x 1Gbps Optical Ethernet (SFP) 1 x Line Cards* (optional) 1 x RJ-45 Ethernet management port 1 x RS232 console port	ESS
	3928A-FI	24 x 100Mbps Optical Ethernet (SFP) 2 x 1Gbps Optical Ethernet (SFP) 1 x Line Cards* (optional) 1 x RJ-45 Ethernet management port 1 x RS232 console port	
	3928A-PS	24 x 100Mbps Base-T (PoE) 2 x 1Gbps Optical Ethernet (SFP) 1 x Line Cards* (optional) 1 x RJ-45 Ethernet management port 1 x RS232 console port	
	3952A	48 x 100Mbps Optical Ethernet (SFP) 4 x 1Gbps Optical Ethernet (SFP) 1 x RJ-45 Ethernet management port 1 x RS232 console port	
	*Line Card: there are 4 kinds of line card supported		

	● 2 x 1Gbps Base-X ● 2 x 1Gbps Optical Ethernet (SFP) ● 1 x 1Gbps Base-X + 1 x 1Gbps Optical Ethernet (SFP) ● 2 x 100Mbps Optical Ethernet (SFP)		
39E Series	3928E	24 x 100Mbps Base-T 4 x 1Gbps Optical Ethernet (QGLB)/ Electrical Ethernet (QGTB) 1 x RJ-45 Ethernet management port 1 x RS232 console port	ESS
	3928E-FI	24 x 100Mbps Optical Ethernet (SFP) 4 x 1Gbps Optical Ethernet (QGLB)/ Electrical Ethernet (QGTB) 1 x RJ-45 Ethernet management port 1 x RS232 console port	
	3952E	16 x 100Mbps Optical Ethernet (SFP) 4 x 8 x 100Mbps Base-T/Optical Ethernet (SFP) (4 line card) 4 x 1Gbps Optical Ethernet (QGLB)/ Electrical Ethernet (QGTB) 1 x RJ-45 Ethernet management port 1 x RS232 console port	

The major difference between models is the type, capacity and number of the physical interfaces described in the above table.

1.3 TOE OVERVIEW

1.3.1 Intended usage and security features of the TOE

An ESS enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/ MPLS-based networks.

The supported protocols arelayer 2 / layer 3 encapsulation and Internet Protocol (IP), and Ethernet. Other protocols may be supported by the product, but are not evaluated (see section 1.4.3).

The major security features of the TOE are:

- Handling of packet flows using the RIPv2, 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

1.3.2 Non-TOE components

The TOE requires the following IT in its environment:

A local or remote console for administration (required)

At least one is needed, but both are allowed.

- For a local console: Any platform that supports terminal emulation to the ANSI X3.64 standard;
- For a remote console, any platform that supports terminal emulation to the ANSI X3.64 standard and the SSH protocol.

A SNMP/SYSLOG server for logging (required)

This may be two platforms or one combined platform.

- For the SNMP server, any platform that supports RFC 3411-RFC 3418 (SNMPv3)
- For the SYSLOG server, any platform that supports RFC 3164 (SYSLOG Protocol);

All logs are stored in the TOE whenever there is new log generated and then the TOE transferred the log files to SNMP/SYSLOG Servers with SNMP/SYSLOG network protocol through internal network in a constant period time. The log file is stored under the ‘data’ directory of the flash disk inside the TOE. For detail content of the log, please reference chapter 5.1.2.1.

A NTP Server (required)

Any platform that supports RFC 1305 (NTPv3)

A RADIUS or TACACS+ server for AAA services (optional)

- For the RADIUS Server, any platform that supports RFC 2865 (Authentication & Authorization) and RFC 2866 (Accounting) for RADIUS.
- For the TACACS+ Server, any platform that supports TACACS+ Version 1.78 (DRAFT);

At least two external networks and an internal network

The major functionality of the TOE is to forward data packets along networks. There should be at least two distinct networks or network segments: commonly two LANs or WANs or a LAN and its ISP's network. There should also be an internal network that connects the SNMP/SYSLOG server, the NTP server and the RADIUS/TACACS+ server to the TOE.

1.4 TOE DESCRIPTION

The TOE is a 3900 series ESS running the operating system ZXROS 4.08.

An ESS is a device with Layer-2 switch and offers Layer-3 capabilities. As a Layer 2 switch – it analyzes 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. ESSs 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, RIPv2 and OSPFv2.

1.4.1 Physical scope

The TOE consists of:

- a 3900 series ESS
- a copy of ZXROS V4.08: located on a compact flash card, which can be inserted in the ESS and is shipped with the ESS. The complete version information of ZXROS V4.08 are as follows:

```
ZXR10_3928E Software, Version ZXR10 3900E&3900A&3200A
V2.8.23.B2.06.P08.IT01, RELEASE SOFTWARE
ZXR10 ROS Version V4.08
Compiled May 26 2011, 19:33:19
```

- guidance documents
  - → ZXR10 3900 Series Switches Running ZXROS_AGD_OPE v1.9
  - → ZXR10 3900 Series Switches Running ZXROS_AGD_PRE v1.6

1.4.2 Logical scope

The TOE is connected to an internal (trusted) network and two or more external (untrusted) networks.

The external networks are the networks to be switched/routed and support the primary function of the TOE: the handling of packet flows from one network to another. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. The packet flows can be manipulated and monitored as well. Routing protocols used are RIPv2, OSPFv2, and BGPv4.

The internal network may contain the following entities:

- A RADIUS or TACACS+ Server for Identification & Authentication (optional)
- A SNMP/SYSLOG server for logging (required)
- A NTP Server for external time synchronisation (required)
- A local console for management or a remote console for management. This remote console connects with the TOE through the SSH. (required)

The TOE provides the following services:

- Handling of packet flows: as described above using the RIPv2, OSPFv2, IS-IS, and BGPv4 protocols which can prevent the communication with trusted routers from modification, insertion and replay errors. Packet flows can be restricted to come only from authorized sources and/or go to authorized destinations.
- Local (through a console port) and remote (protected through SSH) access to the TOE for administrators. These sessions are dropped after a configurable amount of total session time or after a configurable amount of idle time to prevent access to unattended open sessions.
- Authentication: Access permission is controlled using: TACACS+; RADIUS; or local authentication. A profile, which is based on administrator name and password configurations, is applied for the administrator authorization processes. This ST addresses only the client-side support of RADIUS and TACACS+: the servers themselves are out-of-scope.
- Profiles: Administrator profiles are configured to permit or deny access to a hierarchical branch or specific commands.
- Audit: The TOE provides an audit feature for actions related to authentication attempts and administrator actions
- Management: The TOE offers administrators the capability to configure the TOE (primarily the packet flow handling and audit features).
- Mitigate DoS attacks through use of real-time statistics capabilities

1.4.3 Evaluated Configuration

The TOE has many features that can be configured to be on or off. The table below lists these features and shows whether they are:

- Evaluated: this means that the feature can be enabled, and it will work securely.

- Not Permitted: this means that the feature may not be enabled, as this will endanger the security of the entire TOE.
- Not Evaluated: this means that the feature can be enabled, that enabling this feature will not endanger the security of the other features, but the evaluation has not determined whether the feature itself will work securely.

Table 1-2 Evaluated Configuration

Feature	Description	Evaluated	Not Permitted	Not Evaluated
AAA	TACACS+ RADIUS (Remote Access Dial-In User Service)	×		
ACL	Access control lists.	×		
DHCP	Dynamic Host Control Protocol (DHCP) enables you to automatically assign reusable IP addresses to DHCP clients.			×
IGMP			×	×
IPv6			×	×
Media Types (non-Ethernet)	ADSL, ATM, Frame Relay, ISDN, MPLS, PPP, PPPoE, SDH, and SONET.			×
NAT	Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world.			×
NetFlow				×
NTPv3	Network Time Protocol version 3	×		
QoS	Quality of Service features			×
STP	Spanning tree protocol			×
Routing Protocol Disabled	RIP version 1		×	×
Routing Protocols Permitted	RIPv2: Routing Information Protocol (RIP) version 2 (MD5 authentication)	×		
	OSPFv2: Open Shortest Path First (OSPFv2) Mode 2	×		
	BGPv4: Border Gateway Protocol	×		
Static Routing	Static Routing Table	×		

Feature	Description	Evaluated	Not Permitted	Not Evaluated
SSHv1	SSH version 1 client and server support.		×	×
SSHv2	SSH version 2 client and server support.	×		
SNMPv2			×	×
SNMPv3	Simple Network Management Protocol (SNMP):	×		
SYSLOG	Configuration and delivery of SYSLOG messages.	×		
Telnet			×	×
FTP / TFTP			×	×
VLAN(ESS)	Not evaluated: Virtual LAN			×
Mitigate DoS attack	Denial of service	×		
VPN	Not permitted in the evaluated configuration: WebVPN, IPSec, IKE, L2TP (Layer 2 Tunneling Protocol).		×	×

Chapter 2
CONFORMANCE CLAIMS

Table of Contents

2.1 COMMON CRITERIA (CC) CONFORMANCE

This ST conforms to:

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

This ST conforms to no Protection Profile.

This ST conforms to EAL 3+ALC_FLR.2, and to no other packages.

This page intentionally left blank.

Chapter 3
SECURITY PROBLEM DEFINITION

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

1. Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
2. Any organizational security policy statements or rules with which the TOE must comply
3. Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies threats as T.THREAT, assumptions as A.ASSUMPTION and policies as P.POLICY.

Table of Contents

3.1 Threat

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

1. Threat agents are entities that can adversely act on assets – the threat agents in the threats below are unauthorized user, network attacker, authorized user and
2. Assets are entities that someone places value upon – the assets are access to network services,
3. Adverse actions are actions performed by a threat agent on an asset – the adverse actions are: unauthorized changes to configuration, both network routing configuration and management configuration.

Table 3-1 Threat

THREAT	DESCRIPTION
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.

THREAT	DESCRIPTION
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.

3.2 Assumption

The assumptions are ordered into three groups: Personnel Assumptions, Physical Environment Assumptions, and Operational Assumptions.

3.2.1 Personnel Assumptions

Table 3-2 Personnel Assumption

ASSUMPTION	DESCRIPTION
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.

3.2.2 Physical Environment Assumptions

Table 3-3 Physical Assumption

ASSUMPTION	DESCRIPTION
A.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)

ASSUMPTION	DESCRIPTION
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.

3.2.3 Operational Assumptions

Table 3-4 Operational Assumption

ASSUMPTION	DESCRIPTION
A.TIMES	External NTP services will be available.

3.3 ORGANIZATIONAL SECURITY POLICIES

This section describes the organizational security policies to be enforced with respect to the TOE environment.

Table 3-5 Organizational Security Policy

OSP	DESCRIPTION
P.USERS	The TOE is administered by one or more Administrators who have been granted rights to administer the TOE. All administrators are “vetted” to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted.
P.ROUTE	The TOE must be able to accept routing data from trusted routers

This page intentionally left blank.

Chapter 4
SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

Table of Contents

4.1 SECURITY OBJECTIVES FOR THE TOE

Table 4-1 Security Objective

OBJECTIVES	DESCRIPTION
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/RIPv2 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 unattached session to configure the TOE.
O.ROUTE	The TOE shall be able to accept routing data from trusted routers according to BGPv4/OSPFv2/RIPv2.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The following IT security objectives for the environment are to be addressed by the operational environment via technical means.

Table 4-2 Security Objective for the environment

OBJECTIVES	DESCRIPTION
OE.TIMES	NTP server must 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 assessed for 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.
OE.AUDIT_REVIEW	The SYSLOG/SNMP server will provide the privileged administrators and authentication administrators the capability to review Audit data stored in the log servers and will restrict audit review to administrators who have been granted explicit read-access.

Chapter 5
SECURITY REQUIREMENTS

The CC permits four types of operations to be performed on security functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets and italicized text, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].
- Refinement: Indicated by underlined text, e.g., refined item for additions or strikethrough text, e.g., ~~refined~~ ~~item~~ for deleted items.
- Iteration: Indicated by assigning a number at the functional component level, for example: FMT_MTD.1.1 (1), FMT_MTD.1.1 (2), FMT_MTD.1.1 (3), FMT_MTD.1.1 (4) refer to separate instances of the FMT_MTD.1 security functional requirement component.

Table of Contents

5.1 SECURITY FUNCTIONAL REQUIREMENTS

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

The security requirements consist of two groups of requirements:

1. the security functional requirements (SFRs): a translation of the security objectives for the TOE into a standardized language; and
2. the security assurance requirements (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

5.1.1 Overview

The security functional requirements for this ST consist of the following components from Part 2 of the CC.

Table 5-1 TOE Security Functional Requirements

CC Part 2 Security Functional Components	
Identifier	**Name**
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 policy)
FDP_IFF.1(1)	Simple security attributes (unauthenticated policy)
FDP_IFC.1(2)	Subset information flow control (export policy)
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)	Trusted channel for SSH client
FTP_ITC.1(2)	Trusted channel for RADIUS/TACACS+ server
FTP_ITC.1(3)	Trusted channel for NTP

5.1.2 Security Functional Requirements

5.1.2.1 FAU_GEN.1 Audit data generation

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

1. Start-up and shutdown of the audit functions;
2. (refined away)
   - Alarm log: The security event source is all events that affect attempts to breach system:
     - → authentication alarm
       a. I&A authentication success
       b. I&A authentication failure
     - → user management alarm
       a. user account is locked
       b. user account is unlocked
       c. user account is enabled
       d. user account is disabled
     - → RADIUS alarm log
       a. RADIUS authentication group is unreachable
       b. RADIUS accounting server group is unreachable
       c. RADIUS buffer queue exceeds the threshold
     - → NTP alarm log
       a. The clock of NTP server and client are not synchronized
     - → ACL alarm
       a. ACL aggregation is too large
     - → RIP/OSPF/BGP alarm
       a. authentication success
       b. authentication failure
   - Command log: all activities performed by the administrator are recorded in Command log.

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

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the ST [none].

Application Note: There is no success / failure concept for Alarm log. Therefore there is no outcome (success or failure) for alarm log.

5.1.2.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: The Command log record is associated with an administrator. The other types of log are associated with unauthenticated user/application.

5.1.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [authorised administrators] with the capability to read [all audit data] from the audit records stored in the log file of the TOE.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2.4 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.

Application Note: The TOE only protects audit trail that is stored inside the TOE.

5.1.2.5 FAU_STG.4 Prevention of audit data loss

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

Application Note: The TOE only prevents the audit data loss for those stored inside the TOE.

5.1.2.6 FDP_IFC.1(1) Subset information flow control (unauthenticated)

FDP_IFC.1.1 The TSF shall enforce the [unauthenticated SFP] on:

1. [subjects: each IT entity that sends and receives information through the TOE to one another;
2. information: network packets sent through the TOE from one subject to another; and
3. operations: route/filter packets].

5.1.2.7 FDP_IFC.1(2) Subset information flow control (export policy)

FDP_IFC.1.1 The TSF shall enforce the [EXPORT SFP] on.

1. [subjects: each IT entity that receives information from the TOE;
2. information: events sent from the TOE to SNMP trap and SYSLOG servers; and
3. operations: send events].

5.1.2.8 FDP_IFF.1(1) Simple security attributes (unauthenticated)

FDP_IFF.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] based on the following types of subject and information security attributes:

[security subject attributes:

1. IP network address and port of source subject;
2. IP network address and port of destination subject;
3. transport layer protocol and their flags and attributes (UDP, TCP);
4. network layer protocol (IP, ICMP);
5. interface on which traffic arrives and departs;
6. routing protocols (BGPv4, OSPFv2, RIPv2) and their configuration and state].

Application Note: the TOE only accepts routing information from other routers with trusted IPs configured by the administrators.

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:

1. [the identity of the source subject is in the set of source subject identifiers (i.e., addresses);
2. the identity of the destination entity is in the set of destination entity identifiers (i.e., addresses);
3. the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy rule set defined by the Administrator) according to the following algorithm
   - First match algorithm for filtering rule. When multiple policy names are specified, the policies shall be executed in the order they are specified. The first policy that matches is applied;
   - Longest-prefix match algorithm for routing rule. When the maximum prefix length of the destination address is matched to the configured rule.

the selected information flow policy rule specifies that the information flow is to be permitted]

FDP_IFF.1.3 The TSF shall enforce the [rule:

when the semi-connection statistics information of the TCP SYN flood exceeds configured threshold, the TOE suppresses these attacks].

FDP_IFF.1.4 The TSF shall explicitly authorize 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:

1. [The TOE shall reject requests for access or services where the source identity of the information received by the TOE specifies a broadcast identity;
2. The TSF shall reject requests for access or services where the presumed source identity of the information received by the TOE specifies a loopback identifier.
3. The TSF shall drop requests in which the information received by the TOE does not correspond to an entry in the routing table.
4. The TSF shall deny information flows that do not conform to the IP protocol (RFC 791) and the associated routing protocol specification (RFCs for RIPv2, OSPFv2 and BGPv4)].

5.1.2.9 FDP_IFF.1(2) Simple security attributes (export policy)

FDP_IFF.1.1 The TSF shall enforce the [EXPORT SFP] based on the following types of subject and information security attributes:

[Source subject security attributes: source network identifier; and Destination subject security attributes:

1. SYSLOG server IP address;
2. UDP port used to send the SYSLOG message;
3. SYSLOG Facility Code;
4. SYSLOG Severity Threshold;
5. IP address of the SNMP trap receiver;
6. UDP port used to send the SNMP trap;
7. SNMPv3 used to format the SNMP notification; and
8. Security name and level for SNMPv3 trap receivers;].

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:

1. [the identity of the destination subject is in the set of destination identifiers;
2. the information security attributes match the security attributes defined by the administrator) according to the following algorithm [ALL the security attributes must match]; and
3. the selected information flow policy rule specifies that the information flow is to be permitted].

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

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

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

5.1.2.10 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall ~~enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to~~ transmit and receive routing data to/from trusted routers in a manner protected from modification, insertion and replay errors

Application Note: in order to protect the routing data from modification, insertion and replay error, Only RIPv2, OSPFv2 mode 2, and BGPv4 routing protocols are allowed to ensure the integrity. There is no need to protect the confidentiality of the routing data.

5.1.2.11 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer (within a range of values 3 – 16)] unsuccessful authentication attempts occur related to any claimed administrator ID attempting to authenticate to the TOE.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [at the option of the Administrator prevent the administrators except the administrator from performing activities that require authentication until an action is taken by the Administrator, or until an Administrator defined time period (within a range of values 1 -1440 minutes) has elapsed].

5.1.2.12 FIA_SOS.1 Verification of secrets

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

1. a minimum length (characters) default 6 and within a range of 3-32;
2. Complexity requirements: [numeric] [special-character] [mixed-case]
   a. i: at least one (1) numeric character must be present in the password; and
   b. ii) at least one (1) special character must be present in the password. Special characters include: ~!@#$%^&*()_+|{}:”<>?`-=\[];’
   c. iii) at least one (1) upper and one (1) lower case character
3. An administrator defined number of days an administrator password is valid before the administrator must change their password. This parameter shall be used to force the administrator to change the password at the configured interval. The maximum number of days the password is valid shall be definable within a range of values of 15 – 365.
4. Either the administrator must change his password at the first login, or the administrator is not forced to change his password at the first login, as configured by the administrator]

Application Note: the TOE cannot enforce this SFR when performing remote authentication with RADIUS/TACACS+ server.

5.1.2.13 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.

5.1.2.14 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [client RADIUS, TACACS+, and local authentication mechanisms] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by the authorised user].

5.1.2.15 FIA_UID.2 User identification before any action

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

5.1.2.16 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of] the functions [TOE management/administration/security functions listed below] to [the Administrator].

1. Configuring Administrators;
2. Configuring Login control;
3. Configuring local/RADIUS/TACACS+ authentication;
4. Configuring Password Management Parameters;
5. Configuring ACL;
6. Configuring Event logs;
7. Configuring SNMP/SYSLOG;
8. Configuring NTP;
9. Configuring anti-DoS attack;
10. Configuring CPU Protection Policies;

5.1.2.17 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [unauthenticated SFP and EXPORT SFP] to restrict the ability to [change default, query, modify, delete] the security attributes [defined in FDP_IFF.1.1(1) and FDP_IFF.1.1(2)] to [Administrator].

5.1.2.18 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [unauthenticated SFP and EXPORT SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

5.1.2.19 FMT_MTD.1(1) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [create, modify, delete, backup and restore] the [configuration item and filtering rules] to [administrators].

5.1.2.20 FMT_MTD.1(2) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [modify] the [date/time] to [administrators].

5.1.2.21 FMT_MTD.1(3) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [empty] the [audit logs] and to [modify] the [SYSLOG Severity Threshold] to [administrators].

5.1.2.22 FMT_MTD.1(4) Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [create, modify, delete] the [user account attributes] to [administrators].

Application Note for all FMT_MTD.1: Each administrator has his privilege level. These SFRs are used to restrict the management scope for different administrator.

5.1.2.23 FMT_SMF.1 Specification of management functions

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

1. start-up and shutdown;
2. create, modify, delete, and view configuration data;
3. empty, and review the audit log;
4. create, delete, modify, and view filtering rules;
5. perform configuration backup and restore;
6. user account management;
7. modify date/time;
8. trusted router management and
9. security management functions listed in FMT_MOF.1

   Management of security functions behavior.

5.1.2.24 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.

Application Note: although there is only one administrator role. However each administrator account has his privilege level and corresponding management scope. The management scope of each privilege level is configurable. All commands are assigned a required privilege level. The administrator can execute commands with required privilege levels lower than or equal to his privilege level.

5.1.2.25 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [administrator defined period of inactivity within a range of 1 to 1000 minutes].

5.1.2.26 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [maximum number of concurrent remote sessions on the node, values 16].

5.1.2.27 FTP_ITC.1(1) Inter-TSF trusted channel (SSH)

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

identification of its end points and protection of the communicated 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 require the use of the trusted channel for [

1. user authentication,
2. configure management].

5.1.2.28 FTP_ITC.1(2) Inter-TSF trusted channel (RADIUS/TACACS+)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and RADIUS/TACACS+ server that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

Application Note: for information disclosure, the TSF only protects the password information from disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted channel for [user authentication,].

5.1.2.29 FTP_ITC.1(3) Inter-TSF trusted channel (NTP)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and passive NTP server with MD5 authentication that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall require the use of the trusted channel for [time synchronization,].

5.2 SECURITY ASSURANCE REQUIREMENTS

5.2.1 Security Assurance Requirements

The assurance requirements consist of EAL3+ALC+FLR.2 and are summarized in the following table:

Table 5-2 Security Assurance Requirements (EAL3+)

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_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
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

This page intentionally left blank.

Chapter 6
TOE SUMMARY SPECIFICATION

Table of Contents

6.1 TOE SECURITY FUNCTIONS

6.1.1 Security Auditing

The TOE provides an audit feature for actions related to operator authentication attempts and administrator actions

- FAU_GEN.1 Audit data generation

  All logs are stored in the TOE whenever there is new log generated and then the TOE transferred the log files to SNMP/SYSLOG Servers with SNMP/SYSLOG network protocol through internal network in a constant period time. The log file is stored under the 'data' directory of the flash disk inside the TOE. The ZXROS records the start-up and shutdown of the audit function, security events and the activity of the administrator.

Alarm logging: The security event source is all events that affect attempts to breach system security such as failed login attempts. Security events are generated by the security application.

- authentication alarm
  1. I&A authentication success
  2. I&A authentication failure
- user management alarm
  1. user account is locked
  2. user account is unlocked
  3. user account is enabled
  4. user account is disabled
- RADIUS alarm log
  1. RADIUS authentication group is unreachable
  2. RADIUS accounting server group is unreachable
  3. RADIUS buffer queue exceeds the threshold
- NTP alarm log
  1. The clock of NTP server and client are not synchronized ACL alarm

- ACL alarm
  1. ACL aggregation is too large
- RIP/OSPF/BGP alarm
  1. authentication success
  2. authentication failure

Command logging: all activities performed by the administrator are recorded in the Command log.

The TOE is configured to record all auditable events. Logs are configured in the following contexts:

1. Log file — Log files contain log event message streams.
2. SNMP trap groups — SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.
3. SYSLOG — Information is sent to a SYSLOG host that is capable of receiving selected SYSLOG messages from a network element.
4. Event filters — An event filter defines whether to forward or drop an event or trap based on match criteria.

Log level is associated with the Alarm log to control which events will be logged in the event log based on severity where log level shall be configured at least 6 (basic log level).

- FAU_GEN.2 User identity association

  The TOE is able to associate each auditable event with the identity of the administrator that caused the event. The Command log record is associated with an administrator. Other types of logs are associated with unauthenticated user/application.

- FAU_SAR.1 Audit review

  The administrator reads all the information in the log destinations (i.e., memory, or a file on the local file system) via CLI commands.

The administrator executes the following log commands:

1. Configuration Commands;
2. Log File Commands;
3. Alarm level filter Commands;
4. Show Commands;

- FAU_STG.1, FAU_STG.4 Protected audit trail storage and Prevention of audit data loss

  The TOE protects stored audit records stored inside the TOE from unauthorized deletion and modifications by only allow authenticated and authorized administrator to access the audit trail storage. There is no other interface to access the audit trail storage. However the audit trail stored in the SNMP/SYSLOG server is not protected by the TOE;

  The TSF shall overwrite the oldest stored log file in flash when the maximum allowed number of log files reached. This prevents the newest events from lost.

6.1.2 Identification & Authentication

Authentication services can be handled either internally (fixed passwords) or through an external authentication service, such as a RADIUS or TACACS+ server. An operator's authentication parameters must be valid before access is granted to administrative functions.

- FIA_AFL.1 Authentication failure handling (console)

The following is defined by the administrator: (1) The number of unsuccessful login attempts allowed for the specified time. (2) The lockout period in minutes where the administrator is not allowed to login

When the above situation is satisfied, that administrator is locked out from any further login within a specified period of time. However within the period of locking time, an administrator is allowed to unlock the locked account.

Parameters are modifiable from the provided default values:

1. The ZXROS detects when unsuccessful authentication attempts meet an administrator configurable positive integer (within a range of values 3 – 16)
2. When the defined number of unsuccessful authentication attempts has been met, the ZXROS will at the option of the Administrator prevent activities that require authentication until an action is taken by the Administrator, or until an Administrator defined time period (within a range of values 1 - 1440 minutes) has elapsed.

- FIA_SOS.1 Verification of secrets

The verifications of secrets apply to all authentication methods: local console and remote SSH administration.

The password needs to satisfy the following requirements:

1. A minimum length (characters) default 6 and within a range of 3-32,
2. at least one upper and one lower case character;
3. at least one numeric character must be present in the password; and
4. at least one special character must be present in the password. Special characters include:

   ~!@#$%^&*()_+|{}:"<>?`-=\[];',./.

However the passwords specified in RADIUS/TACACS+ server are not setup through the TOE. So this SFR is only enforced when performing local authentication.

- FIA_UAU.2 User authentication before any action

The TOE is configured to use RADIUS, TACACS+, and local/remote authentication to validate administrators requesting access to the network. The password authentication is processed between RADIUS and local or TACACS+ and local passwords are specifically configured. The order of TACACS+ and local can be configured. The allowed authentication models are listed below:

1. Local only
2. RADIUS only
3. TACAS+ only

4. RADIUS first, if RADIUS not response then local authentication
5. TACACS+ first, if TACACS+ not response then local authentication
6. Local first, if local authentication failed then TACACS+ authentication

Authentication validates an administrator name and password combination when an administrator attempts to log in. When an administrator attempts to log in, the TOE sends an access request to a RADIUS, TACACS+, or local database.

- FIA_UID.2 User identification before any action

The ZXROS validates an administrator name and password combination when an administrator attempts to log in

- FIA_UAU.5 Multiple authentication mechanisms

The ZXROS software supports three kinds of user authentication methods: Local Authentication, Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+). Authentication mechanism can be configured. Administrator can be authenticated any of the above authentication mechanisms based on the specification by authentication.

6.1.3 Security Management

The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Security Audit and Information Flow Control. Administrators configure the TOE via remote/local CLI.

- FMT_MTD.1 Management of TSF Data

Management of TSF Data (Configuration Item and Filtering Rule): The TOE restricts the ability to administer the router configuration item and filtering rule. The CLI provides a text-based interface from which the router configuration can be managed and maintained. From this interface, all TOE functions such as BGP, RIP and MPLS protocols can be managed. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

This CLI interface also provides the administrator with the ability to configure an external authentication server, such as a RADIUS or TACACS+ server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE. If authentication-order includes RADIUS or TACACS+, then these will be consulted in the configured order for all users.

Management of TSF Data (Date/time): The TOE will allow only an administrator to modify the date/time setting on the appliance.

Management of TSF Data (Audit logs): The TOE can be configured to clear audit logs and specify the log level by an administrator.

Management of TSF Data (User Account): The TOE restricts the ability to administer user data to only administrators. The CLI provides administrators with a text-based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted.

- FMT_MOF.1 Management of security functions behavior

The administrator will perform the following:

1. Configure administrator profiles used to deny or permit access to CLI command tree permissions, or specific CLI commands.
2. Configure authentication failure handling configurable integer of unsuccessful authentication attempts within configurable range of time, and configurable lock out period of time that occurs related to a administrator's authentication.
3. Configure authentication-order for local, RADIUS and TACACS+ authentication Enables RADIUS or TACACS+ (TOE client-side).
4. Configure password complexity [numeric] [special-character] [capital] [lowercase] and configure password minimum-length value.
5. Configure ACLs and controls where (e.g., from a specific network address or local management interface) administrators, and authorized IT entities access the TOE.
6. Configures audit logs.
7. Configure SNMP/SYSLOG
8. Configure NTP
9. Configure anti-DoS attack
10. Configure CPU protection policies

- FMT_MSA.1 Management of security attributes

Simple security attributes (unauthenticated policy)

The administrator specifies information flow policy rules (i.e., routing protocols and ingress/egress traffic filtering and peer filtering) that contain information security attribute values, and associate with that rule an action that permits the information flow or disallows the information flow. When a packet arrives at the source interface, the information security attribute values of the packet are compared to each information flow policy rule and when a match is found the action specified by that rule is taken.

Subject and information security attributes used are:

1. IP network address and port of source subject;
2. IP network address and port of destination subject;
3. transport layer protocol and their flags and attributes (UDP, TCP);
4. network layer protocol (IP, ICMP);
5. interface on which traffic arrives and departs; and
6. routing protocols and their configuration and state.

Simple security attributes (export policy)

The event log is configured to send events to one SYSLOG destination. SYSLOG destinations have the following properties:

1. SYSLOG server IP address.
2. The UDP port used to send the SYSLOG message.
3. The SYSLOG Facility Code (0 - 23): default 16 (local 0).
4. The SYSLOG Severity Threshold (0 - 7) - events exceeding the configured level will be sent.

The Administrator uses CLI syntax to configure the TOE to send SNMP trap.

Subject and information security attributes used are:

1. Source subject security attributes: and
2. Destination subject security attributes:
3. IP address of the SNMP trap receiver;
4. UDP port used to send the SNMP trap;
5. SNMPv3 used to format the SNMP notification; and
6. Security name and level for SNMPv3 trap receivers;

- FMT_MSA.3 Static attribute initialization

By default, there is no routing/filter rule configured on the router for UNAUTHENTICATED SFP, also there is no log server setup for EXPORT SFP.

- FMT_SMF.1 Specification of management functions

The Administrator performs the following security management functions:

1. start-up and shutdown;
2. create, modify, delete, and view configuration data
3. empty, and review the audit log
4. create, delete, modify, and view filtering rules;
5. perform configuration backup and restore;
6. user account management;
7. modify date/time;
8. trusted router management and
9. security management functions listed in FMT_MOF.1 Management of security functions behavior.

FMT_SMR.1 Security roles

The TOE allows all authorized administrators with the needed authority to configure and control the associated features. Only authenticated administrators are permitted to use or manage the TOE resources. Only authenticated administrators execute certain CLI commands. Authorization features allow administrators to configure administrator profiles which are used to limit what CLI commands are executed by the specific authenticated administrator. Once an administrator has been authenticated the ZXROS is configured to perform authorization. Each command has a corresponding privilege level (0-15) which can be modified by the administrator. These levels associate with users. An authenticated user must belong to a certain privilege level. An authenticated administrator shall only execute commands allowed by his privilege level and can not execute commands of higher level.

6.1.4 TOE Access

Mechanisms place controls on administrator's sessions. Local and remote administrator's sessions are dropped after an Administrator-defined time period of inactivity. Dropping the connection of a local and remote session (after the specified time period) reduces the risk

of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session.

- FTA_SSL.3 TSF-initiated termination

The ZXROS allows configuring login control parameters for console and remote administration sessions.

The ZXROS has the ability to terminate stale connections. The ZXROS terminates interactive session after an administrator defined period of inactivity with a default value of 30 minutes, and within a range of 1 to 1000 minutes. And the ZXROS can configure mandatory termination absolute-time within from 1 to 10000 minutes.

This idle-time parameter configures the idle timeout for console, or remote sessions before the session is terminated by the system. The idle-time and absolute-time would reduce the chance for the unauthorized administrators to access the TOE through an unattended opened session. By default, an idle console, or remote session times out after 30 minutes of inactivity. This timer is set for all session.

- FTA_TSE.1 TOE session establishment

The ZXROS will deny session establishment after 16 active remote sessions is reached. An administrator can configure ACLs to refuse to establishment of a connection, to ensure only connections from trusted address or port is trustable.

The ZXROS has a direct connection via the physical RS232 console interface and a remote console connection to perform security management functions.

6.1.5 User data protection

The TOE provides an Information Flow Control mechanism that supports control of the flow of traffic generated by the network devices. The Information Flow Control Policies are configured on each network devices to allow traffic to only flow between the authorized sources and authorized destinations. Also the TOE provide exporting log to SYSLOG and SNMP servers.

- FDP_IFC.1(1) Subset information flow control (unauthenticated policy)

The TOE enforces an UNAUTHENTICATED SFP whereby the network packets sent and/or received through the TOE to IT entity.

- FDP_IFC.1(2) Subset information flow control (export policy)

The TOE enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap and SYSLOG destinations. The TOE will only send audit and management data to properly configured destinations

- FDP_IFF.1(1) Simple security attributes (unauthenticated policy)

The TOE supports routing of the traffic that is permitted by the information flow policies. All traffic passing through the router is processed by the ACL attached to the interface/protocol. The ACL is processed top-down, with processing continuing until the first match is made according to the source/destination and security attributes in the packet.

All traffic that successfully passedthe ACLs is processed by the routing tables. The routing table may be statically updated by an administrator or dynamically generated according to RIPv2, OSPFv2, and BGPv4 routing protocols.

The TOE explicitly denies packets based on the following rule:

1. where the source identity of the information is not included in the set of source identifiers for the source subject;
2. requests for access or services where the source identity of the packet specifies a broadcast identity;
3. requests for access or services where the presumed source identity of the packet specifies a loopback identifier.
4. packets does not correspond to an entry in the routing table.
5. packets that do not conform to IP protocol or the associated routing protocol specification (RFCs for RIPv2, OSPFv2, BGPv4)].

The TOE suppresses the attacks when the statistics of semi-connection of the TCP SYN flood exceeds configured threshold (Anti-DoS).

Subject and information security attributes used are:

1. IP network address and port of source subject;
2. IP network address and port of destination subject;
3. transport layer protocol and their flags and attributes (UDP, TCP);
4. network layer protocol (IP, ICMP);
5. interface on which traffic arrives and departs; and
6. routing protocols and their configuration and state.

- FDP_IFF.1(2) Simple security attributes (export policy)

The TOE also enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap and SYSLOG destinations.

Subject and information security attributes used are:

1. [Source subject security attributes: source network identifier; and
2. Destination subject security attributes:
    a. IP address of SYSLOG server;
    b. UDP port used to send the SYSLOG message;
    c. SYSLOG Facility Code;
    d. SYSLOG Severity Threshold;
    e. Set of destination network identifiers;
    f. IP address of the SNMP trap receiver;
    g. UDP port used to send the SNMP trap;
    h. SNMPv3 used to format the SNMP notification; and
    i. Security name and level for SNMPv3 trap receivers

For SNMP traps sent packet through the port of the TOE, the source IP address of the trap is the port IP address of the TOE.

The SYSLOG protocol is used to convey event notification messages. Parameters are defined identified in RFC 3164 *The SYSLOG Protocol* which describes the format of a SYSLOG message.

The TOE shall permit the log data to be exported to the SNMP/SYSLOG server when the destination IP address and port of the log packets match the configured server information.

- FDP_UIT.1 Data exchange integrity

The TOE transmits and receives routing data (RIPv2, OSPFv2 mode 2, and BGPv4) to/from trusted routers in the manner of protecting the routing information from modification.

6.1.6 Trusted Channel

The TOE provide secure channel for RADIUS/TACACS+ server, NTP server and the remote terminal to connect to the TOE.

- FTP_ITC.1

The TSF shall provide a communication channel between itself and a remote administration client. Secure remote administration is provided by SSH. The communication between TOE and RADIUS/TACACS+/NTP server is protected by the trusted channel.

This page intentionally left blank.

Chapter 7
RATIONALE

Table of Contents

7.1 RATIONALE FOR SECURITY OBJECTIVES

7.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats/OSP that the TOE is intended to counter. Since the Security Objectives for the TOE were derived directly from the threats/OSP there is a one to one mapping between them. It is also clear since the Security Objectives for the TOE are simply a restatement of the applicable threat/OSP, that each objective is suitable to meet its corresponding threat/OSP.

Table 7-1 Mapping of Security Objectives to Threats/OSP

	O.AUDIT_REVIEW	OE.AUDIT_REVIEW	O.MANAGE	O.IDAUTH	O.MEDIATE	O.TOE_ACCESS	O.ROUTE
T.AUDIT_REVIEW	×	×					
T.NO_PRIVILEGE			×				
T.MEDIATE					×		
T.NO_AUTH_SESSION						×	
T.NO_AUTH_ACCESS				×			
P.ROUTE							×

7.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those assumptions that must be met. Since the Security Objectives for the Operational environment were derived directly from the Assumptions there is a one to one mapping between them. It

is also clear since the Security Objectives for the Operational environment are simply a restatement of the applicable assumption, that each objective is suitable to meet its corresponding assumption.

Table 7-2 Mapping of Assumptions to Security Objectives for the Operational Environment

	OE.NO_EVIL&TRAIN	OE.CONNECTIVITY	OE.PHYSICAL	OE.TIMES	OE.USERS
A.NO_EVIL&TRAIN	×				
A.CONNECTIVITY		×			
A.PHYSICAL			×		
A.TIMES				×	
P.USERS					×

7.2 SECURITY REQUIREMENTS RATIONALE

7.2.1 Rationale for TOE security functional requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

Table 7-3 Mapping of Security Functional Requirements to TOE Security Objectives

	O.AUDIT_REVIEW	O.MANAGE	O.IDAUTH	O.MEDIATE	O.TOE_ACCESS	O.ROUTE
FAU_GEN.1	×					
FAU_GEN.2	×					
FAU_SAR.1	×					
FAU_STG.1	×					
FAU_STG.4	×					
FDP_IFC.1(1)				×		
FDP_IFF.1(1)				×		
FDP_IFC.1(2)				×		
FDP_IFF.1(2)				×		
FDP_UIT.1						×
FIA_AFL.1			×			
FIA_SOS.1			×			
FIA_UAU.2			×			

	O.AUDIT_REVIEW	O.MANAGE	O.IDAUTH	O.MEDIATE	O.TOE_ACCESS	O.ROUTE
FIA_UAU.5			×			
FIA_UID.2			×			
FMT_MOF.1		×				
FMT_MSA.1		×		×		
FMT_MSA.3		×		×		
FMT_MTD.1(1)		×				
FMT_MTD.1(2)		×				
FMT_MTD.1(3)		×				
FMT_MTD.1(4)		×				
FMT_SMF.1		×				
FMT_SMR.1		×				
FTA_SSL.3					×	
FTA_TSE.1					×	
FTP_ITC.1(1)		×			×	
FTP_ITC.1(2)			×			
FTP_ITC.1(3)	×					

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Table 7-4 Mapping of the rationale of TOE Security Requirements to Objectives.

OBJECTIVES	SFR Rationale
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.	This objective is met by: ● FAU_GEN.1 and FAU_GEN.2 outline what events must be audited and if possible a user identity is associated. ● FAU_SAR.1 requires that the audit trail can be read. ● FAU_STG.1 requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions ● FAU_STG.4 requires that unauthorised deletion of audit records does not occur, and thus helps to maintain accountability for actions

OBJECTIVES	SFR Rationale
	• FTP_ITC.1(3) requires that the timestamp is protected by trusted channels.
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.	This objective is met by: • FMT_MOF.1 allows the authorized users (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable. • FMT_MSA.1 and FMT_MSA.3 assist in effective security attribute management. • FMT_MTD.1 restricts the administrator's ability to modify the TSF data. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based. • FTP_ITC.1(1) requires that a trusted channel between the TSF and the remote client be provided for remote administration.
O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.	This objective is met by: • FIA_AFL.1 requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs. • FIA_SOS.1 specifies metrics for authentication to restrict access. • FIA_UAU.2 ensures that users are authenticated to the TOE to restrict access. • FIA_UAU.5 was selected to ensure that appropriate authentication mechanisms can be selected to restrict access. • FIA_UID.2 ensures that users are identified to the TOE to restrict access. • FTP_ITC.1(2) requires that a trusted channel between the TSF and the RADIUS/TACACS+ be provided for user authentication.

OBJECTIVES	SFR Rationale
O.MEDIATE The TOE shall control the flow of information among its network connections according to routing rules and BGPv4/OSPFv2/RIPv2 routing protocol	This objective is met by: ● FDP_IFC.1(1) identifies the entities involved in the unauthenticated Information Flow Control SFP (i.e. external IT entities sending packets). ● FDP_IFF.1(1) identifies the conditions under which information is permitted to flow between entities (the unauthenticated Information Flow Control SFP). ● FDP_IFC.1(2) identifies the entities involved in the export Information Flow Control SFP (i.e. external IT entities sending packets). ● FDP_IFF.1(2) identifies the conditions under which information is permitted to flow between entities (the export Information Flow Control SFP). ● FMT_MSA.1 restricts the ability to modify, delete, or query the parameters for the unauthenticated SFP to an administrator. ● FMT_MSA.3 ensures that there is a default-deny policy for the unauthorized SFP.
O.TOE_ACCESS The TOE will provide mechanisms that control an administrator's logical access to the TOE and to explicitly deny access to specific administrators when appropriate.	This objective is met by: ● FTA_SSL.3 The TOE will terminate an interactive session after an administrator defined time interval of administrator inactivity. ● FTA_TSE.1 provides requirements for denying user's access to the TOE based on attributes. ● FTP_ITC.1(1) requires that a trusted channel between the TSF and the remote client be provided for remote administration.
O.ROUTE The TOE shall be able to accept routing data from trusted routers according to BGPv4/OSPFv2/RIPv2.	This objective is met by: ● FDP_UIT.1 transmits and receives routing data to/from trusted routers in a manner protected from modification, insertion and replay errors.

7.2.2 Rationale for Security Assurance Requirements

The ST requires EAL3 augmented with ALC_FLR.2 assurance. EAL3 augmented with ALC_FLR.2 was chosen because it is based upon good commercial development

practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOE. ALC_FLR.2 demonstrates a sound regime for addressing identified security flaws.

7.2.3 Functional Requirement Dependencies Rationale

The following table presents a mapping of the TOE Security Requirements dependencies.

Table 7-5 Security Functional Requirement Dependencies

SFR	Dependency	SATISFIED
FAU_GEN.1	FPT.STM.1	This is satisfied in the operational environment by OE.Times.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Y FIA_UID.1 Hierarchical to FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Y
FAU_STG.1	FAU_GEN.1	Y
FAU_STG.4	FAU_GEN.1	Y
FDP_IFC.1(1)	FDP_IFF.1(1)	Y
FDP_IFC.1(2)	FDP_IFF.1(2)	Y
FDP_IFF.1(1)	FDP_IFC.1(1) FMT_MSA.3	Y
FDP_IFF.1(2)	FDP_IFC.1(2) FMT_MSA.3	Y
FDP_UIT.1	FDP_ACC.1/FDP_IFC.1 FTP_ITC.1/FTP_TRP.1 1. The dependency on FDP_ACC.1/FDP_IFC.1 is unnecessary since the reference to the policy was refined away. Defining a whole policy to restate FDP_UIT.1 was considered unnecessary. 2. The dependency on FTP_ITC.1 is unnecessary since this SFR specifies confidentiality of the channel data and this is not required. 3. The dependency on FTP_TRP.1 is unnecessary, since a trusted	Y

SFR	Dependency	SATISFIED
	router is not a user but a trusted IT product. There is no applicable dependency.	
FIA_AFL.1	FIA_UAU.1	Y FIA_UAU.1 Hierarchical to FIA_UAU.2
FIA_SOS.1	No dependencies	Y
FIA_UAU.2	FIA_UID.1	Y
FIA_UAU.5	No dependencies	Y
FIA_UID.2	No dependencies	Y
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Y
FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Y
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Y
FMT_MTD.1(1)	FMT_SMR.1 FMT_SMF.1	Y
FMT_MTD.1(2)	FMT_SMR.1 FMT_SMF.1	Y
FMT_MTD.1(3)	FMT_SMR.1 FMT_SMF.1	Y
FMT_MTD.1(4)	FMT_SMR.1 FMT_SMF.1	Y
FMT_SMF.1	No dependencies	Y
FMT_SMR.1	FIA_UID.1	Y
FTA_SSL.3	No dependencies	Y
FTA_TSE.1	No dependencies	Y
FTP_ITC(1)	No dependencies	Y
FTP_ITC(2)	No dependencies	Y
FTP_ITC(3)	No dependencies	Y

There are no unsatisfied dependencies.

This page intentionally left blank.

Appendix A
Document Terminology

The following terms are listed here to aid the reader of the ST:

Table A-1 Document Terminology

ACL	Access Control List	It is filter policy applied on ingress or egress to a service device on an interface to control the traffic access.
ATM	Asynchronous Transfer Mode	ATM is a standardized digital data transmission technology. ATM is a cell-based switching technique that uses asynchronous time division multiplexing.
BGP	Border Gateway Protocol	The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rulesets.
CLI	Command Line Interface	A text based administrator interface to configure a IT node.
LAN	Local Area Network	A system designed to interconnect computing devices over a restricted geographical area (usually a couple of kilometers)
MAC	Media Access Control	A media-specific access control protocol within IEEE802 specifications. The protocol is for medium sharing, packet formatting, addressing, and error detection.
MPLS	Multi-Protocol Label Switching	MPLS technology implements the delivery of highly scalable, differentiated, end-to-end IP and VPN services. The technology allows core network routers to operate at higher speeds without examining each packet in detail, and allows differentiated services.
OSPF	Open Shortest Path First	A link-state routing algorithm that is used to calculate routes based on the number of routers, transmission speed, delays and route cost.

RADIUS	Remote Authentication Dial-In User Service	A client/server security protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize access to the requested system or service.
RFC	Request for Comments	An Internet Engineering Task Force (IETF) memorandum on Internet systems and standards
RIP	Routing Information Protocol	RIP is based on distance-vector algorithms that measure the shortest path between two points on a network, based on the addresses of the originating and destination devices. The shortest path is determined by the number of “hops” between these points. Each router maintains a routing table, or routing database, of known addresses and routes; each router periodically broadcasts the contents of its table to neighboring routers in order that the entire network maintain a synchronized database.
QoS	Quality of Service	A set of performance parameters that characterize the traffic over a given connection
TCP	Transmission Control Protocol	TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
TACACS+	Terminal Access Controller Access Control System Plus	An authentication protocol that allows a remote access server to forward an administrator's logon password to an authentication server to determine whether access is allowed to a given system.
UDP	User Datagram Protocol	UDP is transport layer protocol which do not guarantee delivery of data
VPN	Virtual Private Network	A way to provide secure and dedicated communications between a group of private servers over public Internet.

Tables