Juniper your Net.

Security Target for Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2

Version 1.0
January 30, 2009

Prepared for:
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale
California 94089
USA

Prepared by:
IconSecurity Ltd

Contents

List of tables

1 ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference: Juniper Networks EX3200 and EX4200 switches running JUNOS 9.3R2.8.

ST Reference: Security Target for Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2.

ST Version: Version 1.0.

ST Date: January 30, 2009.

Assurance Level: Evaluation Assurance Level (EAL) 3 augmented with ALC_FLR.3.

ST Author: IconSecurity Ltd

Keywords: Router, IP, Service Manager

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

The TOE is an EX3200 and EX4200 switch providing a wide variety of services to the user.

The switch routes IP traffic over any type of network, with increasing scalability of the traffic volume with each switch model. All packets on the monitored network are scanned and then compared against a set of rules to determine where the traffic should be routed, and then passed to the appropriate destination.

1.3 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 1, September 2006, CCMB-2006-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 2, September 2007, CCMB-2007-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 2, September 2007, CCMB-2007-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004.

[9.3R1_ST] Security Target for Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1, Version 1.0.

1.3.1 TOE Type

The TOE is a switch router (appliance) providing a wide variety of services. The IP switching and routing services are considered in the evaluation.

Management via the CLI and GUI interfaces is considered in the evaluation, although the provision of the GUI communicating via JUNOScript (e.g. JWeb and JUNOScope) is outside the scope of this evaluation.

1.3.2 Required non-TOE hardware/software/firmware

To enable the TOE to communicate with external network entities, the TOE requires physical network interfaces (e.g. Line Cards) to be installed in the switch, as described in section 1.4 below).

1.4 TOE Description

The TOE platforms are designed to provide an efficient and effective IP switch solution that can be managed centrally.

1.4.1 EX Switch

The EX-series platforms provide high-performance, carrier-class networking solutions, supporting a variety of high-speed Ethernet interfaces for medium/large networks. The EX-series platforms share common JUNOS software with the routers, such that control plane features are implemented consistently with those of the routers.

The EX-series platforms are designed as hardware devices, featuring complete Layer 2 and Layer 3 switching capabilities. The EX-series platforms are powered by the same JUNOS modular architecture as the routers. The hardware abstraction layer allows control-plane features to be written once and implemented seamlessly on the underlying hardware. This modular approach also enhances fault-tolerance, as each JUNOS software protocol daemon run in its own protected memory space and can be gracefully restarted independently without impacting the rest of the system.

The platform is physically self-contained, housing the software, firmware and hardware necessary to perform all (layers 2 & 3) network forwarding functions. The hardware has two components: the platform itself and the Line Cards[1] (I/O card) installed in the platform. The various Line Cards installed in the platforms allow it to communicate with the Ethernet networks with the required level of performance.

As with the routers, the EX-series Ethernet platform architecture cleanly separates network switching and control functions from the packet forwarding operations, permitting the platform to maintain a high level of availability. Similarly, each platform consists of two major architectural components:

- The Routing Engine (RE), which provides Layer2 and Layer 3 Ethernet switching and network management;
- The Packet Forwarding Engine (PFE), which provides all operations necessary for packet forwarding.

EX-series platforms use an ASIC based PFE, as in the M- series, MX-Series and T-series routers (see [9.3R1_ST]). The EX3200 and EX4200 are fixed format.

[1] The Line Cards are a monolithic blade.

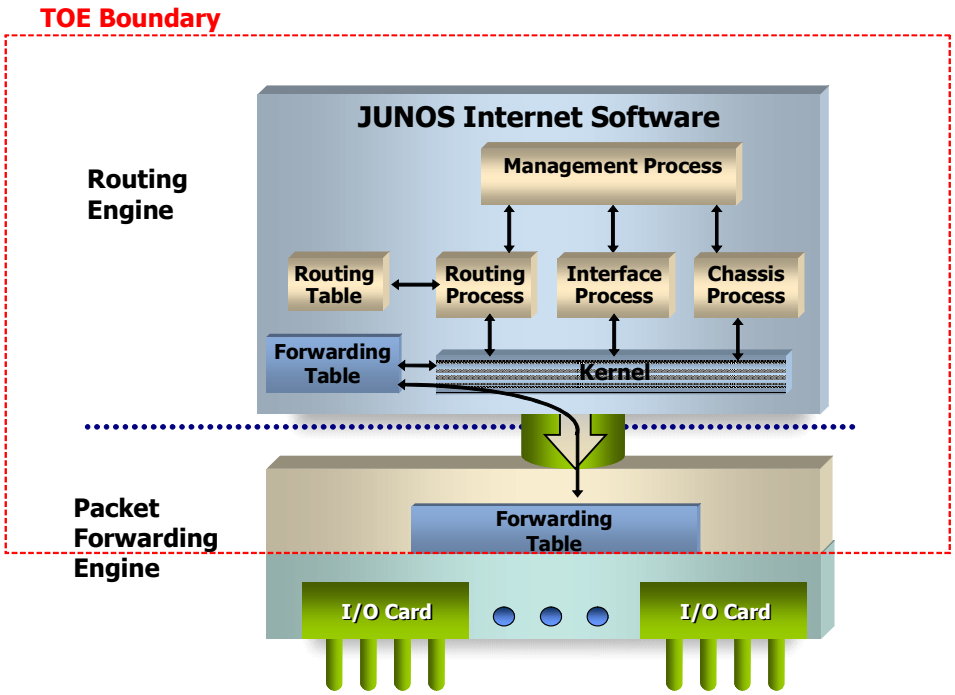
1.5 TOE Boundaries

The TOE includes both physical and logical boundaries.

1.5.1.1 Physical Boundary

The TOE is a software and firmware only TOE operating within the physical boundary of the appliance.

The TOE includes the software implementing the Routing Engine and the software and ASICs implementing the Packet Forwarding Engine. The Line Cards and other appliance hardware components are outside the scope of the TOE.



The interfaces to the TOE are twofold: the switching/routing interfaces and the management interfaces. The management interfaces include the TOE console interface through which the appliance can be managed locally and the in-band management interface via the network interfaces.

The following appliance models are covered by this evaluation:

EX3200
EX4200

1.5.1.2 Logical Boundaries

The logical boundaries of the TOE are defined by the functions that can be carried out at the TOE external interfaces. These functions include network information flow control, identification and authentication for the administrative functions, access control for administrative functions, management of the security configurations, audit and protection of the TOE itself.

- Information Flow Control

The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users.

- Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides three levels of authority for users, providing administrative flexibility (additional flexibility is provided in JUNOS, but is outside the scope of the evaluation). Super-users have the ability to define groups and their authority and they have complete control over the TOE.

The appliances also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, including telnet (out of scope), SSH, SSL, and FTP[2].

Authentication services can be handled either internally (user selected passwords) or through a RADIUS or TACACS+ authentication server in the IT environment (the external authentication server is considered outside the scope of the TOE). For SSH only Public Key Authentication such as RSA can be used for the validation of the user credentials, but the user identity and privileges are still handled internally.

- Security Management

The appliance is managed using XML RPCs (JUNOScript), either through raw XML (API mode) as in the case of J-Web (over HTTP) and JUNOScope (over SSL) or through a Command Line Interface (CLI) protected by SSH. Both interfaces provide equivalent management functionality. Through these interfaces all management can be performed, including user management and the configuration of the switch functions. The CLI interface is accessible through an SSH session, or via a local terminal console.

Net conf is an IETF standardization effort which is closely aligned to JUNOScript. JUNOS only supports netconf via SSH transport, and authentication is handled by SSH.

- Audit

JUNOS auditable events are stored in the syslog files, and although they can be sent to an external log server, the requirements for auditing are met by local storage. Audit events cover authentication activity and configuration changes. Audit records include the date and time, event category, event type, username. An accurate time is gained by the appliance ntp daemon, acting as a client, from an NTP server in the IT environment.

[2] Only the FTP Client is within the scope of the evaluation,

(The NTP server is considered outside the scope of the TOE.) This external time source allows synchronization the TOE audit logs with external audit log servers in the environment. The audit log can be viewed only by a super-user. Search and sort facilities are provided.

- Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all routing functions of the TOE are confined to the appliance itself. The switch is completely self-contained, and are therefore maintains its own execution domain.

- Each sub-component of the appliance software operates in an isolated execution environment, protected from accidental or deliberate interference by others.

- The entire software environment is protected from accidental or deliberate corruption via use of digitally signed binaries.

1.5.1.3 Summary of items out of scope of the TOE

There are no security functionality claims relating to the following items:

- All hardware, including that associated with forwarding interfaces Line Cards
- External servers (audit, NTP, authentication, FTP servers)
- Encryption and integrity checking functionality
- High availability functionality

The following items are out of the scope of the evaluation:

- Use of the auxiliary port
- Use of Telnet
- Use of SNMP
- Use of out-of-band management ports (Management Ethernet interfaces)
- Packet filtering (other than simple access control to restrict the source address for management traffic)
- Media use (other than during installation of the TOE)

The *Security Configuration Guide for Common Criteria and JUNOS-FIPS* details functionality that should/should not be configured to adhere to the evaluated configuration.

2 CC Conformance

CC Identification:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 1, September 2006, CCMB-2006-09-001.
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 2, September 2007, CCMB-2007-09-002.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 2, September 2007, CCMB-2007-09-003.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004.

All applicable international and UK national interpretations up to 12 Dec 2008 are applied. Where specific changes result from application of an interpretation or precedent this is noted in the security target.

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of EAL3 augmented with ALC_FLR.3.

This ST does not claim conformance to any PPs.

3 Security Problem Definition

The security problem definition (SPD) describes the security problem to be addressed.

The statement of TOE security environment defines the following:

- Threats to be countered by the TOE, its operational environment, or a combination of the two;
- Assumptions made on the operational environment in order to be able to provide security functionality;
- Organizational security policies with which the TOE, its' operational environment, or a combination of the two are to enforce.

3.1 Threats

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

- 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
- Assets are entities that someone places value upon – the assets are access to network services,
- 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.

The TOE is intended to protect IP packets against incorrect routing caused by unauthorized changes to the network configuration.

T.ROUTE	Network packets may be routed inappropriately due to accidental or deliberate misconfiguration.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.
T.OPS	An unauthorized process or application may gain access to the TOE security functions and data, inappropriately changing the configuration data for the TOE security functions.
T.MANDAT	Unauthorized changes to the network configuration may be made through interception of in-band switch management traffic on a network
T.CONFLOSS	Failure of network components may result in loss of configuration data that cannot quickly be restored.
T.NOAUDIT	Unauthorized changes to the switch configurations and other management information will not be detected.

T.THREAT Since attackers on the network have no interface to the management functions the likelihood of attack from this route is low.

3.2 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

3.3 Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 Physical Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.2 Personnel Assumptions

A.NOEVIL The authorized users will be competent, and not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.3.3 IT Environment Assumptions

A.EAUTH External authentication services will be available via either RADIUS, TACACS+, or both.

A.TIME External NTP services will be available.

A.CRYPTO In-band management traffic will be protected using SSL or SSH.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

O.FLOW	The TOE shall ensure that network packets flow from source to destination according to available routing information.
O.PROTECT	The TOE must protect against unauthorized accesses and disruptions of TOE functions and data.
O.EADMIN	The TOE must provide services that allow effective management of its functions and data.
O.AMANAGE	The TOE management functions must be accessible only by authorized users.
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.
O.ROLBAK	The TOE must enable rollback of switch configurations to a known state.
O.AUDIT	Users must be accountable for their actions in administering the TOE.
O.EAL	The TOE must be certified to EAL3 augmented with ALC_FLR.3.

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.EAUTH	A RADIUS server, a TACACS+ server, or both must be available for external authentication services.
OE.TIME	NTP server(s) will be available to provide accurate/synchronised time services to the switch.
OE.CRYPTO	SSL or SSH must be enabled for all in-band management traffic.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.ADMIN	Authorized users must follow all administrator guidance.

5 Extended Component Definition

There are no extended components required for this ST as all requirements are drawn from Common Criteria Parts 2 and 3.

6 IT Security Requirements

6.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
  - The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. For an example, see FMT_SMF.1 in this security target.
  - The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by [*italicized text within square brackets*]. For an example, see FMT_MSA.3 in this security target.
  - The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value]. For an example, see FAU_GEN.1 in this security target.
  - The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration sequence letter following the component identifier. For example, see FMT_MTD.1 in this security target.
- Three levels of user privilege are provided by the TOE: read-only user, operator user and super-user. The term “user” is used when all three categories are included. All users are administrative users.

6.2 Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE, organised by CC class. Table 6-1identifies all SFRs implemented by the TOE. Following the table the components are listed, showing completed operations.

Security Functional Class	Security Functional Components
Audit (FAU)	Security alarms (FAU_ARP.1)
	Audit review (FAU_SAR.1)
	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Potential violation analysis (FAU_SAA.1)
	Protected audit trail storage (FAU_STG.1)
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
	Rollback (FDP_ROL.1)

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Verification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	Multiple authentication mechanisms (FIA_UAU.5)
	User identification before any action (FIA_UID.2)
Security management (FMT)	Management of security functions behaviour (FMT_MOF.1a)
	Management of security functions behaviour (FMT_MOF.1b)
	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (Switch configuration) (FMT_MTD.1a)
	Management of TSF data (User attributes) (FMT_MTD.1b)
	Management of TSF data (Audit logs) (FMT_MTD.1c)
	Management of TSF data (Date/time) (FMT_MTD.1d)
	Management of TSF data (Sessions) (FMT_MTD.1e)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Time stamps (FPT_STM.1)
TOE access (FTA)	TOE session establishment (FTA_TSE.1)

Table 6-1 Security Functional Components

6.2.1 Audit (FAU)

6.2.1.1 Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall take [the following configurable actions: create a log entry and drop connection] upon detection of a potential security violation.

6.2.1.2 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [User login/logout;
d) Login failures;
e) Committing the TOE configuration;
f) Changing the TOE configuration].

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [no additional information].

6.2.1.3 User identity association (FAU_GEN.2)

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.

6.2.1.4 Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1
The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2
The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;
b) [No other events].

6.2.1.5 Audit review (FAU_SAR.1)

FAU_SAR.1.1
The TSF shall provide [super-users and operators] with the capability to read [all information] from the audit records.

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

6.2.1.6 Protected audit trail storage (FAU_STG.1)

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.

6.2.2 User data protection (FDP)

6.2.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1
The TSF shall enforce the [UNAUTHENTICATED SFP] on
a.) [subjects:
- unauthenticated external IT entities that send and receive packets through the TOE to one another;

b.) information (packets):
- network packets sent through the TOE from one subject to another;

c.) operation:
- route packets].

6.2.2.2 Simple security attributes (FDP_IFF.1)

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

b.) information security attributes:
- presumed address of source subject
- presumed address of destination subject
- network layer protocol
- TOE interface on which packet arrives and departs
- service]

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:
a.) [subjects on a network can cause packets to flow through the TOE to another connected network if:
- all the packet security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the packet security attributes, created by the authorized user;
- the presumed address of the source subject, in the packet, is consistent with the network interface it arrives on;
- and the presumed address of the destination subject, in the packet, can be mapped to a configured nexthop].

FDP_IFF.1.3
The TSF shall enforce the [no additional UNAUTHENTICATED SFP rules].

FDP_IFF.1.4
The TSF shall explicitly authorise an information flow based on the following rules: [no additional rules that explicitly authorise information flows].

FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: [no additional rules that explicitly deny information flows].

6.2.2.3 Basic rollback (FDP_ROL.1)

FDP_ROL.1.1
The TSF shall enforce [the management access control policy[3]] to permit the rollback of the [committed configuration change] on the [router tables].

FDP_ROL.1.2
The TSF shall permit operations to be rolled back within the [limit of any of the last 50 committed configurations or a designated “golden” configuration].

6.2.3 Identification and authentication (FIA)

6.2.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

[3] As specified by FMT requirements

The TSF shall maintain the following list of security attributes belonging to individual users: [
a) User identity;
b) Authentication data;
c) Privileges].

6.2.3.2 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [password minimum length of 6 characters with at least one change of character set (upper, lower, numeric, punctuation, other)].

6.2.3.3 User authentication before any action (FIA_UAU.2)[4]

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

6.2.3.4 User identification before any action (FIA_UID.2)

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.

6.2.3.5 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1
The TSF shall provide [internal password mechanism, SSH public key and external server (RADIUS or TACACS+) mechanism] to support user authentication.

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

6.2.4 Security management (FMT)

6.2.4.1 Management of security functions behaviour (FMT_MOF.1a)

FMT_MOF.1.1a
The TSF shall restrict the ability to [*modify the behaviour of*] the functions [security violation pattern identification[5]] to [super-users].

6.2.4.2 Management of security functions behaviour (FMT_MOF.1b)

FMT_MOF.1.1b
The TSF shall restrict the ability to [*modify the behaviour of*] the functions [type of identification and authentication] to [super-users].

6.2.4.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

[4] Use of FIA_UAU.2 (rather than FIA_UAU.1) is not intended to preclude the passage of IP packets through the router without authentication. Such traffic is identified by means of an IP address, but is not authenticated. In the terms of this ST, those originating packets are not users.
[5] The only security violation pattern that is configurable is that associated with authentication attempts via Login (from the CLI).

The TSF shall enforce the [UNAUTHENTICATED 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 [super-users] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 Management of TSF data (Switch configuration) (FMT_MTD.1a)

FMT_MTD.1.1a
The TSF shall restrict the ability to [modify] the [router[6] configuration data] to [super-users].

6.2.4.5 Management of TSF data (User attributes) (FMT_MTD.1b)

FMT_MTD.1.1b
The TSF shall restrict the ability to [modify] the [user account attributes] to [super-users].

6.2.4.6 Management of TSF data (Audit logs) (FMT_MTD.1c)

FMT_MTD.1.1c
The TSF shall restrict the ability to [delete] the [audit logs] to [super-users].

6.2.4.7 Management of TSF data (Date/time) (FMT_MTD.1d)

FMT_MTD.1.1d
The TSF shall restrict the ability to [modify] the [date/time] to [super-users].

6.2.4.8 Management of TSF data (Sessions) (FMT_MTD.1e)

FMT_MTD.1.1e
The TSF shall restrict the ability to [modify] the [rules that restrict the ability to establish management sessions] to [super-users].

6.2.4.9 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1
The TSF shall be capable of performing the following **security** management functions: [modify router configuration (including rollback of configuration and control of management session establishment), modify user account attributes (including operation of identification and authentication), delete audit logs, modify the date/time, modify security pattern matching for identification of potential violations].

6.2.4.10 Security roles (FMT_SMR.1)

FMT_SMR.1.1
The TSF shall maintain the roles [read-only user, operator user, super-user].

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

6.2.5 Protection of the TOE security functions (FPT)

6.2.5.1 Time stamps (FPT_STM.1)

FPT_STM.1.1

[6] The term "router configuration" in this context applies to both routers and switches

The TSF shall be able to provide reliable time stamps.

6.2.6 TOE access (FTA)

6.2.6.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1
The TSF shall be able to deny session establishment based on [presumed origin of the request].

6.3 Security Assurance Requirements

The following table describes the TOE security assurance requirements drawn from Part 3 of the CC. The security assurance requirements represent EAL3 augmented with ALC_FLR.3.

Assurance Class	**Assurance Components**
Security Target (ASE)	*ST introduction (ASE_INT.1)*
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	*Security architecture description (ADV_ARC.1)*
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	*Operational user guidance (AGD_OPE.1)*
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	*Authorisation controls (ALC_CMC.3)*
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Systematic flaw remediation (ALC_FLR.3)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)

Vulnerability assessment (AVA)	*Vulnerability analysis (AVA_VAN.2)*

Table 6-3 TOE Assurance Components

7 TOE Summary Specification

7.1 TOE Security Functions

7.1.1 Information flow function

FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes

The TOE is designed primarily to route unauthenticated network traffic. Network traffic represents information flows between source and destination network entities. The specific routing of traffic is based on the routing configuration data that has been created by the TOE users or has been collected (e.g., ARP, BGP) from network peers as defined by the TOE users. The routing decision is based on the presumed source and destination address of the packet, the network layer protocol, service and the interface on which the packet arrives and is to depart on.

FDP_ROL.1 Basic rollback

JUNOS maintains a history of up to 50 versions of the configuration, and can rollback to any of them on request. In addition a configuration can be saved as the rescue ("golden") configuration, without risk of it scrolling off the rollback history. When the appliance is booting, if the primary configuration is missing or corrupt, the rescue configuration will be loaded if present, other wise the first rollback will be loaded if possible. If all else fails a factory default configuration will be loaded.

7.1.2 Identification and authentication function

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password, public key) and privilege (user class). The super-user can export the authentication process to a RADIUS/TACACS+ server.

If a user is authenticated remotely, a template user account on the TOE may be used to determine the privileges, rather than specifying privileges for each user. In this instance, a template user account is configured on the TOE and an individual user account is configured on the external authentication server. When the authentication server successfully authenticates the user they pass the unique username and the template account the username is to be associated with back to the TOE. The user name that was authenticated is used when generating audit records regarding activity by that user.

FIA_SOS.1 Verification of secrets

Locally stored authentication data for password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 6 characters with at least one change of character set (upper, lower, numeric, punctuation, other), and can be up to 127 ASCII characters in length (control characters are not recommended).

FIA_UAU.2 User authentication before any action, FIA_UAU.5 Multiple authentication mechanisms and **FIA_UID.2 User identification before any action**

The TOE requires users to provide unique identification and authentication data (passwords or in case of SSH public key) before any administrative access to the system is granted.

The JUNOS software supports four methods of user authentication: local password authentication, local authentication using public key authentication (via the SSH application), Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, a password is configured for each user allowed to log into the switch. RADIUS and TACACS+ are authentication methods for validating users who attempt to access the switch. Both are distributed client/server systems—the RADIUS and TACACS+ clients run on the appliance, and the server runs on a remote network system in the IT environment.

If the identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS or TACACS+ server, the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless, no administrative actions are allowed until successful authentication as an authorized administrator.

It should be noted that when RADIUS and/or TACACS+ are used for authentication, the TOE can verify only that the remote authentication server has the correct credentials.

The TOE can be configured to allow users to be authenticated via RADIUS and/or TACACS+. The order in which authentication mechanisms are attempted is applied to all users. The configuration can also specify that local passwords can only be used when external authentication servers are unavailable, or as a general fallback. For example, some users (such as 'root') might only be able to authenticate using local password, if they do not have a RADIUS/TACACS+ account configured and password is in the authentication-order. If configured and the request is made via SSH, public key authentication will be the attempted first; this is hard coded and is not specified in the authentication order.

Local authentication via the SSH application utilizes the user's public key stored on the appliance to both establish the SSH session and to authenticate the user to the CLI.

Irrespective of what access method is used for management sessions, successful authentication is required prior to giving a user access to the system. These mechanisms are used for administration of the routing functions as well as the administration of the user accounts used for management.

For non-administrative functions no authentication is required. The primary non-administrative function of the TOE is to route IP packets between Line Cards. This passes the packets from one network to a destination network, enabling network connectivity.[7]

[7] External agencies that pass packets to the TOE for routing are not classed as users in this ST, hence use of UAU.2 and FIA_UID.2, rather than the base component from each family.

Authentication data can be stored either locally or on a separate server. The separate server must support either the RADIUS or TACACS+ protocol to be supported by the TOE.

7.1.3 Security management function

FMT_MOF.1a Management of security functions behaviour

The switch restricts to a super-user the ability to modify the number of failed authentication attempts via Login (for the CLI) or SSH that occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.

The number of failed authentication attempts that represent a potential violation via Jade/checklogin cannot be configured. This is hard coded.

FMT_MOF.1b Management of security functions behaviour

The switch restricts to a super-user the ability to add or delete users, modify their access permissions or manage authentication attributes. This is handled by the management Daemon (MGD).

FMT_MSA.3 Static attribute initialization

The TOE is delivered with restrictive default values such that no traffic can pass across the appliance until specific configuration changes are made.

To enable forwarding between directly connected networks the IP addresses of the appliance interfaces must be configured.

The appliance will not route to an indirectly connected subnet (through another routing device) unless a route is configured in the switch.

FMT_MTD.1a Management of TSF Data (Switch Information)

The switch restricts the ability to administer the router configuration data, including rollback of configurations, to only super-users and equivalent authenticated applications. The CLI provides a text-based interface from which the router configuration can be managed and maintained. From this interface all switch functions, such as BGP, RIP and MPLS protocols can be managed, as well as Line Card configurations, TCP/IP configurations and date/time. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

FMT_MTD.1b Management of TSF Data (User Data)

The switch restricts the ability to administer user data to only super-users. The CLI provides super-users 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. This interface also provides the super-user 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 and/or TACACS+, then these will be consulted in the configured order for all users. Typically, local password is only used as a fallback in such cases.

FMT_MTD.1c Management of TSF Data (Audit logs)

The switch can be configured to automatically delete audit logs, or they can be deleted manually. Both operations can be carried out only by a super-user.

FMT_MTD.1d Management of TSF Data (Date/time)

The switch will allow only a super-user to modify the date/time setting on the appliance.

FMT_MTD.1e Management of TSF Data (Sessions)

The switch will allow only a super-user to create, delete or modify the rules that control the presumed address from which management sessions can be established.

FMT_SMF.1 Management of Security Functions

The TOE provides the ability to manage the following security functions:

a) User authentication (authentication data, roles);

b) switch information;

c) Audit management and review;

d) Modify the time;

e) Session establishment restrictions.

FMT_SMR.1 Security Roles

The TOE has three pre-defined roles[8]. When a new user account is created, it must be assigned one of these roles.

a) Super-user: this role can perform all management functions on the TOE. A user with this role can manage user accounts (create, delete, modify), view and modify the TOE configuration information.

b) Operator user: this role can read some configuration data, and in addition can use the following commands:

- Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands),
- Can access the network by entering the ping, SSH and traceroute commands,
- Can restart software processes using the restart command.
- Can view trace file settings in configuration and operational modes.

c) Read-only user: this role can view status and statistics only.

7.1.4 Protection function

7.1.5 Audit function

FAU_GEN.1 Audit data generation

JUNOS creates and stores audit records for the following events:

[8] Note that JUNOS offers the ability to define additional roles to a very fine granularity of access permissions, but this is beyond the scope of the evaluation. Any new class of user should be given the same permissions as one of these three roles, with the only difference being the specification of an idle-timeout period.

a) Start-up and shutdown of the audit function;
b) User login/logout;
c) Login failures;
d) Configuration is committed;
e) Configuration is changed.

Auditing is done using syslog. This can be configured to store the audit logs locally, or to send them to one or more log servers. The syslogs are automatically deleted locally according to configurable limits on storage volume or number of days of logs to retain. Only a super-user can delete the local audit logs.

FAU_GEN.2 User identity association

JUNOS will record within each audit record the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) Identity of the user that caused the event.

FAU_SAR.1 Audit review

JUNOS provides super-users and operators with the ability to display audit data from the CLI. Commands are available to list entire files, or to select records that match or do not match a pattern. Records can also be saved to files for further analysis offline. Read only users cannot view the audit records.

FAU_STG.1 Protected audit trail storage

Audit records are stored in /var/log/. Both the files and that directory are only modifiable by a super-user.

FAU_ARP.1 Security alarms FAU_SAA.1 Potential violation analysis

The daemons authenticating users to JUNOS perform analysis of the failed authentication attempts to identify activity indicating a potential violation. The following patterns of activity are defined to represent a potential violation and the action specified is triggered:

- 1 failed authentication attempt via Jade/checklogin – the connection will be dropped and an audit event will be generated.
- After each successive login failure via login (for CLI) or SSH throttling will be applied progressively increasing the time delay enforced between login attempts until the configured number of login attempts (default is 10) is reached, at which point the connection will be dropped. An audit event will be generated reporting each failed login. If, after a number of failed authentication attempts, another authentication failure occurs using a different username, an audit record will be generated reporting the number of repeated failures of the original username.

The TOE can also be configured to display selected audit events as they occur.

7.1.6 TOE access function

FTA_TSE.1 TOE session establishment

The switch can be configured by a super-user through use of packet filters such that users can only gain access from specific management networks/stations.

7.1.7 Clock function

FPT_STM.1 Time stamps

The clock function of the TOE provides a source of date and time information for the appliance, used in audit timestamps. The clock function is reliant on the system clock provided by the underlying hardware[9].

[9] This requires the NTP service to be configured, with the switch acting as an NTP client to receive time services from external NTP servers.

8 Rationale

This section provides the rationale for completeness and consistency of the security target. The rationale addresses the following areas:

- Security objectives
- Security functional requirements
- Security assurance requirements
- Dependencies
- Security functions
- Mutual support

8.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and that each security objective addresses at least one assumption or threat.

8.1.1 Rationale for Security Objectives for the TOE

This section provides a mapping of TOE security objectives to those threats that the TOE is intended to counter, and to those assumptions that must be met.

	T.ROUTE	T.PRIVIL	T.OPS	T.MANDAT	T.CONFLOSS	T.NOAUDIT	T.THREAT	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH	A.CRYPTO
O.FLOW	✓											
O.PROTECT	✓	✓	✓									
O.EADMIN	✓				✓							
O.AMANAGE	✓	✓		✓								
O.ACCESS	✓	✓	✓	✓								
O.ROLBAK	✓	✓	✓		✓							
O.AUDIT	✓	✓	✓	✓		✓			✓			
O.EAL							✓					

Table 8-1 TOE Security Objectives Rationale

O.FLOW This objective helps to counters the threat T.ROUTE through the use of routing tables to correctly route information.

O.PROTECT This objective contributes to correct routing of information (T.ROUTE) and prevention of disruption to TOE functions by users (T.PRIVIL) or processes (T.OPS).

O.EADMIN This objective is to provide effective management tools that assist in the correct routing of packets (T.ROUTE) and help to recover from failures (T.CONFLOSS).

O.AMANAGE The objective to limit access to management functions helps ensure correct routing (T.ROUTE), and helps counter the threat of unauthorised access (T.PRIVIL), and interception (T.MANDAT).

O.ACCESS This objective addresses the need to protect the TOE's operations and data. This helps counter the threats of incorrect routing (T.ROUTE), unauthorised access (T.PRIVIL and T.OPS), and interception (T.MANDAT).

O.ROLBAK The objective to restore previous configurations helps ensure correct routing of data (T.ROUTE), and helps recover from loss of configuration data (T.CONFLOSS) and unauthorised changes (T.PRIVIL, T.OPS).

O.AUDIT This objective serves to discourage and detect inappropriate use of the TOE (T.NOAUDIT), and as such helps counter T.ROUTE, T.PRIVIL, T.OPS and T.MANDAT. It also helps to support the assumption A.NOEVIL, by recording actions of users.

O.EAL This objective for assurance is appropriate to the likelihood of threat assumed in T.THREAT.

8.1.2 Rationale for Security Objectives for the Environment

This section provides a mapping of environment security objectives to those threats that the environment is expected to counter, and to those assumptions that must be met.

	T.ROUTE	T.PRIVIL	T.OPS	T.MANDAT	T.CONFLOSS	T.NOAUDIT	T.THREAT	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH	A.CRYPTO
OE.EAUTH		✓									✓	
OE.TIME										✓		
OE.CRYPTO												✓
OE.PHYSICAL								✓				
OE.ADMIN									✓			

Table 8-2 Environment Security Objectives Rationale

OE.EAUTH The objective to have an authentication server in the TOE environment helps to counter the threat of unauthorised access (T.PRIVIL), and supports the assumption that such a server is present (A.EAUTH).

OE.TIME The objective to have an NTP server in the TOE environment supports the assumption (A.TIME) that time services are available to provide the appliance with accurate/synchronised time information.

OE.CRYPTO The objective to use SSL or SSH to protect in-band management traffic supports the assumption that cryptography is used to protect management traffic (A.CRYPTO).

OE.PHYSICAL The objective to provide physical protection for the TOE supports the assumption that the TOE will prevent unauthorised physical access (A.LOCATE).

OE.ADMIN The objective that users should follow administrator guidance supports the assumption that they will not be careless, wilfully negligent or hostile (A.NOEVIL).

8.2 Rationale for Security Requirements

8.2.1 Rationale for TOE security functional requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 8-1 and Table 8-2 demonstrate the relationship between the threats and assumptions and the security objectives. Table 8-3 illustrates the mapping between security functional requirements and security objectives for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT
FAU_ARP.1		✓					✓
FAU_GEN.1							✓
FAU_GEN.2							✓
FAU_SAA.1		✓					✓
FAU_SAR.1							✓
FAU_STG.1							✓
FDP_IFC.1	✓	✓					
FDP_IFF.1	✓	✓					

	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.ROLBAK	O.AUDIT
FDP_ROL.1						✓	
FIA_ATD.1		✓		✓	✓		✓
FIA_SOS.1		✓		✓	✓		
FIA_UAU.2		✓		✓	✓		
FIA_UAU.5		✓		✓	✓		
FIA_UID.2		✓		✓	✓		
FMT_MOF.1a		✓					
FMT_MOF.1b		✓		✓	✓		
FMT_MSA.3	✓		✓				
FMT_MTD.1a	✓	✓		✓			
FMT_MTD.1b		✓		✓	✓		
FMT_MTD.1c				✓			✓
FMT_MTD.1d				✓			✓
FMT_MTD.1e				✓			
FMT_SMF.1	✓	✓	✓	✓	✓		✓
FMT_SMR.1	✓	✓	✓	✓	✓		✓
FPT_STM.1							✓
FTA_TSE.1				✓			

Table 8-3 Security Functional Requirements Rationale

FAU_ARP.1 This component takes action following detection of potential security violations, and therefore contributes to meeting O.PROTECT and O.AUDIT.

FAU_GEN.1 This component outlines what events must be audited, and aids in meeting O.AUDIT.

FAU_GEN.2 This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.

FAU_SAA.1 This component helps to detect potential security violations, and aids in meeting O.PROTECT and O.AUDIT.

FAU_SAR.1 This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_STG.1 This component requires that unauthorised deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.

FDP_IFC.1	This component identifies the entities involved in the UNAUTHENTICATED information flow SFP (i.e. external IT entities sending packets), and aids in meeting O.FLOW and O.PROTECT.
FDP_IFF.1	This component identifies the conditions under which information is permitted to flow between entities (the UNAUTHENTICATED SFP), and aids in meeting O.FLOW and O.PROTECT.
FDP_ROL.1	This component allows previous router configurations to be restored, and aids in meeting O.ROLBAK.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. The component aids in meeting O.PROTECT, O.AMANAGE, O.ACCESS and O.AUDIT.
FIA_SOS.1	This component specifies metrics for authentication, and aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UAU.2	This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UAU.5	This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UID.2	This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FMT_MOF.1a	This component relates to control of the functions that address detected security violations[10], and as such aids in meeting O.PROTECT`.
FMT_MOF.1b	This component relates to control of the functions that address identification and authentication (local or RADIUS/TACACS), and as such aids in meeting O.PROTECT, O.AMANAGE and O.ACCESS.
FMT_MSA.3	This component ensures that there is a default deny policy for the information flow control security rules. As such it aids in meeting O.FLOW. It also assists in effective management, and as such aids in meeting O.EADMIN.
FMT_MTD.1a	This component restricts the ability to modify routing configuration details, and as such aids in meeting O.FLOW, O.AMANAGE and O.PROTECT.
FMT_MTD.1b	This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.PROTECT, O.AMANAGE and O.ACCESS.

[10] For Login events (from the CLI) only as potential violations via all other authentication methods are hardcoded and cannot be modified.

FMT_MTD.1c This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT and O.AMANAGE.

FMT_MTD.1d This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT and O.AMANAGE.

FMT_MTD.1e This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.AMANAGE.

FMT_SMF.1 This component lists the security management functions that must be controlled. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, O.ACCESS and O.AUDIT.

FMT_SMR.1 Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, O.ACCESS and O.AUDIT.

FPT_STM.1 This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

FTA_TSE.1 This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorised access. As such it aids in meeting O.AMANAGE.

8.2.2 Rationale for TOE Environment Security Functional requirements

Multiple authentication mechanisms FIA_UAU.5

This component was chosen to ensure that multiple authentication mechanisms are used appropriately in all attempts to authenticate to the TOE. This component traces back to and aids in meeting the following objective: OE.EAUTH. Note that this requirement is partially satisfied by the TOE and partially by the TOE environment. Its presence under TOE environment security functional requirements is to address authentication using an external authentication server.

OE.CRYPTO

This objective was specified to ensure that all in-band management traffic is protected from network sniffing through encryption of the packets in accordance with the SSL and SSH standards. Any algorithms and key sizes specified in the SSL and SSH standards are acceptable to meet this requirement.

OE.TIME
This objective was specified to ensure a time source is provided in the environment. This time source can be used to synchronise the time of other servers in the TOE IT environment. Any method of providing a response to the TOE's NTP client requests is acceptable to meet this requirement. FTP_STM.1 has not been used as this requirement only specifies providing a time source for the entity's own use.

8.2.3 Rationale for Security Assurance Requirements (SAR)

The ST requires EAL3 augmented with ALC_FLR.3 assurance.

EAL3 augmented with ALC_FLR.3 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 TOEs. ALC_FLR.3 demonstrates a sound regime for addressing identified security flaws.

The chosen assurance level as supported by O.EAL, which is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

8.2.4 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied, with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. The requirement for FMT_MSA.3 is included as a dependency from FDP_IFF.1, to specify how the security attributes associated with the information flow rules are initialised. The subsequent dependency from FMT_MSA.3 on FMT_MSA.1 allows for the specification of the management of the security attributes. However, for this TOE the management of the information flow security attributes is specified using FMT_MTD.1a. Therefore, there is no need to include FMT_MSA.1 as FMT_MTD.1a has satisfied the intent of the dependency.

No additional dependencies have been identified. Dependencies on FIA_UAU.1 and FIA_UID.1 have been satisfied through inclusion of the hierarchical components FIA_UAU.2 and FIA_UID.2, respectively.

8.3 TOE Summary Specification Rationale

This section illustrates that the security functions as described in the TOE Summary Specification (Section 7.1) are necessary and sufficient to implement the SFRs and SARs.

	Information Flow	Identification and authentication	Security management	Protection	Audit	TOE Access	Clock
FAU_ARP.1					✓		
FAU_GEN.1					✓		
FAU_GEN.2					✓		
FAU_SAA.1					✓		
FAU_SAR.1					✓		
FAU_STG.1					✓		

	Information Flow	Identification and authentication	Security management	Protection	Audit	TOE Access	Clock
FDP_IFC.1	✓						
FDP_IFF.1	✓						
FDP_ROL.1			✓				
FIA_ATD.1		✓					
FIA_SOS.1		✓					
FIA_UAU.2		✓					
FIA_UAU.5		✓					
FIA_UID.2		✓					
FMT_MOF.1a			✓		✓		
FMT_MOF.1b		✓	✓				
FMT_MSA.3	✓		✓				
FMT_MTD.1a	✓	✓	✓				
FMT_MTD.1b		✓	✓				
FMT_MTD.1c			✓		✓		
FMT_MTD.1d			✓				✓
FMT_MTD.1e			✓			✓	
FMT_SMF.1	✓	✓	✓		✓	✓	✓
FMT_SMR.1	✓	✓	✓		✓		✓
FPT_STM.1					✓		✓
FTA_TSE.1						✓	

Table 8-5 Security Functions Rationale

The **Security Management Function** permits the super-user (FMT_SMR.1) to perform the following actions (FMT_SMF.1):

- Manage the operation of security violation pattern matching for Login events (via the CLI), (FMT_MOF.1a), other pattern matching relating to authentication attempts via other authentication methods cannot be modified;

- Manage the operation of the identification and authentication function (local or remote) (FMT_MOF.1b);

- Manipulate the routing configuration data (including rollback and management session establishment (FMT_MTD.1a, FMT_MSA.3, FDP_ROL.1, FMT_MTD.1e).

- Manage user accounts (FMT_MTD.1b);
- Delete audit logs (FMT_MTD.1c);
- Modify the date and time (FMT_MTD.1d).

The **Information Flow Function** allows super-users (FMT_SMR.1) to set up traffic flow rules between pairs of network interfaces on the appliance (FDP_IFC.1, FDP_IFF.1, FMT_SMF.1, FMT_MTD.1a). As default, the switch prevents all network connections and will only allow connections through the appliance if a rule has been set up to allow the type of communication to pass (FMT_MSA.3).

Through use of the Information Control Flow Function a super-user can restrict and control the flow of packets between the network interfaces of the appliance. This is based on the following attributes of the packets arriving at a network interface:

- The interface on which the request arrives (FDP_ IFC.1, FDP_IFF.1;
- The presumed source IP address of the packet (FDP_ IFC.1, FDP_IFF.1;
- The presumed destination IP address of the packet (FDP_ IFC.1, FDP_IFF.1;
- The service related to the packet (FDP_ IFC.1 and FDP_IFF.1.

If a packet arrives at one of the interfaces of the appliance and fails to meet a requirement for the rules set on an interface it will be blocked. Unless a rule specifically states that a particular packet can pass from one network interface to another of the appliance the packet will be blocked (FDP_ IFF.1).

The **Audit Function** provides a reliable audit trail of network connections and other events (FAU_GEN.1) that can be managed by a super-user (FMT_MOF.1a, FMT_MTD.1c, FMT_SMF.1). For all events the Audit Function will record the:

- Date and time of the event (FAU_GEN.1), using the date and time information provided by the Clock Function (FPT_STM.1);
- Type of event or service (FAU_GEN.1);
- Success or failure of the event (FAU_GEN.1);
- Identity of user who caused event (FAU_GEN.2).

The TOE can be configured to monitor sequences of events (FAU_SAA.1) and take action when they occur (FAU_ARP.1).

Audit records are stored securely in var/log/ (FAU_STG.1). Both files and that directory are only modifiable by a super-user (FMT_SMR.1, FAU_SAR.1).

The **TOE Access Function** provides for restrictions on session establishment (FTA_TSE.1, FMT_MTD.1e, FMT_SMF.1).

The **Identification and Authentication Function** requires that users be identified (FIA_UID.2, FIA_ATD.1) and authenticated (FIA_UAU.2, FIA_UAU.5, FIA_ATD.1, FIA_SOS.1) before being granted access to any other TOE functions.

The function is controlled by super-users (FMT_SMF.1, FMT_SMR.1, FMT_MOF.1b, FMT_MTD.1b), who may modify user attributes, and manage the number of permitted authentication attempts (FMT_MTD.1a).

The **Clock Function** provides a reliable source of time and date information. This function permits super-users (FMT_SMF.1, FMT_SMR.1) to set and change the time and date (FMT_MTD.1d). The Clock Function also provides the audit function with time stamps (FPT_STM.1).

8.4 IT security functions mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8-5.

9 Acronyms

ACM	Access Control Management
AGD	Administrator Guidance Document
BGP	Border Gateway Protocol
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CLI	Command Line Interface
CM	Control Management
DAC	Discretionary Access Control
DPC	Dense Port Concentrators
EAL	Evaluation Assurance Level
GB	Gigabyte
I/O	Input/Output
JNR	Juniper Networks Router
OSPF	Open Shortest Path First
PFE	Packet Forwarding Engine
PIC	Pluggable Interface Controller
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control