Security Target for Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2

Version 1.0
October 01, 2012

Juniper Networks
1194 North Mathilda Avenue
Sunnyvale
California 94089
USA

Contents

List of tables

1 ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference: Juniper Networks M7i, M10i, M120 & M320 M-Series Multiservice Edge Routers, MX5, MX10, MX40, MX80, MX240, MX480 & MX960 MX-Series 3D Universal Edge Routers, T320, T640 & T1600 T-Series Core Routers and EX2200, EX3200, EX3300, EX4200, EX4500, EX6210 & EX8200[1] EX-Series Ethernet Switches running JUNOS 11.4R2

ST Reference: Security Target for Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2

ST Version: Version 1.0

ST Date: October 01, 2012

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

ST Author: Juniper Networks

Keywords: Router, IP, Service Manager

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

The TOE is the Junos 11.4R2 software, firmware and the following referenced router and switch appliance chassis: M7i, M10i, M120, M320, T320, T640, T1600, MX5, MX10, MX40, MX80, MX240, MX480, and MX960 services router / EX2200, EX3200, EX3300, EX4200, EX4500, EX6210 and EX8200[1] switches providing a wide variety of services to the user.

The TOE routes IP traffic over any type of network, with increasing scalability of the traffic volume with each TOE 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] The EX8200 series includes the EX8208 and the EX8216

1.3 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.

[SCG] Security Configuration Guide for Common Criteria and JUNOS-FIPS, Junos 11.4.

1.3.1 TOE Type

The TOE is a switch/services router (appliance chassis) running the Junos 11.4R2 software and firmware providing a wide variety of services. The routing services considered in the evaluation are Ethernet, and the only management of the appliances considered in the evaluation is via the CLI.

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. PICs, DPCs, Line Cards) to be installed in the TOE, as described in section 1.4 below).

1.4 TOE Description

The TOE is the IP routers/switches appliance chassis (mentioned in section 1.2.1) running Junos 11.4R2 software and firmware. The platforms are designed to provide an efficient and effective IP/Switch solution that can be managed centrally.

1.4.1 M/T/MX Series Routers

Each Juniper Networks M-series, T-series and MX-series routing platform is a complete routing system that supports a variety of high-speed interfaces (only Ethernet is within scope of the evaluation) for medium/large networks and network applications. Juniper Networks routers share common JUNOS software, features, and technology for compatibility across platforms.

The JNR platforms are designed as hardware devices, which perform all routing functions internally to the device. All router platforms are powered by the same JUNOS software, which provides both management and control functions as well as all IP routing.

The hardware has two components: the router itself and the PICs/DPC that have been installed in the router. The various PICs/DPC that have been installed in the router allow it to communicate with the different types of networks that may be required within the environment where the router will be used.

The router architecture of each platform cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

Each router consists of two major architectural components:

- The Routing Engine (RE), which provides Layer 3 routing services and network management and control;
- The Packet Forwarding Engine (PFE), which provides all operations necessary for transit packet forwarding.

The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The Routing Engine consists of an Intel-based PCI platform running JUNOS software. The Routing Engine constructs and maintains one or more routing tables, and controls the routing protocols on the router. From the routing tables, the Routing Engine derives a table of active routes, called the forwarding table, which is then copied into the Packet Forwarding Engine.

Each Routing Engine consists of a CPU; SDRAM for storage of the routing and forwarding tables and other processes; a compact flash disk for primary storage of software images, configuration files, and microcode; a hard disk for secondary storage; a flash PC card slot for storage of software upgrades; and interfaces for out-of-band management access.

The Packet Forwarding Engine uses ASICs to perform Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding. Physical Interface Cards (PICs) are the physical network interfaces that allow the TOE to be customized to the intended environment and interface to the Packet Forwarding Engine.

On M-series routers, the Packet Forwarding Engine includes the router midplane (on an M40 router, the backplane), Flexible PIC Concentrators (FPCs), PICs, and other components, unique to each router, that handle forwarding decisions. Each FPC can accommodate a number of PICs.

The T-series platforms feature multiple Packet Forwarding Engines, up to a maximum of 16 for the T640 Internet routing node and 8 for the T320 Internet router. Each FPC has one or two Packet Forwarding Engines, each with its own memory buffer. Each Packet Forwarding Engine maintains a high-speed link to the Routing Engine.

The MX-series routers feature Dense Port Concentrators (DPCs), which are a fusion of a FPC and its PICs into one monolithic board. This means the interface configuration is fixed according to the DPC installed rather than the flexible configuration provided by FPCs, which allow different PICs to be inserted.

All of the platforms support two or more power supplies, providing redundancy.

The router supports numerous routing standards, allowing it to be flexible as well as scalable. These functions can all be managed through the JUNOS software either from a connected terminal console or via a network connection. Network management can be secured using SSH[2] protocols provided by the operational environment. All management requires successful authentication.

JUNOS only supports netconf (an IETF standardization effort) via SSH transport, and authentication is handled by SSHD.

The packet filtering function in JNR is highly configurable, providing many different options for tailoring the decision of whether or not to accept/forward a packet. The basic packet filtering configuration used for this evaluation, allows only packets from certain addresses to be accepted. This can be used to restrict the addresses from which management and control traffic will be accepted.

1.4.2 EX Switches

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[3] (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 and control;

[2] The TOE uses OpenSSH 4.4.
[3] The Line Cards are a monolithic blade.

- The Packet Forwarding Engine (PFE), which provides all operations necessary for packet forwarding.

The EX2200, EX3200, EX3300 and EX4200 are fixed format. The EX4500 has a combination of fixed port and two uplink modules and connects with both fiber and copper interfaces. The EX6210 and EX8200 can support either copper or fiber line cards.

1.5 TOE Boundaries

The TOE includes both physical and logical boundaries.

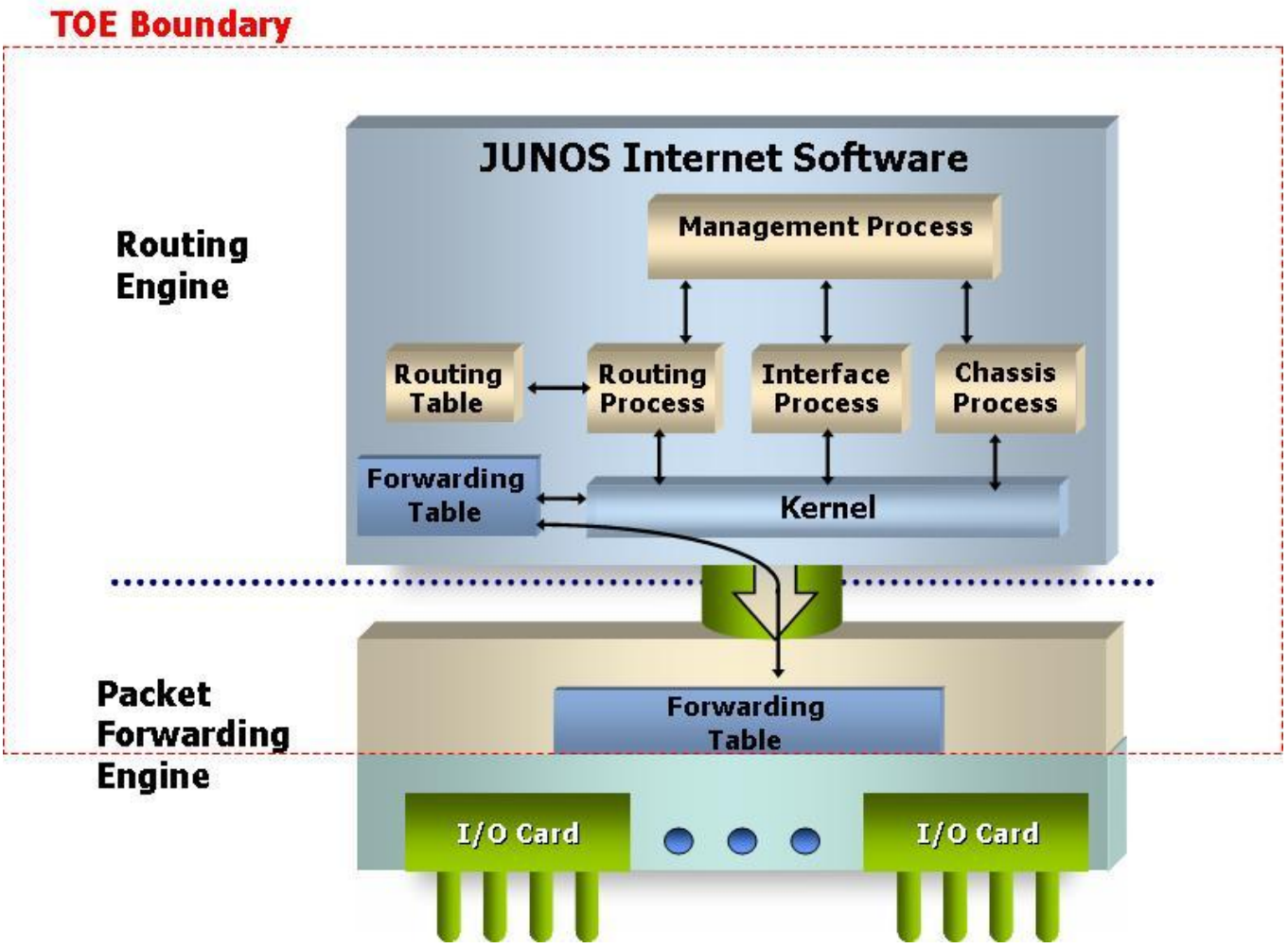
1.5.1.1 Physical Boundary

The TOE is comprised of appliance chassis (appliances listed below) and the Junos 11.4R2.14 software and firmware running on the appliance (including the software implementing the Routing Engine and the software and ASICs implementing the Packet Forwarding Engine[4]). Hence the TOE is contained within the physical boundary of the specified appliance.

The DPC, PIC and Line Card network interface components are outside the scope of the TOE.

The following diagram indicates the boundary between the TOE and the network interface components from both a software and hardware perspective.

[4] The lower layers of the PFE which simply deal with physical interfaces mechanics are out of scope.



The interfaces to the TOE are twofold: the routing interfaces (including control traffic) and the management interfaces. The management interfaces include the TOE console interface through which the appliance can be managed locally, the dedicated management ethernet interface and the in-band management interface via the network interfaces. Use of the TOE console interface is required for initialisation of the TOE, but its use is not supported during operation of the TOE in the evaluated configuration.

The following appliance models are covered by this evaluation:

M7i	T320	EX2200	MX5
M10i	T640	EX3200	MX10
M120	T1600	EX3300	MX40
M320		EX4200	MX80
		EX4500	MX240
		EX6210	MX480
		EX8208	MX960
		EX8216	

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 (control) 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 and SSL (which are out of scope), and SSH (which is provided by the operational environment).

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).

- Security Management

The appliance is managed, including user management and the configuration of the router/switch functions, through a Command Line Interface (CLI) protected by SSH. The CLI interface is accessible over an SSH session; either via the dedicated management ethernet interface or in-band management traffic over the routing interfaces.

- 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. (The NTP server is considered outside the scope of the TOE.) This external time source allows synchronization of 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 TOE is completely self-contained, and maintains its own execution domain as follows:

- 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
- External servers (audit, NTP, authentication, FTP servers)
- Encryption and integrity checking functionality
- SSL and SSH functionality
- High availability functionality

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

- Network interface hardware, including PICs, DPCs, Line Cards
- Use of the auxiliary port
- Use of Telnet
- Use of SNMP
- Use of management console[5]
- Packet filtering (other than simple access control to restrict the source address for management and control traffic)
- Media use (other than during installation of the TOE)
- Use of JUNOScope for the management of the TOE
- Use of JWeb for the management of the TOE[6]

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

[5] This is different to the dedicated management ethernet interface

[6] This includes the use of Junoscript (an XML API for 3rd party managment tools) and netconf (the IETF standardized version of Junoscript.

2 CC Conformance

CC Identification:

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.

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, and authorized user.
- 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 incorrectly.
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 router/switch management or control 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 TOE configurations and other management information may not be detected.

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 Management traffic will be protected using SSH.

A.NWCOMP The network components access the management interface of the TOE will be located within a controlled environment, and the authorized users of the components will not be wilfully negligent or hostile.

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 must 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.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 router/switch configurations to a known state.

O.AUDIT Users must be accountable for their actions in administering the TOE.

O.CONN The TOE must limit the IP addresses from which an administrator is able to manage the TOE and from which control data is accepted.

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) must be available to provide accurate/synchronised time services to the router/switch.

OE.CRYPTO SSH must be enabled for all 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.

OE.NWCOMP Those responsible for the TOE must ensure that the IT environment network components that have access to the management interface of the TOE are protected.

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.

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)

Security Functional Class	Security Functional Components
	Simple security attributes (FDP_IFF.1)
	Rollback (FDP_ROL.1)
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 (Router/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)
	Management of TSF data (Router/Switch routing) (FMT_MTD.1f)
	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: throttle SSH connections, 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 function to modify router configuration (FMT_SMF.1)**[7]] 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
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 8 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)[8]

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.

[7] The access control policy for management is defined by the FMT requirements. Therefore, the access control policy assignment in this SFR has been refined to indicate the FMT requirement that describes the administrator function relating to rollback.
[8] 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, the users associated with those originating packets are not users *of the TOE*.

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 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[9]] 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
The TSF shall enforce the [UNAUTHENTICATED SFP] to provide [*restrictive*[10]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2
The TSF shall allow the [*super-users and the Routing Engine portion of the TSF*[11]] 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 (Router/Switch configuration) (FMT_MTD.1a)

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

[9] The only security violation pattern that is configurable is that associated with authentication attempts via Login (from the CLI).
[10] On the EX-switches this restrictive default is achieved through configuration by the administrator during the installation of the TOE, as detailed in [SCG].
[11] This reflects the automatic updates to the routing table set of security attributes made by the routing engine during operation.

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 [NTP Server address and system clock] 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, delete,* [create]] the [rules that restrict the ability to establish management sessions] to [super-users].

6.2.4.9 Management of TSF data (Router/Switch routing) (FMT_MTD.1f)

FMT_MTD.1.1f
The TSF shall restrict the ability to [*modify and delete*] the [router or switch routing data] to [super-users/routing-peers and operator].

6.2.4.10 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, modification of routing data, deletion of routing data), 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].

6.2.4.11 Security roles (FMT_SMR.1)

FMT_SMR.1.1
The TSF shall maintain the roles [read-only user, operator user, super-user, routing-peer[12]].

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

[12] The routing-peer is not a human user role.

6.2.5 Protection of the TOE security functions (FPT)

6.2.5.1 Time stamps (FPT_STM.1)

FPT_STM.1.1
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 6-2 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 IP 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, otherwise 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) and privilege (user class). The super-user can delegate 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 8 ASCII 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) before any administrative access to the system is granted.

The JUNOS software supports the following methods of user authentication: local password authentication, 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 Services Router/switch. RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router/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.

Local authentication via the SSH application is to be configured to use the local password 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 PICs. This passes the packets from one network to a destination network, enabling network connectivity.[13]

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.

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

7.1.3 Security management function

FMT_MOF.1a Management of security functions behaviour

The TOE 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[14] is enforced for further authentication attempts and before the connection is dropped.

FMT_MOF.1b Management of security functions behaviour

The TOE 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

As default, the TOE prevents all network connections and will only allow connections through the TOE if a rule has been set up to allow the type of communication to pass.

FMT_MTD.1a Management of TSF Data (Router/Switch configuration)

The TOE restricts the ability to administer the router configuration data, including rollback of configurations, to only super-users. 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, as well as PIC 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 Attributes)

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

FMT_MTD.1e Management of TSF Data (Sessions)

The TOE 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.

[14] Throttling functionality enforced by **FAU_ARP.1 Security Alarms**

FMT_MTD.1f Management of TSF Data (Router/Switch routing)

The TOE will allow only a super-user and operator to clear routing information learned from the network and will allow only super-user and routing-peer to modify routing information.

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) Router/Switch configuration (including PIC configurations, TCP/IP configurations, date/time, use of rollback, and update of routing tables and deletion of routing information learned from the network);

c) Audit management and review;

d) Modify the time;

e) Session establishment restrictions.

FMT_SMR.1 Security Roles

The TOE has three pre-defined human roles[15]. 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.
- Can review all audit records.

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

In addition, to the human roles the TOE also recognizes network entities that provide routing information update (via BGP, RIP and MPLS traffic) as routing-peers[16].

7.1.4 Audit function

FAU_GEN.1 Audit data generation

JUNOS creates and stores audit records for the following events:

a) Start-up and shutdown of the audit function;
b) User login/logout;

[15] 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.

[16] These routing-peers are managed by super-users using the Router/Switch configuration aspects of the CLI.

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:

- 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.

7.1.5 TOE access function

FTA_TSE.1 TOE session establishment

The TOE can be configured by a super-user through use of packet filters such that users can only gain access from specific management networks/stations at specific IP addresses and control data is only accepted from specified sources.

7.1.6 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[17].

[17] This requires the NTP service to be configured, with the router 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

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	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH	A.CRYPTO	A.NWCOMP
O.FLOW	✓											
O.PROTECT	✓	✓	✓									
O.EADMIN	✓				✓							
O.ACCESS	✓	✓	✓									
O.ROLBAK	✓	✓	✓		✓							
O.AUDIT	✓	✓	✓	✓		✓		✓				
O.CONN		✓	✓	✓								

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 to provide effective management tools that help to recover from failures (T.CONFLOSS).

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).

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 helps recover from 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, which relate to inappropriate (deliberate or accidental) use of the TOE. It also helps to support the assumption A.NOEVIL, by recording actions of users.

O.CONN This objective helps counter the threats relating to unauthorised modification by an attacker to the TOE configuration (T.PRIVIL & T.OPS) by limiting the IP addresses from which the TOE accepts management and control traffic connections (T.MANDAT).

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	A.LOCATE	A.NOEVIL	A.TIME	A.EAUTH	A.CRYPTO	A.NWCOMP
OE.EAUTH		✓								✓		
OE.TIME									✓			
OE.CRYPTO											✓	
OE.PHYSICAL							✓					
OE.ADMIN								✓				
OE.NWCOMP												✓

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 enforcing authentication of users attempting to access to TOE security functions and data (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 SSH to protect 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).

OE.NWCOMP The objective to protect those network components with access to the management interface of the TOE supports the assumption that these network components will be protected (A.NWCOMP).

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.ACCESS	O.ROLBAK	O.AUDIT	O.CONN
FAU_ARP.1		✓				✓	
FAU_GEN.1						✓	

	O.FLOW	O.PROTECT	O.EADMIN	O.ACCESS	O.ROLBAK	O.AUDIT	O.CONN
FAU_GEN.2						✓	
FAU_SAA.1		✓				✓	
FAU_SAR.1						✓	
FAU_STG.1						✓	
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_MTD.1f				✓			
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.
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.
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.ACCESS and O.AUDIT.
FIA_SOS.1	This component specifies metrics for authentication, and aids in meeting objectives to restrict access (O.PROTECT 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 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 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 and O.ACCESS).
FMT_MOF.1a	This component relates to control of the functions that address detected security violations[18], 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 and O.ACCESS.

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

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 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 and O.ACCESS.

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

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

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

FMT_MTD.1f This component restricts the ability to delete the routing data, and as such contributes to meeting O.ACCESS.

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

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 and O.ACCESS.

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 control data is accepted and a user session can be established, and hence reduces the chance of unauthorised access. As such it aids in meeting O.ACCESS and O.CONN.

8.2.2 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.

8.2.3 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.

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