Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target

Version 1.0

April 3, 2006

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

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. Juniper Networks provides the TOE, which is the Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14. The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, TOE and CC Identification

ST Title – Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target

ST Version – Version 1.0

ST Date – April 3, 2006

TOE Identification – All Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14

- Model numbers J2300, J4300, J6300

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 Conformant
    - Evaluation Assurance Level 2 (EAL2)

1.3 Strength of Environment

The Juniper Networks J-Series Family of Service Routers provides routing solutions for connected networks. In order to successfully maintain control over the routing configuration in a volatile network environment, the Juniper Networks J-Series Family of Service Routers must be protected from physical attacks. Access, therefore, is restricted to authorized users. Additionally, it is required that the Juniper Networks J-Series Family of Service Routers remain physically connected to the networks on which they route.

To ensure that the design of the IT networks is acknowledged and that the risks to the target environment are adequately addressed, the assurance requirements for EAL2, and the minimum strength of function, SOF-Basic, were chosen.

1.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.4.1 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: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4.2 Acronyms

The acronyms used within this Security Target:

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
DO	Delivery Operation

EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
I/O	Input/Output
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
OSPF	Open Shortest Path First
PIM	Pluggable Interface Module
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

2. TOE Description

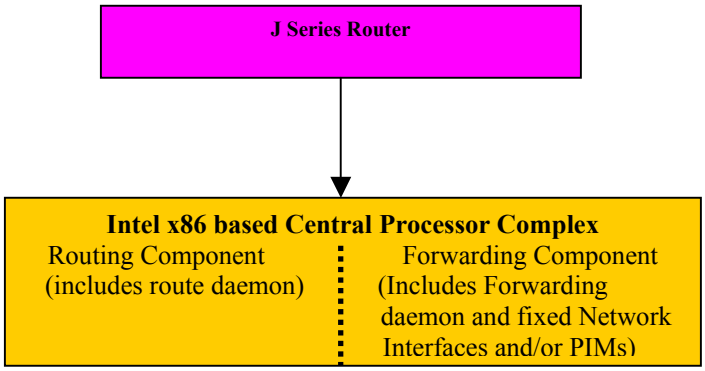
The TOE is all Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14, hereafter called JNR. The products are designed by Juniper Networks, located at 1194 North Mathilda Avenue, Sunnyvale, California 94089.

2.1 Product Type

The TOE is a services router providing a wide variety of services to the user. JNRs route IP traffic over any type of network, with increasing scalability of the traffic volume with each router 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 passes it to the appropriate destination.

2.2 Product Description

The TOE platforms are designed to be efficient and effective IP router solutions. The TOE comprises of two separate functions: the Routing Function and Packet forwarding Function that make up the router platform itself. PIMs are the physical network interfaces that allow the TOE to be customized to the intended environment and they are part of the Packet Forwarding Engine. The J4300 and J6300 models use a common set of PIMs whereas the physical network interface modules are in-built, part of the J2300 model of routers..



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

The TOE 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 ssl, SNMP v3, and ssh protocols. All management, whether from an administrator connecting to a terminal or from the network, requires successful authentication.

2.3 Product Features

The TOE implements the following features:

Modularity - JUNOS software employs a modular software design, providing resilience and ensuring that new capabilities such as IPv6, and new PIMs, can be easily integrated

Routing expertise - Juniper Networks IP routing expertise delivers a full complement of routing protocols

Standards-based - adherence to industry standards for routing, MPLS, and availability mechanisms such as Protocol Graceful Restart translates to improved stability and reduced operational complexity for customers

Security - JUNOS software adds intelligent packet processing to offer customers a potent IP security toolkit

Service richness - JUNOS IP services portfolio enables customers to deliver assured experiences to end users of any profile

Policy and control - Juniper Networks Command Line Interface (CLI) allows customer to invoke and control these JUNOS capabilities; in addition, Juniper Networks JUNOScript XML interface simplifies and accelerates OSS integration

Scalability – the ability of the TOE to scale to the highest levels of throughput to handle backbone level traffic

Flexibility – the ability of the TOE to handle multiple types of network interfaces, from T1 to OC-192 through the PIM interface

2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The TOE physical boundary is the router itself (including any installed PIMs as in the case of the J4300 and J6300). The TOE is completely self-contained, housing the software and hardware necessary to perform all router functions. The hardware has two components: the router itself and the PIMs that have been placed into the router. The various PIMs that have been placed into 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 interfaces to the TOE are twofold: the network interface, as enumerated through the PIMs, and the administrative interface, enumerated through the administrative network connection as well as the terminal console. The PIMs are used for all the routing functions, connecting the TOE to all the environments networks. The administrative network and the terminal console are used solely for the administration of the router.

2.4.2 Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include User Data Proteection for network information flows, Identification and Authentication for the administrative functions, the management of the security configurations and the self-protection of the TOE itself.

2.4.2.1 User Data Protection

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 administrators or indirectly from other network entities (outside the TOE) configured by the TOE administrators.

2.4.2.2 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 the ability to define levels of authority for users, providing administrative flexibility. Full administrators have the ability to define groups and their authority and they have complete control over the TOE.

The TOE also requires that applications exchanging information with the TOE successfully authenticate prior to any exchange. This covers all services used to exchange information, including telnet, ssh, ssl, and ftp.

Authentication services can be handled either internally (fixed passwords) or through an authentication server in the IT environment, such as a RADIUS or TACACS+ server (the external authentication server is considered outside the scope of the TOE). 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.

2.4.2.3 Security Management

The TOE is managed through a Command Line Interface (CLI), or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality. Through these interfaces all management can be performed, including user management and the configuration of the router functions. The CLI interface is accessible through ssh and telnet sessions, as well as a local terminal console.

2.4.2.4 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 functions of the TOE are confined to the device itself. The TOE is completely self-contained, and are therefore maintains its own execution domain.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of TOE security environment defines the following:

- Threats that the product is designed to counter
- Assumptions made on the operational environment and the method of use intended for the product,
- Organizational security policies with which the product is designed to comply.

3.1 Threats to Security

The following are threats identified for the TOE. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides.

3.1.1 TOE Threats

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.

3.2 Organization Security Policies

The following policies apply to the TOE and the intended environment of the TOE.

P.FLOW	The TOE shall ensure that information flows from source to destination according to available routing information.
P.MANAGE	The TOE shall provide effective management functions that can only be utilized by authorized users.
P.PROTECT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Secure Usage 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 administrators are competent, not careless, willfully 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.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 IT Security Objectives for the TOE

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

O.FLOW The TOE must use available routing information to forward network packets to the appropriate destination.

O.PROTECT The TOE must protect itself from unauthorized modifications and access to its 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.

4.2 IT Security Objectives for the Environment

The following security objectives for the IT 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.

4.3 Non-IT Security Objectives for the Environment

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.MANAGE Authorized administrators are non-hostile and follow all administrator guidance.

5. IT Security Requirements

This section provides a list of all security functional requirements for the TOE.

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. This section organizes the SFRs by CC class. Table 1 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components

Security Functional Class	Security Functional Components
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Timing of authentication (FIA_UAU.1)
	Timing of identification (FIA_UID.1)
Security management (FMT)	Static attribute initialization (FMT_MSA.3)
	Management of TSF data (Router Information) (FMT_MTD.1a)
	Management of TSF data (User Data) (FMT_MTD.1b)
	Specification of Management Functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	TSF domain separation (FPT_SEP.1)

Table 1 Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Subset information flow control (FDP_IFC.1)

5.1.1.1.1 FDP_IFC.1.1

The TSF shall enforce the [**UNAUTHENTICATED SFP**] on

a.) **[subjects:**
- **unauthenticated external IT entities that send and receive information through the TOE to one another;**

b.) **information:**
- **network traffic sent through the TOE from one subject to another**

c.) **operation:**
- **pass information].**

5.1.1.2 Security attribute based access control (FDP_IFF.1)

5.1.1.2.1 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**
- **transport layer protocol**
- **TOE interface on which traffic arrives and departs**
- **service]** *(per International Interpretation #104)*

5.1.1.2.2 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 an internal network can cause information to flow through the TOE to another connected network if:**
- **all the information 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 information flow security attributes, created by the authorized administrator**
- **the presumed address of the source subject, in the information, translates to an internal network address**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network**

b.) **Subjects on the external network can cause information to flow through the TOE to another connected network if:**
- **all the information 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 information flow security attributes, created by the authorized administrator**
- **the presumed address of the source subject, in the information, translates to an external network address**
- **and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]**

5.1.1.2.3 FDP_IFF.1.3

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

5.1.1.2.4 FDP_IFF.1.4

The TSF shall provide the following [**no additional UNAUTHENTICATED SFP capabilities**].

5.1.1.2.5 FDP_IFF.1.5

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

5.1.1.2.6 FDP_IFF.1.6

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

5.1.2 Identification and authentication (FIA)

5.1.2.1 Timing of authentication (FIA_UAU.1)

5.1.2.1.1 FIA_UAU.1.1

The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is authenticated.

5.1.2.1.2 FIA_UAU.1.2

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

5.1.2.2 User attribute definition (FIA_ATD.1)

5.1.2.2.1 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]**.

5.1.2.3 Timing of identification (FIA_UID.1)

5.1.2.3.1 FIA_UID.1.1

The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is identified.

5.1.2.3.2 FIA_UID.1.2

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

5.1.3 Security management (FMT)

5.1.3.1 Static attribute initialization (FMT_MSA.3)

5.1.3.1.1 **FMT_MSA.3.1**

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

5.1.3.1.2 **FMT_MSA.3.2**

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

5.1.3.2 Management of TSF data (Router Information) (FMT_MTD.1a)

5.1.3.2.1 FMT_MTD.1a

The TSF shall restrict the ability to [**modify router information**] to [**Authorized Administrators**].

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

5.1.3.3.1 FMT_MTD.1b

The TSF shall restrict the ability to [**modify user account data**] to [**Authorized Administrators**].

5.1.3.4 Specification of Management Functions (FMT_SMF.1)[1]

5.1.3.4.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:[**modify router information and modify user account data**].

[1] This requirement has been added to comply with International Interpretation #65

5.1.3.5 Security roles (FMT_SMR.1)

5.1.3.5.1 FMT_SMR.1.1

The TSF shall maintain the roles [**Authorized Administrator**].

5.1.3.5.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.4 Protection of the TOE security functions (FPT)

5.1.4.1 TSF domain separation (FPT_SEP.1)

5.1.4.1.1 FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.1.4.1.2 FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 IT Environment Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the IT Environment. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	Multiple authentication mechanisms (FIA_UAU.5)

Table 2 EAL2 Assurance Components

5.2.1 Identification and authentication (FIA)

5.2.1.1 Multiple authentication mechanisms (FIA_UAU.5)

5.2.1.1.1 FIA_UAU.5.1

The TSF shall provide [**internal fixed password mechanism and external server (RADIUS or TACACS+) mechanism**] to support user authentication.

5.2.1.1.2 FIA_UAU.5.2

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components as specified in Part 3 of the Common Criteria. The minimum strength of function for mechanisms used within the TOE is SOF-Basic. No operations are applied to the assurance components.

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration items

Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal Function Specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Tests (ATE)	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 3 EAL2 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration Items (ACM_CAP.2)

5.3.1.1.1 ACM_CAP.2.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.2.2D

The developer shall use a CM system.

5.3.1.1.3 ACM_CAP.2.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.2.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.1.5 ACM_CAP.2.2C

The TOE shall be labeled with its reference.

5.3.1.1.6 ACM_CAP.2.3C

The CM documentation shall include a configuration list.

5.3.1.1.7 International Interpretation #3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[2]

5.3.1.1.8 ACM_CAP.2.4C

The configuration list shall describe the configuration items that comprise the TOE.

[2] This requirement has been added to comply with International Interpretation #3

5.3.1.1.9 ACM_CAP.2.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

5.3.1.1.10 ACM_CAP.2.6C

The CM system shall uniquely identify all configuration items.

5.3.1.1.11 ACM_CAP.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

5.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.3.2.2.2 ADO_IGS.1.1C

The **installation, generation and start-up** documentation shall describe **all** the steps necessary for secure installation, generation, and start-up of the TOE.[3]

5.3.2.2.3 ADO_IGS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

[3] This requirement has been modified to comply with International Interpretation #51.

5.3.3 Development (ADV)

5.3.3.1 Informal Function Specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

5.3.3.1.6 ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

5.3.3.2.1 ADV_HLD.1.1D

The developer shall provide the high level design of the TSF.

5.3.3.2.2 ADV_HLD.1.1C

The presentation of the high level design shall be informal.

5.3.3.2.3 ADV_HLD.1.2C

The high level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.1.3C

The high level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.1.4C

The high level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.1.5C

The high level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.1.6C

The high level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.1.7C

The high level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2.10 ADV_HLD.1.2E

The evaluator shall determine that the high level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.3.3 ADV_RCR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documents supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Security Testing (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

5.3.5.1.1 ATE_COV.1.1D

The developer shall provide evidence of the test coverage.

5.3.5.1.2 ATE_COV.1.1C

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

5.3.5.1.3 ATE_COV.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

5.3.5.2.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.5.2.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.5.2.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.5.2.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.5.2.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.5.2.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.5.2.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.5.2.8 ATE_FUN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing – sample (ATE_IND.2)

5.3.5.3.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.5.3.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.5.3.3 ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.3.5.3.4 ATE_IND.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.5.3.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.5.4 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.5.4.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.5.4.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.5.4.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.5.4.4 AVA_SOF.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.4.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.5.5 Developer vulnerability analysis (AVA_VLA.1)

5.3.5.5.1 AVA_VLA.1.1D

~~The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~ **The developer shall perform a vulnerability analysis.**[4]

5.3.5.5.2 AVA_VLA.1.2D

~~The developer shall document the disposition of obvious vulnerabilities.~~ **The developer shall provide vulnerability analysis documentation.** [5]

5.3.5.5.3 AVA_VLA.1.1C

~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.~~ **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.**[6]

5.3.5.5.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[7]

5.3.5.5.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [8]

5.3.5.5.6 AVA_VLA.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

---

[4] This requirement has been modified to comply with International Interpretation #51.
[5] This requirement has been modified to comply with International Interpretation #51.
[6] This requirement has been modified to comply with International Interpretation #51.
[7] This requirement has been added to comply with International Interpretation #51.
[8] This requirement has been added to comply with International Interpretation #51.

5.3.5.5.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 User Data Protection

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 administrators or has been collected (e.g., ARP) from network peers as defined by the TOE administrators.

6.1.2 Identification and Authentication

FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: user name, authentication data (password or an authentication server in the IT environment), and their privileges. Locally stored authentication data for fixed password authentication is a case-sensitive, alpha-meric value that can be up to 128 characters in length. While passwords longer than 128 characters can be used, they do not contribute to the password mechanism strength of function, only the first 128 characters are checked during authentication.

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.

Public Key authentication, such as RSA, is supported using the authentication server in the IT environment for authentication to the TOE.

FIA_UAU.1 Timing of Authentication and **FIA_UID.1 Timing of Identification**

JNR requires users to provide unique identification and authentication data (passwords) before any administrative access to the system is granted. If the identify specified is defined locally, the TOE will 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.

User or application authentication can occur through several mechanisms, including ftp, telnet and ssh. These programs all require successful authentication prior to giving a user access to the system. The ssh application also supports Public Key authentication to the system, for both the connecting client (computer where the administrator is connecting from) and the user. 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 PIMs. This passes the packets from one network to a destination network, enabling network connectivity.

6.1.3 Security Management

FMT_MSA.3 Static attribute initialization

The TOE restricts the ability to administer through the CLI interface (or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality) the router configuration data to only authorized administrators and authenticated applications. The TOE automatically routes traffic based on available routing information, much of which is automatically collected from the TOE environment.

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

The TOE restricts the ability to administer through the CLI interface (or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality)the router configuration data to only authorized administrators and authenticated applications. The CLI provides authorized administrators with a text-based interface from which the router configuration can be managed and maintained. From this interface all router functions, such as BGP, RIP and MPLS protocols can be managed, as well as PIM configurations and TCP/IP configurations.

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

The TOE restricts the ability to administer through the CLI interface (or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality)user data to only authorized administrators. The CLI provides authorized administrators with a text-based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides the authorized administrator the ability to configure an external authentication server, such as a RADIUS or TACACS+ server, for a user. When this is assigned, a user can be authenticated to the external server instead of to directly to the TOE.

FMT_SMF.1 Management of Security Functions

The TOE provides the ability to manage the following security functions: user data (authentication data, roles) and router information. All security function management is done through the CLI (or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality), and is restricted only to authorized administrators.

FMT_SMR.1 Security Roles

The TOE has one pre-defined role, Authorized Administrator. When a new user account is created, it must be assigned this role.

- Authorized Administrator: 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 router configuration information.

6.1.4 Protection of Security Functions

FPT_SEP.1 TSF Domain Separation

The TOE is an appliance in which all operations are self-contained, with all administration and configuration operations are performed within the physical boundary of the TOE. All user and router data can be manipulated via the CLI. However, the traffic directed through the product is routed according to it's configuration but not otherwise subject to security mechanisms. The JUNOS software within the TOE controls all operations. The TOE operates solely as a router and neither performs nor supports other non-router related functions.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Process Assurance;
- Delivery and Guidance;

- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by Juniper ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Juniper ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. Juniper performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation. These activities are documented in:

- Juniper Configuration Management Manual

The Configuration Management assurance measure satisfies the ACM_CAP.2 assurance requirements

6.2.2 Delivery and Guidance

Juniper provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Juniper's delivery procedures describe the steps to be used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions. These procedures are documented in:

- Juniper Delivery and Operation Procedures

Juniper provides administrator guidance in the installation and initialization procedures. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install and operate Juniper products in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration. Since the only users with an interface are administrators, that is the only guidance provided. Non-administrative users have no direct access to the TOE, only using it as a generic network connection component when communicating across connected networks.

The administrator guidance is documented in:

- Juniper Configuration and Management Guide

The Delivery and Guidance assurance measure satisfies the following Assurance requirements:

- ADO_DEL.1;
- ADO_IGS.1;
- AGD_ADM.1; and,
- AGD_USR.1.

6.2.3 Development

The Design Documentation provided for JNR is provided in two documents:

- Juniper Functional Specification
- Juniper High-level Design

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design

abstractions (including the ST). The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.1; and,
- ADV_RCR.1.

6.2.4 Tests

The Test Documentation is found in the following documents:

- Juniper Test Coverage
- Juniper Test Plan
- Juniper Test Procedures

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.1;
- ATE_FUN.1; and,
- ATE_IND.2.

6.2.5 Vulnerability Assessment

Each probabilistic or permutational mechanism used by the TOE must satisfy the SOF-Basic requirements. The only probabilistic or permutational mechanism used in the TOE is the authentication mechanism. Juniper has performed a strength of function analysis that indicates that the authentication mechanism fulfills at least SOF-Basic. Similarly, Juniper performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. Both the strength of function analysis and the vulnerability analysis are documented in:

- Juniper Vulnerability Assessment

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

- AVA_SOF.1; and,
- AVA_VLA.1.

7. Protection Profile Claims

There are no PP claims for this evaluation.

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;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, security threats and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or organizational security policy.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides a mapping of TOE security objectives to those threats that the security objectives that the TOE is designed to counter, assumptions about secure usage, and organizational security policies that the TOE must enforce..

	O.PROTECT	O.EADMIN	O.ACCESS	O.PHYCAL	OE.EAUTH	O.FLOW	O.MANAGE
A.LOCATE				X			
A.NOEVIL							X
A.EAUTH					X		
T.PRIVIL	X		X				
T.OPS	X		X				
P.FLOW						X	
P.MANAGE		X	X				
P.PROTECT	X		X				

Table 4 Environment to Objective Correspondence

8.1.1.1 A.LOCATE

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

The O.PHYCAL provides for the physical protection of the TOE.

8.1.1.2 A.NOEVIL

The authorized administrators are competent, not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The O.MANAGE objective ensures that only non-hostile, competent administrators (following guidance) manage the TOE.

8.1.1.3 A.EAUTH

External authentication services will be available via RADIUS and TACACS+.

The OE.EAUTH objective supports this assumption by requiring that the environment provide RADIUS or TACACS+ services for external authentication.

8.1.1.4 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.

The O.ACCESS objective requires that only authorized users and processes be allowed to access the TOE security functions. The O.PROTECT objective addresses this threat by providing TOE self-protection.

8.1.1.5 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.

The O.PROTECT objective ensures the TOE protects itself from unauthorized modification of security data or functions. The O.ACCESS objective requires that only authorized users and processes be allowed to access the TOE security functions.

8.1.1.6 P.FLOW

The TOE shall ensure that information flows from source to destination according to available routing information.

The O.FLOW object supports this policy by ensuring that information is allowed to flow through the TOE based on available routing information.

8.1.1.7 P.MANAGE

The TOE shall provide effective management functions that can only be utilized by authorized users.

The O.ACCESS objective supports this policy by only allowing authorized and processes users access to the TOE. O.EADMIN ensures there is a set of management functions for administrators to use.

8.1.1.8 P. PROTECT

The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

The O.ACCESS objective supports this policy by only allowing authorized users and processes access to the TOE. The O.PROTECT objective addresses this policy by providing TOE self-protection.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives.

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.FLOW	O.PROTECT	O.EADMIN	O.ACCESS	OE.EAUTH
FDP_IFC.1	X				
FDP_IFF.1	X				
FIA_UAU.1		X		X	
FIA_UAU.5					X
FIA_ATD.1				X	
FIA_UID.1		X		X	
FMT_MSA.3	X				
FMT_MTD.1a			X		
FMT_MTD.1b			X	X	
FMT_SMF.1			X		
FMT_SMR.1		X	X		
FPT_SEP.1		X			

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.FLOW

The TOE must use available routing information to forward network packets to the appropriate destination.

The TOE must enforce a policy and set of rules for information flow ensuring that information is only forwarded to the appropriate destination[FDP_IFC.1, FDP_IFF.1]. The TOE must ensure that appropriate default security attributes are associated with information flows [FMT_MSA.3].

8.2.1.2 O.PROTECT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to authenticate all users prior to any administrative access. [FIA_UAU.1, FIA_UID.1] The TOE requires that users be assigned to roles to determine the level of access granted to the TOE. [FMT_SMR.1] The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

8.2.1.3 O.EADMIN

The TOE must include a set of services that allow effective management of its functions and data.

The TOE must provide the authorized administrators the ability to manage the user accounts of the TOE. [FMT_MTD.1b, FMT_SMF.1] The TOE must provide the authorized administrators and authenticated applications the ability to manage the router configuration. [FMT_MTD.1a, FMT_SMF.1] The TOE allows that privileges be assigned the authorized administrator role, which are then assigned to users, providing a method for ensuring effective management. [FMT_SMR.1] The TOE must provide administrative functions to manage both router functions as well as user data. [FMT_SMF.1]

8.2.1.4 O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data.

Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE requires that all users of the TOE be unique and have unique data. [FIA_ATD.1] Only authorized administrators of the System may manage the TOE data [FMT_MTD.1b]. Only authorized administrators and authenticated applications of the System may manage the TOE data [FMT_MTD.1a]. All user accounts have specific data that must be stored to ensure individual identities as well as unique authentications. [FIA_ATD.1]

8.2.1.5 OE.EAUTH

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

Users can be authenticated to the TOE via two separate authentication mechanisms: the internal fixed password mechanism and the authentication server in the IT environment [FIA_UAU.5].

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL 2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 6 Requirement Dependency Rationale lists each requirement from Section 5.1 with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is proved.

Functional Component	Dependency	Included
FDP_IFC.1	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1	YES
	FMT_MSA.3	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MSA.3	FMT_MSA.1	NO
	FMT_SMR.1	YES
FMT_MTD.1a	FMT_SMF.1	YES
	FMT_SMR.1	YES
FMT_MTD.1b	FMT_SMF.1	YES
	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES

Table 6 Requirement Dependency Rationales

Note that FMT_MSA.1 is not included in this ST given that FMT_MTD.1.a addresses managing router information.

8.5 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements.

8.6 Strength of Function Rationale

The TOE minimum strength of function is SOF-Basic.

This security target includes a probabilistic or permutational function. The list of relevant security functions and security functional requirements includes:

- Identification and Authentication
    - FIA_UAU.1 - Timing of authentication

      The password used at administrator interface via a client application providing a CLI login is the only probabilistic or permutational function on which the strength of the authentication mechanism depends.

The system places the following restrictions on the passwords selected by the user:

- The password must be at least six long;

The password space is calculated as follows:

Patterns of human usage are important considerations that can influence the approach to searching a password space, and thus affect SOF. Assuming the worst case scenario and the user chooses a number comprising only six characters, the number of password permutations is:

52 alpha characters (upper and lower)
10 digits
+ 16 special characters (!, @, #, $, %, ^, &, *, (,), +, =, <, >, :, ;)
78 possible values

78^6 = (78*78*78*78*78*78) = 225,199,600,704

The amount of time it takes to manually type a password given that authentication can only occur based upon manual input is 7 seconds. An attacker can at best attempt (60/7= 8.6 password entries every minute, or 514 password entries every hour.

On average, an attacker would have to enter (225,199,600,704/ 2 = 112,599,800,352) passwords, over (112,599,800,352/ 514) 219,065,759.44 hours, before entering the correct password. The average successful attack would, as a result, occur in slightly less than:

(219,065,759.44 / 24 / 365 =) 25,007.51 years

In accordance with annex B.3 in the CEM, the elapse time of attack is not practical and thus results in a High strength of function rating, which exceeds SOF-Basic.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance

requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	USER DATA PROTECTION	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF SECURITY FUNCTIONS
FDP_IFC.1	X			
FDP_IFF.1	X			
FIA_UAU.1		X		
FIA_ATD.1		X		
FIA_UID.1		X		
FMT_MSA.3			X	
FMT_MTD.1			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_SEP.1				X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See section 7, Protection Profile Claims.