Security Target

Juniper Networks Circuit to Packet Series Version 5.4R2

Document Version 1.3

CMID: 1.1

February 17, 2011

Prepared For:

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
www.juniper.net

Prepared By:

Apex Assurance Group, LLC
530 Lytton Avenue, Ste. 200
Palo Alto, CA 94301
www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Circuit to Packet Series Version 5.4R2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Juniper Networks Circuit to Packet Series Version 5.4R2
ST Revision	1.3
ST Publication Date	February 17, 2011
Author	Apex Assurance Group, LLC

1.2 TOE Reference

TOE Reference	Juniper Networks Circuit to Packet Series Version 5.4R2
TOE Type	Circuit to Packet Platform

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- 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**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms Used in Security Target

1.6 TOE Description

1.6.1 Overview

The TOE is Juniper Networks Circuit to Packet Series Version 5.4R2, which primarily provides the transport Time Division Multiplexing (TDM) and other circuit-based applications across next-generation IP networks.

The Juniper Networks CTP series enables customers to connect circuit-based applications (such as TDM leased line and voice Private Branch Exchange (PBX) connections, serial encryption connections, and analog and digital radio systems networking) across an IP network.

The CTP products are designed to create an IP packet flow from a serial data stream or analog voice connection, providing the necessary processing to re-create the serial bit stream or analog signal from an IP packet flow.

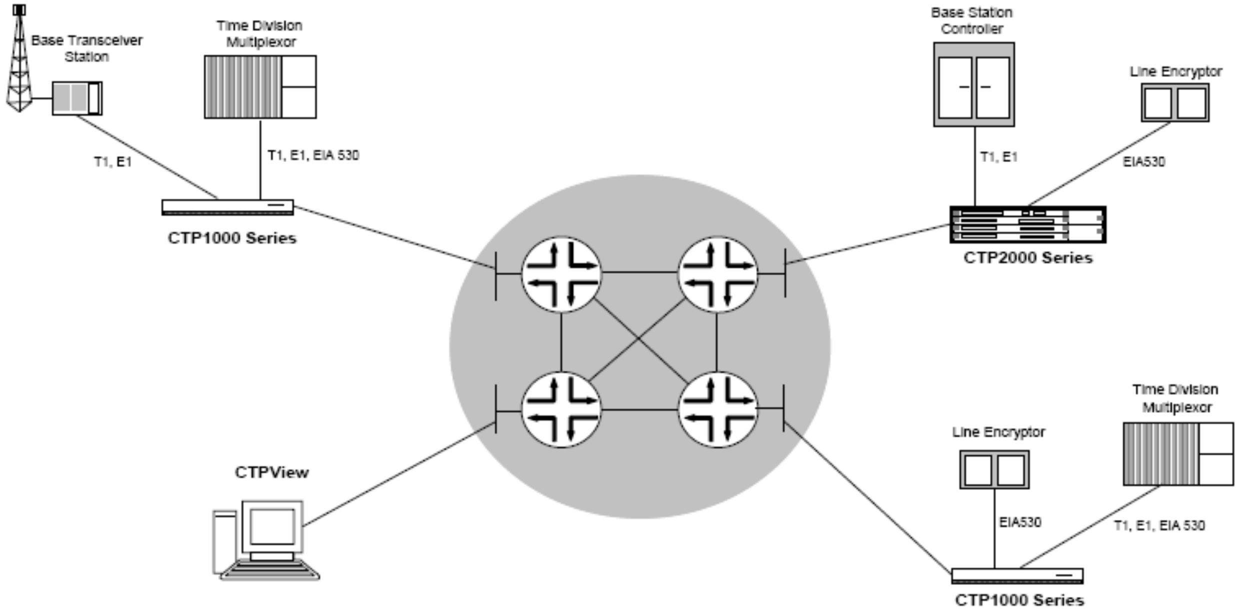

Figure 1 – Common TOE Deployment

Circuit to Packet Series Version 5.4R2 may also be referred to as the TOE in this document.

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

The TOE includes a variety of features to provide security to end users. In addition to controlling the flow of information from a circuit-based network to an IP-based network, the TOE provides for audit, identification/authentication, and security management functions. The TOE is managed using CTPView, a web-based GUI management tool. All management is performed via this interface once the TOE is initialized (initialization occurs over a local terminal console). CTPView requires users to provide unique identification and authentication data before any administrative access to the system is granted. Authentication services are handled internally via fixed user selected passwords. The TOE's audit mechanism (via local syslog) captures authentication activity and configuration changes. Audit details include the date and time, event category, event type, and associated username.

1.6.2 Physical Boundary

The TOE is a combined hardware/software TOE and is defined as the Circuit to Packet Series Version 5.4R2. The TOE boundary is shown below:

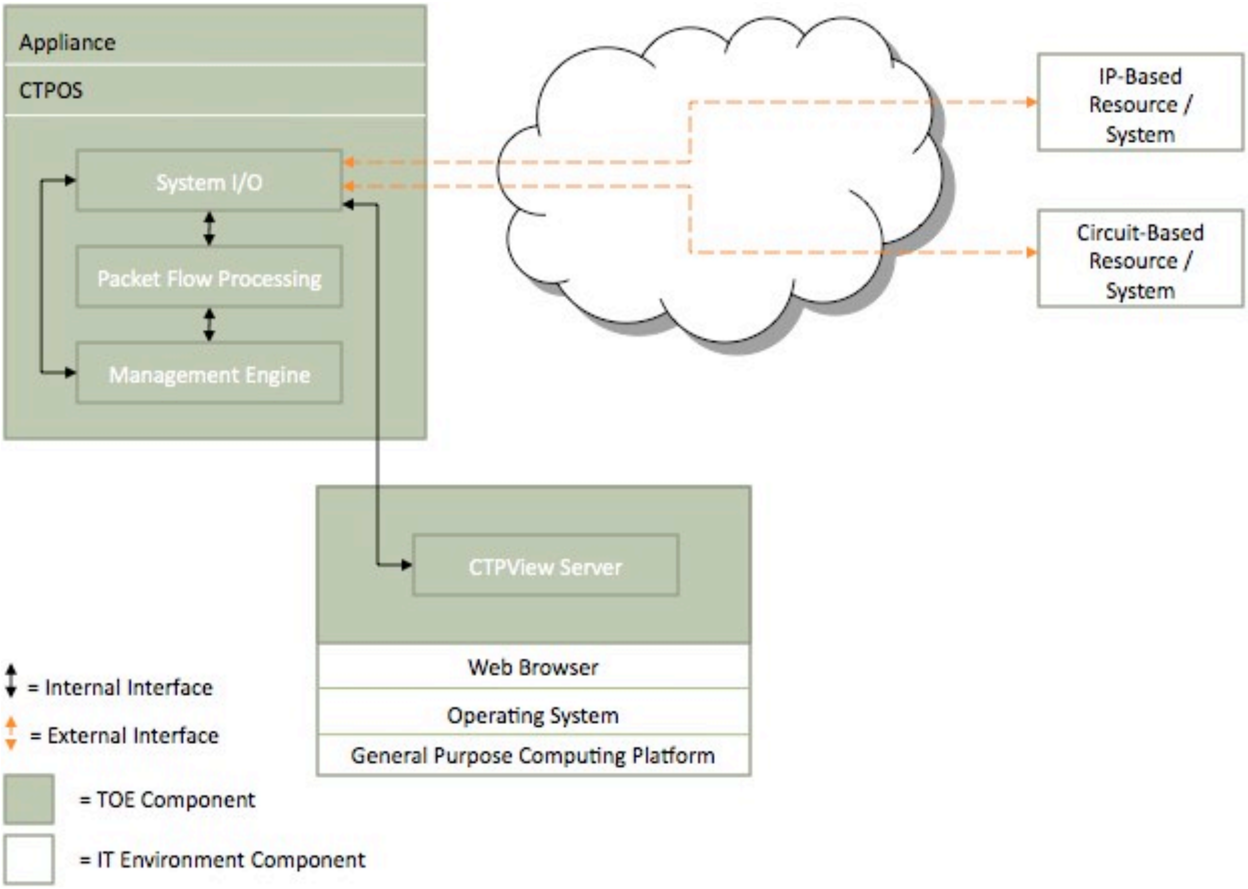

Figure 2 – TOE Boundary

The physical boundary is defined as the entire chassis, as depicted below:

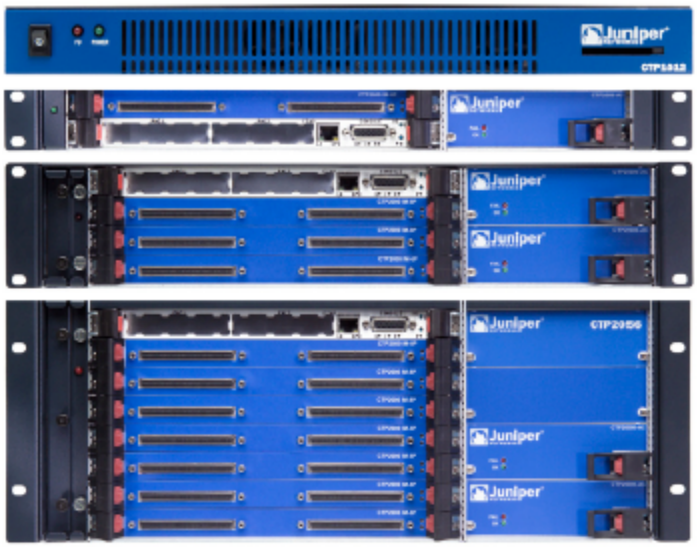

Figure 3 – CTP1004/1012, CTP2008, CTP2024, CTP2056 (Top to Bottom)

In order to comply with the evaluated configuration, the following hardware and software components should be used:

COMPONENT	VERSION/MODEL NUMBER
Software Version	• Appliances: CTPOS Version 5.4R2 • Management: CTPView 3.4R2
Hardware Version	• CTP1004 • CTP1012 • CTP2008 • CTP2024 • CTP2056
IT Environment[1]	• General Purpose Computing Platform • Operating System: CentOS 5.3 • CTPView Server Appliance: CTPView[2] • Web Browser (Firefox, Mozilla, or Internet Explorer 7 required to support Tabbed Browsing feature)
User documentation and evaluation evidence	Please see Table 20 – Security Assurance Rationale and Measures in Section 6.3.6 – Security Assurance Requirements Evidence.

Table 3 – Evaluated Configuration for the TOE

[1] Note that the operating system, database, and webserver running within CTPVIew Server are provided by Juniper as part of the CTPView installation

[2] Note that the CTPView appliance is not distinctly versioned for hardware or software. Administrators must follow the Installation instructions in *Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2.*

The TOE interfaces are comprised of the following:

INTERFACE TYPE	DESCRIPTION
External Interfaces	• Network interfaces to Circuit-based system • Network interfaces to IP-based system
Internal Interfaces	• Management Engine to System I/O and Packet Flow Processing to enforce management actions and gather information for reporting • CTPView to CTP Management Engine to handle management actions. This interface occurs from the CTPView Server to the Ethernet interface on the appliance.

Table 4 – Summary of TOE Interfaces

1.6.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Audit	Auditable events are stored locally in syslog files. Audit events cover authentication activity and configuration changes, and the audit details include the date and time, event category, event type, username. An accurate time is gained by the use of NTP provided by the environment.
Information Flow Control	The TOE is designed to forward circuit-based application data network packets (i.e., information flows) from source network entities to destination network entities based on available routing information. This information is either provided indirectly from other network entities (outside the TOE) or 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. Authentication services are handled internally via fixed user selected passwords.
Management	The TOE is managed using CTPView, a web-based GUI management tool. All management is performed via this interface once the TOE is initialized. Initialization occurs over a local terminal console.

Table 5 – Logical Boundary Descriptions

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant.

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NOAUDIT	Unauthorized changes to the router configurations and other management information will not be detected.
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.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.ROUTE	Network packets may be routed inappropriately due to accidental or deliberate misconfiguration.

Table 6 – Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE is not required to meet any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	The authorized users will be competent, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.COMPONENTS	Components accessing the management interfaces of the TOE will be located within controlled facilities, and the authorized users of these components will be competent, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTECT_COMM	The connection between physically separate TOE components is protected from unauthorized tamper, modification, or eavesdropping.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must only allow authorized users and processes (applications) to access protected TOE functions and data.
O.AMANAGE	The TOE management functions must be accessible only by authorized users.
O.AUDIT	Users must be accountable for their actions in administering the TOE.
O.EADMIN	The TOE must provide services that allow effective management of its functions and data.
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.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMIN	Authorized users must follow all guidance.
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.COMPONENTS	Those responsible for the TOE must ensure that IT environment and non-IT environment components that have access to the management interface of the TOE are protected physically and procedurally.
OE.PROTECT_COMM	Those responsible for the TOE must ensure that IT environment protects the communications between TOE components from unauthorized tamper, modification, or eavesdropping.

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS OBJECTIVES	T.ROUTE	T.PRIVIL	T.OPS	T.NOAUDIT	A.LOCATE	A.COMPONENTS	A.PROTECT COMM	A.NOEVIL
O.FLOW	✓							
O.PROTECT	✓	✓	✓					
O.EADMIN	✓							
O.AMANAGE	✓	✓						
O.ACCESS	✓	✓	✓					
O.AUDIT	✓	✓	✓	✓		✓		✓
OE.PHYSICAL					✓			
OE.ADMIN								✓
OE.COMPONENTS						✓		
OE.PROTECT_COMM							✓	

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.NOAUDIT	This threat is completely countered by O.AUDIT, which ensures users are accountable for their actions in administering the TOE.
T.OPS	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data.
T.PRIVIL	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AMANAGE which ensures that the TOE management functions are accessible only by authorized users. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data.

THREAT	RATIONALE
T.ROUTE	This threat is completely countered by • O.ACCESS which ensures the TOE only allows authorized users and processes (applications) to access protected TOE functions and data. • O.AUDIT which ensures users are accountable for their actions in administering the TOE. • O.AMANAGE which ensures that the TOE management functions are accessible only by authorized users. • O.EADMIN which ensures that the TOE provides services that allow effective management of its functions and data • O.FLOW which ensures that network packets flow from source to destination according to available routing information in the TOE configuration. • O.PROTECT which ensures the TOE protects against unauthorized accesses and disruptions of TOE functions and data.

Table 11 – Mapping of Objectives to Threats

4.3.2 Rationale for Security Objectives of the TOE and IT Environment

OBJECTIVE	RATIONALE
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) and unauthorized access (T.PRIVIL and T.OPS).
O.AMANAGE	The objective to limit access to management functions helps ensure correct routing (T.ROUTE), and helps counter the threat of unauthorized access (T.PRIVIL).
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, and T.OPS. It also helps to support the assumption A.NOEVIL, by recording actions of users.
O.EADMIN	This objective is to provide effective management tools that assist in the correct routing of packets (T.ROUTE).
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).
OE.ADMIN	The objective that users should follow guidance supports the assumption that they will not be careless, willfully negligent or hostile (A.NOEVIL).
OE.PHYSICAL	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.LOCATE).
OE. COMPONENTS	The objective to provide physical and procedural protection components with access to the TOE management interface supports the assumption that those components will be located within controlled access facilities and users will follow all guidance (A.LOCATE).

OBJECTIVE	RATIONALE
OE.PROTECT_COMM	The objective to protect the communications between TOE components from unauthorized tamper, modification, or eavesdropping supports the assumption that the IT environment will provide a means to secure the communication between components.

Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

This evaluation does not include extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 13 – TOE Security Functional Requirements

All dependencies for Security Functional Requirements are satisfied as described in Part 2 of the Common Criteria.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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) Configuration is committed on a device;

f) Configuration is changed;

g) Errors during processing of the Virtual Circuit Flow Control SFP]

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 other audit relevant information].

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [Virtual Circuit Flow Control SFP] on

[Subjects: unauthenticated external IT entities that send and receive data through the TOE to one another,

Information: network packets sent through the TOE from one subject to another, and

Operations: send and receive].

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

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

[Subject security attributes:

- Presumed address

Information security attributes:

- Bundle type (i.e., the packetization and transport mechanisms of the physical port data)
  - CTP: circuit to packet
  - SAToP: TDM over packet
  - CESoPSN: circuit emulation services of packet structure network
- Port Type
- Port Number
- Port Speed
- Packet Size
- Presumed address of source subject

- Presumed address of destination subject].

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:

[

- 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 that destination subject

].

FDP_IFF.1.3 The TSF shall enforce the [Network Address Translation operations with Destination IP address translation and/or Source IP address translation if configured to do so].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional Virtual Circuit Flow Control SFP rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [no additional Virtual Circuit Flow Control SFP rules].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Data, Group, Role].

6.1.3.2 FIA_SOS.1 Verification of secrets

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

- Password may not contain the Username
- Password must be alphanumeric or the characters @ { } # % ~ [ ] = & , - _ . !
- Minimum password length is 15 characters
- Maximum password length is 56 characters

- Password must contain at least 1 lower case letter(s)
- Password must contain at least 1 upper case letter(s)
- Password must contain at least 1 digit(s)
- Password must contain at least 1 non-alphanumeric character(s)
- Same password cannot be reused for at least 10 password changes
- Passwords cannot be in the excluded password list

].

6.1.3.3 FIA_UAU.2 User Authentication before Any Action

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

6.1.3.4 FIA_UID.2 User Identification before Any Action

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

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to **control** the [data described in the table below] to [roles specified in the table below]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE
Virtual Circuit Flow Control SFP	G_A N_A	G_A N_A N_V	G_A N_A	G_A N_A
Rules that restrict the ability to establish management sessions	G_A	G_A	G_A	G_A
User Identity	G_A	G_A	G_A	G_A
Authentication Data	G_A			G_A
Group	G_A	G_A	G_A	G_A
Role	G_A	G_A	G_A	G_A

Table 14 – Management of TSF data (G_A=Global_Admin, N_A=Net_Admin, N_V=Net_View)

6.1.4.2 FMT_SMF.1 Specification of Management Functions

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

a) modify TOE configuration, including

  1. control of management session establishment

  2. configuration of Virtual Circuit Flow Control SFP

b) modify user account attributes (including operation of identification and authentication and group)].

6.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Net_View, Net_Admin, Global_Admin].

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

6.2 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.3.4 – Security Assurance Requirements.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements

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

OBJECTIVE SFR	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.AUDIT
FAU_GEN.1						✓
FDP_IFC.1	✓	✓				
FDP_IFF.1	✓	✓				
FIA_ATD.1		✓		✓	✓	✓
FIA_SOS.1		✓		✓	✓	
FIA_UAU.2		✓		✓	✓	
FIA_UID.2		✓		✓	✓	

OBJECTIVE SFR	O.FLOW	O.PROTECT	O.EADMIN	O.AMANAGE	O.ACCESS	O.AUDIT
FMT_MTD.1	✓	✓		✓	✓	
FMT_SMF.1	✓	✓	✓	✓	✓	
FMT_SMR.1	✓	✓	✓	✓	✓	

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2 Sufficiency of Security Requirements

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

SFR	RATIONALE
FAU_GEN.1	This component outlines what events must be audited, and aids in meeting O.AUDIT.
FDP_IFC.1	This component identifies the entities involved in the Virtual Circuit Flow Control SFP (i.e. external IT entities sending packets), and aids in meeting O.FLOW and O.PROTECT.
FDP_IFF.1	This component identifies the conditions under which information is permitted to flow between entities (the Virtual Circuit Flow Control SFP), and aids in meeting O.FLOW and O.PROTECT.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. The component aids in meeting O.PROTECT, O.AMANAGE, O.ACCESS and O.AUDIT.
FIA_SOS.1	This component specifies metrics for authentication, and aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UAU.2	This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).
FIA_UID.2	This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access (O.PROTECT, O.AMANAGE and O.ACCESS).

SFR	RATIONALE
FMT_MTD.1	This component restricts the ability to modify the Virtual Circuit Flow Control SFP and as such aids in meeting O.FLOW, O.AMANAGE, and O.PROTECT. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.PROTECT, O.AMANAGE and O.ACCESS. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.AMANAGE.
FMT_SMF.1	This component lists the security management functions that must be controlled. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, and O.ACCESS.
FMT_SMR.1	Each of the components in the FMT class listed above relies on this component. It defines the roles on which access decisions are based. As such it aids in meeting O.FLOW, O.PROTECT, O.EADMIN, O.AMANAGE, and O.ACCESS.

Table 16 – Rationale for TOE SFRs to Objectives

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

OBJECTIVE	RATIONALE
O.ACCESS	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE. • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MTD.1 which restricts the ability to TOE data • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.AMANAGE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE. • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MTD.1 which restricts the ability to modify the Virtual Circuit Flow Control SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, and restricts the ability to modify the data relating to TOE access locations • FMT_SMF.1 which lists the security management functions that must be controlled. • FMT_SMR.1 which defines the roles on which access decisions are based.
O.AUDIT	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited. • FIA_ATD.1 which provides users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users.
O.EADMIN	This objective is completely satisfied by • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.FLOW	This objective is completely satisfied by • FDP_IFC.1 identifies the entities involved in the Virtual Circuit Flow Control SFP (i.e. external IT entities sending packets). • FDP_IFF.1 identifies the conditions under which information is permitted to flow between entities (the Virtual Circuit Flow Control SFP). • FMT_MTD.1 restricts the ability to query, modify, delete, clear, or change default values for the Virtual Circuit Flow Control SFP. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.

OBJECTIVE	RATIONALE
O.PROTECT	This objective is completely satisfied by • FDP_IFC.1 identifies the entities involved in the Virtual Circuit Flow Control SFP (i.e. external IT entities sending packets). • FDP_IFF.1 identifies the conditions under which information is permitted to flow between entities (the Virtual Circuit Flow Control SFP). • FIA_ATD.1 exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users. • FIA_SOS.1 specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 ensures that users are authenticated to the TOE and as such it aids in meeting objectives to restrict access. • FIA_UID.2 ensures that users are identified to the TOE. • FMT_MTD.1 restricts the ability to modify user account attributes. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based

Table 17 – Rationale for TOE Objectives to SFRs

6.3.3 Rationale for SFR Dependency

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

SFR	CC DEPENDENCY	ST DEPENDENCY
FAU_GEN.1	FPT_STM.1	Provided by the IT environment
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 (FMT_MSA.3 not applicable[3])
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	None
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Table 18 – SFR Dependency

[3] FMT_MSA.3 does not impact the security required by FDP_IFF.1 for this particular TOE because there are no configurable security attributes.

6.3.4 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorisation Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer defined life-cycle model
ATE: Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 19 – Security Assurance Requirements at EAL3

6.3.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3. EAL3 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. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.3.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Juniper Networks Circuit to Packet Series Version 5.4R2
ADV_FSP.3 Functional Specification with Complete Summary	Functional Specification: Juniper Networks Circuit to Packet Series Version 5.4R2
ADV_TDS.2 Architectural Design	Architectural Design: Juniper Networks Circuit to Packet Series Version 5.4R2

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2 CTP Software Configuration Guide Hardware, Installation, and Software Configuration Guide CTPOS Release Notes CTPView Server Release Notes
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2 CTP Software Configuration Guide Hardware, Installation, and Software Configuration Guide CTPOS Release Notes CTPView Server Release Notes
ALC_CMC.3 Authorisation Controls	Configuration Management Processes and Procedures: Juniper Networks Circuit to Packet Series Version 5.4R2
ALC_CMS.3 Implementation representation CM coverage	Configuration Management Processes and Procedures: Juniper Networks Circuit to Packet Series Version 5.4R2
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: Juniper Networks Circuit to Packet Series Version 5.4R2
ALC_DVS.1 Identification of Security Measures	Security Measures: Juniper Networks Circuit to Packet Series Version 5.4R2
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Model: Juniper Networks Circuit to Packet Series Version 5.4R2
ATE_COV.2 Analysis of Coverage	Testing Evidence Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2
ATE_DPT.1 Testing: Basic Design	Testing Evidence Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2
ATE_FUN.1 Functional Testing	Testing Evidence Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2

Table 20 – Security Assurance Rationale and Measures

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Audit
- Information Flow Control
- Identification and Authentication
- Security Management

7.2 Audit

CTPOS creates and stores audit records for the following events:

a) User login/logout;

b) Login failures;

c) Configuration is committed on a device;

d) Configuration is changed;

e) Errors during processing of the Virtual Circuit Flow Control SFP

Audit records are stored in syslog format in the IT Environment; the use of an external syslog server is not included as part of the evaluated configuration. The syslogs are automatically deleted locally according to configurable limits on storage volume or number of days of logs to retain.

CTPOS 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.

Audit logs are time-stamped with time values derived from the IT environment via NTP..

The Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1

7.3 Information Flow Control

The TOE supports one information flow control policy: the Virtual Circuit Flow Control SFP. This policy enforces rules for the transit traffic, in terms of what traffic can pass through the TOE.

The TOE is designed to route circuit-based 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 from network peers as defined by the TOE users. The routing decision is based on the presumed source and destination address of the packet, service, and the interface on which the packet arrives and is to depart on.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.1
- FDP_IFF.1

7.4 Identification and Authentication

User accounts in the TOE have the following attributes: user name, authentication data (password) and role (i.e., Global_Admin, Net_Admin, Net_View).

Locally stored authentication data for fixed password authentication is a case-sensitive, alphanumeric value. The password requirements are as follows:

- Password may not contain the Username
- Password must be alphanumeric or the characters @ { } # % ~ [ ] = & , - _ . !
- Minimum password length is 15 characters
- Maximum password length is 56 characters
- Password must contain at least 1 lower case letter(s)
- Password must contain at least 1 upper case letter(s)
- Password must contain at least 1 digit(s)
- Password must contain at least 1 non-alphanumeric character(s)
- Same password cannot be reused for at least 10 password changes
- Passwords cannot be in the excluded password list

The TOE requires users to provide unique identification and authentication data before any access to the system is granted. The TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Regardless, no administrative actions are allowed until successful authentication. The authentication 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 circuit data between nodes. This passes the packets from one network to a destination network, enabling network connectivity.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UID.2

7.5 Security Management

The functionality in the TOE requires management to ensure proper configuration control.

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

1. Net_View—Users belonging to this role are restricted to query-only access to CTP systems.
2. Net_Admin— Users belonging to this role are able to configure CTP systems; however, they do not have the ability to create or modify CTPView user accounts.
3. Global_Admin— Users belonging to this role have all the privileges of the Net_Admin class. They are also able to create and modify user accounts.

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

a) User roles(authentication data, roles);

b) Session establishment restrictions;

c) Parameters for Virtual Circuit Flow Control SFP.

The TOE is delivered with restrictive default values such that no traffic can pass across the TOE until specific configuration changes are made; moreover, configuration changes can only be made by an authorized Global_Admin, which is defined in the initialization of the TOE. The TOE restricts the ability to administer the TOE configuration data to only Global_Admins. The CLI provides a text-based interface from which the initial configuration can be managed and maintained. All subsequent management occurs via the CTPView GUI. From this interface new accounts can be created, and existing accounts can be modified or deleted by the Global_Admin.

The TOE restricts the ability to administer user data to only Global_Admin. TOE will allow only a Global_Admin create, delete or modify the rules that control the presumed address from which management sessions can be established.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1