122-B

CERTIFICATION REPORT No. CRP258

Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 and EX8200 Switches running JUNOS 10.0R3.10

Version 10.0R3.10

Issue 1.1

March 2011

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.			
Sponsor:	Juniper Networks Inc.	Developer:	Juniper Networks Inc.
Product and Version:	JUNOS Version 10.0R3.10		
Platform(s):	M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480, MX960, EX3200, EX4200, EX8200		
Description:	The evaluated version of this product routes IP traffic over a network with increasing scalability of the traffic volume with each router model. Each packet is scanned and then compared against a set of rules to determine where the traffic should be routed.		
CC Version:	Version 3.1		
CC Part 2:	Conformant	CC Part 3:	Conformant
EAL:	EAL3 augmented by ALC_FLR.3		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	CRP258	Date Certified:	8 October 2010

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements in this Certification Report, excluding ALC_FLR.3, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Juniper Networks Services Routers and Switches running JUNOS R10.0R3.10 to the Sponsor, Juniper Networks Inc, as summarised on page 2 ‘Certification Statement’ of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC EAL3 augmented by ALC_FLR.3 on 7 October 2010:

> **JUNOS 10.0R3.10 running on M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 and EX8200 Switches.**

4. The Developer was Juniper Networks Inc.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III ‘Evaluated Configuration’ of this report.

6. The Juniper Networks Services Routers and Switches run the same JUNOS software (version 10.0R3.10) in order to provide IP routing, together with management and control functions. The architecture separates routing and control functions from packet forwarding functions, thereby permitting the routers to maintain a high level of performance.

7. The scope of the JUNOS 10.0R3.10 TOE *excludes* the use of GUI management tools (e.g. J-web and JUNOScope); all management is to be performed via the CLI.

8. An overview of the TOE and its product architecture can be found in Chapter IV ‘Product Architecture’ of this report. Configuration requirements are specified in Section 1.5 of [ST].

Security Claims

9. The Security Target [ST] fully specifies the TOE’s Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) that elaborate the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

10. The environmental assumptions related to the operating environment are detailed in Chapter III (in ‘Environmental Requirements’) of this report.

Evaluation Conduct

11. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of JUNOS 9.3R1.7, which had previously been certified [CR], with assurance continuity activity [MR], by the UK IT Security Evaluation and Certification Scheme to the CC EAL3 assurance level. For the evaluation of JUNOS 10.0R3.10, the Evaluators made some reuse of the previous evaluation results where appropriate.

12. The CESG Certification Body monitored the evaluation, which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in October 2010, were reported in the Evaluation Technical Report ([ETR], [ETRS]).

13. As part of their evaluation, the Evaluators examined the 'Secure Configuration Guide for Common Criteria and JUNOS-FIPS' [SCG], as reported in the Evaluation Technical Report ([ETR], [ETRS]) and Issue 1.0 of this Certification Report. However the version on the JUNOS webpage is [SCG1], because [SCG] was actually a pre-publication copy. [SCG1] is identical to [SCG], apart from minor corrections to contributor names, formatting and date, that do not affect its content. Hence this Certification Report has been updated to Issue 1.1, to refer to [SCG1].

Conclusions and Recommendations

14. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

15. Prospective consumers of JUNOS 10.0R3.10 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in [ST]. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

16. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

17. In addition, the Evaluators' comments and recommendations are as follows:

a) TOE consumers should not use the J-Web or JUNOScope interfaces[2] for the administration of the TOE;

b) all guidance necessary to determine that the TOE has been securely delivered and to securely install and operate the TOE is provided in, or referenced from, [SCG1] which is available for download from the JUNOS webpage, linked from http://www.juniper.net/techpubs/.

[2] Note that these interfaces are not in scope of the TOE, but the recommendation is provided to prevent any confusion.

Disclaimers

18. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

19. Certification is not a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

20. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

21. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

22. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

23. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery

24. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied and check that the TOE's security has not been compromised during delivery.

25. [SCG1] section "Identification of Secure Delivery" directs the consumer to:

a) Perform specified checks of the package received to verify it has not been tampered with or delivered from a source masquerading as Juniper Networks Inc.

b) Download the TOE from the Juniper Networks Inc. website at http://www.juniper.net as detailed in [SCG1]. Administration guidance for the TOE is on that site. A consumer is required to have a username and password to access that site's secure area. A username and password is provided to the consumer when they purchase the TOE.

c) Validate the MD5 and/or SHA-1 checksums, which are provided on the http://www.juniper.net website and in [SCG1].

d) Although the TOE is the same, regardless of the Router or Switch on which it is installed, there are different download packages: one for each of the EX3200, EX4200 and EX8200 Switches and one for the M-, T- and MX-series Routers.

Installation and Guidance Documentation

26. The Installation and Secure Configuration documentation is as follows:

a) Secure Configuration Guide for Common Criteria and JUNOS-FIPS [SCG1];

b) Software Installation and Upgrade Guide [Install].

27. The User Guide and Administration Guide documentation is as follows:

a) CLI User Guide [CLI];

b) Routing Protocols Configuration Guide [RPCG];

c) System Basics Configuration Guide [SBCG];

d) Secure Configuration Guide for Common Criteria and JUNOS-FIPS [SCG1];

e) System Log Messages Reference [SLMR];

f) JUNOS XML API Configuration Reference [XML].

III. EVALUATED CONFIGURATION

TOE Identification

28. The TOE is JUNOS 10.0R3.10, which consists of: software implementing the Routing Engine, and firmware, running on Application-Specific Integrated Circuits (ASICs), implementing the Packet Forwarding Engine (PFE).

TOE Documentation

29. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

30. The TOE Scope is defined in the Security Target [ST] Section 1.5. Functionality that is outside the TOE Scope is defined in [ST] Section 1.5.1.3. It should be noted that use of the GUI interfaces (e.g. J-web and JUNOScope) is to be disabled in the evaluated configuration, as detailed in [SCG1] section "Supported User Interface for Configuring JUNOS OS".

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

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

a) all hardware, including that associated with forwarding interfaces Pluggable Interface Controllers (PICs), Flexible PIC Concentrators (FPCs), Line Cards;

b) external servers (audit, NTP, authentication, FTP Servers);

c) encryption and integrity checking functionality;

d) high availability functionality.

TOE Configuration

33. The evaluated configuration of the TOE is defined in [ST] Section 1.5.

34. The evaluated TOE configuration comprises any of the following Juniper Routers and Switches running JUNOS 10.0R3.10:

M7i
M10i
M40e
M120
M320
T320
T640
T1600
EX3200
EX4200
EX8200
MX240
MX480
MX960

35. The router and switch hardware is part of the environment.

36. In the evaluated configuration, an external authentication server (either RADIUS or TACACS+) can be used in order to authenticate administrative connections.

Environmental Requirements

37. The environmental assumptions for the TOE are stated in [ST] Section 1.5.1.2.

38. The TOE was evaluated running on the platforms detailed in TOE Configuration above.

39. The environmental IT configuration is as follows:

a) network connection to NTP server;

b) network connection to RADIUS or TACAS+ server(s), to provide external authentication services as necessary.

Test Configuration

40. The Developer used the configuration shown in Figure 1 below for their testing:

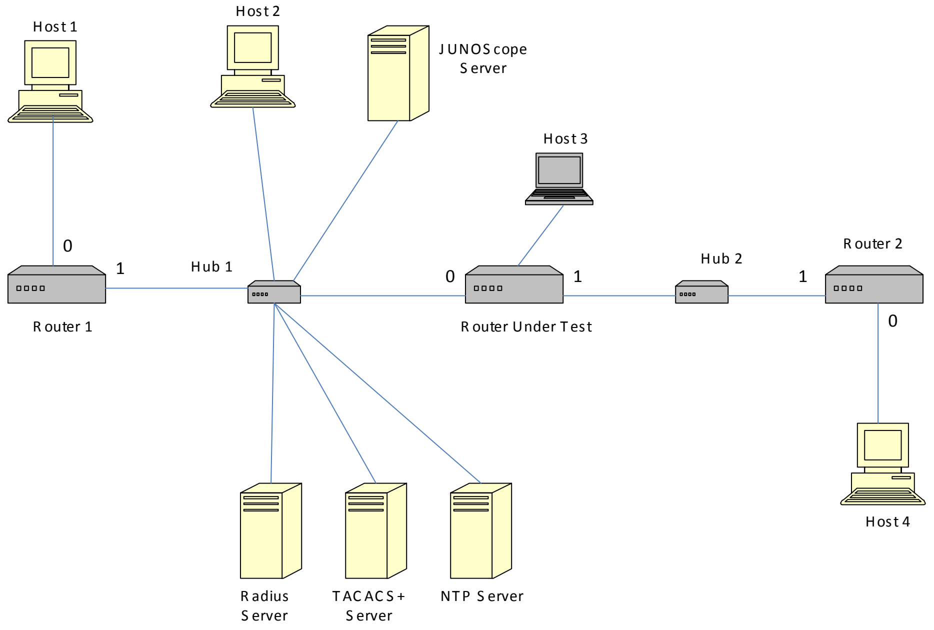

Figure 1 – Developer's Test Configuration and Evaluators' First Testing Configuration

41. At the time of developer testing, the JUNOScope server formed part of the IT environment. That server was subsequently removed, as detailed in Chapter V (in 'Vulnerability Analysis') of this report.

42. The Evaluators performed two sets of testing activities. For their first testing activity, they used the Developer’s test configuration shown in Figure 1. For their second testing activity, they used the configuration shown in Figure 2 below:

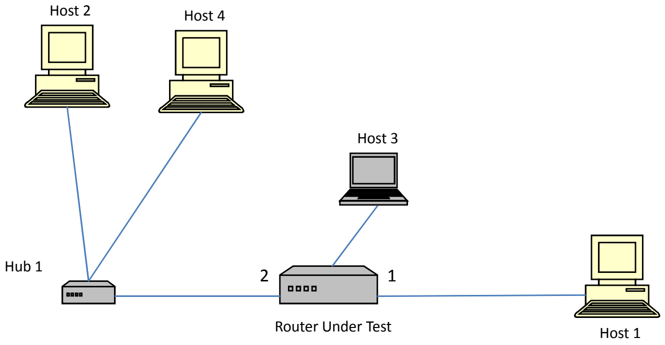

Figure 2 – Evaluators’ Second Testing Configuration

IV. PRODUCT ARCHITECTURE

Introduction

43. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

44. The TOE architecture, as shown in Figure 3, consists of the following two main features:

a) The Routing Engine, which provides layer 2 and layer 3 routing services and network management;

b) The Packet Forwarding Engine, which provides all operations necessary for packet forwarding.

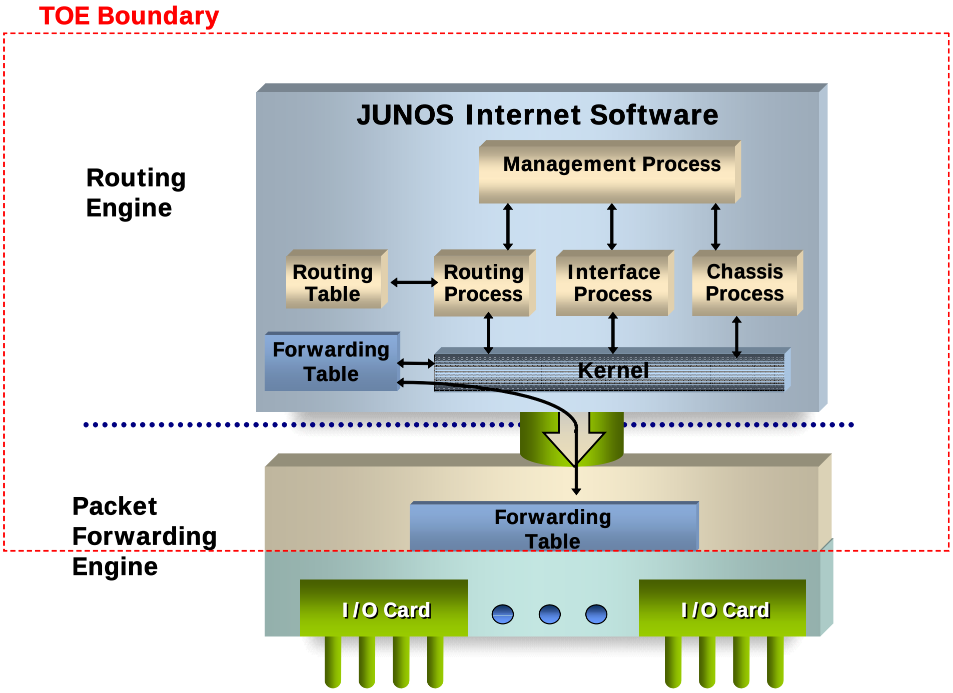

Figure 3 – TOE Architecture

45. The TOE forwards network packets from source network entities to destination network entities based on available routing information. This routing information is either provided directly by TOE users, or indirectly from other network entities (outside the TOE).

46. The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted. Authentication can be handled either internally (user selected passwords), or through a RADIUS or TACACS+ authentication server in the environment.

47. The Routers and Switches are managed using a CLI protected by SSH.

48. Auditable events (as defined in [ST]) are stored in local syslog files. An accurate timestamp is gained by the router ntp daemon, acting as a client to an NTP Server in the environment.

TOE Design Subsystems

49. The TOE subsystems, and their security features/functionality, are as follows:

a) Chassisd. This is the daemon that is responsible for initialising and maintaining the state of the hardware including the physical interfaces.

b) DCd. The DCd initialises and maintains the state of the logical interfaces.

c) PFE. Through packets (with a presumed destination address different to that of the router) are forwarded by the Packet Forwarding Engine (PFE), based on information in the forwarding table.

d) RPD. The Routing Protocol Daemon (RPD) exchanges routing information with network peers. This daemon also accepts local configuration changes from the MGD, and is responsible for building the forwarding table.

e) MGD. The Management Daemon (MGD) interprets all user commands. Each time a user enters a command, the MGD parses the command and checks whether the user has the correct permissions. If so, the MGD allows the user to update the configuration.

f) JUNOS Kernel. The JUNOS Kernel is responsible for mediating all access between daemons, and for keeping track of all listening sockets.

g) INETD. INETD opens sockets bound to ports for SSH connections. It then performs a 'listen' system call to tell the JUNOS Kernel that it will accept new connections on these sockets.

h) SSHD. The SSHD daemon is started by INETD, and receives SSH management connections from the JUNOS Kernel.

i) PAM. PAM (Portable Authentication Module) is responsible for performing the actual authentication of users. This is either a local password authentication, or communication with an external RADIUS or TACACS+ server.

j) Access Daemons. This subsystem consists of access daemons responsible for managing the authentication of connections, including Login for console connections.

k) EVENTD. The event daemon manages the audit logs and is responsible for generating audit records for all auditable events as detailed in [ST].

l) NTPD. The Network Time Protocol Daemon receives NTP packets from an external NTP Server, and uses them to synchronise the local clock.

TOE Dependencies

50. The TOE dependencies are as follows:

a) external authentication server (RADIUS or TACACS+) to support user authentication;

b) external NTP server for provision of time;

c) underlying Juniper Ethernet Services Router (M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 or MX960) or Ethernet Switch (EX3200, EX4200 or EX8200).

TOE Interfaces

51. The external TOE Security Functions Interface (TSFI) is described as follows:

a) External traffic interface to the PFE: All traffic, whether management traffic to the TOE or packets to be routed through the TOE, is received at this interface.

b) Logical XML Administrative Interface to the MGD: This interface is described by the user commands available to an administrator, and the XML generated by the CLI.

V. TOE TESTING

TOE Testing

52. The Developer's tests covered:

a) all SFRs;

b) all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;

c) all Security Functions (SFs);

d) the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

53. The Developer carried out testing on all platforms listed in Chapter III (in 'TOE Configuration') of this report, using the test configuration(s) detailed in Chapter III (in 'Test Configuration') of this report.]

54. The Evaluators devised and ran a total of 17 independent functional tests, different from those performed by the Developer. No anomalies were found.

55. The Evaluators also devised and ran a total of 14 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

56. The evaluators carried out testing on the M7i, MX960, EX4200 and EX8208[3] platforms using the test configurations detailed in Chapter III (in 'Test Configuration') of this report.

57. The Evaluators finished running their penetration tests on 20th September 2010.

Vulnerability Analysis

58. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR] and [ETRS], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the developer's vulnerability analysis.

59. The Evaluators found no exploitable vulnerabilities in the TOE, when used in its evaluated configuration. (The Evaluators identified a vulnerability in the J-web GUI tool, however the scope of the evaluation excluded the use of GUI tools for management of the TOE.)

Platform Issues

60. The evaluators compiled a multi-platform rationale, considering the variations in the hardware platforms across the range of routers and switches specified in [ST]. As a result of this analysis, and considering the PFE variations and different software packages necessary to support them, the Evaluators selected the following sample of platforms:

[3] EX8208 is a representative model in the EX8200 series.

a) M7i (100Base-TX Fast Ethernet);

b) MX960 (10Gb Ethernet);

c) EX4200 (100Base-FX Ethernet);

d) EX8200 (100Base-FX Ethernet), represented by the EX8208 model.

61. These selected platforms included an example of each PFE variant and two of the three EX-series images, to provide further evidence that two images on the same hardware format (line cards) behave in the same manner, even though separate software images are used for each EX platform. Therefore, it was determined that the selected sample of platforms was representative of the complete set of platforms addressed in the evaluation.

VI. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[CLI] CLI User Guide,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-12.

[CR] Common Criteria Certification Report No. CRP248,
UK IT Security Evaluation and Certification Scheme,
CRP248, Issue 1.0, February 2009.

[ETR] Evaluation Technical Report,
SiVenture CLEF,
LFV/T009/ETR, Issue 1.0, September 2010.

[ETRS] Review Form (LFV/T009 Supplement to the ETR),
CESG Certification Body and SiVenture CLEF,
CB/101007/LFV/T009, 8 October 2010.

[Install] Software Installation and Upgrade Guide,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-12.

[MR] Assurance Maintenance Report MR1 (supplements Certification Report CRP248),
UK IT Security Evaluation and Certification Scheme,
MR1, Issue 1.0, February 2009.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010)

[RPCG] Routing Protocols Configuration Guide,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-13.

[SBCG] System Basics Configuration Guide,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-12.

[SCG][4] Secure Configuration Guide for Common Criteria and JUNOS-FIPS,
Juniper Networks Inc.,
Part Number: September, Revision 2; Published 2010-09-17.

[SCG1][4] Secure Configuration Guide for Common Criteria and JUNOS-FIPS,
Juniper Networks Inc.,
Part Number: October, Revision 2; Published 2010-10-21.

[SLMR] System Log Messages Reference,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-14.

[ST] Security Target for Juniper Networks M-Series Multiservice Edge Routers, MX-Series Ethernet Services Routers, T-Series Core Routers and EX Series Ethernet Switches running JUNOS 10.0R3.10,
Juniper Networks Inc.,
Issue 1.3, 7 October 2010.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

[XML] JUNOS XML API Configuration Reference,
Juniper Networks Inc.,
Release 10.0, Published 2009-10-19.

[4] The evaluators evaluated [SCG], whereas [SCG1] is formally published on the Juniper website. [SCG1] is identical to [SCG], apart from minor changes to contributors, formatting and date, that do not affect its content.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

ASIC	Application-Specific Integrated Circuit
CLI	Command Line Interface
DPC	Dense Port Concentrator
FPC	Flexible PIC Concentrator
GUI	Graphical User Interface
MGD	Management Daemon
PAM	Pluggable Authentication Module
PFE	Packet Forwarding Engine
PIC	Pluggable Interface Controller