122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP248

Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1

Version 9.3R1

Issue 1.0

February 2009

UK Certification Body
CESG, Hubble Road
Cheltenham, GL51 0EX
United Kingdom

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

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement 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 contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

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 and Developer	**Juniper Networks, Inc.**
Product and Version	**Juniper Networks Services Routers and Switches running JUNOS 9.3R1**
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 Part 2	**Conformant**
CC Part 3	**Conformant**
EAL	**EAL3** augmented by ALC_FLR.3
CLEF	**BT**
Date authorised	3 February 2009

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a 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 [d], 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 [e] and CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

Trademarks:

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

TABLE OF CONTENTS

CERTIFICATION STATEMENT 2

TABLE OF CONTENTS 3

I. EXECUTIVE SUMMARY 4

Introduction 4
Evaluated Product and TOE Scope 4
Security Claims 4
Evaluation Conduct 5
Conclusions and Recommendations 5

II. PRODUCT SECURITY GUIDANCE 7

Introduction 7
Delivery 7
Installation and Guidance Documentation 8

III. EVALUATED CONFIGURATION 9

TOE Identification 9
TOE Documentation 9
TOE Scope 9
TOE Configuration 10
Environmental Requirements 11
Test Configuration 11

IV. PRODUCT SECURITY ARCHITECTURE 14

Introduction 14
Product Description and Architecture 14
Design Subsystems 14
Hardware and Firmware Dependencies 17
Product Interfaces 17

V. PRODUCT TESTING 18

IT Product Testing 18
Vulnerability Analysis 19
Platform Issues 19

VI. REFERENCES 20

VII. ABBREVIATIONS 22

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Juniper Networks Services Routers and Switches running JUNOS 9.3R1 to the Sponsor, Juniper Networks, Inc., 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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

   Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1

   It should be noted that the actual release number for the TOE is 9.3R1.7. However as the 'seventh' spin of the 9.3R1 build was the only build released, the two versions are synonymous and can be referred to as JUNOS 9.3R1.

4. The Developer was Juniper Networks, Inc.

5. The Juniper Networks Services Routers and Switches run the same JUNOS software (version 9.3R1) 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.

6. The evaluated subset and 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'.

7. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Security Claims

8. The Security Target [d] fully specifies the TOE's security objectives, the threats that these objectives counter, and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. All of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

9. The TOE security policy is detailed in the Security Target [d].

10. The Security Target [d] states that there are no organisational security policies with which the TOE must comply.

Evaluation Conduct

11. The TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Juniper Networks M/T/J Series of Service Routers running JUNOS 8.1R1, which had previously been certified by the UK IT Security Evaluation and Certification Scheme to CC EAL3 augmented with ALC_FLR.3 [i].

12. In addition, assurance was maintained on two subsequent versions of the software: JUNOS 8.1R3 [j] and JUNOS 8.5R3 [k].

13. For the evaluation of Juniper Networks Services Routers and Switches running JUNOS 9.3R1, the Evaluators addressed every CEM [h] EAL3 work unit, making use of some previous results where appropriate.

14. The Certification Body monitored the evaluation, which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in January 2009, were reported in the ETR [l].

Conclusions and Recommendations

15. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

16. **Prospective consumers of Juniper Networks Services Routers and Switches running JUNOS 9.3R1 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements, and to give due consideration to the recommendations and caveats of this report.

17. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III ‘Evaluated Configuration’.

18. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II ‘Product Security Guidance’ includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

19. The product provides some features that were not within the scope of the evaluation, as identified in Chapter III 'Evaluated Configuration'. **Those features should therefore not be used if the TOE is to comply with its evaluated configuration.**

20. If any changes are proposed to the TOE's functionality, or to components that were examined during the evaluation, such changes should be handled under the Assurance Continuity Scheme. If the change falls outside the scope of Assurance Continuity, a partial or complete re-evaluation of the product should be performed.

21. **Certification is not a guarantee of freedom from security vulnerabilities:** there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued, and, if appropriate, should check with the Vendor to see if any patches exist for the product, and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

22. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

23. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery**.

24. Consumers must download the TOE from the Juniper Networks, Inc., website at www.juniper.net as detailed in the Security Configuration Guide [m]. All administration guidance for the TOE is also on that website. A consumer is required to have a username and password, in order to access the secure area of the site. A username and password is provided to the user when they purchase the TOE.

25. When consumers have downloaded the TOE, they are required to validate the MD5 checksum, which is provided on the www.juniper.net website and in the Security Configuration Guide [m].

26. Although the TOE is the same, regardless of the Router or Switch on which it is installed, there are two different download packages: one for the EX series switch and one for the M, T and MX series routers. This is because by default the M, T and MX series download packages do not include the optional J-Web software. This package (making the installation of the M, T and MX series routers the same as for the EX series switches) should also be downloaded from the www.juniper.net website.

27. Version 9.3R1 of the TOE for the EX series switches is not available for public download. Due to operational reasons, this version of the TOE was never made available to the general public. However the installation package for version 9.3R1 of the TOE on the EX series switches was produced internally within Juniper Networks, Inc., and it is this version that has been evaluated and tested.

28. Although it is not possible to download version 9.3R1 of the TOE for the EX series switches from the www.juniper.net website, the evaluators downloaded it from the Juniper Networks, Inc., internal website, and then installed and configured it in the same way as for the install packages for the M, T and MX series routers. The evaluators also downloaded version 9.3R1 of the TOE for the M, T and MX series routers from the www.juniper.net website and confirmed that the checksum was correct.

29. In addition to the TOE, consumers should download the Security Configuration Guide, Release 9.3 [m] and the following guidance from the www.juniper.net website:

    a. Software Installation and Upgrade Guide, Release 9.3 [n];

    b. System Basics Configuration Guide, Release 9.3 [o];

    c. CLI User Guide, Release 9.3 [p];

    d. Routing Protocols Configuration Guide, Release 9.3 [q];

    e. JUNOS XML API Configuration Reference, Release 9.3 [r];

    f. System Log Messages Reference, Release 9.3 [s].

Installation and Guidance Documentation

30. Guidance is provided in the documents detailed in paragraph 29 above.

31. The Security Configuration Guide [m] describes the procedures that must be followed to install and configure the product in its evaluated configuration, and to operate it securely. It also describes the procedures that must be followed to configure the environment. Hence it is recommended that these procedures are read first.

32. The intended audience of the installation and guidance documents is the administrator.

III. EVALUATED CONFIGURATION

TOE Identification

33. The TOE is identified as:

Juniper Networks Services Routers and Switches running JUNOS 9.3R1

34. The TOE consists of software implementing the Routing Engine, and firmware running on ASICs implementing the Packet Forwarding Engine.

35. The figure below shows the components and scope of the TOE:

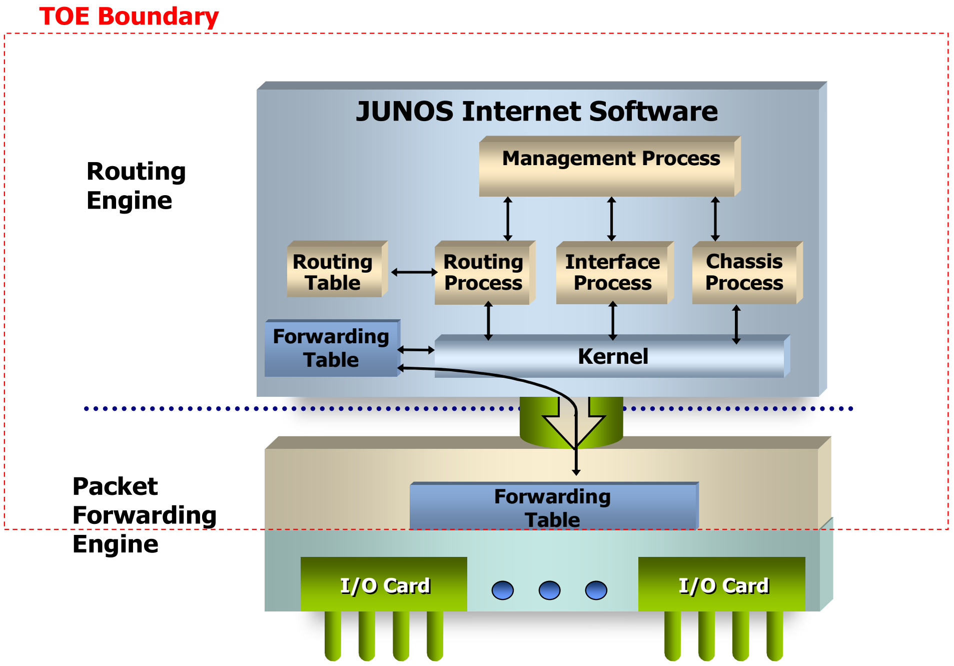

Figure 1: Components and Scope of the TOE

TOE Documentation

36. The relevant guidance documentation for the evaluated configuration is identified in Chapter II ‘Product Security Guidance’.

TOE Scope

37. The TOE is identified above under ‘TOE Identification’.

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

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

    a. all hardware, including that associated with forwarding interfaces PICs, FPCs, Line Cards;

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

    c. encryption and integrity checking functionality;

    d. high availability functionality.

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

    a. use of the auxiliary port;

    b. use of Telnet;

    c. use of SNMP;

    d. use of out-of-band management ports (Management Ethernet Interfaces) on M and T series routers;

    e. packet filtering (other than simple access control to restrict the source address for management traffic);

    f. media use (other than during installation of the TOE).

TOE Configuration

41. The evaluated TOE configuration comprises any of the following Juniper Routers and Switches running JUNOS 9.3R1:

M7i
M10i
M40e
M120
M320

T320
T640
T1600

MX240
MX480
MX960

EX3200
EX4200

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

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

Environmental Requirements

44. The Security Target [d] identifies the threats that are met by the environment, or are met collectively by the TOE and the environment.

45. The Security Target [d] makes physical, personnel and connectivity assumptions as follows:

    a. (A.LOCATE): The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorised physical access.

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

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

    d. (A.TIME): External NTP services will be available.

    e. (A.CRYPTO): In-band management traffic will be protected using SSL and SSH.

Test Configuration

46. The environmental configuration used by the developer and the evaluators to test the TOE is summarised below and in Figure 2 on page 13.

Router 1 not under test (Pom):
Juniper Networks M7i Services router

Router 2 not under test (Chin):
Juniper Networks M7i Services router

Machine running the JUNOScope server:

O/S:	Sun Solaris Sparc edition 5.9
RAM:	4 GB
JUNOScope:	8.2R2.2

Machine running the RADIUS/TACACS+/NTP server:

O/S:	FreeBSD 4.11
RAM:	512 MB

Machine hosting the bthost1 client:

O/S:	FreeBSD 4.11
RAM:	500 MB

Machine hosting the bthost4 client:

O/S:	FreeBSD 4.11
RAM:	500 MB

Machine hosting the bt-winxp client

O/S:	Windows XP Professional SP3
RAM:	2 GB

Test Laptop 1

O/S:	Windows XP Professional SP2
RAM:	767 MB

Test Laptop 2

O/S:	Windows XP Professional SP2
RAM:	1024 MB

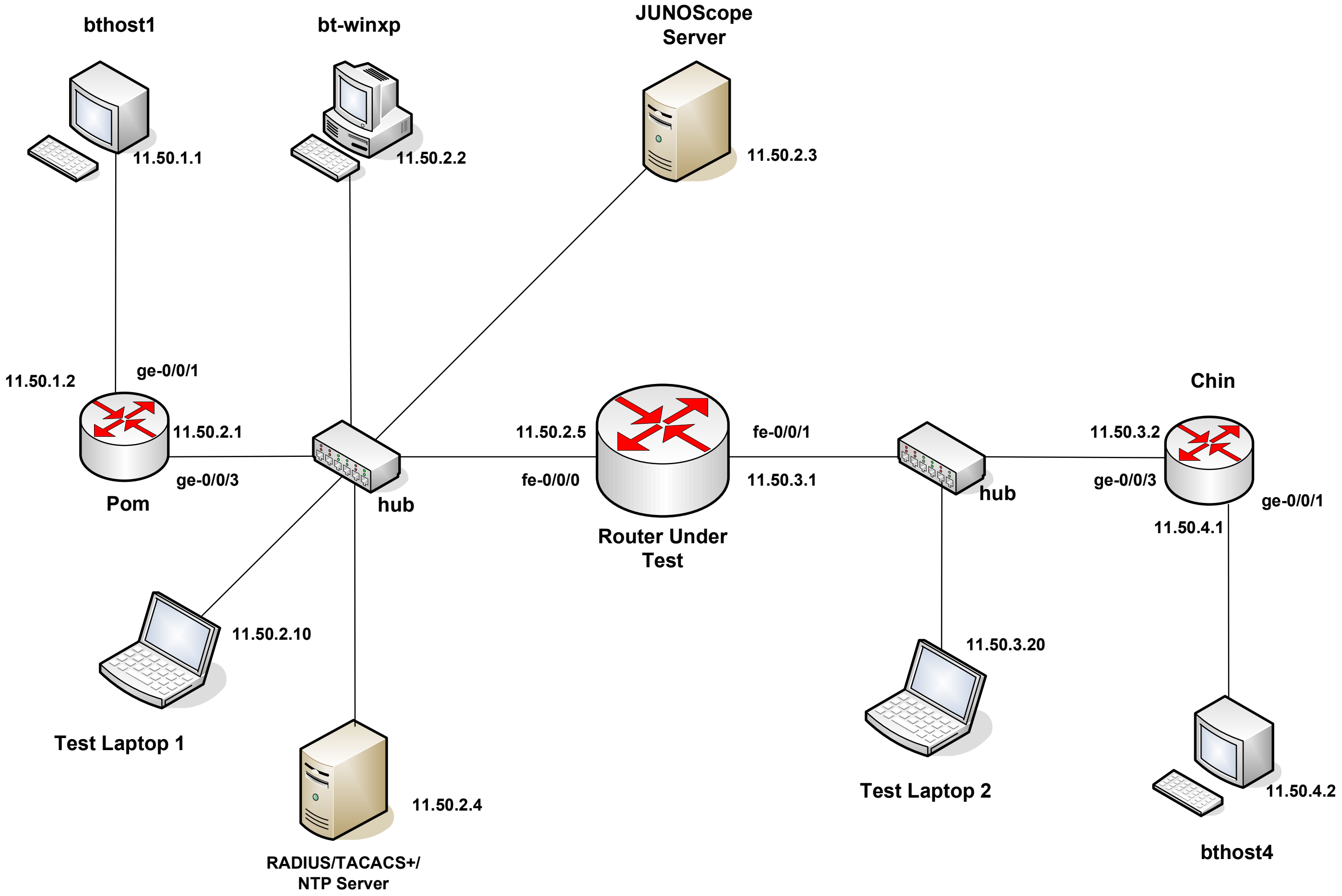

Figure 2: TOE Configuration Tested

IV. PRODUCT SECURITY ARCHITECTURE

Introduction

47. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

48. The product consists of two main architectural features (see Figure 1):

    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.

49. 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).

50. 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.

51. The Routers and Switches can be managed using XML RPCs (JUNOScript), either through J-Web (over HTTPS), JUNOScope (over SSL), or through a Command Line Interface protected by SSH. These interfaces all provide equivalent management functionality, and allow all management and configuration of the router or switch.

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

53. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Design Subsystems

54. The design subsystems of the TOE are:

    a. Chassid. 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. Packet Forwarding Engine (PFE). Through packets (with a presumed destination address different to that of the router) are forwarded by the 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 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 HTTPS, SSH and SSL connections. It then performs a 'listen' system call to tell the JUNOS Kernel that it will accept new connections on these sockets;

h. HTTPD. The HTTPD daemon is started by INETD, and receives J-Web management connections from the JUNOS Kernel;

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

j. Stunnel. Stunnel is started by INETD, and receives SSL JUNOScope management connections from the JUNOS Kernel;

k. 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;

l. Access Daemons. This subsystem consists of three access daemons: Jade, Checklogin and Login. Jade is responsible for managing the authentication of JUNOScript connections over SSL (JUNOScope), Checklogin is responsible for managing the authentication of J-Web connections, and Login handles console connections;

m. EVENTD. The event daemon manages the audit logs and is responsible for generating audit records for all auditable events as detailed in the Security Target [d];

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

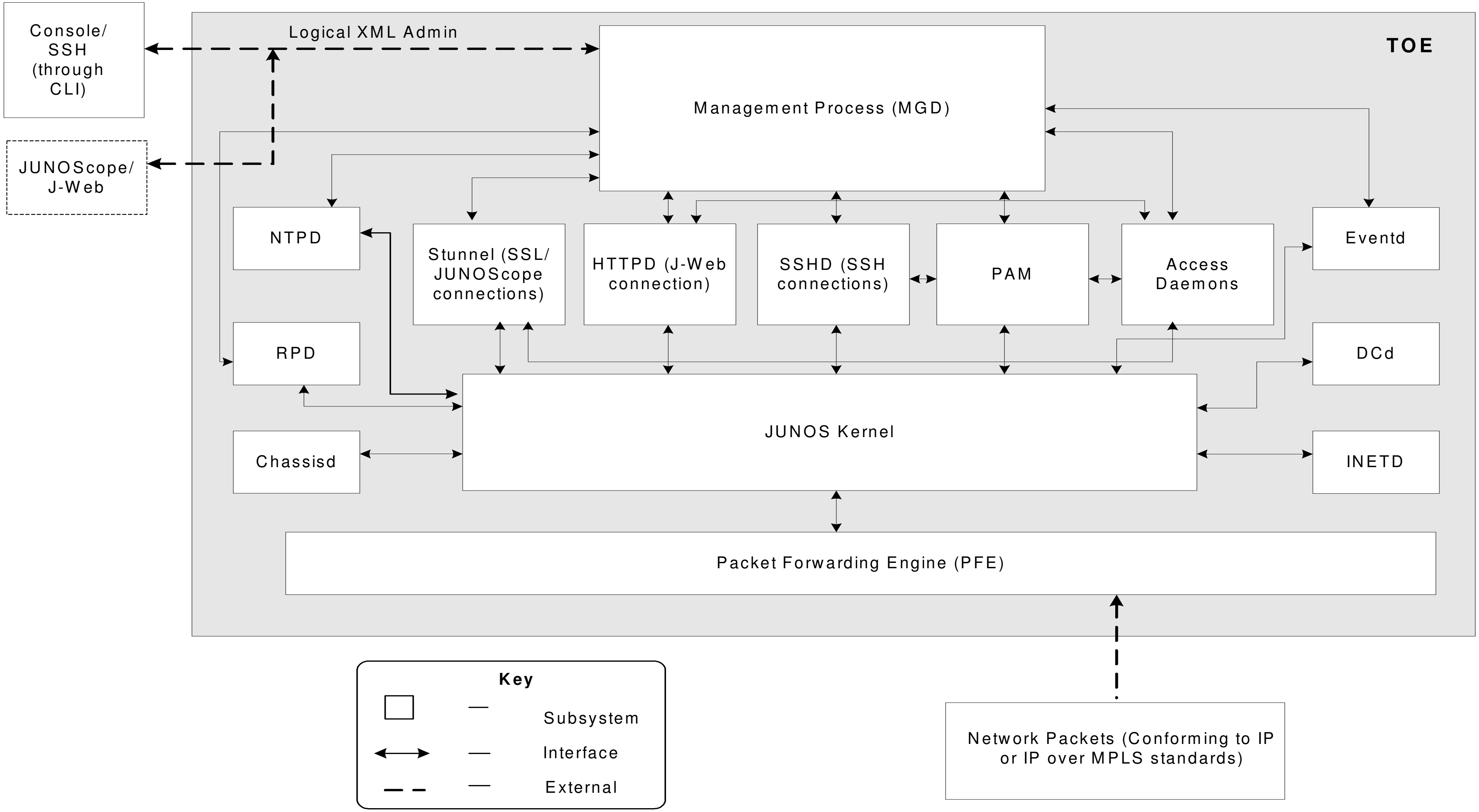

Figure 3: TOE Subsystems

Hardware and Firmware Dependencies

55. The TOE is software and firmware only, it has no hardware components.

56. One function can be provided by the environment – namely the environment should provide an external server (Radius or TACACS+) to support user authentication.

Product Interfaces

57. The external interfaces (i.e. the TOE Security Functions Interface (TSFI)) are:

    a. External traffic interface to the Packet Forwarding Engine: 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 Command Line Interface.

V. PRODUCT TESTING

IT Product Testing

58. During their on-site testing, the evaluators used the Security Configuration Guide [m] to check that the TOE was installed and configured in a secure manner.

59. The environmental configuration used by the evaluators to test the TOE was equivalent to that used by the developers to test the TOE, as summarised in Figure 2.

60. The TOE was tested against the set of external interfaces that comprise the TSFI, as listed above in Chapter IV 'Product Interfaces'.

61. The developer performed tests against all aspects of the TSFI. Those tests also exercised:

    a. all related security functions specified in the Security Target [d];

    b. all subsystems identified in 'Design Subsystems' in Chapter IV.

62. All developer tests were automated and driven through a set of scripts. Other than this, no specialist tools or techniques were used.

63. The evaluators performed the following independent testing:

    a. A sample of the developer's tests was repeated to validate the developer's testing. The sample included developer tests on the M10i, T640, MX960 and EX4200 platforms.

    b. For each functional area, a test was devised that was different from those performed by the developer, wherever possible.

64. The evaluators also devised and performed penetration tests to confirm the non-exploitability of potential vulnerabilities noted during the evaluation, and to confirm the developer's vulnerability analysis.

65. The evaluators used the following tools for the functional and penetration tests:

    - Nmap version 4.6;
    - IRPAS version 1;
    - WireShark version 0.99.4-3;
    - OpenSSL version 0.9.8c-4;
    - Sing version 1.1;
    - Packit version 1.0.

Vulnerability Analysis

66. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation deliverables.

Platform Issues

67. Chapter III 'Evaluated Configuration' lists the hardware platforms that are within the scope of the evaluation.

68. Developer tests were performed on all hardware platforms. The evaluators repeated developer tests on the M10i, T640, MX960 and EX4200 platforms. The evaluators performed all their functional and penetration testing on an EX4200 platform, and performed a sample of the functional and penetration tests on an M10i platform, a T320 platform and an MX240 platform.

69. The evaluators also performed a number of tests on the T320 platform with different types of PICs (Portable Interface Controllers) installed.

70. The range of testing performed by the developer and the evaluators, across the range of platforms and using different PICs, produced exactly the same results, and the evaluators did not identify any parts of the TSF that behaved differently on different hardware platforms.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[d] Security Target for Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1,
Juniper Networks, Inc.,
Version 1.0, 13 January 2009.

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

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2007-09-002, Version 3.1 Revision 2, September 2007.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2007-09-003, Version 3.1 Revision 2, September 2007.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2007-09-004, Version 3.1 Revision 2, September 2007.

[i] Common Criteria Certification Report: Juniper Networks M/T/J Series of Service Routers running JUNOS 8.1R1,
UK IT Security Evaluation and Certification Scheme,
CRP237, Issue 1.0 April 2007.

[j] Common Criteria Maintenance Report MR1 (supplementing Certification Report No. CRP237): Juniper Networks M/T/J Service Routers running JUNOS 8.1R3 covering J2300, J4350, J6350, M7i and M10i,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 2008.

[k] Common Criteria Maintenance Report MR2 (supplementing Certification Report No. CRP237): Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3.
UK IT Security Evaluation and Certification Scheme.
Issue 1.0, September 2008.

[l] Evaluation Technical Report: Juniper Networks Services Routers running JUNOS 9.3R1,
BT CLEF,
LFS/T556/ETR, Version 1.0, 15 January 2009.

[m] Security Configuration Guide for Common Criteria and JUNOS-FIPS,
Juniper Networks, Inc.,
Release 9.3, January 2009.

[n] JUNOS Software – Software Installation and Upgrade Guide,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008-Revision 1

[o] JUNOS Software System Basics Configuration Guide,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008-Revision 1.

[p] JUNOS Software CLI User Guide,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008-Revision 1,

[q] JUNOS Software Routing Protocols Configuration Guide,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008-Revision 1.

[r] JUNOS Software JUNOS XML API Configuration Reference,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008-Revision 1.

[s] JUNOS Software System Log Messages Reference,
Juniper Networks, Inc.,
Release 9.3, 10 October 2008.

VII. ABBREVIATIONS

This list contains only abbreviations that are specific to the TOE. It does not include well-known IT terms (such as GUI, HTML) or standard CC abbreviations (such as TOE, TSF; see CC Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [UKSP00]).

CVS	Concurrent Version System
FIPS	Federal Information Processing Standard
FPC	Flexible PIC Concentrator
INETD	Internet Services Daemon
JUNOS	Juniper Operating System
MGD	Management Daemon
NTPD	Network Time Protocol Daemon
PAM	Portable Authentication Module
PFE	Packet Forwarding Engine
PIC	Portable Interface Controller
RPC	Remote Procedure Call
RPD	Routing Protocol Daemon