122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP238

Juniper Networks JUNOScope IP Service Manager

Version 8.2R2

Issue 1.0

July 2007

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 JUNOScope IP Service Manager 8.2R2**
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	26 July 2007

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

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Juniper Networks JUNOScope IP Service Manager 8.2R2 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 JUNOScope IP Service Manager 8.2R2

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’.

6. It should be noted that the actual release number for the TOE is 8.2R2.4. However, as the ‘fourth’ spin of the 8.2R2 build was the only build released, the two versions are synonymous and are therefore referred to as 8.2R2.

7. Juniper Networks JUNOScope IP Service Manager 8.2R2 provides a web based management interface for the management of IP services for configured devices, such as a Juniper Networks M/T/J Series router. Administrative tasks such as monitoring, configuration and software management of a device can be efficiently performed.

8. An overview of the product and its security architecture can be found in Chapter IV ‘Product Security Architecture’.

Security Claims

9. The Security Target [d] fully specifies the TOE’s security objectives, the threats that those 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.

10. The TOE Security Policy is detailed in the Security Target [d].

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

Strength of Function Claims

12. **The minimum Strength of Function (SoF) was SoF-Medium**. This was claimed for SFR FIA_SOS.1, in respect of the authentication mechanism using passwords. **The Certification Body has determined that this claim was met.**

13. The password must be at least 6 characters in length and contain at least one change of character set (upper, lower, numeric, other).

Evaluation Conduct

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 July 2007, were reported in the Evaluation Technical Report (ETR) [i].

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 JUNOScope IP Service Manager 8.2R2 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' below 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 TOE 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 Juniper Networks' website at www.juniper.net, as detailed in the JUNOScope Software Release Notes [k]. All administration guidance for the TOE is also on the 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. Consumers should also download the JUNOScope Software Release Notes [k] and the following guidance from the www.juniper.net website:

a. JUNOScope Software User Guide [j];

b. JUNOS Internet Software JUNOScript API Guide [l].

26. When consumers have downloaded the TOE they are required to validate the MD5 or SHA1 checksums, which are provided both on the www.juniper.net website and in the JUNOScope Software Release Notes [k].

Installation and Guidance Documentation

27. Guidance is provided in the documents detailed in paragraph 25.

28. The JUNOScope Software Release Notes [k] describe the procedures that must be followed to install and configure the product in its evaluated configuration, and to operate it securely. Those notes also describe the procedures that must be followed to configure the environment. Hence it is recommended that those notes are read first.

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

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is identified as:

Juniper Networks JUNOScope IP Service Manager 8.2R2

31. The TOE consists of software to monitor and manage router operations via a web-based interface, running on the Sun Solaris operating system.

32. Figure 1 below shows the components and scope of the TOE:

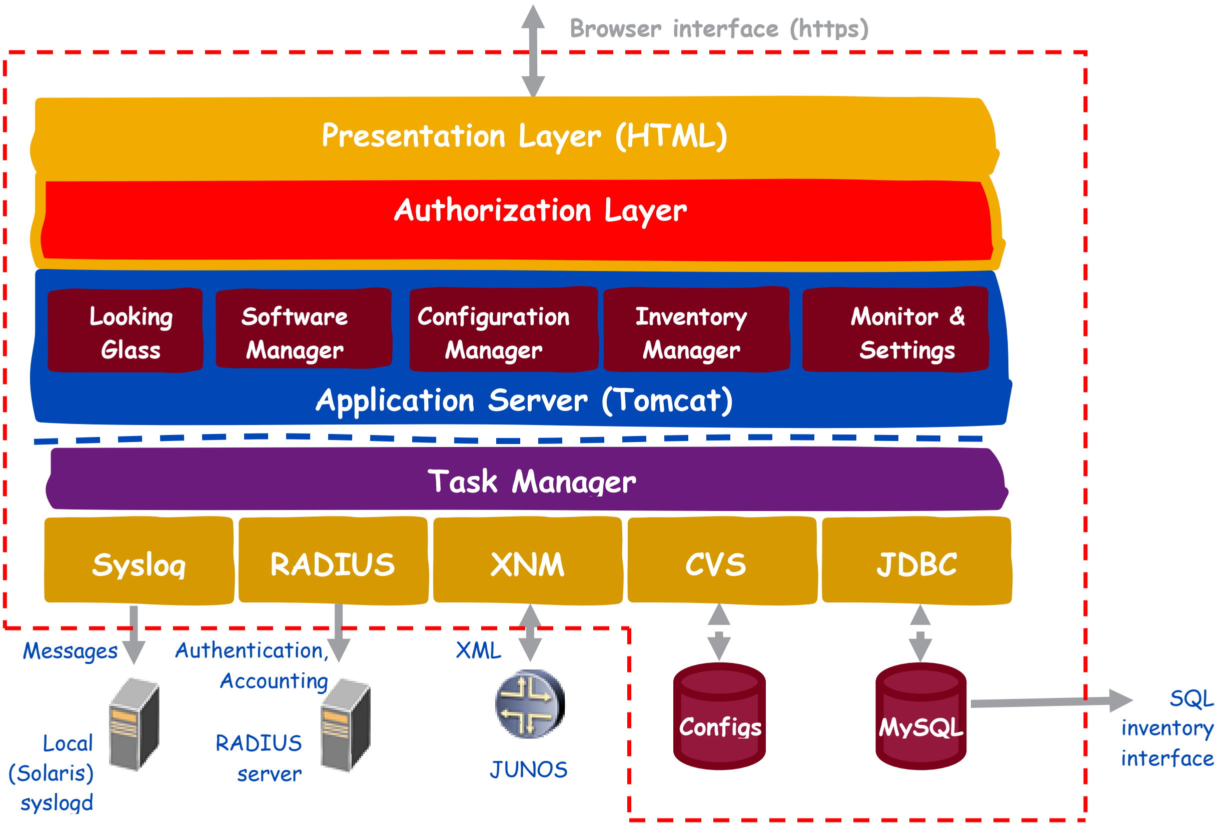

Figure 1: Components and Scope of the TOE

33. The following components, included in Figure 1 above, are non-security supporting subsystems within the TOE that are not involved in the implementation of the SFRs:

- Looking Glass;
- Inventory Manager;
- Task Manager;
- Syslog.

TOE Documentation

34. The relevant guidance documentation for the evaluated configuration is identified in Chapter II 'Product Security Guidance'.

TOE Scope

35. The TOE is identified above under 'TOE Identification'.

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

37. There are no security functionality claims relating to the following item:

- client web browser.

38. The following items are outside the scope of the evaluation:

- use of SSL;
- inventory interface to the MySQL database;
- importing/exporting of MySQL data from/to another JUNOScope server.

TOE Configuration

39. In the evaluated configuration, the TOE runs on Sun Solaris version 9/04 or 10.

40. The underlying operating system is part of the environment.

41. In the evaluated configuration, an external authentication server (e.g. RADIUS) can be used to authenticate administrative connections. Network level diagrams are provided in Figures 1 and 2.

Environmental Requirements

42. The Security Target [d] identifies the objectives that are met by the environment, or are met collectively by the TOE and the environment, as follows:

a. (OE.AUTH): a RADIUS server must be available for external authentication services;

b. (OE.BYPASS): the IT environment for JUNOScope must ensure that the TOE is not bypassed and will provide access control to TOE processes;

c. (OE.BROWSE): the IT environment must secure the communication channel between the browser interface and the TOE;

d. (OE.CRYPTO): SSL must be enabled for all management traffic.

43. 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, willfully 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 RADIUS;

d. (A.THREAT): the threat level in the environment where the TOE will be deployed is considered low;

e. (A.ACCESS): access to data and processes on the Solaris platform underlying the TOE will be restricted to authorised personnel (i.e. JUNOScope Installer);

f. (A.CRYPTO): management traffic will be protected using SSL.

Test Configuration

44. The environmental configuration used by the developer and the evaluators to test the TOE is summarised below and in Figure 2:

Router:
Juniper Networks J2300 router running JUNOS 8.1R1.5

Solaris Machine:

O/S:	Sun Solaris 9/04
RAM:	4 GB
CPU:	1800 MHz
JUNOScope:	8.2R2
Patches:	All Solaris recommended patches as of 16th May 2007
Hard Disk:	73Gb
NIC:	Sun Internal PCI 10/100 Base T Ethernet

RADIUS server:

O/S:	Microsoft Windows XP Professional SP2
RAM:	4 GB
RADIUS:	Funk Software Steel-Belted Radius server, Version 5.3.0

PC:

O/S:	Microsoft Windows XP Professional SP2
Web Browser:	Microsoft Internet Explorer 6
RAM:	1GB

Evaluators' Laptop:

O/S:	Windows XP Professional SP1
RAM:	512 MB
CPU:	590 MHz

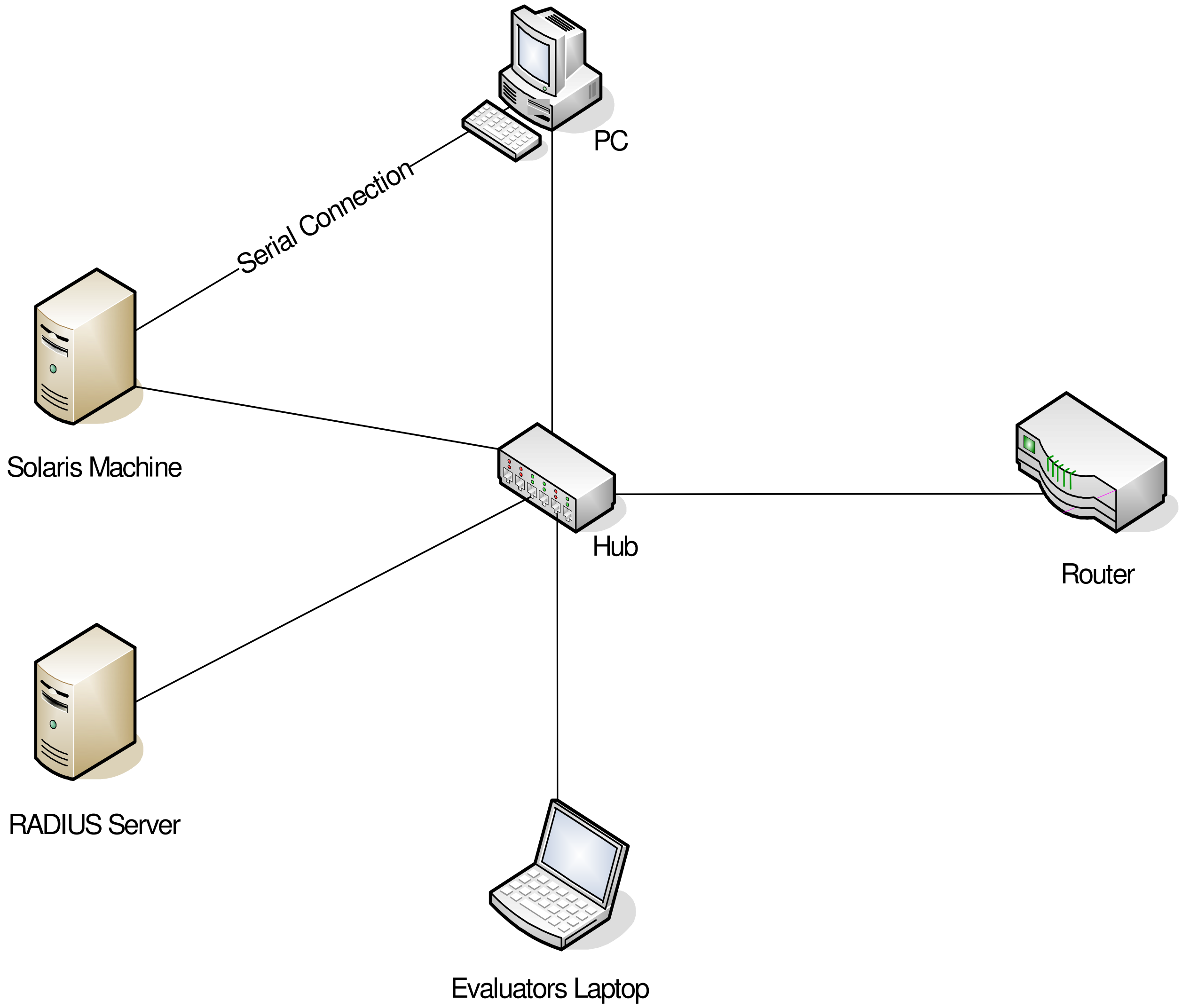

Figure 2 – Test Configuration

IV. PRODUCT SECURITY ARCHITECTURE

Introduction

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

Product Description and Architecture

46. A description of the product is provided in Chapter 2 of the Security Target [d].

47. The main protection mechanisms of the product can be summarised as follows:

a. Identification and Authentication: 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 an external RADIUS authentication server in the environment.

b. Domain Separation: The underlying Solaris operating system provides fundamental operating system protection mechanisms, such as virtual memory protection, to prevent unauthorised interference with the TOE’s processes and data.

c. Access Control Policy: A security attribute based access control policy is applied to all administrative operations within the TOE.

48. The TOE can be managed using XML APIs (JUNOScript), either through HTTP (over SSL) via a web browser, or through a console connection via the Solaris operating system. The console interface only provides the option to install or reconfigure the TOE installation.

49. Auditable events (as defined in the Security Target [d]) are stored in the MySQL database. A reliable timestamp is obtained from the underlying operating system.

50. Figures 1 and 3 of this report detail the logical architecture topology of the TOE.

Design Subsystems

51. The high-level design subsystems of the TOE are as follows, detailed in Figure 3:

a. Presentation Layer: this handles the communication between the client web browser and the Application Server;

b. Authorisation Layer: this authorises all management and operation requests;

c. Application Server: this forwards all authorised operation requests to the relevant subsystem for processing;

d. Configuration Manager: this handles the management of current or archived configuration files held in CVS;

e. Software Manager: this controls the downloading, importing and installation of JUNOS software images across all configured devices;

f. Monitor and Settings: this manages the configuration of administrative and management settings;

g. XNM: this handles communication between JUNOScope and all managed devices;

h. CVS: this controls and handles access requests to the Config DB;

i. Config DB: this provides a storage area for the device configuration files;

j. RADIUS: this handles the RADIUS authentication requests received for the external RADIUS server;

k. JDBC: this handles the read and write operation requests to the MySQL DB;

l. MySQL DB: this stores information relating to devices, groups, authorisation, operations and users in a relational database;

m. JUNOScope Installer: this consists of two scripts that are used for the initial installation of the TOE and for reconfiguring of TOE installation settings.

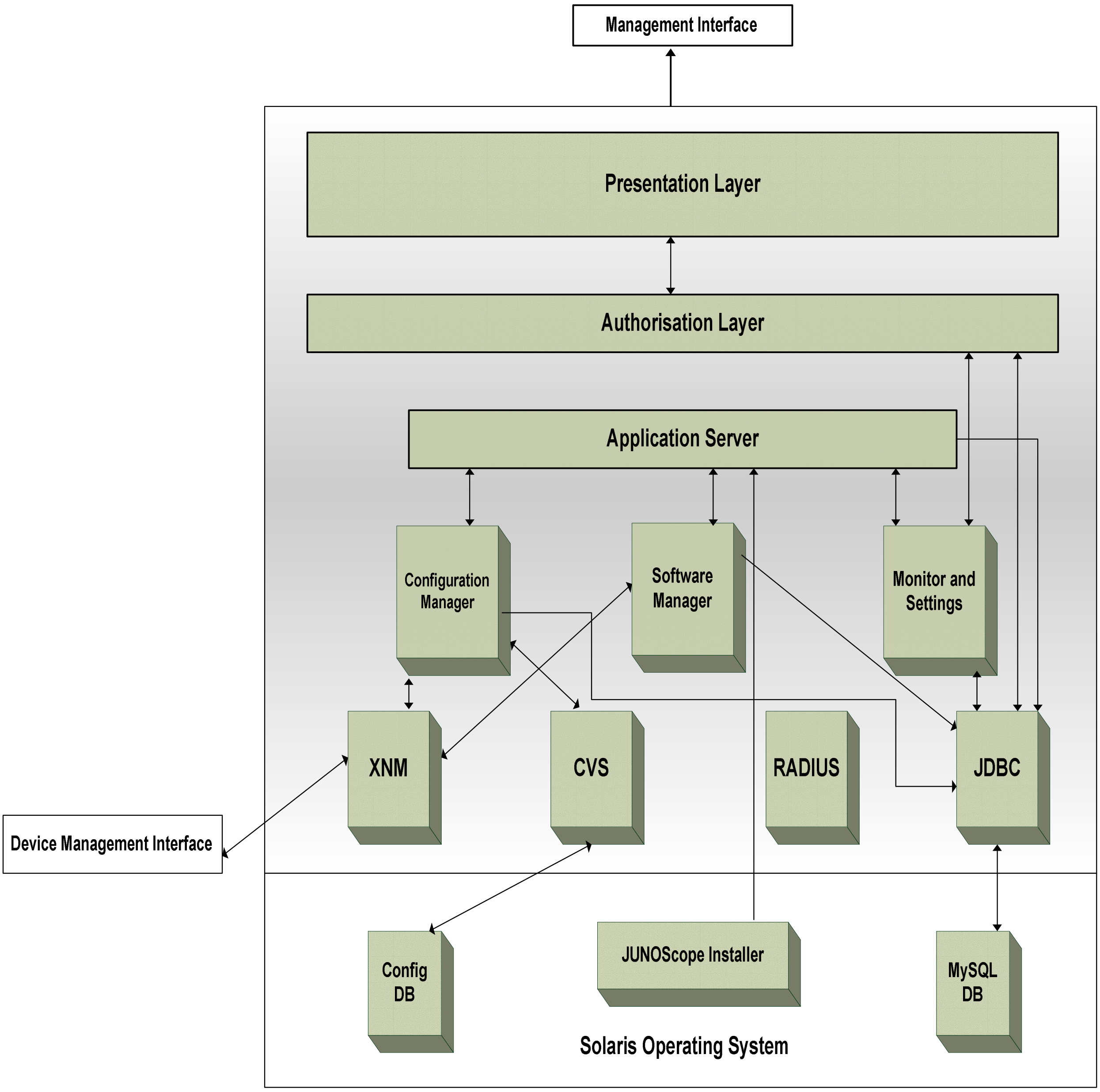

Figure 3 - TOE High-Level Design Subsystems

Hardware and Firmware Dependencies

52. The TOE is software only, it has no hardware components.

53. Three functions can be provided by the environment, namely:

a. The environment should provide an external server (RADIUS), to support user authentication.

b. The environment should provide reliable time stamps for use by the TOE.

c. The environment shall enforce separation between the security domains under the scope of the TOE. A description of how this is provided by the environment is detailed in paragraph 47.b.

Product Interfaces

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

a. Management interface to the TOE: All management traffic to the TOE is received at this interface. This interface is defined by the user commands available to an administrator.

b. Device Management interface to the TOE: This interface is defined by the set of JUNOScript API XML commands sent from the TOE to a configured device.

55. There is also an external interface between the underlying operating system and the TOE. However, as that interface is not security enforcing and is not visible to the administrator, it is not detailed in Paragraph 54 above.

V. PRODUCT TESTING

IT Product Testing

56. During their on-site testing, the evaluators consulted the JUNOScope Software User Guide [j] and the JUNOScope Software Release Notes [k], in order to install and generate a secure configuration, and to start-up the TOE. The evaluators performed these tasks on the TOE running on a Sun Solaris version 9/04 platform.

57. 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 above.

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

59. 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 high-level design subsystems identified in Chapter IV 'Design Subsystems' above.

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

61. 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 25% of the developer's automated tests and 33% of the developer's manual tests.

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

62. The evaluators also devised and performed penetration tests to confirm the non-exploitability of potential vulnerabilities that had been noted during the evaluation, and to confirm the developer's vulnerability analysis and strength of function claim.

63. The evaluators used the following tools in order to perform their functional and penetration tests:

- Tcpreplay, version 1.4.5;
- Ethereal, version 0.9.13;
- OpenSSL, version 0.9.7c.

64. The evaluators' on-site functional and penetration tests were performed at Juniper Networks, Sunnyvale, California, from the 21st May to 24th May 2007.

Vulnerability Analysis

65. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE given by the evaluation deliverables. The evaluators did not identify any vulnerabilities, relating to the TOE, in the public domain sources.

66. The evaluators devised functional and penetration tests to test potential vulnerabilities not fully addressed by the developer testing. The evaluators were satisfied that the TOE is resistant to all identified potential vulnerabilities.

Platform Issues

67. Chapter III 'TOE Configuration' above 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 Sun Solaris version 10 and 9/04 platforms. The evaluators performed all of their functional and penetration testing on a Sun Solaris version 9/04 platform.

69. The range of testing performed both by the developer and by the evaluators produced exactly the same results, across the two platforms, 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 Operation,
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 JUNOScope IP Service Manager 8.2R2,
Juniper Networks, Inc.,
Version 1.1, July 2007.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[i] Evaluation Technical Report for
Juniper Networks JUNOScope IP Service Manager 8.2R2,
BT CLEF,
LFS/T523/ETR, Version 1.0, June 2007.

[j] JUNOS Internet Software JUNOScope Software User Guide, Release 8.2,
Juniper Networks, Inc.,
12 January 2007.

[k] JUNOScope 8.2 Software Release Notes (Common Criteria Certified),
Juniper Networks, Inc.,
25 May 2007.

[l] JUNOS Internet Software JUNOScript API Guide, JUNOS Release 8.2,
Juniper Networks, Inc.,
January 2007.

VII. ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, HTML, ... and standard Common Criteria abbreviations such as TOE, TSF, ... (see Common Criteria Part 1 [e]):

CVS	Concurrent Versions System
DB	Database
JDBC	Java Database Connectivity
XNM	XML-based Network Management