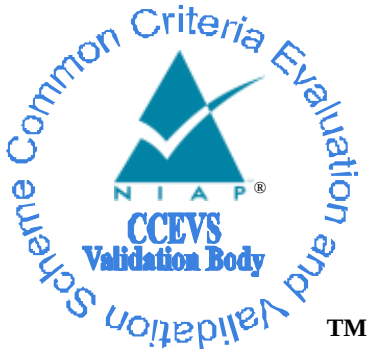
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2 R2S4

Report Number: CCEVS-VR-VID10402-2013
Dated: 22 April 2013
Version: 0.3

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

The Aerospace Corporation
Columbia, MD

Ken Stutterheim

The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, both running Junos 11.2 R2S4, was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in March 2013. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, Revision 3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The evaluation team determined that the products comprising the Target of Evaluation (TOE) satisfy conformance claims of Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL4, augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Security Target, the Evaluation Technical Report (ETR) and associated test reports produced during the evaluation. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The TOE comprises the following two router appliances, both running Junos 11.2S4:

- LN1000-V Mobile Secure Router—intended for deployment within defense communities and public sector safety organizations, such as first responders
- SRX650 Services Gateway—intended for deployment at remote and branch locations in the network to provide all-in-one secure WAN connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching.

Network packets that enter and exit the devices are processed in accordance with the settings of packet filters, security policies, and pre-configured filters for common attacks (also known as "screens"). For example, the software can determine:

- Whether the packet is allowed into the device
- Which firewall screens to apply to the packet
- The route the packet takes to reach its destination
- Whether to apply Network Address Translation (NAT) to translate the packet's IP address
- Whether the packet requires an Application Layer Gateway (ALG).

Packets undergo both flow-based and packet-based processing:

- Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that were established for the first packet of the packet stream, which is referred to as a flow. This is also known as "stateful packet processing".
- Packet-based, or stateless, packet processing treats packets discretely. Each packet is assessed individually for treatment.

Interfaces provide the physical means for packets to enter and exit the device. Many interfaces can share exactly the same security requirements, but different interfaces can also have different

security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together into a single security zone.

Security zones are the building blocks for policies; they are logical entities to which one or more interfaces are bound. Security zones provide a means of distinguishing groups of hosts (user systems and other hosts, such as servers) and their resources from one another in order to apply different security measures to them.

Security zones have the following properties:

- Interfaces—a list of interfaces in the zone.
- Policies—active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.
- Screens—a Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, and the management zone, a set of predefined screen options can be enabled that detect and block various kinds of traffic that the device determines as potentially harmful.
- Address Books—an administrator defined rule-set containing the IP address or domain names of hosts and subnets whose traffic is either permitted, denied, encrypted, or user-authenticated. An address book is a management object that assists the administrator manage the IP addresses for the firewall ruleset. It does not play a direct role in the enforcement of the information flow policy.

Junos screen options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone. Junos then applies firewall policies, which can contain content filtering and IDS components, to the traffic that passes the screen filters.

The Junos IDS system selectively enforces various attack detection and prevention techniques on network traffic traversing the secure routers. It enables the definition of policy rules to match traffic based on a zone, network, and application, and then take active or passive preventive actions on that traffic.

The signature database is stored on the device and contains definitions of predefined attack objects and groups. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic. In response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper web site.

The TOE supports IPsec to provide confidentiality and integrity services for network traffic transmitted between TOE devices and for traffic transmitted from a TOE device to an external IT system (e.g., a peer router). The TOE does not provide support for general-purpose VPN clients to connect to the TOE.

The routers, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4 Security Target.

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, both running Junos 11.2S4
Sponsor:	Juniper Networks 1194 North Mathilda Ave. Sunnyvale, CA 94089-1206
Developer:	Juniper Networks 1194 North Mathilda Ave. Sunnyvale, CA 94089-1206
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	January 22, 2010
Completion Date:	March 4, 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1 Revision 3, July 2009.
Evaluation Class:	EAL4, augmented with ALC_FLR.2
Description:	The Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, both running Junos 11.2S4, primarily support the definition and enforcement of information flow policies among network nodes, using stateful inspection.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, both running Junos 11.2S4, by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Dawn Campbell Katie Sykes

Validation Body: National Information Assurance Partnership CCEVS

Validation Personnel: Jim Donndelinger, The Aerospace Corporation
Kenneth Stutterheim, The Aerospace Corporation

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE is intended to counter.

T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
T.ADMIN_ROGUE	An administrator's intentions may become malicious resulting in user or TSF data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.CRYPTO_COMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE.
T.MALICIOUS_TSF_COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
T.REPLAY	A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).

T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.RESOURCE_EXHAUSTION	A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
T.SPOOFING	An entity may misrepresent itself as the TOE to obtain authentication data.
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTHORIZED_PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.UNIDENTIFIED_ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNIDENTIFIED_INTRUSIONS	The IDS Administrator may fail to notice potential intrusions, thus limiting the IDS Administrator's ability to identify and take action against a possible intrusion.
T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

2 Identification

The evaluated product is **Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4**.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

3.1 Security Audit

Security audit events related to router and firewall functionality are stored in a circular in-memory buffer—the requirements for auditing are met by local in-memory storage. IDS events are similarly stored in a separate in-memory IDS event trail. The TOE provides the capability of analyzing potential intrusions via signature analysis, which uses patterns corresponding to known attacks, and by detecting protocol anomalies. The TOE implements two roles related to the security audit function: the Audit Administrator; and the IDS Audit Administrator. The audit log can be viewed by all administrators, but the IDS audit log can be viewed only by the IDS Administrator. Search and sort facilities are provided. In conjunction with the audit capabilities, the TOE provides an alarm mechanism that provides immediate notification of potential security violations and potential intrusions.

3.2 Cryptographic Support

The TOE devices constitute cryptographic modules that satisfy the requirements of FIPS 140-2 Security Level 2. The cryptographic module provides confidentiality, integrity, and authentication services in support of the following cryptographic protocols: Secure Shell (SSH), used for remote administrator access to the appliance; and IPsec/IKE, used for secure communications between the appliance and external peer routers.

3.3 User Data Protection

The TOE is designed to forward network packets from source network entities to destination network entities based on available routing information. This information is either provided directly by administrators or indirectly from other network entities (outside the TOE) configured by the administrators. The TOE has the capability to regulate the information flow across its interfaces—traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number).

3.4 Identification and Authentication

The TOE provides an authentication mechanism for administrative users through an internal authentication database. Administrative login is supported through the locally connected console, when enabled, or remotely via an SSH protected communication channel.

A known administrator user id and its corresponding authentication data must be entered correctly in order for the administrator to successfully logon and thereafter gain access to administrative functions. For local authentication, all administrator user name and password pairs are managed in a database internal to the TOE. Excessive failed login attempts while initiating a remote administration session can cause the session being created to be closed.

3.5 Security Management

The TOE supports four separate and distinct administrative roles: Audit Administrator; Cryptographic Administrator; IDS Administrator; and Security Administrator. When configured in accordance with the supplied guidance documentation, the TOE ensures administrators are restricted to performing functions allowed by their assigned role.

The TOE provides a command line administrative interface and supports remote administration through an SSH command line interface. To execute the CLI, the administrator can establish a trusted SSH connection to the TOE and utilize the CLI offered through the SSH connection. Regardless of the interface, the authorized administrator must be successfully identified and authenticated before they are permitted to perform any security management functions on the TOE.

3.6 Protection of the TSF

The TOE is a hardware and firmware device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. Junos is a special purpose OS that provides no general purpose programming capability. The TOE also preserves its configuration for trusted recovery in the event that the configuration has been modified and not saved or if the TOE has been ungracefully shutdown.

The TOE provides a recovery and self testing mechanism. The recovery mechanism allows administrators to return the TOE to a secure state, while the self test mechanism allows administrators to verify the integrity of the TOE and its cryptographic functions.

3.7 Resource Utilization

The TOE provides features to protect itself from Denial of Service attacks. These features limit TCP connections and offer administrators the ability to limit the number of resources a particular address or set of addresses can use over a specified time period.

3.8 TOE Access

The TOE provides the ability to restrict the establishment of an administrative session based on a schedule or based upon the originating source IP address (or subnet). The TOE also provides inactivity timeouts and logon banners that can be configured by administrators.

3.9 Trusted Path/Channels

The TOE creates trusted channels between itself and remote trusted authorized IT product entities that protect the confidentiality and integrity of communications. The TOE creates trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications.

4 Assumptions

The following assumptions are identified in the ST:

A.NO_GENERAL_PURPOSE	The administrator ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL4 augmented with ALC_FLR.2).
- This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
- The TOE boundary does not include the LN1000-V Rear Transition Module (RTM) or the SRX650 Services and Routing Engine (SRE) module.
- The following product capabilities are excluded from use in the evaluated configuration:
    - Use of telnet, since it violates the Trusted Path requirement
    - Use of FTP, since it violates the Trusted Path requirement
    - Use of SNMP, since it violates the Trusted Path requirement

- Management via J-Web, since it violates the Trusted Path requirement
- Media use (other than during installation of the TOE)
- External authentication via RADIUS or TACACS+ authentication servers.

5 Architectural Information

The TOE hardware is manufactured to Juniper's specifications by sub-contracted manufacturing facilities. Juniper's custom operating system, Junos 11.2S4, runs in firmware. The hardware devices provide no extended permanent storage such as disk drives. Audit information is stored in memory. The main components of the appliances are the processor, ASIC, memory, interfaces, and surrounding chassis and components. The differences between the appliances are the types of processor, traffic interfaces, management interfaces, number of power supplies, and type of ASIC.

The LN1000 is an embedded router that operates identically in both wire-line and wireless environments and with communication nodes that are either mobile or stationary. The LN1000 is a single hardware card designed to operate in a VITA 46.0 chassis (the chassis is part of the operational environment). The card conforms to the VITA 46.0 IEEE 1101.2 specifications and is a 3U compact node slot interface. A single slot VITA 46 card is approximately 3"x 6". It supports eight Gigabit Ethernet ports.

The physical boundary of the SRX650 is the physical device. It features four fixed 10/100/1000 Ethernet LAN ports and eight Gigabit Ethernet-backplane Physical Interface Module (GPIM) slots. The exterior dimensions are 17.5 x 3.5 x 18.2 in (44.4 x 8.8 x 46.2 cm); it weighs 24.9 lbs (11.3 kg). The device has 2 GB DRAM, 2 GB compact flash, and an external compact flash slot for additional storage.

Junos firmware powers the entire system. At its core is the Junos kernel, which is based on FreeBSD and provides an integrated platform for its functions, including:

- Routing
- Firewalling
- Intrusion detection.

Junos does not support a programming environment.

The TOE design decomposes Junos into 7 subsystems, each of which is further decomposed into one or more related modules. Each subsystem is responsible for a specific area of TOE security functionality, as follows:

- Kernel—implements kernel services to support the operation of the other subsystems, such as task management, inter-process communication, and interrupt handling
- Initialization—responsible for bringing the TOE up from the initial power-on state to full operation
- Cryptography—implements all of the FIPS 140-2 approved cryptographic algorithms to support SSH and IPsec
- Authentication—responsible for authentication of users attempting to gain access to the TOE, including enforcement of restrictions on when and from where administrative sessions can be established

- Security Management—implements the administrative interface to the TOE (the Command Line Interface) and enforces role-based restrictions on access to specific commands
- Audit—responsible for the configuration and operation of the audit security function, generating audit events and traffic and self logs on behalf of all other subsystems
- Flow Control—processes all network packets arriving on the TOE's network interfaces, whether addressed to the TOE or intended to traverse the TOE, thus implementing the TOE's firewall capabilities, including detection of attempted network-based attacks.

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

- Juniper Networks Junos OS Common Criteria Configuration Guide for LN1000 Mobile Secure Routers and SRX650 Services Gateways, Release 11.2 R2, 11 December 2012
- Juniper Networks Junos OS CLI Reference, Release 11.2, 4 August 2011
- Juniper Networks Junos OS System Basics Configuration Guide, Release 11.2, 17 May 2011
- Juniper Networks Junos OS Software Installation and Upgrade Guide, Release 11.2, 17 May 2011
- Juniper Networks Junos OS Security Configuration Guide, Release 11.2, 13 May 2011
- Juniper Networks LN1000-V Mobile Secure Router Hardware Guide, 20 Jul 2010
- Juniper Networks SRX650 Services Gateway Hardware Guide, 1 Dec 2010.

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4.

Evaluation team testing was conducted at the vendor's development site in February 2012.

7.1 Developer Testing

The vendor's approach to testing for the Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4 is based on testing the claimed security functions of the TOE as represented by the SFRs specified in the ST. The vendor has developed a test suite comprising various automated tests designed to demonstrate that the TSF satisfies the SFRs specified in the ST.

The vendor addressed test depth by mapping SFRs to specific subsystems and modules and by simultaneously mapping SFRs to specific test cases. The vendor's tests are focused on demonstrating the satisfaction of specific SFRs, but the vendor also analyzed the functionalities addressed in the TOE design and also mapped test cases that address those functionalities.

The vendor ran the entire test suite on all TOE models on the test configuration described in the test documentation and gave the evaluation team the actual results. The evaluation team verified the results demonstrated all vendor tests had passed.

The evaluation team noted the vendor's test suite is comprehensive, including positive and negative test cases and a significant number of vulnerability tests.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite for the TOE per the evaluated configuration as described in the vendor's test documentation ("Juniper Networks, Inc. Junos 11.2 Common Criteria MRPP ATE Test Plan Volume 1-Introduction and Overview"), using the vendor's test infrastructure.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results. Both of the appliances covered by the evaluation were included in evaluation team testing.

The evaluation team performed additional functional tests covering the following aspects of the TSF:

- Confirmation alarms are displayed on the console as specified in the ST
- Confirmation that, when configured, audible alarms on the console sound until acknowledged by an administrator
- Confirmation of the TOE's behavior when the audit trail storage is exhausted
- Validation of ST statement regarding auditing of failed authentication attempts
- Application Layer Gateway mechanism
- Behavior of TOE in processing firewall rules
- Allowed and excluded user types
- Authentication failure handling
- Authentication failure threshold
- Login process and throttling
- Password constraints enforcement
- Administrative role revocation
- Security management functions
- TOE access banners.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE, identifying six vulnerabilities reported against earlier versions of Junos. The evaluation team determined, through analysis of vulnerability descriptions and consideration of the method of use of the TOE that one of these reported vulnerabilities is not relevant to the TOE in its evaluated configuration — it relates to the Web user interface, which is not permitted in the evaluated configuration. The evaluators confirmed, through examination of the vendor's CM records, that the other

vulnerabilities have had fixes developed and applied to Junos and do not exist in the evaluated version of the TOE.

In addition to the open source search, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities.

8 Evaluated Configuration

The evaluated version of the TOE is Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4.

9 Results of the Evaluation

The evaluation was conducted based upon Version 3.1, Revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that a certificate rating of EAL4 augmented with ALC_FLR.2 be issued for Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures

Assurance Component ID	Assurance Component Name
ALC_FLR.2	Flaw reporting procedures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

10 Validator Comments/Recommendations

The following items are excluded from use in the evaluated configuration:

- Telnet
- SSL
- FTP
- SNMP
- Management via J-Web
- Media use (other than during installation of the TOE)
- Use of the LN1000-V RTM or SRX650 SRE
- RADIUS and TACACS+ external authentication servers
- Use of syslog

In the evaluated configuration, the CLI provides the only mechanism for TOE management; access to the Unix shell is prohibited.
Please note that the TOE is not IPv6 aware.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4**, Version 3.2, dated 11 January 2013.

13 Glossary

Please consult the CC and CEM for definitions of abbreviations and terms used within this document.

14 Bibliography

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/testing-accreditation/common-criteria.html/)
- Juniper Networks, Inc. (http://www.juniper.net)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 3.1, Revision 3, July 2009
- *Common Evaluation Methodology for Information Technology Security*, version 3.1, Revision 3, July 209.

Other Documents:

- *Juniper Networks LN1000-V Mobile Secure Router and SRX650 Services Gateway, Running Junos 11.2S4*, Version 3.2, 11 January 2013.