National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks

J-Series Family of Service Routers running JUNOS 7.3R2.14

Report Number: CCEVS-VR-06-0019
Dated: 20 April 2006
Version: 1.0

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Victoria A. Ashby
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 31 March 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2, Revision 256, January 2004, and the Common Methodology for IT Security Evaluation (CEM), Version 2.2, Revision 256, January 2004.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). The TOE, which is the J-Series Family of Service Routers running JUNOS 7.3R2.14, The TOE is a services router providing a wide variety of services to the user. The J-Series Family routes IP traffic over any type of network, with increasing scalability of the traffic volume with each router model. All packets on the monitored network are scanned by the J-Series Family router and then compared against a set of rules to determine where the traffic should be routed, and then the J-Series Family router passes it to the appropriate destination.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC. The TOE is a combination hardware and software TOE consisting of Juniper Networks IP routers models J2300, J4300, and J6300, all running JUNOS 7.3R2.14. The TOE comprises of two separate functions: the Routing Function and Packet forwarding Function that make up the router platform itself. Pluggable Interface Modules (PIMs) are the physical network interfaces that allow the TOE to be customized to the intended environment and they are part of the Packet Forwarding Engine. The J4300 and J6300 models use a common set of PIMs whereas the physical network interface modules are in-built as part of the J2300 model of routers. This Validation Report applies only to the specific version of the TOE as evaluated.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the J-Series Family of Service Routers running JUNOS 7.3R2.14 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, discussed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the

validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.2, Version 256, January 2004. All interpretations after this time until the time that the evaluation started in May 2005 were applied during the evaluation.

1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data, inappropriately changing the configuration data for TOE security functions.
- An unauthorized process or application may gain access to the TOE security functions and data, inappropriately changing the configuration data for the TOE security functions.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14
Protection Profile	Not applicable.
ST:	Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target, Version 1.0, 3 April 2006
Evaluation Technical Report	*Evaluation Technical Report for* Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Part 1 (Non-Proprietary) *,* Version 3.0, 20

Item	Identifier
	April, 2006
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Juniper Networks
Developer	Juniper Networks
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Vicky Ashby, The MITRE Corporation

3 Security Policy

The TOE logically supports the following security functions at its interfaces: User Data Protection, Identification and Authentication, Security Management, and Protection of Security Functions. Each is discussed in more detail as follows:

- **User Data Protection**

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

- **Identification and Authentication**

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides the ability to define levels of authority for users, providing administrative flexibility. Full administrators have the ability to define groups and their authority and they have complete control over the TOE.

The TOE also requires that applications exchanging information with the TOE successfully authenticate prior to any exchange. This covers all services used to exchange information, including telnet, ssh, ssl, and ftp.

Authentication services can be handled either internally (fixed passwords) or through an authentication server in the IT environment, such as a RADIUS or TACACS+ server (the external authentication server is considered outside the scope of the TOE). Public Key Authentication such as RSA can be used for the validation of the user credentials, but the user identity and privileges are still handled internally.

- **Security Management**

The TOE is managed through a Command Line Interface (CLI), or optionally using XML (Junoscript) or HTTPS (J-Web) interfaces which provide equivalent management functionality. Through these interfaces all management can be performed, including user management and the configuration of the router functions. The CLI interface is accessible through ssh and telnet sessions, as well as a local terminal console.

- **Protection of Security Functions**

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of routes. Another protection mechanism is that all functions of the TOE are confined to the device itself. The TOE is completely self-contained, and therefore maintains its own execution domain.

4 Assumptions

The following assumptions are identified in the Security Target:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The authorized administrators are competent, not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- External authentication services will be available via either RADIUS, TACACS+, or both.

5 Architectural Information

The TOE platforms are designed to be efficient and effective IP router solutions. The TOE comprises of two separate functions: the Routing Function and Packet forwarding Function that make up the router platform itself. Pluggable Interface Modules (PIMs) are the

physical network interfaces that allow the TOE to be customized to the intended environment and they are part of the Packet Forwarding Engine. The J4300 and J6300 models use a common set of PIMs whereas the physical network interface modules are in-built, part of the J2300 model of routers. The TOE platforms are designed as hardware devices, which perform all routing functions internally to the device. All TOE platforms are powered by JUNOS software, which provides both management functions as well as all IP routing functions.

The TOE supports numerous routing standards, allowing it to be flexible as well as scalable. These functions can all be managed through the JUNOS software, either from a connected terminal console or via a network connection. Network management can be secured using ssl, SNMP v3, and ssh protocols. All management, whether from an administrator directly connecting from a terminal to the router, or connecting from the network, requires successful authentication.

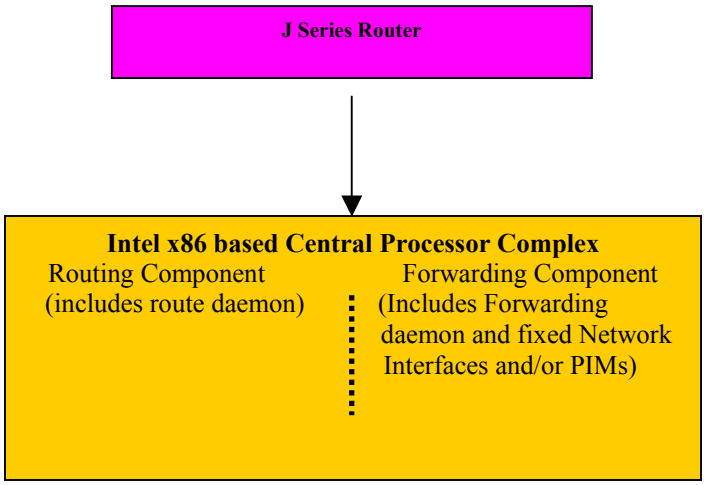

Figure 1 – Juniper Networks J-Series Family of Service Routers running JUNOS 7.3

6 Documentation

Design Documentation

Document	Version	Date
Juniper Networks J-Series Services Routers High Level	Revision 2.1	8 February 2006
Authentication and Authorization Functional Specification	v1.11	January 2006
Representation Correspondence embedded in the High Level Design, referenced above		

Guidance Documentation

Document	Version	Date
J-series Services Router Getting Started Guide, Release 7.3 http://www.juniper.net/techpubs/software/jseries/junos73/jseries73-getting-started/jseries73-getting-started.pdf	Revision 2	See web site
J-series Services Router Configuration Guide, Release 7.3 http://www.juniper.net/techpubs/software/jseries/junos73/jseries73-config-guide/jseries73-config-guide.pdf	Revision 2	See web site
J-series Services Router Administration Guide, Release 7.3 http://www.juniper.net/techpubs/software/jseries/junos73/jseries73-admin-guide/jseries73-admin-guide.pdf	Revision 2	See web site

Configuration Management Documentation

Document	Version	Date
JUNOS Software Configuration Management Plan	Revision 0.4	August 2, 2005
Product Revision Policy Document Control	Revision 01	

Delivery and Operation Documentation

Document	Version	Date
Juniper Networks Standard Delivery Procedures	Revision 0.2	June 10, 2003
J-series Services Router Getting Started Guide, Release 7.3	Revision 2	See web site

Document	Version	Date
http://www.juniper.net/techpubs/software/jseries/junos73/jseries73-getting-started/jseries73-getting-started.pdf		
J-series Services Router Configuration Guide, Release 7.3 http://www.juniper.net/techpubs/software/jseries/junos73/jseries73-config-guide/jseries73-config-guide.pdf	Revision 2	See web site

Test Documentation

Document	Version	Date
System Test Plan	Revision 1.15	16 March 2006
Log files for the various test cases and [TOE] models		Various

Vulnerability Assessment Documentation

Document	Version	Date
Juniper J-Series Family of Service Routers Vulnerability Analysis	Revision 0.1	25 January 2006
Strength of Function is embedded in the ST		

Security Target

Document	Version	Date
Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target	1.0	3 April 2006

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

Juniper's approach to security testing for the TOE is security functional requirement based. Essentially, Juniper developed a set of test cases that correspond to a security functional requirement. Each test case is subdivided into security functions and each test procedure targets the specific security behavior associated with that security function. Each test case was checked and it was determined that the test case supported the security function to which it was mapped. The test procedures are designed to be exercised manually using the subsystem interfaces, although the developer has automated scripts that have been designed to exercise the same test cases.

Prior to independent testing, the evaluation team analyzed the vendor test procedures to ensure adequate coverage. At EAL 2 it is not required to test all functionality, though the Vendor did update the Test Plan to include test cases to test the enforcement of the information flow policies. In addition, the Evaluation Team devised test cases to supplement the Vendor test cases and to ensure complete test coverage.

The evaluation team examined the vendor's actual test results for the TOE configuration for all three (J2300, J4300, and J6300) router models.

7.2 Evaluation Team Independent Testing

The vendor provided two TOE configurations at its site for installation and testing. The test lab included the RADIUS and TACACS+ servers identified as needed in the IT environment. The Evaluation Test Team examined the J6300 router but ran tests only on the J2300 and J4300 routers. The Evaluation Team installed the TOEs on these two router models using the vendor's installation documentation. While installing each TOE configuration, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration. SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The Evaluation Team chose to run a subset of the tests that the developer performed for the J2300 and J4300 TOE configurations. This ensured that the Evaluation Team adequately addressed all security functions. The Evaluation Team chose to use telnet to connect to each router, instead of using a direct connection to the TOE. This provided a more realistic configuration for the testing. The Evaluation Team was able to configure different interfaces as part of the testing.

The vendor provided a complete set of expected and actual test results for analysis. The actual results received by the Evaluation Team exercising the Vendor's test suite, matched the vendor's expected and actual results.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, to identify penetration test cases. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests. These tests concentrated on using malformed packets to attempt to shut down the router. No malformed packets were discovered that affected the router availability.

8 Evaluated Configuration

The TOE for this evaluation is completely self contained, and consists of hardware and software. The evaluated configurations for this TOE consist of one of the following three sets of hardware:

- Juniper J2300
- Juniper J4300
- Juniper J6300

In addition, the software consists of only the JUNOS 7.3R2.14 operating system.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component and the ALC_FLR.2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

"The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of entire set of the vendor's test suites, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST."

The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for* Juniper Networks J-Series Family of Service Routers running JUNOS *7.3R2.14, Part 2,* which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

"The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:

- *J-series™ Services Router Getting Started Guide, Release 7.3 and J-series™ Services Router Configuration Guide, Release 7.3*

The Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 TOE (see product identification below) satisfies the Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target, Version 1.0, 3 April 2006."

The validation team followed the procedures outlined in the *Common Criteria Evaluation and Validation Scheme (CCEVS) Publication # 3* for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

10 Validator Comments/Recommendations

The security functions claimed in the ST for the TOE do not include audit. Although the product provides extensive logging capabilities, the audit or logging capabilities were not claimed or tested as part of this evaluation.

Administrators connect to the TOE remotely using telnet. During testing, the evaluators did confirm that session key could be created and used to establishe SSH connection. The ST requires that users authenticate before any administrative operations can be performed on the system, and allows use of SSH to support that authentication. However, SSH is not claimed as a protection mechanism for the TOE-provided security functions. The TOE is a self contained device.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target,* Version 1.0, dated 3 April 2006. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Juniper Networks J-Series Family of Service Routers running JUNOS 7.3 refers to the TOE.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 97/01/11, CEM-97/017.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.2, Revision 256, January 2004.
- *Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14 Security Target,* Version 1.0, 3 April 2006.
- *Evaluation Technical Report for Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14, Part 1* (Non-Proprietary), Version 3.0, 20 April 2006.
- *Evaluation Technical Report for Juniper Networks J-Series Family of Service Routers running JUNOS 7.3R2.14, Part 2* (SAIC and Juniper Proprietary), Version 1.0, 3 April 2006.