National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1

Report Number: CCEVS-VR-04-0055
Dated: January 23, 2004
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
Paul Olson
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team
Science Applications International Corporation (SAIC)
7125 Columbia Gateway Drive
Suite 300
Columbia, MD 21046

Executive Summary

The evaluation of the Juniper Internet Routers Version 1.0 was performed by the SAIC CCTL, an accredited testing laboratory. The TOE identified in this Validation Report has been evaluated using the Common Methodology for IT Security Evaluation (Version 2.11) for conformance to the EAL 2 requirements of the Common Criteria for IT Security Evaluation (Version 2.1).

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.

The information contained in this Validation Report is not an endorsement of the Juniper Internet Routers by any agency of the US Government and no warranty of the product is either expressed or implied.

The SAIC Lab evaluation team concluded that the Common Criteria requirements for a product Evaluation have been met.

The technical information included in this report was obtained from the Evaluation Technical Report For Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1, dated 15 January 2004, produced by the SAIC CCTL.

The TOE is a set of eight routers all running Juniper Operating System (JUNOS) 6.0r1. The software is identical on each router.

Evaluation Details

Dates of Evaluation: June 2003 to January 2004
Evaluated Product: M and T-Series of Internet Routers running JUNOS 6.0r1
Developer: Juniper Networks, Inc.
CCTL: SAIC, Columbia
Validation Team: Paul Olson, National Security Agency, Ft. Meade, MD
TOE Conformance: Part 2 Conformant; Part 3 Conformant

TOE Identification

The TOE comprises eight Juniper Networks Internet Routers running JUNOS 6.0r1, from their M-Series and T-Series. The eight routers refer to Juniper Networks model numbers M5, M10, M20, M40e, M7i, M160, T320, T640.

The TOE includes the physical router itself, including any installed PICs, and the JUNOS software. This is equivalent to the product as shipped.

Security Policy

The Security Policy of the TOE is enforced by the functions of the TOE hardware and software. These functions include Identification and Authentication for the administrative interfaces, the management of the security configurations and the self-protection of the TOE itself.

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 external authentication service, such as a RADIUS or TACACS+ server (the external authentication server was not evaluated and 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 TOE's user memberships and privileges are handled by the TOE.

Security Management

The TOE is managed through a Command Line Interface (CLI). Through this interface all management can be performed, including user management and the configuration of the router functions. This interface is accessible through ssh and telnet sessions, as well as a local terminal console. The CLI provides an interface, which is used to perform all management functions.

Protection of the 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.

Assumptions and Clarification of Scope.

The TOE does not protect against misuse by untrusted users, because there are no non-administrative interfaces on these Routers. The TOE does not protect against attacks by untrusted software, for there is no untrusted software on the TOE. The TOE does not protect against attacks on packets entering or leaving the TOE (after packets enter the TOE, they are handled exclusively by the TOE software). The TOE's only protection mechanisms are the three listed above. Together, they ensure that only authorized administrators gain access to the administrator interface, and therefore to the routing tables that control network traffic.

Threats to Security

T.PRIVIL	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.
T.OPS	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.

Assumptions

There are three security aspects of the environment that must be handled by the owning organization

A.LOCATE	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

A.NOEVIL Those responsible for the TOE must ensure that authorized administrators are non-hostile and follow all administrator guidance.

A.EAUTH A RADIUS or TACACS+ server must be available for external authentication services.

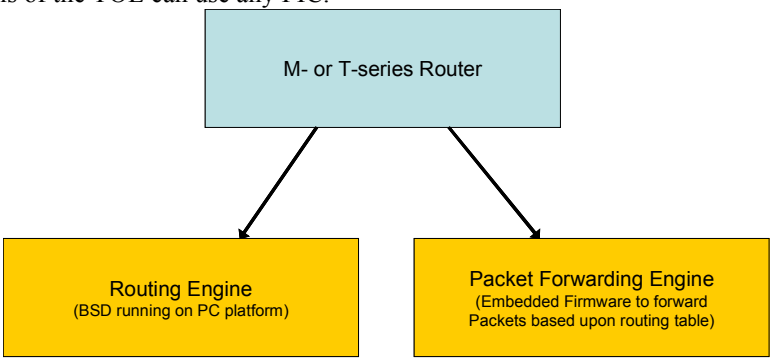
Policies

P.MANAGE The TOE shall provide effective management functions that can only be utilized by authorized users.

P.PROTECT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Architecture

The TOE is an internet router suitable for use in a controlled access facility such as a computer laboratory or a network installation. The TOE is made from two separate pieces: the Routing Engine and Packet forwarding Engine that comprise the router platform itself. PICs 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. All models of the TOE can use any PIC.



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 via the TACACS+ or RADIUS server. All management, whether from an administrator connecting to a terminal or from the network, requires successful authentication.

Documentation

The following documents were presented as evidence for the claims in the ST:

Juniper Networks routers High Level Design, Revision 3.0, December 19, 2003

Authentication and Authorization Functional Specification, v1.10, 26 August 2003
(Representation Correspondence embedded in the High Level Design)

Juniper Networks Technical Documentation Release 6.0 Security Target for Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1, Version 1.0, 14 January 2004

JUNOS Software Configuration Management Plan, Revision 0.3, December 19, 2003
Product Revision Policy Document Control revision 01

Juniper Networks Standard Delivery Procedures, Revision 0.2, June 10, 2003
JUNOS Internet Software Configuration Guide: Getting Started Release 6.0, Revision 1

System Test Plan, Revision 1.11, 19 December 2003 Test Logs containing actual results

JUNOS Vulnerability Analysis, Revision: 1.2, 7 July 2003 (Strength of Function is embedded in the ST)

Additionally, the evidence included:

Book	Description
JUNOS Internet Software Configuration Guides	
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
Getting Started	Provides an overview of the JUNOS software and describes how to install and upgrade the software. This manual also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
Multicast	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
Network Interfaces and Class of Service	Provides an overview of the network interface and class-of-service functions of the JUNOS software and describes how to configure the network interfaces on the router.
Network Management	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP, accounting options, and cflowd.
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
Routing and Routing Protocols	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
VPNs	Provides an overview of Layer 2 and Layer 3 Virtual Private Networks (VPNs), describes how to configure VPNs, and provides configuration examples.
JUNOS Internet Software References	
Operational Mode Command Reference: Interfaces	Describes the JUNOS Internet software operational mode commands you use to monitor and troubleshoot network and services interfaces on Juniper Networks M-series and T-series routers.
Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management	Describes the JUNOS Internet software operational mode commands you use to monitor and troubleshoot most aspects of Juniper Networks M-series and T-series routers.
System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
JUNOScript API Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript API to monitor and configure Juniper Networks routers.
JUNOScript API Reference	Provides a reference page for each tag in the JUNOScript API.
JUNOS Internet Software Comprehensive Index	
Comprehensive Index	Provides a complete index of all JUNOS Internet software books and the *JUNOScript API Guide*.
Hardware Documentation	
Hardware Guide	Describes how to install, maintain, and troubleshoot routers and router components. Each platform has its own hardware guide.
PIC Guide	Describes the router Physical Interface Cards (PICs). Each router platform has its own PIC guide.

Interpretations

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. The table summarizes the set of interpretations determined to have an impact on the evaluation and identifies the impact.

Impact on Security Target Requirement	Impact on ETR Work Unit	Interpretation ID
New element added after ACM.CAP.2-3C		RI #003
	ASE_DES.1.1C changed (no work unit change indicated)	RI #038
	ASE_OBJ.1.2C and ASE_OBJ.1.3C changed (no work unit change indicated)	RI #043
ADO_IGS.1.1C and AVA_VLA changed		RI #051
FMT_SMF, family addition to CC Part 2		RI #065
	ASE_REQ.1-20 work unit changed	RI #084
	ASE_REQ.1.10C (ASE_REQ.1-16 work unit changed)	RI #085

Evaluation Results

The Evaluation Team conducted the evaluation in accordance with the EAL 2 section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the EAL 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 in the draft ETR sections for an evaluation activity (e.g., ASE) that recorded the Evaluation Team's evaluation results which the Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. 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. No constraints or assumptions were identified in performing this evaluation.

Chapter 6, Conclusions, in the Evaluation Team's ETR, states:

Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1 Security Target is a CC compliant ST.

The Chapter also 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:

JUNOS Internet Software Configuration Guide: Getting Started. Release 6.0 Revision 1

The TOE satisfies the Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1 Security Target, Version 1.0, January 14, 2003.

Validator Comments/Recommendations

The validator wishes to clarify that security policy or analysis on the internet traffic passing through the router were not evaluated. Firewall or Gateway capabilities have not been tested under this evaluation. The security functions only protect the router functions from being attacked through the administrator interface by an unauthorized individual.

Abbreviations

ACM	Access Control Management
AGD	Administrator Guidance Document
BGP	Border Gateway Protocol
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CLI	Command Line Interface
CM	Control Management
DAC	Discretionary Access Control
DO	Delivery Operation
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
I/O	Input/Output
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
OSPF	Open Shortest Path First
PIC	Physical Interface Card
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSF	TOE Security Functions

TSP	TOE Security Policy
TSC	TSF Scope of Control

Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Evaluation Technical Report for Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1 Part II.

[8] Juniper Networks M & T-Series Family of Internet Routers running JUNOS 6.0r1 Security Target, Version 1.0, January 14, 2004.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.