National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5

Report Number: CCEVS-VR-VID10517-2014
Dated: 7 March 2014
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Ken Stutterheim

Mike Allen

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

1

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in March 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. 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 Leidos evaluation team determined that the product is conformant to *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. The information in this Validation Report is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team. 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 Juniper network devices within the scope of the evaluation comprise the following series and models, all running Junos 12.1R3.5:

- M-Series Multiservice Edge Routers: M7i; M10i; M120; M320
- MX-Series 3D Universal Edge Routers: MX5; MX10; MX40; MX80; MX240; MX480; MX960
- T-Series Core Routers: T320; T640; T1600
- EX-Series Ethernet Switches: EX3300; EX4200; EX4500; EX6200; EX8200.

The Juniper network devices, in the context of the evaluation, are network devices that provide a secure base (comprising auditing, cryptographic support for network communications and update integrity, user identification and authentication, and secure management) for operational functions related to switching and routing IP network traffic.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in Security Target: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5.

1.1 Interpretations

Not applicable.

1.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

1.3 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

2 Identification

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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 (if any); and
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Details

Evaluated Product:	Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5
Sponsor:	Juniper Networks, 1194 North Mathilda Ave., Sunnyvale, CA 94089-1206
Developer:	Juniper Networks, 1194 North Mathilda Ave., Sunnyvale, CA 94089-1206
CCTL:	Leidos (formerly Science Applications International Corporation) 6841 Benjamin Franklin Drive, Columbia, MD 21046
Kickoff Date:	18 December 2012
Completion Date:	3 February 2014
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	None
PP:	Security Requirements for Network Devices, Version 1.1, 8 June 2012
Evaluation Personnel:	Leidos (formerly Science Applications International Corporation): Anthony J. Apted, Chris Keenan
Validation Body:	National Information Assurance Partnership CCEVS Ken Stutterheim, Mike Allen

3 Security Policy

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

> ***Note:*** *Much of the description of the security policy has been derived from Security Target: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5 and the Final ETR.*

3.1 Security Audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an authorized TOE User and also to send the logs to a designated log server using SSHv2 to protect the logs on the network.

3.2 Cryptographic Support

The TOE includes a cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols—SSHv2 in the evaluated configuration.

3.3 User Data Protection

The TOE performs a wide variety of network routing functions, passing network traffic among its various network connections. While implementing applicable network protocols associated with network traffic routing, the TOE is carefully designed to ensure that it doesn't inadvertently reuse data found in network traffic. When a memory buffer is allocated to build a network packet, any previous data in the buffer is overwritten by new data being received by the TOE to build the next packet. The TOE keeps track of the length of the packet and when the end of the packet being built is reached, pads out the remainder of the allocated memory resource with zeroes as necessary.

3.4 Identification & Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules.

3.5 Security Management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators), who can access the CLI only after they have provided acceptable user identification and authentication data to the TOE.

3.6 Protection of the TOE's Security Functions

The TOE protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

3.7 TOE Access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

3.8 Trusted Path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access, for which both integrity and disclosure protection is ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established. The TOE additionally protects communication with an external audit server, using TLS connections to prevent unintended disclosure or modification of logs.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in *Protection Profile for Network Devices* and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

Each TOE appliance is a network device that protects itself largely by offering only a minimal logical interface to the network and attached nodes. All router platforms are powered by the same JUNOS software, which is a special purpose OS that provides no general purpose programming capability. JUNOS provides both management and control functions as well as all IP routing.

Each Juniper Networks M-series, T-series and MX-series routing platform is a complete routing system that supports a variety of high-speed interfaces (only Ethernet is within scope of the evaluation) for medium/large networks and network applications. Juniper Networks routers share common JUNOS software, features, and technology for compatibility across platforms.

The hardware has two components: the router itself and the PICs/DPC that have been installed in the router. The various PICs/DPC that have been installed in the router allow it to communicate with the different types of networks that may be required within the environment where the router will be used.

The router architecture of each platform cleanly separates routing and control functions from packet forwarding operations, thereby eliminating bottlenecks and permitting the router to maintain a high level of performance.

Each router consists of two major architectural components:

- The Routing Engine (RE), which provides Layer 3 routing services and network management and control;
- The Packet Forwarding Engine (PFE), which provides all operations necessary for transit packet forwarding.

The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The EX-series platforms provide high-performance, carrier-class networking solutions, supporting a variety of high-speed Ethernet interfaces for medium/large networks. The EX-series platforms share common JUNOS software with the routers, such that control plane features are implemented consistently with those of the routers.

The EX-series platforms are designed as hardware devices, featuring complete Layer 2 and Layer 3 switching capabilities. The EX-series platforms are powered by the same JUNOS modular architecture as the routers. The hardware abstraction layer allows control-plane features to be written once and implemented seamlessly on the underlying hardware. This modular approach also enhances fault-tolerance, as each JUNOS software protocol daemon runs in its own protected memory space and can be gracefully restarted independently without impacting the rest of the system.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Junos OS: Secure Configuration Guide for Common Criteria Network Device Protection Profile for Devices Running Junos OS 12.1, Release 12.1, Published 2014-01-09
- Junos OS: System Basics Configuration Guide, Release 12.1, Published 8 May 2012
- Juniper Networks Junos OS System Log Messages Reference, Release 12.1, Published 1 Mar 2012.

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

7 Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the following:

- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – EX3300
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – EX4200
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – EX4500
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – EX6200
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – EX8200
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – MX80
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – MX240
- Evaluation Team Test Report for Juniper Networks Secure Network Devices Running Junos 12.1R3.5 – T320.

7.1 Developer Testing

The assurance activities in the Protection Profile for Network Devices do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Network Devices. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test reports listed above. All tests were executed on the following sample of platforms claimed in the ST:

- EX3300
- EX4200
- EX4500
- EX6200
- EX8200
- M320—the other M-series platforms included in the TOE (M7i, M10i, M120) are functionally equivalent to the M320. The same firmware image is executed on all platforms and the only differences are in the number of external network connections and network capacity
- MX80—the MX5, MX10, and MX40 platforms included in the TOE are functionally equivalent to the MX80. The same firmware image is executed on all platforms and the only differences are in the number of external network connections and network capacity

- MX240—the MX480 and MX960 platforms included in the TOE are functionally equivalent to the MX240. The same firmware image is executed on all platforms and the only differences are in the number of external network connections and network capacity
- T320—the T640 and T1600 platforms included in the TOE are functionally equivalent to the MX240. The same firmware image is executed on all platforms and the only differences are in the number of external network connections and network capacity.

Testing was conducted the week of the week of October 1, 2012 at the vendor's facility in Sunnyvale, CA. With the exception of the testing of SSH for AES-CBC-256, the testing in October demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for Network Devices. In reviewing the logs from the referenced SSH testing in October, it was determined that an incorrect test setup for SSH with AES-CBC-256 had been performed. Supplemental testing was performed on March 5, 2014 to complete confirmation that the TOE performed as specified.

The testing performed by the evaluation team is summarized as follows:

- The evaluation team confirmed the TOE's ability to generate the audit events specified in the ST
- The evaluation team confirmed the TOE's ability to establish a trusted channel with an external audit server and transfer audit records to the audit server via the trusted channel
- The evaluation team confirmed the TOE supports RSA for public key authentication and password-based authentication over SSH
- The evaluation confirmed the TOE drops an SSH connection if it receives a packet over 256K bytes in length
- The evaluation team confirmed the TOE supports SSH connections using AES-CBC-128 and AES-CBC-256
- The evaluation team confirmed the TOE does not support DH Group 1 and that it does support DH Group 14
- The evaluation team confirmed the TOE supports the specified password composition requirements, including the specified minimum length
- The evaluation team confirmed the TOE provides only obscured feedback when authentication information is entered at the local console
- The evaluation team confirmed, for all supported methods of administrator access, the TOE allows access to the CLI when the correct authentication credentials are provided, and denies access when incorrect credentials are provided, and that the services available without authentication are as specified in the ST
- The evaluation team confirmed the time could be set by the administrator
- The evaluation team confirmed a legitimate update could be installed successfully on the TOE and that an illegitimate update was rejected
- The evaluation team confirmed the TOE terminated a remote interactive session after the configured period of inactivity had elapsed. The evaluation team used values of 2, 5, and 8 minutes
- The evaluation team confirmed the user was able to terminate both an interactive local session at the TOE console and a remote interactive session over the SSH-provided trusted path
- The evaluation team confirmed the TOE displayed a configured notice and consent warning message for each method of access supported by the TOE, i.e., local interactive console, remote

interactive SSH using password authentication, and remote interactive SSH using public-key authentication

- The evaluation team confirmed the TOE was able to establish a trusted channel with an external syslog server using SSHv2. Testing additionally demonstrated the trusted channel was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE. A test was also performed to physically interrupt the connection between the TOE and the external syslog server and to verify that communications remained protected when connectivity was restored
- The evaluation team confirmed the only method of remote administration for the TOE is via SSH—the evaluation team did not identify any interface that could be used to establish a remote administrative session without invoking the trusted path. Testing additionally demonstrated the trusted path was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerabilities applicable to the TOE in its evaluated configuration.

8 Evaluated Configuration

The evaluated version of the TOE is Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5, including the following series and models:

- M-Series Multiservice Edge Routers: M7i; M10i; M120; M320
- MX-Series 3D Universal Edge Routers: MX5; MX10; MX40; MX80; MX240; MX480; MX960
- T-Series Core Routers: T320; T640; T1600
- EX-Series Ethernet Switches: EX3300; EX4200; EX4500; EX6200; EX8200.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP), in conjunction with 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's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the NDPP, and correctly verified that the product meets the claims in the ST.

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

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration. In order to remain CC compliant, the device(s) must first be configured for FIPS mode, then into Common Criteria Mode. Some devices may require the installation of a Junos FIPS image prior to the configuration of the Common Criteria mode.

An account for the user 'root' is always present in the configuration; for the evaluated configuration the use of this root account is restricted to the initial configuration of the device. Otherwise the 'root' account is outside of the scope of the evaluated configuration.

As was noted in in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality implemented by the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities prescribed in the NDPP and that the evaluation team correctly verified that the product meets the claims of the associated security target.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Security Target: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5, version 1.6, 7 January 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.
5. Protection Profile for Network Devices, Version 1.1, 8 June 2012.
6. Security Target: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running Junos 12.1R3.5, version 1.6, 7 January 2014.