National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Juniper Networks, Inc.

Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30

Report Number: CCEVS-VR-VID10681-2015
Dated: December 28, 2015
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 Panel

Sheldon Durrant

The MITRE Corporation, Bedford, MA

Jean Petty

The MITRE Corporation, McLean, VA

Common Criteria Testing Laboratory

Kenji Yoshino, Michael Baron

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both 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 evaluated.

The Target of Evaluation (TOE) consist of the EX4600 and QFX5100 models, which are infrastructure networking devices (switches), operating on Junos OS 14.1X53-D30 firmware. The EX-series and QFX-series switches provide high-performance, carrier-class networking solutions, supporting a variety of high-speed Ethernet interfaces for medium/large networks.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE:

Component	Description
Syslog Server	Syslog server supporting SSHv2 connections to send audit logs
SSH Client	SSHv2 client for remote administration
Serial Connection	Serial connection client for local administration
SFP/Line Cards	Small Form-factor Pluggable (SFP)/Line Cards are required by the TOE to operate, communicate with the connected network. These are detailed for each TOE appliance in Section 10 of the [ST].

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30
Protection Profile	• Protection Profile for Network Devices, Version 1.1, 08 June 2012 • Security Requirements for Network Devices Errata #3, 3 November 2014
Security Target	Security Target Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30, Version 1.0, December 10, 2015
Dates of Evaluation	July 8 – November 12, 2015
Conformance Result	Pass
Common Criteria Version	Version 3.1 Revision 3 (July 2009)
Common Evaluation Methodology (CEM) Version	Version 3.1, Revision 3, July 2009
Evaluation Technical Report (ETR)	15-3650-R-0045 V1.0, December 18, 2015
Sponsor/Developer	Juniper Networks, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Kenji Yoshino, Michael Baron
CCEVS Validators	Sheldon Durrant, Jean Petty

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common

Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before August 21, 2015.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptography
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.1 Audit

Junos auditable events are stored in the syslog files, and can be sent to an external log server (via Netconf over SSH). Auditable events include start-up and shutdown of the audit functions, authentication events, service requests, as well as the events listed in the table in Section 8 of the ST. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local syslog storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten.

4.2 Cryptographic Operations

The TOE includes a baseline cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems.

4.3 User Data Protection

The TOE is designed to process network packets and forward them as appropriate. The packet handling is implemented in such a manner as to prevent the leakage of user data from one packet into other packet(s) that was not intended by the originator.

4.4 Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The devices also require that applications exchanging information with them successfully authenticate prior to any exchange. This covers all services used to exchange information, including Secure Shell (SSH). Telnet, File Transfer Protocol (FTP), and Secure Socket Layer (SSL) are out of scope and are not used in the evaluated configuration.

4.5 Security Management

The TOE provides an Authorized Administrator role that is responsible for:

- The configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product
- The regular review of all audit data
- All administrative tasks (e.g., creating the security policy)

The TOE is managed through a Command Line Interface (CLI). The CLI is accessible through a remote administrative session, as well as a local console session.

4.6 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is to protect TSF data (e.g. cryptographic keys, administrator passwords). The TOE does not provide a CLI interface to permit the viewing of keys. Cryptographic keys are protected through the enforcement of kernel-level file access rights, limiting access to the contents of cryptographic key containers to processes with cryptographic rights or shell users with root permission.

Another protection mechanism is to ensure the integrity of any software/firmware updates which can be verified utilizing an ECDSA (P-256 with SHA-256) digital signature prior to installation on the TOE.

In addition, the kernel maintains a set of fingerprints (SHA1 digests) for executable files and other files which should be immutable. No executable can be run or shared object loaded unless the fingerprint is correct. The fingerprints are loaded as the filesystems are mounted, from digitally signed manifests.

The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states. Junos OS is designed to fail securely. In the event of a transiently corrupt state or failure condition, the system will report an error; the event will be logged and the system restarted, having ceased to process network traffic. When the system restarts, the system boot process does not proceed without passing all self-tests for cryptographic algorithms, RNG tests, and software integrity tests.

The TOE also maintains a real-time clock to provide reliable timestamp for its own use.

4.7 TOE Access

The TOE can be configured to terminate interactive user sessions after a user defined time-out variable is set. In addition, the TOE is able to present an access banner with warning messages prior to authentication. The TOE also allows the user to manually terminate an interactive session.

4.8 Trusted Path/Channels

The TOE creates trusted channels between itself and remote trusted authorized IT product (e.g. syslog server) 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.

The TOE uses the SSHv2 protocol, configured to use FIPS Approved algorithms, to provide Trusted Channels and Trusted Paths. Mutual authentication for Trusted Channels is provided by SSH public key authentication for both the client (remote IT entity) and the server (TOE). Remote administrators authenticate to the TOE using Trusted Paths is provided by SSH public key authentication or password-based authentication. The TOE identifies itself to remote Administrators using SSH public key authentication.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

ASSUMPTION	DESCRIPTION
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all admin guidance in a trusted manner.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

THREAT	DESCRIPTION
T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	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.
T.UNAUTHORIZED_ACCESS	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.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

POLICY NAME	POLICY DESCRIPTION
P.ACCESS_BANNER	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.

6 Architectural Information

The TOE is classified as a Network Device for Common Criteria purposes. The TOE is made up of hardware and software components.

6.1 Architecture Overview

The Target of Evaluation (TOE) is a network device (switch), and includes the following secure network devices running Junos OS 14.1X53-D30

- EX4600
- QFX5100

The TOE consists of the following IT components:

- Network devices (as detailed in Table 3 below).
- Junos OS 14.1X53-D30 package: incorporating the Junos OS 14.1X53 operating system for security switching appliances and the CentOS 6.4 providing full hardware virtualization.

6.1.1 TOE Hardware

The hardware has two (2) components: the switch chassis and the Small Form-factor Pluggable (SFP)/Line Cards that have been installed in the switch. The various SPF/Line Cards that have been installed in switch allow it to communicate with the different types of networks that may be required within the environment where the switch will be used; however, they are considered non-TOE hardware and consequently, do not fall within the evaluated scope of the TOE.

The physical boundary of the TOE is detailed in Table 3 below:

Series	Model	Ports[1]	Firmware[2]
EX-Series	EX4600	1GbE SFP: 24(40) (with 10GbE expansion modules) 10GbE SFP+: 24(40/72) (with 10GbE expansion modules/with fixed 40GbE ports using breakout cables) 40GbE QSFP+: 4(12) (with expansion modules)	Junos OS 14.1X53-D30.3

[1] The SFP/line cards plugged into the chassis ports are considered to be non-TOE hardware/software/firmware entities.

Series	Model	Ports[1]	Firmware[2]
QFX-Series	QFX5100	100 Mbps RJ-45 1GbE RJ-45 10GbE RJ-45 1GbE SFP 10GbE SFP+ 40GbE QSFP+	Junos OS 14.1X53-D30.3

Table 3 – TOE Physical Boundary

6.1.2 TOE Software

The software package is comprised of two components: the CentOS 6.4 kernel providing full hardware virtualization and the Junos OS 14.1X53 providing security switching. A combined install package is created of the Junos OS virtual machine (VM), together with the CentOS kernel.

CentOS 6.4 provides full hardware virtualization using *hardware-assisted virtualization*. This allows Junos OS to run on the virtualization platform as an unmodified guest operating systems. CentOS is responsible for presenting the (emulated) hardware devices to Junos OS, which Junos OS can then address as it would address any physical device.

The Junos OS consists of the following major architectural components:

- The Routing Engine (RE), which provides Layer 3 routing services and network management and control;
- The Packet Forwarding Engine (PFE)[3], 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.

The TOE is comprised of the Junos OS 14.1X53-D30 firmware together with the CentOS kernel (providing the virtualized environment in which Junos OS VM executes) running on the appliance chassis listed in Table 3 above (including the software implementing the Routing Engine and the software and ASICs implementing the Packet Forwarding Engine). Hence the TOE is contained within the physical boundary of the specified appliance chassis.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE.

[3] The network interface components form the lower layers of the PFE (the SPFs and Line Cards) which simply deal with physical interfaces mechanics.

7.1 Guidance Documentation

Document	Revision	Date
Junos OS Common Criteria Evaluation Configuration Guide for EX4600/QFX5100 Devices Release 14.1	14.1X53-D30	November 9, 2015

7.2 Test Documentation

Document	Revision	Date
QFX5100 Test Report, Document Number:15-3650-R-0046	Version 1.0	December 18, 2015

7.3 Vulnerability Assessment Documentation

Document	Revision	Date
Juniper Junos Vulnerabilities	N/A	November 11, 2015
OpenBSD OpenSSH Vulnerabilities	N/A	November 11, 2015

7.4 Security Target

Document	Revision	Date
Security Target Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30	1.0	December 10, 2015
Seeding of JUNOS Kernel RBG (Yarrow)	1.27.5	November 20, 2015

8 IT Product Testing

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

8.1 Evaluation Team Independent Testing

The developer and the CCTL (InfoGard Laboratories, Inc.) generated the testing plan and designed the testing activities specified in the Protection Profile for Network Device Protection Profile, Version 1.1, and the Security Requirements for Network Devices Errata #3, and generated automated and manual tests to execute the designed test plan. The Evaluation Team moderated and observed the testing of the TOE as performed by the vendor. The testing activities were conducted as specified in the Protection Profile for Network Device Protection Profile, Version 1.1, and the Security Requirements for Network Devices Errata #3.

8.2 Vulnerability Analysis

The Evaluator performed the vulnerability analysis while performing testing as described in the Test Plan. While performing the Test Plan, the Evaluator configured the TOE according to the Configuration Guide. The Evaluator performed a full TCP port scan and a UDP port scan of the top 1000 ports using NMAP 6.49BETA4. These scans attempted to identify the service and version running on any open port.

OpenSSH 6.4 was the only TCP service identified by NMAP. NMAP did not discover any services available over UDP (Note "open|filtered" indicates that the TOE did not respond to the packets sent to theses ports).

Based on the NMAP scan, the Evaluator performed a public vulnerability search for Junos 14.1X53 and OpenSSH 6.4. Juniper Junos vulnerabilities and OpenBSD OpenSSH 6.4 vulnerabilities were the best results the Evaluator was able to identify. The search was performed on October 21, 2015 and re-run on November 11, 2015 and the following known vulnerabilities were identified:

Junos:

- CVE-2015-7752: N/A: This applies to versions of Junos 14.1X53 prior to D25, The TOE is D30.
- CVE-2015-7749: N/A: The TOE is no a vSRX device.
- CVE-2015-7748: N/A: The TOE does not contain "Trio" Chipset linecards.
- CVE-2015-5363: N/A: The TOE is not an SRX device.
- CVE-2015-5362: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2015-5360: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2015-5359: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2015-5358: N/A: This applies to versions of Junos 14.1X53 prior to D16, The TOE is D30.
- CVE-2015-5357: N/A: This applies to versions of Junos 14.1X53 prior to D10, The TOE is D30.
- CVE-2014-6386: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-6385: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-6382: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-6380: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-6378: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-3825: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-3822: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-3819: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-3818: N/A: This vulnerability does not apply to Junos 14.1X53.
- CVE-2014-3817, CVE-2014-3815, CVE-2014-2714, CVE-2014-2713, CVE-2014-0618, CVE-2014-0617, CVE-2014-0616, CVE-2014-0614, CVE-2014-0613, CVE-2014-0612, CVE-2013-7313, CVE-2013-6170, CVE-2013-4688, CVE-2013-4687, CVE-2013-4686, CVE-2013-4684, CVE-2007-6372, CVE-2006-3529 , CVE-2004-0468, and CVE-2004-0467: N/A: These are older vulnerabilities that came up in the list for all Junos vulnerabilities; however none

of these apply to Junos 14.1.

OpenSSH:

- CVE-2014-2653: N/A, This vulnerabilities applies to the SSH client portion of OpenSSH. The TOE does not operate as an SSH client.
- CVE-2014-2532: not exploitable: while this is identified as a remote vulnerability, it requires modification of the sshd_config file which is a file stored on the TOE. Administrative users cannot edit the sshd_config file directly. It can only be edited through the restrictive CLI which does not allow for editing of the AcceptEnv setting.
- CVE-2014-1692: N/A: The OpenSSH was not compiled with the J-PAKE option enabled.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which claims compliance with the Protection Profile for Network Device Protection Profile, Version 1.1, June 8, 2012, and the Security Requirements for Network Devices Errata #3, November 3, 2014. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in November 2015.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the product. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFRs within the Security Target was evaluated.

11 Security Target

Security Target Juniper Networks EX4600 and QFX5100 Switches Running Junos OS 14.1X53-D30, Version 1.0, December 10, 2015.

12 Terms

12.1 Acronyms

CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CLI	Command Line Interface
CSP	Critical Security Parameters

DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
FTP	File Transfer Protocol
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
PFE	Packet Forwarding Engine
RE	Routing Engine
SF	Security Functions
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirements
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.