



Common Criteria Guidance Supplement

Juniper SRX Series with Junos OS 20.2R1

Document Version 0.2

2021-11-18

Table of Contents

1	Introduction	3
2	Setting up the deployment environment for the TOE	4
3	Notes on the role Administrator.....	5
4	Installation Guidelines and Preparative Procedures	7
4.1	<i>Verification of Proper Delivery</i>	<i>7</i>
4.2	<i>Verification of Hardware</i>	<i>7</i>
4.3	<i>Verification of Software</i>	<i>8</i>
4.4	<i>Verification of guidance documents.....</i>	<i>8</i>
4.5	<i>Tamper-evident seals</i>	<i>9</i>
5	Setup of the TOE.....	10
5.1	<i>Setting up Administrator passwords</i>	<i>10</i>
5.2	<i>Setting up administrator access.....</i>	<i>10</i>
5.3	<i>Setting up Logging</i>	<i>10</i>
6	Operation of the TOE.....	11

1 Introduction

This document provides the evidence required by the following assurance components of the Common Criteria (CC) Version 3.1, Revision 5, Part 3:

- AGD_OPE.1
- AGD_PRE.1

The evidence concerns with the Juniper SRX Series with Junos OS 20.2R1 (the TOE). This document must be read prior to the deployment and configuration of the TOE. The TOE and the environment in which it is deployed must be set up in accordance with this guidance. Once set up, the TOE must also be operated in accordance with this guidance.

There are five variants of the TOE:

- SRX345, SRX345-DUAL-AC and SRX380 which run the Junos OS 20.2R1 in bare metal configuration, and
- SRX4100 and SRX4200 which run the Junos OS 20.2R1 in hypervisor configuration.

The TOE functionality is nearly identical to other Junos OS versions. Therefore, the guidance for the secure setup and operation of SRX345, SRX345-DUAL-AC and SRX380 is, except when otherwise stated in this document, in accordance with

[AGD-3] Common Criteria Guide for SRX345, SRX345-DUAL-AC, and SRX380 Devices, Release 20.2R1, 2021-10-01

The guidance for the secure setup and operation of SRX4100 and SRX4200 is, except when otherwise stated in this document, in accordance with

[AGD-4] Common Criteria Guide for SRX4100 and SRX4200 Devices, Release 20.2R1, 2021-10-01

Detailed guidance on the installation and upgrading of the TOE software is given in

[SWIUG] Junos OS, Software Installation and Upgrade Guide, Published 2020-03-30

The users are Administrators of the TOE. They must, prior to the deployment and operation of the TOE, familiarize themselves with the requirements for the Administrators as stated in Chapter 2 of [AGD-3] for SRX35, SRX345-DUAL-AC and SRX380, and [AGD-4] for SRX4100 and SRX4200. All requirements stated for the Administrators and FIPS Users of the TOE apply to the Administrators of the TOE.

The TOE must at all times be operated in accordance with the guidance given in this document and in [AGD-3] and [AGD-4].

2 Setting up the deployment environment for the TOE

In order for the TOE to be operated in a secure manner, the environment in which it is deployed must meet the minimum-security requirements. These security requirements are formally stated as security requirements for the operational environment of the TOE.

In order to fulfill these requirements, the users of the TOE must ensure that the following are addressed in the operational environment of the TOE:

1. The TOE, the management workstation and the syslog server connected to the TOE reside in a physically secure data center. The security countermeasures controlling access to the data center are selected and implemented based on a methodical assessment of risks and are sufficient to prevent physical access to the TOE or connected devices by unauthorised users with medium attack potential. The physical security measures include policy, procedural and technical measures for preventing, detecting and responding to attempted violations of physical security.
2. 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. No such capabilities shall be installed on the TOE by Administrators.
3. Administrators are vetted for security, trusted to follow and apply all guidance documentation in a trusted manner, and act with integrity in accordance with all the policies governing the use of the TOE in the interest of the using organisation's security. The administrators shall monitor the operational environment of the TOE for changes in security characteristics (e.g., expiration of revocation of X.509 certificates) and when a security-relevant change is detected, take the necessary administrative action to ensure that the TOE remains in a secure state.
4. The TOE firmware and software is updated by an Administrator on a regular basis as required to respond to the release of product updates addressing known vulnerabilities.
5. The Administrators' secrets used to access the TOE are protected on any other platform on which they reside. This is achieved by using well known, recognized software in the management workstation and syslog server and ensuring that the software and the underlying operating system are patched when vulnerabilities are discovered. The management workstation and the syslog server reside in the same data center as the TOE and are protected by the same physical security measures as the TOE.
6. TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.

3 Notes on the role Administrator

The only user of the TOE is the Administrator. A user with sufficient credentials is assigned by the TOE to a role Administrator upon being successfully authenticated with a username and password. All TOE functions shall be available to the Administrator.

The TOE is not formally FIPS 140-2 certified but shall be used with the FIPS mode enable to ensure that cryptographic self-tests and other security mechanisms are deployed in the TOE. Formally FIPS 140-2 certified cryptographic module would require additional roles which are not used in the TOE.

Any the FIPS 140-2 specific roles and tasks referred to in the TOE documentation shall be carried out by the Administrators of the TOE. There are no additional roles within the TOE.

The Administrator has the following security related tasks to perform to ensure that the TOE is set up to and remains in a secure state:

1. Set the initial root password. All passwords within the TOE must be in accordance with the guidance given in Sect.5.1 to ensure that secure values are entered.
2. Reset user passwords for FIPS-approved algorithms during upgrades from Junos OS. All passwords within the TOE must be in accordance with the guidance given in Sect.5.1 to ensure that secure values are entered.
3. All passwords must be kept secret. They must not be written down and they shall not be surrendered for anybody. If there is any suspicion of a password being compromised, that password must be changed without delay.
4. Set up manual IPsec Security Associations (SA) for configuration with dual Routing Engines. IPsec is used for implementing Virtual Private Networks (VPN) within the TOE. For ensuring a secure VPN setup, the VPN configuration must be carried out in accordance with Chapter 7 of [AGD-3] for SRX345, SRX345-DUAL-AC and SRX380 variants of the TOE and in accordance with Chapter 7 of [AGD-4] for SRX4100 and SRX4200 variants of the TOE.
5. Examine log and audit files for events of interest. The Administrators are to examine the audit logs using the preferred tools and their expertise and experience to ensure that no audit events have occurred which might indicate an attempted or successful attack against the TOE.
6. Erase user-generated files and data on (zeroize) the device. This ensures that the TOE boots up to a FIPS mode which is a secure state ensuring that all cryptographic and start-up self-tests are carried out. To ensure a secure state, zeroization is to be carried out in accordance with the guidance given in the Section "Understanding Zeroization " of [AGD-3] and [AGD-4].
7. When stored or deployed, the TOE and the documentation thereof must be placed inside a secure data center with physical access only granted to authorised Administrators. The

organisation deploying the TOE must ensure that the necessary policies and procedures are in place to ensure that the Administrators are trusted and that the data center is sufficiently secure to prevent unauthorised physical and logical access to the TOE. The management workstation and the console used by the Administrator for accessing the TOE must reside in the same data center.

8. All Administrators must be vetted in accordance with the security policy and procedures of the organisation using the TOE. Administrator rights shall only be granted to the users passing the vetting. Additionally, all Administrators must formally commit to the secure information processing practices in association with the TOE and to at all times conforming to the security guidance of the TOE and not intentionally engage in any malicious or otherwise harmful actions when using the TOE.

4 Installation Guidelines and Preparative Procedures

The TOE is to be installed and configured in accordance with the guidance given in this section. Installation and configuration may occur for two distinct scenarios:

- New Installation where a previously unused TOE is received from the developer, installed and configured for use
- Existing Installation where a previously installed TOE is configured for use.

Verification of the proper delivery of the TOE is only required for a new installation of the TOE whereas the verification of the TOE hardware and TOE software versions must be carried out both for new and existing installations.

4.1 Verification of Proper Delivery

The TOE is packed in a manner that allows the recipient to verify that a correct TOE has been received and it has not been tampered with during the shipment to the user.

For SRX345, SRX345-DUAL-AC and SRX380 models the verification of the TOE authenticity must be carried out in accordance with the section "Identifying Secure Product Delivery" of [AGD-3].

For SRX4100 and SRX4200 models the verification of the TOE authenticity must be carried out in accordance with the section "Identifying Secure Product Delivery" of [AGD-4].

4.2 Verification of Hardware

The hardware version of the TOE is etched into the TOE casing. The recipient of the TOE must verify that the version is correct and in accordance with the purchased version of the TOE. The hardware version is etched into the casing of the TOE as illustrated in Figure 1.



Figure 1 TOE hardware verification

4.3 Verification of Software

The version of the TOE software can be checked by the command **show version brief** which displays the software version. If the version is not 20.2R1, the correct software version must be downloaded and installed in accordance with the guidance given in the section "Downloading Software Packages from Juniper Networks", and the section "Installing Junos Software Packages" of [AGD-3] for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380 variants of the TOE, and the same sections of [AGD-4] for SRX4100 and SRX4200 variants of the TOE.

The TOE must be deployed in the FIPS mode which ensures that the cryptographic parameters and primitives are properly initialized prior to the use of the TOE. To enter the FIPS Mode, the critical cryptographic parameters of the TOE must be zeroized prior to the commencement of the use. This is to be done in accordance with the guidance given in the section "Understanding Zeroization " of [AGD-3] and [AGD-4].

The TOE software may require upgrading in case of bug fixes to the TOE software have been issued by the developer. All upgrading and downloading of software updates must be carried out by the Administrators of the TOE in accordance with [SWIUG].

The TOE software is issued as a complete distribution which is digitally signed. The digital signature is automatically verified when the distribution is installed. There are no partial distributions. The distribution is uniquely identified by a file name and the digital signature is attached to the installation package. The Administrator may verify the digital signature to ensure authenticity of the installation package. This is described in the section "Validating the Installation Package with the Current Configuration" and Sect. "Junos OS and Junos OS Evolved Installation Package Names" on Chapter 3 of [SWIUG].

If for any reason the validation of the installation package fails, the package shall not be installed. The user is to contact Juniper either through a sales representative or through J-TAC to resolve the issue.

4.4 Verification of guidance documents

The TOE is delivered together with the security guidance (this document and the documents this document refers to). When the TOE is packaged, a printout is added to the physical packaging of the TOE to indicate how the guidance documents can be downloaded.

The downloading of the documentation for each variant of the TOE is from the Juniper secure web site. The documents are identified by document name and the document release date. The secure web site ensures that only authentic documents are available for downloading and the name and release date of each document allows the Administrators to verify that each document is exactly as identified in section 1. No other documents must be followed in the configuration and use of the TOE.

4.5 Tamper-evident seals

Tamper-evident seals are not part of the TOE and the Administrator shall ignore the setting up of the tamper-evident seals in the physical configuration of the TOE.

5 Setup of the TOE

5.1 Setting up Administrator passwords

The TOE is operated through a Command Line Interface (CLI) either from a console or from a management workstation connected to the TOE over SSH. All TOE functions are only accessible to Administrators of the TOE. Each user is authenticated using a username and a password and if the authentication is successful and the user possesses sufficient privileges, he/she shall be assigned to the role of an Administrator.

Consequently, it is essential that all users of the TOE select strong passwords and keep them secure from other users - whether legitimate or not. Passwords must be selected and managed, and Administrator users configured, in accordance with Chapter 3 of [AGD-3] for SRX345, SRX345-DUAL-AC and SRX380 variants of the TOE and in accordance with Chapter 3 of [AGD-4] for SRX4100 and SRX4200 variants of the TOE.

It is expected that the users of the TOE set an idle timeout value to dissuade misuse of the TOE's CLI. This may be set using the "set cli idle-timeout" command. The timeout value should be set to 1 minute.

5.2 Setting up administrator access

The TOE may be accessed by authorised Administrators from console or from a management workstation over a SSH connection. Both access methods must be specifically configured for security. Access to the TOE must be configured in accordance with Chapter 4 of [AGD-3] for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380 variants of the TOE and in accordance with Chapter 4 of [AGD-4] for SRX4100 and SRX4200 variants of the TOE.

5.3 Setting up Logging

The TOE implements a rich set of audit logs to assist Administrators in troubleshooting and maintaining the security of the TOE. The TOE maintains an internal log but may also be configured to forward the audit records to an external Syslog server. The configuration of the audit function and Syslog server is to be done in accordance with Chapters 5 and 6 of [AGD-3] for SRX345, SRX345-DUAL-AC and SRX380 variants of the TOE and in accordance with Chapters 5 and 6 of [AGD-4] for SRX4100 and SRX4200 variants of the TOE.

6 Operation of the TOE

Once the TOE is configured, the Administrator has access to the CLI functions for configuring and operating the TOE Security features of the TOE. The functions available for administrators are to be used in accordance with the security guidance as per Table 1.

Table 1 Operation of the TOE

Security feature	Guidance for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC SRX380	Guidance for SRX4100 and SRX4200
Configuring cryptographic characteristics of the TOE¹	Chapter 2 of [AGD-3]	Chapter 10 of [AGD-4]
Configuring security flow policies of the TOE	Chapter 8 of [AGD-3]	Chapter 8 of [AGD-4]
Configuring traffic filtering rules of the TOE	Chapter 9 of [AGD-3]	Chapter 9 of [AGD-4]
Configuring the protection from network attacks	Chapter 10 of [AGD-3]	Chapter 10 of [AGD-4]
Configuring the TOE intrusion detection capabilities	Chapter 11 of [AGD-3]	Chapter 11 of [AGD-4]
Performing self-tests on the TOE	Chapter 12 of [AGD-3]	Chapter 12 of [AGD-14]

Overall information of the TOE configuration statements is given in Chapter 13 of [AGD-3] and [AGD-4] to assist the Administrators in the use of the CLI commands for configuring the TOE.

¹ The values of Critical Security Parameters (CSP) as stated in Table 5 of [AGD-3] and [AGD-4] are not directly configurable by the Administrator. The TOE software sets the values automatically as per secure parameter values for the protocol or other service selected by the Administrator. Therefore, it is not possible for the TOE to enter an insecure state through misconfiguration of the CSP values.