National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Juniper vSRX3.0 with Junos OS 22.2R2

Report Number:	**CCEVS-VR-VID11397-2024**
Dated:	**01/22/2024**
Version:	**0.1**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

Meredith Martinez

Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Yogesh Pawar

Pratheek Mendon

Adarsh Pandey

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) 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 for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this 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 5 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 vSRX3.0 with Junos OS 22.2R2 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices, version 2.2e, dated 27 March 2020 [CPP_ND_V2.2E], collaborative Protection Profile Module for Stateful Traffic Filter Firewalls, Version 1.4e, dated 01 July 2020 [MOD_CPP_FW_V1.4E], PP-Module for Virtual Private Network (VPN) Gateways Version 1.2, dated 31 March 2022 [MOD_VPNGW_V1.2] and PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, dated 11 May 2021 [MOD_IPS_V1.0].

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 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0. 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 provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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).

Based on these findings, 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.

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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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(s) 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 vSRX3.0 with Junos OS 22.2R2
Protection Profile	CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0
Security Target	Juniper vSRX3.0 with Junos OS 22.2R2 Security Target
Evaluation Technical Report	Evaluation Technical Report for Juniper vSRX3.0 with Junos OS 22.2R2
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Juniper Networks, Inc.
Developer	Juniper Networks, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395, Rockville, MD 20850, USA
CCEVS Validators	Jim Donndelinger Meredith Martinez Mike Quintos

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST.

3.1 TOE Overview

The TOE is the Juniper Networks, Inc. Juniper vSRX3.0 with Junos OS 22.2R2 Virtual Firewall. It is intended for deployment with service providers and large enterprises. The TOE may be operated in single mode or in cluster mode. Cluster mode is a High Availability (HA) mode in which two instances of a TOE are connected and configured to operate like a single device. This ensures high availability in the case of equipment malfunction in one of the devices.

The TOE allows definition of packet filtering policies which are enforced on all traffic traversing to, from or through it. Each packet is also subjected to stateful inspection. Further security is added by an intrusion prevention function. All traffic is monitored against signatures of known attacks and for abnormalities in traffic patterns. If potentially malicious traffic is detected, protective action is taken. Security policies are managed, and the TOE configuration controlled by Security Administrators. Management occurs via a Command Line Interface (CLI) from a local or remote management station.

The TOE is deployed as a gatekeeper between two networks so that all traffic between the two networks passes through an instance of the TOE. This ensures that all traffic between the two networks is subject to the security policies the TOE enforces. Traffic and information flows are controlled based on the rules set by TOE Administrators concerning network node addresses, protocol, type of access requested, and the service requested. The TOE implements a default deny rule, i.e. it drops any network traffic not explicitly allowed by the rules. All security relevant activities and events are audited.

Additionally, the TOE implements a multi-site Virtual Private Network (VPN) gateway functionality for tunneling traffic between itself and a VPN peer. In Cluster Mode, the link between the two instances of TOE may also be secured with IPsec. If the audit records are forwarded to an external syslog server, the connection between the TOE and the syslog server may be protected with SSH. The connection between the TOE and a remote management station is also protected by SSH.

TOE software is deployed with a hypervisor and a x86 server. The user configures the hypervisor on the selected server and installs the TOE software on the hypervisor. The software is downloaded from the Juniper web site. TOE Software is protected with a digital signature and hash values. The TOE verifies the signatures and hash values at the boot up and executes a full suite of self-tests to ensure that the TOE functions correctly and only authentic TOE software is executed.

3.2 TOE Description

The TOE implements Junos Control Plane (JCP) and Packet Forwarding Engine (PFE) which constitutes the Junos data plane. JCP and PFE are executed on the virtual CPUs (vCPU) which are part of the environment of the TOE. JCP is executed on one vCPU and the PFE on at least one vCPU. The vCPU number can be increased for improved performance. The complete vSRX3.0 architecture and the TOE within it is illustrated in Figure 1.

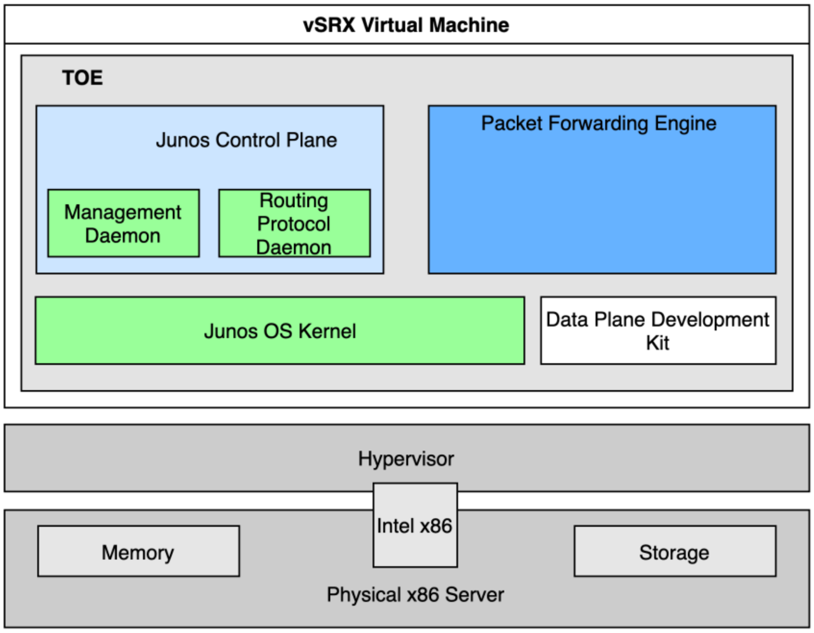

Figure 1 – vSRX3.0 Architecture

Junos Control Plane (JCP) is the virtual Routing Engine (vRE) which implements Layer 3 routing services. It also implements all network management functions for the configuration and operation of the TOE and controls the flow of information through the TOE. Controlling the flow of information through the TOE includes Network Address Translation (NAT) and the encryption and decryption of packets for secure communication over IPsec.

Packet Forwarding engine (PFE) implements all operations necessary for the forwarding of transit packets. That includes Flow Processing and Advanced Services.

JCP and PFE operate independently but communicate constantly over a high-speed internal link implemented by the Junos OS. This ensures effective forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The Junos OS kernel uses the underlying hypervisor as a virtualization infrastructure to create multiple virtual machines (VMs). Only a single VM is allowed in an evaluated configuration and no additional appliances may be installed. The hypervisor is not part of the TOE and functions as a pass-through layer only.

The TOE is configured with from three to eight virtual Network Interface Cards (vNIC). Each vNIC must be mapped to a different physical NIC. The physical server must have at least as many physical NICs as the number of vNICs configured in vSRX3.0.

The default mode for the TOE is a single mode but it may be configured for Cluster Mode by connecting ge-0/0/1 on node 0 to ge-0/0/1 on node 1. An example of a Cluster Mode configuration is given in Figure 2. Any other configuration of the physical ports has to be removed prior to the Cluster Mode configuration. The two instances of the TOE must be in an identical configuration except for one being configured to node 0 and the other to node 1.

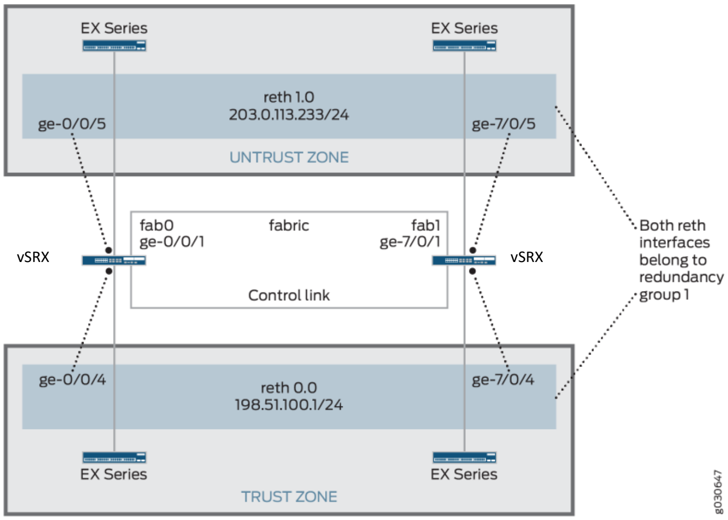

Figure 2 – Cluster Mode Configuration of the TOE

A dedicated physical interface acts as the fxp0 interface for the HA management of the TOE. The fxp1 interface for HA control link is ge-0/0/1. Administrators may define the preferred fiber interface. Once the Administrator has defined and set up the cluster, the two devices constitute a chassis cluster have an identical cluster-id, but each has a different node ID. One of the hosts has node ID 0 and the other one node ID 1.

Node 1 renumbers its interfaces by adding the total number of system FPCs to the interface's original FPC number. The fabric interface remains Administrator-defined. Critical security parameters shared by the two instances of the TOE are protected by IPsec.

4 Security Policy

The TOE implements the security functions required by the Collaborative Protection Profile for Network Devices, referred to as [CPP_ND_V2.2E]. The TOE also implements the additional security functions required by the PP-Module for Stateful Traffic Filter Firewalls ([MOD_FW_V1.4E]), PP-Module for Virtual Private Network (VPN) Gateways ([MOD_VPNGW_V1.2]) and PP-Module for Intrusion Prevention Systems (IPS) ([MOD_IPS_V1.0]). The security functions the TOE implements are summarized in the following.

4.1 Security Audit

The TOE implements an audit function which generates an audit record for each auditable event. Audit logs containing audit records are stored in protected syslog files in the VM filesystem. Syslog files may be forwarded to an external log server via Netconf over SSH.

Auditable events include start-up and shutdown of the audit functions, authentication events, configuration changes, management operations on cryptographic keys, resetting of passwords, IPS events, service requests, and each other event listed in Table 9 and Table 10 of the Security Target. Audit records include, where applicable, the date and time of the event, event category, event type, username of the user causing the event, and the success or failure of the event.

The amount of storage available for local syslog files is configurable by the Administrator. The TOE monitors the size of the syslog file against the configured limits. If the storage limit is reached, the TOE shall overwrite the existing audit records. The oldest audit records shall be overwritten first.

4.2 Cryptographic Support

The TOE implements IPSec with Internet Key Exchange IKEv1 and IKEv2 as well as SSH to protect communication with peer entities. All required cryptographic algorithms, key management functions and random bit generation methods are implemented by the TOE.

IPSec is implemented in tunnel mode with the payload encrypted with AES in GCM, CBC and CTR modes with 128-bit, 192-bit and 256-bit key lengths using HMAC-SHA-256. The symmetric keys used for IPSec are generated using IKEv1 and IKEv2. The TOE implements a random bit generator which generates the secret exponent for use in IKE DH-key exchange. Random bits are generated using HMAC-DRBG seeded by hardware and software noise sources.

Both RSA and ECDSA are implemented. DH Groups 14, 19 and 20 are implemented and the secret exponent is generated to be of appropriate length for each, i.e. 112 bits for DH Group 14, 128 bits for DH Group 19 and 192 bits for DH Group 20. The random number generator is also used for generating the nonces. Both RSA and ECDSA may be used for peer authentication with RFC 4945-conformant X.509 certificates in the IKE exchange. Pre-shared keys may also be used.

SSH is implemented in accordance with the relevant RFC suite. Both public key based and password based authentication are implemented. Public key authentication uses ECDSA with SHA on NIST curve P-256, P-384 or P-521. Key exchange may additionally use DH Group 14 with SHA-1. AES is used for protecting the payload in CBC or CTR mode with a 128-bit or 256-bit key and with HMAC-SHA1, HMAC-SHA2-256 or HMAC-SHA2-256 as data integrity algorithm. Maximum key life-time is one hour or at most one GB of data. After any of the thresholds are met, a rekeying shall be performed. Cryptographic keys are destroyed both from the volatile and the non-volatile memory when no longer required.

4.3 Identification and Authentication

Identification and authentication concerns with human users and with the peer entities of the TOE. Human users are identified with a user name and authenticated with a password. IPsec peer entities are identified by a Security Association (SA) established by IKE and authenticated using X.509 certificates or pre-shared key. SSH peer entities are identified by IP address and authenticated by a public key protocol or a password.

Human users accessing the TOE from the console are authenticated by password. When human users access the TOE from a remote management station the TOE first establishes an SSH connection between the management workstation and itself, then authenticates the human user over the SSH connection with a password.

When authenticating peer entities for VPN connection establishment, the TOE first authenticates the IPSec peer entity using X.509 certificates or pre-shared keys, and then the SSH peer entity using public-key or password based authentication. Upon successful IPSec and SSH peer entity authentication the TOE establishes a VPN session with SSH tunneled over IPSec.

The TOE may have several human users but only implements a single role, Security Administrator. Each user has a unique user name and a password which shall be entered to the TOE for identification and authentication. The password should be known only to the user and is not displayed in clear by the TOE. Only upon successful identification and authentication shall the user be assigned to the role of a Security Administrator. The TOE displays a warning banner at the authentication window to inform the users of the restrictions on access and of the consequences of unauthorized use.

If a user authentication attempt fails, the user is required to re-attempt authentication. The TOE keeps track of the number of failed attempts and compares it to an Administrator-configured number of maximum allowed authentication attempts. If the maximum number is met, the TOE shall prevent the user from establishing any remote sessions with the TOE until an Administrator-defined time-out period has elapsed.

Users may select their own password, but the TOE only accepts them if they meet a defined quality criterion. A password must contain characters of at least two of the character groups (upper case letters, lower case letters, numbers, and special characters). The length of a password must be at least the minimum length configured by Administrators but not less than ten characters.

The TOE implements X.509 authentication for IPSec peers. Alternatively, pre-shared key based authentication may be used. X.509 certificates are validated against pre-defined rules and require a minimum path length of three certificates. The certificates are validated from the Root CA upon the TOE receiving a CA Certificate Response. In case the TOE cannot establish the validity of a certificate, the Administrator is prompted to reject or accept the certificate.

4.4 Security Management

The TOE implements a rich Command Line Interface (CLI) the Administrators (i.e. users successfully authenticated and assigned to the role Security Administrator) may use to configure and manage the TOE. No other method of management but the CLI exists. All security management functions are available to the Administrators via the CLI locally from the console or remotely over SSH.

4.5 Protection of the TSF

The TOE ensures that the cryptographic keys and passwords are stored in a secure manner.

The TOE provides a reliable timestamp for its own use. The reliable timestamp can be set by a security administrator or authenticated NTP.

Cryptographic keys may only be accessed by authorized processes. Keys are erased when no longer required. Passwords are hashed before storage and may not be recovered to. When a password is read from a user, it is obscured on the screen and hashed prior to comparison to the stored password.

TOE Software is associated to a digital signature and a hash value. The signature and the hash value may be used by Administrators to verify the integrity of the software. In case of an upgraded software being made available by the developers, the Administrator may download the upgraded software from the developer's web site for installation on the TOE. The upgrade is associated with a digital signature which must be successfully verified prior to the installation of the upgrade.

The TOE also implements a set of critical self-tests at the start-up. These tests include power-on tests, file integrity test, cryptographic function and key integrity test, authentication test, known answer tests for cryptographic algorithms, and health tests for the noise sources used in the random bit generation. If any of the power-on self-tests, verification of the TOE software digital signature, or the testing of the noise source health fails, the TOE shall shut itself down as a defensive measure.

4.6 TOE Access

The TOE implements measures to ensure that inactive sessions may not be used by unauthorized users. The TOE keeps track of session inactivity and terminates any session where the maximum inactivity time has been reached. The CLI used for administering the TOE includes a logout call which the users may use to terminate their own sessions.

The TOE also displays an access banner at each authentication exchange. The access banner may be configured by the Administrators and contains an advisory notice and consent warning informing users of the legitimate use of the TOE and the sanctions for attempts of unauthorized use.

4.7 Trusted Path/Channels

The TOE implements a VPN gateway functionality which allows a trusted channel between itself and VPN peers for tunneling network traffic. The VPN peer may request a VPN connection between itself and the TOE. The VPN connection is an SSH connection tunneled over IPSec.

In Cluster Mode, the Administrators may configure the communication between the two nodes be protected with IPsec.

The TOE also implements an SSH server for a trusted path between itself and a remote management station. The management station may request establishment of an SSH connection. Upon successful connection establishment, all communication between the remote management station and the TOE, including the authentication exchange between the user and the TOE as well as all subsequent CLI commands, shall be exchanged over SSH.

4.8 Packet Filtering

Administrators may define rules for the TOE to use to filter each TCP/IP packet. The rules may be assigned to any network interface. Each packet is inspected individually, and the TOE ensures that each packet is erased from the buffer it is stored for inspection prior to the storage of the next packet in the same buffer. This ensures that each inspection is only on the fields of the packet and no residual information from previously inspected packets influences the inspection.

Packet filtering rules may be defined on IPv4, IPv6, TCP and UDP header information. IP packet rules may use source and destination addresses as well as the protocol (or next header in IPv6). TCP and UDP datagrams are filtered by rules using source and destination ports. Each packet is handled according to the first matching rule in the rule base. Any traffic for which there is no matching rule shall be dropped. For a matching rule, the TOE shall permit the packet depending on the rule and may also log the event.

4.9 Firewall

Administrators of the TOE may also define rules for stateful traffic filtering of network traffic based on ICMPv4, ICMPv6, IPv4, IPv6, TCP and UDP protocol fields. Rules may be defined for each network port of the TOE individually. The TOE inspects all incoming and outgoing traffic against those rules and permits or denies the traffic based on the rules. Additional rules are enforced to ensure that traffic which is illegitimate on high likelihood shall be dropped and a log entry generated. The rules are examined in order and the traffic is examined and filtered according to the first matching rule. If no rule matches the traffic, the traffic shall be dropped.

4.10 Intrusion Prevention

The TOE implements intrusion prevention capabilities to prevent potentially malicious network traffic from reaching the protected network. The capabilities are implemented by three distinct means:

- The TOE allows Administrators to define lists of known-good and known-bad IP source and destination addresses. Any IP datagram matching an entry in the known-bad list shall be dropped and any IP datagram matching an entry in the known-good list shall be allowed.
- The TOE maintains a list of attack signature on network traffic headers and payload and inspects all network traffic against those attack signatures. Administrator action is not required to define the rules, but the Administrator may configure the TOE action taken when traffic matches an attack signature. The Administrator may decide to allow the traffic flow, send a TCP reset to the source or destination of the malicious traffic, or block the traffic flow.
- Administrators may also define patterns for regular network traffic and express threshold values indicating a deviation from the expected, regular traffic. Deviations may occur because of an unusual traffic volume, an unusual time of the day, or an unusual frequency of traffic. Upon detecting a deviation from regular traffic, the TOE shall take Administrator-configured action to prevent the potentially malicious traffic from reaching the protected network.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The assumptions included in Table 2 are drawn directly from [CPP_ND_V2.2E], [MOD_CPP_FW_V1.4E], [MOD_IPS_V1.0] and [MOD_VPNGW_V1.2]. For each assumption, the source of the statement is explicitly stated.

Table 2 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION (Drawn from [CPP_ND_V2.2E])	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY (Drawn from [CPP_ND_V2.2E])	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform. **Application note**: Revised in accordance with TD0591.

ID	Assumption
A.NO_THRU_TRAFFIC_PROTECTION (Drawn from [CPP_ND_V2.2E])	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR (Drawn from [CPP_ND_V2.2E])	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES (Drawn from [CPP_ND_V2.2E])	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE (Drawn from [CPP_ND_V2.2E])	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION (Drawn from [CPP_ND_V2.2E])	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR (Drawn from [CPP_ND_V2.2E])	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

ID	Assumption
A.VS_REGULAR_UPDATES (Drawn from [CPP_ND_V2.2E])	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION (Drawn from [CPP_ND_V2.2E])	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION (Drawn from [CPP_ND_V2.2E])	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.CONNECTIONS (Drawn from [MOD_VPNGW_V1.2] and [MOD_IPS_V1.0])	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks. **RATIONALE**: The statement of assumption is not included in [CPP_ND_V2.2E] or [MOD_FW_V1.4E]. The statement of the assumption is identical in [MOD_VPNGW_V1.2] and [MOD_IPS_V1.0].

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threats applicable to the TOE are drawn from [CPP_ND_V2.2E], [MOD_CPP_FW_V1.4E], [MOD_IPS_V1.0] and [MOD_VPNGW_V1.2]. The threat statements are given in Table 1. Each one states explicitly from which source it is drawn.

Table 1 – Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (Drawn from [CPP_ND_V2.2E])	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY (Drawn from [CPP_ND_V2.2E])	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute

ID	Threat
	force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS (Drawn from [CPP_ND_V2.2E])	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS (Drawn from [CPP_ND_V2.2E])	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE (Drawn from [CPP_ND_V2.2E])	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY (Drawn from [CPP_ND_V2.2E])	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE (Drawn from [CPP_ND_V2.2E])	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING (Drawn from [CPP_ND_V2.2E])	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE (Drawn from [CPP_ND_V2.2E])	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore

ID	Threat
	subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE (Drawn from [MOD_CPP_FW_V1.4E])	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported. **RATIONALE**: [MOD_IPS_V1.0] and [MOD_VPNGW_V1.2] offer alternative wordings for the threat description. Effectively, they are identical as they refer to an attacker monitoring the traffic to and from the TOE to determine potentially sensitive information that may be used for attacking the target system in the protected network. Therefore, it is sufficient to include the wording as in [MOD_CPP_FW_V1.4E].
T.NETWORK_ACCESS (Drawn from [MOD_IPS_V1.0])	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information. **RATIONALE**: [MOD_CPP_FW_V1.4E] offers an alternative wording. That wording states a threat which is a subset of the wording of the threat stated in [MOD_IPS_V1.0]. The broader wording is included as it shall ensure that the threat is covered to the full extent required by [MOD_IPS_V1.0] as well as [MOD_CPP_FW_V1.4E]. Furthermore, the wording of the threat statement in [MOD_IPS_V1.0] is effectively identical to the corresponding statement in [MOD_VPNGW_V1.2]. Including the wording as in [MOD_CPP_FW_V1.4E] would not fully address the threat as stated in [MOD_IPS_V1.0] and [MOD_VPNGW_V1.2].
T.NETWORK_MISUSE (Drawn from [MOD_CPP_FW_V1.4E])	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others. **RATIONALE**: [MOD_IPS_V1.0] and [MOD_VPNGW_V1.2] offer alternative wordings for the threat description. Effectively, they are identical as they refer to the services available in a protected network being used in a manner not allowed by the security policy. Therefore, it is sufficient to include the wording as in [MOD_CPP_FW_V1.4E].
T.MALICIOUS_TRAFFIC (Drawn from [MOD_CPP_FW_V1.4E])	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

ID	Threat
T.NETWORK_DOS (Drawn from [MOD_IPS_V1.0])	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.
T.DATA_INTEGRITY (Drawn from [MOD_VPNGW_V1.2])	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.REPLAY_ATTACK (Drawn from [MOD_VPNGW_V1.2])	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these.

5.3 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:

- This evaluation covers only the specific model and software as identified in this document, and not any earlier or later versions released or in process.
- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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.

5.3.1 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- Telnet, FTP, SSL and SNMP as they violate the secure access requirements.
- Management of the TOE via J-Web, JUNOScript or JUNOScope.
- Any use of CLI account super-user or Linux root account.
- Hosting of more than one Virtual Machines on one physical platform.
- Hardware of the x86 server hosting the VMWare ESXi 7 Hypervisor.

6 Documentation

The following guidance document was provided by the vendor with the TOE for evaluation:

- Common Criteria Guide for vSRX3.0 Release 22.2R2, December 13,2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration is the Juniper vSRX3.0 with Junos OS 22.2R2 configured in accordance with the documentation identified in section 6 of this report.

TOE Software consists of the following:

- Junos OS 22.2R2 for vSRX3.0 software, including the vSRX3.0 Virtual Machine

TOE Hardware must have at least the number of NICs as there are vNICs configured in the TOE. It must be one of the following:

- HP ProLiant DL380p Gen9 with Intel Xeon E5-2600 v4 series
- PacStar 451 with Intel Xeon E-2200M series

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- Telnet, FTP, SSL and SNMP as they violate the secure access requirements.
- Management of the TOE via J-Web, JUNOScript or JUNOScope.
- Any use of CLI account super-user or Linux root account.
- Hosting of more than one Virtual Machines on one physical platform.
- Hardware of the x86 server hosting the VMWare ESXi 7 Hypervisor.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Juniper vSRX3.0 with Junos OS 22.2R2, which is not publicly available. The Assurance Activities Report (AAR) provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. In the AAR, Section 3.5 lists the tested devices, and Section 4 provides diagrams of the test environment and a list of test tools.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Juniper vSRX3.0 with Junos OS 22.2R2 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Juniper vSRX3.0 with Junos OS 22.2R2 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0 related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0 related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources examined are as follows:

- https://nvd.nist.gov/vuln/search
- https://cve.mitre.org/cve/search_cve_list.html

- https://www.cvedetails.com/vulnerability-search.php
- https://www.exploit-db.com
- https://www.rapid7.com/db/?type=nexpose
- https://supportportal.juniper.net/s/knowledge

The evaluator examined public domain vulnerability information sources by performing a keyword search. The latest search was performed on January 9, 2024. The terms used for this search were based on the vendor name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- JunOS 22.2
- Juniper vSRX
- Intel Xeon E5-2600 v4
- Intel Xeon E-2200M
- FreeBSD 12
- Junos OS Kernel
- Junos OS libmd
- Junos OS libquicksec
- Junos OS openssl

The result of these searches did not find any vulnerabilities that are applicable to the TOE in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

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 CPP_ND_V2.2E, MOD_CPP_FW_V1.4E, MOD_VPNGW_V1.2 and MOD_IPS_V1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the document listed in Section 6. The evaluated configuration is limited to the software and hardware identified in Section 7. No other versions of the TOE, either earlier or later, were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product were not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed in other sections of this report.

11 Annexes

Not applicable.

12 Security Target

Juniper vSRX3.0 with Junos OS 22.2R2 Security Target Version 0.9.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
4. Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
5. collaborative Protection Profile for Network Devices, Version 2.2e, March 2020 [CPP_ND_V2.2E].
6. PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e, July 2020 [MOD_CPP_FW_V1.4E].
7. PP-Module for VPN Gateways, Version 1.2, March 2022 [MOD_VPNGW_V1.2].
8. PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, May 2021 [MOD_IPS_V1.0].
9. Juniper vSRX3.0 with Junos OS 22.2R2 Security Target, Version 0.9, December 14,2023.
10. Common Criteria Guide for vSRX3.0, Release 22.2R2, December 13, 2023.
11. Assurance Activity Report for Juniper vSRX3.0 with Junos OS 22.2R2, Version 0.6, January 19, 2024.
12. Evaluation Technical Report for Juniper vSRX3.0 with Junos OS 22.2R2, Version 0.4, December 28, 2023.
13. Vulnerability Assessment for Juniper Networks Inc., Junos OS 22.2R2 for vSRX3.0, Version 1.5, January 9, 2024.