# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


# Validation Report

# for the Junos OS 17.4R2 for vSRX, Version 1.0

**Report Number:** CCEVS-VR-10887-2019

**Dated:** January 15, 2019

**Version:** 0.1

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

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

# ACKNOWLEDGEMENTS


## Validation Team

Jerome Myers

Marybeth Panock

## Common Criteria Testing Laboratory

Padmavathi Gari

*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 Junos OS 17.4R2 for vSRX 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 January 2019. 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 Common Criteria v3.1, Revision 4.

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 (CEM), Version 3.1, Rev. 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1, Rev. 4, as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; the Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway (VPNGWEP), Version 2.1 (VPNGWEP v2.1) dated 8 March 2017; and the collaborative Protection Profile for Network Devices /collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) Version 2.11 dated 15 June 2017. 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** | Junos OS 17.4R2 for vSRX |
| **Protection Profile** | • collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018,<br>• collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018,<br>• collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017,<br>• Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017 |
| **Security Target** | Security Target Junos OS 17.4R2 for vSRX |
| **Evaluation Technical Report** | vSRX OS 17.4R2 TOE ETR |
| **CC Version** | Version 3.1, Revision 4 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Conformant |

| | |
|---|---|
| **Sponsor** | Juniper Networks |
| **Developer** | Juniper Networks |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>Montgomery Village, MD |
| **CCEVS Validators** | Jerome Myers, Marybeth Panock |

# 3 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 17.4R2 for vSRX Virtual Firewall. The vSRX Virtual Firewall delivers a complete virtual firewall solution, including advanced security, robust networking, and automated virtual machine life cycle management capabilities for service providers and enterprises.

The vSRX Virtual Firewall supports the definition of, and enforces, information flow policies among network nodes, also providing for stateful inspection of every packet that traverses the network and central management to manage the network security policy. All information flow from one network node to another passes through an instance of the TOE. Information flow is controlled based on network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that their own functions are protected from potential attacks, and provides the security tools to manage all the security functions. The TOE provides multi-site virtual private network (VPN) gateway functionality, and implements Intrusion Prevention System (IPS) functionality, capable of monitoring information flows to detect potential attacks based on pre-defined attack signature and anomaly characteristics in the traffic.

The deployment of the Junos OS 17.4R2 for vSRX TOE includes the KVM hypervisor (Ubuntu 16.04 OpenVSwitch (OVS) 2.7.0), which runs as a virtual machine (VM) on a standard x86 server. For the purposes of testing the TOE the following platform was used:

Hypervisor: VMWare ESXi 6.0 installed on an x86 server whose processor chipset supports RDRAND

The server hardware used in the testing of the TOE was an HP ProLiant DL380p Gen9 Processor Intel Xeon E5.

# 4 Security Policy

| Security Functionality | Description |
|---|---|
| Protected Communications | The TOE provides an SSH server to support protected communications for administrators to establish secure sessions and to connect to external syslog servers.<br><br>The TOE also supports IPsec connections to provide multi-site virtual private network (VPN) gateway functionality and as a tunnel for remote administrate SSH connections. The TOE requires that applications exchanging information with it are successfully authenticated prior to any exchange (i.e. applications connecting over SSH and IPsec).<br><br>Telnet, File Transfer Protocol (FTP), and Secure Socket Layer (SSL) are out of scope.<br><br>The TOE includes cryptographic modules that provide the underlying cryptographic services, including key management and protection of stored keys, algorithms, random bit generation and crypto-administration. The cryptographic modules provide confidentiality and integrity services for authentication and for protecting communications with adjacent systems. No host cryptographic modules are used by the TOE. |
| Administrator Authentication | Administrative users must provide unique identification and authentication data before any administrative access to the system is granted. Authentication data entered and stored on the TOE is protected. The TOE can be configured to terminate interactive user sessions and to present an access banner with warning messages prior to authentication. |
| Correct Operation | The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states. |
| Trusted Update | The administrator can initiate update of the TOE software (this includes both Junos VM (Hypervisor +Junos OS for SRX) and the Wind River Linux Host OS). The integrity of any software updates is verified prior to installation of the updated software. |

| Security Functionality | Description |
|---|---|
| Audit | TOE auditable events are stored in the syslog files in the VM filesystem, 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, IPS events, as well as the events listed in Table 3 and Table 4. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). Local (VM) syslog storage limits are configurable and are monitored. In the event of storage limits being reached the oldest logs will be overwritten. |
| Management | The TOE provides a Security Administrator role that is responsible for:<br>• the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product<br>• the regular review of all audit data;<br>• initiation of trusted update function;<br>• administration of VPN, IPS and Firewall functionality;<br>• all administrative tasks (e.g., creating the security policy).<br>The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session.<br>The Security Administrator role includes the capability to manage the Junos VM within the KVM virtualized environment. Access to manage the Junos VM and Linux host can only be gained through the JCP. |
| Packet Filtering/Stateful Traffic Filtering | The TOE provides stateful network traffic filtering based on examination of network packets and the application of information flow rules. |
| Intrusion Prevention | The TOE can be configured to analyse IP-based network traffic forwarded to the TOE's interfaces, and detect violations of administratively-defined IPS policies. The TOE can initiate a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow. |

| Security Functionality | Description |
|---|---|
| User Data Protection/Information Flow Control | The TOE is designed to forward network packets (i.e., information flows) from source network entities to destination network entities based on available routing information using Virtual Routers. This information is either provided directly by TOE users or indirectly from other network entities (outside the TOE) configured by the TOE users. The TOE has the capability to regulate the information flow across its interfaces; traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier (TCP or UDP port number). |

**Table 2: Logical Boundary**

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FAU_GEN.1 | None | None |
| FAU_GEN.2 | None | None |
| FAU_STG_EXT.1 | None | None |
| FAU_STG.1 | None | None |
| FCS_CKM.1 | None | None |
| FCS_CKM.2 | None | None |
| FCS_CKM.4 | None | None |
| FCS_COP.1/DataEncryption | None | None |
| FCS_COP.1/SigGen | None | None |
| FCS_COP.1/Hash | None | None |
| FCS_COP.1/KeyedHash | None | None |
| FCS_RBG_EXT.1 | None | None |
| FDP_RIP.2 | None | None |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | Origin of the attempt (e.g., IP address). |
| FIA_PMG_EXT.1 | None | None |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism. | Provided user identity, origin of the attempt (e.g., IP address). |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None | None |
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update | None |
| FMT_MTD.1/CoreData | All management activities of TSF data, | None |

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FMT_SMF.1 | None | None |
| FMT_SMR.2 | None | None |
| FPT_SKP_EXT.1 | None | None |
| FPT_APW_EXT.1 | None | None |
| FPT_TST_EXT.1 | None | None |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success or failure) | None. |
| FPT_STM.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process. | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). |
| FTA_SSL_EXT.1 | The termination of a local interactive session by the session locking mechanism. | None. |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | None |
| FTA_SSL.4 | The termination of an interactive session. | None |
| FTA_TAB.1 | None | None |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1/Admin | Initiation of the trusted path.<br>Termination of the trusted path.<br>Failure of the trusted path functions. | None. |
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Reason for failure |
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate | Reason for failure |
| FIA_X509_EXT.2 | None | None |
| FIA_X509_EXT.3 | None | None |

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FPT_TUD_EXT.2 | Failure of update | Reason for failure (including identifier of invalid certificate) |
| FMT_MOF.1/Functions | Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full. | None. |
| FMT_MOF.1/Services | Starting and stopping of services. | None |
| FMT_MTD.1/CryptoKeys | Management of cryptographic keys. | None. |
| FFW_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses<br>Source and destination ports<br>Transport Layer Protocol<br>TOE Interface |
| | Indication of packets dropped due to too much network traffic | TOE interface that is unable to process packets<br>Identifier of rule causing packet drop |
| FFW_RUL_EXT.2 | None | None |
| FCS_IPSEC_EXT.1 | Session Establishment with peer | Entire packet contents of packets transmitted/received during session establishment |
| FIA_X509_EXT.1 | Session establishment with CA | Entire packet contents of packets transmitted/received during session establishment |
| FPF_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses<br>Source and destination ports<br>Transport Layer Protocol<br>TOE Interface |
| | Indication of packets dropped due to too much network traffic | TOE interface that is unable to process packets |

**Table 3: Audit Events from NDcPP**

| Requirement | IPS Auditable Events | Additional Details |
|---|---|---|
| FMT_SMF.1/IPS | Modification of an IPS policy element. | Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known- |

| | | |
|---|---|---|
| | | good/known-bad list was modified. |
| IPS_ABD_EXT.1 | Inspected traffic matches an anomaly-based IPS policy. | Source and destination IP addresses. |
| | | The content of the header fields that were determined to match the policy. |
| | | TOE interface that received the packet. |
| | | Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, frequency, etc.). |
| | | Network-based action by the TOE (e.g. allowed, blocked, sent reset to source IP, sent blocking notification to firewall). |
| IPS_IPB_EXT.1 | Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy. | Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list). |
| | | TOE interface that received the packet. |
| | | Network-based action by the TOE (e.g. allowed, blocked, sent reset) |
| IPS_NTA_EXT.1 | Modification of which IPS policies are active on a TOE interface.<br>Enabling/disabling a TOE interface with IPS policies applied.<br>Modification of which mode(s) is/are active on a TOE interface. | Identification of the TOE interface |
| | | The IPS policy and interface mode (if applicable). |
| IPS_SBD_EXT.1 | Inspected traffic matches a signature-based IPS with logging enabled. | Name or identifier of the matched signature. |
| | | Source and destination IP addresses. |
| | | The content of the header fields that were determined to match the signature. |
| | | TOE interface that received the packet. |

| | | |
|---|---|---|
| | | Network-based action by the TOE (e.g. allowed, blocked, sent reset) |

**Table 4 Audit Events and Details from IPSEP**

# 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 TO

| Assumption | Assumption Definition |
|---|---|
| A.PHYSICAL_PROTECTION | The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/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 will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will 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. |
| A.LIMITED_FUNCTIONALITY | 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 computing platform for general purpose applications (unrelated to networking functionality). |
| A.TRUSTED_ADMINISTRATOR | 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 being 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 can defend against a malicious administrator that actively works to bypass or compromise the security of the device. |
| A.REGULAR_UPDATES | 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. |

| Assumption | Assumption Definition |
|---|---|
| A.ADMIN_CREDENTIALS_SECURE | The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. |
| A.RESIDUAL_INFORMATION | 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.NO_THRU_TRAFFIC_PROTECTION | The assumption A.NO_THRU_TRAFFIC_PROTECTION defined in [NDcPP] is not relevant to this TOE as it is addressed by additional requirements introduced through conformance to [FWcPP]. |
| A.CONNECTIONS | The assumption A.CONNECTIONS is introduced through compliance to [VPN_EP] and [IPS_EP]. It is typically understood that an ST claiming exact compliance to a Protection Profile cannot introduce assumptions. However, that is on the understanding this limits applicability of the security functional requirements for the TOE, whereas this assumption is a clarification of how the way the TOE is to be connected to distinct networks. |

No assumptions are identified for this TOE in addition to those specified in the collaborative Protection Profiles and Extended Packages.

## 5.2 Threats

The following tables 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.

The following threats for this TOE are as defined in [NDcPP] Section 4.1, which are also stated in [FWcPP], with editorial and terminology changes to reflect focus on firewall rather than general purpose network devices.

| Threat | Threat Definition |
|---|---|
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | 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 | 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 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 | Threat agents may attempt to target network devices that do not use standardized secure tunneling 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.<br>An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit. |

| Threat | Threat Definition |
|---|---|
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., 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 | 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 | 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 | Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include 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 | 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. |

| Threat | Threat Definition |
|---|---|
| T.SECURITY_FUNCTIONALITY_FAILURE | An external, unauthorized entity could make use of failed or compromised security functionality and might therefore 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. |

The following threats additional threats specified in [FWcPP], [IPS_EP] and [VPN_EP] are also detailed for this TOE.

| Threat | Threat Definition |
|---|---|
| T.NETWORK_DISCLOSURE | Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions. |
| T. NETWORK_ACCESS | 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.<br>An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization. |
| T.NETWORK_MISUSE | Access to services made available by a protected network might be used counter to Operational Environment policies. |

The following threat specified in [FWcPP] only is also detailed for this TOE:

| Threat | Threat Definition |
|---|---|
| T. MALICIOUS_TRAFFIC | 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. |

The following threat specified in [IPS_EP] only is detailed for this TOE.

| Threat | Threat Definition |
|---|---|
| T. NETWORK_DOS | 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. |

The following threat specified in [VPN_EP] only is detailed for this TOE.

| Threat | Threat Definition |
|---|---|
| T.REPLAY_ATTACK | If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver. |
| T.DATA_INTEGRITY | A malicious party attempts to change the data being sent – resulting in loss of integrity. |
| T.HIJACKED_SESSION | There may be an instance where a remote client's session is hijacked due to session activity. This could be accomplished because a user has walked away from the machine that was used to establish the session. |
| T.UNAUTHORIZED_CONNECTION | While a VPN client may have the necessary credentials (e.g., certificate, pre-shared key) to connect to a VPN gateway, there may be instances where the remote client, or the machine the client is operating on, has been compromised and attempts to make unauthorized connections. |
| T.UNPROTECTED_TRAFFIC | A remote machine's network traffic may be exposed to a hostile network. A user may be required to use a hostile (or unknown) network to send network traffic without being able to route the traffic appropriately. |

### 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:

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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; the Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway (VPNGWEP), Version 2.1 (VPNGWEP v2.1) dated 8 March 2017; and the collaborative Protection Profile for Network Devices /collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) Version 2.11 dated 15 June 2017.

- 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.

- 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. In particular, the following limitations are identified in Section 1.6.5 of the Security Target as being disabled or otherwise outside the scope of the evaluation:
    - Use of telnet, since it would violate the Trusted Path requirement set
    - Use of FTP, since it would violate the Trusted Path requirement set
    - Use of SNMP, since it would violate the Trusted Path requirement set
    - Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it would violated the Trusted Path requirement set
    - Use of CLI account super-user and linux root account.
    - Hosting multiple (Junos) VMs on one physical platform.
    - Other x86 server hardware used to host the VMWare ESXi 6.0 Hypervisor, which provides the TOE platform.

# 6 Documentation

The following public documents were provided by the vendor with the TOE for evaluation:

- [ST] Security Target Junos OS 17.4R2 for vSRX, version 1.16, dated January 14, 2019
- [ECG] Junos OS Common Criteria and FIPS Evaluated Configuration Guide for vSRX Instances Release 17.4R2, dated 2019-01-14
- [vSRX_KVM] Juniper Networks vSRX Guide for KVM, modified 2017-09-01

Those are the only documents that should be used to configure and use the TOE in the evaluated configuration. Any other documents delivered with the product or available on a vendor web site should not be trusted for TOE configuration and use.

# 7 TOE Evaluated Configuration

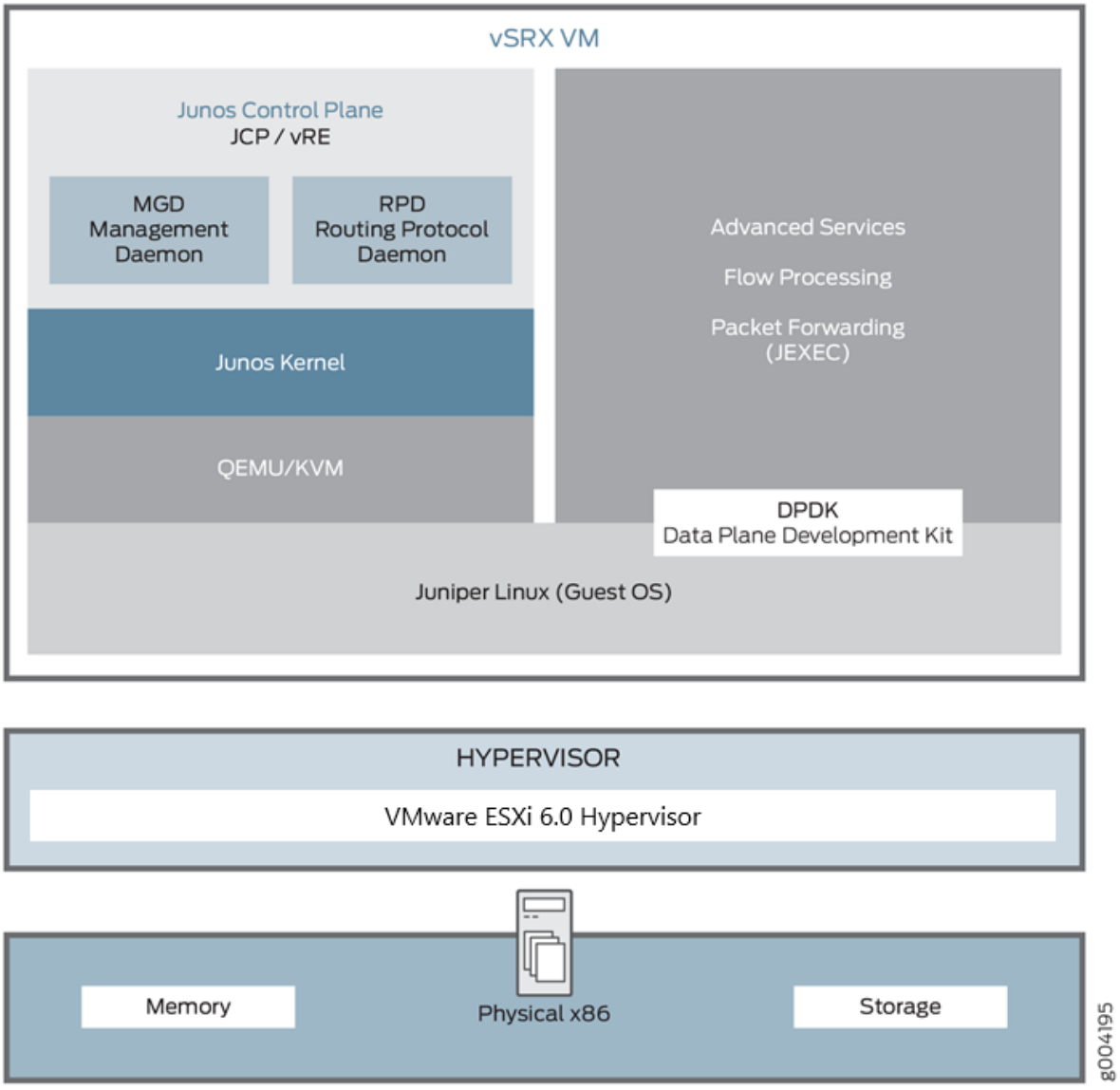
## 7.1 Evaluated Configuration

The evaluated configuration of the TOE is consists of the following items configured and operated in accordance with the documentation identified in Section 6:

Junos OS 17.4R2 for vSRX software: junos-vsrx-x86-64-17.4R2-S1.2.tgz

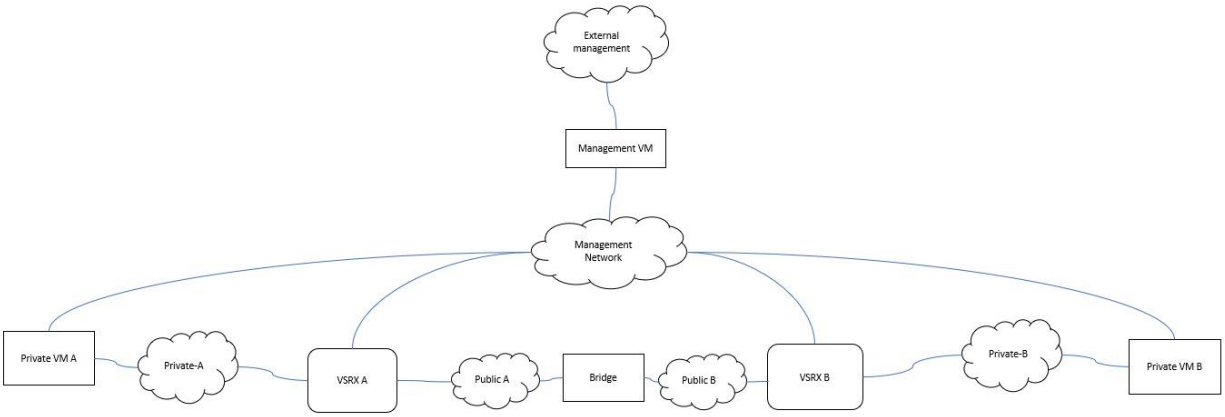
VMWare ESXi 6.0 Hypervisor

HP ProLiant DL380p Gen9 with Intel Xeon E5 with 3 to 8 NICs (at least as many as the number of configured vNICs in vSRX)



**vSRX Architecture**

Below is a visual representation of the components included in the test bed:



# 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 Junos OS 17.4R2 for vSRX, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities. A detailed description of the test tools and test configurations used for this evaluation may be found in Section 4 of that Assurance Activity Report.

## 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 the vendor-provided guidance documentation and ran the tests specified in the:

- collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018,
- Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018,
- collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017,
- Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017

The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

# 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 4 and CEM version 3.1 rev 4. The evaluation determined the Junos OS 17.4R2 for vSRX 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 Junos OS 17.4R2 for vSRX 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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; the Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway (VPNGWEP), Version 2.1 (VPNGWEP v2.1) dated 8 March 2017; and the collaborative Protection Profile for Network Devices /collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS) Version 2.11 dated 15 June 2017.

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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017, and Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter

Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017 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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017, and Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017 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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018;

collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017, and Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017 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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018, Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018, 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. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. A list of the databases searched, the search terms, and the date when the search was performed may be found in Section 6.4.1 of the Assurance Activity Report.

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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017, and Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017, 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 collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018; Collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018; collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), version 2.11, dated 15 June 2017, and Network

Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, version 2.1, dated 08 March 2017, and correctly verified that the product meets the claims in the ST.

## 10 Validator Comments & Recommendations

Users should be careful when using the Configuration Guide. The Common Criteria and FIPS Evaluated Configuration Guides are combined into one document. The FIPS configuration allows a wider range of ciphersuites than the Common Criteria. The ciphersuites that are disallowed in the CC evaluated are high-lighted in red in the document and this constraint is noted. If the document is printed in black-and-white, the highlighting might be missed by the administrators.

All other items and scope issues have been sufficiently addressed elsewhere in the document.

## 11 Annexes

Not applicable.

## 12 Security Target

Security Target Junos OS 17.4R2 for vSRX, version 1.16

## 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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Security Target Junos OS 17.4R2 for vSRX, version 1.16, dated January 14, 2019
6. Junos OS Common Criteria and FIPS Evaluated Configuration Guide for vSRX Instances Release 17.4R2, dated 2019-01-14
7. Assurance Activity Report for Junos OS 17.4R2 for vSRX Security Target Junos OS 17.4R2 for vSRX Version 1.16, dated 2019-01-15
8. Junos OS 17.4R2 for vSRX Evaluation Technical Report, version 1.4, January 2019
9. Vulnerability Assessment for Junos OS 17.4R2 for vSRX, Version 1.1, January 7, 2019
10. Test Plan for a Target of Evaluation, Version 1.4, Date January 15, 2019