National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Junos OS 19.2R1-S2 for NFX150

Report Number:	**CCEVS-VR-VID11010-2020**
Dated:	**2/24/2020**
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan

Kenneth Stutterheim

Common Criteria Testing Laboratory

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 acting on behalf of 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 imposed upon 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 placed upon the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Junos OS 19.2R1-S2 for NFX150 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 February 2020. 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 2.0+Errata 20180314, dated 14 March 2018,
- collaborative Protection Profile for Stateful Traffic Filter Firewalls, 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 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. 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 Protection Profiles and Extended packages as noted above. 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 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 19.2R1-S2 for NFX150
Protection Profile	• collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018, • collaborative Protection Profile for Stateful Traffic Filter Firewalls, 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.
Security Target	Security Target Junos OS 19.2R1-S2 for NFX150
Evaluation Technical Report	ETR for Junos OS 19.2R1-S2 for NFS150
CC Version	Version 3.1, Revision 4

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
CCEVS Validators	Meredith Hennan, Kenneth Stutterheim

3 Architectural Information

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 19.2R1-S2 for NFX150 Network Services Platform. The NFX150 is a network device that integrates routing, switching, and security functions on a single platform.

The NFX150 supports the definition of, and enforces, information flow policies among network nodes, provides for stateful inspection of every packet that traverses the network and provides central management of the network security policy. All information flow between network nodes passes through an instance of the TOE. Information flow is controlled on the basis of 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 TOE functions are protected from potential attacks and provides the security tools to manage the security functions. The TOE provides multi-site virtual private network (VPN) gateway functionality, and implements Intrusion Prevention System 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 19.2R1-S2 for NFX150 TOE includes a hypervisor, which runs a virtual machine (VM) on the following NFX150 series hardware model:

- NFX150-C-S1
- NFX150-S1
- NFX150-S1E

4 Security Policy

The logical boundary of the TOE includes the following security functionality:

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. The TOE also supports IPsec connections to provide multi-site virtual private network (VPN) gateway functionality and also 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). Telnet, File Transfer Protocol (FTP), and Secure Socket Layer (SSL) are out of scope. 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.
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. 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 4 and Table 5. 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: • the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product • the regular review of all audit data; • initiation of trusted update function; • administration of VPN, IPS and Firewall functionality; • all administrative tasks (e.g., creating the security policy). The devices are managed through a Command Line Interface (CLI). The CLI is accessible through local (serial) console connection or remote administrative (SSH) session. The Security Administrator role includes the capability to manage all NFX150 services. Access to manage the device's FreeBSD 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 analyze IP-based network traffic forwarded to the TOE's interfaces and detect violations of administratively-defined IPS policies. The TOE is capable of initiating 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).

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 made for this TOE are as defined in [NDcPP] Section 4.2 and [FWcPP] Section 3.2 (with appropriate editorial and terminology differences to reflect general network device vs. firewall), namely:

- A.PHYSICAL_PROTECTION
- A.LIMITED_FUNCTIONALITY
- A.TRUSTED_ADMINSTRATOR
- A.REGULAR_UPDATES
- A.ADMIN_CREDENTIALS_SECURE
- A.RESIDUAL_INFORMATION

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]

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 based upon the understanding this limits applicability of the security functional requirements for the TOE, whereas this assumption is a clarification of the manner in which 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 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.

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. Namely:

- T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
- T.WEAK_CRYPTOGRAPHY
- T.UNTRUSTED_COMMUNICATION_CHANNELS
- T.WEAK_AUTHENTICATION_ENDPOINTS
- T.UPDATE_COMPROMISE

- T.UNDETECTED_ACTIVITY
- T.SECURITY_FUNCTIONALITY_COMPROMISE
- T.PASSWORD_CRACKING
- T.SECURITY_FUNCTIONALITY_FAILURE

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

- T.NETWORK_DISCLOSURE
- T.NETWORK_ACCESS
- T.NETWORK_MISUSE

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

- T.MALICIOUS_TRAFFIC

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

- T.NETWORK_DOS

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

- T.DATA_INTEGRITY
- T.HIJACKED_SESSION
- T.REPLAY_ATTACK
- T.UNAUTHORIZED_CONNECTION
- T.UNPROTECTED_TRAFFIC

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

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that may benefit from clarification. 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 NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11.
- 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.
- The following items as stated in the Security Target are explicitly excluded from scope:
    - Use of telnet, since it violates the Trusted Path requirement
    - Use of FTP, since it violates the Trusted Path requirement
    - Use of SNMP, since it violates the Trusted Path requirement
    - Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement
    - Use of CLI account super-user and linux root account.
    - Hosting of multiple VMs on one physical platform.

6 Documentation

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

- Junos OS 19.2R1-S2 for NFX150 Security Target, version 1.1, February 18, 2020.
- Common Criteria Configuration Guide for NFX150 Network Services Platform, Release 19.2R1-S2, February 19, 2020.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate 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 guide from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The Target of Evaluation (TOE) is Juniper Networks, Inc. Junos OS 19.2R1-S2 for NFX150 Network Services Platform. The NFX150 is a network device that integrates routing, switching, and security functions on a single platform.

The deployment of the Junos OS 19.2R1-S2 for NFX150 TOE includes a hypervisor, which runs a virtual machine (VM) on an NFX150 series hardware model:

- NFX150-C-S1
- NFX150-S1
- NFX150-S1E

The physical boundary of the TOE is the:

- NFX150 series hardware with Intel ATOM processor and Junos OS 19.2R1-S2

The Junos OS 19.2R1-S2 for NFX150 software includes the KVM Hypervisor as well as the URE and PFE. Hence the TOE is contained within the physical boundary of each server specified above. The TOE is delivered as a single device with the Junos OS software installed. The TOE model number can be verified through the shipping label and device front panel. The software version can be verified by the show version command once the device is configured.

The Management platform and external syslog server are outside the boundary of the TOE.

7.2 Excluded Functionality

- Use of telnet, since it violates the Trusted Path requirement set (see Section 5.7.2 of the ST)
- Use of FTP, since it violates the Trusted Path requirement set (see Section 5.7.2 of the ST)
- Use of SNMP, since it violates the Trusted Path requirement set (see Section 5.7.2 of the ST)
- Use of SSL, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set (see Section 5.7.2 of the ST)
- Use of CLI account super-user and linux root account.
- Hosting multiple (Junos) VMs on one physical platform.

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 19.2R1-S2 for NFX150, which is not publicly available. The Assurance Activities Report 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 the vendor-provided guidance documentation and ran the tests specified in the NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11. 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 19.2R1-S2 for NFX150 to be Part 2 extended, and meets the SARs contained in the PP. The evaluator performed the Assurance Activities specified in the Protection Profiles, Extended Packages and any Supporting Documents related to same.

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 19.2R1-S2 for NFX150 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. The evaluator performed an assessment of the Assurance Activities specified in the NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11.

The validators 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. The evaluator performed the Assurance Activities specified in NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11 related to the examination of the information contained in the TOE Summary Specification.

The validators 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. 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. The evaluator performed the Assurance Activities specified in the NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11 related to the examination of the information contained in the operational guidance documents.

The validators 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 uniquely identified and appropriately labeled.

The validators 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 NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11 and recorded the results in a Test Report, which were summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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 NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11, 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. The vulnerability search was performed on January 3, 2019 and a follow-up search was conducted on February 18, 2020.

The validators 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 NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11, 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 NDcPP 2.0, FWcPP 2.0, VPN_EP 2.1, IPS_EP 2.11, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities that may be included in the product were not covered by this evaluation and no conclusions regarding their effectiveness should be drawn from the evaluation performed.
- On a NFX150 device, Junos OS Release 19.2R1-S2 is certified for Common Criteria with FIPS mode enabled on the device.

- Although the NFX150 is available in seven models, only the following models are supported by this evaluation:

  - NFX150-C-S1
  - NFX150-S1
  - NFX150-S1E

The other models have not been evaluated.

- Administrators should pay special attention to Chapter 5 of the Configuration Guide on how to configure event logging to a Remote Server. Event logging is handled by using NETCONF over SSH to the remote system event log.

11 Annexes

Not applicable.

12 Security Target

Junos OS 19.2R1-S2 for NFX150 Security Target, Version 1.1, February 18, 2020.

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. Junos OS 19.2R1-S2 for NFX150 Security Target, Version 1.1, February 18, 2020. [ST]
6. Common Criteria Configuration Guide for NFX150 Network Services Platform, Release 19.2R1-S2, February 19, 2020. [AGD]
7. Vulnerability Assessment for Junos OS 19.2R1-S2 for NFX, Version 1.2, February 24, 2020. [AVA]
8. Assurance Activity Report for Junos OS 19.2R1-S2 for NFX150, Version 1.1, February 18, 2020. [AAR]
9. Evaluation Technical Report for Junos OS 19.2R1-S2 for NFX150, Version 1.1, February 18, 2020. [ETR]
10. Test Report for Junos OS 19.2R1-S2 for NFX150, Version 1.1, February 18, 2020. [DTR] <evaluation sensitive>
11. collaborative Protection Profile for Network Devices, version 2.0+Errata 20180314, dated 14 March 2018 [NDcPP]
12. collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018
13. 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
14. 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