Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australasian Information Security Evaluation Program

Certification Report

Collaborative Protection for Network Devices, Version 2.1, 19 September 2018

Certification number 2019/124

Version 1.0, 02 October 2019

cyber.gov.au

Table of contents

Executive summary 4

Introduction 5

Overview 5

Purpose 5

Identification 5

NDcPP description 7

Overview 7

Security Problem Description, Objectives and Extended Components 7

Threats 7

Assumptions 10

Organisational Security Policies 11

Security Objectives 11

Extended Components Definition 12

Network iTC Interpretations 14

Security Requirements 15

Assurance Requirements 20

Evaluation 21

Overview 21

Evaluation procedures 21

Results 21

Certification 22

Overview 22

Assurance 22

Certification result 22

Recommendations 22

Annex A – References and abbreviations 23

References 23

Abbreviations 23

Executive summary

This report describes the findings of the evaluation of *the collaborative Protection Profile for Network Devices, version 2.1, dated 24 September 2018* [4] also referred to as the Network Device collaborative Protection Profile (NDcPP). It presents a summary of the NDcPP and the evaluation results.

The evaluation was conducted concurrently with the following AISEP evaluation tasks, all of which claimed exact conformance to NDcPP v2.1:

- EFT-T002: Junos OS 19.2R1 for MX204 and EX9251
- EFT-T004: Junos OS 19.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Series
- EFT-T005: Junos OS 19.2R1 for SRX1500, SRX4100, SRX4200 and SRX4600 Series

These Security Target (ST) evaluations addressed the base requirements of the NDcPP, as well as a few of the additional requirements contained in Appendices A and B.

The evaluation included all the applicable modifications to the cPP as specified by the Network iTC in their Interpretations published up to the date of this report.

The cPP was evaluated against the requirements of the following APE assurance components: APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1, APE_REQ.1 and APE_SPD.1. These components are specified in the NDcPP.

The evaluation determined that the NDcPP v2.1 is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this certification report has been evaluated at an AISEP approved evaluation facility using the *Common Methodology for IT Security Evaluation (Version 3.1, Rev 5)* [3] for conformance to the *Common Criteria for IT Security Evaluation (Version 3.1, Rev 5)*. Because the STs contain only material drawn directly from the NDcPP, the majority of the ASE work units served to satisfy the APE work units as well.

The report concludes that the NDcPP has complied with the APE class assurance requirements of the Common Criteria and that the evaluation was conducted in accordance with the requirements of the Australasian Information Security Evaluation Program (AISEP).

The Australasian Certification Authority (ACA) recommends that:

- None.

This report includes information about the TOE, and information regarding the conduct of the evaluation.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluations (TOEs).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the evaluation of the *collaborative Protection Profile for Network Devices, version 2.1, dated 24 September 2018* [4] also referred to as the Network Device collaborative Protection Profile (NDcPP) against the requirements of the Common Criteria
- provide a source of information about the evaluation of the NDcPP for any interested parties.

Identification

The evaluation of the NDcPP was performed concurrently with the following AISEP evaluation tasks:

- EFT-T002: Junos OS 19.2R1 for MX204 and EX9251
- EFT-T004: Junos OS 19.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Series
- EFT-T005: Junos OS 19.2R1 for SRX1500, SRX4100, SRX4200 and SRX4600 Series

These evaluations addressed the base requirements of the NDcPP, as well as a few of the additional requirements contained in its optional and selection-based requirement sections.

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOEs	▪ collaborative Protection Profile for Network Devices, version 2.1, dated 24 September 2018 ▪ Junos OS 19.2R1 for MX204 and EX9251 ▪ Junos OS 19.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Series ▪ Junos OS 19.2R1 for SRX1500, SRX4100, SRX4200 and SRX4600 Series
Previously certified Protection Profile	Collaborative Protection Profile for Network Devices (NDcPP), Version 2.0 + Errata 20180314, 14 March 2018
STs (base)	*Security Target Junos OS 19.2R1 for MX204 and EX9251, v1.0, dated 9 September 2019*

	Security Target Junos OS 19.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX550M, SRX5400, SRX5600 and SRX5800 Series, v3.2, dated 14 June 2019 *Security Target Junos OS* 19.2R1 for SRX1500, SRX4100, SRX4200 and SRX4600 Series*, v3.2, dated 14 June 2019*
Evaluation Technical Report (Base)	*Evaluation Technical Report v1.0, dated 09 September 2019* Document reference EFT-T002-ETR 1.0
Evaluation Technical Report	*Evaluation Technical Report v1.0, dated 22 September 2019* Document reference EFT-T006-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Developer	Network international Technical Community
Evaluation facility	Teron Labs, Level 7, 221 London Circuit, Canberra, ACT 2601, Australia

The NDcPP contains a set of 'base' requirements that all conformant STs must include, and additionally contains 'optional' and 'selection-based' requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

Because the STs contain material drawn directly from the NDcPP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the evaluation facility performed the outlying APE work units as part of this evaluation.

Additionally, where possible, the evaluation of NDcPP v2.1 leverages analyses from the evaluation of NDcPP v2.0E [6], which are assumed to have been performed correctly. This approach is in agreement with Section 9.2.1 ('Re-using the evaluation results of certified PPs') of the CEM [3].

NDcPP description

Overview

The NDcPP describes security requirements for network-based devices, which in the context of this PP are defined as both hardware and software devices that are connected to the network and have an infrastructure role within the network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of the PP.

The NDcPP provides a minimal baseline of security requirements that are targeted at mitigating well defined and described threats in the following functional areas:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Communication (optional)

Security Problem Description, Objectives and Extended Components

Threats

The NDcPP defines a set of threats, assumptions and OSPs to be included in the ST of a compliant TOE.

Threats are defined in terms of a threat agent, asset and adverse action. The following table lists the applicable threats defined in the NDcPP.

Threat Name	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 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	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	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 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	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	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.

Assumptions

The table below lists the assumptions about the operational environment of the TOE defined by the NDcPP.

Assumption Name	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 a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	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 NDcPP. 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	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 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	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	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
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.

Organisational Security Policies

The following table lists the only organisational security policy defined by the NDcPP.

OSP Name	OSP Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Security Objectives

The NDcPP does not define any security objectives for the TOE, but it defines a set of objectives for the operational environment, which are listed below:

Objective Name	Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures 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.

Extended Components Definition

The NDcPP defines the extended functional components as listed in table below. All other components in the NDcPP are from CC Part 2 or CC Part 3.

The evaluation determined that the extended components definition describes how each extended component is related to existing CC Part 2 components, families, and classes; and that it follows CC Part 2 as a model for presentation. This includes operations such as assignments, selections and refinements.

Each element in each extended component was determined to be measurable and states objective evaluation requirements, such that conformance or non-conformance can be demonstrated during the evaluation of a compliant TOE. To reach this conclusion, the evaluation relied upon a combination of results from evaluations EFT-T002, EFT-004 and EFT-T005, as well as direct review of the extended components definition in the PP and review of the evaluation activities defined in the Supporting Document for the NDcPP.

Component Identifier
FAU_GEN_EXT.1
FAU_STG_EXT.1
FAU_STG_EXT.2
FAU_STG_EXT.3
FAU_STG_EXT.4
FCO_CPC_EXT.1
FCS_DTLSC_EXT.1
FCS_DTLSC_EXT.2
FCS_DTLSS_EXT.1
FCS_DTLSS_EXT.2
FCS_HTTPS_EXT.1
FCS_IPSEC_EXT.1
FCS_NTP_EXT.1.
FCS_RBG_EXT.1
FCS_SSHC_EXT.1
FCS_SSHS_EXT.1
FCS_TLSC_EXT.1
FCS_TLSC_EXT.2
FCS_TLSS_EXT. 1
FCS_TLSS_EXT.2
FIA_PMG_EXT.1
FIA_UAU_EXT.2

FIA_UIA_EXT.1
FIA_X509_EXT.1.
FIA_X509_EXT.2
FIA_X509_EXT.3
FPT_APW_EXT.1
FPT_SKP_EXT.1
FPT_STM_EXT.1
FPT_TST_EXT.1
FPT_TST_EXT.2
FPT_TUD_EXT.1
FPT_TUD_EXT.2
FTA_SSL_EXT.1

Network iTC Interpretations

The evaluation included all modifications to the NDcPP and Supporting Document [5] specified by the Network iTC in their Interpretations published to date and listed in the table below:

Network Device Interpretation #	Description
201828 Rev2	Different Handling of TLS1.1 and TLS1.2
201801	FCS_TLSC_EXT.1.1, Test 2
201815	Fixing AES-CTR Mode Tests
201817	FCS_SSH*EXT.1.1 RFCs for AES-CTR
201820 Rev3	Manual installation of CRL (FIA_X509_EXT.2)
201826	FCS_CKM.2 and elliptic curve-based key establishment
201823	Reliance on external servers to meet SFRs

201835Rev2	RSA-based FCS_CKM.2 Selection
201827	Handling Certification of Cloud Deployments
201818	local vs. remote administrator accounts
201829	for Applicability of FIA_AFL.1 to key-based SSH authentication
201827 Rev2	Redundant assurance activities associated with FAU_GEN.1
201832	FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused
201836	FCS_SSHS_EXT.1.5 SFR and AA discrepancy
201840	Clarification about application of Rfi#201726rev2
201908	NDcPP v2.1 Clarification - FCS_SSHC/S_EXT.1.5
201910	Cut-and-paste Error for Guidance AA

Security Requirements

Requirements in the NDcPP are comprised of mandatory 'base', optional and selection-based SFRs, and these requirements are listed in tables below.

The following table contains the 'base' requirements that were evaluated as part of a ST and PP evaluation.

Requirements Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FAU_GEN.2: User Identity Association	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FAU_STG_EXT.1FAU_STG_EXT.1: Protected Audit Event Storage	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_CKM.2: Cryptographic Key Establishment	PP evaluation, EFT-T002, EFT-T004 and EFT-T005

	FCS_CKM.4: Cryptographic Key Destruction	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_RBG_EXT.1: Random Bit Generation	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Management	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FIA_PMG_EXT.1: Password Management	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FIA_UIA_EXT.1: User Identification and Authentication	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FIA_UAU_EXT.2: Password-based Authentication Mechanism	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FIA_UAU.7: Protected Authentication Feedback	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behaviour	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FMT_MTD.1/CoreData: Management of TSF Data	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FMT_SMF.1: Specification of Management Functions	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FMT_SMR.2: Restrictions on Security Roles	PP evaluation, EFT-T002, EFT-T004 and EFT-T005

FTA: TOE Access	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FPT_APW_EXT.1: Protection of Administrator Passwords	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FPT_TST_EXT.1: TSF Testing	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FPT_TUD_EXT.1: Trusted Update	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FPT_STM_EXT.1: Reliable Time Stamps	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
FTP: Trusted Path/Channels	FTA_SSL_EXT.1: TSF-initiated Session Locking	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FTA_SSL.3: TSF-initiated Termination	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FTA_SSL.4: User-initiated Termination	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FTA_TAB.1: Default TOE Access Banners	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FTP_TRP.1/Admin: Trusted Path	PP evaluation, EFT-T002, EFT-T004 and EFT-T005

The following table contains the optional requirements that were evaluated as part of a ST evaluation and/or PP evaluation.

Requirements Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected audit trail storage	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FAU_STG_EXT.2/LocSpace: Counting lost audit data	PP evaluation

	FAU_STG.3/LocSpace: Action in case of possible audit data loss	PP evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certificate Validation	PP evaluation
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection	PP evaluation
FTP: Trusted Path/Channels	FTP_TRP.1/JoinFTP_TRP.1/Join: Trusted Path	PP evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP evaluation

The following table contains the selection-based requirements that were evaluated as part of a ST evaluation and/or PP evaluation.

Requirements Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN_EXT.1: Security Audit Data Generation for Distributed TOE component	PP evaluation
	FAU_STG_EXT.3: Protected Local Audit Event Storage for Distributed TOEs	PP evaluation
	FAU_STG_EXT.4: Protected Remote Audit Event Storage for Distributed TOEs	PP evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	PP evaluation, EFT-T004 and EFT-T005
	FIA_X509_EXT.2: X.509 Certificate Authentication	PP evaluation, EFT-T004 and EFT-T005
	FIA_X509_EXT.3: X.509 Certificate Requests	PP evaluation, EFT-T004 and EFT-T005
FCS: Cryptographic Support	FCS_DTLSC_EXT.1: DTLS Client Protocol	PP evaluation
	FCS_DTLSC_EXT.2: DTLS Client Protocol – with authentication	PP evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol	PP evaluation

	FCS_DTLSS_EXT.2: DTLS Server Protocol with mutual authentication	PP evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	PP evaluation
	FCS_IPSEC_EXT.1: IPsec Protocol	PP evaluation
	FCS_NTP_EXT.1: NTP Protocol	PP evaluation
	FCS_SSHC_EXT.1: SSH Client Protoco	PP evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FCS_TLSC_EXT.1: TLS Client Protocol	PP evaluation
	FCS_TLSC_EXT.2: TLS Client Protocol with authentication	PP evaluation
	FCS_TLSS_EXT.1: TLS Server Protocol	PP evaluation
	FCS_TLSS_EXT.2: TLS Server Protocol with mutual authentication	PP evaluation
FPT: Protection of the TSF	FPT_TST_EXT.2: Self-tests based on certificates	PP evaluation
	FPT_TUD_EXT.2: Trusted Update based on certificates	PP evaluation
FMT: Security Management	FMT_MOF.1/AutoUpdate: Management of security functions behaviour	PP evaluation
	FMT_MOF.1/Service: Management of security functions behaviour	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FMT_MOF.1/Functions: Management of security functions behaviour	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
	FMT_MTD.1/CryptoKeys: Management of TSF data	PP evaluation, EFT-T002, EFT-T004 and EFT-T005

Appendix E of the NDcPP provides the SFR dependency rationale. Each SFR in the cPP that has one or more dependencies of another SFR has those dependencies satisfied by the SFRs defined within the cPP.

Assurance Requirements

The following table lists the assurance requirements contained in the NDcPP and that were evaluated as part of ST evaluations.

Requirements Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	EFT-T002, EFT-T004 and EFT-T005
	ASE_ECD.1: Extended Components Definition	EFT-T002, EFT-T004 and EFT-T005
	ASE_INT.1: ST Introduction	EFT-T002, EFT-T004 and EFT-T005
	ASE_OBJ.1: Security Objectives for the Operational Environment	EFT-T002, EFT-T004 and EFT-T005
	ASE_REQ.1: Stated Security Requirements	EFT-T002, EFT-T004 and EFT-T005
	ASE_SPD.1: Security Problem Definition	EFT-T002, EFT-T004 and EFT-T005
	ASE_TSS.1: TOE Summary Specification	EFT-T002, EFT-T004 and EFT-T005
ADV: Development	ADV_FSP.1 Basic Functional Specification	EFT-T002, EFT-T004 and EFT-T005
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	EFT-T002, EFT-T004 and EFT-T005
	AGD_PRE.1: Preparative Procedures	EFT-T002, EFT-T004 and EFT-T005
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	EFT-T002, EFT-T004 and EFT-T005
	ALC_CMS.1: TOE CM Coverage	EFT-T002, EFT-T004 and EFT-T005
ATE: Tests	ATE_IND.1: Independent Testing – conformance	EFT-T002, EFT-T004 and EFT-T005
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	EFT-T002, EFT-T004 and EFT-T005

Evaluation

Overview

This chapter contains information about the procedures used in conducting the cPP evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDcPP [4] and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [12].

The evaluation was performed with the first product evaluation against the NDcPP requirements. In this case, the TOE for this first product was the *Junos OS 19.2R1 for MX204 and EX9251*, based on its Security Target (ST) [8].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [11].

Results

The evaluation results for the APE requirements as verified by the APE and ASE work units are listed in the table below:

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	PP evaluation
APE_ECD.1	Pass	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
APE_INT.1	Pass	PP evaluation
APE_OBJ.1	Pass	PP evaluation
APE_REQ.1	Pass	PP evaluation, EFT-T002, EFT-T004 and EFT-T005
APE_SPD.1	Pass	PP evaluation

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of the collaborative Protection Profile for Network Devices (NDcPP).

Because the STs contain material drawn directly from the NDcPP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the evaluation facility performed the outlying APE work units as part of this evaluation.

The ST evaluations addressed the base requirements of the NDcPP, as well as a few of the additional requirements contained in optional and selection-based requirements tables above.

Additionally, where possible, the evaluation of NDcPP v2.1 leverages analyses from the evaluation of NDcPP v2.0E [6], which are assumed to have been performed correctly. This approach is in agreement with Section 9.2.1 ('Re-using the evaluation results of certified PPs') of the CEM [3].

Certification result

After due consideration of the conduct of the evaluation as reported to the certifier and of the Evaluation Technical Report [10], the Australasian Certification Authority **certifies** the evaluation of the collaborative Protection Profile for Network Devices (NDcPP) version 2.1 performed by the Australasian Information Security Evaluation Facility (AISEF), Teron Labs.

The AISEF Teron Labs **has determined** that the collaborative Protection Profile for Network Devices (NDcPP) version 2.1 uphold the APE assurance requirements of the Common Criteria Part 3.

Recommendations

The Australasian Certification Authority (ACA) recommends that:

- None.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. *collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 24 September 2018*
5. *Supporting Document, Evaluation Activities for Network Device cPP, Version 2.1, September-2018*
6. *Collaborative Protection Profile for Network Devices (NDcPP), Version 2.0 + Errata 20180314, 14 March 2018*
7. *Supporting Documents, Evaluation Activities for NDcPP2.0 + Errata 20180314, 14 March 2018*
8. *Security Target Junos OS 19.2 R1 for MX204 and EX9251, v1.0, 9 September 2019*
9. Evaluation Technical Report - *Junos OS 19.2R1 for MX204 and EX9251, v1.0, 9 September 2019*
10. Evaluation Technical Report – *collaborative Protection Profile for Network Devices, v1.1, 25 September 2019*
11. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
12. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/publications/aisep-policy-manual

Abbreviations

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
TOE	Target of Evaluation