Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Australasian Information Security Evaluation Program

# Certification Report
## PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019

Version 1.1, 08 December 2020

cyber.gov.au

# Table of contents

cyber.gov.au

# Executive summary

This report describes the findings of the evaluation of the *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019* [10] also referred to as CFG_NDcPP-FW_V1.3. It presents a summary of the CFG_NDcPP-FW_V1.3 and the evaluation results.

The CFG_NDcPP-FW_V1.3 brings together the requirements from the Base-PP *collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018* (NDcPP_V2.1) [6]  with those from the *PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27-September-2019* (FW_MOD_V1.3) [8].

The evaluation of CFG_NDcPP-FW_V1.3  was conducted concomitant with the AISEP evaluation task listed below which claimed conformance to the Protection Profiles (PPs) in CFG_NDcPP-FW_V1.3 as well as the greater functionality contained within the *PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version: 1.0* (CFG_NDcPP-FW-VPNGW_1.0) [15]. The CFG_NDcPP-FW-VPNGW_V1.0 also brings in the requirements of *PP-Module for Virtual Private Network (VPN) Gateways Version 1.0, 17-September-2019* (MOD_VPNGW_V1.0) [13]. The concomitant evaluation task was:

▪ EFT-T013: Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500.

The concomitant EFT-T013 task included all the security functional requirements (SFRs) from FW_MOD_V1.3 including the optional SFR "FFW_RUL_EXT.2 Stateful Filtering of Dynamic Protocols". The EFT-T013 evaluation carried out the relevant evaluation activities contained in the *Supporting Document, Mandatory Technical Document, Evaluation Activities for Network Device cPP Version 2.1* (NDcPP-SD_V2.1) [7] and the *Supporting Document, Mandatory Technical Document, Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module Version 1.3* (FW_MOD-SD_V1.3) [9].

The PP-Configuration CFG_NDcPP-FW_V1.3 was exercised on a first-use basis by the evaluation task EFT-013 described above.  On a more formal basis CFG_NDcPP-FW_V1.3 was evaluated against the requirements of the following ACE assurance components: ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.1, ACE_ECD.1, ACE_REQ.1, ACE_MCO.1, ACE_CCO.1. These components are specified in the Common Criteria Part 3, Version 3.1, Rev 5 [2]. The evaluation determined that the CFG_NDcPP-FW_V1.3 is both Common Criteria Part 2 Extended and Part 3 Conformant. The evaluators have followed the *Common Methodology for IT Security Evaluation, Version 3.1, Rev 5* [3].

The report concludes that the CFG_NDcPP-FW_V1.3 has complied with the ACE 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 the identification of the Target of Evaluation (TOE).

## Purpose

The purpose of this Certification Report is to:

- report the certification of results of the evaluation of the *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3 dated 27 September 2019* [10] also referred to as CFG_NDcPP-FW_V1.3 against the requirements of the Common Criteria

- provide a source of information about the evaluation of the CFG_NDcPP-FW_V1.3 for any interested parties.

## TOE Identification

PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3 dated 27 September 2019

## Identification of related and concomitant evaluations

The evaluation of the CFG_NDcPP-FW_V1.3 was also performed as a basis for the related follow-on AISEP evaluation task:

- EFT-T021: PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020

The evaluation of the CFG_NDcPP-FW_V1.3 was performed concomitant with the following AISEP evaluation task:

- EFT-T013: Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500

The EFT-T013 evaluation gathered requirements from the Base-PP NDcPP_V2.1, the PP-Modules FW_MOD_V1.3 and MOD_VPNGW_V1.0, as well as requirements from the Intrusion Prevention System Extended Package [16].

| Description | Version |
| --- | --- |

| | |
|---|---|
| Evaluation scheme | Australasian Information Security Evaluation Program |
| TOE | ▪ *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3, 27-September-2019* |
| Previously certified Protection Profile | collaborative Protection Profile for Network Devices , Version 2.1, 24 September 2018  (AISEP certified) |
| Concomitant evaluation TOE details | ▪ Security Target for Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500, Version 1.4,  02 November 2020<br><br>▪ Evaluation Technical Report – Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 v1.0,  dated 06 November 2020 (Document reference EFT-T013-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 (CEM) [3] |
| Developer | NDFW international Technical Community (NDFW iTC) |
| Evaluation facility | Teron Labs Pty Ltd<br>Unit 3, 10 Geils Court<br>Deakin ACT 2600<br>Australia |

The CFG_NDcPP-FW_V1.3 gathers together the security problem definition, security objectives, security requirements and evaluation methodology of the Base-PP NDcPP_V2.1 [6] and the PP-Module FW_MOD_V1.3 [8].  The next section of this report gives a summary of the gathered elements of these Common Criteria Protection Profiles.

Because the concomitant TOE evaluation contains material from the Base-PP NDcPP_V2.1 [6] and the PP-Module FW_MOD_V1.3 [8] that appeared to be mutually consistent for evaluation purposes it provides extra practical evidence that the PP-Configuration can be used as the basis for a security product evaluation.

Additionally, where possible, the evaluation of CFG_NDcPP-FW_V1.3 leverages analyses from the recent evaluation of NDcPP_V2.1, which is 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].

# CFG_NDcPP-FW description

## Overview

The PP-Configuration CFG_NDcPP-FW_1.3 describes security requirements for network-based devices with a stateful firewall function. In the context of this PP-Configuration these devices are defined as both hardware and software devices that are connected to the network and have a stateful firewall function 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-Configuration.

The PP-Configuration CFG_NDcPP-FW_V1.3 calls-in a set of security requirements that are targeted at mitigating well defined and described threats.

## Security Problem Definition

The Threats, Organisational Security Policies and Assumptions called in by the PP-Configuration CFG_NDcPP-FW_V1.3 are listed below.  To make it stand out more, material in the table below introduced from the FW_MOD_V1.3 or modified by it is shown in GREEN. The Security Problem Definition aspects of the CFG_NDcPP-FW_V1.3 were examined as part of the sub-activity ACE_SPD.1 evaluation. Consistency aspects were examined as part of the sub-activity ACE_MCO.1 evaluation.

| Threat, OSP or Assumption | Keywords | Source |
|---|---|---|
| **Threats** | | |
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | Threat Agent gains admin | NDcPP S4.1.1.1 |
| T.WEAK_CRYPTOGRAPHY | Encryption, brute force | NDcPP S4.1.1.2 |
| T.UNTRUSTED_COMMUNICATION_CHANNELS | Protocols, Key management | NDcPP S4.1.1.3 |
| T.WEAK_AUTHENTICATION_ENDPOINTS | Shared/plaintext passwords | NDcPP S4.1.1.4 |
| T.UPDATE_COMPROMISE | Non-validated updates | NDcPP S4.1.2.1 |
| T.UNDETECTED_ACTIVITY | Audit | NDcPP S4.1.3.1 |
| T.SECURITY_FUNCTIONALITY_COMPROMISE | Credentials | NDcPP S4.1.4.1 |
| T.PASSWORD_CRACKING | Weak | NDcPP S4.1.4.2 |
| T.SECURITY_FUNCTIONALITY_FAILURE | Self-test | NDcPP S4.1.5.1 |

| | | |
|---|---|---|
| T.NETWORK_DISCLOSURE | Map addresses/ports | FW_MOD S4.1.1.1 |
| T.NETWORK_ACCESS | Attacks against services | FW_MOD S4.1.2.1 |
| T.NETWORK_MISUSE | services | FW_MOD S4.1.3.1 |
| T.MALICIOUS_TRAFFIC | Malformed, crash, replay | FW_MOD S4.1.4.1 |

**Organizational Security Policy**

| | | |
|---|---|---|
| P.ACCESS_BANNER | Describing restrictions | NDcPP S4.3.1 |

**Assumptions**

| | | |
|---|---|---|
| A.PHYSICAL_PROTECTION | Not subject to physical attack | NDcPP S4.2.1 |
| A.LIMITED_FUNCTIONALITY | Not general purpose | NDcPP S4.2.2 |
| A.NO_THRU_TRAFFIC_PROTECTION | This device endpoint only | NDcPP S4.2.3 |
| A.TRUSTED_ADMINISTRATOR | Act in best interest | NDcPP S4.2.4 |
| A.REGULAR_UPDATES | Firmware and software | NDcPP S4.2.5 |
| A.ADMIN_CREDENTIALS_SECURE | Protected by the platform | NDcPP S4.2.6 |
| A.COMPONENTS_RUNNING | Distributed TOEs availability | NDcPP S4.2.7 |
| A.RESIDUAL_INFORMATION | Keys discarded equipment | NDcPP S4.2.8 |
| A.NO_THRU_TRAFFIC_PROTECTION | Does not apply to FW ports | FW_MOD S4.2 |

# Security Objectives

The NDcPP_V2.1 [6] is written in a way that does not state TOE Objectives, so the only NDcPP_V2.1 objectives stated are objectives on the environment that meet NDcPP_V2.1 assumptions. As far as TOE requirements are concerned the NDcPP_V2.1 maps directly from threats and OSPs to security requirements. The PP-Module FW_MOD_V1.3 [8] uses a different approach and does introduce TOE objectives.

The security objectives called in by the PP-Configuration CFG_NDcPP-FW_V1.3 are listed below. To make it stand out more, objectives from the PP-Module FW_MOD_V1.3 are shown in GREEN. The Security Objectives aspects of the CFG_NDcPP-FW_V1.3 were examined as part of the sub-activity ACE_OBJ.1 evaluation. Consistency aspects were examined as part of the sub-activity ACE_MCO.1 evaluation.

| Objective | Keywords | Source |
|---|---|---|
| **Objectives on the TOE** | | |
| O.* | None stated, refer to NDcPP threats and OSP | NDcPP |
| O.RESIDUAL_INFORMATION **(*)** | Clear packet buffers | FW_MOD S5.1.1 |
| O.STATEFUL_TRAFFIC_FILTERING | Rules, interface, deny, flow | FW_MOD S5.1.2 |
| **Objectives on the Environment** | | |
| OE.PHYSICAL | Commensurate TOE value | NDcPP S5.1.1 |
| OE.NO_GENERAL_PURPOSE | Only necessary services | NDcPP S5.1.2 |
| OE.NO_THRU_TRAFFIC_PROTECTION | Traversing traffic out of scope | NDcPP S5.1.3 |
| OE.TRUSTED_ADMIN | Follow guidance, monitor certs | NDcPP S5.1.4 |
| OE.UPDATES | Firmware, software regular | NDcPP S5.1.5 |
| OE.ADMIN_CREDENTIALS_SECURE | Private keys protected | NDcPP S5.1.6 |
| OE.COMPONENTS_RUNNING | Distributed TOEs only | NDcPP S5.1.7 |
| OE.RESIDUAL_INFORMATION **(*)** | Keys discarded equipment | NDcPP S5.1.8 |
| OE.NO_THRU_TRAFFIC_PROTECTION | Does not apply for FW ports | FW_MOD S5.2 |

*(*) - O.RESIDUAL_INFORMATION and OE.RESIDUAL_INFORMATION are not related*

# Security Functional Requirements

The SFR summary table below is broken into 3 groupings:  Mandatory Requirements, Optional Requirements and Selection based requirements. The Common Criteria convention of using alphabetical ordering is respected inside each grouping.  To make it stand out more, material in the table below from the PP-Module FW_MOD_V1.3 is shown in GREEN.  The Security Functional Requirement aspects of the CFG_NDcPP-FW_V1.3 were examined as part of the sub-activities ACE_ECD.1 and ACE_REQ.1 evaluation.  Consistency aspects were examined as part of the sub-activities ACE_MCO.1 evaluation.

| SFR (Family or Component) | Keywords | Source |
|---|---|---|
| **Mandatory Requirements** | | |
| FAU_GEN.1.* | Audit data generation | NDcPP |
| FAU_GEN.1.* | Extra events and info | FW_MOD |
| FAU_GEN.2.1 | User identity association | NDcPP |
| FAU_STG_EXT.1.* | Protected external store | NDcPP |
| FCS_CKM.(1,2,4).* | Generation, establishment, destruction | NDcPP |
| FCS_COP.1.1/DataEncryption | AES, CBC, CTR, GCM | NDcPP |
| FCS_COP.1.1/SigGen | DSA, ECDSA | NDcPP |
| FCS_COP.1.1/Hash | SHA | NDcPP |
| FCS_COP.1.1/KeyedHash | HMAC-SHA | NDcPP |
| FCS_RBG_EXT.1.* | Deterministic, seeded | NDcPP |
| FDP_RIP.2.1 | Buffers cleared | FW_MOD |
| FFW_RUL_EXT.1.* | Stateful rules | FW_MOD |
| FIA_AFL.1.* | Authentication failure management | NDcPP |
| FIA_PMG_EXT.1.1 | Password management | NDcPP |

| | | |
|---|---|---|
| FIA_UIA_EXT.1.* | Identified, authenticated | NDcPP |
| FIA_UAU_EXT.2.1 | Local password | NDcPP |
| FIA_UAU.7.1 | Console obscured feedback | NDcPP |
| FMT_MOF.1.1/ManualUpdate | Security administrators initiate | NDcPP |
| FMT_MTD.1.1/CoreData | Security administrators manage | NDcPP |
| FMT_SMF.1.1 | Management functions | NDcPP |
| FMT_SMF.1.1/FFW | Manage firewall rules | FW_MOD |
| FMT_SMR.2.* | Security administrator role | NDcPP |
| FPT_SKP_EXT.1.1 | Protect keys | NDcPP |
| FPT_APW_EXT.1.* | Passwords protected | NDcPP |
| FPT_TST_EXT.1.1 | A suite of self tests | NDcPP |
| FPT_TUD_EXT.1.* | Query, initiate, authenticate | NDcPP |
| FPT_STM_EXT.1.* | Time stamps | NDcPP |
| FTA_SSL_EXT.1.1 | Session locking | NDcPP |
| FTA_SSL.(3,4).1 | Session termination | NDcPP |
| FTA_TAB.1.1 | Access banner | NDcPP |
| FTP_ITC.1.* | Encrypted trusted channel | NDcPP |
| FTP_TRP.1.*/Admin | Encrypted trusted path | NDcPP |

**Optional Requirements**

| | | |
|---|---|---|
| FAU_STG.1.* | Protected audit store | NDcPP |

| | | |
|---|---|---|
| FAU_STG_EXT.2.1/LocSpace | Counting lost audit data | NDcPP |
| FAU_STG.3.1/LocSpace | Audit store overflow | NDcPP |
| FFW_RUL_EXT.2.1 | Dynamic protocols | FW_MOD |
| FIA_X509_EXT.1.*/ITT | Validation chain, basicConstraints | NDcPP |
| FPT_ITT.1.1 | Crypto distributed TOE | NDcPP |
| FTP_TRP.1.*/Join | Distributed TOE joining components | NDcPP |
| FCO_CPC_EXT.1.* | Distributed TOE control components | NDcPP |

**Selection Based Requirements**

| | | |
|---|---|---|
| FAU_GEN_EXT.1.1 | Distributed TOE records | NDcPP |
| FAU_STG_EXT.(3,4).1 | Distributed TOE protected stores | NDcPP |
| FCS_DTLSC_EXT.*.* | DTLS client crypto, protocols, authentication | NDcPP |
| FCS_DTLSS_EXT.*.* | DTLS server crypto, protocols, mutual authentication | NDcPP |
| FCS_HTTPS_EXT.1.* | RFC 2818, TLS | NDcPP |
| FCS_IPSEC_EXT.1.* | RFC 4301, crypto, modes, | NDcPP |
| FCS_NTP_EXT.1.* | Authenticated time update | NDcPP |
| FCS_SSHC_EXT.1.* | SSH Client | NDcPP |
| FCS_SSHS_EXT.1.* | SSH Server | NDcPP |
| FCS_TLSC_EXT.*.* | TLS Client | NDcPP |
| FCS_TLSS_EXT.*.* | TLS Server | NDcPP |

| | | |
|---|---|---|
| FIA_X509_EXT.1.*/Rev | X.509 Certificate Validation | NDcPP |
| FIA_X509_EXT.(2,3).* | Authentication, requests | NDcPP |
| FPT_TST_EXT.2.1 | Self-tests certificates | NDcPP |
| FPT_TUD_EXT.2.* | Trusted update certificates | NDcPP |
| FMT_MOF.1.1/* | Management by security administrators | NDcPP |
| FMT_MTD.1.1/CryptoKeys | Security administrators manage keys | NDcPP |

## Security Assurance Requirements

The SAR summary table below simply lists the SARs from the Base-PP NDcPP_V2.1.  The PP-Module FW_MOD_V1.3 inherits the NDcPP_V2.1 SARs.  There is a case of an implied change in scope of the ASE_OBJ.1 component when FW_MOD_V1.3 is incorporated because it introduces Objectives on the TOE.  Table 3 of the NDcPP_V2.1 only indicates Security Objectives on the operational environment are applicable for the ASE_OBJ.1 component.  In the context of the CFG_NDcPP-FW_V1.3 the scope of the ASE_OBJ.1 component would logically include Security Objectives on the TOE.

| SAR | Keywords |
|---|---|
| ASE_CCL.1 | Conformance claims |
| ASE_ECD.1 | Extended components definition |
| ASE_INT.1 | ST introduction |
| ASE_OBJ.1 | Security objectives |
| ASE_REQ.1 | Stated security requirements |
| ASE_SPD.1 | Security problem Definition |
| ASE_TSS.1 | TOE summary specification |
| ADV_FSP.1 | Basic Functional Specification |
| AGD_OPE.1 | Operational User Guidance |

| | |
|---|---|
| AGD_PRE.1 | Preparative procedures |
| ALC_CMC.1 | TOE labelling |
| ALC_CMS.1 | TOE CM coverage |
| ATE_IND.1 | Independent testing - conformance |
| AVA_VAN.1 | Vulnerability survey – basic attack potential |

# Evaluation

## Overview

This chapter contains information about the procedures used in conducting the PP-Configuration CFG_NDcPP-FW_V1.3 evaluation.  It also describes the concomitant network device evaluation that contributed to the PP-Configuration evaluation.

## Evaluation procedures

The evaluation was performed on the *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3*, developed by the Network Device Fundamentals and Firewalls (NDFW) international Technical Community (iTC).

The PP components of the evaluated configuration profiles are:

- Base-PP: collaborative Protection Profile for Network Devices, Version 2.1, 24-September-2018 (NDcPP_V2.1)

- PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27-September-2019 (MOD_FW_V1.3)

The evaluation included all the applicable modifications to the above PP-Module as specified by the NDFW iTC in their interpretations published up to the date of the evaluation.

The evaluation process for the PP-Configuration consisted of its evaluation against the requirements of the assurance class ACE defined in Common Criteria Part 3 [2].

Some of these ACE assurance components simply call-in similar APE class components.  These call-ins are listed in the table below:

| ACE Component | APE Call-in |
| --- | --- |
| ACE_INT.1 | APE_INT.1 |
| ACE_SPD.1 | APE_SPD.1 |
| ACE_OBJ.1 | APE_OBJ.2 |

A concomitant product evaluation provided extra practical assurance on the consistency of the evaluation methodology associated with the PP-Configuration. Due to the presence of optional and selection based SFRs in the NDcPP_V2.1 that were not used in the product evaluation, only a subset of the possible evaluation methodology was exercised on this first-use basis.

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [23].

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 [4].

For consideration of the aspects of the evaluation concerning exact conformance the DRAFT document – "CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs  May 2017, Version 0.5" [5] was referenced.

## Concomitant product evaluation procedures

The PP-Configuration evaluation was performed concomitant with the AISEP evaluation task EFT-T013 involving a network security appliance with stateful firewall and VPN gateway functionality.  The relevant criteria against which the EFT-T013 Target of Evaluation (TOE) has been evaluated are contained in the NDcPP_V2.1 [6], FW_MOD_V1.3[8], MOD_VPNGW_V1.0 [13] and the *Common Criteria, Version 3.1, Rev 5, Parts 2 and 3* [1, 2].

Relevant testing methodology was drawn from the NDcPP-SD_V2.1 [7], FW_MOD-SD_V1.3 [9], MOD_VPNGW-SD_V1.0 [14] and the *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* (CEM) [3].

Functional tests were developed to provide a suitable and achievable coverage of the security functions claimed by the TOE.  Testing was developed against the chosen subset of requirements taken from the Protection Profiles, using tests as specified in the relevant supporting documents.

Vulnerability assessments made against the CFG_NDcPP-FW_V1.3 are primarily based on the methodology specified in NDcPP-SD_V2.1.  The NDcPP-SD_V2.1 evaluation activities are provided in an effort to specify an adequate level of vulnerability testing. More details can be found in the NDcPP_V2.1 and NDcPP-SD_V2.1 documents.  The FW_MOD-SD_V1.3 document added some extra considerations for the AVA_VAN.1 evaluation activities.

# 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 *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3* [10]. The successful certification provides assurance that the PP-Configuration is sound and consistent. It can be used to specify Security Targets (STs) for network devices with a stateful firewall function.

It is expected that any product using the CFG_NDcPP-FW_V1.3 as a model will be resistant to attackers with basic attack potential, have well defined auditing and management functions, can be remotely managed in a secure way, has protected firmware update functionality, does not leak information between machines on the network and importantly, can provide stateful firewall functions that are essential to protect resources on interconnected computer networks.

Additionally, where possible, the evaluation of CFG_NDcPP-FW_V1.3 leveraged analyses from the evaluation of NDcPP V2.1 [6] which are assumed to have been carried out 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 certifiers, and of the Evaluation Technical Report [20], the Australasian Certification Authority **certifies** the evaluation of the *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3* performed by the Australasian Information Security Evaluation Facility, Teron Labs.

The AISEF Teron Labs **has determined** that *the PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3* upholds the ACE assurance requirements of the Common Criteria Part 3 [2].

## Recommendations

The Australasian Certification Authority 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.      Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014

5.      CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs  May 2017, Version 0.5  CCDB-2017-05-xxx

6.      collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018, (NDcPP V2.1)

7.      Supporting Document, Mandatory Technical Document, Evaluation Activities for Network Device cPP, September 2018, version 2.1 (NDcPP-SD_V2.1)

8.      PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 (FW_MOD_V1.3)

9.      Supporting Document, Mandatory Technical Document, Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, September 2019, Version 1.3 (FW_MOD-SD_V1.3)

10.     PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.3, 27-September-2019 (CFG_NDcPP-FW_V1.3)

11.     NDFW iTC allowed-with list for Network Device cPP,  V2.1r8, 01 July 2020  (available as PDF to members at CC Users Forum/Documents/Projects/Network ITC/Allowed-With Lists)

12.     NDFW iTC allowed-with list for Stateful Traffic Filter Firewall PP-Module V1.4r5, 01 July 2020 (available as PDF to members at CC Users Forum/Documents/Projects/Network ITC/Allowed-With Lists)

13.     PP-Module for Virtual Private Network (VPN) Gateways, version 1.0, dated 2019-09-17 (MOD_VPNGW_V1.0)

14.     Supporting Document, Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Gateways, version 1.0, dated 2019-09-17, (MOD_VPNGW-SD_V1.0)

15.     PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version: 1.0, 2020-03-06  (CFG_NDcPP-FW-VPNGW_V1.0)

16.     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 (IPS_EP)

17.     Certification Report, Collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 19 September 2018, Version 1.0, 02 October 2019

18.     Security Target for Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380, SRX1500 , V1.4, 02 November 2020

19.     Evaluation Technical Report - Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 v1.0, dated 06 November 2020  (Document reference EFT-T013-ETR 1.0)

20. *Evaluation Technical Report – PP-Configuration for Network Device and Stateful Traffic Filter Firewalls v1.0, dated 03 November 2020*  (Document reference EFT-T020-ETR 1.0*)*

21. *Australian Government Information Security Manual: https://www.cyber.gov.au/ism*

22. *New Zealand Information Security Manual: https://www.nzism.gcsb.govt.nz/ism-document/*

23. *AISEP Policy Manual (APM): https://www.cyber.gov.au/publications/aisep-policy-manual*

## Abbreviations

| | |
|---|---|
| AISEF | Australasian Information Security Evaluation Facility |
| AISEP | Australasian Information Security Evaluation Program |
| ASD | Australian Signals Directorate |
| CCRA | Common Criteria Recognition Arrangement |
| DTLS S/C | Datagram Transport Layer Security Server/Client |
| HTTPS | HyperText Transfer Protocol Secure |
| IPsec | Internet Protocol Security |
| NDcPP | CCRA-approved collaborative Protection Profile for Network Devices |
| NDFW iTC | Network Device Fundamentals and Firewalls international Technical Community |
| NTP | Network Time Protocol |
| PP | Protection Profile |
| SSH S/C | Secure SHell Server/Client |
| TLS S/C | Transport Layer Security Server/Client |
| TOE | Target of Evaluation |
| VPN | Virtual Private Network |