Australian Government
Department of Defence

Australasian Information Security Evaluation Program (AISEP)

Network Device Protection Profile (NDPP) Extended Package for Intrusion Prevention Systems (IPS EP) Version 1.0, dated 26 June 2014

Certification Report
2017/108

12-April-2017
Version 1.0

Amendment Record

Version	Date	Description
0.1	06 April 2017	Internal
0.2	12 April 2017	Minor update from internal review
1.0	12 April 2017	External release

Executive Summary

This report describes the findings of the IT security evaluation of the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) against the APE class as defined in chapter 10 of CC Part 3 (Ref. 4).

The Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) (the TOE) (Ref. 2) is an extended package for the Network Device Protection Profile (Ref. 1). The IPS EP augments the base functionality of NDPP-compliant TOEs by providing intrusion prevention/detection capabilities.

This evaluation addressed the base and additional requirements of the IPS EP. Since the IPS EP is an extended package of the Network Device Protection Profile (NDPP), this evaluation also included requirements from this PP, although this is outside the scope of this certification report.

The evaluation of the IPS EP was performed with the first product evaluation against the EP's requirements. In this case the TOE for this first product was the Juniper Networks, Inc. Junos 12.3 X48-D30 for SRX Platforms.

The report concludes that the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) 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 evaluation was performed by BAE Systems Applied Intelligence and was completed on 31 March 2017.

The Australasian Certification Authority (ACA) recommends that:

- Compliant TOE **must** update the objectives and mappings between objectives/SFRs and other amendments in line with NIAP Technical Decision TD 0162 (Ref. 6).

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

Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and the identity information of the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) against the requirements of the Common Criteria (CC)

b) Provide a source of security information about the TOE for any interested parties.

1.3 Identification

The TOE is the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS), version 1.0 (IPS EP).

The IPS EP contains a set of “base” requirements that all conformant STs must include as well as “additional” requirements that are conditionally expected to be included if conformant TOEs provide that capability. The vendor may choose to include such requirements in the ST and still claim conformance to this EP. Since this is an extended package of the NDPP, the ST and TOE must also claim conformance to the “base” NDPP, which includes any applicable optional requirements from that PP.

The evaluation of the IPS EP was performed with the first product evaluation against the EP’s requirements. In this case the TOE for this first product was the Juniper Networks, Inc. Junos 12.3 X48-D30 for SRX Platforms.

The EP’s optional requirements may not be included in a particular ST; however, the initial evaluation that was performed (and subsequently used as a basis for this report) included the optional requirements; therefore, the report has been written with respect to both the base and additional requirements of the EP.

Because the ST contains material drawn directly from the IPS EP, 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 lab performed the outlying APE work units as part of this evaluation. Note that the ST also contains materials from the base NDPP that the IPS EP is an extension of. Items in the ST that were taken from the base NDPP and do not relate to the IPS EP were not examined for this report.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS)
Version	1.0, dated 26 June 2014
Evaluation Technical Report	Evaluation Technical Report - NDPP Extended Package for Intrusion Prevention Systems Version 1.0, dated 31 March 2017
ST (base)	Junos 12.3 X48-D30 for SRX Series Platforms. Version 1.1, dated 09 February 2017
ETR (base)	Evaluation Technical Report Junos 12.3 X48-D30 for SRX Series Platforms, dated 11 November 2016
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, September 2012, Version 3.1.Rev 4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev 4
Conformance	Common Criteria for IT Security Evaluation Version 3.1, Rev 4
Developer	National Information Assurance Partnership (NIAP) Department of Defense, National Security Agency, 9800 Savage Road, Fort Meade, MD 20755-6940, United States
Evaluation Facility (both ST and EP)	BAE Systems Applied Intelligence Level 1, 14 Childers Street Canberra ACT 2600

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE) and a description of functionalities provided.

2.2 Description of the TOE

The TOE is the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS).

The IPS EP specifically addresses network-based Intrusion Prevention Systems (IPS). A conformant IPS is a product that is connected to one or more distinct networks and is managed as part of an overall enterprise security solution. In particular, a compliant IPS provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious network traffic. The IPS EP is focused on inspecting IP traffic (TCP, UDP, ICMP, etc.).

2.3 TOE Functionality

The functionality defined in the Protection Profile that compliant TOEs may provide is as follows:

- **Audit Generation**

A compliant TOE generates audit log events for IPS events, including all dissimilar IPS events and reactions.
Each event log contains the date and time, type of event and specifically-defined auditable event information.

- **Security Management**

A compliant TOE allows administrators to perform a suite of management functions, including (but not limited to) enabling and disabling IPS signatures, modifying the parameters that define network traffic to be collected/analysed and the reaction(s) to be taken when a signature/anomaly match is detected.

- **Protection of the TSF**

A compliant TOE is able to preserve a secure state for inline interfaces in the event of defined failure events.

- **Resource Utilization**

A compliant TOE allows administrators to impose quotas on exhaustible resources (such as bandwidth).

- **Intrusion Prevention**

A compliant TOE provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious network traffic. The IPSEP is focused on inspecting IP traffic (TCP, UDP, ICMP, etc.).

Chapter 3 – IPS Extended Package description

3.1 Security Problem Definition

The IPS EP 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 threats are defined by the IPS EP:

- **T.NETWORK_DISCLOSURE**: Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
- **T.NETWORK_ACCESS**: Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information.
- **T.NETWORK_MISUSE**: Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. E.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools and botnets.
- **T.NETWORK_DOS**: Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources.

The following assumptions are defined by the IPSEP:

- **A.CONNECTIONS**: It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

The following organisational security policies (OSP) are defined by the IPSEP:

- **P.ANALYZ**: Analytical processes and information to derive conclusions about potential intrusions must be applied to IPS data and appropriate response actions taken.

3.2 Security Objectives

The IPS EP defines a set of objectives for compliant TOEs. These objectives are a superset of the objectives from the NDPP (Ref. 1) extended with additional IPS EP details; and new objectives defined for IPS EP-compliant TOEs.

The following objectives are defined for compliant TOEs:

- **O.IPSSENSE**: To be able to analyze and react to potential network policy violations, the IPS must be able to collect and store essential data elements of network traffic on monitored networks.
- **O.IPSANALYZE**: Entities that reside on or communicate across monitored networks must have network activity effectively analyzed for potential violations of approved network usage.

- The TOE must be able to effectively analyze data collected from monitored networks to reduce the risk of unauthorized disclosure of information, inappropriate access to services, and misuse of network resources.
- **O.IPSREACT**: The TOE must be able to react in real-time as configured by the IPS administrators to terminate and/or blocking traffic flows that have been determined to violate administrator-defined IPS policies.
- **O.TOE_ADMINISTRATION**: To address the issues involved with a trusted means of administration of the intrusion prevention capability this security objective, which originated in the NDPP, is extended as follows.

  Compliant TOEs will provide the functions necessary for an administrator to configure the IPS policies that are enforced by the TOE. Note it is assumed that use of the functions indicated below is protected in accordance with the requirements in the NDPP.

The following objectives are defined for the operational environment:

- **OE.CONNECTIONS**: TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.

3.3 Extended Components Definition

The IPS EP defines the following extended components:

- FAU_GEN.1(2)
- FMT_SMF.1(2)
- IPS_NTA_EXT.1
- IPS_IPB_EXT.1
- IPS_SBD_EXT.1
- IPS_ABD_EXT.1.

FAU_GEN.1(2) and FMT_SMF.1(2) are extended versions of the base components declared in CC Part 2 (Ref. 3).

The IPS family of SFRs has been defined to allow for the definition of intrusion prevention functionality provided by IPS EP-compliant TOEs. No components within CC Part 2 were suitable for describing this functionality.

The IPS family of SFRs uses the existing families of components in 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 could be demonstrated during the evaluation of a compliant TOE.

3.4 Requirements

The statement of security requirements contained in the IPS EP (Ref. 2) described the Security Functional Requirements (SFRs). The SFRs were conformant to CC part 2, with the exception of the extended components as described in Section 3.3 above.

A single dependency, that of FAU_GEN.1(2) requiring FPT_STM.1, is implicitly met. As the IPS EP extends the NDPP (Ref. 1), which includes FPT_STM.1 as a mandatory SFR, any TOEs claiming conformance to both the NDPP and IPS EP will meet the dependency requirements.

The IPS EP does not define any SARs beyond those defined in the NDPP. TOE that is evaluated against this EP is inherently evaluated against the NDPP as well.

Section 7.1.4 of the IPS EP provides a rationale tracing each SFR to one or more objectives.
Note: The mapping above must be augmented/modified in line with NIAP Technical Decision TD0162 (Ref. 6).

The updated Table 7-4 as per TD0162 is shown below:

Table 2 Mapping of SPD to Security Objectives and SFRs

Threat, OSP or Assumption	**Security Objective(s)**	**SFRs**
A.CONNECTIONS	OE.CONNECTIONS	N/A
T.NETWORK_DISCLOSURE	O.IPSSENSE O.IPSANALYZE O.IPSREACT O.TOE_ADMINISTRATION	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1, FMT_SMF.1(2) **Optional SFRs**: FAU_ARP.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(2), FPT_FLS.1, FRU_RSA.1
T.NETWORK_ACCESS	O.IPSSENSE O.IPSANALYZE O.IPSREACT O.TOE_ADMINISTRATION	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1, FMT_SMF.1(2) **Optional SFRs**: FAU_ARP.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4,

		FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(2), FPT_FLS.1, FRU_RSA.1
T.NETWORK_MISUSE	O.IPSSENSE O.IPSANALYZE O.IPSREACT O.TOE_ADMINISTRATION	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1, FMT_SMF.1(2) **Optional SFRs**: FAU_ARP.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(2), FPT_FLS.1, FRU_RSA.1
T.NETWORK_DOS	O.IPSSENSE O.IPSANALYZE O.IPSREACT O.TOE_ADMINISTRATION	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1, FMT_SMF.1(2) **Optional SFRs**: FAU_ARP.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FMT_MOF.1, FMT_MTD.1(2), FMT_SMR.1(2), FPT_FLS.1, FRU_RSA.1
P.ANALYZ	O.IPSANALYZE	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1 **Optional SFRs:** FRU_RSA.1

Chapter 4 – Evaluation

4.1 Overview

This chapter contains information about the conduct and result of the evaluation.

4.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Refs. 3 and 4).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref. 5).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Ref. 7).

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 (Ref. 11).

The evaluation was performed with the first product evaluation against the EP's requirements. In this case the TOE for this first product was the Juniper Networks, Inc. Junos 12.3 X48-D30 for SRX Platforms based on its Security Target (ST) (Ref. 8).

4.3 Results summary

Table 3 - Summary of evaluation results

Work Package	Requirement	Verdict
Protection Profile Evaluation (APE)	APE_INT.1.1E	PASS
	APE_CCL.1.1E	PASS
	APE_SPD.1.1E	PASS
	APE_OBJ.2.1E	PASS
	APE_ECD.1.1E	PASS
	APE_ECD.1.2E	PASS
	APE_REQ.2.1E	PASS

Chapter 5 – Certification

5.1 Overview

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

5.2 Assurance

This certification is focused on the evaluation of the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS), version 1.0 (IPS EP).

Because the ST contains material drawn directly from the IPS EP, 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 lab performed the outlying APE work units as part of this evaluation. Note that the ST also contains materials from the base NDPP that the IPS EP is an extension of. Items in the ST that were taken from the base NDPP and do not relate to the IPS EP were not examined for this report.

5.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the Certifiers and of the Evaluation Technical Report (Ref. 10) the Australasian Certification Authority **certifies** the evaluation of the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS), version 1.0 (IPS EP) performed by the Australasian Information Security Evaluation Facility, BAE Applied intelligence.

The AISEF BAE Applied Intelligence **has determined** that the Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS), version 1.0 (IPS EP) uphold the APE assurance requirements of the Common Criteria Part 3.

5.4 Recommendations

The Australasian Certification Authority (ACA) recommends that:

- Compliant TOE **must** update the objectives and mappings between objectives/SFRs and other amendments in line with NIAP Technical Decision TD 0162 (Ref. 6).

Annex A – References and Abbreviations

A.1 References

1. US Government approved Protection Profile – Protection Profile for Network Devices (NDPP) version 1.1 June 8, 2012

2. Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS) Version 1.0 26 June 2014 (IPS EP)

3. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4

4. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

5. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1, Revision 4

6. NIAP 2017, TD0162 - Consistency of mapping between Security Objectives and SFRs, accessed 17-Mar-17, https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=166

7. AISEP Policy Manual Release: 30 August 2011 Version 4.0

8. Security Target - Junos 12.3 X48-D30 for SRX Series Platforms Version 1.1, 09 February 2017

9. Evaluation Technical Report - JUNOS 12.3 X48-D30 for SRX Series Platforms Version 1.1 Ref EFS-T041-ETR 1.1

10. Evaluation Technical Report - NDPP Extended Package for Intrusion Prevention Systems Version 1.0 Ref EFS-T046-ETR

11. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
ICMP	Internet Control Message Protocol
IPS EP	Network Device Protection Profile (NDPP) Extended Package (EP) for Intrusion Prevention Systems (IPS)
NDPP	US Government approved Protection Profile for Network Devices

OSP	Organisation Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol