Supporting Document

Mandatory Technical Document

PP-Module for Intrusion Prevention Systems (IPS)

Version: 1.0

2021-05-11

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria Version 3.1 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the Common Criteria Recognition Arrangement (CCRA).

Technical Editor:

National Information Assurance Partnership (NIAP)

Document History:

V1.0, 11 May 2021 (Initial)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of an Intrusion Prevention System (IPS).

Field of Special Use:

Intrusion Prevention Systems (IPS).

Acknowledgements:

The NIAP Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia supported the development of this SD.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the Intrusion Prevention Systems (IPS) PP-Module is to describe the security functionality of an IPS in terms of [CC] and to define functional and assurance requirements for such products.

The PP-Module is intended for use with the following Base-PP:

- Protection Profile for Network Devices (NDcPP) Version 2.2e

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the following PP-Module:

- PP-Module for Intrusion Prevention Systems (IPS), Version 1.0

As such, it defines Evaluation Activities (EAs) for the functionality described by the IPS PP-Module as well as any impacts to the NDcPP Evaluation Activities that are required by the PP-Configuration.

Although EAs are defined mainly for the evaluators to follow, in general they will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis).

1.2 Structure of the Document

This document contains modifications and additions to the SD for the NDcPP to accommodate the evaluation of a network device TOE that also provides IPS functionality.

The remainder of this section introduces terminology that is relevant to IPS functionality.

Section 2 is divided into three parts. Section 2.1 defines the test environment that the evaluator should expect to have to perform the required test EAs. Section 2.2 lists the NDcPP SFRs that are applicable to the IPS functionality and provides instructions for whether the evaluator performs the NDcPP EAs for those SFRs as described in the NDcPP SDs, or whether any additional or alternative actions are required. Section 2.2 lists the mandatory SFRs added by the IPS PP-Module and provides EAs for them.

Similar to the structure of the NDcPP SD, Sections 3-4 identify EAs for any optional and selection-based SFRs defined by the PP-Module.

Section 5 identifies EAs for any objective SFRs defined by the PP-Module.

Section 6 defines Security Assurance Requirement (SAR) EAs for the PP-Module, specifically any cases where the SAR EAs must be supplemented to ensure that the IPS portion of the TSF is adequately evaluated.

1.3 Terminology

1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

Supplementary Information

Information that is not necessarily included in the ST or operational guidance, and that may not necessarily be public. Examples of such information could be entropy analysis, or description of a cryptographic key management architecture used in (or in support of) the TOE. The requirement for any such supplementary information will be identified in the corresponding PP or PP-Module.

Reference the terminology section of [NDcPP] in addition to the terms listed below.

Table 1: Technology Terms and Definitions

Term	Definition
Anomaly / Anomalous (network traffic)	Traffic that does not fit into a defined baseline and is therefore unexpected or atypical traffic. Anomalous traffic is not necessarily dangerous, and does not necessarily indicate any threat to the monitored network.
Baseline / Base-lining (network traffic)	Defining what is to be considered expected or typical network traffic on a monitored network. A traffic baseline does not indicate that all traffic that matches the baseline is safe, or that the traffic is not a potential threat to the monitored network. For example: traffic that matches a baseline can still match a list of known-bad IP addresses; or can match signatures of known threats.
Flooding	Causing an excessive amount of traffic on an IP subnet or targeted against a specific IP address.
Inline mode	The deployment of the TOE (or TOE component) such that monitored network traffic must flow across the TOE, thus providing the TOE with the opportunity to block the traffic.
IPS policy	Any set of rules for traffic analysis, traffic blocking, signature detection, and/or anomaly detection. Many IPS policies could be defined and stored on the TOE, but an IPS policy will not have any affect unless is applied to (made active on) one or more IPS interfaces.
Normalization (of network traffic)	Filtering of network traffic such that only the useful packets/fragments are allowed through to the destination. Normalization can only be performed by the TOE when the TOE is deployed in inline mode. Normalization can include filtering out any of
Profiling (network traffic)	See base-lining.
Promiscuous mode	The state of an IPS interface in which it's listening (collecting and inspecting) network traffic. A promiscuous interface could be one that is only listening and never transmitting traffic, or could be an interface through which traffic flows both inbound and outbound as in an inline mode deployment.
Sensor interface	Any interface of the TOE that has an IPS policy applied to it.

1.3.2 Acronyms

Reference the acronyms section of [NDcPP] in addition to the acronyms listed below

Table 2: Acronyms

Acronym	Meaning
DDoS	Distributed Denial of Service
DoS	Denial of Service

Acronym	Meaning
FTP	File Transfer Protocol
GRE	Generic Route Encapsulation
HTTP	Hypertext transfer protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
OSI	Open Systems Interconnection
PP	Protection Profile
PPTP	Point to Point Tunneling Protocol
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SQL	Structured Query Language
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
ToS	Type of Service
TSF	TOE Security Functionality
TTL	Time to Live
UDP	User Datagram Protocol

2 Evaluation Activities for SFRs

The EAs presented in this section are intended to supplement those defined in the NDcPP SD.

The IPS PP-Module relies on several NDcPP SFRs to help in the implementation of its required functionality. These NDcPP SFRs are listed in this section along with any impact to how they are to be evaluated in a TOE that includes the PP-Module. This section also defines the EAs for the mandatory SFRs that are introduced in the PP-Module.

Successful completion of these EAs assists in the completion of the relevant portions of ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1, which are required to be applied to the entire TOE as per NDcPP, version 2.2e.

2.1 Test Environment for Evaluation Activities

This section contains the expectations for the evaluator test environment that is used to perform the test specified by the EAs.

It is assumed the evaluator will have tools suitable to establish sessions, modify or create session packets, and perceive whether packets are getting through the TOE as well as to examine the content of those packets. In general, it is expected that IPS rule configuration and logging capabilities of the TOE can be used to reach appropriate determinations where applicable.

The tests need to be repeated for each distinct network interface type capable of monitoring network traffic on all 'sensor' interfaces of the TOE, which may include 'promiscuous' interfaces (with or without an IP address or IP stack, and whether or not the interfaces are capable of attempting to terminate unapproved traffic flows by transmitting packets such as TCP resets), and inline (pass-through) interfaces with or without an IP address or IP stack, but not management interfaces used to remotely access the TOE, or used by the TOE to initiate outbound connections to syslog servers, AAA servers, remote traffic filtering devices, etc.

The evaluators shall minimally create a test environment that is functionally equivalent to the test environment illustrated below. The evaluators must provide justification for any differences in the test environment. The TOE may be a distributed TOE in which some SFRs or elements of SFRs are enforced by separate TOE components distributed across a network. For distributed TOEs:

- the "TOE" in the "inline mode test topology" must be the TOE component that controls the flow of traffic, but that TOE component does not need to be the same component that collects or analyzes the traffic;
- the "TOE" in the "promiscuous mode test topology" must be the TOE component that communicates with the non-TOE traffic filtering device, but that TOE component does not need to be the same component that collects or analyzes the traffic.

Figure 1: Sample Inline Mode Test Topology

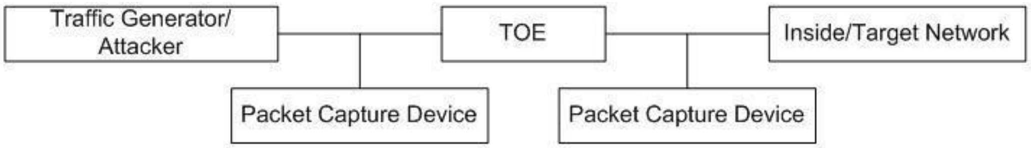
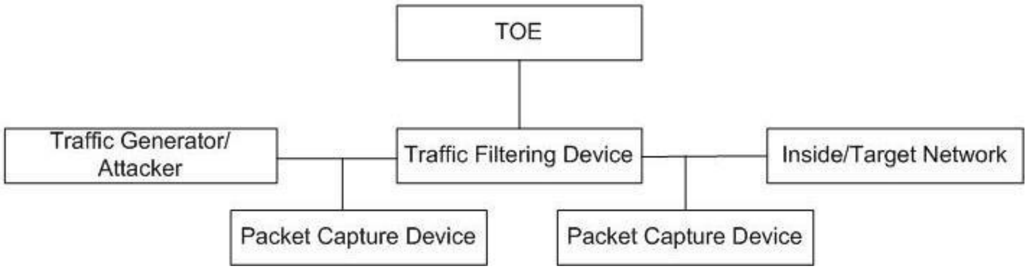


Figure 2: Sample Promiscuous Mode Test Topology



IPS devices that can be deployed in more than one mode, two instantiations of the TOE will more than likely make it easier to conduct testing, however, the evaluator is free to construct a test-bed where one instance of a TOE exists and there is a device that provides the necessary functions to interact with the TOE to satisfy the testing activities.

It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability to simulate network attacks. The traffic generator can be a COTS (commercial off the shelf), shareware, or freeware product; special equipment is not necessary.

2.2 NDcPP Evaluation Activities

This PP-Module does not modify any EAs required by the Base-PP. However, when testing the TOE, it is necessary to ensure the SFRs are tested specifically in conjunction with the IPS portion of the TOE where applicable, either directly or as a dependency to the functionality defined in this PP-Module.

2.3 TOE SFR Evaluation Activities

2.3.1 Security Audit (FAU)

2.3.1.1 Security Audit Data Generation (FAU_GEN)

FAU_GEN.1/IPS Audit Data Generation (IPS)

TSS

The evaluator shall verify that the TSS describes how the TOE can be configured to log IPS data associated with applicable policies.

The evaluator shall verify that the TSS describes what (similar) IPS event types the TOE will combine into a single audit record along with the conditions (e.g., thresholds and time periods) for so doing. The TSS shall also describe to what extent (if any) that may be configurable.

For IPS_SBD_EXT.1, for each field, the evaluator shall verify that the TSS describes how the field is inspected and if logging is not applicable, any other mechanism such as counting that is deployed.

Operational Guidance

The evaluator shall verify that the operational guidance describes how to configure the TOE to result in applicable IPS data logging.

The evaluator shall verify that the operational guidance provides instructions for any configuration that may be done in regard to logging similar events (e.g., setting thresholds, defining time windows, etc.).

Test

The evaluator shall test that the interfaces used to configure the IPS polices yield expected IPS data in association with the IPS policies. A number of IPS policy combination and ordering scenarios need to be configured and tested by attempting to pass both allowed and anomalous network traffic matching configured IPS policies in order to trigger all required IPS events.

Note the following:

- This activity should have been addressed with a combination of the Test EAs for the other IPS requirements.
- As part of testing this activity, the evaluator shall also ensure that the audit data generated to address this SFR can be handled in the manner that FAU_STG_EXT.1 requires for all audit data.

2.3.2 Security Management (FMT)

2.3.2.1 Specification of Management Functions (FMT_SMF)

FMT_SMF.1/IPS Specification of Management Functions (IPS)

TSS
The evaluator shall verify that the TSS describes how the IPS data analysis and reactions can be configured. This may be performed in conjunction with the evaluation of IPS_ABD_EXT.1, IPS_IPB_EXT.1, and IPS_SBD_EXT.1.

Operational Guidance
The evaluator shall verify that the operational guidance describes the instructions for each function defined in the SFR, describes how to configure the IPS data analysis and reactions, including how to set any configurable defaults and how to configure each of the applicable analysis pattern matching methods and reaction modes.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall use the operational guidance to create a signature and enable it on an interface. The evaluator shall then generate traffic that would be successfully triggered by the signature. The evaluator should observe the TOE applying the corresponding reaction in the signature.

Test 2: The evaluator shall then disable the signature and attempt to regenerate the same traffic and ensure that the TOE allows the traffic to pass with no reaction.

Test 3: The evaluator shall use the operational guidance to import signatures and repeat the test conducted in Test 1.

Other testing for this SFR is performed in conjunction with the EAs for IPS_ABD_EXT.1 and IPS_SBD_EXT.1.

2.3.3 Intrusion Prevention System (IPS)

2.3.3.1 Anomaly-Based IPS Functionality (IPS_ABD_EXT)

IPS_ABD_EXT.1 Anomaly-Based IPS Functionality

TSS
The evaluator shall verify that the TSS describes the composition, construction, and application of baselines or anomaly-based attributes specified in IPS_ABD_EXT.1.1.

The evaluator shall verify that the TSS provides a description of how baselines are defined and implemented by the TOE, or a description of how anomaly-based rules are defined and configured by the administrator.

If ‘frequency’ is selected in IPS_ABD_EXT.1.1, the TSS shall include an explanation of how frequencies can be defined on the TOE.

If ‘thresholds’ is selected in IPS_ABD_EXT.1.1, the TSS shall include an explanation of how the thresholds can be defined on the TOE.

The evaluator shall verify that each baseline or anomaly-based rule can be associated with a reaction specified in IPS_ABD_EXT.1.3.

The evaluator shall verify that the TSS identifies all interface types capable of applying baseline or anomaly-based rules and explains how they are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions to manually create baselines or anomaly-based rules according to the selections made in IPS_ABD_EXT.1.1. Note that dynamic “profiling” of a network to establish a baseline is outside the scope of the PP-Module.

The evaluator shall verify that the operational guidance provides instructions to associate reactions specified in IPS_ABD_EXT.1.3 with baselines or anomaly-based rules.

The evaluator shall verify that the operational guidance provides instructions to associate the different policies with distinct network interfaces.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall use the instructions in the operational guidance to configure baselines or anomaly-based rules for each attributes specified in IPS_ABD_EXT.1.1. The evaluator shall send traffic that does not match the baseline or matches the anomaly- based rule and verify the TOE applies the configured reaction. This shall be performed for each attribute in IPS_ABD_EXT.1.1.

Test 2: The evaluator shall repeat the test above to ensure that baselines or anomaly- based rules can be defined for each distinct network interface type supported by the TOE.

2.3.3.2 IP Blocking (IPS_IPB_EXT)

IPS_IPB_EXT.1 IP Blocking

TSS
The evaluator shall verify how good/bad lists affect the way in which traffic is analyzed with respect to processing packets. The evaluator shall also very that the TSS provides details for the attributes that create a known good list, a known bad list, and their associated rules, including how to define the source or destination IP address (e.g. a single IP address or a range of IP addresses).

If the TSF uses address types other than a single IP or a range of IP addresses (e.g. MAC addresses), the evaluator shall check that the TSS explains what configurations would cause non-IP lists of known-good and known-bad addresses to take precedence over IP-based address lists.

The evaluator shall also verify that the TSS identifies all the roles and level of access for each of those roles that have been specified in the requirement.

Operational Guidance
The evaluator shall verify that the administrative guidance provides instructions with how each role specified in the requirement can create, modify and delete the attributes of a known good and known bad lists.

If the TSF uses address types other than a single IP or a range of IP addresses (e.g. MAC addresses), the evaluator shall check that the operational guidance includes instructions for any configurations that would cause non-IP lists of known-good and known-bad addresses to take precedence over IP-based address lists.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall use the instructions in the operational guidance to create a known-bad address list. Using a single IP address, a list of addresses or a range of addresses from that list, the evaluator shall attempt to send traffic through the TOE that would otherwise be allowed by the TOE and observe the TOE automatically drops that traffic.

Test 2: The evaluator shall use the instructions in the operational guidance to create a known-good address list. Using a single IP address, a list of addresses or a range of addresses from that list, the evaluator shall attempt to send traffic that would otherwise be denied by the TOE and observe the TOE automatically allowing traffic.

Test 3: The evaluator shall add conflicting IP addresses to each list and ensure that the TOE handles conflicting traffic in a manner consistent with the precedence in IPS_NTA_EXT.1.1.

2.3.3.3 Network Traffic Analysis (IPS_NTA_EXT)

IPS_NTA_EXT.1 Network Traffic Analysis

IPS_NTA_EXT.1.1

TSS
The evaluator shall verify that the TSS explains the TOE's capability of analyzing IP traffic in terms of the TOE's policy hierarchy (precedence). The TSS should identify if the TOE's policy hierarchy order is configurable by the administrator for IPS policy elements (known-good lists, known-bad lists, signature-based rules, and anomaly-based rules).

Regardless of whether the precedence is configurable, the evaluator shall verify that the TSS describes the default precedence as well as the IP analyzing functions supported by the TOE.

Operational Guidance
The evaluator shall verify that the guidance describes the default precedence.

If the precedence is configurable, the evaluator shall verify that the guidance explains how to configure the precedence.

Test
There are no test EAs for this element.

IPS_NTA_EXT.1.2

TSS
The evaluator shall verify that the TSS indicates that the following protocols are supported:

- IPv4
- IPv6
- ICMPv4
- ICMPv6
- TCP
- UDP

The evaluator shall verify that the TSS describes how conformance with the identified protocols has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing).

Operational Guidance
There are no guidance EAs for this element.

Test
There are no test EAs for this element.

IPS_NTA_EXT.1.3

TSS
The evaluator shall verify that the TSS identifies all interface types capable of being deployed in the modes of promiscuous, and or inline mode as well as the interfaces necessary to facilitate each deployment mode (at a minimum, the interfaces need to support inline mode). The evaluator shall also check that the TSS provides a description for how the management interface is logically distinct from any sensor interfaces.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions on how to deploy each of the deployment methods outlined in the TSS. The evaluator shall also verify that the operational guidance provides instructions of applying IPS policies to interfaces for each deployment mode. If the management interface is configurable, the evaluator shall verify that the operational guidance explains how to configure the interface as a management interface.

The evaluator shall verify that the operational guidance explains how the TOE sends commands to remote traffic filtering devices if this functionality is supported.

Test
Testing for this element is performed in conjunction with testing where promiscuous and inline interfaces are tested.

2.3.3.4 Signature-Based IPS Functionality (IPS_SBD_EXT)

IPS_SBD_EXT.1 Signature-Based IPS Functionality

TSS
IPS_SBD_EXT.1.1

The evaluator shall verify that the TSS describes what is comprised within a signature rule.

The evaluator shall verify that each signature can be associated with a reaction specified in IPS_SBD_EXT.1.5.

The evaluator shall verify that the TSS identifies all interface types that are capable of applying signatures and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions with how to create and/or configure rules using the following protocols and header inspection fields:

- IPv4: version; header length; packet length; ID; IP flags; fragment offset; time to live (TTL); protocol; header checksum; source address; destination address; and IP options.
- IPv6: Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options.
- ICMP: type; code; header checksum; and rest of header (varies based on the ICMP type and code).
- ICMPv6: type; code; and header checksum.
- TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options.
- UDP: source port; destination port; length; and UDP checksum.

The evaluator shall verify that the operational guidance provides instructions with how to select and/or configure reactions specified in IPS_SBD_EXT.1.5 in the signature rules.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall use the instructions in the operational guidance to test that packet header signatures can be created and/or configured with the selected and/or configured reactions specified in IPS_SBD_EXT.1.5 for each of the attributes listed below. Each attribute shall be individually assigned to its own unique signature:

- IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; and IP Options.
- IPv6: Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options.
- ICMP: Type; Code; Header Checksum; and Rest of Header (varies based on the ICMP type and code).
- ICMPv6: Type; Code; and Header Checksum.
- TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options.
- UDP: Source port; destination port; length; and UDP checksum.

The evaluator shall generate traffic to trigger a signature and shall then use a packet sniffer to capture traffic that ensures the reactions of each rule are performed as expected.

Test 2: The evaluator shall repeat the test above to ensure that signature-based IPS policies can be defined for each distinct network interface type capable of applying signatures as supported by the TOE.

IPS_SBD_EXT.1.2

TSS
The evaluator shall verify that the TSS describes what is comprised within a string-based detection signature.

The evaluator shall verify that each packet payload string-based detection signature can be associated with a reaction specified in IPS_SBD_EXT.1.5.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions with how to configure rules using the packet payload string-based detection fields defined in IPS_SBD_EXT.1.2.

The evaluator shall verify that the operational guidance provides instructions with how to configure reactions specified in IPS_SBD_EXT.1.5 for each string-based detection signature.

The evaluator shall verify that the operational guidance provides instructions with how rules are associated with distinct network interfaces that are capable of being associated with signatures.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall use the instructions in the operational guidance to test that packet payload string-based detection rules can be assigned to the reactions specified in IPS_SBD_EXT.1.5 using the attributes specified in IPS_SBD_EXT.1.2. However it is not required (nor is it feasible) to test all possible strings of protocol data, the evaluator shall ensure that a selection of strings in the requirement is selected to be tested. At a minimum at least one string using each of the following attributes from IPS_SBD_EXT.1.2 should be tested for each protocol. The evaluator shall generate packets that match the string in the rule and observe the corresponding reaction is as configured.

- Test at least one string of characters for ICMPv4 data: beyond the first 4 bytes of the ICMP header.
- Test at least one string of characters for ICMPv6 data: beyond the first 4 bytes of the ICMP header.
- TCP data (characters beyond the 20 byte TCP header):

i) Test at least one FTP (file transfer) command: help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, and type.
ii) HTTP (web) commands and content:
    (1) Test both GET and POST commands
    (2) Test at least one administrator-defined strings to match URLs/URIs, and web page content.
iii) Test at least one SMTP (email) state: start state, SMTP commands state, mail header state,

mail body state, abort state.

iv) Test at least one string in any additional attribute type defined within the “other types of TCP payload inspection” assignment, if any other types are specified.

- Test at least one string of UDP data: characters beyond the first 8 bytes of the UDP header;
- Test at least one string for each additional attribute type defined in the “other types of packet payload inspection” assignment, if any other types are specified.

Test 2: The evaluator shall repeat Test 1 above to ensure that signature-based IPS policies can be defined for each distinct network interface type capable of applying signatures as supported by the TOE.

IPS_SBD_EXT.1.3

TSS
The evaluator shall verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.3 are processed by the TOE and what reaction is triggered when these attacks are identified.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.3 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5.

Test
The evaluator shall create and/or configure rules for each attack signature in IPS_SBD_EXT.1.3. For each attack, the TOE should apply its corresponding signature and enable it to each distinct network interface type capable of applying the signatures. The evaluator shall use packet captures to ensure that the attack traffic is detected by the TOE and a reaction specified in IPS_SBD_EXT.1.5 is triggered and stops the attack. Each attack should be performed one after another so as to ensure that its corresponding signature successfully identified and appropriately reacted to a particular attack.

IPS_SBD_EXT.1.4

TSS
The evaluator shall verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.4 are processed by the TOE and what reaction is triggered when these attacks are identified.

Operational Guidance
The evaluator shall verify that the operational guidance provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.4 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5.

Test
The evaluator shall configure individual signatures for each attack in IPS_SBD_EXT.1.4. For each attack, the TOE should apply its corresponding signature and enable it to each distinct network interface type capable of applying signatures. The evaluator shall use packet captures to ensure that the attack traffic is detected by the TOE and a reaction specified in IPS_SBD_EXT.1.5 is triggered and stops the attack. Each attack should be performed one after another so as to ensure that its corresponding signature successfully identified and appropriately reacted to a particular attack.

IPS_SBD_EXT.1.5

TSS
There are no TSS EAs for this element.

Operational Guidance
The guidance EAs for this element are performed in conjunction with IPS_SBD_EXT.1.1, IPS_SBD_EXT.1.3, and IPS_SBD_EXT.1.4.

Test
The test EAs for this element are performed in conjunction with those for IPS_SBD_EXT.1.1, IPS_SBD_EXT.1.2, IPS_SBD_EXT.1.3, and IPS_SBD_EXT.1.4.

IPS_SBD_EXT.1.6

TSS
There are no TSS EAs for this element.

Operational Guidance
The evaluator shall verify that the operational guidance provides configuration instructions, if needed, to detect payload across multiple packets.

Test
The evaluator shall repeat one of the tests in IPS_SBD_EXT.1.2 Test 1 but generate multiple non-fragmented packets that contain the string in the rule defined. The evaluator shall verify that the malicious traffic is still detected when split across multiple non-fragmented packets.

3 Evaluation Activities for Strictly Optional Requirements

3.1 Security Audit (FAU)

3.1.1 Security Audit Event Storage (FAU_STG)

3.1.1.1 FAU_STG.1/IPS Protected Audit Trail Storage (IPS Data)

TSS
The evaluator shall ensure that the TSS identifies how IPS data is protected from unauthorized modification and deletion.

Operational Guidance
The evaluator shall confirm the guidance documentation describes how to protect IPS data from unauthorized modification and deletion.

Test
The evaluator shall devise tests that demonstrate that IPS data can be protected from unauthorized modification and deletion.

3.1.1.2 FAU_STG.4 Prevention of Audit Data Loss

TSS
The evaluator shall ensure that the TSS identifies how IPS data logging is handled once the IPS data trail is full.

Operational Guidance
The evaluator shall confirm the guidance documentation describes any steps involved to manage IPS data logging when the IPS audit trail is full.

Test
There are no test EAs for this component.

3.2 Protection of the TSF (FPT)

3.2.1 Fail Secure (FPT_FLS)

3.2.1.1 FPT_FLS.1 Failure with Preservation of Secure State

TSS
The evaluator shall examine the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall ensure that the TSS identifies all failures that will result in the TOE preserving a secure state if triggered. The evaluator shall then ensure that the TOE will attain a secure state after inserting each specified failure mode type. The evaluator shall also examine the TSS to determine whether the fail-secure functionality is configurable.

Operational Guidance
There are no operational guidance EAs for this component.

Test
For each type of failure listed in the assignment, the TOE vendor must provide the evaluator with the means to trigger the failure, and the evaluator shall reproduce each type of failure to ensure that an

applied IPS policy remains enforced during the failure. For example, various causes including temporary loss of power could result in a reboot of the TOE. If the active IPS policy at the time of the failure (e.g. reboot) ensured that ICMP echo packets were dropped by the TOE, the evaluator shall confirm that at no point during the shutdown or restart of the TOE is any ICMP echo packet allowed through the TOE (though in this example, it should be understood that there will be a period at which IPS events are not audited while the audit mechanism is pending restart).

3.3 Intrusion Prevention (IPS)

3.3.1 Signature-Based IPS Functionality (IPS_SBD_EXT)

3.3.1.1 IPS_SBD_EXT.2 Traffic Normalization

IPS_SBD_EXT.2.1

TSS
The evaluator shall verify that the TSS describes how the TOE is able to inspect traffic inside the encapsulation protocols claimed in the requirement.

Operational Guidance
The evaluator shall examine the operational guidance to determine that it contains instructions for inspecting tunneled packets through the encapsulation methods identified in the requirement.

Test
The evaluator shall set up the conditions necessary to execute testing from IPS_SBD_EXT.1 except that the traffic to be inspected is encapsulated in one of the tunneling protocols that the TOE is capable of inspecting. The evaluator shall transmit the encapsulated traffic and observe that the TSF is able to inspect it and respond in the configured manner. The evaluator shall repeat this test for each type of encapsulated traffic supported by the TSF.

IPS_SBD_EXT.2.2

TSS
The evaluator shall verify that the TSS describes how audit records are generated when packets cannot be reassembled after fragmentation. Also, for inline mode, the evaluator shall examine the TSS to ensure packets are dropped.

Operational Guidance
There are no guidance EAs for this element.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall generate packets that cannot be reassembled after fragmentation; the evaluator shall ensure audit events are generated for all instances of IP normalization.

Test 2: For inline mode: The evaluator shall test for automatic packet rejection for when packets cannot be reassembled after fragmentation. The evaluator shall use packet captures to ensure that the IP traffic is detected by the TOE and packets are dropped.

Test 3: The evaluator shall generate packets that can be reassembled after fragmentation; the evaluator shall ensure audit events are generated for all instances of IP normalization.

IPS_SBD_EXT.2.3

TSS
The evaluator shall verify that the TSS describes that packets are automatically dropped for the following normalization:

- duplicate packets
- changed packets
- out of sequence packets
- other packet types claimed in the requirement, if any

Operational Guidance
There are no guidance EAs for this element.

Test
The evaluator shall generate the following types of packets and observe that they are discarded by the TSF:

- duplicate packets
- changed packets
- out of sequence packets
- other packet types claimed in the requirement, if any

4 Evaluation Activities for Implementation-Dependent Requirements

There are currently no implementation-dependent requirements defined by the PP-Module.

4.1 Resource Utilization (FRU)

4.1.1 Resource Allocation (FRU_RSA)

4.1.1.1 FRU_RSA.1 Maximum Quotas

TSS
The evaluator shall examine the TSS to ensure that it identifies all resources controlled through the quota mechanism, and that this list contains those resources used to support traffic inspection. The evaluator shall ensure that the TSS describes how each resource is counted as "used" and how a maximum quota or use is determined, as well as the action taken when the quota is reached.

Operational Guidance
The evaluator shall examine the operational guidance to determine that it contains instructions for establishing quotas (if they are configurable) and that it describes any actions administrators can or should take in response to a quota being reached.

Test
The evaluator shall follow the operational guidance to configure quotas for the resource (if such a capability is provided). The evaluator then causes the resource quota to be reached, and observes that the action specified in the TSS occurs.

5 Evaluation Activities for Objective Requirements

5.1 Security Audit (FAU)

5.1.1 Security Alarms (FAU_ARP)

5.1.1.1 FAU_ARP.1 Security Alarms

TSS
The evaluator shall verify that the TSS includes a description of the alerts specified in the requirement and the events that may trigger these alerts to be generated. The evaluator shall also verify that the TSS states that audit data cannot be transmitted through the security alarms interface.

Operational Guidance
The evaluator shall verify that the guidance explains how to enable alerts specified in the requirement based on the events that the TSS identifies as potential security violations.

Test
For each action that can be taken by the TSF upon detection of a potential security violation, the evaluator shall configure the TOE to take that action when a particular event occurs. The evaluator shall then perform some action to trigger the event (e.g. by transmitting network traffic that represents the event to the TOE's sensor interfaces) and observe that the configured action occurs in response.

5.1.2 Security Audit Review (FAU_SAR)

5.1.2.1 FAU_SAR.1 Audit Review

TSS

The evaluator shall examine the TSS to verify that it describes the ability of administrators to view IPS data from the IPS events, the format in which this IPS data is displayed, and how an administrator is authorized to view this data.

Operational Guidance
The evaluator shall examine the operational guidance to verify that it provides instructions on how to access and interpret IPS events using the TOE's management interface.

Test
The evaluator shall devise tests that demonstrate that IPS data (generated as defined in FAU_GEN.1/IPS) can be interpreted by authorized administrators from the TOE's management interface.

5.1.2.2 FAU_SAR.2 Restricted Audit Review

TSS
The evaluator shall examine the TSS to determine that it identifies what group of users is considered to be 'administrators' for the purpose of being granted access to view IPS data.

Operational Guidance
The evaluator shall examine the operational guidance to determine what actions are needed to grant or revoke a user's ability to view IPS data.

Test
The evaluator shall log on to the TOE as various users to confirm that only those users that are intended to be granted read access to IPS data are able to view it.

5.1.2.3 FAU_SAR.3 Selectable Audit Review

TSS
The evaluator shall verify that the TSS includes a description of how the TOE has the ability to apply filtering and sorting of IPS data using the parameters listed in the requirement.

Operational Guidance
The evaluator shall review the operational guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain instructions on how to set the pre- selection, as well as explain the syntax (if present) for multi-value pre-selection. The administrative guidance shall also identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.

Test
The evaluator shall perform the following tests:

Test 1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.

Test 2 [conditional]: If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

6 Evaluation Activities for Selection-Based Requirements

There are currently no selection-based requirements defined by the PP-Module.

7 Evaluation Activities for SARs

To evaluate the SARs specified by NDcPP and the PP-Module, the evaluator shall perform the SAR EAs defined in the NDcPP SD against the entire TOE (i.e., both the generic network device portion and the portion responsible for implementation of IPS). In particular, the evaluator shall ensure that the vulnerability testing defined in section A.1.4 of the NDcPP SD is applied to the TOE’s IPS interfaces in addition to any other security-relevant network device interfaces that the TOE may have.

8 Required Supplementary Information

This SD has no required supplementary information beyond the ST, operational guidance, and testing.

9 References

Table 3: References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 2020
[NDcPP SD]	Supporting Document – Mandatory Technical Document – Evaluation Activities for Network Device cPP, Version 2.2, December 2019
[IPS]	PP-Module for Intrusion Prevention Systems (IPS), Version 1.0, May 11, 2021