PP-Module for Intrusion Prevention Systems (IPS)

Version: 1.0
2021-05-11
National Information Assurance Partnership

Contents

1. Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of an Intrusion Prevention System (IPS) in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

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

This Base-PP is valid because a device that implements IPS is a specific type of network device, and there is nothing about the implementation of IPS that would prevent any of the security capabilities defined by the Base-PP from being satisfied.

A TOE that conforms to a PP-Configuration containing this PP-Module may be a 'Distributed TOE' as defined in the NDcPP. For example, the TOE could have distributed 'sensor' components monitoring various logically separated networks, each of which reports to a centralized 'manager' component for configuration of IPS policies and aggregation of IPS data.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this PP-Module.

1.2.1 Common Criteria Terms

Table 1: CC Terms and Definitions

Term	Definition
Assurance	Grounds for confidence that a TOE meets the SFRs.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a specific category of technology.
Protection Profile Configuration	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.

Term	Definition
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technology Terms

Table 2: 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 Compliant Targets of Evaluation

This PP-Module specifically addresses network-based IPSs. 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. This PP-Module is focused on inspecting IP traffic (TCP, UDP, ICMP, etc.). This limited scope is intentional for a number of reasons including: to define a reasonable boundary for the scope of testing (assurance measures) defined within the PP-Module and to allow future PP-Modules to address other IPS and functionality that includes scanners, analyzers,

sensors, etc. The scope of the PP-Module does not preclude support for inspection of other IP protocols (e.g. GRE, ESP, AH), but the scope of this PP-Module does not include the evaluation of non-IP protocols including layer 2 protocols, or Ethernet.

The baseline requirements of this PP-Module are those determined necessary for an Intrusion Prevention product, though conformant TOEs may provide IPS functionality entirely independently from other network components, and/or be deployed to operate in conjunction with other components of a larger enterprise security solution. For example, though all conformant IPS TOEs must have some capacity to monitor, collect, analyze, and react to network traffic, a conformant TOE could:

- Monitor all network traffic passively detected by one or more its interfaces, and/or monitor only specific traffic flows that are passed by or through the IPS for inspection.
- Transmit IPS data to an external audit storage host, and optionally store IPS data internally. IPS audit data can be pushed (initiated by the TOE) or pulled (initiated by the remote host). Regardless of whether IPS data is pushed or pulled, the transmission must be protected in a manner consistent with protected communications required by FAU_STG_EXT.1 of the NDcPP.
- Analyze network traffic based on rules that an administrator can configure directly on the TOE, and optionally analyze network traffic based on rules imported/applied from another system.
- React independently to potentially malicious traffic (such as by blocking traffic flows, or by transmitting session resets to the endpoints), and optionally react in collaboration with non-TOE components of the overall enterprise security solution by initiating a connection to non-TOE components to cause/configure the non-TOE component to obstruct the traffic flow.

Many similarities exist between a conformant IPS TOE and an Intrusion Detection System (IDS), but there are some important distinctions. The conformant IPS TOE differs from an IDS in that the conformant TOE must be capable of initiating a proactive response to terminate/interrupt an active potential threat, and to initiate a response in real time that would cause interruption of the suspicious traffic flow. It is not sufficient for the TOE to only be able to generate an audit event or other alert when potentially malicious traffic is detected. However, the Security Administrator may choose to configure the TOE such that such proactive responses are not enabled, and such a configuration would be a valid configuration for the TOE. Though a conformant TOE may be deployed with only its IDS functionalities enabled, the conformant TOE must demonstrate that capability during the evaluation.

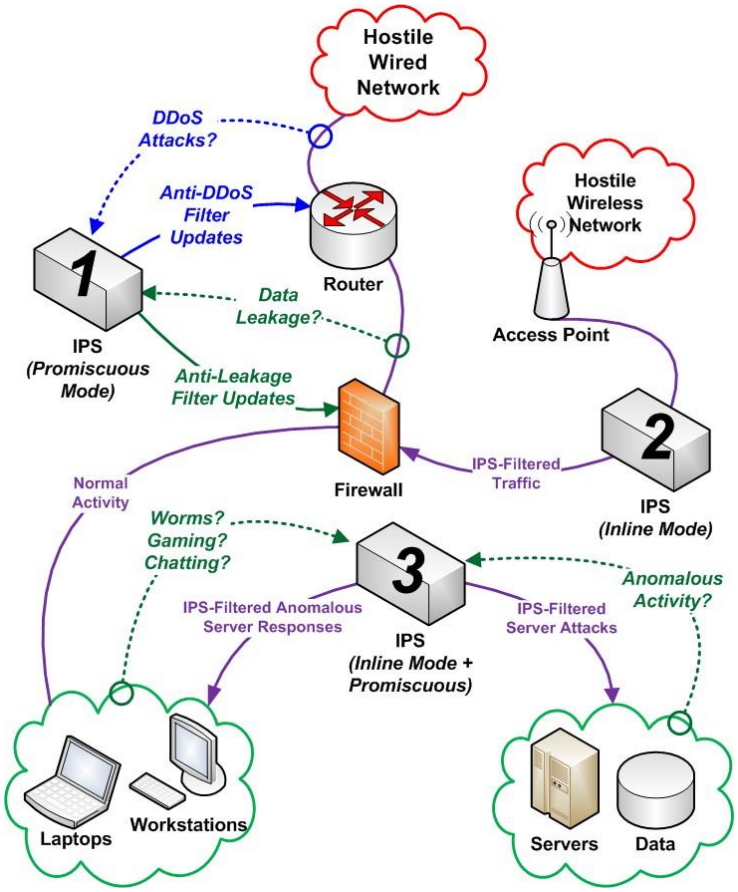
Conformant TOEs will detect potentially malicious network traffic using various approaches. Broadly speaking, the traffic analysis could be based on identification of ‘known’ threats, or ‘unknown’ threats. Identification of ‘known’ threats may be performed through pattern matching, e.g. by matching strings of characters within an IP packet, or by matching traffic patterns common with reconnaissance or denial of service (DoS) attacks. Identification of ‘unknown’ threats may be performed through use of various forms of ‘anomaly’ detection whereby the IPS is provided with (or ‘learns/creates’) a definition of ‘expected/typical’ traffic patterns, such that it’s able to detect and react to ‘anomalous’ (unexpected/atypical) traffic patterns.

The TOE may be a distributed TOE in which some SFRs or elements of SFRs are enforced by separate TOE components distributed across an IP network. In such cases, the NDcPP guidance on the handling of distributed TOEs applies. This PP-Module does not mandate that specific SFRs be assigned to specific components in a distributed TOE; however, it is expected that any TOE component that enforces any IPS function must enforce all dependent functionality for management and audit at minimum.

Deployment scenarios supported by the TOE include those shown in Figure 1, which includes a number of possible deployments or use cases for IPS functionality within a single network. Note that this is just an example of an IPS deployment where individual devices implement specific IPS functionality differently; per the requirements in this PP-Module (specifically IPS_NTA_EXT.1), a conformant TOE must implement both promiscuous and inline mode interfaces, though it is not a requirement for every TOE component to implement both modes.

- IPS 1 is operating in promiscuous mode, capturing data from two separate networks outside the perimeter firewall, and sending traffic filter updates as needed to the perimeter router and perimeter firewall to block unwanted traffic in real-time.
- IPS 2 is operating in inline mode, analyzing traffic to and from a wireless network, and blocking in real-time any traffic that violates the admin-defined IPS policies.
- IPS 3 is operating in a combination of promiscuous mode and inline mode. The IPS has at least one pair of interfaces creating a bridge or routing across the TOE, and is analyzing and filtering traffic in real-time as traffic traverses the TOE. The same IPS has one or more promiscuous interfaces collecting and analyzing traffic traversing within each separate network, and reacting to anomalous activity, worms, or otherwise unapproved activity.

Figure 1: TOE Deployment Scenario Diagram



1.4 TOE Boundary

The physical boundary for a TOE that conforms to this PP-Module is a physical or virtual network device, that also provides generalized network device functionality, such as auditing, I&A, and cryptographic services for network communications. 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 fulfill the requirements of this PP-Module. The TOE's logical boundary includes all functionality required by the Base-PP as well as the IPS functionality and related capabilities that are defined in this PP-Module. Any functionality that is provided by the network device that is not relevant to the security requirements defined by this PP-Module or the Base-PP is considered to be outside the scope of the TOE.

1.5 Use Cases

This PP-Module defines two potential use cases for the IPS TOE:

[Use Case 1] Standalone System

The TOE exists as a standalone device that is capable of enforcing all of the mandatory requirements defined in this PP-Module by itself.

[Use Case 2] Distributed System

The TOE exists as a distributed system that is able to apply different IPS functions to different network segments. In this case, distributed nodes may each implement all required IPS functionality, or different node types may offer different functions so long as the evaluated configuration collectively addresses all of the mandatory requirements defined in this PP-Module. In this deployment, it is expected (though not required) that a single device be used as a central point to perform configuration and collect relevant log data for the rest of the TOE.

This PP-Module also defines optional and objective requirements for functionality including separation of management roles and ability to use the TSF to review collected IPS data. These functions are not dependent on a particular use case being chosen.

2. Conformance Claims

2.1 CC Conformance

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

The following PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module.

- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claim

This PP-Module does not claim conformance to any packages.

3. Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

IPS devices address a range of security threats related to detection of and reaction to potentially malicious traffic on monitored networks, to which the security policies will be enforced on applicable network traffic. The malicious traffic may pose a threat to one or more endpoints on the monitored networks, to the network infrastructure, or to the TOE itself. The term 'monitored networks' is used here to represent any network to which the TOE is directly connected, as well as network segments/subnets that have had their traffic forwarded (redirected or copied) to the IPS for analysis.

The term 'IPS Data' will be used throughout this PP-Module and includes any or all of: the data extracted from network traffic and stored on the TOE; the results of analysis performed by the TOE; and messages that indicate the TOE's reaction to that analysis. This 'IPS Data' described in this PP-Module refers to the network traffic collected by the IPS and the resulting audit records related to analysis of that network traffic, all of which is separate from the 'audit data' as defined in FAU_GEN from the Base-PP, such as audit records related to authentication of administrators and establishment/termination of trusted channels.

A site is responsible for developing its security policy and configuring a rule set that the IPS will enforce and provide an appropriate response to meet their needs, relative to their own risk analysis and their perceived threats. Threats mitigated by the conformant TOE can include attempts to:

- Perform network-based reconnaissance (probing for information about a monitored network or its endpoints), such as through use of various scanning or mapping techniques.
- Obstruct the normal function of monitored networks, endpoints, or services, such as through denial of service attacks.
- Gain inappropriate access to one or more networks, endpoints, or services, such as through brute force password guessing attacks, or by transmitting malicious executable code, scripts, or commands.
- Disclose/transmit information in violation of policy, such as sending credit card numbers. Note, relative to the data, it does not matter where the threat agent is located. Example: data exfiltration means that data was removed without proper authorization to remove it. This may be a pull or a push. It can result from intrusion from the outside or by the actions of the insider.

Note that this PP-Module does not repeat the threats identified in the NDcPP, though they all apply given the conformance and hence dependence of this PP-Module on the NDcPP. Additionally, this PP-Module describes TOE functionality (such as security management functions) that are subject to the same threats as those that are defined in the NDcPP. A full mapping between threats and objectives is provided in Section 4.3 of this PP-Module.

The NDcPP contains only threats to the ability of the TOE to provide its own functions. This PP-Module defines threats to resources in the operational environment that will be met by an IPS TOE. Together, the threats of the Base-PP and those defined in this PP-Module define the comprehensive set of security threats addressed by an IPS TOE.

3.1 Threats

The following threats defined in this PP-Module extend the threats defined by the Base-PP.

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_DISCLOSURE

Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.

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.

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).

3.2 Assumptions

All assumptions for the operational environment of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

The following additional assumption is made on the operational environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an operational environment that does not meet this assumption, the TOE may no longer be able to provide all of its security functionality.

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.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the Base-PP.

P.ANALYZE

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

4. Security Objectives

4.1 Security Objectives for the TOE

O.IPS_ANALYZE

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.

Addressed by: IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1, FPT_FLS.1 (optional), IPS_SBD_EXT.2 (optional), FRU_RSA.1 (implementation-dependent)

O.IPS_REACT

The TOE must be able to react in real-time as configured by the Security Administrator to terminate and block traffic flows that have been determined to violate administrator-defined IPS policies.

Addressed by: IPS_ABD_EXT.1, IPS_SBD_EXT.1, FAU_ARP.1 (objective)

O.SYSTEM_MONITORING

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.

Addressed by: FAU_GEN.1/IPS, FAU_STG.1/IPS (optional), FAU_STG.4 (optional), FAU_SAR.1 (objective), FAU_SAR.2 (objective), FAU_SAR.3 (objective)

O.TOE_ADMINISTRATION

To address the threat of unauthorized administrator access that is defined in the Base-PP, conformant TOEs will provide the functions necessary for an administrator to configure the IPS capabilities of the TOE.

Addressed by: FMT_SMF.1/IPS

4.2 Security Objectives for the Operational Environment

All objectives for the operational environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

This PP-Module defines the following additional environmental security objectives, which extend those defined in the Base-PP.

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.

4.3 Security Objectives Rationale

The security objectives defined for the TOE and its operational environment are appropriate to address the security problem based on the following rationale:

Table 3: Security Objective Rationale

Objective	Threat, Assumption, or OSP	Rationale
O.IPS_ANALYZE	T. NETWORK_ACCESS	The TOE mitigates the threat of unauthorized network access by implementing measures to detect and respond to network traffic that may indicate this activity.
	T.NETWORK_DISCLOSURE	The TOE mitigates the threat of unauthorized network data disclosure by implementing measures to detect and respond to network traffic that may indicate this activity.
	T.NETWORK_DOS	The TOE mitigates the threat of denial of service attempts by implementing measures to detect and respond to network traffic that may indicate this activity.
	T.NETWORK_MISUSE	The TOE mitigates the threat of misuse of network resources by implementing measures to detect and respond to network traffic that may indicate this activity.
	P.ANALYZE	The TOE supports this policy by providing a means of analyzing collected network data.
O.IPS_REACT	T. NETWORK_ACCESS	The TOE mitigates the threat of unauthorized network access by implementing measures to detect and respond to network traffic that may indicate this activity.
	T.NETWORK_DISCLOSURE	The TOE mitigates the threat of unauthorized network data disclosure by implementing measures to detect and respond to network traffic that may indicate this activity.
	T.NETWORK_DOS	The TOE mitigates the threat of denial of service attempts by implementing measures to

Objective	Threat, Assumption, or OSP	Rationale
		detect and respond to network traffic that may indicate this activity.
	T.NETWORK_MISUSE	The TOE mitigates the threat of misuse of network resources by implementing measures to detect and respond to network traffic that may indicate this activity.
O.SYSTEM_MONITORING	T. NETWORK_ACCESS	The TOE mitigates the threat of unauthorized network access by implementing measures to record and securely network traffic for further analysis.
	T.NETWORK_DISCLOSURE	The TOE mitigates the threat of unauthorized network data disclosure by implementing measures to record and securely network traffic for further analysis.
	T.NETWORK_DOS	The TOE mitigates the threat of denial of service attempts by implementing measures to record and securely network traffic for further analysis.
	T.NETWORK_MISUSE	The TOE mitigates the threat of misuse of network resources by implementing measures to record and securely network traffic for further analysis.
O.TOE_ADMINISTRATION	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (from Base-PP)	This objective further mitigates the threat of unauthorized administrative access defined in the Base-PP by ensuring that only authorized administrators can interact with IPS-related management interfaces.
	P.ANALYZE	The TOE supports this policy by providing authorized administrators with sufficient tools to perform the required analysis.

Objective	Threat, Assumption, or OSP	Rationale
OE.CONNECTIONS	A.CONNECTIONS	The objective supports the assumption by setting the expectation that administrators will deploy the TOE in such a manner that there is no network path that will be exempt from the TOE's inspection capabilities.

5. Security Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignments are indicated with *italicized text*.
- Refinements made by the PP-Module author are indicated with **bold text**. Refinements are only applied to significant technical changes to existing SFRs; minor presentation changes with no technical impact (such as British vs American spelling differences) are not marked as refinements. Refinements are also indicated when an operation is added or substituted for an existing operation (e.g. the PP-Module completes an assignment in such a way that it introduces a selection into the assignment)
- Selections are indicated with *italicized text*.
- Iterations are indicated by appending the SFR name either with a slash and unique identifier suggesting the purpose of the iteration, e.g. '/IPS' for an SFR relating to IPS functionality
- Extended SFRs are identified by having a label "EXT" after the SFR name.

5.1 Base-PP Security Functional Requirements Direction

In a PP-Configuration that includes the NDcPP, the TOE is expected to rely on some of the security functions implemented by the network device as a whole and evaluated against the Base-PP. However, this PP-Module does not change how any of the NDcPP functions are implemented so there is no modification to the NDcPP SFRs used with this PP-Module. Note in particular that requirements that apply to distributed TOEs (e.g. FCO_CPC_EXT.1, FPT_ITT.1) remain optional as this PP-Module supports but does not mandate a distributed deployment.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that conforms to a PP-Configuration containing this PP-Module. These SFRs must be included regardless of which PP-Configuration is used to define the TOE.

5.2.1 Security Audit (FAU)

FAU_GEN.1/IPS: Audit Data Generation (IPS)

FAU_GEN.1.1/IPS The TSF shall be able to generate an **IPS** audit record of the following **IPS** auditable events:

a) Start-up and shut-down of the **IPS** functions;
b) All **IPS** auditable events for the [*not specified*] level of audit; and
c) [*All dissimilar IPS events;*
d) *All dissimilar IPS reactions;*
e) *Totals of similar events occurring within a specified time period;*
f) *Totals of similar reactions occurring within a specified time period;*
g) *The events in the IPS Events table*.

h) *[selection*: *no other auditable events, [assignment: other auditable events]*].

***Application Note**:* *This SFR exists in addition to the FAU_GEN.1 SFR in the Base-PP. All required auditable events from the Base-PP still apply. As the data that this SFR addresses is still considered to be "audit data," the requirement for secure remote transmission per FAU_STG_EXT.1 applies to this SFR in the same manner as the Base-PP's iteration of FAU_GEN.1.*

The ST author is not limited to the list presented and should update the list of auditable events with any additional information generated. The ST Author should use FAU_GEN.1 as defined in the Base-PP for standard (non-IPS data) audit functions.

For all requirements marked as optional, it is expected that if the requirement is claimed, the corresponding IPS events should be generated by the TSF; if the requirement is not claimed, then the ST author may also omit these events.

With regards to 'similar' and 'dissimilar' type events, dissimilar events are those whose characteristics differ from other events by something other than merely a timestamp, whereas 'similar' events are multiple occurrences of the same auditable event within some time period where the only significant difference between these events is the timestamp. For example, it is not expected that the TOE generate an individual audit message for every event of the same kind that occurs within a reasonable time period (e.g. the TSF need only generate one audit message for an event that repeated X times during Y seconds).

FAU_GEN.1.2/IPS The TSF shall record within each **IPS auditable event** record at least the following information:

a) Date and time of the event, type of event **and/or reaction,** ~~subject identity, and the outcome (success or failure) of the event;~~ and;

b) For each **IPS** audit**able** event type, based on the auditable event definitions of the functional components included in the PP~~/ST~~, [*information specified in column three of the IPS Events table*].

Application Note: *For IPS_SBD_EXT.1 and IPS_ABD_EXT.1 there may be several circumstances in which it would not be necessary to explicitly identify the action within the audit messages. For example, if the TOE's action is implied within the policy definition or if the default action is to allow traffic, then the absence of 'blocked' would imply the traffic was allowed.*

For IPS_SBD_EXT.1, if certain header fields are inspected and dropped or modified by default (e.g., packets with bad checksum, reserved bits set to zero), this logging requirement is not applicable.

The ST author should update IPS Events table below with any additional information generated such as source and destination addresses, IP, signature that trigged event, port, etc.

Table 4: IPS Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_STG.4 (optional)	A local audit store reaches its storage limit.	Indication that the audit store is full, and (if configurable) how the TOE is responding (e.g. failing to audit new auditable events, or
FMT_SMF.1/IPS	Modification of an IPS policy element.	Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known-good/known-bad list was modified).
FPT_FLS.1 (optional)	Failure of the TSF.	The type of failure that occurred.
FRU_RSA.1 (implementation-dependent)	Traffic flow volume exceeds the maximum quota.	Identification of the TOE interface at which the quota was exceeded.
IPS_ABD_EXT.1	Inspected traffic matches an anomaly-based IPS policy.	Source and destination IP addresses.
		The content of the header fields that were determined to match the policy.
		TOE interface that received the packet.
		Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, frequency, etc.).
		Network-based action by the TOE (e.g. allowed, blocked, sent reset to source IP, sent blocking notification to firewall).
IPS_IPB_EXT.1	Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy.	Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list).
		TOE interface that received the packet.
		Network-based action by the TOE (e.g. allowed, blocked, sent reset).
IPS_NTA_EXT.1	Modification of which IPS policies are active on a TOE interface. Enabling/disabling a TOE interface with IPS policies applied. Modification of which mode(s) is/are active on a TOE interface.	Identification of the TOE interface.
		The IPS policy and interface mode (if applicable).
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS rule with logging enabled.	Name or identifier of the matched signature.
		Source and destination IP addresses.
		The content of the header fields that were determined to match the signature.
		TOE interface that received the packet.
		Network-based action by the TOE (e.g. allowed, blocked, sent reset).

IPS_SBD_EXT.2.1 (optional)	Inspection of encapsulated packets.	Indication of the encapsulation method.
IPS_SBD_EXT.2.2 (optional)	Failure to re-assemble a fragmented packet.	Source and destination IP addresses.
		TOE interface that received the fragment(s).
IPS_SBD_EXT.2.3 (optional)	Normalization of traffic by the TOE.	Source and destination IP addresses of discarded packet(s).
		TOE interface that received the packet(s).

5.2.2 Security Management (FMT)

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

FMT_SMF.1.1/IPS The TSF shall be capable of performing the following management functions: [

- *Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality*
- *Modify these parameters that define the network traffic to be collected and analyzed:*
  - *Source IP addresses (host address and network address)*
  - *Destination IP addresses (host address and network address)*
  - *Source port (TCP and UDP)*
  - *Destination port (TCP and UDP)*
  - *Protocol (IPv4 and IPv6)*
  - *ICMP type and code*
- *Update (import) signatures*
- *Create custom signatures*
- *Configure anomaly detection*
- *Enable and disable actions to be taken when signature or anomaly matches are detected*
- *Modify thresholds that trigger IPS reactions*
- *Modify the duration of traffic blocking actions*
- *Modify the known-good and known-bad lists (of IP addresses or address ranges)*
- *Configure the known-good and known-bad lists to override signature-based IPS policies*].

5.2.3 Intrusion Prevention (IPS)

IPS_ABD_EXT.1 Anomaly-Based IPS Functionality

IPS_ABD_EXT.1.1 The TSF shall support the definition of [*selection: baselines ('expected and approved'), anomaly ('unexpected') traffic patterns*] including the specification of [*selection:*

- *throughput ([assignment: data elements (e.g. bytes, packets, etc.) per time period (e.g. minutes, hours, days)]);*
- *time of day;*

- *frequency;*
- *thresholds;*
- *[assignment: other methods]*]

and the following network protocol fields:

- [*selection: all packet header and data elements defined in IPS_SBD_EXT.1; [assignment: subset list of packet header and data elements from IPS_SBD_EXT.1]*].

Application Note: *Baselines are the definition of known-good traffic (to be allowed per IPS_ABD_EXT.1.3) whilst anomaly traffic is definition of ('offending') traffic that is to be handled per other actions defined in IPS_ABD_EXT.1.3. Frequency can be defined as a number of occurrences of an event (such as detection of packets matching a signature) over a defined period of time, such as the number of new FTP sessions established during 1 hour. Thresholds can be defined as an amount or percentage of deviation from expected levels or limits, such as a number of megabytes of data transferred via FTP per hour.*

IPS_ABD_EXT.1.2 The TSF shall support the definition of anomaly activity through [*selection: manual configuration by administrators, automated configuration*].

Application Note: *The "baseline" and "anomaly" can be something manually defined/configured by a TOE administrator (or importing definitions), or something that the TOE is able to automatically define/create by inspecting network traffic over a period of time (a.k.a. "profiling"). It is not essential for the IPS TOE to have a capability of "profiling" a network to dynamically defining a baseline or rule; if the product has this functionality, it is outside the scope of this PP-Module.*

IPS_ABD_EXT.1.3 The TSF shall allow the following operations to be associated with anomaly-based IPS policies:

- In any mode, for any sensor interface: [*selection:*
  - *allow the traffic flow*
  - *send a TCP reset to the source address of the offending traffic*
  - *send a TCP reset to the destination address of the offending traffic*
  - *send an ICMP [selection: host, destination, port] unreachable message*
  - *trigger a non-TOE network device to block the offending traffic pattern*]
- In inline mode:
  - [*allow the traffic flow*
  - *block/drop the traffic flow*
  - *and [selection: modify and forward packets before they pass through the TOE, no other actions]*].

IPS_IPB_EXT.1 IP Blocking

IPS_IPB_EXT.1.1 The TSF shall support configuration and implementation of known-good and

known-bad lists of [*selection: source, destination*] IP addresses and [*selection: no additional address types, [assignment: list of address types]*].

Application note: *The address types defined in this SFR are limited to IP addresses (e.g. a single IP address or a range of IP addresses) because this IPS PP-Module is limited to inspection of IP traffic. IPS TOEs are not prohibited from enabling functionality that would allow/prohibit traffic flow based on other address types, such as MAC addresses.*

IPS_IPB_EXT.1.2 The TSF shall allow [*Security Administrators*] to configure the following IPS policy elements: [*selection: known-good list rules, known-bad list rules, IP addresses, [assignment: other IPS policy elements], no other IPS policy elements*].

IPS_NTA_EXT.1 Network Traffic Analysis

IPS_NTA_EXT.1.1 The TSF shall perform analysis of IP-based network traffic forwarded to the TOE's sensor interfaces, and detect violations of administratively-defined IPS policies.

Application Note: *Though it might be the case in some TOEs that any TOE interface can be a sensor interface, that capability is not a requirement. This SFR uses the term "sensor interface" to refer to any TOE interface to which one or more IPS policy has been applied. An administratively-defined IPS policy is any set of rules for traffic analysis, traffic blocking, signature detection, and/or anomaly detection applied to one or more TOE interfaces. The TOE may be capable of allowing the administrator to configure the precedence of IPS policy elements (known-good lists, known-bad lists, signature-based rules, and anomaly- based rules), but any such configurability is not required by this PP-Module.*

IPS_NTA_EXT.1.2 The TSF shall process (be capable of inspecting) the following network traffic protocols:

- [*Internet Protocol version 4 (IPv4), RFC 791*
- *Internet Protocol version 6 (IPv6), RFC 2460*
- *Internet control message protocol version 4 (ICMPv4), RFC 792*
- *Internet control message protocol version 6 (ICMPv6), RFC 2463*
- *Transmission Control Protocol (TCP), RFC 793*
- *User Data Protocol (UDP), RFC 768*].

Application Note: *The identification of protocol RFCs does not imply that the TOE must ensure all packets are conformant to the identified protocol RFCs at all times, nor does it imply that the TOE would be able to enforce full conformance with the RFCs for any traffic flow at any time. The identification of RFCs provides a frame of reference for understanding the packet contents (headers, fields, states, commands, etc.) identified else in this and other SFRs. The implication is that the TOE must be capable of understanding the RFC implementation to the extent the RFC parameters are identified throughout the SFRs.*

IPS_NTA_EXT.1.3 The TSF shall allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as 'management' for

communication between the TOE and external entities without simultaneously being sensor interfaces.

- Promiscuous (listen-only) mode: [*assignment: list of interface types*];
- Inline (data pass-through) mode: [*assignment: list of interface types*];
- Management mode: [*assignment: list of interface types*];
- [*selection:*
    - *[Session-reset-capable interfaces: [assignment: list of session-reset-capable interfaces];*
    - *[assignment: other interface types]];*
    - *no other interface types*].

Application Note: *Interface types may be Ethernet, Gigabit Ethernet, etc. Promiscuous interfaces are ones that listen to network traffic for the sole purpose of inspecting the traffic, but do not provide any OSI Layer 2, Layer 3, or higher layer functionality, so network services are not listening on the interface, and no IP protocol stack enabled on the interface so no IP address is assigned to the interface. Inline interfaces are interface pairings that provide a path for network traffic to traverse the TOE such that traffic flows can be blocked or modified by the TOE in real-time. Like promiscuous interfaces, inline interfaces typically do not support OSI Layer 3 and higher functionality, though they may provide OSI Layer 2 functionality (with MAC address assigned to the interfaces) to allow adjacent network devices to forward traffic to/through the TOE.*

The TOE may support separate interfaces to be used for administration/management purposes that can be configured as OSI Layer 3 interfaces for communication between the TOE and remote entities including all entities defined in FTP_ITC, and FTP_TRP. The TOE may optionally support additional interface types. Session-reset interfaces can be the same as any of the promiscuous, inline, management, or other interfaces, or can be separate interfaces. Session-reset functionality is not mandatory functionality for the TOE, but is a selectable option within the SFR.

As mentioned in the application note for IPS_NTA_EXT.1.1, it's not necessary for the TOE to have multiple single-purpose interfaces (e.g. "sensor" interface, "management" interface, etc.), though it is expected that the TOE be able to enable specific ports to serve one or more specific interface functions.

IPS_SBD_EXT.1 Signature-Based IPS Functionality

IPS_SBD_EXT.1.1 The TSF shall support inspection of packet header contents and be able to inspect at least the following header fields: [

- *IPv4: version; header length; packet length; ID; IP flags; fragment offset; time to live (TTL); protocol; header checksum; source address; destination address; IP options; and [selection: type of service (ToS), no other field].*
- *IPv6: version; payload length; next header; hop limit; source address; destination address; routing header; and [selection: traffic class, flow label, no other field].*

- *ICMP: type; code; header checksum; and [selection: ID, sequence number, [assignment: other field in the ICMP header]].*
- *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*].

IPS_SBD_EXT.1.2 The TSF shall support inspection of packet payload data and be able to inspect at least the following data elements to perform string-based pattern-matching: [

- *ICMPv4 data: characters beyond the first 4 bytes of the ICMP header.*
- *ICMPv6 data: characters beyond the first 4 bytes of the ICMP header.*
- *TCP data (characters beyond the 20 byte TCP header), with support for detection of:*

    i) FTP (file transfer) commands: 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: commands including GET and POST, and administrator- defined strings to match URLs/URIs, and web page content.
    iii) SMTP (email) states: start state, SMTP commands state, mail header state, mail body state, abort state.
    iv) [selection: [assignment: other types of TCP payload inspection], no other types of TCP payload inspection];

- *UDP data: characters beyond the first 8 bytes of the UDP header;*
- *[assignment: other types of packet payload inspection]*].

IPS_SBD_EXT.1.3 The TSF shall be able to detect the following header-based signatures (using fields identified in IPS_SBD_EXT.1.1) at IPS sensor interfaces: [

a) IP Attacks

i) IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)
ii) IP source address equal to the IP destination (Land attack)

b) ICMP Attacks

i) Fragmented ICMP Traffic (e.g. Nuke attack)
ii) Large ICMP Traffic (Ping of Death attack)

c) TCP Attacks

i) TCP NULL flags
ii) TCP SYN+FIN flags
iii) TCP FIN only flags
iv) TCP SYN+RST flags

d) UDP Attacks

i) UDP Bomb Attack
ii) *UDP Chargen DDoS Attack*].

IPS_SBD_EXT.1.4 The TSF shall be able to detect all the following traffic-pattern detection signatures, and to have these signatures applied to IPS sensor interfaces: [

a) Flooding a host (DoS attack)

i) ICMP flooding (Smurf attack, and ping flood)
ii) TCP flooding (e.g. SYN flood)

b) Flooding a network (DoS attack)

c) Protocol and port scanning

i) IP protocol scanning
ii) TCP port scanning
iii) UDP port scanning
iv) *ICMP scanning*].

Application Note: *This SFR defines the minimum set of packet header fields, packet payload strings, signature types, and potentially malicious traffic patterns (e.g. flooding and scanning) that the TOE must be able to detect. Valid signatures can be comprised of one, some, or all attributes listed in this SFR, and IPS TOEs may support inspection of additional attributes not listed in this SFR, but only those listed in the SFR will be tested by the evaluators. The set of signature types, traffic patterns, etc. identified in this SFR are not intended to be an exhaustive or completely representative list of malicious activity, nor is it meant to address DDoS attacks – the intent of this SFR is addressing attacks form a single source IP.*

Protocol and port scanning refers to reconnaissance attacks that scan target IP addresses for open/listening/responsive services by targeting multiple protocols/ports on one or more target IP address using obvious (sequentially numbered) patterns of target protocol/port numbers or by randomizing the protocol/port numbers and/or randomizing the time delays between transmissions.

It is understood and expected that IPS product vendors will support pre-defined signatures, but inspection of the efficacy of the pre-defined signatures themselves is not objective of this PP-Module. Instead, this PP-Module focuses on the ability of the TOE to perform detailed analysis of network traffic, and those pre-defined signatures may be used during evaluation, the evaluation team is expected to make use of custom-made signatures as well. This set of signature types, traffic patterns, etc. has been selected to: 1) place reasonable boundaries around the scope of testing; and 2) provide a sufficient sampling of packet contents, and traffic patterns to demonstrate the TOE's ability to inspect packet contents, to collect traffic pattern statistics over a period of time, and to correlate collected data.

An IPS sensor interface refers to any TOE interface to which an IPS policy is currently applied.

IPS_SBD_EXT.1.5 The TSF shall allow the following operations to be associated with signature-based IPS policies:

- In any mode, for any sensor interface: [*selection:*
  - *allow the traffic flow;*
  - *send a TCP reset to the source address of the offending traffic;*
  - *send a TCP reset to the destination address of the offending traffic;*
  - *send an ICMP [selection: host, destination, port] unreachable message;*
  - *trigger a non-TOE network device to block the offending traffic pattern*]
- In inline mode:
  - block/drop the traffic flow;
  - and [*selection:*
    - *allow all traffic flow;*
    - *allow the traffic flow with following exceptions: [assignment: malicious traffic such as but not limited to IPS_EXT.1.3 and IPS_EXT.1.4 if always dropped];*
    - *modify and forward packets before they pass through the TOE*].

Application Note: *The term "trigger" is used to allow for multiple types of interactions, including: one in which the TOE initiates a authenticated connection to the remote device across an IP network and uses a remote administration interface of the remote device to modify the active configuration on that device; or one in which the connection between the TOE and the non-TOE network device does not traverse an IP network. If the ST author selects "trigger a non-TOE network device…" and the connection between the TOE and the non-TOE network device traverses an IP network, the ST author must ensure that the non- TOE device type is identified within FTP_ITC.1.3 (of the base), and the connection between the TOE and the remote device must be secured in accordance with FTP_ITC.1. In the last bullet of the SFR, "modify and forward packets before they pass through the TOE," could include such actions as removing from packet data character strings that match regular expression (regex) conditions that violate policies, such as transmitting personally identifiable information or other private data (phone numbers, credit-card numbers, etc.).*

IPS_SBD_EXT.1.6 The TSF shall support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 5: SFR-Objective Rationale

Objective	Addressed By	Rationale
O.IPS_ANALYZE	IPS_ABD_EXT.1	This SFR supports the objective by defining the TOE's ability to analyze network traffic for anomalous behavior that could indicate malicious activity.
	IPS_IPB_EXT.1	This SFR supports the objective by defining how the TOE can analyze traffic representing known-good and known-bad activities based on IP address.
	IPS_NTA_EXT.1	This SFR supports the objective by defining the TOE's ability to analyze network traffic based on supported protocols and network architecture characteristics.
	IPS_SBD_EXT.1	This SFR supports the objective by defining the TOE's ability to detect potential malicious activity based on packet signatures.
	FPT_FLS.1 (optional)	This SFR supports the objective by optionally defining the TOE's ability to fail closed for inline traffic if a TSF failure occurs. This ensures that network traffic will not be processed without analysis.
	IPS_SBD_EXT.2 (optional)	This SFR supports the objective by optionally defining the ability of the TSF to inspect traffic that is embedded in an encapsulation protocol.
	FRU_RSA.1 (implementation-dependent)	This SFR supports the objective by optionally enforcing maximum quotas for network traffic inspection resources so that the rate network traffic flow cannot exceed the ability of the TSF to process the traffic as it is received.
O.IPS_REACT	IPS_ABD_EXT.1	This SFR supports the objective by specifying the TOE's reaction to the detection of anomalous network traffic.
	IPS_SBD_EXT.1	This SFR supports the objective by specifying the TOE's reaction to the detection of an IPS signature in processed network traffic.
	FAU_ARP.1 (objective)	This SFR supports the objective by optionally defining the actions taken if a potential security violation is detected.

Objective	Addressed By	Rationale
O.SYSTEM_MONITORING	FAU_GEN.1/IPS	This SFR supports the objective by defining the network traffic data that the TSF collects.
	FAU_STG.1/IPS (optional)	This SFR supports the objective by optionally defining the TOE's ability to protect the stored network traffic data from unauthorized changes or removal.
	FAU_STG.4 (optional)	This SFR supports the objective by optionally defining the TOE's behavior in the case where storage of network traffic data has been exhausted.
	FAU_SAR.1 (objective)	This SFR supports the objective by optionally defining a mechanism that can be used to review the stored network traffic data.
	FAU_SAR.2 (objective)	This SFR supports the objective by optionally defining a mechanism that can be used to review the stored network traffic data.
	FAU_SAR.3 (objective)	This SFR supports the objective by optionally defining a mechanism that can be used to review the stored network traffic data.
O.TOE_ADMINISTRATION	FMT_SMF.1/IPS	This SFR supports the objective by defining the management functions used to manage the TOE's IPS functionality. The Base-PP's FMT_SMR.2 requirement ensures that only authorized administrators can perform these functions.

5.4 TOE Security Assurance Requirements

This PP-Module does not define any SARs beyond those defined by the Base-PP. It is important to note that these SARs are applied to the entire TOE and not just to the portion of the TOE defined by the PP or PP-Module in which the SARs are located.

This PP-Module does provide specific guidance on how the SARs are evaluated for conformance to this PP-Module. The Supporting Document that accompanies this PP-Module defines the additional Evaluation Activities that are to be performed.

6. Consistency Rationale

6.1 NDcPP Base

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include IPS functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

Table 6: Threat Consistency Rationale

PP-Module Threat	Consistency Rationale
T.NETWORK_ACCESS	The NDcPP only defines a security problem that relates to network traffic bound to or originating from the TOE. This PP-Module expands the security problem to include a logical interface for network traffic between two non-TOE endpoints that is intercepted (inline) or observed (promiscuous) by the TSF. This is not inconsistent because the PP-Module introduces a new logical interface for this functionality that is beyond the scope of the NDcPP.
T.NETWORK_DISCLOSURE	The NDcPP only defines a security problem that relates to network traffic bound to or originating from the TOE. This PP-Module expands the security problem to include a logical interface for network traffic between two non-TOE endpoints that is intercepted (inline) or observed (promiscuous) by the TSF. This is not inconsistent because the PP-Module introduces a new logical interface for this functionality that is beyond the scope of the NDcPP.
T.NETWORK_DOS	The NDcPP only defines a security problem that relates to network traffic bound to or originating from the TOE. This PP-Module expands the security problem to include a logical interface for network traffic between two non-TOE endpoints that is intercepted (inline) or observed (promiscuous) by the TSF. This is not inconsistent because the PP-Module introduces a new logical interface for this functionality that is beyond the scope of the NDcPP.
T.NETWORK_MISUSE	The NDcPP only defines a security problem that relates to network traffic bound to or originating from the TOE. This PP-Module expands the security problem to include a logical interface for network traffic between two non-TOE endpoints that is intercepted (inline) or observed (promiscuous) by the TSF. This is not inconsistent because the PP-Module introduces a new logical interface for this functionality that is beyond the scope of the NDcPP.

The assumptions defined in this PP-Module are consistent with the NDcPP based on the following rationale:

Table 7: Assumptions Consistency Rationale

PP-Module Assumption	Consistency Rationale
A.CONNECTIONS	This assumption requires a specific network configuration to ensure that network traffic cannot be routed in a way that allows it to bypass the TOE's inspection interfaces. This does not interfere with any of the assumptions in

PP-Module Assumption	Consistency Rationale
	the NDcPP because the NDcPP doesn't make any assumptions about the TOE's position in a network architecture.

The organizational security policies defined in this PP-Module are consistent with the NDcPP based on the following rationale:

Table 8: Organizational Security Policies Consistency Rationale

PP-Module Policy	Consistency Rationale
P.ANALYZE	This organizational security policy does not conflict with the NDcPP because it sets expectations for administrative use of the data that is specifically collected by the TOE's IPS function.

6.1.3 Consistency of Objectives

The Base-PP does not define any TOE objectives; the TOE objectives that are defined by this PP-Module are all mapped to SFRs defined in the Base-PP and PP-Module. Because of this, consistency of the PP-Module's TOE objectives with the Base-PP is demonstrated in Section 6.1.4 below.

The objectives for the TOE's operational environment are consistent with the NDcPP based on the following rationale:

Table 9: Environmental Objective Consistency Rationale

PP-Module Environmental Objective	Consistency Rationale
OE.CONNECTIONS	This objective expects the TOE to be deployed in a network architecture that insures that network traffic cannot be routed in a way that allows it to bypass the TOE's inspection interfaces. This does not interfere with any of the environmental objectives in the NDcPP because the NDcPP doesn't have any objectives that relate to the TOE's position in a network architecture.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support IPS functionality. This is considered to be consistent because the functionality provided by the network device is being used for its intended purpose. The PP-Module also identifies a number of new SFRs that are used entirely to provide IPS functionality. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 10: SFR Consistency Rationale

PP-Module Requirement	Consistency Rationale
Mandatory SFRs	
FAU_GEN.1/IPS	The PP-Module iterates an SFR defined in the Base-PP to define additional audit events specific to IPS functionality that the IPS part of the TOE must generate.
FMT_SMF.1/IPS	The PP-Module iterates an SFR defined in the Base-PP to define additional management functions specific to the IPS functionality that the IPS part of

PP-Module Requirement	Consistency Rationale
	the TOE must generate. Authorizations to perform these functions are based on FMT_SMR.2 defined by the Base-PP.
IPS_ABD_EXT.1	This SFR applies to IPS functionality, which is beyond the original scope of the Base-PP.
IPS_IPB_EXT.1	This SFR applies to IPS functionality, which is beyond the original scope of the Base-PP.
IPS_NTA_EXT.1	This SFR applies to IPS functionality, which is beyond the original scope of the Base-PP.
IPS_SBD_EXT.1	This SFR applies to IPS functionality, which is beyond the original scope of the Base-PP.
Optional SFRs	
FAU_STG.1/IPS	The PP-Module iterates an SFR defined in the Base-PP to define an optional capability for the protection of the IPS data generated by FAU_GEN.1/IPS.
FAU_STG.4	This SFR applies to IPS audit data, which is beyond the original scope of the Base-PP.
FPT_FLS.1	This SFR applies to secure failure for inline interfaces, which is a type of logical interface that was introduced in this PP-Module and therefore doesn't interfere with the Base-PP.
FRU_RSA.1	This SFR applies to quota enforcement on network interfaces that perform scanning of network traffic for enforcement of IPS requirements. This functionality was introduced in this PP-Module and therefore doesn't interfere with the Base-PP.
IPS_SBD_EXT.2	This SFR applies to IPS functionality, which is beyond the original scope of the Base-PP.
Objective SFRs	
FAU_ARP.1	This SFR applies to IPS functionality, which is beyond the scope of the original Base-PP.
FAU_SAR.1	This SFR applies to review of collected IPS data, which is beyond the scope of the original Base-PP.
FAU_SAR.2	This SFR applies to review of collected IPS data, which is beyond the scope of the original Base-PP.
FAU_SAR.3	This SFR applies to review of collected IPS data, which is beyond the scope of the original Base-PP.

A. Optional Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP-Module. This Appendix contains three other types of optional requirements that may be included in the ST but are not required in order to conform to this PP-Module.

The first type (in A.1) are strictly optional requirements that are independent of the TOE implementing any function. If the TOE fulfills any of these requirements or supports a certain functionality, the vendor is encouraged but not required to add the related SFRs.

The second type (in A.2) are objective requirements that describe security functionality not yet widely available in commercial technology. The requirements are not currently mandated in the body of this PP-Module, but will be included in the baseline requirements in future versions of this PP-Module. Adoption by vendors is encouraged and expected as soon as possible.

The third type (in A.3) are implementation-dependent requirements that are dependent on the TOE implementing a particular function. If the TOE fulfills any of these requirements, the vendor must either add the related SFR or disable the functionality for the evaluated configuration.

A.1 Strictly Optional Requirements

A.1.1 FAU_STG.1/IPS Protected Audit Trail Storage (IPS Data)

FAU_STG.1.1/IPS The TSF shall protect the stored ~~audit records~~ **IPS data** from unauthorized deletion.

FAU_STG.1.2/IPS The TSF shall be able to [*prevent*] unauthorized modifications to the stored ~~audit records~~ **IPS data** ~~in the audit trail~~.

A.1.2 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall **be able to** [*selection: ignore* ***~~audited~~ generation of IPS*** *events* ***that would otherwise be generated****, prevent audited* ***IPS*** *events,* ~~*except those taken by the authorized user with special rights,*~~ *overwrite the oldest stored* ~~*audit records*~~ *IPS data*], and [*no other actions*] if the ~~audit~~ **IPS data** trail is full.

A.1.3 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall **be able to** preserve a secure state **for inline interfaces** when the following types of failures occur: [*assignment: list of types of failures in the TSF*].

Application Note: *The intent of this SFR is to allow the ST author to define the types of failures that can occur on the TOE which could result in failure to effectively detect and react to IPS policy violations for traffic traversing inline interface, and to not allow traffic to traverse those interfaces. The first refinement "to be able" is included to allow the TOE administrator to configure the TOE to allow traffic to traverse inline interfaces when the TOE is in a partially of fully failed state, but to provide assurance that the TOE is capable of blocking traffic if it has been configured to do so. The purpose of this SFR, as stated in CC Part 2, is to "ensure that the TOE will always enforce its SFRs in the event of identified categories of failures in the TSF." Since some of the SFRs require inspection of data, and that*

inspection cannot occur when a network interface fails, it will not always be true that "all" the SFRs will continue to be enforced in the event of failure of certain components. The intent here is to ensure that if network traffic is not capable of being inspected by the TSF, then it should automatically be treated as untrusted.

A.1.4 IPS_SBD_EXT.2 Traffic Normalization

IPS_SBD_EXT.2.1 The TSF shall be able to inspect packets encapsulated through the following means: [*selection: GRE, IP-in-IP, IPv4-in-IPv6, MPLS, PPTP, [assignment: other encapsulation methods]*].

IPS_SBD_EXT.2.2 The TSF shall be able to perform IP normalization to reassemble fragmented packets for inspection, and: [*selection:*

- *For data collected at promiscuous interfaces: generate an alert if the packet cannot be reassembled;*
- *For data collected at inline interfaces: do not forward any packet fragments and generate an alert if the TSF cannot reassemble the entire packet*].

IPS_SBD_EXT.2.3 The TSF shall be able to perform TCP normalization for traffic flows through the TOE when the TOE is deployed in inline mode, and prohibit forwarding of: [*selection:*

- *duplicate packets;*
- *changed packets;*
- *out-of-sequence packets;*
- *[selection: [assignment: other packet types that should not be forwarded], no other packets]*]

A.2 Objective Requirements

A.2.1 FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [*assignment: list of actions*] upon detection of a potential security violation.

Application Note: *At minimum, the set of potential security violations must include network traffic in excess of maximum quotas. Therefore, when this SFR is included, the ST author must also include FRU_RSA.1.*

In CC Part 2, FAU_ARP is intended to depend on FAU_SAA to define a potential violation of the SFRs. FAU_SAA is not included in this IPS EP; FRU_RSA and the various IPS class requirements are used instead to define the "potential security violation" relevant to FAU_ARP, namely that the TOE has detected potential malicious network traffic or has experienced a spike in network traffic that has exceeded its ability to inspect all network traffic which may result in some network traffic being uninspected by the TSF. This SFR should be used to define actions that the IPS TOE can take which may include generating one or more messages that are not part of the audit trail that must be transmitted securely to a remote audit server.

Messaging actions defined by this SFR that are not specifically relevant to FAU_GEN.1/IPS do not need to be encrypted during transit. The primary intent of this functionality is the speed of notification, not the integrity, or confidentiality of the data in transit. In most cases, the audit trail applicable to FAU_STG_EXT.1 will be syslog data, and is being protected in transit to help ensure integrity of remotely stored audit data. This SFR is intended to cover transmission of messages related to single events through protocols such as SNMP (traps) and SMTP (email). In TOEs that support securing SNMP traps, SMTP email, or other messaging types within trusted channels (as defined by FTP_ITC.1), the ST author can choose to list these messaging methods within FTP_ITC.1 and/or within this SFR. There are no additional auditable IPS events that need to be included in FAU_GEN.1/IPS.

A.2.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*authorized administrators*] with the capability to read [*IPS data*] from the ~~audit records~~ **IPS events**.

FAU_SAR.1.2 The TSF shall provide the ~~audit records~~ **IPS data** in a manner suitable for the ~~user~~ **administrators** to interpret the information.

Application Note: *It is anticipated, but not required, that TOEs would provide a graphical user interface that would allow searching and sorting, and it would be acceptable for such output to group similar events together to ease administrative review of the IPS data. For example, the display might allow grouping of data by event type, or by source IP address, where multiple events that occurred in a time period are displayed on a single line as in the sample table below. Regardless whether such a view is provided, it is expected that the administrator will be able to view the details of individual event occurrences.*

Time/Date	Event Type	Reaction	Event total
2013-01-1 10:45:00	Port scan from 10.1.2.3	Blocked all traffic from 10.1.2.3	34

A.2.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all ~~users~~ **administrators** read access to the ~~audit records~~ **IPS data,** except those that have been granted explicit read-access.

A.2.4 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering and sorting*] of ~~audit~~ **IPS data** based on [*filtering parameters: risk rating, time period, source IP address, destination IP address and* [*selection: [assignment: other filtering parameters]; no other filtering parameters*]; *and sorting parameters: event ID, event type, time, signature ID, IPS actions performed, and* [*selection: [assignment: other sorting parameters; no other sorting parameters]*].

A.3 Implementation-Dependent Requirements

A.3.1 FRU_RSA.1 Maximum Quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*resources supporting inspection of network traffic*] that [*subjects*] can use [*simultaneously*].

Application Note: *This SFR is optional but the behavior specified by FAU_ARP.1 requires this function to be implemented. Therefore, this SFR is implementation-dependent on the condition that it be claimed if FAU_ARP.1 is claimed. If FAU_ARP.1 is not claimed this SFR should also not be claimed because effective enforcement of maximum quotas requires an alert mechanism when quotas are exceeded. Otherwise it is not possible for an administrator to determine whether a lack of potential security violations is caused by an absence of potential malicious activity or by the inability of the TSF to detect such activity due to an inability to process the volume of traffic being received.*

Conformant TOEs will impose quotas on exhaustible resources used to support inspection of network traffic that 'subjects' (inspected network traffic flows) can use simultaneously. The intent of this requirement is to ensure that the TOE is not deployed in such a way that the flow of data across its sensor interfaces can exceed the amount of traffic that the TOE is capable of inspecting. If the flow (volume/speed) of data to be inspected exceeds the defined quota, the TOE should trigger an alert signifying effect of the exceeded quota. For example, when the TOE is deployed inline, exceeding the quota may result in the TSF dropping (not forwarding) and failing to inspect network traffic; or when the TOE is not deployed inline, exceeding the quota may result in traffic having been forwarded without inspection. In any case, exceeding the maximum quota results in a "potential security violation" relevant to FAU_ARP.1 in that the TSF may have failed to inspect some network traffic.

B. Selection-Based Requirements

There are no selection-based requirements defined for this PP-Module.

C. Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

C.1 Background and Scope

This Appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

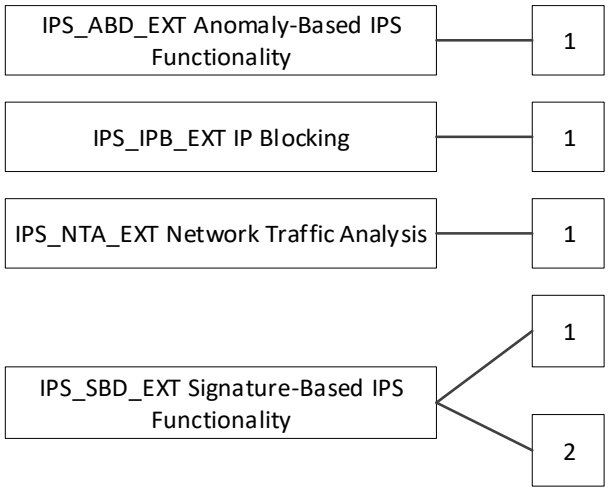
Table 11: Extended Components Definitions

Functional Class	Functional Components
Intrusion Prevention System (IPS)	IPS_ABD_EXT Anomaly-Based IPS Functionality
	IPS_IPB_EXT IP Blocking
	IPS_NTA_EXT Network Traffic Analysis
	IPS_SBD_EXT Signature-Based IPS Functionality

C.2 Extended Component Definitions

C.2.1 Class IPS: Intrusion Prevention System

Intrusion prevention involves the TOE's ability to collect network packets, examine their contents for information that suggests malicious activity, and to perform some action in response such as terminating the connection.

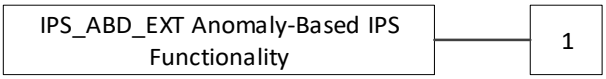


IPS_ABD_EXT Anomaly-Based IPS Functionality

Family Behavior

This family defines requirements for detection of anomalous network traffic and how the TSF should respond if an anomaly is detected.

Component Leveling



IPS_ABD_EXT.1 Anomaly-Based IPS Functionality, requires the TSF to detect anomalous network traffic based on some criteria and to define the response that is issued if an anomaly is detected.

Management: IPS_ABD_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuration of anomaly detection.
b) Enabling and disabling actions to be taken when anomaly matches are detected.
c) Modification of thresholds that trigger IPS reactions.
d) Modification of the duration of traffic blocking actions.

Audit: IPS_ABD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Inspected traffic that matches an anomaly-based IPS policy.

IPS_ABD_EXT.1 Anomaly-Based IPS Functionality

Hierarchical to: No other components.

Dependencies: IPS_NTA_EXT.1 Network Traffic Analysis

IPS_SBD_EXT.1 Signature-Based IPS Functionality

IPS_ABD_EXT.1.1 The TSF shall support the definition of [*selection: baselines ('expected and approved'), anomaly ('unexpected') traffic patterns*] including the specification of [*assignment: attributes or characteristics of network traffic*].

and the following network protocol fields:

- [*assignment: protocol fields*].

IPS_ABD_EXT.1.2 The TSF shall support the definition of anomaly activity through [*selection: manual configuration by administrators, automated configuration*].

IPS_ABD_EXT.1.3 The TSF shall allow the following operations to be associated with anomaly-based IPS policies:

- In any mode, for any sensor interface: [*assignment: action taken by TSF in response to detection of anomaly*]
- In inline mode: [*assignment: action taken by TSF In response to detection of anomaly]*].

IPS_IPB_EXT IP Blocking

Family Behavior

This family defines requirements for handling of inspected network traffic based on IP address.

Component Leveling

IPS_IPB_EXT.1 IP Blocking, requires the TSF to enforce IPS policies that are based on IP address.

Management: IPS_IPB_EXT.1

The following actions could be considered for the management functions in FMT:

a) Modification of the known-good and known-bad lists (of IP addresses or address ranges).
b) Configuration of the known-good and known-bad lists to override signature-based IPS policies.

Audit: IPS_IPB_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy.

IPS_IPB_EXT.1 IP Blocking

Hierarchical to:	No other components.
Dependencies:	IPS_NTA_EXT.1 Network Traffic Analysis
	FMT_SMR.1 Security Roles
IPS_IPB_EXT.1.1	The TSF shall support configuration and implementation of known-good and known-bad lists of [*selection: source, destination*] IP addresses and [*selection: no additional address types, [assignment: list of address types]*].
IPS_IPB_EXT.1.2	The TSF shall allow [*assignment: authorized roles*] to configure the following IPS policy elements: [*assignment: IPS policy elements*].

IPS_NTA_EXT Network Traffic Analysis

Family Behavior

This family defines the network traffic protocols the TOE is capable of analyzing and detecting violations for.

Component Leveling

IPS_NTA_EXT.1 Network Traffic Analysis, requires the TSF to be able to inspect traffic for certain network protocols and in certain architectural deployments.

Management: IPS_NTA_EXT.1

The following actions could be considered for the management functions in FMT:

a) Modification of the parameters that define the network traffic to be collected and analyzed.

Audit: IPS_NTA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Modification of which IPS policies are active on a TOE interface.
b) Enabling/disabling a TOE interface with IPS policies applied.
c) Modification of which mode(s) is/are active on a TOE interface.

IPS_NTA_EXT.1 Network Traffic Analysis

Hierarchical to: No other components.

Dependencies: No dependencies.

IPS_NTA_EXT.1.1 The TSF shall perform analysis of IP-based network traffic forwarded to the TOE's sensor interfaces, and detect violations of administratively-defined IPS policies.

IPS_NTA_EXT.1.2 The TSF shall process (be capable of inspecting) the following network traffic protocols:

- [*assignment: network protocols and any standard(s) that define their implementation*].

IPS_NTA_EXT.1.3 The TSF shall allow the signatures to be assigned to sensor interfaces configured for promiscuous mode, and to interfaces configured for inline mode, and support designation of one or more interfaces as 'management' for communication between the TOE and external entities without simultaneously being sensor interfaces.

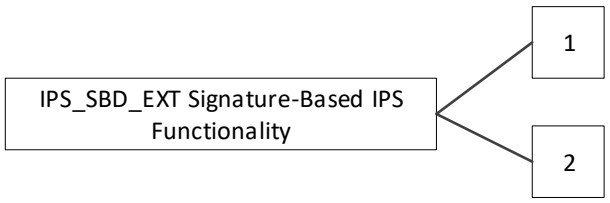
- Promiscuous (listen-only) mode: [*assignment: list of interface types*];
- Inline (data pass-through) mode: [*assignment: list of interface types*];
- Management mode: [*assignment: list of interface types*];
- [*selection:*
  - *[assignment: other interface types];*
  - *no other interface types*].

IPS_SBD_EXT Signature-Based IPS Functionality

Family Behavior

This family defines requirements for analysis of network traffic based on packet characteristics.

Component Leveling



IPS_SBD_EXT.1 Signature-Based IPS Functionality, requires the TSF to detect network traffic with certain packet characteristics and take some action when this traffic is detected.

IPS_SBD_EXT.2 Traffic Normalization, requires the TSF to support the inspection of encapsulated or fragmented traffic by normalizing it.

Management: IPS_SBD_EXT.1

The following actions could be considered for the management functions in FMT:

a) Enabling and disabling signatures applied to sensor interfaces.
b) Updating (importing) signatures.
c) Creating custom signatures.
d) Enabling and disabling actions to be taken when signature matches are detected.

Audit: IPS_SBD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Inspected traffic matches a signature-based IPS rule with logging enabled.

Management: IPS_SBD_EXT.2

No specific management functions are identified.

Audit: IPS_SBD_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Inspection of encapsulated packets Session
b) Failure to re-assemble a fragmented packet
c) Normalization of traffic by the TOE

IPS_SBD_EXT.1 Signature-Based IPS Functionality

Hierarchical to: No other components.

Dependencies: IPS_NTA_EXT.1 Network Traffic Analysis

IPS_SBD_EXT.1.1 The TSF shall support inspection of packet header contents and be able to inspect at least the following header fields: [*assignment: applicable header fields for each supported network protocol*].

IPS_SBD_EXT.1.2 The TSF shall support inspection of packet payload data and be able to inspect at least the following data elements to perform string-based pattern-matching: [*assignment: applicable packet payload data elements for each supported network protocol*].

IPS_SBD_EXT.1.3 The TSF shall be able to detect the following header-based signatures (using fields identified in IPS_SBD_EXT.1.1) at IPS sensor interfaces: [*assignment: applicable header-based signatures for identified header fields*].

IPS_SBD_EXT.1.4 The TSF shall be able to detect all the following traffic-pattern detection

signatures, and to have these signatures applied to IPS sensor interfaces: [*assignment: list of traffic patterns*].

IPS_SBD_EXT.1.5 The TSF shall allow the following operations to be associated with signature-based IPS policies:

- In any mode, for any sensor interface: [*assignment: action taken by TSF in response to detection of signature*]
- In inline mode:
  - block/drop the traffic flow;
  - and [*assignment: action taken by TSF in response to detection of signature*].

IPS_SBD_EXT.1.6 The TSF shall support stream reassembly or equivalent to detect malicious payload even if it is split across multiple non-fragmented packets.

IPS_SBD_EXT.2 Traffic Normalization

Hierarchical to: No other components.

Dependencies: IPS_NTA_EXT.1 Network Traffic Analysis

IPS_SBD_EXT.2.1 The TSF shall be able to inspect packets encapsulated through the following means: [*assignment: traffic encapsulation methods*].

IPS_SBD_EXT.2.2 The TSF shall be able to perform IP normalization to reassemble fragmented packets for inspection, and: [*selection:*

- *For data collected at promiscuous interfaces: generate an alert if the packet cannot be reassembled;*
- *For data collected at inline interfaces: do not forward any packet fragments and generate an alert if the TSF cannot reassemble the entire packet*].

IPS_SBD_EXT.2.3 The TSF shall be able to perform TCP normalization for traffic flows through the TOE when the TOE is deployed in inline mode, and prohibit forwarding of: [*assignment: characteristics of invalid packets*].

D. Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP. However, these requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Table 12: Implicitly Satisfied Requirements Rationale

Requirement	Rationale for Satisfaction
FAU_ARP.1 – Security Alarms	FAU_ARP.1 has a dependency on FAU_SAA.1. This is because FAU_SAA.1 defines the behavior that the TSF may consider to be a potential security violation while FAU_ARP.1 defines what actions the TSF takes when such behavior is detected. This dependency is implicitly satisfied in this PP-Module because the behavior defined in FRU_RSA.1 and the various IPS class requirements collectively define potential security violation behavior so a separate SFR to enumerate this is redundant.
FAU_GEN.1/IPS – Audit Data Generation (IPS)	FAU_GEN.1 has a dependency on FPT_STM.1 The extended SFR FPT_STM_EXT.1 that is defined in the Base-PP provides equivalent functionality to FPT_STM.1 and therefore satisfies this dependency.

E. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PP.

F. References

Table 13: References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2070-04-001, 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 • CC and CEM addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB-2017-05-xxx, Version 0.5, May 2017
[NDcPP]	Collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[SD]	Supporting Document Mandatory Technical Document, PP-Module for IPS, Version 1.0, May 11, 2021

G. Acronyms

The acronym definitions in the NDcPP should be consulted in addition to those defined here.

Table 14: Acronyms

Acronym	Meaning
DDoS	Distributed Denial of Service
DoS	Denial of Service
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