Network Device Protection Profile (NDPP)
Extended Package (EP) for Intrusion Prevention Systems (IPS)

26 June 2014
Version 1.0

Table of Contents

Tables

Figures

1 Introduction

This Extended Package (EP) describes security requirements for a network-based Intrusion Prevention System (IPS) (defined to be an intrusion prevention product located within or at the edge of a private network that can collect, inspect, analyze, and react to network traffic in real-time) and is intended to provide a minimal baseline set of requirements that are targeted at mitigating well defined and described threats. This EP is not complete in itself, but rather extends the *Security Requirements for Network Devices* protection profile (NDPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDPP.

1.1 Conformance Claims

The *Security Requirements for Network Devices* Protection Profile (NDPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDPP baseline with additional SFRs and associated 'Assurance Activities' specific to IPS devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 3. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

As an EP of the NDPP, it is expected that the content of both this EP and the NDPP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in so doing. An ST must identify the applicable versions of the NDPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

When this EP is used to build on the NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

It is intended that the set of requirements in this EP is limited in scope in order to promote quicker, less costly evaluations that provide some value to end users.

1.3 Compliant Targets of Evaluation

This EP specifically addresses network-based Intrusion Prevention Systems (IPS). A conformant IPS is a product that is connected to one or more distinct networks and is managed as part of an overall enterprise security solution. In particular, a compliant IPS provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious network traffic. This EP 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 EP and to allow future EPs to address other IPS and functionality that includes scanners, analyzers, sensors, etc. The scope of the EP does not preclude support for inspection of other IP protocols (e.g. GRE, ESP, AH), but the scope of this EP does not include the evaluation of non-IP protocols including layer-2 protocols, or Ethernet.

The baseline requirements of this EP 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, 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 FCS_STG_EXT.1 of the NDPP.
- 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's 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 IPS 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 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.

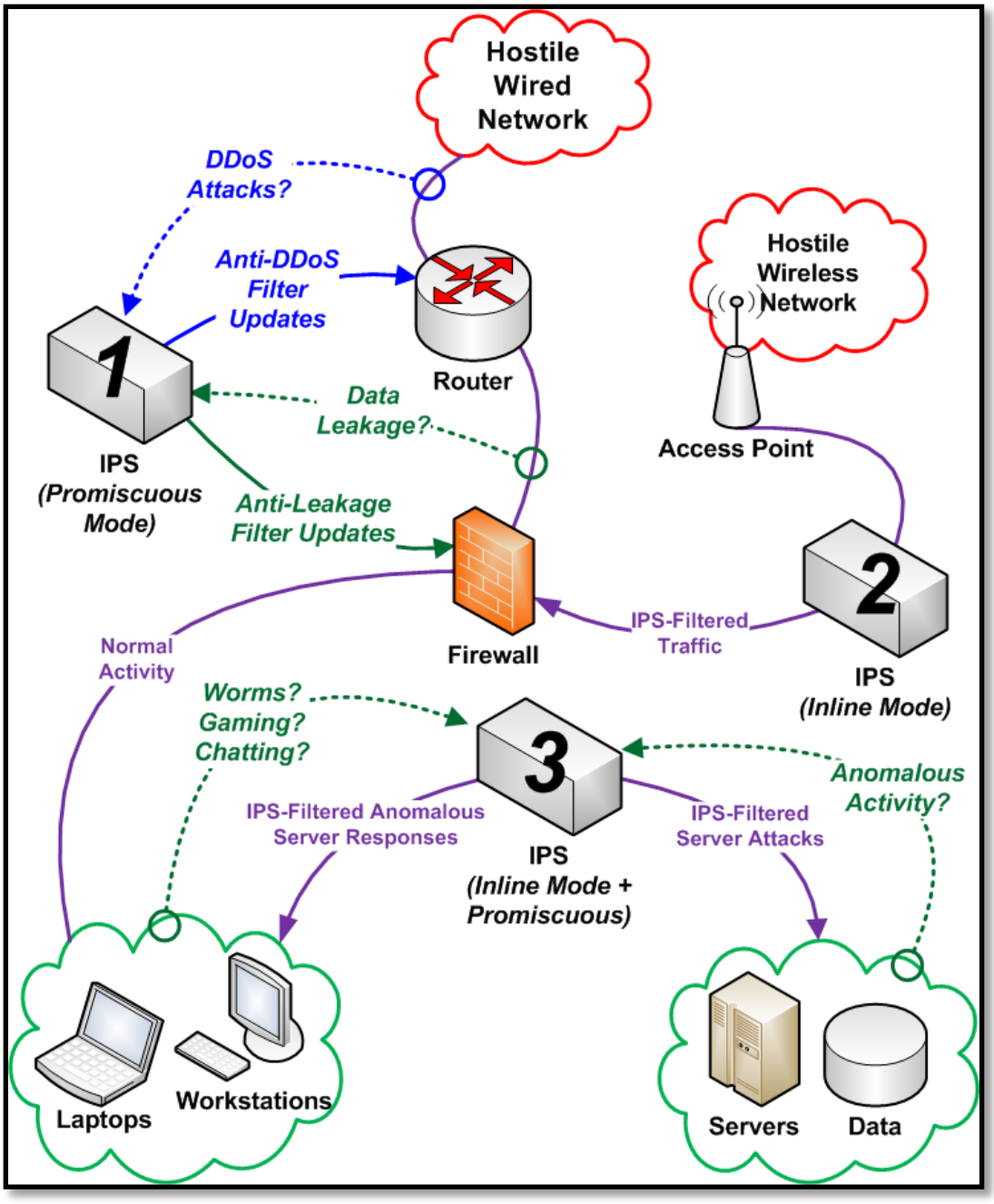
ST authors should consider whether it would be appropriate for the IPS TOE to also claim conformance to the TFFW-EP. In some ways the IPS EP may be incompatible with a TOE configured to meet the TFFW-EP because the TFFW-EP requires that all interfaces block certain types of traffic at all times, while that may not be appropriate for all IPS TOE deployments. However, if the ST author is willing to have all the certified IPS TOE configurations conform to all SFRs of this IPS-EP and the TFFW-EP, the authors of this IPS-EP have not intended to make the two EPs incompatible.

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 IP-based connections between the components most meet FPT_ITT.1 as defined in the NDPP.

Deployment scenarios supported by the TOE would include those shown in Figure 1, which includes a number of possible deployments of IPS functionality within a single network.

- **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



2 Security Problem Definition

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, or 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 EP 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 EP 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" described in the NDPP as defined in FAU_GEN from the NDPP, 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 EP does not repeat the threats identified in the NDPP, though they all apply given the conformance and hence dependence of this EP on the NDPP. Note also that while the NDPP contains only threats to the ability of the TOE to provide its security functions, this EP focuses on threats to resources in the operational environment. Together the threats of the NDPP and those defined in this EP define the comprehensive set of security threats addressed by an IPS TOE.

2.1 Unauthorized Disclosure of Information

Sensitive information on a protected network might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted credit card numbers. The IPS TOE will be capable of inspecting packet payloads for data strings and patterns of characters.

(T.NETWORK_DISCLOSURE)

2.2 Unauthorized Access

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. . If

malicious external devices are able to communicate with devices on the protected network, then those devices may be susceptible to the unauthorized disclosure of information.

(T.NETWORK _ACCESS)

2.3 Inappropriate Access to Services

Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. E.g. Manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools and botnets.

(T.NETWORK_MISUSE)

2.4 Disruption or Denial of Services

Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources. Though most IPS will provide some protection from DDoS (distributed denial of service) attacks, providing protection against DDoS attacks is not a requirement for conformant TOEs, as this is best counteracted by firewalls, cloud computing and design, DOS protection is required however.

(T.NETWORK_DOS)

3 Security Objectives

The Security Problem described in Section 2 will be addressed by a combination of IPS capabilities, with the understanding that the TOE is installed in manner to which it can effectively enforce its policies on the network traffic of the monitored networks. Compliant TOEs will provide security functionality that addresses threats to the TOE, applies analytical processes to network traffic data collected and enforces enterprise policies as applied to the IPS by the IPS administrator. The following subsections provide a description of the security objectives required to meet the threats/policies previously discussed. The description of that security objectives are in addition to that described in the NDPP.

Note: in each subsection below particular security objectives are identified (highlighted by O.) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

3.1 System Monitoring

To address the issues of System Administrators needing to be able to monitor the operations of the IPS functionality, this security objective, which originated in the NDPP, is extended as follows.

To be able to analyze and react to potential network policy violations, the IPS must be able to collect and store essential data elements of network traffic on monitored networks.

(O.SYSTEM_MONITORING -> FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1)

3.2 Analysis of Network Traffic Policy Violations

Entities that reside on or communicate across monitored networks must have network activity effectively analyzed for potential violations of approved network usage. The TOE must be able to effectively analyze data collected from monitored networks to reduce the risk of unauthorized disclosure of information, inappropriate access to services, and misuse of network resources.

(O.IPSANALYZE -> IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1)

3.3 Reaction to Network Traffic Policy Violations

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

(O.IPSREACT -> IPS_ABD_EXT.1.3, IPS_SBD_EXT.1.5)

3.4 TOE Administration

To address the issues involved with a trusted means of administration of the intrusion prevention capability this security objective, which originated in the NDPP, is extended as follows. Compliant TOEs will provide the functions necessary for an administrator to configure the IPS policies that are enforced by the TOE. *Note it is assumed that use of the functions indicated below is protected in accordance with the requirements in the NDPP.*

(O.TOE_ADMINISTRATION -> FMT_SMF.1(2))

4 Security Requirements

This section specifies a Security Functional Requirement for the TOE, as well as specifying the assurance activities the evaluator performs.

4.1 Conventions

While the SFR in this EP is extended, it is defined in a flexible manner for use in this and other EPs, or PPs, and as such operations are performed in the context of this EP.

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:

- Assignment: Indicated with *italicized* text;
- Refinement made by EP author: Indicated with **bold text** and ~~**strikethroughs**~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text; and
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

4.2 TOE Security Functional Requirements

There are four newly introduced SFRs contained in this EP, and eight audit events are specified as well.

Table 4-1: Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Audit Generation	FAU_GEN.1(2)	Audit Data Generation (IPS)
IPS: Intrusion Prevention System	IPS_NTA_EXT.1	Network Traffic Analysis
	IPS_IPB_EXT.1	IP Blocking
	IPS_SBD_EXT.1	Signature-Based IPS Functionality
	IPS_ABD_EXT.1	Anomaly-Based IPS Functionality
FMT: Security Management	FMT_SMF.1(2)	Specification of Management Functions

4.2.1 PP Security Functional Requirement Direction

This section instructs the ST Author what selections must be made to certain SFRs contained in the NDPP in order to support related SFRs in this IPS EP. This is captured by expressing the element where the mandatory selection has been made. The ST Author may complete the remaining selection items as they wish. To ensure specific capabilities or behavior is present in the TOE selections in SFR elements have been made as well.

Assurance activities are not repeated for the requirements in this section, as those are already captured in the NDPP. When assessing the ST and TOE against the SFRs as specified here, it is important for the evaluator when they confirm the proper selections have been made and the appropriate tests are performed to demonstrate compliance to the requirements.

4.2.2 Security Audit

There are additional auditable IPS events that serve to extend the FAU_GEN.1 SFR found in the NDPP. As such, the following events should be combined with those of the NDPP in the context of a conforming Security Target.

4.2.2.1 FAU_GEN.1(2): Audit Data Generation (IPS)

FAU_GEN.1.1(2) Refinement: The TSF shall be able to generate an **IPS** audit record of the following auditable **IPS** events:

a) Start-up of the **IPS** functions;

b) All **IPS** auditable events for the not specified level of audit; and

~~*c) All administrative actions;*~~

d) [All dissimilar IPS events;

e) All dissimilar IPS reactions;

f) Totals of similar events occurring within a specified time period; and

g) *Totals of similar reactions occurring within a specified time period].*

Application Note: *The ST author is not limited to the list presented and should update 'Table of events' below with any additional information generated. The EP Author should use the NDPP FAU_GEN.1 for standard (non-IPS data) audit functions.*

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 essential indications that a single event has re-occurred. 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(2) Refinement : 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~~, [*Specifically defined auditable events listed in Table 2: Auditable Events and Additional Audit Record Contents*.

Application Note: *As with the previous application note, the ST author should update Table of Events below with any additional information generated such as source and destination addresses, IP, signature that trigged event, port, etc.*

Table 2: Auditable Events and Additional Audit Record Contents

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMF.1(2)	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.
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)	Identification of the TOE interface, and (when applicable) the IPS policy and interface mode.

Requirement	Auditable Events	Additional Audit Record Contents
	is/are active on a TOE interface.	
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)[1]
IPS_SBD_EXT.1	Inspected traffic matches a signature-based IPS policy.	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)[2]
IPS_SBD_EXT.1.6	Inspection of encapsulated packets.	Indication of the encapsulation method.
IPS_SBD_EXT.1.7	Failure to re-assemble a fragmented packet.	Source and destination IP addresses. TOE interface that received the fragment(s).
IPS_SBD_EXT.1.8	Normalization of traffic by the TOE.	Source and destination IP addresses of discarded packet(s). TOE interface that received the packet(s).
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)[3]

[1] See application note.
[2] See application note.
[3] See application note.

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.*

4.2.3 Intrusion Prevention

4.2.3.1 IPS_NTA_EXT.1Network 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 EP.*

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

- Internet Protocol (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 interface types*];
  - [*Assignment: other interface types [assignment: list of interface types]];*
  - *and no other interface types*].

Application note: Interface types may be Ethernet, GigabitEthernet, 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.

4.2.3.2 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.

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 EP 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, but where that functionality exists, the TSS and guidance documentation must explain what configurations would cause non-IP lists of known-good and known-bad addresses to take precedence over IP-based address lists.*

IPS_IPB_EXT.1.2: The TSF shall allow IPS Administrators and [selection: no other roles, [assignment: other roles] to configure IPS policy elements (known-good list rules, known-bad list rules, IP addresses).

4.2.3.3 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 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; 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.

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

In addition, 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.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 DoS 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 (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 of by randomizing the protocol/port numbers and/or randomizing the time delays between transmissions)
   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.*

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 EP. Instead, this EP 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:
  - allow the traffic flow
  - block/drop the traffic flow
  - and [selection: modify and forward packets before they pass through the TOE, no other actions]

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 NDPP), 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.).*

4.2.3.4 IPS_ABD_EXT.1 Anomaly-Based IPS Functionality

IPS_ABD_EXT.1.1 The TSF shall support the definition of [selection (choose at least one or both): 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, etc.)*]);
- time of day;
- frequency
- thresholds
- [*assignment: other methods*] and no 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. If 'frequencies' is selected the TSS shall include an explanation of how frequencies can be define on the TOE. 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. If 'thresholds' is selected the TSS shall include an explanation of how the thresholds can be defined on the TOE.*

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's not essential for the IPS TOE to have a capability of "profiling" a network to dynamically defining a baseline or rule, and if the IPS TOE has that functionality, such functionality is not being evaluated as part of the IPS EP.*

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]

4.2.4 Security Management

The NDPP includes FMT_SMF.1 requiring the existence of specific security management functions. The following security management functions are applicable when IPS SFRs are claimed. As such, the following security management functions should be iterated in the ST such that the SFR from the NDPP becomes FMT_SMF.1(1).

4.2.4.1 FMT_SMF.1(2) Specification of Management Functions

FMT_SMF.1.1(2) The TSF shall be capable of performing the following **security** management functions:

1) Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality
2) Modify these parameters that define the network traffic to be collected and analyzed:
   a) Source IP addresses (host address and network address)
   b) Destination IP addresses (host address and network address)
   c) Source port (TCP and UDP)
   d) Destination port (TCP and UDP)
   e) Protocol (IPv4 and IPv6)
   f) ICMP type and code
3) Update (import) signatures
4) Create custom signatures
5) Configure anomaly detection
6) Enable and disable actions to be taken when signature or anomaly matches are detected
7) Modify thresholds that trigger IPS reactions
8) Modify the duration of traffic blocking actions
9) Modify the known-good and known-bad lists (of IP addresses or address ranges)
10) Configure the known-good and known-bad lists to override signature-based IPS policies

5 Assurance Activities

This section contains the assurance activities associated with the SFRs contained within this EP. The assurance activities are grouped according to the CC component they are associated with.

The assurance activities are intended to address the required content of the TOE Summary Specification (TSS) of the ST, the required content of the TOE's operational guidance, and required test activities to be independently performed by the evaluators.

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 specified above 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 2: Sample Inline Mode Test Topology

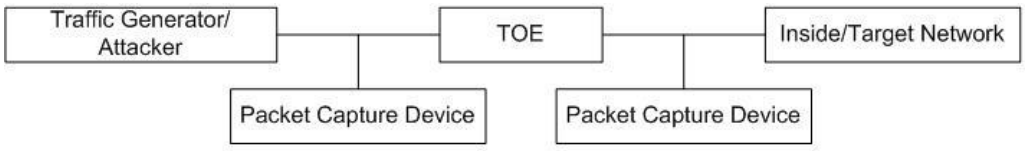
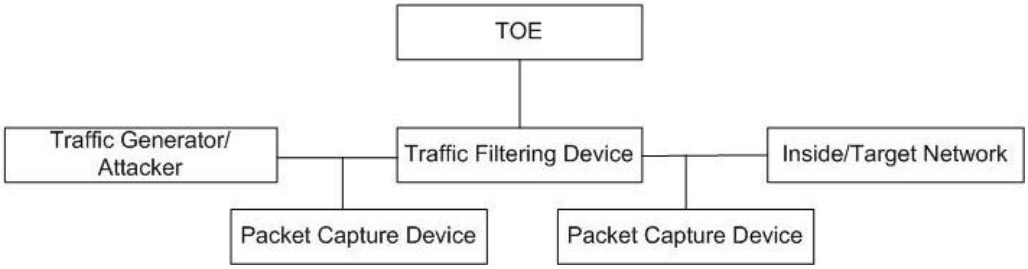


Figure 3: Sample Promiscuous Mode Test Topology



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 simulate network attacks. The traffic generator does not need to be specialized equipment, but can be a COTS (commercial off the shelf) commercial, shareware, or freeware FMT_SMF.1(2) Specification of Management Functions.

Table 5-1: Assurance Activities for FAU_GEN.1(2)

Activity	Assurance Activity
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.
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.).
Tests	Test 1: 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 that this activity should have been addressed with a combination of the Test assurance activities for the other IPS requirements.

Table 5-2: Assurance Activities for IPS_NTA_EXT.1.1

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS explains the TOE's capability of analyzing IP traffic in terms of the TOE's policy precedence hierarchy order. 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. The TSS associated with this requirement is assessed in the subsequent assurance activities.

Activity	Assurance Activity
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.
Tests	The testing associated with this requirement is assessed in the subsequent assurance activities.

Table 5-3: Assurance Activities for IPS_NTA_EXT.1.2

Activity	Assurance Activity
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)
Guidance	The Guidance associated with this requirement is assessed in the subsequent assurance activities.
Tests	The testing associated with this requirement is addressed in the subsequent test assurance activities.

Table 5-4: Assurance Activities for IPS_NTA_EXT.1.3

Activity	Assurance Activity
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 TSS should also provide descriptions how the management interface is distinct from sensor interfaces.
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 operational guidance explains how to configure the interface into a management interface. The evaluator shall verify that the operational guidance explains how the TOE sends

Activity	Assurance Activity
	commands to remote traffic filtering devices. Note: the secure channel configurations between the TOE and the remote device would be discussed as per NDPP FTP_ITC (if the ST author selects other interface types) and FTP_TRP (for interfaces in management mode).
Tests	The tests associated for this requirement have been completed in subsequent assurance activities in which promiscuous and inline interfaces are tested (e.g. tests for IPS_SBD_EXT.1.7) and in the requirement of FTP_ITC (if the ST author selects other interface types) and FTP_TRP (for interfaces in management mode) of NDPP.

Table 5-5: Assurance Activities for IPS_IPB_EXT.1.1/IPS_IPB_EXT.1.2

Activity	Assurance Activity
TSS	The evaluator shall verify how good / bad lists affect the way in which traffic is analyzed with respect to processing packets. The TSS should also provide detail with the attributes that create a known good list, a known bad list, 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). 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.
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.
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.

Table 5-6: Assurance Activities for IPS_SBD_EXT.1.1/IPS_SBD_EXT.1.5

Activity	Assurance Activity
TSS	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 reactions specified in IPS_SBD_EXT.1.5.

Activity	Assurance Activity
	The evaluator shall verify that the TSS identifies all interface types 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.
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.
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. Using packet sniffers, the evaluator will generate traffic to trigger a signature and using packet captures will ensure that the reactions of each rule are performed as expected. Test 2: Repeat the test assurance activity 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.

Table 5-7: Assurance Activities for IPS_SBD_EXT.1.2/ IPS_SBD_EXT.1.5

Activity	Assurance Activity
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 reactions specified in IPS_SBD_EXT.1.5.
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 operational guidance shall provide configuration instructions, if needed, to detect payload across multiple packets. 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.
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 [selection: [assignment: other types of TCP payload inspection]; • 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 [*assignment:*

Activity	Assurance Activity
	other types of packet payload inspection]] Test 2: The evaluator shall repeat one of the tests in Test 1 but generate multiple non-fragmented packets that contain the string in the rule defined. Test 3: Repeat the test assurance activity 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.

Table 5-8: Assurance Activities for IPS_SBD_EXT.1.3/ IPS_SBD_EXT.1.5

Activity	Assurance Activity
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.
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.
Tests	Test 1: 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.

Table 5-9: Assurance Activities for IPS_SBD_EXT.1.4/ IPS_SBD_EXT.1.5

Activity	Assurance Activity
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.
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.
Tests	Test 1: 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.

Table 5-10: Assurance Activities for IPS_ABD_EXT.1.1, IPS_ABD_EXT.1.2, and IPS_ABD_EXT.1.3

Activity	Assurance Activity
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. 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.
Guidance	The evaluator shall verify that the operational guidance provides instructions with how 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 this PP. 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.
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: Repeat the test assurance activity above to ensure that baselines or anomaly-based rules can be defined for each distinct network interface type supported by the TOE.

Table 5-11: Assurance Activities for FMT_SMF.1(2)

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS describes how the IPS data analysis and reactions can be configured. Note that this activity should have been addressed with the TSS assurance activities for IPS_SBD_EXT.1, IPS_SBD_EXT.1 and IPS_ABD_EXT.1
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

Activity	Assurance Activity
	applicable analysis pattern matching methods and reaction modes.
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. Note that all other functions should have been address with a combination of the test assurance activities for IPS_ABD_EXT.1, IPS_SBD_EXT.1,

6 Security Assurance Requirements

This EP does not define any SARs beyond those defined within the NDPP. It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDPP as well. The NDPP includes a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that similarly refine the SARs of the NDPP.

7 Rationale

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats addressed by IPS devices; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artifacts that can be used for the evaluation activities associated with this document.

7.1 Security Problem Definition

7.1.1 Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions are in addition to those defined in the NDPP and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 7-1: TOE Assumptions

Assumption Name	Assumption Definition
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.

7.1.2 Threats

The threats listed below are addressed by IPS devices. Note that these threats are in addition to those defined in the PP, all of which apply to IPS devices.

Table 7-2: Threats

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized

Threat Name	Threat Definition
	disclosure of information.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. E.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools and botnets.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network. Resource exhaustion may occur in the event of co-ordinate service request flooding from a small number of sources

7.1.3 Organizational Security Policies

The policy listed below is addressed by IPS devices. Note that this policy is in addition to those defined in the PP, all of which apply to IPS devices.

Table 7-3: Policies

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

7.1.4 Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

Table 7-4: Security Problem Definition Correspondence

Threat or Assumption	Security Objectives	SFR
O.CONNECTIONS	OE.CONNECTIONS	N/A
T.NETWORK_DISCLOSURE	O.SYSTEM_MONITORING O.IPSANALYSE, O.IPS_REACT	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1
T. NETWORK_ACCESS	O.SYSTEM_MONITORING O.IPSANALYSE, O.IPS_REACT	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1
T.NETWORK_MISUSE	O.SYSTEM_MONITORING O.IPSANALYSE, O.IPS_REACT	FAU_GEN.1(2), IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1
T.NETWORK_DOS	O.SYSTEM_MONITORING	FAU_GEN.1(2), IPS_NTA_EXT.1,

Threat or Assumption	Security Objectives	SFR
	O.IPSANALYSE, O.IPS_REACT	IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1
P.ANALYSE	O.IPSANALYZE	IPS_NTA_EXT.1, IPS_IPB_EXT.1, IPS_SBD_EXT.1, IPS_ABD_EXT.1

7.2 Security Objectives

7.2.1 Security Objectives for the TOE

The following table contains security objectives specific to IPS devices. These security objectives are in addition to those defined in the PP, all of which apply to IPS devices.

Table 7-5: Security Objectives for the TOE

Security Objective Name	Security Objective Definition
O.IPSSENSE	The IPS must collect and store information about all events that may indicate an IPS policy violation related to misuse, inappropriate access, or malicious activity on monitored networks.
O.IPSANALYZE	The IPS must apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations.
O.IPSREACT	The IPS must respond appropriately to its analytical conclusions about IPS policy violations.

7.2.2 Security Objectives for the Operational Environment

The following table contains security objectives specific to the operational environments for IPS devices. These security objectives are in addition to those defined in the PP, all of which apply to the operational environments for IPS devices.

Table 7-6: Security Objectives for the Operational Environment

Security Objective Name	Security Objective Definition
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.

7.2.3 Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.

7.3 Rationale for Security Functional Requirements

Table 7-7: Rationale for Explicitly Stated Requirements

SFR	Rationale
FAU_GEN.1(2)	This extended SFR was created to correctly specify the TOE's ability to collect IPS data from the operational environment.
IPS_NTA_EXT.1	This SFR was created to correctly specify the TOE's ability to analyze traffic and network protocols for both signature-based and anomaly-based detection.
IPS_IPB_EXT.1	This SFR was created to correctly specify the TOE's ability to create white lists and black lists of known source IP addresses to optimize the TOE's blocking capability by overriding the signature-based analysis of the traffic.
IPS_SBD_EXT.1	This SFR was created to correctly specify the TOE's ability to analyze signatures and react to matches of the signature from traffic collected from the operational environment.
IPS_ABD_EXT.1	This SFR was created to correctly specify the TOE's ability to analyze and react to anomalies from traffic collected from the operational environment.
FMT_SMF.1(2)	This extended SFR was created to correctly specify the TOE's ability to manage the TOE ability to analyze traffic from the operational environment.

Table 7-8: SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1(2)	FPT_STM.1	FPT_STM.1 (NDPP)
FMT_SMF.1(2)	No dependencies	Not Applicable
IPS_NTA_EXT.1	No dependencies	Not Applicable
IPS_IPB_EXT.1	No dependencies	Not Applicable
IPS_SBD_EXT.1	No dependencies	Not Applicable
IPS_ABD_EXT.1	No dependencies	Not Applicable

8 Appendix "C": Additional Requirements

As indicated in the body of this EP, there are several methods by which conformant TOEs can monitor, collect, report and manage the audit and IPS data.

8.1 Requirements

The eleven additional security functional requirements are as follows:

8.1.1 FAU: Security Audit

The term "IPS Data" includes 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 definition of "IPS Data" excludes the "audit data" relevant to the NDPP, which includes data defined in FAU_GEN from the NDPP, such as authentication of administrators, and establishment/termination of

trusted channels. If IPS Data review and/or storage and security alarms are supported by the TOE then the following audit requirements must be included in the ST, as appropriate.

8.1.1.1 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: *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, and FRU_RSA is used instead to define the "potential security violation" relevant to FAU_ARP, namely that the TOE has experienced a spike in network traffic that has exceeded its ability to inspect all network traffic, and that event has result in network traffic being dropped or passed without inspection. 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(2) 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(2).*

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS includes a description of the alerts specified in the requirement. The evaluator shall also verify that the TSS states that audit data cannot be transmitted through the security alarms interface.
Guidance	The evaluator shall verify that the guidance explains how to enable alerts specified in the requirement as applicable to FRU_RSA.1.
Tests	Test 1: The evaluator shall devise tests that demonstrate that transmission of messages related to single events through the defined actions. Note that this activity can be addressed with a combination of the test assurance activities for IPS_ABD_EXT.1, IPS_SBD_EXT.1, and FRU_RSA.1.

8.1.1.2 FAU_SAR.1: Audit Review (IPS Data)

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

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

Application note: *It's 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. There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).*

Table 8-1: Table of Events (some examples inserted)

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

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

8.1.1.3 FAU_SAR.2: Restricted Audit Review (IPS Data)

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

Assurance Activity: *Since administrative roles are needed to view the IPS data, the analysis performed by the evaluators in the Assurance Activity for FMT_MTD.1(2) will demonstrate that this requirement is met. There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).*

8.1.1.4 FAU_SAR.3: Selectable Audit Review (IPS Data)

FAU_SAR.3.1 Refinement: 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]*].

There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).

Activity	Assurance Activity
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.
Guidance	The evaluator shall review the administrative 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

Activity	Assurance Activity
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.
	selection criteria currently being enforced.
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.

8.1.1.5 FAU_STG.1: Protected Audit Trail Storage (IPS Data)

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

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

There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).

Activity	Assurance Activity
TSS	The evaluator shall ensure that the TSS identifies how IPS data is protected from unauthorized modification and deletion.
Guidance	The evaluator shall confirm the guidance documentation describes how to protect IPS data from unauthorized modification and deletion.
Tests	Test 1: The evaluator shall devise tests that demonstrate that IPS data can be protected from unauthorized modification and deletion.

8.1.1.6 FAU_STG.4: Prevention of Data Loss (IPS Data)

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

Auditable Events	Additional Audit Record Contents

A local audit store reaches its storage limit.[4]	Indication that the audit store is full, and (if configurable) how the TOE is responding (e.g. failing to audit new auditable events, or preventing auditable events from occurring).

Activity	Assurance Activity
TSS	The evaluator shall ensure that the TSS identifies how IPS data logging is handled once the IPS data trail is full. The TSS shall also identify how IPS data logging is restored.
Guidance	The evaluator shall confirm the guidance documentation describes the steps involved to manage IPS data logging for when the IPS data trail is full.

8.1.2 FMT: Security Management Requirements.

If the TOE allows for multiple administration roles, then these requirements must be included in the ST.

8.1.2.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to modify the behavior of the functions **of IPS data collection, analysis and reaction** to authorized IPS Administrators.

Application Note:
The TOE may have administrative roles on the Operating System that do not have permissions to change the configuration options of the System.

There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).

Activity	Assurance Activity
TSS	The evaluator shall examine the TSS to determine that, for each administrative function identified in the operational guidance; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the configuration of the system through this interface is disallowed for non-administrative users.
Guidance	The evaluator shall review the operational guidance to determine that each of the functions implemented in response to the requirements of this EP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

8.1.2.2 FMT_MTD.1(2) Management of IPS data

[4] *The audit event for FAU_STG.4 does not apply to audit stores that overwrite the oldest records when full.*

FMT_MTD.1.1(2) The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [*assignment: other operations*]] the [*assignment: list of ~~TSF~~ **IPS** data*] to [*assignment: the **IPS Administrator, IPS Analyst** and other IPS-specific roles identified in FMT_SMR.1*].

Application Note: *The ST should define which roles are permitted to access the IPS data (IPS Administrator, IPS Analyst, and other IPS-specific roles identified in FMT_SMR.1). The ST may define any number of roles to meet this requirement. There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).*

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS includes a description of each identified role in regards to the responsibly of the role and the access permissions associated with that role on the TOE.
Guidance	The evaluator shall review the operational guidance to ensure that it contains instructions for configuring authorized administrators restrict the ability for authorized identified roles in the requirement the and authorized roles.
Tests	It is not necessary for all operations described in this SFR to be accessible through all TOE interfaces. In the course of performing the testing activities for the evaluation, the evaluator shall make use of all interfaces applicable to each administrative function described in this SFR, although it is not necessary to repeat each test involving an administrative action with each interface. Test 1: The evaluator shall demonstrate that after configuring the TOE for first use from the operational guidance, it is possible to restrict the ability to query and modify IPS Data using each of the authorized identified roles as defined in the requirement.

8.1.2.3 FMT_SMR.1(2) Security roles (IPS)

FMT_SMR.1.1 Refinement: The TSF shall maintain the **following *roles:* IPS Administrator**, **IPS Analyst, and *[assignment: other authorized IPS roles]***.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: *The roles defined in this SFR are intended to be specific to management of IPS functionality. The "Authorized Administrator" role defined in the NDPP within FMT_SMR.2 may be the same role as the "IPS Administrator" defined in FMT_SMR.1, or may be a different role where the Authorized Administrator has full rights to administer the entire TOE, and the IPS Administrator only has full rights to IPS-specific functionality. The IPS Analyst role is intended to represent a role that has less than full rights, or may have limited read-only rights. Other roles can be defined by the ST author. There are no additional auditable IPS events that need to be included in FAU_GEN.1(2).*

Activity	Assurance Activity
TSS	The evaluator shall review the TSS to ensure it describes the distinction between rights of the IPS Administrator, the IPS Analyst, and any other roles identified in the assignment of

Activity	Assurance Activity
	this SFR. The TSS should also describe any distinctions, if any, between the rights of the IPS Administrator identified in this SFR, and the Authorized Administrator identified in FMT_SMR.2 of the NDPP.
Tests	Since administrative roles are need to view the TSF data, the analysis performed by the evaluators in the Assurance Activity for FMT_MTD.1 will demonstrate that this requirement is met.

8.1.3 FPT: Protection of the TSF

8.1.3.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 Refinement: 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 in the IPS EP 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.*

Auditable Events	Additional Audit Record Contents
Failure of the TSF.	The type of failure that occurred.

Activity	Assurance Activity
TSS	The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall first examine the TSS section to ensure that all failure modes specified in the ST are described. The evaluator shall then ensure that the TOE will attain a secure state after inserting each specified failure mode type. The evaluator shall review the TSS to determine whether the TOE administrator would be able to configure how the traffic-forwarding will be impacted by those failures.
Testing	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 must 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

Activity	Assurance Activity
	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).

8.1.4 Resource Utilization (FRU)

8.1.4.1 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: *Compliant 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 in that the TSF may have failed to inspect some network traffic.*

Auditable Events	Additional Audit Record Contents
Traffic flow volume exceeds the maximum quota.	Identification of the TOE interface at which the quota was exceeded.

Activity	Assurance Activity
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.
Guidance	The evaluator shall examine the operational guidance to determine that it contains instructions for establishing quotas (if they are configurable), and describes any actions administrators can or should take in response to a quota being reached.
Tests	Test 1: The evaluator follows 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.

8.1.5 IPS: Intrusion Prevention

In the case that the TOE supports the implementation of normalization of network packets, then the following requirements can be included in the ST.

IPS_SBD_EXT.1.6: 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*], no other methods]

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS describes how the TOE is able to inspect traffic within inside tunnels defined in the requirement.
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	Test 1: The evaluator shall re-run a pervious signature-based test within the tunnel defined in the requirement.

IPS_SBD_EXT.1.7: 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 and alert if the TSF cannot reassemble the entire packet].

Activity	Assurance Activity
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.
Test	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.1.8: 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; [*assignment: other types of normalization*]]

Activity	Assurance Activity
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 • Any other methods defined in the requirement.
Test	Test 1: The evaluator shall generate the following types of packets and observe that packets are dropped: • Duplicate packets • Changed packets • Out of sequence packets • Any other methods defined in the requirement..

9 Appendix D: Definitions

9.1 Definitions of Attacks

Title	Description
DoS	Denial of Service
Flooding	Causing an excessive amount of traffic on an IP subnet or targeted against a specific IP address.
IP Impossible Packet (Land)	IP packet detected with source equal to destination address (Land Attack).
IP options Bad Option List	IP datagram where the list of IP options in the IP datagram header is incomplete or malformed.
IP options Record Packet Route	IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).
IP options Timestamp	IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
IP options Security	IP datagram where the IP option list for the datagram includes option 2 (Security options).
IP options Loose Source Route	IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
IP options Strict Source Route	IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
IP Overlapping Fragments (Teardrop, Bonk)	Two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B.
ICMP fragments (Ping of Death, Nuke)	IP datagram with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535. The IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
ICMP flooding (Smurf, ping flood)	The destination IP address in the packet is the broadcast address of the destination subnet so all machines on that subnet respond to the broadcast.
Scanning (IP protocols,	Attempting to determine whether any listening services exist on specific IP

Title	Description
TCP ports, UDP ports)	protocol numbers, TCP ports, or UDP ports by transmitting traffic to generate an expected response.
TCP FIN only flags	Orphaned TCP FIN packet is sent to a privileged port (port number less than 1024).
TCP flood (SYN flood)	Sending an excessive number of TCP packets with the SYN flag set in order to exhaust the target hosts limit of half-open TCP sessions.
TCP NULL flags	TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
TCP SYN+FIN flags	TCP packet with the SYN and FIN flags are set.
UDP Bomb attack	UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
UDP Chargen DoS attack	UDP packet is detected with a source port of 7 and a destination port of 19.

9.1 Definitions of Terms and Acronyms

Title	Description
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.
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	Intrusion Prevention System
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	Filtering of network traffic such that only the useful packets/fragments are

Title	Description
network traffic)	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 duplicate packets; fragments that cannot be re-assembled, packets determined to be invalid such as with invalid checksums, out-of-sequence packets, etc.
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.