PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS)

Version: 1.0

2020-09-30

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-09-30	Initial Release - PP-Module for NDcPP

Contents

1 Introduction

1.1 Overview

This Protection Profile Module (PP-Module) describes security requirements for a 802.11 Wireless Intrusion Detection System (WIDS) defined to be an IEEE 802.11 network intrusion detection product located at the edge of a private network that can collect, inspect, and analyze real-time network traffic and alert the administrator of policy violations. This PP-Module is intended to provide a minimal baseline set of requirements that are targeted at mitigating well defined and described threats.

This PP-Module contains optional requirements for a Wireless Intrustion Protection System (WIPS), a security product that in addition to the 802.11 WIDS capability, provides network security administrators with the additional ability to react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.

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

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

A TOE that conforms to a PP-Configuration containing this PP-Module must be a 'Distributed TOE' as defined in the NDcPP. The expectation for this PP-Module is that a WIDS must include distributed sensor nodes to ensure that the full physical range of a wireless network to ensure that user interactions with the network cannot evade detection.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Access Point (AP)	A device that provides the network interface that enables 802.11 wireless client hosts to access a wired network.
End User Device (EUD)	An 802.11 enabled device that has the ability to process, transmit, and/or store information.
Service Set Identifier (SSID)	The primary name associated with an 802.11 wireless local area network (WLAN).
Wireless Intrustion Detection System (WIDS)	A security product that provides network security administrators with the ability to monitor, collect, and log real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Intrustion Prevention System (WIPS)	A security product that provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Local Area Network (WLAN)	An 802.11 wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

This PP-Module specifically addresses WIDS/WIPS. A conformant WIDS is a product that can monitor, collect, inspect, and analyze real-time network traffic and alert the administrator of policy violations. WIPS functionality is not required to conform to this PP-Module, and it is optional for the TOE to have the additional ability to react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.

A WIDS/WIPS TOE consists of multiple sensors that passively scan the RF environment on the WLAN radio frequency spectrum and a centralized mechanism such as a Server or Controller that processes the data collected by the sensors. Conformant TOEs must use a secure communication path(s) between WIDS/WIPS components.

A WIDS/WIPS can be Integrated (be part of the WLAN infrastructure) or Standalone (independent from WLAN) architecture depending on vendor implementation. The two different architectures are illustrated in Figure 1 below. The TOE boundary is indicated by the yellow box.

A WIDS/WIPS is expected to inspect layers 1 and 2 network traffic, per the OSI network model, and monitor wireless frames in the RF spectrum utilized by IEEE 802.11 a, b, g, n, and ac. Monitoring and inspection of other technologies (e.g., cellular) and protocols are optional.

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 a frame with known patterns, or by matching traffic patterns common with reconnaissance or denial of service (DoS) attacks). Identification of 'unknown' threats may be performed through use of various forms of anomaly detection whereby the WIDS/WIPS 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.

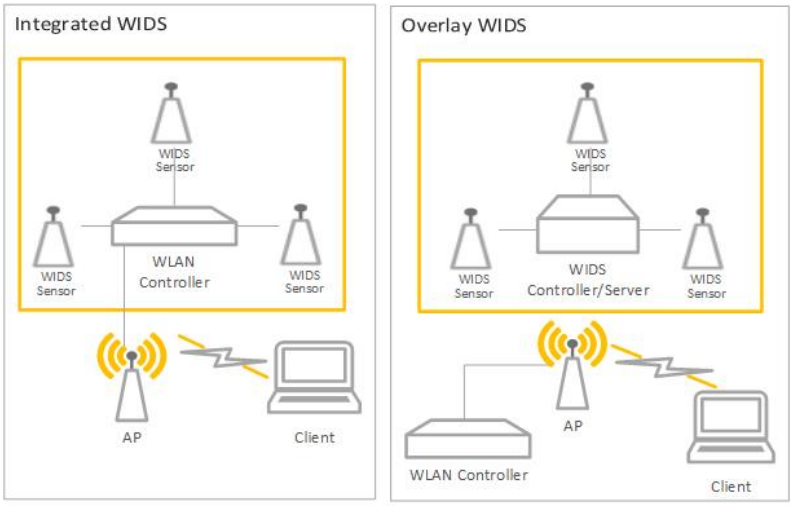

Figure 1: General TOE

1.4 Use Cases

[USE CASE 1] Use Case 1

A WIDS consists of sensors (preferably dedicated) and a central controller working together to provide 24/7 monitoring, primarily to the 802.11 Wireless Local Area Network (WLAN) spectrum and protocol, to detect, identify, and geo-locate WLAN devices within a controlled space.

The WIDS may be capable of detecting or monitoring traffic other than 802.11WLAN, such as 802.15.4 based protocols, which enhances the security of the controlled space. However, a WIDS is not required to monitor additional protocols outside of 802.11. A WIDS monitors all 802.11 WLAN traffic emanating from and traversing the controlled space, thus inadvertant collection of any 802.11 signals is possible when operating a WIDS.

2 Conformance Claims

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

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

- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1

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

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

3 Security Problem Description

WIDS address a range of security threats related to detection of and reaction to potentially malicious WLAN traffic. The malicious traffic may pose a threat to one or more endpoints on the monitored networks, to the network infrastructure, or to the TOE itself. Attacks against a WLAN could compromise the confidentiality and integrity of WLAN users and system data as well as the availability of the WLAN to legitimate users.

The term “monitored network” is used here to represent any WLAN and/or wired network that the TOE is configured to monitor and detect intrusions on. This extends to the wired networks as intrusions on the wireless network can also be damaging to the wired infrastructure. The WIDS/WIPS also protect the wired infrastructure by detecting rogue devices that are directly connected to the wired infrastructure, which may expose the wired network, or unauthorized WLAN devices deployed in a no-wireless zone.

The proper installation, configuration, and administration of the WIDS is critical to its correct operation. A site is responsible for developing its security policy and configuring a rule set that the WIDS will enforce and provide an appropriate response to meet their needs, relative to their own risk analysis and their perceived threats.

Note that this PP-Module does not repeat the threats identified in the NDcPP, though they all apply given the conformance and hence dependence of this PP-Module on the NDcPP. Note also that while the NDcPP contains only threats to the ability of the TOE to provide its security functions, this PP-Module addresses only threats to resources in the operational environment. Together the threats of the NDcPP and those defined in this PP-Module define the comprehensive set of security threats addressed by a WIDS TOE.

3.1 Threats

T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION
A malicious actor may take advantage of unintended/unauthorized disclosure of sensitive information on a protected WLAN, such as sending unencrypted sensitive data, without detection. A malicious actor may also force the modification or disclosure of data in transit between distributed components of a WIDS to impede or gain visibility into its data collection capabilities.

T.UNAUTHORIZED_ACCESS
An attacker may attempt to gain unauthorized access to a network, endpoints, or services, by methods such as impersonation of an authorized AP to get an EUD to connect to the unauthorized AP If malicious external APs or EUDs are able to communicate with APs or EUDs on the protected WLAN, then those devices may be susceptible to the unauthorized disclosure of information.

T.DISRUPTION
Attacks against the WLAN infrastructure might lead to denial of service (DoS) attacks within a protected WLAN. A wireless DoS may occur in two ways: at the physical layer through RF Jamming, or at the data link layer through packet injection.

3.2 Assumptions

These assumptions are made on the Operational Environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

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

A.PROPER_ADMIN
The administrator of the WIDS is not careless, willfully negligent or hostile, and administers the WIDS within compliance of the applied enterprise security policy.

3.3 Organizational Security Policies

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

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

4 Security Objectives

4.1 Security Objectives for the TOE

O.SYSTEM_MONITORING
To be able to analyze and react to potential network policy violations, the WIDS must be able to collect and store essential data elements of network traffic on monitored networks. A conformant TOE may also implement a self-protection mechanism to ensure that undetected network policy violations cannot occur when a sensor is unavailable.

Addressed by: FAU_GEN_EXT.1 (from Base-PP), FAU_STG_EXT.1 (from Base-PP), FAU_GEN.1/WIDS, FAU_RPT_EXT.1, FAU_STG_EXT.1/PCAP, FPT_FLS.1 (objective)

O.WIDS_ANALYZE
The WIDS must be able to analyze collected or observedWLAN activity on monitored network to identify potential violations of approved WLAN policies, unauthorized connections involving internal WLAN devices, and non-secure communications.

Addressed by: FAU_ARP.1, FAU_ARP_EXT.1, FAU_IDS_EXT.1, FAU_INV_EXT.1, FAU_INV_EXT.2, FAU_INV_EXT.3, FAU_SAA.1, FAU_WID_EXT.1, FAU_WID_EXT.2, FDP_IFC.1, FAU_WID_EXT.3 (optional), FAU_WID_EXT.4 (optional), FAU_ANO_EXT.1 (selection-based), FAU_SIG_EXT.1 (selection-based), FAU_INV_EXT.4 (objective), FAU_INV_EXT.5 (objective), FAU_MAC_EXT.1 (objective)

O.WIDS_REACT
The TOE must be able to react, as configured by the administrators, to configured policy violations or other potential malicious activity.

Addressed by: FAU_ARP.1, FAU_SAA.1, FMT_SMF.1/WIDS, FAU_ANO_EXT.1 (selection-based), FAU_WIP_EXT.1 (objective)

O.TOE_ADMINISTRATION
To address the threat of unauthorized administrator access that is defined in the Base-PP, conformant TOEs will provide the functions necessary for an administrator to configure the WIDS capabilities of the TOE. A conformant TOE may also implement a self-protection mechanism to ensure that a TSF failure cannot be used as a way to modify theTOE's configuration without authorization.

Addressed by: FMT_SMF.1/WIDS, FPT_FLS.1 (objective)

O.TRUSTED_COMMUNICATIONS
To further address the threat of untrusted communications channels that is defined in the Base-PP, conformant TOEs will provide trusted communications between distributed components if any exist.

Addressed by: FCO_CPC_EXT.1 (from Base-PP), FPT_ITT.1 (from Base-PP), FTP_ITC.1 (from Base-PP)

4.2 Security Objectives for the Operational Environment

The Operational Environment of the TOE implements technical and procedural measures to assist theTOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment. The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track the assumptions about the environment.

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

OE.PROPER_ADMIN
The administrator of the WIDS is not careless, willfully negligent or hostile, and administers the WIDS within compliance of the applied enterprise security policy.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Threat, Assumption, or OSP	Security Objectives	Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	O.SYSTEM_MONITORING	The threat T.UNAUTHORIZED_DISCLOSURE_OF_IN is countered by O.SYSTEM_MONITORING provides for visibility into the network which detection of network violations.
	O.TRUSTED_COMMUNICATIONS	The threat T.UNAUTHORIZED_DISCLOSURE_OF_IN is countered by O.TRUSTED_COMMUNICA this ensures that data in transit is protected unauthorized disclosure through authenticat endpoints and use of trusted protocols.
	O.WIDS_ANALYZE	The threat T.UNAUTHORIZED_DISCLOSURE_OF_IN is countered by O.WIDS_ANALYZE as this detection of potential violations of approved usage.
	O.WIDS_REACT	The threat T.UNAUTHORIZED_DISCLOSURE_OF_IN

		is countered by O.WIDS_REACT as this pro containment of unauthorized APs and EUDs
T.UNAUTHORIZED_ACCESS	O.SYSTEM_MONITORING	The threat T.UNAUTHORIZED_ACCESS is O.SYSTEM_MONITORING as this provides into the network which enables detection of APs and EUDs.
	O.WIDS_ANALYZE	The threat T.UNAUTHORIZED_ACCESS is O.WIDS_ANALYZE as this provides detecti violations of approved network usage.
	O.WIDS_REACT	The threat T.UNAUTHORIZED_ACCESS is O.WIDS_REACT as this provides containme unauthorized APs and EUDs.
	O.TOE_ADMINISTRATION	The threat T.UNAUTHORIZED_ACCESS is O.TOE_ADMINISTRATION.
T.DISRUPTION	O.SYSTEM_MONITORING	The threat T.DISRUPTION is countered by O.SYSTEM_MONITORING as this provides into the network which enables detection of
	O.WIDS_ANALYZE	The threat T.DISRUPTION is countered by O.WIDS_ANALYZE as this provides for dete potential violations of approved network usa
	O.WIDS_REACT	The threat T.DISRUPTION is countered by O.WIDS_REACT as this provides containme unauthorized APs and EUDs.
A.CONNECTIONS	OE.CONNECTIONS	The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.
A.PROPER_ADMIN	OE.PROPER_ADMIN	The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.
P.ANALYZE	O.WIDS_ANALYZE	The organizational security policy P.ANALY facilitated through O.WIDS_ANALYZE.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 NDcPP Security Functional Requirements Direction

In a PP-Configuration that includes NDcPP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDcPP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDcPP in addition to what is mandated by Section 5.2 TOE Security Functional Requirements.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDcPP and relevant to the secure operation of the TOE.

5.1.1.1 Security Audit (FAU)

FAU_GEN_EXT.1 Security Audit Data Generation for Distributed TOE Components

FAU_GEN_EXT.1.1 The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

Application Note: This SFR is selection-based in the Base-PP but is mandated by this PP-Module because the ST author must claim a distributed TOE selection in FAU_STG_EXT.1.2.

FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [**selection**:

- *The TOE shall be a distributed TOE that stores audit data on the following TOE components: [**assignment**: identification of TOE components]*,
- *The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [**assignment**: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data]*

].

Application Note: This SFR is modified from its definition in the Base-PP by removing the selection option for the TOE to be standalone. A TOE that conforms to this PP-Module is expected to be distributed.

5.1.1.2 Communications (FCO)

FCO_CPC_EXT.1 Communication Partner Control

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [**selection**:

- *A channel that meets the secure channel requirements in [**selection**: FTP_ITC.1, FPT_ITT.1]*,
- *A channel that meets the secure registration channel requirements in FTP_TRP.1/Join*,
- *No channel*

] for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

Application Note: This SFR is optional in the NDcPP but is mandated by this PP-Module because the WIDS TOE is expected to be a distributed system.

5.1.1.3 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use of [**selection**: *IPsec*, *SSH*, *TLS*, *DTLS*, *HTTPS*].

Application Note: FPT_ITT.1 is optional in NDcPP, however, since a WIDS/WIPS TOE is distributed, FPT_ITT.1 shall be included in the ST and is applicable to the data transmitted

between the sensors and controller.

This requirement ensures all communications between components of a distributed TOE is protected through the use of an encrypted communications channel. The data passed in this trusted communication channel are encrypted as defined in the protocol chosen in the selection. The ST author chooses the mechanisms supported by the TOE, and then ensures that the detailed protocol requirements in Appendix B of NDcPP corresponding to their selection are included in the ST, if not already present.

5.1.1.4 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be capable of using [**selection**: *IPsec*, *SSH*, *TLS*, *DTLS*, *HTTPS*] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [**selection**: *authentication server*, ***database server***, *[**assignment**: other capabilities]*, *no other capabilities*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: This SFR is modified from its definition in the Base-PP by adding a selection for a database server capability. If the TSF uses a separate database server to support its security-relevant functionality, this selection must be included in the ST.

The intent of the database server is to store WIDS/WIPS data that must be queryable, such as events/alarms, triangulation calculations, wireless spectrum analysis (including RF jammer/Denial of Service (DoS)), and packet capture analysis. Authorized Administrators must be permitted to view alarms, raw event data, and any other data stored in the database. The Administrator must access the database through a trusted channel if done so remotely.

The intent of this requirement is to provide a means by which a cryptographic protocol may be used to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. The TOE uses at least one of the listed protocols for communications with the server that collects the audit information.

If other authorized IT entities are protected, the ST author makes the appropriate assignments (for those entities) and selections (for the protocols that are used to protect those connections). The ST author selects the mechanism or mechanisms supported by the TOE, and then ensures that the detailed protocol requirements in Appendix B of NDcPP corresponding to their selection are included in the ST.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall **display an alert to Authorized Administrator in sufficient detail to include identity of APs and EUDs involved, signal strength, accurate event timestamp, description of alert and severity level and [selection: *capture raw frame traffic that triggered the violation*, *no other actions*]** upon detection of a potential security violation.

Application Note: If "capture raw frame traffic that triggers the violation" is selected then FAU_STG_EXT.1/PCAP must be included in the ST.

FAU_SAA.1 defines the rules for monitoring the wireless traffic to detect for potential security violations. FAU_INV_EXT.2 defines the information the TOE needs to collect for all APs and EUDs within range of the the TOE's sensors. Device attributes can then be individually filtered and/or selected in order to be displayed as part of the alert.

FAU_ARP_EXT.1 Security Alarm Filtering

FAU_ARP_EXT.1.1 The TSF shall provide the ability to apply [**assignment**: *methods of selection*] to selectively exclude alerts from being generated.

FAU_GEN.1/WIDS Audit Data Generation (WIDS)

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [not specified] level of audit;
c. [*Auditable events listed in the Auditable Events table (Table 1);*
d. *Failure of wireless sensor communication*].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ANO_EXT.1 (selection-based)	None	None
FAU_ARP.1	Actions taken due to potential security violations	None
FAU_ARP_EXT.1	None	None
FAU_GEN.1/WIDS	None	None

FAU_IDS_EXT.1	None	None
FAU_INV_EXT.1	Presence of allowedlisted device	Type of device (AP or EUD), MAC Address
FAU_INV_EXT.2	None	None
FAU_INV_EXT.3	Location of AP or EUD	MAC Address, device type, classification of device, sensor(s) that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s)
FAU_INV_EXT.4 (objective)	None	None
FAU_INV_EXT.5 (objective)	None	None
FAU_MAC_EXT.1 (objective)	None	None
FAU_RPT_EXT.1	None	None
FAU_SAA.1	None	None
FAU_SIG_EXT.1 (selection-based)	None	None
FAU_STG_EXT.1/PCAP (selection-based)	None	None
FAU_WID_EXT.1	Detection of rogue AP or EUD	None
	Detection of unauthorized SSID	None
FAU_WID_EXT.2	Sensor wireless transmission capabilities	Wireless transmission capabilities are turned on
FAU_WID_EXT.3 (optional)	Detection of network devices operating in selected RF bands	Frequency band, channel used within frequency band, identification information (MAC address if applicable or other similar unique ID), device technology (i.e., cellular), sensor(s) that detected devices
FAU_WID_EXT.4 (optional)	None	None
FAU_WIP_EXT.1 (objective)	Isolation of AP or EUD	Description of violation, type of containment used, was containment triggered manually or automatically, sensor performing the containment (if wireless), details about the device (s) being contained (classification, device type, MAC address)
FDP_IFC.1	None	None
FMT_SMF.1/WIDS	None	None
FPT_FLS.1 (objective)	Information about failure	Indication that there was a failure, type of failure, device that failed, and time of failure

Table 1: Auditable Events

Application Note: The auditable events defined in Table 1 are for the SFRs that are explicitly defined in this PP-Module and are intended to extend FAU_GEN.1 in the Base-PP. The events in the Auditable Events table should be combined with those of the NDcPP in the context of a conforming Security Target.

The Auditable Events (Table 1) includes optional and objective SFRs. The auditing of optional and objective SFRs is only required if that SFR is included in the ST.

Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel.

FAU_GEN.1.2/WIDS The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, and subject identity (if applicable);
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*auditable events listed in Auditable Events table (Table 1)*].

Application Note: The subject identity in this case is the allowlisted inventory item.

FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

FAU_IDS_EXT.1.1 The TSF shall provide the following methods of intrusion detection [**selection**: *anomaly-based*, *signature-based*, *[**assignment**: other detection method]*].

Application Note: At least one detection method must be selected. If multiple detection methods are supported, each supported method must be selected. If anomaly-based detection is selected, then FAU_ANO_EXT.1 shall be included in the ST. If signature-based detection is selected, then FAU_SIG_EXT.1 shall be included in the ST.

FAU_INV_EXT.1 Environmental Inventory

FAU_INV_EXT.1.1 The TSF shall determine if a given AP is authorized based on [**selection**: *MAC addresses*, *[**assignment**: other unique device identifier]*]

FAU_INV_EXT.1.2 The TSF shall determine if a given EUD is authorized based on [**selection**: *MAC addresses*, *[**assignment**: other unique device identifier]*]

FAU_INV_EXT.1.3 The TSF shall detect the presence of non-allowlisted EUDs and APs in the Operational Environment.

Application Note: This inventory is used as an allowlist to indicate to the WIDS which APs and EUDs are authorized members of the wireless network. The inventory of authorized APs and EUDs is configured by FMT_SMF.1/WIDS.

The terminology used to describe an inventoried or allowlisted device may vary by vendor product. This PP-Module utilizes allowlisted to describe APs and EUDs that are part of the inventory and non-allowlisted to describe APs and EUDs that are not part of the inventory.

FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.2.1 The TSF shall detect the

- Current RF band
- Current channel
- MAC Address
- Received signal strength
- Device detection timestamps
- Classification of APs and EUDs
- [**selection**: *[**assignment**: other details]*, *no other details*]

of all APs and EUDs within range of the TOE's wireless sensors.

FAU_INV_EXT.2.2 The TSF shall detect the following additional details for all APs within range of the TOE's wireless sensors:

- encryption
- number of connected EUDs.
- Received frames/packets
- Beacon rate
- SSID of AP (if not hidden).

Application Note: For detection of encryption type, the TSF should be able to differentiate between the different WLAN encryption methods and when no encryption is in use.

FAU_INV_EXT.2.3 The TSF shall detect the follow additional details for all EUDs within range of the TOE's wireless sensors:

- SSID and BSSID of AP it is connected to.
- DHCP configuration.

FAU_INV_EXT.3 Location of Environmental Objects

FAU_INV_EXT.3.1 The TSF shall detect the physical location of APs and EUDs to within [**assignment**: *value equal or less than 25*] feet of their actual location.

FAU_INV_EXT.3.2 The TSF shall detect received signal strength and [**selection**: *RF power levels above a predetermined threshold*, *no other characteristics*] of hardware operating within range of the TOE's wireless sensors.

FAU_RPT_EXT.1 Intrusion Detection System - Reporting Methods

FAU_RPT_EXT.1.1 The TSF shall provide [**selection**:

- *Syslog using [**selection**: defined API, Syslog, [**assignment**: other detection method]]*,
- *SNMP trap reporting using [**selection**: defined API, Simple Network Management Protocol (SNMP), [**assignment**: other detection method]]*

] for reporting of collected data.

Application Note: Syslog and/or SNMP trap reporting can be used. At least one reporting method must be selected.

FAU_RPT_EXT.1.2 The TSF shall provide the ability to import data, such as an allowlist of APs and EUDs, and WIDS/WIPS configuration files from the system using [**selection**: *custom API*, *Syslog*, *common log format*, *CSV*, *[**assignment**: vendor detection method]*].

Application Note: The system must provide the ability to interact with an extensible interface to a third party wireless monitoring system for the purposes of importing data from the wireless system.

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules for monitoring **the wireless traffic** and based upon these rules indicate a potential **malicious action**.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring **wireless traffic:**

a. Accumulation or combination of [**assignment**: *subset of defined auditable events*]

known to indicate a potential security violation,
b. *Detection of non-allowlisted AP*,
c. *Detection of non-allowlisted EUD*,
d. *Detection of authorized EUD establishing peer-to-peer connection with any otherEUD*,
e. *Detection of EUD bridging two network interfaces*,
f. *Detection of unauthorized point-to-point wireless bridges by allowlisted APs*,
g. *Alert generated by violation of user defined signature*,
h. *Detection of ICS connection*,
i. *Detection of traffic with excessive transmit power level*,
j. *Detection of MAC spoofing*,
k. *Detection of unauthorized AP broadcasting authorized SSIDs*,
l. *Detection of authorized AP broadcasting an unauthorized SSID*,
m. *Detection of allowlisted EUD connected to unauthorized SSID*,
n. *Detection of NULL SSID associations*,
o. *Detection of active probing*,
p. *Detection of packet flooding/DoS/DDoS*,
q. *Detection of RF-based denial of service*,
r. *Detection of deauthentication flooding*,
s. *Detection of disassociation flooding*,
t. *Detection of request-to-send/clear-to-send abuse*,
u. *Detection of unauthorized authentication scheme use*,
v. *Detection of unauthorized encryption scheme use*,
w. *Detection of unencrypted traffic*,
x. *Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations*,
y. *Detection of extremely high numbers of client devices using a particular allowlistedAP*,
z. *Detection of a high number of failed attempts to join theWLAN in a short period of time*,
aa. *Detection of the use of activeWLAN scanners (e.g. wardriving tools) to generateWLAN traffic, such as Probes, Auths, and Assoc frames*,
ab. *Detection of the physical location of an identifiedWLAN threat by using triangulation*,
ac. *Detection of an SSID using weak/unsupported/disallowed encryption options*,
ad. *Detection of AP SSID larger than 32 bytes*,
ae. *[**assignment**: any other rules]*.

Application Note: These rules are used to detect a potential security violation. Maintenance of the rules by adding, modifying or deletion of rules from the set of rules is handled by FMT_SMF.1/WIDS.

If a potential security violation is detected the alert generated for the Administrator is handled by FAU_ARP.1.

FAU_WID_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects

FAU_WID_EXT.1.1 The TSF shall distinguish between benign and malicious APs and EUDs based on if the APs and EUDs are authorized and [**selection**: *automatic detection metrics*, *no other method*].

Application Note: FAU_INV_EXT.1 defines that an AP or EUD is authorized based on if the AP/EUD is allowlisted as configured in FMT_SMF.1. A non-allowlisted device does not always have to be conducting malicious activity. However, it is acceptable to equate an allowlisted AP/EUD as both authorized/benign and a nonallowlistedAP/EUD as both not authorized and thus malicious. If the TOE supports automatic malicious device detection, based on in-depth network traffic analysis, "automatic detection metrics" must be selected. This can be used to further distinguish if the AP/EUD is benign or malicious. If theTOE does not support automatic detection metrics, "no other method" must be selected.

FAU_WID_EXT.1.2 The TSF shall provide the ability to determine if a givenSSID is authorized.

Application Note: FMT_SMF.1/WIDS defines the subset of authorizedSSID(s).

FAU_WID_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring

FAU_WID_EXT.2.1 The TSF shall [**selection**: *simultaneously*, *nonsimultaneously*] monitor and analyze network traffic matching the 802.11 monitoring SFP for all channels in the following RF frequencies:

- 2.4 GHz
- 5.0 GHz

and [**selection**:

- *[**assignment**: specified Wi-Fi channels] in the 4.9 GHz regulatory domain*,
- *channels outside regulatory domain*,
- *non-standard channel frequencies*,
- *no other domains*

].

Application Note: If "nonsimultaneously" is selected, then "Define the amount of time sensor monitors a specific channel" must be selected in FMT_SMF.1/WIDS.

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1 and defined through FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

FAU_WID_EXT.2.2 The TSF shall provide wireless sensors to detect network traffic matching the 802.11 monitoring SFP that [**selection**: *can be configured to prevent transmission of data*, *does not transmit data*].

Application Note: If "can be configured to prevent transmission of data" is selected then "Enable/Disable transmission of data by wireless sensor" must be selected in FMT_SMF.1/WIDS.

The intent of this SFR is to employ WIDS sensors that can have all wireless transmission capabilities disabled for instances where a site wishes to implement a no wireless policy.

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1 and defined through FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

FAU_WID_EXT.2.3 The TSF shall perform stateful frame inspection and log attacks spanning multiple frames.

Application Note: Attackers possess the capability to distribute an attack across multiple frames in an attempt to avoid traditional detection measures that solely focus on packet headers. Stateful frame inspection will allow for the identification of obfuscation techniques centered around spreading an attack across multiple frames.

5.2.2 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*802.11 monitoring SFP*] on [*all IEEE 802.11 a, b, g, n, ac frame types and subtypes between:*

- *authorized APs and authorized EUDs*
- *authorized APs and unauthorized EUDs*
- *unauthorized APs and authorized EUDs*].

Application Note: "Authorized" EUDs/APs are those that are assigned to the allowlist as defined by FMT_SMF.1/WIDS.

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1 and defined through FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

5.2.3 Security Management (FMT)

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

FMT_SMF.1.1/WIDS The TSF shall be capable of performing the following management functions for WIDS functionality:

- Define an inventory of authorized APs based on [**selection**: *MAC addresses*, *[**assignment**: other unique device identifier]*],
- Define an inventory of authorized EUDs based on MAC addresses,
- Define rules for monitoring and alerting on the wireless traffic,
- Define authorized SSID(s),
- Define authorized WLAN authentication schemes,
- Define authorized WLAN encryption schemes,
- [**selection**:
  - *Specify periods of network activity that constitute baseline of expected behavior*,
  - *Define anomaly activity*,
  - *Define classification rules to detect rogue APs*,
  - *[**selection**: enable, disable] transmission of data by wireless sensor*,
  - *Define attack signatures*,
  - *Define rules for overwriting previous packet captures*,
  - *Define the amount of time sensor monitors a specific [**selection**: frequency, channel]*,
  - *Define authorized and unauthorized TCP/IP and UDP traffic*,
  - *Define known malicious activity ports*,
  - *No other capabilities*

  ].

Application Note: Define authorized WLAN authentication and encryption schemes does not enforce, but rather establishes a baseline to determine if an unauthorized scheme is used.

If FAU_ANO_EXT.1 is included in the ST, "Specification of periods of network activity that constitute baseline of expected behavior" must be selected. If FAU_ANO_EXT.1 is included in the ST and "manual configuration by administrators" is selected in FAU_ANO_EXT.1, then "Definition of anomaly activity" must be selected.

If "can be configured to prevent transmission of data" is selected in FAU_WID_EXT.2 then "Enable/Disable transmission of data by wireless sensor" must be selected.

It is expected that an Authorized Administrator will be responsible for configuring the AP to operate on a specific frequency pursuant to the 802.11 standard. The TSF will have the ability to adjust the amount of time it passively monitors and captures WLAN traffic on a given frequency and channel.

5.3 TOE Security Functional Requirements Rationale

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

OBJECTIVE	ADDRESSED BY	RATIONALE
O.SYSTEM_MONITORING	FAU_GEN_EXT.1 (from Base-PP), FAU_STG_EXT.1 (from Base-PP), FAU_GEN.1/WIDS, FAU_RPT_EXT.1, FAU_STG_EXT.1/PCAP, FPT_FLS.1 (objective)	FAU_GEN_EXT.1 supports the objective by requiring the TSF to identify the records of its own operation that its various components generate.

		FAU_STG_EXT.1 supports the objective by requiring the TSF to implement an external storage method for the records it generates of its own operation. FAU_GEN.1/WIDS supports the objective by defining the auditable events that the TSF must implement in support of the behavior this PP-Module defines. FAU_RPT_EXT.1 supports the objective by requiring the TSF to implement an external import and reporting mechanism for its monitoring data to integrate with third-party components. FAU_STG_EXT.1/PCAP supports the objective by defining an optional reporting mechanism for monitored data. FPT_FLS.1 supports the objective by ensuring that a potential sensor failure triggers the TOE to fail into a secure state, which prevents undetected wireless communications.
O.WIDS_ANALYZE	FAU_ARP.1, FAU_ARP_EXT.1, FAU_IDS_EXT.1, FAU_INV_EXT.1, FAU_INV_EXT.2, FAU_INV_EXT.3, FAU_SAA.1, FAU_WID_EXT.1, FAU_WID_EXT.2, FDP_IFC.1, FAU_WID_EXT.3 (optional), FAU_WID_EXT.4 (optional), FAU_ANO_EXT.1 (selection-based), FAU_SIG_EXT.1 (selection-based), FAU_INV_EXT.4 (objective), FAU_INV_EXT.5 (objective), FAU_MAC_EXT.1 (objective)	FAU_ARP.1 supports the objective by defining how the TSF must react when data consistent with an IDS violation is collected. FAU_ARP_EXT.1 supports the objective by defining a filtering method that the TSF may implement to suppress certain reactions. FAU_IDS_EXT.1 supports the objective by defining the specific IDS methods that the TSF may implement to detect potential malicious activity. FAU_INV_EXT.1 supports the objective by defining how the TSF takes an inventory of allowed and disallowed devices in its operational environment. FAU_INV_EXT.2 supports the objective by requiring the TSF to collect and report on specific properties of inventoried devices. FAU_INV_EXT.3 supports the objective by requiring the TSF to implement measures that can be used to determine the physical location of inventoried devices. FAU_SAA.1 supports the objective by defining the specific conditions that the TSF must apply to determine if collected data is indicative of potential malicious activity. FAU_WID_EXT.1 supports the objective by requiring the TSF to implement a method to distinguish between benign and malicious devices in its

		operational environment. FAU_WID_EXT.2 supports the objective by requiring the TSF to implement stateful monitoring of network traffic on various RF bands. FDP_IFC.1 supports the objective by defining the specific network traffic that the TSF must have the ability to monitor. FAU_WID_EXT.3 supports the objective by optionally requiring the TSF to detect network devices operating on frequency bands beyond what is required by FAU_WID_EXT.2. FAU_WID_EXT.4 supports the objective by optionally requiring the TOE to implement wireless spectrum analysis functionality on a dedicated sensor. FAU_ANO_EXT.1 supports the objective by defining the specific anomaly-based detection mechanisms that the TSF is required to implement if it claims to support anomaly-based detection. FAU_SIG_EXT.1 supports the objective by requiring the TSF to support user-defined and customizable attack signatures if it claims to support signature-based detection. FAU_INV_EXT.4 supports the objective by optionally requiring the TSF to detect when unauthorized wireless devices connect to a protected network over a wired interface. FAU_INV_EXT.5 supports the objective by optionally requiring the TSF to include a signal library. FAU_MAC_EXT.1 supports the objective by optionally requiring the TSF to detect potential device impersonation through MAC spoofing.
O.WIDS_REACT	FAU_ARP.1, FAU_SAA.1, FMT_SMF.1/WIDS, FAU_ANO_EXT.1 (selection-based), FAU_WIP_EXT.1 (objective)	FAU_ARP.1 supports the objective by defining how the TSF reacts when anomalous or potentially malicious traffic is detected. FAU_SAA.1 supports the objective by defining potentially malicious traffic patterns that the TSF must detect. FMT_SMF.1/WIDS supports the objective by allowing administrators to define potentially malicious or anomalous behavior. FAU_ANO_EXT.1 supports the objective by optionally requiring the TSF to detect when traffic is detected that meets a condition for anomalous behavior. FAU_WIP_EXT.1 supports

		the objective by requiring the TSF to implement wireless containment as a method of enforcing wireless intrusion prevention.
O.TOE_ADMINISTRATION	FMT_SMF.1/WIDS, FPT_FLS.1 (objective)	FMT_SMF.1/WIDS supports the objective by requiring the TSF to implement management functions that support its configuration. FPT_FLS.1 supports the objective by ensuring that a potential compromise of the TSF triggers the TOE to fail into a secure state, which prevents unauthorized administration.
O.TRUSTED_COMMUNICATIONS	FCO_CPC_EXT.1 (from Base-PP), FPT_ITT.1 (from Base-PP), FTP_ITC.1 (from Base-PP)	FCO_CPC_EXT.1 supports the objective by ensuring that distributed components are properly registered and authenticated. FPT_ITT.1 supports the objective by defining the trusted communications protocol used to secure communications between TOE components. FTP_ITC.1 supports the objective by defining the trusted communications protocol used to secure communications between the TOE and its operational environment.

6 Consistency Rationale

6.1 collaborative Protection Profile for Network Devices

6.1.1 Consistency of TOE Type

When this PP-Module extends the Network Device cPP, the TOE type for the overall TOE is still WIDS/WIPS products.

6.1.2 Consistency of Security Problem Definition

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

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	This threat is similar to the T.UNDETECTED_ACTIVITY threat in the Base-PP but it applies to the attacker performing malicious actions on the network monitored by the TOE rather than against the TOE itself.
T.UNAUTHORIZED_ACCESS	This threat is similar to the T.UNAUTHORIZED_ADMINISTRATOR_ACCESS threat in the Base-PP but it applies to the attacker gaining unauthorized access to an asset on the network monitored by the TOE rather than against the TOE itself.
T.DISRUPTION	This threat is for a denial-of-service attack against an asset on the network monitored by the TOE. The Base-PP does not define any threats for availability but there is no consistency issue here because the threat applies to an interface that doesn't exist in the Base-PP.
A.CONNECTIONS	This assumption defines the TOE's placement in a network such that it is able to perform its required security functionality. The Base-PP does not define any assumptions about the TOE's architectural deployment so there is no conflict here.
A.PROPER_ADMIN	This assumption is comparable to the A.TRUSTED_ADMINISTRATOR assumption from the Base-PP, applied to the specific administrative functions defined in this PP-Module.
P.ANALYZE	This organizational security policy expects the data produced by the TSF about the behavior of external entities to be used in an organization's analytical process. There is no conflict with the Base-PP because the Base-PP does not define any functionality for the TOE to produce data about any entities other than itself.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the NDcPP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.SYSTEM_MONITORING	The Base-PP does not define any TOE objectives. However, it does define requirements for the collection and secure remote transmission of audit data. The PP-Module adds requirements for the similar handling of network traffic data.
O.WIDS_ANALYZE	This objective refers to behavior on wireless interfaces that are beyond the original scope of the Base-PP.
O.WIDS_REACT	This objective refers to behavior on wireless interfaces that are beyond the original scope of the Base-PP.
O.TOE_ADMINISTRATION	The Base-PP does not define any TOE objectives. However, it does define requirements for the execution of security-relevant management functions. The PP-Module expands upon this by adding requirements for the security-relevant management functions that are introduced by the PP-Module.
O.TRUSTED_COMMUNICATIONS	The Base-PP does not define any TOE objectives. However, it clearly intends to ensure that communications are trusted because the SFRs the PP-Module uses to demonstrate this objective is satisfied are derived from the Base-PP.

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

PP-Module Operational Environment Objective	Consistency Rationale
OE.CONNECTIONS	This objective expects the TOE to be placed in a network such that it is able to perform its required security functionality. The Base-PP does not define any objectives about the TOE's architectural deployment so there is no conflict here.
OE.PROPER_ADMIN	This objective is comparable to the OE.TRUSTED_ADMIN objective from the Base-PP, applied to the specific administrative functions defined in this PP-Module.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) functionality. This is considered to be consistent because the functionality provided by the NDcPPis being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDcPP that are used entirely to provide functionality for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS). The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
FAU_GEN_EXT.1	This PP-Module mandates the inclusion of this selection-basedSFR because a TOE that conforms to this PP-Module will always be deployed in a configuration that requires thisSFR to be claimed.
FAU_STG_EXT.1	This PP-Module modifies the Base-PP SFR to remove a selection that is not permitted by the TOE architecture that it specifies.
FCO_CPC_EXT.1	This PP-Module mandates the inclusion of this optionalSFR because it is required to implement functionality required by this PP-Module.
FPT_ITT.1	This PP-Module mandates the inclusion of this optionalSFR because it is required to implement functionality required by this PP-Module.
FTP_ITC.1	This PP-Module refines the Base-PP SFR to add a selection for a specific external entity that may be applicable to a TOE that conforms to this PP-Module.
	Mandatory SFRs
FAU_ARP.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_ARP_EXT.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_GEN.1/WIDS	This SFR iterates the FAU_GEN.1 SFR defined in the Base-PP to define auditable events for the functionality that is specific to this PP-Module.
FAU_IDS_EXT.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_INV_EXT.1	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_INV_EXT.2	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_INV_EXT.3	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_RPT_EXT.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_SAA.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_WID_EXT.1	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_WID_EXT.2	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FDP_IFC.1	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FMT_SMF.1/WIDS	This SFR iterates the FMT_SMF.1 SFR defined in the Base-PP to define management functions for the functionality that is specific to this PP-Module.
	Optional SFRs
FAU_WID_EXT.3	This SFR defines operations to be performed on assets in theTOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of theTOE beyond what the Base-PP defines.
FAU_WID_EXT.4	This SFR defines an optional capability for a distributed component to be dedicated to one particular function. This function (wireless spectrum analysis) is defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
	Selection-based SFRs
FAU_ANO_EXT.1	This SFR defines operations to be performed on collectedWIDS data, which is collected using an

	external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
FAU_SIG_EXT.1	This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
FAU_STG_EXT.1/PCAP	This SFR iterates the FAU_STG_EXT.1 SFR defined in the Base-PP for storage of audit data and applies it to storage of packet captures.
Objective SFRs	
FAU_INV_EXT.4	This SFR defines operations to be performed on assets in the TOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
FAU_INV_EXT.5	This SFR defines operations to be performed on assets in the TOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
FAU_MAC_EXT.1	This SFR defines operations to be performed on assets in the TOE's operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines.
FAU_WIP_EXT.1	This SFR defines WIPS behavior in response to detection of potential malicious activity in the TOE's operational environment. This extends the logical scope of the TOE beyond what the Base-PP defines.
FPT_FLS.1	This SFR defines preservation of a secure state in the event that a failure condition is detected. The Base-PP does not define an SFR for this behavior but this SFR mitigates the T.SECURITY_FUNCTIONALITY_FAILURE threat defined in the Base-PP, so it is clear that this behavior is consistent with the security expectations of the Base-PP.

Appendix A - Optional SFRs

FAU_WID_EXT.3 Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring

FAU_WID_EXT.3.1 The TSF shall detect the presence of network devices that operate in the following RF bands: [**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular bands*].

Application Note: This SFR refers to Non-WLAN (IEEE 802.11 a, b, g, n, and ac) network devices that operate in the specified frequencies. There is an understanding that this capability requires a TOE to use specialized, licensed radio systems. This SFR will allow for the introduction of an open API, set of defined interoperability standards, or other proprietary solution(s), to allow for third-party integrations.

FAU_WID_EXT.4 Wireless Intrusion Detection - Wireless Spectrum Analysis

FAU_WID_EXT.4.1 The TSF shall provide a dedicated sensor for wireless spectrum analysis.

Appendix B - Selection-based SFRs

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

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

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

] and the following network protocol fields:

- all management and control frame header elements.

FAU_ANO_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").

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

FAU_SIG_EXT.1.1 The TSF shall support user-defined and customizable attack signatures.

FAU_STG_EXT.1/PCAP Protected Audit Event Storage (Packet Captures)

FAU_STG_EXT.1.1/PCAP The TSF shall be able to transmit the generated **packet captures** to an external IT entity **hosting a protocol analyzer** using a trusted channel according to FTP_ITC.1.

Application Note: Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel per FTP_ITC.1. Note that this PP-Module modifies FTP_ITC.1 from the Base-PP. If "capture raw frame traffic that triggers the violation" is selected in FAU_ARP.1, then this SFR must be included in the ST, and this iteration is for the PCAPs generated as a selectable action completed upon detection of a potential security violation in FAU_ARP.1.

FAU_STG_EXT.1.2/PCAP The TSF shall be able to store generated **packet captures** on the TOE itself. In addition [**selection**:

- *The TOE shall be a distributed TOE that stores **packet capture** data on the following TOE components: [**assignment**: identification of TOE components]*,
- *The TOE shall be a distributed TOE with storage of **packet capture** data provided externally for the following TOE components: [**assignment**: list of TOE components that do not store **packet capture** data locally and the other TOE components to which they transmit their generated **packet capture** data]*

].

FAU_STG_EXT.1.3/PCAP The TSF shall [**selection**: *drop new **packet capture** data*, *overwrite previous **packet captures** according to the following rule: [**assignment**: rule for overwriting previous **packet captures**]*, *[**assignment**: other action]*] when the local storage space for **packet capture** data is full.

Appendix C - Objective SFRs

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

FAU_INV_EXT.4 Detection of Unauthorized Connections

FAU_INV_EXT.4.1 The TSF shall detect when non-allowlisted APs have a wired connection to the internal corporate network.

FAU_INV_EXT.5 Signal Library

FAU_INV_EXT.5.1 The TSF shall include a signal library.

Application Note: The TSF will need to have the ability to import, export, or update the exisiting signal library.

FAU_MAC_EXT.1 Device Impersonation

FAU_MAC_EXT.1.1 The TSF shall detect when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously.

Application Note: The intent of this SFR is to detect MAC spoofing where an attacker is able to cause the allowlisted EUD to disconnect and promptly connects a non-allowlisted device using the MAC address of the allowlisted EUD.

FAU_MAC_EXT.1.2 The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-allowlisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors.

Application Note: The intent of this SFR is to allow the administrator to determine the time that should be allowed between an allowlisted EUD connecting in two distant locations.

FAU_WIP_EXT.1 Wireless Intrusion Prevention

FAU_WIP_EXT.1.1 The TSF shall allow an Authorized Administrator to isolate a wireless AP or EUD from the network monitored by the TSF using the following methods: [**selection**: *wireless containment*, *wire-side containment of an unauthorized AP connected to the internal corporate wired network*].

Application Note: It is expected that an Authorized Administrator will be responsible for confirming the AP or EUD as a rogue AP or EUD to initiate wireless containment.

In this SFR the containment of an an unauthorized AP connected to the internal corporate wired network refers to an unauthorized AP that is physically connected (via wire) to the protected internal wired infrastructure.

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*sensor functionality failure, potential compromise of the TSF*].

Application Note: At minimum, the preservation of a secure state requires the generation of audit records when the defined failure conditions occur.

Appendix D - Extended Component Definitions

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

D.1 Background and Scope

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

Functional Class	Functional Components
Security Audit (FAU)	FAU_ANO_EXT Anomaly-Based Intrusion Detection FAU_ARP_EXT Security Alarm Filtering FAU_IDS_EXT Intrusion Detection Methods FAU_INV_EXT Environmental Inventory FAU_MAC_EXT Device Impersonation FAU_RPT_EXT Reporting Methods FAU_SIG_EXT Signature-Based Intrusion Detection FAU_WID_EXT Wireless Intrusion Detection FAU_WIP_EXT Wireless Intrusion Prevention

D.2 Extended Component Definitions

FAU_ARP_EXT Security Alarm Filtering

Family Behavior

This family defines requirements for suppression of audit events. It is intended to complement the FAU_ARP family already defined in CC Part 2.

Component Leveling

FAU_ARP_EXT.1, Security Alarm Filtering, requires the TSF to implement a filtering mechanism to selectively suppress the generation of security alarms.

Management: FAU_ARP_EXT.1

No specific management functions have been identified.

Audit: FAU_ARP_EXT.1

There are no auditable events foreseen.

FAU_ARP_EXT.1 Security Alarm Filtering

Hierarchical to: No other components.

Dependencies to: FAU_ARP.1 Security Alarms

FAU_ARP_EXT.1.1

The TSF shall provide the ability to apply [**assignment**: *methods of selection*] to selectively exclude alerts from being generated.

FAU_IDS_EXT Intrusion Detection Methods

Family Behavior

This family defines requirements for supported methods of intrusion detection.

Component Leveling

FAU_IDS_EXT.1, Intrusion Detection System - Intrusion Detection Methods, requires the TSF to specify the methods of intrusion detection that it supports.

Management: FAU_IDS_EXT.1

No specific management functions are identified.

Audit: FAU_IDS_EXT.1

There are no auditable events foreseen.

FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_IDS_EXT.1.1

The TSF shall provide the following methods of intrusion detection [**selection**: *anomaly-based*, *signature-based*, *[**assignment**: other detection method]*].

FAU_INV_EXT Environmental Inventory

Family Behavior

This family defines requirements for detection and inventorying of network assets in theTOE's operational environment.

Component Leveling

FAU_INV_EXT.1, Environmental Inventory, requires the TSF to determine if inventoried objects are authorized or unauthorized.

Management: FAU_INV_EXT.1

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

- Definition of inventory of authorized APs based on MAC address
- Definition of inventory of authorized EUDs based on MAC address

Audit: FAU_INV_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Presence of allowlisted device

FAU_INV_EXT.1 Environmental Inventory

Hierarchical to: No other components.

Dependencies to: FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.1.1

The TSF shall determine if a given AP is authorized based on [**selection**: *MAC addresses*, *[**assignment**: other unique device identifier]*]

FAU_INV_EXT.1.2

The TSF shall determine if a given EUD is authorized based on [**selection**: *MAC addresses*, *[**assignment**: other unique device identifier]*]

FAU_INV_EXT.1.3

The TSF shall detect the presence of non-allowlisted EUDs and APs in the Operational Environment.

Component Leveling

FAU_INV_EXT.2, Characteristics of Environmental Objects, requires the TSF to discover network assets in its operational environment and maintain an inventory of them based on collected attributes.

Management: FAU_INV_EXT.2

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

- Definition of classification rules to detect rogue APs

Audit: FAU_INV_EXT.2

There are no auditable events foreseen.

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.2.1

The TSF shall detect the

- Current RF band
- Current channel
- MAC Address
- Received signal strength
- Device detection timestamps
- Classification of APs and EUDs
- [**selection**: *[**assignment**: other details]*, *no other details*]

of all APs and EUDs within range of theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the following additional details for all APs within range of theTOE's wireless sensors:

- encryption
- number of connected EUDs.
- Received frames/packets
- Beacon rate
- SSID of AP (if not hidden).

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for all EUDs within range of theTOE's wireless sensors:

- SSID and BSSID of AP it is connected to.
- DHCP configuration.

Component Leveling

FAU_INV_EXT.3, Location of Environmental Objects, requires the TSF to approximate the physical location of network assets in its operational environment based on triangulation of wireless emissions.

Management: FAU_INV_EXT.3

No specific management functions are identified.

Audit: FAU_INV_EXT.3

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in thePP/ST:

- Physical location and identification of AP or EUD

FAU_INV_EXT.3 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to: FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.3.1

The TSF shall detect the physical location of APs and EUDs to within [**assignment**: *value equal or less than 25*] feet of their actual location.

FAU_INV_EXT.3.2

The TSF shall detect received signal strength and [**selection**: *RF power levels above a predetermined threshold*, *no other characteristics*] of hardware operating within range of theTOE's wireless sensors.

Component Leveling

FAU_INV_EXT.4, Detection of Unauthorized Connections, requires the TSF to identify if an unauthorized network asset in its inventory is attempting to access a protected network using a wired connection.

Management: FAU_INV_EXT.4

No specific management functions are identified.

Audit: FAU_INV_EXT.4

There are no auditable events foreseen.

FAU_INV_EXT.4 Detection of Unauthorized Connections

Hierarchical to: No other components.

Dependencies to: FAU_INV_EXT.1 Environmental Inventory

FAU_INV_EXT.4.1

The TSF shall detect when non-allowlisted APs have a wired connection to the internal corporate network.

Component Leveling

FAU_INV_EXT.5, Signal Library, requires the TSF to maintain a signal library.

Management: FAU_INV_EXT.5

No specific management functions are identified.

Audit: FAU_INV_EXT.5

There are no auditable events foreseen.

FAU_INV_EXT.5 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.5.1

The TSF shall include a signal library.

FAU_RPT_EXT Reporting Methods

Family Behavior

This family defines requirements for the format of generated reports.

Component Leveling

FAU_RPT_EXT.1, Intrusion Detection System - Reporting Methods, requires the TSF to implement a specified reporting mechanism for collected data for compatibility with third parties that may consume this data.

Management: FAU_RPT_EXT.1

No specific management functions are identified.

Audit: FAU_RPT_EXT.1

There are no auditable events foreseen.

FAU_RPT_EXT.1 Intrusion Detection System - Reporting Methods

Hierarchical to: No other components.

Dependencies to: FAU_GEN.1 Audit Data Generation

FAU_RPT_EXT.1.1

The TSF shall provide [**selection**:

- *Syslog using [**selection**: defined API, Syslog, [**assignment**: other detection method]]*,
- *SNMP trap reporting using [**selection**: defined API, Simple Network Management Protocol (SNMP), [**assignment**: other detection method]]*

] for reporting of collected data.

FAU_RPT_EXT.1.2

The TSF shall provide the ability to import data, such as an allowlist of APs and EUDs, and WIDS/WIPS configuration files from the system using [**selection**: *custom API*, *Syslog*, *common log format*, *CSV*, *[**assignment**: vendor detection method]*].

FAU_WID_EXT Wireless Intrusion Detection

Family Behavior

This family defines requirements for data collection of potentially malicious wireless network activity.

Component Leveling

FAU_WID_EXT.1, Wireless Intrusion Detection - Malicious Environmental Objects, requires the TSF to implement a mechanism to distinguish between authorized and unauthorized network assets.

Management: FAU_WID_EXT.1

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

- Definition of authorized SSID(s)
- Definition of authorized WLAN authentication schemes
- Definition of authorized WLAN encryption schemes
- Definition of authorized WLAN traffic schemes

Audit: FAU_WID_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Detection of rogue AP or EUD
- Detection of unauthorized SSID

FAU_WID_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects

Hierarchical to: No other components.

Dependencies to: FAU_INV_EXT.1 Environmental Inventory

FAU_WID_EXT.1.1

The TSF shall distinguish between benign and malicious APs and EUDs based on if the APs and EUDs are authorized and [**selection**: *automatic detection metrics*, *no other method*].

FAU_WID_EXT.1.2

The TSF shall provide the ability to determine if a given SSID is authorized.

Component Leveling

FAU_WID_EXT.2, Wireless Intrusion Detection - Passive Information Flow Monitoring, requires the TSF to surveil certain wireless frequency bands and perform stateful inspection of traffic on them.

Management: FAU_WID_EXT.2

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

- Definition of authorized and unauthorized TCP/IP and UDP traffic
- Definition of known malicious activity ports
- Definition of the amount of time that a sensor monitors a specific frequency or channel

Audit: FAU_WID_EXT.2

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Sensor wireless transmission capabilities

FAU_WID_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_WID_EXT.2.1

The TSF shall [**selection**: *simultaneously*, *nonsimultaneously*] monitor and analyze network traffic matching the 802.11 monitoring SFP for all channels in the following RF frequencies:

- 2.4 GHz
- 5.0 GHz

and [**selection**:

- *[**assignment**: specified Wi-Fi channels] in the 4.9 GHz regulatory domain*,
- *channels outside regulatory domain*,
- *non-standard channel frequencies*,
- *no other domains*

].

FAU_WID_EXT.2.2

The TSF shall provide wireless sensors to detect network traffic matching the 802.11 monitoring SFP that [**selection**: *can be configured to prevent transmission of data*, *does not transmit data*].

FAU_WID_EXT.2.3

The TSF shall perform stateful frame inspection and log attacks spanning multiple frames.

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring, requires the TSF to surveil certain radio frequency bands that fall outside the typical wireless spectrum used by consumer-grade electronics.

Management: FAU_WID_EXT.3

No specific management functions are identified.

Audit: FAU_WID_EXT.3

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in thePP/ST:

- Detection of network devices operating in selected RF bands

FAU_WID_EXT.3 Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_WID_EXT.3.1

The TSF shall detect the presence of network devices that operate in the following RF bands: [**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular bands*].

Component Leveling

FAU_WID_EXT.4, Wireless Intrusion Detection - Wireless Spectrum Analysis, requires the TSF to implement wireless spectrum analysis in a dedicated physical component.

Management: FAU_WID_EXT.4

No specific management functions are identified.

Audit: FAU_WID_EXT.4

There are no auditable events foreseen.

FAU_WID_EXT.4 Wireless Intrusion Detection - Wireless Spectrum Analysis

Hierarchical to: No other components.

Dependencies to: [FAU_WID_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring, or

FAU_WID_EXT.3 Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring]

FAU_WID_EXT.4.1

The TSF shall provide a dedicated sensor for wireless spectrum analysis.

FAU_ANO_EXT Anomaly-Based Intrusion Detection

Family Behavior

This family defines requirements for detection of malicious network activity based on anomalous behavior.

Component Leveling

FAU_ANO_EXT.1, Anomaly-Based Intrusion Detection, requires the TSF to define how it determines anomalous network traffic that may be indicative of malicious activity.

Management: FAU_ANO_EXT.1

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

- Specification of periods of network activity that constitute baselines of expected behavior
- Definition of anomaly activity

Audit: FAU_ANO_EXT.1

There are no auditable events foreseen.

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

Hierarchical to: No other components.

Dependencies to: FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

FAU_ANO_EXT.1.1

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

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

] and the following network protocol fields:

- all management and control frame header elements.

FAU_ANO_EXT.1.2

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

FAU_SIG_EXT Signature-Based Intrusion Detection

Family Behavior
This family defines requirements for detection of malicious network activity based on traffic signatures.

Component Leveling
FAU_SIG_EXT.1, Signature-Based Intrusion Detection, requires the TSF to support the definition of traffic signatures that can be compared to observed network traffic for the purpose of identifying potential malicious activity.

Management: FAU_SIG_EXT.1
The following actions could be considered for the management functions in FMT:

- Definition of attack signatures

Audit: FAU_SIG_EXT.1
There are no auditable events foreseen.

FAU_SIG_EXT.1 Signature-Based Intrusion Detection
Hierarchical to: No other components.

Dependencies to: FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

FAU_SIG_EXT.1.1

The TSF shall support user-defined and customizable attack signatures.

FAU_MAC_EXT Device Impersonation

Family Behavior
This family defines requirements for detection of potential device impersonation on the basis of MAC address spoofing.

Component Leveling
FAU_MAC_EXT.1, Device Impersonation, requires the TSF to detect possible MAC address spoofing using various methods.

Management: FAU_MAC_EXT.1
No specific management functions are identified.

Audit: FAU_MAC_EXT.1
There are no auditable events foreseen.

FAU_MAC_EXT.1 Device Impersonation
Hierarchical to: No other components.

Dependencies to: FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_MAC_EXT.1.1

The TSF shall detect when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously.

FAU_MAC_EXT.1.2

The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-allowlisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors.

FAU_WIP_EXT Wireless Intrusion Prevention

Family Behavior
This family defines requirements for wireless intrusion prevention.

Component Leveling
FAU_WIP_EXT.1, Wireless Intrusion Prevention, requires the TSF to support reactive behavior if potential malicious traffic is observed to be originating from or targeted to a particular network asset.

Management: FAU_WIP_EXT.1
The following actions could be considered for the management functions in FMT:

- Enabling or disabling transmission of data by wireless sensor

Audit: FAU_WIP_EXT.1
The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Isolation of AP or EUD

FAU_WIP_EXT.1 Wireless Intrusion Prevention
Hierarchical to: No other components.

Dependencies to: FAU_WID_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects

FAU_WIP_EXT.1.1

The TSF shall allow an Authorized Administrator to isolate a wireless AP or EUD from the network monitored by the TSF using the following methods: [**selection**: *wireless containment*, *wire-side containment of an unauthorized AP connected to the internal corporate wired network*].

Appendix E - Implicitly Satisfied Requirements

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

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

Requirement	Rationale for Satisfaction
FDP_IFF.1 - Information Flow Control Functions	CC Part 2 specifies FDP_IFF.1 as a dependency ofFDP_IFC.1 because the TSF must define the information flow control SFP rules associated with a given SFP. This dependency is implicitly addressed through FAU_WID_EXT.2, which defines the rules for the 802.11 monitoring SFP defined byFDP_IFC.1.

Appendix F - Allocation of Requirements in Distributed TOEs

For a distributed TOE, the security functional requirements in thisPP-Module need to be met by the TOE as a whole, but not all SFRs will necessarily be implemented by all components. The following categories are defined in order to specify when each SFR must be implemented by a component:

- **All Components ("All")** - All components that comprise the distributedTOE must independently satisfy the requirement.
- **At least one Component ("One")** - This requirement must be fulfilled by at least one component within the distributed TOE.
- **Feature Dependent ("Feature Dependent")** - These requirements will only be fulfilled where the feature is implemented by the distributed TOE component (note that the requirement to meet the PP-Module as a whole requires that at least one component implements these requirements if they are claimed by the TOE).

The table below specifies how each of the SFRs in this PP-Module must be met, using the categories above.

Requirement	Description	Distributed TOE SFR Allocation
FAU_ANO_EXT.1	Anomaly-Based Intrusion Detection	Feature Dependent
FAU_ARP.1	Security Alarms	One
FAU_ARP_EXT.1	Security Alarm Filtering	One
FAU_GEN.1/WIDS	Audit Data Generation (WIDS)	Feature Dependent
FAU_IDS_EXT.1	Intrusion Detection System - Intrusion Detection Methods	Feature Dependent
FAU_INV_EXT.1	Environmental Inventory	Feature Dependent
FAU_INV_EXT.2	Characteristics of Environmental Objects	Feature Dependent
FAU_INV_EXT.3	Location of Environmental Objects	Feature Dependent
FAU_INV_EXT.4	Detection of Unauthorized Connections	Feature Dependent
FAU_INV_EXT.5	Signal Library	Feature Dependent
FAU_MAC_EXT.1	Device Impersonation	Feature Dependent
FAU_RPT_EXT.1	Intrusion Detection System - Reporting Methods	Feature Dependent
FAU_SAA.1	Potential Violation Analysis	Feature Dependent
FAU_SIG_EXT.1	Signature-Based Intrusion Detection	Feature Dependent
FAU_STG_EXT.1/PCAP	Protected Audit Event Storage (Packet Captures)	Feature Dependent
FAU_WID_EXT.1	Wireless Intrusion Detection - Malicious Environmental Objects	Feature Dependent
FAU_WID_EXT.2	Wireless Intrusion Detection - Passive Information Flow Monitoring	Feature Dependent
FAU_WID_EXT.3	Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring	Feature Dependent
FAU_WID_EXT.4	Wireless Intrusion Detection - Wireless Spectrum Analysis	Feature Dependent
FAU_WIP_EXT.1	Wireless Intrusion Prevention	Feature Dependent
FDP_IFC.1	Subset Information Flow Control	Feature Dependent
FMT_SMF.1/WIDS	Specification of Management Functions (WIDS)	Feature Dependent
FPT_FLS.1	Basic Internal TSF Data Transfer Protection	Feature Dependent

Appendix G - Entropy Documentation and Assessment

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

Appendix H - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019

Appendix I - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AP	Access Point
BSSID	Basic Service Set Identifier
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
DoS	Denial of Service
EUD	End User Device
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
MAC	Media Access Control
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
SSID	Service Set Identifier
ST	Security Target
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
WEP	Wired Equivalent Protocol
WIDS	Wireless Intrustion Detection System
WIPS	Wireless Intrustion Prevention System
WLAN	Wireless Local Area Network
WPA	WLAN Protected Access