PP-Module for Wireless Intrusion Detection/Prevention System

Version: 3.0
2026-01-21
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-09-30	Initial Release - PP-Module for NDcPP
2.0	2022-09-30	Added 6 GHz spectrum slice
3.0	2026-01-21	Incorporate NIAP Technical Decisions, Update to CC:2022

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 Intrusion 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:

- Network Device collaborative Protection Profile Version 4.0

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.

A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP. The security policy enforced by an SF.

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.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
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.

Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 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 Intrusion 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 Intrusion 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.

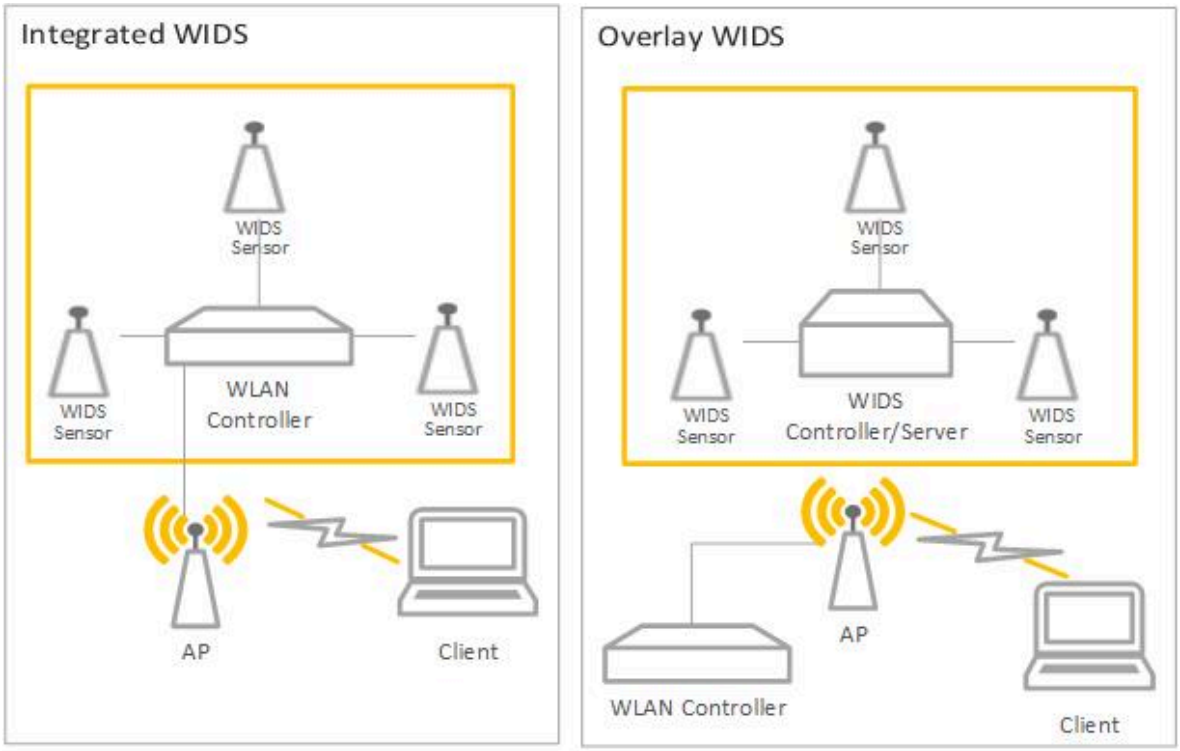


Figure 1: General TOE

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 geolocate WLAN devices within a controlled space.

The WIDS may be capable of detecting or monitoring traffic other than 802.11 WLAN, 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 inadvertent collection of any 802.11 signals is possible when operating a WIDS.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (conformant) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

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

- Network Device collaborative Protection Profile Version 4.0

Package Claim

This PP-Module is not conformant to any Functional or Assurance Packages.

3 Security Problem Definition

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 (OE) 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 OE 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 Operational 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 the TOE 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.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
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	OE.CONNECTIONS	The proper placement of the TOE within a network allows the P.ANALYZE policy to be enforced.

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 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 Collaborative Protection Profile for Network Device Security Functional Requirements Direction

In a PP-Configuration that includes the NDcPP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the 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

This SFR has been modified from its definition in the NDcPP to mandate the selection of options that correspond to distributed TOEs. A TOE that conforms to this PP-Module will always be a distributed TOE.

The text of FAU_GEN_EXT.1.1 is replaced with:

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

Any element not specified in this section is unchanged from its definition in the Base-PP.

FAU_STG_EXT.1.2: This SFR has been modified from its definition in the NDcPP to remove a selection that is not permitted by the architecture required by the PP-Module.

The text of FAU_STG_EXT.1.2 is replaced with:

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

This SFR is mandated for inclusion by this PP-Module because the WIDS TOE is expected to be a distributed system. Any element not specified in this section is unchanged from its definition in the Base-PP.

FCO_CPC_EXT.1.2: This SFR has been modified from its definition in the NDcPP to specify which communications channels are acceptable for registration.

The text of FCO_CPC_EXT.1.2 is replaced with:

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.

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

This SFR is unchanged from its definition in the Base-PP, it is only mandated for inclusion because a TOE that conforms to this PP-Module is expected to be a distributed system.

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

This SFR is modified from its definition in the Base-PP to add a selection for database server capability. Any element not specified in this section is unchanged from its definition in the Base-PP.

The text of FTP_ITC.1.1 is replaced with:

FTP_ITC.1.1 The TSF shall be capable of using [**selection:** *IPsec, SSH **[v2]**, TLS **[1.2 or 1.3]**, 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: 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.

TLS and DTLS are defined in the Functional Package for TLS. SSH is defined in the Functional Package for SSH.

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 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to potential security violations	None.
FAU_ARP_EXT.1	No events specified	N/A
FAU_GEN.1/WIDS	Any authentication event	• User login attempts and outcome • Changes to WIDS native authentication system
FAU_IDS_EXT.1	No events specified	N/A
FAU_INV_EXT.1		

	Presence of allowlisted device	• Type of device (AP or EUD) • MAC Address
FAU_INV_EXT.2	No events specified	N/A
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_RPT_EXT.1	No events specified	N/A
FAU_SAA.1	No events specified	N/A
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.
FDP_IFC.1	No events specified	N/A
FMT_SMF.1/WIDS	No events specified	N/A

5.2.2 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.1/PCAP and FAU_STG.5/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 TOE's sensors. Device attributes can then be individually filtered and/or selected in order to be displayed as part of the alert.

Evaluation Activities

FAU_ARP.1
TSS
The evaluator shall verify that the TSS describes where to find the WIDS alerts on the Administrator console/interface.

Guidance

The evaluator shall use the operational guidance for instructions on where the alerts generated are displayed within the WIDS interface. If "capture raw frame traffic that triggers the violation is selected", the evaluator shall use the operational guidance to configure the traffic capture capabilities.

Tests

- *Test FAU_ARP.1:1: The evaluator shall perform a series of events or generate traffic that would successfully trigger an alert for each of the rules defined in FAU_SAA.1. The evaluator should verify and record whether the TOE generated the alert for each rule, and provided sufficient details. The evaluator should also record the events or traffic that was generated as each alert was attempted to be triggered and record the details provided by the TOE in the alert.*
- *Test FAU_ARP.1:2: [conditional] If capturing of raw frames was selected, verify that the packet capture was triggered and stored as appropriate.*

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.

Evaluation Activities

FAU_ARP_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to filter WIDS/WIPS alerts.

Guidance
The evaluator shall verify that the operational guidance includes instructions on enabling and disabling alerts.

Tests

- *Test FAU_ARP_EXT.1:1:*
  - ***Step 1:*** *The evaluator shall use the operational guidance to enable/disable detection of available detection capabilities through the WIDS administrator interface. The evaluator shall then generate traffic that would successfully trigger the alert. The evaluator should verify that the TOE generated the alert.*
  - ***Step 2:*** *The evaluator shall disable the alert. The evaluator shall then generate events as in previous test that should successfully trigger the alert. The evaluator shall verify that the TOE did not generate an alert.*

FAU_GEN.1/WIDS Audit Data Generation (WIDS)

FAU_GEN.1.1/WIDS

The TSF shall be able to generate audit data 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 for Mandatory SFRs table (Table 2);*
d. *Failure of wireless sensor communication*;

e. *[**selection**:*
- *Auditable events listed in the Auditable Events for Optional SFRs table (Table 7) for SFRs that are present in the ST*
- *Auditable events listed in the Auditable Events for Objective SFRs table (Table 8) for SFRs that are present in the ST*
- *no other events*

]

].

Application Note: The auditable events defined in Table 2 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.

If the ST includes any optional or objective SFRs, the selection for the respective "Auditable events listed in the Auditable Events..." must be included. If no optional or objective SFRs are included in the ST, "no other events" should be selected. The auditing of the specific 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 the audit data at least the following information:

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*information specified in column three of the Auditable Events table in which the auditable event was defined*].

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

Evaluation Activities

FAU_GEN.1/WIDS

TSS

There are no TSS evaluation activities for this SFR.

Guidance

There are no operational guidance activities for this SFR.

Tests

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the evaluation activities associated with the functional requirements in this PP-Module. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

FAU_IDS_EXT.1.1

The TSF shall detect intrusions using [**selection**: *anomaly-based, signature-based, [**assignment**: other detection method]*] methods.

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.

Evaluation Activities

FAU_IDS_EXT.1

TSS

The evaluator shall verify that the TSS includes which intrusion detection method(s) the TOE utilizes. If multiple methods are selected, the evaluator shall confirm that the TSS describes how the different methods are incorporated.

Guidance

The evaluator shall verify that the operational guidance provides instructions on how to configure the TOE in order for it to detect such intrusions.

Tests

Depending on the detection technique used by the TOE, the evaluator shall confirm and note the existence of the capability and test for the appropriate selection-based requirements.

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.

Evaluation Activities

FAU_INV_EXT.1
TSS
The evaluator shall verify that the TSS describes how the presence of authorized EUDs and APs is presented by the TOE. The evaluator shall verify that the TSS includes where in the WIDS interface the list of detected APs and EUDs is displayed.

Guidance
The evaluator shall verify that the operational guidance provides instructions on how to view authorized and unauthorized APs and EUDs that are within range of the TOE sensors.

Tests

- *Test FAU_INV_EXT.1:1:*
  - ***Step 1:*** *Per guidance in FMT_SMF.1/WIDS, add MAC Addresses or other unique device identifier for an AP and EUD to the allowlist.*
  - ***Step 2:*** *Deploy the AP and EUD that were added to allowlist within the range of the TOE's sensors.*
  - ***Step 3:*** *Verify that the devices are classified as authorized.*
  - ***Step 4:*** *Remove the EUD from the allowlist.*
  - ***Step 5:*** *Verify that the EUD is classified as unauthorized.*
  - ***Step 6:*** *Remove the AP from the allowlist.*
  - ***Step 7:*** *Verify that the AP is classified as unauthorized.*
- *Test FAU_INV_EXT.1:2:*
  - ***Step 1:*** *Deploy an allowlisted AP and EUD, and connect the EUD to the AP.*
  - ***Step 2:*** *Verify that the list of detected APs and EUDs contains the allowlisted AP and EUD that were just deployed.*
  - ***Step 3:*** *If the AP and EUD are detected verify that they are classified as allowlisted devices.*
- *Test FAU_INV_EXT.1:3:*
  - ***Step 1:*** *Deploy a non-allowlisted AP and EUD and connect the EUD to the AP.*
  - ***Step 2:*** *Verify that the list of detected APs and EUDs contains the non-allowlisted AP and EUD that were just deployed.*
  - ***Step 3:*** *If the AP and EUD are detected verify that they are not classified as allowlisted devices.*

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 following additional details for all EUDs within range of the TOE's wireless sensors:

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

Evaluation Activities

FAU_INV_EXT.2
TSS
The evaluator shall verify that the TSS explains the capability of detecting the information specified in the requirements for all APs and EUDs within the TOE's wireless range.

Guidance
The evaluator shall review the operational guidance in order to verify that there are instructions that show how to locate the device inventory mentioned above.

Tests

- *Test FAU_INV_EXT.2:1:*
  - ***Step 1:*** *Deploy an allowlisted AP, non-allowlisted AP and two allowlisted EUDs.*
  - ***Step 2:*** *Connect one allowlisted EUD to the allowlisted AP and one to the non-allowlisted AP.*
  - ***Step 3:*** *Check the WIDS user interface for a list of detected APs and EUDs.*
  - ***Step 4:*** *Verify that current RF band, current channel, MAC Address, received signal strength, device detection timestamps, classification of device, are part of the information presented on the WIDS user interface for all the APs and EUDs detected. For APs verify that encryption, number of connected EUDs, SSID (if not hidden), received frames/packets and beacon rate are presented. For EUDs verify that the SSID and BSSID of AP it is connected and DHCP configuration is presented.*

FAU_INV_EXT.3 Location of Environmental Objects

FAU_INV_EXT.3.1

The TSF shall detect the physical location of rogue APs and EUDs, and [**selection**: *allow-listed APs, allow-listed EUDs, neighboring APs and EUDs, no other devices*] to within [**assignment**: *value equal or less than 25 feet*].

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.

Evaluation Activities

FAU_INV_EXT.3
TSS
The evaluator shall verify that the TSS includes information on location tracking, optimal number of sensors and sensor placement to meet the required level of accuracy.

The evaluator shall verify that the TSS contains information regarding the TSF's ability to record signal strength of hardware operating within range of its sensors.

Guidance
The evaluator shall review the operational guidance for instructions on how to configure location tracking, how to load a location map (if applicable), and where in the TSF administrator interface the location of APs and EUDs can be viewed.

If the option for detection of RF power levels above a predetermined threshold is selected, the evaluator shall use the operational guidance to set or check what the threshold is in a given test. The evaluator should also verify that the operational guidance provides instruction on how to configure the TOE to generate an alert when the threshold is exceeded.

Tests
- *Test FAU_INV_EXT.3:1:*
  - ***Step 1:*** *Deploy an AP within 25 feet of the sensors.*
  - ***Step 2:*** *Verify the TSF provides location tracking information about the AP.*
  - ***Step 3:*** *Verify the AP location presented is within 25 feet of the actual location.*
- *Test FAU_INV_EXT.3:2:*
  - ***Step 1:*** *Deploy an AP within range of the sensors.*
  - ***Step 2:*** *Check the WIDS user interface for a list of detected APs and EUDs.*
  - ***Step 3:*** *Verify that the current received signal strength is part of the information presented on the WIDS user interface about the APs and EUDs.*

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, comma separated values (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.

Evaluation Activities

FAU_RPT_EXT.1
TSS
The evaluator shall verify that the TSS includes which method the TOE utilizes.

Guidance
There are no operational guidance activities for this SFR.

Tests
Depending on the detection technique used by the TOE, the evaluator shall confirm and note the existence of the capability.

- *Test FAU_RPT_EXT.1:1:*
  - ***Step 1:*** *Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire.*
  - ***Step 2:*** *Confirm that the TSF can observe and capture traffic and events generated by the AP.*
  - ***Step 3:*** *Confirm that the TSF can use the reporting mechanisms specified in the TSS.*
  - ***Step 4:*** *Verify that the TSF can import and export observable event data in each of the formats specified in the TSS.*

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in 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 [**selection**: [**assignment**: subset of defined auditable events], no 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 (P2P) connection with any other EUD,*
e. *Detection of a single EUD, or multiple EUDs, 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 MAC spoofing,*
j. *Detection of unauthorized AP broadcasting authorized SSIDs,*

k. *Detection of authorized AP broadcasting an unauthorized SSID,*
l. *Detection of allowlisted EUD connected to unauthorized SSID,*
m. *Detection of NULL SSID associations,*
n. *Detection of active probing,*
o. *Detection of packet flooding/DoS/DDoS,*
p. *Detection of RF-based denial of service,*
q. *Detection of deauthentication flooding,*
r. *Detection of disassociation flooding,*
s. *Detection of request-to-send/clear-to-send abuse,*
t. *Detection of unauthorized authentication scheme use,*
u. *Detection of unauthorized encryption scheme use,*
v. *Detection of unencrypted traffic,*
w. *Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations,*
x. *Detection of extremely high numbers of client devices using a particular allowlisted AP,*
y. *Detection of a high number of failed attempts to join the WLAN in a short period of time,*
z. *Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic, such as Probes, Auths, and Assoc frames,*
aa. *Detection of the physical location of an identified WLAN threat by using triangulation,*
ab. *Detection of an SSID using weak/unsupported/disallowed encryption options,*
ac. *Detection of AP SSID larger than 32 bytes,*
ad. *[**assignment**: any other rules].*

]

Application Note: These rules are used to detect a potential security violation. A malicious actor who has gained unauthorized access to the TSF possesses the ability to alter its configuration and overall security posture. Maintenance of the rules by adding, modifying or deletion of rules from the set of rules is handled by FMT_SMF.1/WIDS. There is no expectation that the TOE classify or categorize audit records related to TSF configuration changes as malicious activity. If a potential security violation is detected the alert generated for the Administrator is handled by FAU_ARP.1.

Evaluation Activities

FAU_SAA.1

TSS

The evaluator shall verify that the TSS describes the ability of the TOE to detect the network behavior described by the SFR. The evaluator shall verify that the TSS describes the methods that the TOE uses to detect the presence of unauthorized connections and unauthorized network traffic. The evaluator shall examine the TSS to verify that it describes the denial of service attacks that can be detected by the TOE. The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized WLAN authentication schemes and encryption schemes are used. The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized APs and EUDs send or receive unencrypted data.

Guidance

If the ability of the TSF to detect the different potential security violations is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure the TOE. The TSF

should generate an alert or audit event for all potential violations contained within rule set forth in FAU_SAA.1.

Tests

- *Test FAU_SAA.1:1:* ***Detection of non-allowlisted AP****:*
  - ***Step 1:*** *Deploy a non-allowlisted AP.*
  - ***Step 2:*** *Verify that the AP is detected as a non-allowlisted AP.*

- *Test FAU_SAA.1:2:* ***Detection of non-allowlisted EUD****:*
  - ***Step 1:*** *Deploy a non-allowlisted EUD.*
  - ***Step 2:*** *Verify that the EUD is detected as an non-allowlisted EUD.*

- *Test FAU_SAA.1:3:* ***Detection of authorized EUD establishing peer-to-peer connection with any other EUD****:*
  - *Test FAU_SAA.1:3.1: Create the following connections between two allowlisted EUDs.*
    - *Windows ad hoc*
    - *Mac OS ad hoc*
    - *Linux ad hoc*
    - *Wi-Fi Direct*
  - *Test FAU_SAA.1:3.2: Create the following connections between one allowlisted EUD and a non-allowlisted EUD*
    - *Windows ad hoc*
    - *Mac OS ad hoc*
    - *Linux ad hoc*
    - *Wi-Fi Direct*

  Verify that alerts were generated by each of the connections in each test.
- *Test FAU_SAA.1:4:* ***Detection of EUD bridging two network interfaces****:*
  Bridge two network interfaces on an allowlisted EUD (one must be the wireless card listed as allowlisted).
  - ***Step 1:*** *Create a Windows Hosted Network with an allowlisted EUD.*
  - ***Step 2:*** *Connect a different allowlisted EUD to the network.*

  Verify that alerts were generated by each of the connections in each test.
- *Test FAU_SAA.1:5:* ***Detection of unauthorized point to point wireless bridges by allowlisted APs****:*
  - ***Step 1:*** *Setup a point-to-point wireless bridge using allowlisted APs in the range of the wireless sensors.*
  - ***Step 2:*** *Verify that the TSF detects the bridge.*

- *Test FAU_SAA.1:6:* ***Alert generated by violation of user defined signature****:*
  - ***Step 1:*** *Setup a user defined detection signature.*
  - ***Step 2:*** *Verify that the TSF generates an alert once the rules of signature have been violated.*

- *Test FAU_SAA.1:7:* ***Detection of ICS connection****:*
  - ***Step 1:*** *Setup an Internet Connection Sharing (ICS) connection.*
  - ***Step 2:*** *Verify that the TSF detects the establishment of the ICS connection.*

- *Test FAU_SAA.1:8:* ***Detection of MAC spoofing****:*
  - *Test FAU_SAA.1:8.1:*
    - ***Step 1:*** *Spoof mac address of an allowlisted EUD connected to an allowlisted AP on a second EUD.*

        - ***Step 2:*** *Connect EUD with spoofed MAC address to another allowlisted AP while the valid EUD it is spoofing is connected to the first AP.*
        - ***Step 3:*** *Verify that the TSF detected the MAC spoofing.*
    - *Test FAU_SAA.1:8.2:*
        - ***Step 1:*** *Spoof mac address of an allowlisted AP on a second AP.*
        - ***Step 2:*** *Verify that the TSF detected the MAC spoofing.*

- *Test FAU_SAA.1:9:* ***Detection of unauthorized AP broadcasting authorized SSIDs****:*
    - ***Step 1:*** *Configure a non-allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an authorized SSID.*
    - ***Step 2:*** *Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID.*
    - ***Step 3:*** *Repeat the test utilizing the 5 GHz band.*
    - ***Step 4:*** *Repeat the test utilizing the 6 GHz band.*

- *Test FAU_SAA.1:10:* ***Detection of authorized AP broadcasting an unauthorized SSID****:*
    - ***Step 1:*** *Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an unauthorized SSID.*
    - ***Step 2:*** *Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID.*
    - ***Step 3:*** *Repeat the test utilizing the 5 GHz band.*
    - ***Step 4:*** *Repeat the test utilizing the 6 GHz band.*

- *Test FAU_SAA.1:11:* ***Detection of allowlisted EUD connected to unauthorized SSID****:*
    - ***Step 1:*** *Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band with an unauthorized SSID.*
    - ***Step 2:*** *Connect an allowlisted EUD to the AP.*
    - ***Step 3:*** *Verify that the TSF detects the allowlisted EUD associated to the allowlisted AP broadcasting an unauthorized SSID.*
    - ***Step 4:*** *Repeat the test utilizing the 5 GHz band.*
    - ***Step 5:*** *Repeat the test utilizing the 6 GHz band.*

- *Test FAU_SAA.1:12:* ***Detection of NULL SSID associations****:*
    - ***Step 1:*** *Deploy allowlisted AP.*
    - ***Step 2:*** *Configure the AP to have null SSID.*
    - ***Step 3:*** *Attempt to connect an allowlisted EUD to the AP without supplying the correct AP SSID.*
    - ***Step 4:*** *Verify that the AP does not permit the EUD to complete an association by returning a Probe Request.*
    - ***Step 5:*** *If an association does occur, confirm that an alert is triggered due to a violation of policy.*

- *Test FAU_SAA.1:13:* ***Detection of active probing****:*
    - ***Step 1:*** *Perform an active scan on the subnet of the WLAN.*
    - ***Step 2:*** *Record tools used and type of scan performed.*
    - ***Step 3:*** *Verify that the TSF detects the active probing.*

- *Test FAU_SAA.1:14:* ***Detection of packet flooding/DoS/DDoS****:*
    - ***Step 1:*** *Generate a large amount of TCP and UDP traffic from a single EUD.*
    - ***Step 2:*** *Verify that the TSF detects the network-based DoS.*
    - ***Step 3:*** *Generate a large amount of TCP and UDP traffic from multiple EUDs.*
    - ***Step 4:*** *Verify that the TSF detects the network-based DDoS.*

- *Test FAU_SAA.1:15:* ***Detection of RF-based denial of service****:*

- ***Step 1:*** *Deploy an allowlisted AP and configure to stay in a particular channel.*
- ***Step 2:*** *Connect an allowlisted EUD to the AP.*
- ***Step 3:*** *Use an RF Jammer or signal generator on the same frequency as the AP and EUD to create a RF-based DoS.*
- ***Step 4:*** *Verify that the TOE detects the RF-based DoS.*

- *Test FAU_SAA.1:16:* ***Detection of deauthentication flooding****:*
  - *Test FAU_SAA.1:16.1:*
    - ***Step 1:*** *Deploy allowlisted AP and configure to a set channel.*
    - ***Step 2:*** *Connect an allowlisted EUD to the AP.*
    - ***Step 3:*** *Send an flood of deauthentication frames to the EUD using the MAC address of allowlisted AP it is connected to.*
    - ***Step 4:*** *Verify that the TSF detects the deauthentication flood.*
  - *Test FAU_SAA.1:16.2:*
    - ***Step 1:*** *Deploy allowlisted AP and configure to a set channel.*
    - ***Step 2:*** *Connect an allowlisted EUD to the AP.*
    - ***Step 3:*** *Send an flood of deauthentication frames with the MAC address of allowlisted AP as the source and destination as a broadcast.*
    - ***Step 4:*** *Verify that the TSF detects the deauthentication flood.*

- *Test FAU_SAA.1:17:* ***Detection of disassociation flooding****:*
  - ***Step 1:*** *Deploy an allowlisted AP and connect authorized EUDs.*
  - ***Step 2:*** *Generate disassociation frames from an unauthorized EUD.*
  - ***Step 3:*** *Verify that the TSF detected the disassociation flooding.*

- *Test FAU_SAA.1:18:* ***Detection of request-to-send/clear-to-send abuse****:*
  - ***Step 1:*** *Deploy allowlisted AP and configure to a set channel.*
  - ***Step 2:*** *Connect two allowlisted EUDs to the AP.*
  - ***Step 3:*** *Send an flood of CTS frames to reserve RF medium.*
  - ***Step 4:*** *Verify that the TSF detects the CTS abuse.*

- *Test FAU_SAA.1:19:* ***Detection of unauthorized authentication scheme use****:*
  The evaluator shall configure the TOE, per FMT_SMF.1/WIDS, with 802.1x authentication as the only mode of authorized WLAN authentication scheme.
  - *Test FAU_SAA.1:19.1:*
    - ***Step 1:*** *Deploy an allowlisted AP with open authentication.*
    - ***Step 2:*** *Verify that the TSF detects the AP broadcasting an unauthorized authentication scheme. If detected the test is satisfied. If not detected perform steps 3 and 4.*
    - ***Step 3:*** *Connect an allowlisted EUD to AP.*
    - ***Step 4:*** *Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.*
  - *Test FAU_SAA.1:19.2:*
    - ***Step 1:*** *Deploy an allowlisted AP that uses pre-shared key authentication.*
    - ***Step 2:*** *Verify that the TSF detects the AP broadcasting an unauthorized authentication scheme. If detected the test is satisfied. If not detected perform steps 3 and 4.*
    - ***Step 3:*** *Connect an allowlisted EUD to AP.*
    - ***Step 4:*** *Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.*

- *Test FAU_SAA.1:20:* ***Detection of unauthorized encryption scheme use****:*
  - *Test FAU_SAA.1:20.1:*
    - ***Step 1:*** *Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.*
    - ***Step 2:*** *Deploy an allowlisted AP with no encryption.*
    - ***Step 3:*** *Connect an allowlisted EUD to AP.*
    - ***Step 4:*** *Verify that the TOE detects the AP and the EUD using unauthorized encryption schemes.*
  - *Test FAU_SAA.1:20.2:*
    - ***Step 1:*** *Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.*
    - ***Step 2:*** *Deploy an allowlisted AP that uses TKIP encryption only.*
    - ***Step 3:*** *Connect an allowlisted EUD to AP.*
    - ***Step 4:*** *Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.*

- *Test FAU_SAA.1:21:* ***Detection of unencrypted traffic****:*
  - *Test FAU_SAA.1:21.1:*
    - ***Step 1:*** *Deploy an allowlisted AP with no encryption.*
    - ***Step 2:*** *Connect an allowlisted EUD to AP and generate traffic.*
    - ***Step 3:*** *Verify that the TOE detects unencrypted data frames being sent between the allowlisted AP and EUD.*
    - ***Step 4:*** *Attempt to connect a non-allowlisted EUD to AP.*
    - ***Step 5:*** *If the connection attempt succeeds, generate traffic from the non-allowlisted EUD and verify that the TSF detects unencrypted data frames being sent between the allowlisted AP and non-allowlisted EUD.*
  - *Test FAU_SAA.1:21.2:*
    - ***Step 1:*** *Deploy a non-allowlisted AP with no encryption.*
    - ***Step 2:*** *Connect an allowlisted EUD to AP and generate traffic.*
    - ***Step 3:*** *Verify that the TSF detects unencrypted data frames being between the non-allowlisted AP and allowlisted EUD.*

- *Test FAU_SAA.1:22:* ***Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations****:*
  - ***Step 1:*** *Deploy an allowlisted AP that utilizes the 802.11g or older WLAN protocol.*
  - ***Step 2:*** *Verify that the TSF detects the weak/outdated WLAN protocol and generates an alert.*

- *Test FAU_SAA.1:23:* ***Detection of extremely high numbers of client devices using a particular allowlisted AP****:*
  - ***Step 1:*** *Deploy an allowlisted AP.*
  - ***Step 2:*** *Configure a threshold amount of client devices that can use a particular AP.*
  - ***Step 3:*** *Connect enough client devices to the AP to purposely exceed the defined threshold.*
  - ***Step 4:*** *Verify that the TSF detects when the client usage exceeds the threshold.*

- *Test FAU_SAA.1:24:* ***Detection of a high number of failed attempts to join the WLAN in a short period of time****:*
  - ***Step 1:*** *Deploy an allowlisted AP.*
  - ***Step 2:*** *Configure a threshold amount of connection attempts that can occur in a particular timeframe.*

- ***Step 3:*** *Attempt to authenticate to the AP with enough client devices to purposely exceed the defined threshold.*
- ***Step 4:*** *Verify that the TSF detects when the connection attempts within the specific timeframe exceeds the threshold.*

- *Test FAU_SAA.1:25:* ***Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic****:*
  - ***Step 1:*** *Deploy an allowlisted AP.*
  - ***Step 2:*** *Verify that the TSF detects when WLAN scanners are the source of WLAN traffic.*

- *Test FAU_SAA.1:26:* ***Detection of the physical location of an identified WLAN threat by using triangulation****:*
  - ***Step 1:*** *Deploy a non-allowlisted AP or EUD within range of the TSF.*
  - ***Step 2:*** *Verify that the TSF can track and locate the AP or EUD to within 25 feet.*

- *Test FAU_SAA.1:27:* ***Detection of an SSID using weak/unsupported/disallowed encryption options****:*
  - ***Step 1:*** *Deploy an allowlisted AP and configure its encryption options.*
  - ***Step 2:*** *Change the encryption options the AP advertises.*
  - ***Step 3:*** *Verify that the TSF detects when the AP's encryption options change.*

- *Test FAU_SAA.1:28:* ***Detection of AP SSID larger than 32 bytes****:*
  - ***Step 1:*** *Deploy an allowlisted AP and configure its SSID to be larger than 32 bytes.*
  - ***Step 2:*** *Configure a user defined signature on the WIDS to detect when an SSID is larger than 32 bytes.*
  - ***Step 3:*** *Verify that the TSF detects when the AP's SSID is larger than 32 bytes.*

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 non-allowlisted AP/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 the TOE 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 given SSID is authorized.

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

Evaluation Activities

FAU_WID_EXT.1

TSS

The evaluator shall verify that the TSS describes how the TOE detects malicious APs/EUDs and whether the TOE supports automatic detection. The evaluator shall verify that the TSS includes how the TOE determines if a given SSID is authorized.

Guidance

If TOE supports automatic detection, the evaluator shall verify that the operational guidance contains instructions for configuring the automatic detection metrics. The evaluator shall verify that the operational guidance provides instructions on how to configure SSIDs as authorized.

Tests

For test 1 and 2 below the evaluator shall verify that the TOE detects and appropriately classifies the APs and EUDs. It is acceptable if the TOE uses different but equivalent descriptors for the classification. If the TOE does not support automatic detection metrics and equates a non-allowlisted AP/EUD as malicious, than it is sufficient that the classification given to the AP/EUD in step 1 is the same as in step 2. If the TOE supports automatic detection metrics and distinguishes between a non-allowlisted AP/EUD and a malicious AP/EUD, then the classification for the AP/EUD should differ between step 1 and step 2.

- *Test FAU_WID_EXT.1:1:*
  - ***Step 1:** Deploy a non-allowlisted AP in the area of the WIDS sensor, but take no action against the network. Verify that the AP is classified as non-authorized.*
  - ***Step 2:** Deploy a non-allowlisted AP in the area of the WIDS sensor and launch an attack against the network. This can be any variation of Fake AP, Spoof AP, Flood or DoS attack.*
  - ***Step 3:** Verify that the AP is classified as malicious.*
- *Test FAU_WID_EXT.1:2:*
  - ***Step 1:** Deploy a non-allowlisted EUD in the area of the WIDS sensor, but take no action against the network. Verify that the EUD is classified as non-authorized.*
  - ***Step 2:** Launch an RF Flooding, DoS/DDoS, masqueraded or spoofing attack against authorized AP with an unauthorized EUD.*
  - ***Step 3:** Verify that the EUD is classified as malicious.*
- *Test FAU_WID_EXT.1:3:*
  - ***Step 1:** Deploy an AP with an unauthorized SSID in the area of the WIDS sensor.*
  - ***Step 2:** Verify that the TOE detects the unauthorized SSID.*

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**:*

- *6.0 GHz*
- *[**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/RF 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/RF 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.

Evaluation Activities

FAU_WID_EXT.2
TSS
The evaluator shall verify that the TSS includes which channels the TOE can detect and monitor. Additionally, the TSS shall include whether the TOE simultaneously or nonsimultaneously monitors network traffic across these channels. The evaluator shall verify that the TSS includes information on if the sensors are completely passive, by default, or if the sensors ability to transmit data is configurable.

Guidance
The evaluator shall review the operational guidance for how to configure the TOE to monitor the channels as selected in the SFR. If the sensor ability to transmits data is configurable, the evaluator shall review the operational guidance for how to disable wireless transmissions from the sensor. The

evaluator shall verify that the operational guidance provides instructions on how to specify and confirm that stateful frame capture and inspection is being performed.

Tests
Channels Monitored

- *Test FAU_WID_EXT.2:1: Channels on On 5 GHz band*
  - ***Step 1:*** *Configure the TSF to monitor the channels as selected in the SFR.*
  - ***Step 2:*** *Deploy an AP on at least 2 different channels within the regulatory domain on 5 GHz band.*
  - ***Step 3:*** *Verify that the AP gets detected on each channel tested.*
- *Test FAU_WID_EXT.2:2: Channels on 2.4 GHz band*
  - ***Step 1:*** *Configure the TSF to monitor the channels as selected in the SFR.*
  - ***Step 2:*** *Deploy AP on at least 2 different channels within the regulatory domain on 2.4 GHz band.*
  - ***Step 3:*** *Verify that the AP gets detected on each channel tested.*
- *Test FAU_WID_EXT.2:3: Channels on 4.9 GHz band (if selected)*
  - ***Step 1:*** *Configure the TSF to monitor the channels specified in the SFR.*
  - ***Step 2:*** *Deploy AP and set to channels within the 4.9 GHz band outlined in the TSS.*
  - ***Step 3:*** *Verify that the AP gets detected on each channel tested.*
- *Test FAU_WID_EXT.2:4: Channels on 6 GHz band (if selected)*
  - ***Step 1:*** *Configure the TSF to monitor the channels specified in the SFR.*
  - ***Step 2:*** *Deploy AP and set to channels within the 6 GHz band outlined in the TSS.*
  - ***Step 3:*** *Verify that the AP gets detected on each channel tested.*
- *Test FAU_WID_EXT.2:5: Non-standard channel frequencies (if selected)*
  - ***Step 1:*** *Configure the TSF to monitor the channels as selected in the SFR.*
  - ***Step 2:*** *Deploy AP on at least 2 different channels on non-standard channel frequencies.*
  - ***Step 3:*** *Verify that the AP gets detected on each channel tested.*
- *Test FAU_WID_EXT.2:6: Channels outside regulatory domain (if selected)*
  - ***Step 1:*** *Configure the TSF to monitor the channels as selected in the SFR.*
  - ***Step 2:*** *Deploy an AP on at least 2 different channels outside the regulatory domain on 5GHz band.*
  - ***Step 3:*** *Deploy AP on at least 2 different channels outside the regulatory domain on 2.4GHz band.*
  - ***Step 4:*** *Verify that the AP gets detected on each channel tested.*

Wireless Sensor Transmission of Data

If the TOE provides the ability to disable wireless transmission, the evaluator shall follow the operational guidance to configure the sensor to not transmit wirelessly. The evaluator shall then deploy a signal analyzer in order to check for wireless emanations from the TOE.
Repeat the two tests below, for both the 2.4 GHz, 5 GHz, and 6 GHz band.

- *Test FAU_WID_EXT.2:7:*
  - ***Step 1:*** *Boot a sensor and using the signal analyzer observe to check if any emanations are coming from the sensor.*
  - ***Step 2:*** *Verify that the signal analyzer does not pick up emanations from the sensor.*
- *Test FAU_WID_EXT.2:8:*
  - ***Step 1:*** *During normal sensor operations, observe the analyzer for about 10 minutes to check if any emanations are coming from the sensor.*
  - ***Step 2:*** *Verify that the signal analyzer does not pick up emanations from the sensor.*

Stateful Frame Inspection

- *Test FAU_WID_EXT.2:9:*

- ***Step 1:*** *Deploy allowlisted AP.*
- ***Step 2:*** *Connect an allowlisted EUD to the AP.*
- ***Step 3:*** *Deploy a protocol analyzer or native capability within the WIDS Controller between the AP and EUD.*
- ***Step 4:*** *Verify from the network traffic packet capture that all frames are being inspected to validate their connection state from the TSF*

5.2.3 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/RF and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

Evaluation Activities

FDP_IFC.1
TSS
There are no TSS evaluation activities for this SFR.

Guidance
If this functionality is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure the TOE to monitor different types of IEEE 802.11 frame types and subtypes.

Tests

- *Test FDP_IFC.1:1:*
  - *Deploy an allowlisted AP/WIDS*
  - *Start a traffic capture from the AP/WIDS sensor*
  - *Send a set number of frames to the sensor for all IEEE 802.11 a, b, g, n, ac frame types and subtypes from/to the following:*
    - *authorized APs and authorized EUDs*
    - *authorized APs and unauthorized EUDs*
    - *unauthorized APs and authorized EUDs*
  - *Verify that there are frames from all the types and subtypes in the capture.*

5.2.4 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 frequency*
  - *Define the amount of time sensor monitors a specific 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.

Evaluation Activities

FMT_SMF.1/WIDS
TSS
The evaluator shall review the TSS to verify that it includes information on the ability of the TOE to define inventory of authorized APs and EUDs.

The evaluator shall verify that the TSS describes the ability of the TOE to allow authorized administrators to define authorized WLAN authentication schemes.

Guidance

The evaluator shall review the operational guidance for instructions on how to configure and change classification of APs and EUDs to indicate that they are part of the allowlist.

The evaluator shall review the operational guidance to determine how to configure which SSIDs are permitted on the network.

The evaluator shall examine the operational guidance to verify that it provides instructions on how to define a WLAN authentication scheme as authorized or unauthorized for the purposes of detection.

The evaluator shall examine the operational guidance to verify that it provides instructions on how to define a WLAN encryption scheme as authorized or unauthorized for the purposes of detection.

Tests

- *Test FMT_SMF.1/WIDS:1: The evaluator shall define an inventory of authorized APs and EUDs. The ability to detect allowlisted and non-allowlisted APs and EUDs will be tested in FAU_INV_EXT.1 and FAU_SAA.1.*
- *Test FMT_SMF.1/WIDS:2: The evaluator shall define authorized SSIDs. The ability to detect authorized and unauthorized SSIDs will be tested in FAU_WID_EXT.2.3 and FAU_SAA.1.*
- *Test FMT_SMF.1/WIDS:3: The evaluator shall configure the TSF with a set of allowed authentication and encryption schemes. The ability to detect violation of this policy will be tested in FAU_SAA.1.*
- *Test FMT_SMF.1/WIDS:4: (conditional): If "Define the amount of time sensor monitors a specific frequency or channel" is selected:*
  - ***Step 1:** Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire.*
  - ***Step 2:** Confirm that the TSF can observe and capture traffic and events generated by the AP.*
  - ***Step 3:** Verify that the TSF can be configured to capture traffic on each of the selected channel(s) for the specified interval of time.*
  - ***Step 4:** Confirm that the TSF remains on the frequency and channel for the time period specified.*

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 3: SFR Rationale

Threat	Addressed by	Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	FAU_GEN_EXT.1 (from Base-PP)	Mitigates the threat by generating audit data on each component of the TOE.
	FAU_STG_EXT.1 (from Base-PP)	Mitigates the threat by storing audit data in specified locations and optionally forwarding this data to a central point.

FCO_CPC_EXT.1 (from Base-PP)	Mitigates the threat by securely registering components to the TOE.
FAU_ARP.1	Mitigates the threat by generating alerts for potential violations of security policy.
FAU_ARP_EXT.1	Mitigates the threat by allowing for nuisance or undesirable alarms from generation, preventing alarm fatigue.
FAU_GEN.1/WIDS	Mitigates the threat by generating audit data related to operation, including abnormal conditions and potential threat detections.
FAU_IDS_EXT.1	Mitigates the threat by detecting intrusions or potential intrusions.
FAU_INV_EXT.1	Mitigates the threat by defining an allowlist of authorized equipment for use in the network.
FAU_INV_EXT.2	Mitigates the threat by detecting all wireless devices present in the vicinity.
FAU_INV_EXT.3	Mitigates the threat by determining the physical location of wireless devices in the vicinity.
FAU_RPT_EXT.1	Mitigates the threat by transmitting audit data to a central location.
FAU_SAA.1	Mitigates the threat by defining rules that indicate a potential malicious action.
FAU_WID_EXT.1	Mitigates the threat by classifying wireless devices as benign or malicious based on device metrics.
FAU_WID_EXT.2	Mitigates the threat by monitoring 802.11 wireless traffic in the vicinity.
FDP_IFC.1	Mitigates the threat by enforcing monitoring on all wireless 802.11 traffic that involves an authorized device as at least one party.
FMT_SMF.1/WIDS	Mitigates the threat by allowing configuration of rules, configuration, and other TOE operational settings.
FPT_FLS.1/WIDS (objective)	Mitigates the threat by at minimum generating an audit record when potential security failures of the TSF are detected, which could include failures to properly monitor or alert to potential threats.
FTP_ITC.1 (from Base-PP)	Mitigates the threat by securely transmitting data from the TOE to other trusted entities.
FPT_ITT.1 (from Base-PP)	Mitigates the threat by securely transmitting data between TOE components.

	FAU_WID_EXT.3/BT (optional)	Mitigates the threat by monitoring Bluetooth wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.3/CELL (optional)	Mitigates the threat by monitoring cellular wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.3/RF (optional)	Mitigates the threat by monitoring non-802.11 wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.4 (optional)	Mitigates the threat by using a dedicated sensor for analysis of wireless traffic.
	FAU_INV_EXT.4 (objective)	Mitigates the threat by detecting non-authorized wireless equipment being attached to an internal wired network.
	FAU_INV_EXT.5 (objective)	Mitigates the threat by including a signal library.
	FAU_MAC_EXT.1 (objective)	Mitigates the threat by detecting when a device is attempting to spoof a trusted device's MAC address.
	FAU_WIP_EXT.1 (objective)	Mitigates the threat by isolating confirmed threats to the internal network, either wired (unauthorized AP) or wireless.
	FAU_ANO_EXT.1 (selection-based)	Mitigates the threat by defining thresholds of baseline and anomalous traffic for analysis and action.
	FAU_SIG_EXT.1 (selection-based)	Mitigates the threat by defining signatures for an attack.
	FAU_STG.1/PCAP (selection-based)	Mitigates the threat by storing packet captures generated by the TOE, and optionally forwarding this data to a central point.
	FAU_STG.5/PCAP (selection-based)	Mitigates the threat by defining how storage of packet capture data is prioritized in the case of limited storage space.
T.UNAUTHORIZED_ ACCESS	FAU_IDS_EXT.1	Mitigates the threat by detecting intrusions or potential intrusions.
	FAU_INV_EXT.1	Mitigates the threat by defining an allowlist of authorized equipment for use in the network.
	FAU_INV_EXT.2	Mitigates the threat by detecting all wireless devices present in the vicinity, to use against the allowlist for detection of potentially unauthorized access points or end-user devices.
	FAU_INV_EXT.3	Mitigates the threat by determining the physical location of wireless devices in the vicinity, to allow

	for locating any potentially rogue devices.
FAU_SAA.1	Mitigates the threat by defining rules that indicate a potential malicious action.
FAU_WID_EXT.1	Mitigates the threat by classifying wireless devices as benign or malicious based on device metrics.
FAU_WID_EXT.2	Mitigates the threat by monitoring 802.11 wireless traffic in the vicinity for comparison against defined policies.
FDP_IFC.1	Mitigates the threat by enforcing monitoring on all wireless 802.11 traffic that involves an authorized device as at least one party.
FMT_SMF.1/WIDS	Mitigates the threat by allowing configuration of rules, configuration, and other TOE operational settings.
FAU_WID_EXT.3/RF (optional)	Mitigates the threat by monitoring non-802.11 wireless traffic in the vicinity for potential violations of policy.
FAU_WID_EXT.3/BT (optional)	Mitigates the threat by monitoring Bluetooth wireless traffic in the vicinity for potential violations of policy.
FAU_WID_EXT.3/CELL (optional)	Mitigates the threat by monitoring cellular wireless traffic in the vicinity for potential violations of policy.
FAU_WID_EXT.4 (optional)	Mitigates the threat by using a dedicated sensor for analysis of wireless traffic.
FAU_INV_EXT.4 (objective)	Mitigates the threat by detecting non-authorized wireless equipment being attached to an internal wired network.
FAU_INV_EXT.5 (objective)	Mitigates the threat by including a signal library.
FAU_MAC_EXT.1 (objective)	Mitigates the threat by detecting when a device is attempting to spoof a trusted device's MAC address.
FAU_WIP_EXT.1 (objective)	Mitigates the threat by isolating confirmed threats to the internal network, either wired (unauthorized AP) or wireless.
FAU_ANO_EXT.1 (selection-based)	Mitigates the threat by defining thresholds of baseline and anomalous traffic for analysis and action.
FAU_SIG_EXT.1 (selection-based)	Mitigates the threat by defining signatures for an attack.

T.DISRUPTION	FAU_IDS_EXT.1	Mitigates the threat by detecting intrusions or potential intrusions.
	FAU_INV_EXT.1	Mitigates the threat by defining an allowlist of authorized equipment for use in the network.
	FAU_INV_EXT.2	Mitigates the threat by detecting all wireless devices present in the vicinity, to use against the allowlist for detection of potentially unauthorized access points or end-user devices.
	FAU_INV_EXT.3	Mitigates the threat by determining the physical location of wireless devices in the vicinity, to allow for locating any potentially rogue devices.
	FAU_SAA.1	Mitigates the threat by defining rules that indicate a potential malicious action, including signs of a DoS attack.
	FAU_WID_EXT.1	Mitigates the threat by classifying wireless devices as benign or malicious based on device metrics, including throughput (which may indicate a DoS threat).
	FAU_WID_EXT.2	Mitigates the threat by monitoring 802.11 wireless traffic in the vicinity for comparison against defined policies.
	FAU_WIP_EXT.1	Mitigates the threat by isolating confirmed threats to the internal network, either wired (unauthorized AP) or wireless.
	FDP_IFC.1	Mitigates the threat by enforcing monitoring on all wireless 802.11 traffic types that involve an authorized device as at least one party.
	FMT_SMF.1/WIDS	Mitigates the threat by allowing configuration of rules, configuration, and other TOE operational settings.
	FAU_WID_EXT.3/BT (optional)	Mitigates the threat by monitoring Bluetooth wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.3/CELL (optional)	Mitigates the threat by monitoring cellular wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.3/RF (optional)	Mitigates the threat by monitoring non-802.11 wireless traffic in the vicinity for potential violations of policy.
	FAU_WID_EXT.4 (optional)	Mitigates the threat by using a dedicated sensor for analysis of wireless traffic.
	FAU_INV_EXT.4 (objective)	Mitigates the threat by detecting non-authorized wireless equipment being attached to an internal

	wired network.
FAU_INV_EXT.5 (objective)	Mitigates the threat by including a signal library.
FAU_MAC_EXT.1 (objective)	Mitigates the threat by detecting when a device is attempting to spoof a trusted device's MAC address.
FAU_ANO_EXT.1 (selection-based)	Mitigates the threat by defining thresholds of baseline and anomalous traffic for analysis and action.
FAU_SIG_EXT.1 (selection-based)	Mitigates the threat by defining signatures for an attack.

6 Consistency Rationale

6.1 Collaborative Protection Profile for Network Device

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

Table 4: Consistency of Security Problem Definition (NDcPP base)

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 does not 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 OE Objectives

Table 5: Consistency of OE Objectives (NDcPP base)

PP-Module OE 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 System functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 6: Consistency of Requirements (NDcPP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_GEN_EXT.1	This PP-Module mandates the inclusion of this selection-based SFR because a TOE that conforms to this PP-Module will always be deployed in a configuration that requires this SFR 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 optional SFR because it is required to implement functionality required by this PP-Module.
FPT_ITT.1	This PP-Module mandates the inclusion of this optional SFR 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.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
FAU_ARP.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_ARP_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_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 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_INV_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_INV_EXT.2	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.3	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_RPT_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_SAA.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_WID_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_WID_EXT.2	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.
FDP_IFC.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.
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/BT	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_WID_EXT.3/CELL	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_WID_EXT.3/RF	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_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.
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/WIDS	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.
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent requirements.	
Selection-based SFRs	
FAU_ANO_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_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.1/PCAP	This SFR iterates the FAU_STG.1 SFR defined in CC Part 2 for storage of audit data and applies it to storage of packet captures.
FAU_STG.5/PCAP	This SFR iterates the FAU_STG.5 SFR defined in CC Part 2 for storage of audit data and applies it to storage of packet captures.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 Auditable Events for Optional SFRs

Table 7: Auditable Events for Strictly Optional Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_WID_EXT.3/BT	Detection of Bluetooth devices (for each selection made that includes an action of "log")	• MAC address or other unique device identifier. • Information contained within each selection that contains a requirement to log information.
FAU_WID_EXT.3/CELL	Detection of cellular devices (for each selection made that includes an action of "log")	• MAC address or other unique device identifier • Information contained within each selection that contains a requirement to log information.
FAU_WID_EXT.3/RF	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	No events specified	N/A

A.1.2 Security Audit (FAU)

FAU_WID_EXT.3/BT Wireless Intrusion Detection - Spectrum Monitoring (Bluetooth)

FAU_WID_EXT.3.1/BT

The TSF shall detect the presence of devices [*that operate a specified protocol and take a specified action: [**selection**:*

- *Detect and log the presence of 2.4 GHz Bluetooth BR/EDR devices operating within a controlled space*
- *Detect and log the presence of Bluetooth Low Energy (BLE) devices operating within a controlled space*
- *Detect and log the Bluetooth BR/EDR devices LAP and half the Bluetooth MAC address within a controlled space*
- *Detect and log the BLE device's Bluetooth MAC address within a controlled space*
- *Geo-locate Bluetooth BR/EDR devices within 25 feet of their actual location*
- *Geo-locate BLE devices within 25 feet of their actual location*

- *Detect and log Bluetooth BR/EDR devices conducting the Inquiry Procedure within a controlled space*
- *Detect and log Bluetooth BR/EDR devices responding to the Inquiry Procedure within the controlled space*
- *Capture and log any device information transmitted during the Bluetooth BR/EDR Inquiry Procedure when occurring within a controlled space*
- *Detect and log BLE devices advertisements on the Advertisement channels*
- *Detect and log BLE devices exchanging information or data on the Advertisement channels*
- *Detect and log Bluetooth BR/EDR devices using the SDP procedure*
- *Capture and log any device information exchanged during the Bluetooth BR/EDR SDP procedure*
- *Detect and log any Bluetooth BR/EDR devices performing the Paging Procedure*
- *Detect and log any BLE device performing the Paging Procedure*
- *Detect and log the piconet membership of any Bluetooth BR/EDR device. This includes role in the piconet (Central or Peripheral), piconet ID, device ID, and number of piconets which they are members of*
- *Detect and log the piconet membership of any Low Energy (LE) device. This includes role in the piconet (Central or Peripheral), piconet ID, device ID, and number of piconets which they are members of*
- *Use Bluetooth BR/EDR Inquiry Procedure to detect Bluetooth BR/EDR devices in discoverable mode within a controlled area*
- *Use Bluetooth BR/EDR SDP procedure to gather information about Bluetooth BR/EDR devices within a controlled area*
- *Use BLE SDP procedure to gather information about BLE devices within a controlled area*

]].

Application Note: This SFR refers to Bluetooth and Bluetooth Low-Energy (BLE) (IEEE 802.15) 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 integration.

Evaluation Activities

FAU_WID_EXT.3/BT

TSS

The evaluator shall verify that the TSS includes the set of RF bands and technologies that the TSF can detect the use of. The TSS should also include instructions on how to enable and the hardware that is necessary for the additional band detection.

Guidance

The evaluator shall verify that the operational guidance describes how to enable and configure detection of the technologies included in the ST as well as the hardware that is needed to perform this function.

Tests

The evaluator shall enable and configure detection of the selected technologies.

- *Test FAU_WID_EXT.3/BT:1: Deploy a device within the given technology and verify that the TSF detects the device.*

FAU_WID_EXT.3/CELL Wireless Intrusion Detection - Spectrum Monitoring (Cellular)

FAU_WID_EXT.3.1/CELL

The TSF shall detect the presence of devices [*that operate a specified protocol and take a specified action: [**selection**:*

- *Detect and log the presence of cellular 3G devices operating within a controlled space*
- *Detect and log the presence of cellular 4G/LTE devices operating within a controlled space*
- *Detect and log the presence of cellular 5G low and mid-band devices operating within a controlled space*
- *Detect and identify base stations which had clients within the area monitored by the WIDS*
- *Capture temporary identifiers (e.g. TMSI) of cellular devices within a controlled space*
- *Detect and identify which cellular technology (such as 3G, LTE, UTMS, 5G, etc.) the cellular device is using within a controlled space*
- *Detect and identify which cellular carrier a cellular device is using within a controlled space*
- *Detect and identify which base station a cellular device is connected to while operating within a controlled space*
- *Detect and identify whether a cellular device is using a cellular uplink or downlink operating within a controlled space*
- *Geo-locate cellular devices operating within the operation area of the WIDS*

]].

Application Note: This SFR refers to Bluetooth and Bluetooth Low-Energy (BLE) (IEEE 802.15) 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 integration.

Evaluation Activities

FAU_WID_EXT.3/CELL

TSS

The evaluator shall verify that the TSS includes the set of RF bands and technologies that the TSF can detect the use of. The TSS should also include instructions on how to enable and the hardware that is necessary for the additional band detection.

Guidance

The evaluator shall verify that the operational guidance describes how to enable and configure detection of the technologies included in the ST as well as the hardware that is needed to perform this function.

Tests

The evaluator shall enable and configure detection of the selected technologies.

- *Test FAU_WID_EXT.3/CELL:1: Deploy a device within the given technology and verify that the TSF detects the device.*

FAU_WID_EXT.3/RF Wireless Intrusion Detection - Spectrum Monitoring (Non-Wireless RF)

FAU_WID_EXT.3.1/RF

The TSF shall detect the presence of devices [*that operate in the following RF bands: [**selection**: 3.6 GHz, 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, y, ac, ad and ay) 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 integration.

Evaluation Activities

FAU_WID_EXT.3/RF

TSS

The evaluator shall verify that the TSS includes the set of RF bands and technologies that the TSF can detect the use of. The TSS should also include instructions on how to enable and the hardware that is necessary for the additional band detection.

Guidance

The evaluator shall verify that the operational guidance describes how to enable and configure detection of the technologies included in the ST as well as the hardware that is needed to perform this function.

Tests

The evaluator shall enable and configure detection of the selected technologies.

- *Test FAU_WID_EXT.3/RF:1: Deploy a device within the given technology and verify that the TSF detects the device.*

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.

Evaluation Activities

FAU_WID_EXT.4

TSS

The evaluator shall verify that the TSS to verify that the TOE provides a dedicated sensor for wireless spectrum analysis.

Guidance

The evaluator shall verify that the operational guidance describes how to enable and configure dedicated spectrum analysis as well as the hardware that is needed to perform this function.

Tests

The evaluator shall enable and configure dedicated spectrum analysis and test the capabilities listed in the TSS.

A.2 Objective Requirements

A.2.1 Auditable Events for Objective SFRs

Table 8: Auditable Events for Objective Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_INV_EXT.4	No events specified	N/A
FAU_INV_EXT.5	No events specified	N/A
FAU_MAC_EXT.1	No events specified	N/A
FAU_WIP_EXT.1	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)
FPT_FLS.1/WIDS	Information about failure	• Indication that there was a failure • Type of failure • Device that failed • Sensor connectivity and operating status • Time of failure

A.2.2 Security Audit (FAU)

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.

Evaluation Activities

FAU_INV_EXT.4

TSS

The evaluator shall verify that the TSS includes guidance on whether the TSF has the capability of detecting APs connecting to the protected wired network infrastructure. If the capability is present the TSS shall include configuration guidance for this feature.

Guidance

The evaluator shall review the operational guidance for instructions on how to configure the WIDS to detect unauthorized APs connected to the protected wired infrastructure.

Tests

- *Test FAU_INV_EXT.4:1:*
  - ***Step 1:*** *Deploy a non-allowlisted AP.*
  - ***Step 2:*** *Connect the AP via wire to the protected network infrastructure.*
  - ***Step 3:*** *Check the WIDS user interface for a list of detected APs and EUDs.*

- ***Step 4:*** *Verify that the rogue AP is detected and an alert generated on the detection of an AP connected to the protected wired infrastructure.*

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 existing signal library.

Evaluation Activities

FAU_INV_EXT.5
TSS
There are no TSS evaluation activities for this SFR.

Guidance
The evaluator shall review the operational guidance for instructions on how to locate and verify that the WIDS comes preloaded with a signal library, as well as possesses the ability to import, export, and update the existing signal library if present.

Tests
Depending on operation guidance provided for the TOE, the evaluator shall confirm and note the existence of the signal library, and test for the ability to import, export, and update the signal library.

- *Test FAU_INV_EXT.5:1:*
  - ***Step 1:*** *Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire.*
  - ***Step 2:*** *Confirm and note whether the TSF has an existing signal library.*
  - ***Step 3:*** *If existence is confirmed, verify that the TSF can import, export, and update the existing 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.

Evaluation Activities

FAU_MAC_EXT.1

TSS

The evaluator shall verify that the TSS describes the behavior of the TOE when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously.

Guidance

The evaluator shall verify that the operational guidance provides instructions on how to deploy the TOE in a manner that allows the TSF to detect when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously (i.e. information about the range and placement of sensors to ensure non-overlapping coverage).

The evaluator shall verify that the operational guidance provides instructions on how to configure the timeframe that should be allowed between two subsequent attempts for an EUD to connect from two separate locations.

Tests

- *Test FAU_MAC_EXT.1:1:*
  - ***Step 1:*** *Setup an allowlisted AP (Location 1).*
  - ***Step 2:*** *Connect an allowlisted EUD to AP.*
  - ***Step 3:*** *Setup a second allowlisted AP and a non-allowlisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-overlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).*
  - ***Step 4:*** *Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the allowlisted AP in location 2. Make sure both EUDs are connected at the same time.*
  - ***Step 5:*** *Verify that the TSF detected and generated an alert.*
- *Test FAU_MAC_EXT.1:2:*
  - ***Step 1:*** *Configure the timeframe allowed between connection of two EUDs in two separate locations (Location 1, Location 2).*
  - ***Step 2:*** *Setup an allowlisted AP (Location 1).*
  - ***Step 3:*** *Connect an allowlisted EUD to AP.*
  - ***Step 4:*** *Setup a second allowlisted AP and a non-allowlisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-overlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).*
  - ***Step 5:*** *Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the allowlisted AP in location 2. Make sure that the time between connections is shorter than the time timeframe allowed/configured.*
  - ***Step 6:*** *Verify that the TSF detected and generated an alert.*

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 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.

Evaluation Activities

FAU_WIP_EXT.1

TSS

The evaluator shall verify that the TSS includes a list of available containment methods on the TSF and how to configure them.

Guidance

There are no operational guidance activities for this SFR.

Tests

Configure the containment methods available on the TSF and perform the following test for each method.

- *Test FAU_WIP_EXT.1:1:*
  - ***Step 1:*** *Deploy a non-allowlisted AP and connect to the protected wired infrastructure via wire (make sure it gets classified as rogue, or manually classify as such).*
  - ***Step 2:*** *Connect an allowlisted EUD to the AP.*
  - ***Step 3:*** *Verify that TSF generates an alert, breaks the connection of the allowlisted EUD from the rogue AP, and contains the rogue AP.*

A.2.3 Protection of the TSF (FPT)

FPT_FLS.1/WIDS Basic Internal TSF Data Transfer Protection (WIDS)

FPT_FLS.1.1/WIDS

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.

Evaluation Activities

FPT_FLS.1/WIDS

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 examine the TSS section to ensure that all failure modes specified in the ST are described.

Guidance

The evaluator shall review the operational guidance to verify that it identifies the potential TOE failures, how the TSF preserves a secure state following these failures, and any actions that are required to restore the TOE to normal operation following the transition to a failure state.

Tests

- *Test FPT_FLS.1/WIDS:1: For each failure mode specified in the ST, the evaluator shall ensure that the TOE attains a secure state after initiating each failure mode type.*

A.3 Implementation-dependent Requirements

This PP-Module does not define any Implementation-dependent SFRs.

Appendix B - Selection-based Requirements

B.1 Audit Events for Selection-Based SFRs

Table 9: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ANO_EXT.1	No events specified	N/A
FAU_SIG_EXT.1	No events specified	N/A
FAU_STG.1/PCAP	No events specified	N/A
FAU_STG.5/PCAP	Configuration of TOE audit storage behavior (if configurable)	No additional information

B.2 Security Audit (FAU)

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

The inclusion of this selection-based component depends upon selection in FAU_IDS_EXT.1.1.

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").

Evaluation Activities

FAU_ANO_EXT.1

TSS

The evaluator shall verify that the TSS describes the composition and construction of baselines or anomaly-based attributes specified in the SFR. The evaluator shall verify that the TSS provides a description of how baselines are defined and implemented by the TSF, or a description of how anomaly-based rules are defined and configured by the administrator.

The evaluator shall verify that the TSS describes the available modes of configuration (manual or automatic) and how to configure or import the baseline.

Guidance

The evaluator shall verify that the operational guidance describes how to configure baseline and/or anomalous traffic patterns based on what is stated in the TSS.

The evaluator shall verify that the operational guidance describes how to perform automatic and/or manual definition of anomaly activity based on what is selected in the ST.

Tests

The evaluator shall use the instructions in the operational guidance to configure baselines or anomaly-based rules through automated and/or manual means based on what is selected in the ST. The evaluator shall send traffic that does not match the baseline or matches the anomaly-based rule and verify the TSF detects the anomalous behavior and generates an alert.

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

The inclusion of this selection-based component depends upon selection in FAU_IDS_EXT.1.1.

FAU_SIG_EXT.1.1

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

Evaluation Activities

FAU_SIG_EXT.1

TSS

The evaluator shall verify that the TSS describes the user-defined and customizable attack signatures that the TOE can define.

Guidance

The evaluator shall verify that the operational guidance provides information on how to configure user-defined and customizable attack signatures, including a description of the customization options that are available.

Tests

- *Test FAU_SIG_EXT.1:1:*
  - ***Step 1:*** *Craft a signature with the available fields indicated in the TSS.*
  - ***Step 2:*** *Send a crafted frame that matches the signature to an allowlisted EUD*
  - ***Step 3:*** *Verify that the TSF triggers an alert based on the newly defined signature.*

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

The inclusion of this selection-based component depends upon selection in FAU_ARP.1.1.

FAU_STG.1.1/PCAP

The TSF shall be able to store generated **packet captures** on the [***[assignment: list of distributed TOE components on which packet capture data is stored] components of the*** *TOE itself, transmit the generated audit data to an external IT entity* ***hosting a protocol analyzer*** *using a trusted channel according to FTP_ITC*].

Application Note: This SFR is modified from its definition in CC Part 2 to define storage for packet capture data. Specifically, it is required that this data be stored both on the TOE itself and that it be transmitted securely to an external entity. Since the TOE is distributed, the first item has been refined to require the ST author to identify the specific TOE components on which the data is stored, since not all components will necessarily store them. If capture raw frame traffic that triggered the violation is selected in FAU_ARP.1.1, then this SFR must be included in the ST, and this iteration is for the packet captures generated as a selectable action completed upon detection of a potential security violation in FAU_ARP.1.

Evaluation Activities

FAU_STG.1/PCAP

TSS

The evaluator shall verify that the TSS includes the list of trusted channels (as specified in FTP_ITC.1) available to the TSF to transmit packet captures to an external entity. The evaluator shall also verify that the TSS describes which TOE components are responsible for the storage of packet capture data and any internal transmission between TOE components that is done in support of placing this data into storage.

Guidance

The evaluator shall verify that the operational guidance provides instructions on how to configure the trusted channel for remote storage of packet capture data.

Tests

- *Test FAU_STG.1/PCAP:1: The evaluator shall configure packet captures according to the guidance specified. The evaluator shall then trigger an event that starts a capture and verify through the tests in FTP_ITC.1 that the captured traffic being sent to the external device is being sent through a trusted channel.*
- *Test FAU_STG.1/PCAP:2: The evaluator shall configure packet captures to be stored on the TSF according to the guidance specified. The evaluator shall then trigger an event that starts a capture and verify that the packet capture was stored by the TOE component specified in the TSS.*

FAU_STG.5/PCAP Prevention of Audit Data Loss (Packet Captures)

The inclusion of this selection-based component depends upon selection in FAU_ARP.1.1.

FAU_STG.5.1/PCAP

The TSF shall [**selection**: *ignore **packet captures**, overwrite the oldest stored **packet captures**, [**assignment**: other actions to be taken in case of **packet capture** storage failure and conditions for the actions]*] if the **packet capture** storage is full.

Application Note: This SFR is modified from its definition in CC Part 2 to define storage for packet capture data. If capture raw frame traffic that triggered the violation is selected in FAU_ARP.1.1, then this SFR must be included in the ST, and this iteration is for the packet captures generated as a selectable action completed upon detection of a potential security violation in FAU_ARP.1.

Evaluation Activities

FAU_STG.5/PCAP

TSS

The evaluator shall verify that the TSS describes the behavior of the TOE when local storage space for packet capture data is exhausted and whether this behavior is configurable.

Guidance

If the TOE's behavior is configurable when local storage space for packet capture data is exhausted, the evaluator shall verify that the operational guidance provides information on what the configurable behaviors are and how they can be set.

Tests

- *Test FAU_STG.5/PCAP:1: The evaluator shall configure packet captures to be stored on the TSF according to the guidance specified (if necessary). Once configured, or if no such configuration is necessary, the evaluator shall then trigger an event that starts a capture and verify that the packet capture was stored on the TSF.*
- *Test FAU_STG.5/PCAP:2: If the TOE's behavior is configurable when local storage space for packet capture is exhausted, the evaluator shall use this functionality to configure different behavior to verify that the configuration has the intended effect.*

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 10: Extended Component Definitions

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

C.2 Extended Component Definitions

C.2.1 Security Audit (FAU)

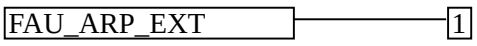
This PP-Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

C.2.1.1 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

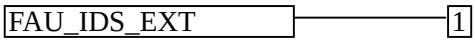
The TSF shall provide the ability to apply [**assignment**: *methods of selection*] to selectively exclude alerts from being generated.

C.2.1.2 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

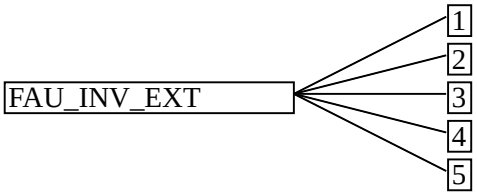
The TSF shall detect intrusions using [**assignment**: *detection strategies*] methods.

C.2.1.3 FAU_INV_EXT Environmental Inventory

Family Behavior

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

Component Leveling



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

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.

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.

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.

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

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 FMT_SMF.1 Specification of Management Functions

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.

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 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).

FAU_INV_EXT.2.3

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

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

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 the PP/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 rogue APs and EUDs, and [**selection**: *allow-listed APs, allow-listed EUDs, neighboring APs and EUDs, no other devices*] to within [**assignment**: *value equal or less than 25 feet*].

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.

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.

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

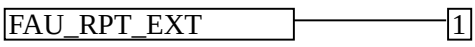
The TSF shall include a signal library.

C.2.1.4 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: No dependencies.

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

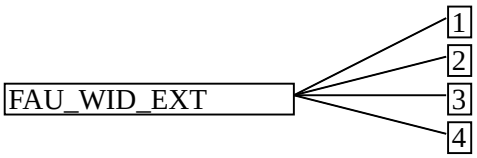
The TSF shall provide the ability to import data, such as an allowlist of APs and EUDs, and WIDS/WIPS configuration files from the system using [**selection**: *custom API*, *Syslog*, *common log format*, *comma separated values (CSV)*, *[**assignment**: vendor detection method]*].

C.2.1.5 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.

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.

FAU_WID_EXT.3, Wireless Intrusion Detection - Spectrum Monitoring, requires the TSF to surveil specified radio frequency bands or protocols to detect potential unauthorized devices.

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.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.

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: [**assignment**: *a list of frequency ranges*].

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.

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 the PP/ST:

- Detection of network devices operating in selected RF bands and/or protocols

FAU_WID_EXT.3 Wireless Intrusion Detection - Spectrum Monitoring

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_WID_EXT.3.1

The TSF shall detect the presence of devices [**selection**:

- *that operate in the following RF bands: [**assignment**: RF bands]*
- *that operate a specified protocol and take a specified action: [**assignment**: specify protocol and action]*

].

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 - Spectrum Monitoring]

FAU_WID_EXT.4.1

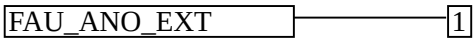
The TSF shall provide a dedicated sensor for wireless spectrum analysis.

C.2.1.6 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

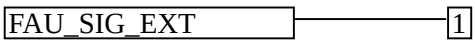
The TSF shall support the definition of anomaly activity through [**selection**: *manual configuration by administrators, automated configuration*].

C.2.1.7 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

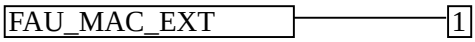
The TSF shall support user-defined and customizable attack signatures.

C.2.1.8 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

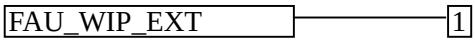
The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-allowlisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors.

C.2.1.9 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 D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. 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, 8.3 Dependencies between components.

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

Requirement	Rationale for Satisfaction
FDP_IFF.1 - Information Flow Control Functions	CC Part 2 specifies FDP_IFF.1 as a dependency of FDP_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 by FDP_IFC.1.

Appendix E - Allocation of Requirements in Distributed TOEs

For a distributed TOE, the security functional requirements in this PP-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 distributed TOE 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.1/PCAP	Protected Audit Event Storage (Packet Captures)	Feature Dependent
FAU_STG.5/PCAP	Prevention of Audit Data Loss (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 - 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/WIDS	Basic Internal TSF Data Transfer Protection	Feature Dependent

Appendix F - 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 G - Acronyms

Table 11: Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
AP	Access Point
Base-PP	Base Protection Profile
BSSID	Basic Service Set Identifier
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EUD	End User Device
FP	Functional Package
HTTPS	Hypertext Transfer Protocol Secure
ICS	Internet Connection Sharing
IPsec	Internet Protocol Security
MAC	Media Access Control
OE	Operational Environment
OSI	Open Systems Interconnection
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
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
TSFI	TSF Interface
TSS	TOE Summary Specification
WEP	Wired Equivalent Protocol
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WPA	WLAN Protected Access

Appendix H - Bibliography

Table 12: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025