collaborative Protection Profile for Network Devices Extended Package (EP) for Wireless Intrusion Detection/Prevention Systems (PP-Module for WIDS/WIPS)

This page is best viewed with JavaScript enabled!
Contents

1. Introduction
   1.1 Overview
   1.2 Terms
      1.2.1 Common Criteria Terms
      1.2.2 Technology
         Technical Terms
   1.3 Conformance Claims

1.4 How to Use This Extended Package

1.5 Compliant Targets of Evaluation

2. Security Problem Definition
   2.1 Threats
   2.2 Assumptions
   2.3 Organizational Security Policies

3. Security Objectives
   3.1 Compliant Targets of Evaluation
   3.2 TOE Boundary
   3.4 Use Cases
   3.5 Conformance Claims

3.6 Security Problem Description
   3.1 Threats
   3.2 Assumptions
   3.3 Organizational Security Policies

4. Security Objectives
   4.1 Security Objectives for the TOE
   4.2 Security Objectives for the Operational Environment
   4.4 Security Objectives Rationale

5. Security Requirements
   5.1 NDPP Security Functional Requirements
   5.2 Security Audit
      5.1.1 Protection of the TSF (FPT)
         5.1.2 Trusted Paths/Channels (FTP)
   5.2.1 TOE Security Functional Requirements
   5.2.2 User Data Protection
   5.2.3 User Data Protection (FDP)
   5.2.4 Security Management
   5.2.5 Consistency Rationale
   5.2.6 Network Device Protection Profile

4.2 Security Assurance Requirements
1 Introduction

1.1 Overview

This Extended Package (EP) Protection Profile Module (PP-Module) describes security requirements for a Wireless Intrusion Prevention System (WIDS/WIPS) defined to be an IEEE 802.11 network intrusion prevention-detection product located at the edge of a private network that can collect, inspect, and analyze 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 EP is not complete in itself, but rather extends the collaborative Protection Profile for Network Devices (NDcPP).

This PP-Module extends the collaborative Protection Profile for Network Devices (NDcPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDcPP.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document. The following sections provide both Common Criteria and technology terms used in this Protection Profile.

1.2.1 Common Criteria Terms


EP (Extended Package) - An implementation-independent set of security requirements for a product category that extend the requirements from a base PP to cover security requirements that are specific to a product type. In this case, the WIDS/WIPS EP extends the NDcPP Protection Profile (PP) specific subset of products described.

PP (Protection Profile) - An implementation-independent set of security requirements for a category of products.

Security Assurance Requirement (SAR) - A requirement to assure the security of the TOE.

Security Functional Policy (SFP) - The security policy enforced by a security function.

Security Functional Requirement (SFR) - A requirement for security enforcement by the TOE.
<table>
<thead>
<tr>
<th><strong>ST (Security Target)</strong></th>
<th>A set of implementation-dependent security requirements for a specific product.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TOE (Target of Evaluation)</strong></td>
<td>The product under evaluation. In this case, the <strong>Wireless Intrusion Detection/Prevention System</strong> as described in section <strong>Operating System</strong> as described in section Section 1.3.1 TOE Boundary and its supporting documentation.</td>
</tr>
<tr>
<td><strong>TSF (TOE Security Functionality)</strong></td>
<td>The security functionality of the product under evaluation.</td>
</tr>
<tr>
<td><strong>TSS (TOE Summary Specification)</strong></td>
<td>A description of how a TOE satisfies the SFRs in a ST.</td>
</tr>
<tr>
<td><strong>SFR (Security Functional Requirement)</strong></td>
<td>A requirement for security enforcement by the TOE.</td>
</tr>
<tr>
<td><strong>SAR (Security Assurance Requirement)</strong></td>
<td>A requirement to assure the security of the TOE.</td>
</tr>
</tbody>
</table>

### 1.2.2 Technology Terms

**WIDS/WIPS (Wireless Intrusion Detection/Prevention System)**

**AP (Access Point)**
A device that provides the network interface that enables wireless client hosts to access a wired network.

**EUD (End User Device)**
A device that has the ability to process, transmit, and/or store information.

**SSID (Service Set Identifier)**
The primary name associated with an 802.11 wireless local area network (**WLAN**).

**WIDS (Wireless Intrusion Detection System)**
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.

### 1.3 Conformance Claims

The collaborative Protection Profile for Network Devices (NDcPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the requirements and activities defined in the NDcPP, with additional SFRs and associated ‘Assurance Activities’ specific to WIDS/WIPS devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE’s compliance to the SFRs.

This EP is conformant to Parts 2 (extended) and 3 of Common Criteria Version 3.1, Revision 4 [CC].

### 1.4 How to Use This Extended Package

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

### 1.5 Compliant Targets of Evaluation

This EP

**WIPS (Wireless Intrusion Prevention System)**
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.

**WLAN (Wireless Local Area Network)**
A 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 Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS). A conformant WIDS/WIPS is a product that provides network security administrators with the ability to monitor, collect, log, and 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 typically/WIPS TOE consists of multiple sensors that passively scan their surrounding RF environment on the WLAN radio frequency spectrum for IEEE 802.11 traffic and a centralized mechanism such as a Server or Controller that processes the data collected by the sensors. The 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 Overlay (independent from WLAN) architecture depending on vendor implementation.

This EP is focused on inspecting The two different architectures are illustrated in the Figure 1 figure below.

A WIDS/WIPS is expected to inspect layers 1 and 2 of network traffic, per the OSI network model as the traffic that the WIDS/WIPS monitors is and monitor wireless frames in the RF spectrum utilized by IEEE 802.11 a, b, g, n, and ac. Requirements for 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.

The following are to be part of the evaluation:

- Monitoring, detection and reporting capabilities offered by the WIDS/WIPS.
- Location Tracking.
- Use of secure communication paths between WIDS/WIPS components.
- Use of secure communication paths for WIDS/WIPS management and event monitoring.
- Use of secure communication paths with external components (e.g., database and log server).

Two different architectures are illustrated in the Figure 1 figure below.

![Figure 1: General TOE](image)

### 2. Security Problem Definition

WIDS/WIPS
1.4 Use Cases

[USE CASE 1] Use Case 1

2 Conformance Claims

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

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:
- Network Device cPP, version 2.1

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

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

3 Security Problem Description

WIDS address a range of security threats related to detection of and reaction to potentially malicious WLAN traffic. The malicious traffic may pose a threat to one or more endpoints on the monitored networks, to the network infrastructure, or to the TOE itself. Attacks against a WLAN could compromise the confidentiality and integrity of WLAN user data 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 protects 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 terms “Wi-Fi”, “Wi-Fi Network” and “WLAN” will be used interchangeably to represent an IEEE 802.11 a Wi-Fi network.

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

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

3.1 Threats
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION

Sensitive unintended/unauthorized disclosure of sensitive information on a protected WLAN might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted sensitive data. The WIDS/WIPS will be capable of collecting and analyzing WLAN data to detect unauthorized disclosure of information.

T.UNAUTHORIZED_ACCESS

An attacker may attempt to gain inappropriate unauthorized access to one or more networks, network endpoints, or services, by methods such as by getting an impersonation of an authorized AP to get an EUD to connect to an unauthorized AP by impersonating an authorized 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 Assumptions

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

A.CONNECTIONS

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

A.PROPER_ADMIN

The administrator of the WIDS/WIPS is not careless, willfully negligent or hostile, and administers the WIDS/WIPS 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/WIPS data and appropriate response actions taken.

4 Security Objectives

4.1 Security Objectives for the TOE

O.SYSTEM_MONITORING

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

Addressed by: FAU.Gen.1/WIDS, FAU.Stg.Ext.1/PCAP

O.WIDS_ANALYZE

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

Addressed by: FAU.ARP.1, FAU.ARP.Ext.2, FAU.IDS.Ext.1, FAU.INV.Ext.1, FAU.INV.Ext.2, FAU.INV.Ext.3, FAU.SAA.1, FAU.WID.Ext.1, FAU.WID.Ext.2, FAU.WID.Ext.3, FAU.WID.Ext.4, FAU.WID.Ext.5, FDP.IFC.1, FAU.ANO.Ext.1, FAU.INV.Ext.4, FAU.INV.Ext.4/CELL, FAU.INV.Ext.5, FAU.MAC.Ext.1, FAU.SIG.Ext.1, FAU.WID.Ext.6, FAU.WID.Ext.7, FAU.WID.Ext.8

O.WIPS_REACT

The TOE must be able to react as configured by the administrators to isolate/contain WLAN devices that have been determined to violate administrator-defined WIPS policies.

Addressed by: FAU.WIP.Ext.1
O.TOE_ADMINISTRATION
To address the threat of unauthorized administrator access that is defined in the base PP, Conformant TOEs will provide the functions necessary for an administrator to configure the WIDS/WIPS Capabilities of the TOE.

Addressed by: FMT_SMF.1/WIDS

O.INSECURE_OPERATIONS
There may be instances where the TOE’s hardware malfunctions or the integrity of the TOE’s software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down, log or produce an alert upon discovery of a problem reported via the self-test mechanism.

Addressed by: FPT_FLS.1

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

Addressed by: FPT_ITT.1, FTP_ITC.1

4.2 Security Objectives for the Operational Environment

The Operational Environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the Operational Environment consist of a set of statements describing the goals that the Operational Environment should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment. The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with 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/WIPS is not careless, willfully negligent or hostile, and administers the WIDS/WIPS within compliance of the applied enterprise security policy.

4.3 Security Objectives Rationale

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

<table>
<thead>
<tr>
<th>Threat, Assumption, or OSP</th>
<th>Security Objectives</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.UNAUTHORIZED_ACCESS</td>
<td>O.SYSTEM_MONITORING</td>
<td>The threat T.UNAUTHORIZED_ACCESS is countered by O.SYSTEM_MONITORING as this provides visibility into the network which enables detection of unauthorized APs and EUDs.</td>
</tr>
<tr>
<td>T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION</td>
<td>O.WIDS_ANALYZE, O.WIPS.REACT</td>
<td>T.Unauthorized_Disclosure_of_Information is countered by O.WIDS_ANALYZE as this provides containment of unauthorized APs and EUDs.</td>
</tr>
<tr>
<td></td>
<td>O.SYSTEM_MONITORING</td>
<td>The threat T.Unauthorized_Disclosure_of_Information is countered by O.SYSTEM_MONITORING as this provides visibility into the network which enables detection of unauthorized APs and EUDs.</td>
</tr>
</tbody>
</table>
The threat T.UNAUTHORIZED_ACCESS is countered by O.WIDS_ANALYZE as this provides detection of potential violations of approved network usage.

The threat T.UNAUTHORIZED_ACCESS is countered by O.WIPS_REACT as this provides containment of unauthorized APs and EUDs.

The threat T.UNAUTHORIZED_ACCESS is countered by O.TOE_ADMINISTRATION.

The threat T.DISRUPTION is countered by O.SYSTEM_MONITORING as this provides for visibility into the network which enables detection of DoS attacks.

The threat T.DISRUPTION is countered by O.WIDS_ANALYZE as this provides for detection of potential violations of approved network usage.

The threat T.DISRUPTION is countered by O.WIPS_REACT as this provides containment of unauthorized APs and EUDs.

The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.

The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.

The organizational security policy P.ANALYZE is facilitated through O.WIDS_ANALYZE.

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

- **Refinement** operation (denoted by bold text or strikethrough text): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by italicized text): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by italicized text): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: are identified with a number inside parentheses (e.g. "(1)"

### 5.1 ND PP Security Functional Requirements Direction

In a PP-Configuration that includes ND PP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the ND PP. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

#### 5.1.1 Modified SFRs

The SFRs listed in this section are defined in the ND Protection Profile and relevant to the secure operation of the TOE.
5.1.1.1 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

**FPT_ITT.1**
The TSF shall take the following actions: display alert to Authorized Administrator in sufficient detail to show identity of APs and EUDs involved, description of alert and severity level, [selection: capture raw frame traffic that triggers the violation, no other actions] upon detection of a potential security violation.

**Application Note:** The capturing of raw frames that triggers the violation is an objective requirement. If the ST author selects capturing of raw frames that triggers the violation, the ST author must include the following SFRs: FAU_STG_EXT.1.1/PCAP, FAU_STG_EXT.1.2/PCAP, FAU_STG_EXT.1.3/PCAP.

**Assurance Activity:**

**TSS**
The evaluator shall verify that the TSS describes where to find the WIDS/WIPS 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/WIPS interface. If the objective requirement to capture the raw frame that triggered an alert is selected, the evaluator must also test for corresponding selection-based requirements. The evaluator shall use the operational guidance to configure the traffic capture capabilities.

**Tests**
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall perform a series of events or generate traffic that would successfully trigger an alert. The evaluator should verify and record whether the TOE generated the alert. The evaluator should also record the events or traffic that was generated and what alert was attempted to be triggered and record the details provided by the TOE in the alert.

- **Test 2:** If capturing of raw frames was selected, verify that the packet capture was triggered and stored as appropriate. protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use of [selection: IPsec, SSH, TLS, HTTPS].

**Application Note:** FPT_ITT.1 is optional in NDcPP, however, since a WIDS/WIPS TOE is distributed, FPT_ITT.1 shall be included in the ST as modified in this PP-Module and is applicable to the data transmitted between the sensors and controller.

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

5.1.1.2 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

**FTP_ITC.1**
The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, selection: 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.

**FTP_ITC.1.2**
The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

**FTP_ITC.1.3**
The TSF shall initiate communication via the trusted channel for [assignment: list of services for which the TSF is able to initiate communications].

**Application Note:** The intent of the above 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 the TSF uses a separate database server, the database server selection must included in the ST.

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

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

5.2.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

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

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

FAU_ARP_EXT.2 Security Alarm Filtering

FAU_ARP_EXT.2.1 The TSF shall provide the ability to apply [assignment: methods of selection] to selectively exclude alerts from being generated.

Assurance Activity

TSS

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

Guidance

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

Tests

The evaluator shall perform the following tests:

Test 1:
- The evaluator shall use the operational guidance to enable/disable detection of available detection capabilities through the WIDS/WIPS administrator interface. The evaluator shall then generate traffic that would successfully trigger the alert. The evaluator shall verify that the TOE generated the alert. The evaluator shall record the attack/intrusion that was generated and indicate which alert was triggered as well as the details that were provided by the WIDS about the alert.
- The evaluator shall disable the alert. The evaluator shall then generate events as in previous test that should successfully trigger the alert. The evaluator should check if the TOE generated an alert for the attack and record the findings.

FAU_GEN.1/WIDS Audit Data Generation

FAU_GEN.1/WIDS

The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [not specified] level of audit;
- [Auditable events listed in Table 1];
- Failure of wireless sensor communication.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU_ANO_EXT.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ARP.1</td>
<td>Actions taken due to potential</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>security violations</td>
<td></td>
</tr>
<tr>
<td>FAU_ARP_EXT.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_GEN.1/WIDS</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_IDS_EXT.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.3</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.4</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.4/CELL</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.5</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_SAA.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_SIG_EXT.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_STG_EXT.1/PCAP</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

11
The Auditable Events (Table 1) includes optional and objective SFRs. The auditing of optional and objective SFRs is only required if that SFR is included in the ST.

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

The TSF shall record within each WIDS auditable event as comma separated values (CSV), common log format (CLF), JavaScript Object Notation (JSON), syslog at least the following information:

a. Date and time of the event, type of event, and subject identity (if applicable);

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, at least the following information:

Application Note: The subject identity in this case is the whitelisted inventory item. Deploy an AP and EUD that should be classified as authorized devices.

Test 1: If the whitelist is configured automatically:

- Check the list of whitelisted devices and verify that the list is correct.
- Verify that the devices are classified as whitelisted.
- Remove or reclassify a device from the inventory.
- Verify that the device is not marked as whitelisted after removing or reclassifying.

Test 2: If the set of authorized devices is configured manually:

- Add an AP and EUD to the list. Record whether AP and EUD are displayed on the inventory.
- Verify that the devices are classified as whitelisted in the list of whitelisted devices.
- Remove the AP from the inventory.
- Verify that the removed device does not appear in the inventory after removal.

FAU_IDS_EXT.1 Intrusion Detection System – Intrusion Detection and Reporting Methods

FAU_IDS_EXT.1.1
The TSF shall provide the following methods of intrusion detection:

- [selection: anomaly-based, signature-based, behavior-based, hybrid, proprietary vendor, other detection method],
- [assignment:]

Application Note: At least one detection method must be selected based on the selection made in this SFR, the following SFRs must also be included:

If multiple detection methods are supported, each method supported shall be selected.

If anomaly-based detection is selected

...
shall be included in the ST. If signature-based detection is selected, then FAU_SIG_EXT.1 shall be included in the ST.

A hybrid detection method is one that incorporates two or more detection methods (e.g., both anomaly and signature based or signature and another method). If one of the detection methods in a hybrid solution includes either anomaly-based or signature-based detection methods, the corresponding selection based requirements must also be met.

### Assurance Activity

**TSS**

The evaluator shall verify that the TSS includes guidance on which intrusion detection technique(s) the TOE utilizes. If a hybrid intrusion detection is selected as the intrusion detection method, the TSS should provide details on the detection techniques utilized. Furthermore, when using a hybrid detection method that includes detection methods other than anomaly or signature based, the TSS shall include more details about such detection methods. If proprietary vendor detection method is selected, technical details on the method must be provided.

**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 note detection technique used and test for the appropriate selection based requirements.

### FAU_INV_EXT.1 Environmental Inventory

**FAU_INV_EXT.1.1**

The TSF shall provide Authorized Administrators with the ability to define an inventory of [authorized APs and EUDs], based on [EUD MAC addresses, AP MAC addresses].

**Application Note:** This inventory is used as a whitelist to indicate to the WIDS/WIPS which APs and EUDs are legitimate members of the wireless network. The terminology used to describe a inventoried or whitelisted device may vary by vendor product. This EP utilizes whitelisted and non-whitelisted to describe APs and EUDs that are part of the inventory.

**Assurance Activity:**

**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 whitelist.

**Tests**

The evaluator shall perform the following tests:

**FAU_IDS_EXT.1.2**

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

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

**FAU_IDS_EXT.1.3**

The TSF shall provide the ability to import data from the system: [selection]: custom API, Syslog, [assignment]: vendor detection method (e.g. Splunk)

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

### FAU_INV_EXT.1 Environmental Inventory
The TSF shall detect the presence and current information of [EUDs, APs] in the Operational Environment that are part of the defined inventory. Application Note: When referring to current information that should be detected by the TSF, it is referring to information about the detected EUD or AP as is observed by the WIDS/WIPS such as operating channel and band, SSID of an AP, client(s) connected to an AP, and the AP that an EUD is connected to. The TSF shall determine if a given AP or EUD is authorized based on MAC addresses. FAU_INV_EXT.2.3 has a full list of the details about the AP or EUD that should be detected by the WIDS/WIPS.

FAU_INV_EXT.2.3 has a full list of the details about the AP or EUD that should be detected by the WIDS/WIPS.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes how the presence of authorized EUDs and APs is presented by the TOE and what information about the devices is provided.

Guidance

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

Tests

The evaluator shall perform the following tests:

- **Test 1:** Deploy a whitelisted AP and EUD, and connect the EUD to the AP.
- **Test 2:** Verify that the list of detected APs and EUDs contains the whitelisted AP and EUD that were just deployed.
- **Test 3:** If the AP and EUD are detected verify that they are classified as whitelisted devices.

1.2 The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

FAU_INV_EXT.1.3

The TSF shall detect the presence and current information of [EUDs, APs] of non-whitelisted EUDs and APs in the Operational Environment that are not part of the defined inventory.

- **Test 1:** Deploy a non-whitelisted AP and EUD and connect the EUD to the AP.
- **Test 2:** Verify that the list of detected APs and EUDs contains the non-whitelisted AP and EUD that were just deployed.
- **Test 3:** If the AP and EUD are detected verify that they are not classified as whitelisted devices.

Application Note: When referring to current information that should be detected by the TSF, it is referring to information about the detected AP or EUD as is observed by the WIDS/WIPS such as operating channel and band, SSID of an AP, client(s) connected to an AP, and the AP that an EUD is connected to. FAU_INV_EXT.2.3 has a full list of the details about the AP or EUD that should be detected by the WIDS/WIPS.

Assurance Activity

TSS

The evaluator shall verify that the TSS includes guidance on where in the WIDS/WIPS 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 unauthorized APs and EUDs that are within range of the TOE sensors.

Tests

The evaluator shall perform the following tests:

- The inventory of authorized APs and EUDs is defined by FMT_SMF.1.

This inventory is used as a whitelist to indicate to the WIDS which APs and EUDs are legitimate members of the wireless network. The terminology used to describe an inventoried or whitelisted device may vary by vendor product. This PP-Module utilizes whitelisted to describe APs and EUDs that are part of the inventory and non-whitelisted to describe APs and EUDs that are not part of the inventory.
FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.2.1
The TSF shall detect information on the current physical location of inventoried EUDs and malicious EUDs, APs within range of the TOE's wireless sensors.

Application Note: This SFR only checks for the ability of the WIDS to track the location of APs and EUDs either by placing them on a map or providing the distance of the AP or EUD from the sensor but does not mandate a certain degree of accuracy. Objective requirement FAU_INV_EXT.4 is more stringent on the accuracy of the location tracking capabilities.

Assurance Activity

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.

Guidance
The evaluator shall review the operational guidance for instructions on how to configure location tracking and where in the TSF administrator interface the location of APs and EUDs can be viewed.

Tests
The evaluator shall perform the following test:

- **Test 1:**
  - **Step 1:** Deploy an AP within range of the sensors.
  - **Step 2:** Verify that TSF is able to provide location information on the AP.
  - **Step 3:** Verify that the location presented by the TSF appears within the range of the sensors.

FAU_INV_EXT.2.2
The TSF shall detect the 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.

Assurance Activity

TSS
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
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
The evaluator shall perform the following test:

- **Test 1:**
  - **Step 1:** Deploy an AP within range of the sensors.
  - **Step 2:** Check the WIDS/WIPS 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/WIPS user interface.
The TSF shall detect the current RF band, current channel, MAC Address, classification of APs and EUDs of all APs and EUDs within range of the TOE’s wireless sensors.

For [APs] the TOE, the TSF shall detect the following additional details for APs:

- encryption
- number of connected EUDs.

For [EUDs] the TOE shall detect the following additional details: SSID and BSSID of AP it is connected to.

Application Note: For detection of encryption type, the TSF should be able to differentiate between no encryption, WEP, TKIP and AES.

Assurance Activity

The evaluator shall verify that the TSS explains the capability of detecting the current RF band, current channel, MAC Address, classification of 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

The evaluator shall perform the following test:

**Test 1:**

- **Step 1:** Deploy a whitelisted AP, non-whitelisted AP and two whitelisted EUDs.
- **Step 2:** Connect one whitelisted EUD to the whitelisted AP and one to the non-whitelisted AP.
- **Step 3:** Check the WIDS/WIPS user interface for a list of detected APs and EUDs.
- **Step 4:** Verify that current RF band, current channel, MAC Address, classification of device, are part of the information presented on the WIDS/WIPS user interface for all the APs and EUDs detected. For APs verify that encryption, number of connected EUDs is presented. For EUDs verify that the different WLAN encryption methods and when no encryption is in use.
The TSF shall detect the following additional details for EUDs:

- SSID and BSSID of AP it is connected to.

FAU_INV_EXT.3 Behavior of Environmental Objects

FAU_INV_EXT.3.1 The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An EUD establishes a peer-to-peer connection with any other EUD.

[selection:]

- An EUD bridges two network interfaces.

[selection:]

- An EUD uses internet connection sharing.

[selection:]

- assignment: other connection types.

[selection:]

- no other connections types.

Application Note: For this requirement, it is acceptable for the WIDS to use a generic term for bridges or peer-to-peer connections when generating an alert for the detection of different types of bridges or peer-to-peer connections. The specific type of connection does not have to be specific.

Assurance Activity:

TSS

The evaluator shall verify that the TSS describes the ability of the TOE to detect the network behavior described by the SFR.

Guidance

The evaluator shall review the operational guidance to verify that it provides instructions on how alerts are presented to the administrator as well as information regarding the format of each alert.

Tests

The evaluator shall perform the following tests:

Test 1:

Create the following connections between two whitelisted EUDs.
• Windows Ad Hoc Connection
• Mac OS Ad Hoc
• Linux Ad Hoc
• Wi-Fi Direct

Test 2: Create the following connections between one whitelisted EUD and a non-whitelisted EUD
• Windows Ad Hoc Connection
• Mac OS Ad Hoc
• Linux Ad Hoc
• Wi-Fi Direct

Test 3: (Optional) Bridge two network interfaces on a whitelisted EUD (one must be the wireless card listed as whitelisted).

Test 4:
• Create a Windows Hosted Network with a whitelisted EUD.
• Connect a different whitelisted EUD to the network.

Verify that alerts were generated by each of the connections in each test. Provide a description of the alert.

FAU_SAA.1 Potential Violation Analysis

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

Assurance Activity

TSS
There are no TSS assurance activities for this SFR.

Guidance
There are no operational guidance activities for this SFR.

Tests
There are no tests for this SFR. Testing detection of potential malicious events is tested through the ability to detect intrusions in other SFRs.

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

a. Accumulation or combination of assignment: subset of defined auditable events known to indicate a potential security violation;

b. Other potential security violations as defined by Table 1 below

1. SFR Potential Security Violation.
   - Detection of authorized EUD establishing peer-to-peer connection with any other EUD.
   - Detection of EUD bridging two network interfaces.
   - Detection of rogue AP.
   - Detection of malicious EUD.
   - Detection of traffic with excessive transmit power level.
   - Detection of active probing.
   - Detection of MAC spoofing.
   - Detection of RF-based denial of service.
   - Detection of deauthentication flooding.
   - Detection of disassociation flooding.
   - Detection of request-to-send/clear-to-send abuse.
   - Detection of unauthorized authentication scheme use.
   - Detection of unauthorized encryption scheme use.
   - Detection of unencrypted traffic.

Table 1: Potential Security Violations
FAU_WID_EXT.1 Wireless Intrusion Detection – Malicious Environmental Objects

FAU_WID_EXT.1.1
The TSF shall apply [assignment selection: user-defined configurable, automatic] classification rules to detect the following types of malicious environmental objects: [rogue APs].

Assurance Activity
TSS
The evaluator shall verify that the TSF describes how the TOE can detect rogue APs and whether this behavior is configurable.

Guidance
The evaluator shall review the operational guidance for instructions on how to configure user-defined classification rules, if supported.

Tests
The evaluator shall perform configure an AP classification rule, then perform the following test:

- Test 1:
  - Deploy an AP following the user-defined classification rule.
  - Verify that the AP gets correctly classified.

Application Note: If "configurable" is selected then, "Define classification rules to detect rogue APs" shall be selected in FMT_SMF.1

FAU_WID_EXT.1.2
The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Assurance Activity
TSS
There are no TSS assurance activities for this SFR.

Guidance
There are no operational guidance activities for this SFR.

Tests
There are no tests for this SFR; testing of monitoring capabilities is tested through the ability to detect intrusions in other SFRs.
The evaluator shall perform the following test:

- **Test 1:**
  - Deploy a non-whitelisted AP in the area of the WIDS sensor but take no action against the network.
  - Deploy a non-whitelisted AP in the area of the WIDS sensor and connect it to the internal wired infrastructure (optional for overlay WIDS).
  - Connect a whitelisted EUD to a non-whitelisted AP.
  - Connect a non-whitelisted EUD to a whitelisted AP.
  - Launch an attack against authorized AP with an unauthorized EUD.
  
  For each step above verify that the TSF detects APs and EUDs and that they are classified appropriately.

**FAU_WID_EXT.2 Wireless Intrusion Detection – Passive Information Flow Monitoring**

**FAU_WID_EXT.2.1**

The TSF shall monitor and analyze network traffic matching the

- 802.11 monitoring SFP

for all channels in the following RF 

- **frequencies:**
  - 2.4 GHz
  - 4.9/5.0 GHz

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

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 SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

**Assurance Activity:**

**TSS**

The evaluator shall verify that the TSS includes information on the channels the TSF can detect.

**Guidance**

The evaluator shall review the operational guidance for the channels that the TSF is able to monitor and how to configure the TSF to monitor the channels as selected in the SFR. Depending on the channel dwelling times implemented by the vendor it might take a while for the detection of devices.

**Tests**

The evaluator shall perform the following tests:

- **Test 1: Channels on On 5GHz 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 5GHz band.
  - **Step 3:** Deploy AP on at least 2 different channels outside the regulatory domain on 5GHz band.
  - **Step 4:** Verify that the AP gets detected on each channel tested.

- **Test 2: Channels on 2.4GHz 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 2.4GHz 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.

Test 3: Non-standard channel frequencies.

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.

**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" shall be selected in FMT_SMF_1.

The intent of this SFR is to employ WIDS

AWIPS

sensors that can have all wireless transmission capabilities disabled for instances where a site wishes to implement a no wireless policy.

**Application Note:**

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.1.1 and defined through FAU_WID_EXT SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

**Assurance Activity**

The evaluator shall verify that the TSS includes information on how to configure the sensors as completely passive. Specifically, the TSS shall indicate whether the TOE can configured as a dedicated sensor with prevention disabled, or, if the sensor transmits data even with no prevention capabilities are enabled, how to disable wireless transmissions.

**Guidance**

Specifically, the TSS shall indicate whether the TOE can configured as a dedicated sensor with prevention disabled, or, if the sensor transmits data even with no prevention capabilities are enabled, how to disable wireless transmissions.

**Tests**

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.

The evaluator shall then perform the following tests:

**Deploy a signal analyzer and configure on the bands specified in the tests below. On 2.4 GHz band**

- **Test 1:**
  - **Step 1:** Boot a sensor and using the signal analyzer observe to check if any eminations are coming from the sensor.
  - **Step 2:** Verify that the signal analyzer does not pick up emanations from the sensor.

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

**On 5GHz band**

- **Test 1:**
  - **Step 1:** Boot a sensor and using the signal analyzer observe to check if any emissions are coming from the sensor.
  - **Step 2:** Verify that the signal analyzer does not pick up emanations from the sensor.

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

**FAU_WID_EXT.2.3**

The TSF shall provide the ability to define a subset of [SSID(s)] as determine if a given SSID is authorized.

Application Note:
The administrator should have the ability to configure which SSIDs are permitted on the network.

**Assurance Activity**
No TSS assurance activity specified

**Guidance**

The evaluator shall verify that the TSS includes instructions on how to set the allowed SSIDs.

**Tests**

The evaluator shall configure the TSF with a set of authorized channels and SSIDs. The ability to detect violation of this policy will be tested in FAU_WID_EXT.2.4. FMT_SMF.1 defines the subset of authorized SSID(s).

FAU_WID_EXT.2.4

The TSF shall detect the presence of the following unauthorized traffic on the network through the following methods:

- detection of unauthorized APs broadcasting authorized SSIDs
- detection of APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- detection of authorized EUDs associating to unauthorized SSIDs
- detection of unauthorized EUDs associating to authorized APs
- detection of unauthorized point to point wireless bridges by whitelisted APs
- detection of active probing

**NULL SSID associations**

- illegal state transitions
- protocol violations for [selection: 802.11, 802.1X]

- [assignment: proprietary vendor protocol(s)]


no other

methods

- no other

1. Detection of illegal state transitions and protocol violations are objective requirements and will be mandatory in future PP versions.

Application Note: “Authorized” EUDs/APs are those that are assigned to the whitelist as defined by FAU FMT INV EXT SMF 1.

Assurance Activity

TSS

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.

Guidance

The evaluator shall verify that the operational guidance provides instructions on how to configure SSIDs as authorized.

Tests

The evaluator shall configure the TSF with a set of authorized SSIDs and perform the following tests:

Unauthorized SSID, Unauthorized Connections – 2.4 GHz band

Test 1:

- Step 1: Configure a whitelisted AP to operate on a set channel on the 2.4 GHz band with an authorized SSID.
- Step 2: Connect a non-whitelisted EUD to AP.
- Step 3: Verify that the TSF detects the non-whitelisted EUD connecting to the whitelisted AP.
- Step 4: Change the AP’s SSID to one not on the authorized list.
- Step 5: Connect a whitelisted EUD to AP.
- Step 6: Verify that the TSF detects the whitelisted AP using unauthorized SSID and the EUD associating to an unauthorized SSID.

Unauthorized SSID, Unauthorized Connections – 5 GHz band

Test 2:

- Step 1: Configure a whitelisted AP to operate on a set channel on the 5 GHz band with an authorized SSID.
- Step 2: Connect a non-whitelisted EUD to AP.
- Step 3: Verify that the TSF detects the non-whitelisted EUD connecting to the whitelisted AP.
- Step 4: Change the AP’s SSID to one not on the authorized list.
- Step 5: Connect a whitelisted EUD to AP.
- Step 6: Verify that the TSF detects the whitelisted AP using unauthorized SSID and the EUD associating to an unauthorized SSID.

MAC Spoofing

Test 1:

- Spoof mac address of whitelisted EUD connected to a whitelisted AP on a second EUD.
- Connect EUD with spoofed MAC address to another whitelisted AP while the valid EUD it is spoofing is connected to the first AP.
- Verify that the TSF detected the MAC spoofing.

Test 2:

- Spoof mac address of whitelisted AP on a second AP.
- Verify that the TSF detected the MAC spoofing.

Active Probing

Test 1:

- Perform an active scan on the subnet of the WLAN.
- Record tools used and type of scan performed. Verify that the TSF detects the active probing.

Point-to-Point Wireless Bridges

Test 1:
Setup a point-to-point wireless bridge using whitelisted APs in the range of the wireless sensors. Verify that the TSF detects the bridge.

The 802.11 standard allows APs to beacon with the SSID field set to null. This is referred to as a hidden or cloaked SSID. The client seeking to associate with an AP using a hidden SSID must first send out a Probe Request that contains the SSID of that network, then the AP will return with a Probe Request of its own. The TSF needs to be able to detect if an AP is allowing clients to associate without providing the valid SSID of the AP.

FAU_WID_EXT.2.5 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.

FAU_WID_EXT.3 Wireless Intrusion Detection – Denial of Service

FAU_WID_EXT.3.1 The TSF shall detect the following intrusions:
- RF-based denial of service, deauthentication flooding, disassociation flooding,
- request-to-send/clear-to-send abuse, and [selection: [assignment: other DoS methods], no other DoS methods].

Assurance Activity: 

TSS

The evaluator shall examine the TSS to verify that it describes the denial of service attacks that can be detected by the TOE.

Guidance

If the ability of the TOE to detect different types of denial of service attacks is configurable, the evaluator shall verify that the operational guidance provides instructions on how to specify the attack(s) that are detected.

Tests

RF-based DoS

Test 1:
- Deploy whitelisted AP and configure to stay in a particular channel.
- Connect a whitelisted EUD to the AP.
- Use an RF Jammer or signal generator on the same frequency as the AP and EUD to create a DoS.
- Verify that the TSF detects the RF-based DoS.

Traffic injection based-DoS

Test 1: Deauthentication Flood
- Deploy whitelisted AP and configure to a set channel.
- Connect a whitelisted EUD to the AP.
- Send an flood of deauthentication frames to the EUD using the MAC address of whitelisted AP it is connected to.
- Verify that the TSF detects the deauthentication flood.
- Send an flood of deauthentication frames with the MAC address of whitelisted AP as the source and destination as a broadcast.
- Verify that the TSF detects the deauthentication flood.

Test 2: Disassociation Flood
- Deploy whitelisted AP and configure to a set channel.
- Connect two whitelisted EUDs to the AP.
- Send an flood of CTS frames to reserve RF medium.
- Verify that the TSF detects the CTS abuse.

FAU_WID_EXT.4 Wireless Intrusion Detection – Unauthorized Authentication Schemes

FAU_WID_EXT.4.1 The TSF shall provide Authorized Administrators the ability to define authorized WLAN authentication schemes.

Assurance Activity: 

TSS

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 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.
Tests

The evaluator shall configure the TSF with a set of authorized WLAN authentication schemes. The ability to detect violation of this policy will be tested in FAU_WID_EXT.4.2.

FAU_WID_EXT.4.2

The TSF shall detect when [whitelisted APs and EUDs defined in FAU_INV_EXT.1.1] attempt to use WLAN authentication schemes that are not authorized.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized WLAN authentication schemes are used.

Guidance

There are no operational guidance activities for this SFR.

Tests

The evaluator shall configure the TSF with 802.1x authentication as the only mode of authorized WLAN authentication schemes and perform the following tests:

- **Test 1:**
  - Deploy a whitelisted AP with open authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.
  - Deploy a whitelisted AP that uses pre-shared key authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.

FAU_WID_EXT.5 Wireless Intrusion Detection—Unauthorized Encryption Schemes

FAU_WID_EXT.5.1

The TSF shall provide Authorized Administrators the ability to define authorized WLAN encryption schemes.

Assurance Activity

TSS

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

Guidance

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

The evaluator shall configure the TSF with 802.1x authentication as the only mode of authorized WLAN authentication schemes and perform the following tests:

- **Test 1:**
  - Deploy a whitelisted AP with open authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.
  - Deploy a whitelisted AP that uses pre-shared key authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.

FAU_WID_EXT.5 Wireless Intrusion Detection—Unauthorized Encryption Schemes

FAU_WID_EXT.5.1

The TSF shall provide Authorized Administrators the ability to define authorized WLAN encryption schemes.

Assurance Activity

TSS

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

Guidance

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

The evaluator shall configure the TSF with 802.1x authentication as the only mode of authorized WLAN authentication schemes and perform the following tests:

- **Test 1:**
  - Deploy a whitelisted AP with open authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.
  - Deploy a whitelisted AP that uses pre-shared key authentication.
  - Connect a whitelisted EUD to AP.
  - Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.

FAU_WID_EXT.5 Wireless Intrusion Detection—Unauthorized Encryption Schemes

FAU_WID_EXT.5.1

The TSF shall provide Authorized Administrators the ability to define authorized WLAN encryption schemes.

Assurance Activity

TSS

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

Guidance

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

The evaluator shall configure the TSF with 128 bit AES encryption type as the only allowed encryption scheme and perform the following test:
Test 1:
- Deploy a whitelisted AP with no encryption.
- Connect a whitelisted EUD to AP.
- Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.
- Deploy a whitelisted AP that uses TKIP encryption only.
- Connect a whitelisted EUD to AP.
- Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.

**FAU_WID_EXT.6.3**
The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

**Application Note:** When referring to unencrypted data being received by a whitelisted AP or EUD it refers to unencrypted data being sent to a whitelisted AP or EUD from either a non-whitelisted or whitelisted AP or EUD.

**Assurance Activity:**
- Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.

**TSS**
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**
There are no operational guidance activities for this SFR.

**Tests**
- **Test 1:**
  - Deploy a whitelisted AP with no encryption.
  - Connect a whitelisted EUD to AP and generate traffic.
  - Verify that the TSF detects unencrypted data frames being sent between the whitelisted AP and EUD.
  - Connect a non-whitelisted EUD to AP and generate traffic.
  - Verify that the TSF detects unencrypted data frames being sent between the whitelisted AP and non-whitelisted EUD.

- **Test 2:**
  - Deploy a non-whitelisted AP with no encryption.
  - Connect a whitelisted EUD to AP and generate traffic.
  - Verify that the TSF detects unencrypted data frames being sent between the non-whitelisted AP and whitelisted EUD.

**FAU_GEN.1/WIDS Audit Data Generation**

**FAU_GEN.1/WIDS**
The TSF shall be able to generate an

**FAU_WID_EXT.4 Wireless Intrusion Detection – Unauthorized Authentication Schemes**

**FAU_WID_EXT.4.1**
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

**Application Note:** Whitelisted APs and EUDs are defined in FMT_SMF.1.

**FAU_WID_EXT.5 Wireless Intrusion Detection – Unauthorized Encryption Schemes**

**FAU_WID_EXT.5.1**
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

**Application Note:** Whitelisted APs and EUDs are defined in FMT_SMF.1.

**FAU_WID_EXT.5.2**
The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

**Application Note:** Whitelisted APs and EUDs are defined in FMT_SMF.1. When referring to unencrypted data being received by a whitelisted AP or EUD it refers to unencrypted data being sent to a whitelisted AP or EUD from either a non-whitelisted or whitelisted AP or EUD.

**5.2.2 User Data Protection (FDP)**

**FDP_IFC.1 Information Flow Control Policy**

**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 whitelist as defined by FMT_SMF.1.

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** SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

### 5.2.3 Security Management (FMT)

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

The TSF shall be capable of performing the following management functions for **WIDS** functionality:

- Define an inventory of authorized APs based on **MAC** addresses,
- 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]**:
- Specification of periods of network activity that constitute baseline of expected behavior,
- Definition of abnormal activity,
- Define classification rules to detect rogue APs,
- **[selection]**: Enable, Disable] transmission of data by wireless sensor,
- Define attack signatures,
- Define rules for overwriting previous packet captures,
- Define the amount of time sensor monitors a specific **selection**: frequency, channel, 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" shall be selected. If **FAU_ANO_EXT.1** is included in the ST and "manual configuration by administrators" is selected in **FAU_ANO_EXT.1.2**, then "Definition of anomaly activity" shall be selected.

If "can be configured to prevent transmission of data" is selected in **FAU_WID_EXT.2.2** then "Enable/Disable transmission of data by wireless sensor" shall be selected.

### 6 Consistency Rationale

#### 6.1 Network Device Protection Profile

##### 6.1.1 Consistency of TOE Type

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

##### 6.1.2 Consistency of Security Problem Definition

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

<table>
<thead>
<tr>
<th>PP-Module Threat</th>
<th>Consistency Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION</td>
<td></td>
</tr>
<tr>
<td>T.UNAUTHORIZED_ACCESS</td>
<td></td>
</tr>
<tr>
<td>T.DISRUPTION</td>
<td></td>
</tr>
</tbody>
</table>

##### 6.1.3 Consistency of Objectives

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

<table>
<thead>
<tr>
<th>PP-Module TOE Objective</th>
<th>Consistency Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.SYSTEM_MONITORING</td>
<td></td>
</tr>
<tr>
<td>O.WIDS_ANALYZE</td>
<td></td>
</tr>
<tr>
<td>O.WIPS_REACT</td>
<td></td>
</tr>
<tr>
<td>O.TOE_ADMINISTRATION</td>
<td></td>
</tr>
<tr>
<td>O.INSECURE_OPERATIONS</td>
<td></td>
</tr>
<tr>
<td>O.TRUSTED_COMMUNICATIONS</td>
<td></td>
</tr>
</tbody>
</table>

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

| PP-Module Operational Environment Objective Consistency Rationale |
|------------------------------------------------------------------|---------|
| OE.CONNECTIONS                                                  |         |
6.1.4 Consistency of Requirements

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

**PP-Module Requirement Consistency Rationale**

<table>
<thead>
<tr>
<th>Modified SFRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPT_ITT.1</td>
</tr>
<tr>
<td>FTP_ITC.1</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

### Mandatory SFRs

- FAU_ARP.1
- FAU_ARP_EXT.2
- FAU_GEN.1
- FAU_IDE_EXT.1
- FAU_INV_EXT.1
- FAU_INV_EXT.2
- FAU_INV_EXT.3
- FAU_SAA.1
- FAU_WID_EXT.1
- FAU_WID_EXT.2
- FAU_WID_EXT.3
- FAU_WID_EXT.4
- FAU_WID_EXT.5
- FDP_IFC.1
- FMT_SMF.1

### Optional SFRs

- FAU_WID_EXT.6
- FAU_WID_EXT.7

### Selection-based SFRs

- FAU_ANO_EXT.1
- FAU_INV_EXT.4
- FAU_SIG_EXT.1
- FAU_STG_EXT.1

### Objective SFRs

- FAU_GEN.1
- FAU_INV_EXT.4
- PLACEHOLDER
- FAU_INV_EXT.5
- FAU_MAC_EXT.1
- FAU_WIP_EXT.1
- FPT_FLS.1

---

**Appendix A - Optional SFRs**

**FAU_WID_EXT.6** Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring

- **FAU_WID_EXT.6.1**
  The TSF shall detect the presence of network devices that operate in the following RF bands: [selection: 3.6 GHz, 60 GHz, sub-GHz (0-900 MHz), all cellular bands]

  Application Note: This SFR refers to Non-Wi-Fi (IEEE 802.11 a, b, g, n, and ac) network devices that operate in the specified frequencies. If the ST author selects detection of devices in the cellular bands, FAU_INV_EXT.4.1 must be included in the ST.

**FAU_WID_EXT.7** Wireless Intrusion Detection – Wireless Spectrum Analysis

- **FAU_WID_EXT.7.1**
  The TSF shall provide a dedicated sensor for wireless spectrum analysis.

---

**Appendix B - Selection-based SFRs**

**FAU_ANO_EXT.1** Anomaly-Based Intrusion Detection
This is a selection-based component. Its inclusion depends upon selection from 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”).

FAU_INV_EXT.4/CELL Location of Environmental Objects (Cellular Devices)
This is a selection-based component. Its inclusion depends upon selection from FAU_WID_EXT.6.1.

FAU_INV_EXT.4.1/CELL
The TSF shall detect the physical location of cellular devices to within [assignment: distance degree of accuracy] of their actual location.

FAU_SIG_EXT.1 Signature-Based Intrusion Detection
This is a selection-based component. Its inclusion depends upon selection from FAU_IDS_EXT.1.1.

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

FAU_STG_EXT.1/PCAP Protected Audit Event Storage (Packet Captures)
This is a selection-based component. Its inclusion depends upon selection from FAU_ARP.1.1.

FAU_STG_EXT.1.1/PCAP
The TSF shall be able to transmit the generated packet captures to an external IT entity using a trusted channel according to FTP_ITC.1.
Application Note: Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel per FTP_ITC.1. Note that this PP-Module modifies FTP_ITC.1 from the Base-PP. If “capture raw frame traffic that triggers the violation” is selected in FAU_ARP.1, then this SFR shall be included in the ST, and this iteration is for the PCAPs generated as a selectable action completed upon detection of a potential security violation in FAU_ARP.1.

FAU_STG_EXT.1.2/PCAP
The TSF shall be able to store generated packet captures on the TOE itself.

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

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

FAU_GEN.1/WIDS2 Alerts Data Generation (WIDS)

FAU_GEN.1.1/WIDS2
The TSF shall be able to generate a WIDS audit record of the following auditable events:

a. Start-up and shutdown of the

audit

a. WIDS functions;
b. All WIDS auditable events for the [not specified] level of audit;
c. [Auditable events listed in Table 3;
### Failure of wireless sensor communication

**a. Totals of similar events occurring within a specified time period**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU_ANO_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ANO_EXT_1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ARP_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_GEN_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>/WIDS</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_IDS_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_2.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_2.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_3.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_3.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_4.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT_4.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.3</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.4</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.5</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_MAC_EXT_1.6</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_SAA_EXT_1.1</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

- **whitelisted devices**
  - Type of device (AP or EUD), MAC Address.

- **Alerts generated by detection of rogue device**
  - Description of alert, MAC address of the device that the whitelisted device made a connection with, connection start and end.
  - Information on location of device: MAC address, device type, classification of device, sensors that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s) (in meters).

- **Alerts generated by detection of mac spoofing**
  - Description of alert, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue, IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP).
Alert generated by violation of user defined signature.

Name of alert being triggered (as provided when creating the signature), description of alert (as provided when creating the signature), MAC address of devices involved.

Details about what SSIDs are set as authorized.

SSIDs set by administrator as authorized.

Sensor wireless transmissions capabilities. Wireless transmission capabilities are turned on.

Unauthorized activity description of violation (i.e. whitelisted EUD connected to unauthorized SSID), identity information of the devices involved.

Alert generated for DoS. MAC Address, device type, and classification AP or EUD attacked, DoS details (RF or injection based), for injection-based, indicate type (i.e., deauth flood).

Information about devices and unauthorized authentication methods.

MAC Address, device type, and classification of devices involved, authentication method used.

Information about devices and unauthorized encryption methods.

MAC Address, device type, and classification of devices involved, encryption method used.

Information about devices involved.

MAC Address, device type, and classification of devices involved (sending and receiving devices).

Information about detected devices.

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.

Information about action taken.

description of violation, the 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).
None

None

FPT_ITT.1

None

None

FTP_ITC.1

None

None

Table 3: Auditable Events

WIDS Alerts

Application Note: There are additional auditable events in this SRF serve to extend the FAU_GEN.1 SFR found in the ND cPP. The events in the table should be combined with those of the ND cPP in the context of a conforming Security Target. The Auditable Events The alerts table contains the contents of the alert produced by the WIDS. The Alert table includes optional and objective requirements. The auditing of optional and objective requirements is only required if the vendor chooses to have the requirement evaluated by NIAP.

Assurance Activity:

TSS

There are no TSS assurance activities for this SRF.

Guidance

There are no operational guidance activities for this SFR.

Tests

The evaluator shall perform the following test:

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this EP. 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.

4.1.2 User Data Protection

FDP_IFC.1 Information Flow Control Policy

FDP_IFC.1

The TSF shall enforce the [802.11 monitoring SFP] for [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 whitelist as defined by FAU_INV_EXT.1.1. 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.1.1 and defined through FAU_WID_EXT SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

Assurance Activity:

TSS

There are no TSS assurance 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 1:
  - Set the WIDS sensor for a set channel
  - Start a traffic capture from the WIDS sensor
- Send a set number of frames on the channel the sensor's operating channel for all IEEE 802.11 a, b, g, n, ac frame types and subtypes from/to the following:
  1. authorized APs and authorized EUDs
  2. authorized APs and unauthorized EUDs
  3. unauthorized APs and authorized EUDs

- Verify that there are frames from all the types and subtypes in the capture.

4.1.3 Security Management

**FMT.SM.F1/WIDS Specification of Management Functions (WIDS)**

**FMT.SM.F1.1/WIDS**

The TSF shall be capable of performing the following management functions for WIDS functionality: [management functions listed in Table 2]:

- **SPR**
  - Management Function
- **FAU.ANO.EXT.1**
  - Specification of periods of network activity that constitute baseline of expected behavior (optional).

Table 2: Management Functions

**Assurance Activity**

**TSS**

The evaluator shall verify that the TSS describes how the baseline can be configured.

**Guidance**

The evaluator shall verify that the operational guidance describes the instructions for defining a baseline.

**Tests**

The evaluator shall perform the following test:

- **Test 1:** Following the instructions in the operational guidance verify that the period of network activity that constitutes a baseline can be indicated in the TSF.

4.1.4 Protection of the TSF

**FPT.ITT.1 Basic Internal TSF Data Transfer Protection**

**FPT.ITT.1.1 REFINEMENT**

The TSF shall use [selection, at least one of: IPsec, SSH, TLS, TLS/HTTPS] with security strength commensurate with all other trusted communications to protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

**Application Note:** 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 the appropriate requirements from the NDcPP corresponding to their selection are copied to the ST if not already present. For the purposes of this requirement, security strength is defined by NIST SP 800-57, “commensurate” means that the strengths must, at a minimum, meet the requirements for the cryptographic primitives listed in the EP, and “other trusted communications” refers to the mechanisms specified in FPT.ITC.

**Assurance Activity**

**TSS**

The evaluator shall examine the TSS to determine that the methods and protocols used to protect distributed TOE components are described. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

**Guidance**

The evaluator shall confirm that the operational guidance contains instructions for establishing the communication paths for each supported method.

**Tests**

The evaluator shall also perform the following tests:

- **Test 1:** The evaluators shall ensure that communications using each specified (in the operational guidance)
communications method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.

- **Test 2:** The evaluator shall ensure, for each method of communication, the channel data is not sent in plaintext.

Further assurance activities are associated with the specific protocols:

### 4.1.5 Trusted Paths/Channels

**FTP-ITC.1 Inter-TSF trusted channel**

**FTP-ITC.1.1 REFINEMENT**

The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [selection: database server, assignment: other capabilities, none] that is logically distinct from other communication channels and provides assured identification of its endpoints 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, the database server selection must included in the ST.

*Assurance Activity:* The evaluator shall perform the following activities in addition to the assurance activity specified in the base NDcPP for this SFR:

**TSS**

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

*Guidance*

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

**Tests**

- **Test 1:** The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
- **Test 2:** For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
- **Test 3:** The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
- **Test 4:** The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, physically interrupt an established connection. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.

Further assurance activities are associated with the specific protocols:

### 4.2 Security Assurance Requirements

This EP does not define any SARs beyond those defined within the NDcPP. It is important to note that a TOE that is evaluated against this EP is inherently evaluated against NDcPP. When evaluating the TOE, it is necessary to apply the SARs defined for the base PP to the entire TOE and not just the portion that is described by the base PP.

### A. Optional Requirements

As indicated in Section 1.3, the baseline requirements (those that must be performed by the WIDS/WIPS) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C. The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a WIDS/WIPS to claim conformance to this EP. The second type (in Appendix B) are requirements based on selections in the body of the EP. If certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this EP, so adoption by vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

**FAU_WID_EXT.6 Wireless Intrusion Detection – Wireless Spectrum Monitoring**

**FAU_WID_EXT.6.1**

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

*Application Note:* This SFR refers to Non-WiFi (IEEE 802.11 a, b, g, n, and ac) network devices that operate in the specified frequencies. If the ST author selects detection of devices in the cellular bands, the ST author must include selection-based requirement **FAU_INV_EXT.4.1.**
Assurance Activity

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 1:** Deploy a device within the given technology and verify that the TSF detects the device.

FAU_WID_EXT.6.2

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

Assurance Activity

TSS

The evaluator shall verify that the TSS verifies 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.

B. Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE) are contained in the body of this EP. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

FAU_INV_EXT.4 CELL Location of Environmental Objects (Cellular Devices)

*This component depends upon selection in [FAU_WID_EXT.6.1]*

With regards to ‘similar’ type events, ‘similar’ events are multiple occurrences of the same auditable event within some time period where the only significant difference between these events is the timestamp. For example, it is not expected that the TOE generate an individual audit message for every event of the same kind that occurs within a reasonable time period. An alert must, at a minum, include the details as outlined on the table, but may contain additional details.

Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel per FTP_ITC.1. Note that this PP-Module modifies FTP_ITC.1 from the Base-PP.

FAU_GEN.1.2/WIDS2

The TSF shall record within each WIDS auditable event as |selection: comma separated values (CSV), common log format (CLF), JavaScript Object Notation (JSON), syslog| at least the following information:

- a. Date and time of the event, type of event, and subject identity (if applicable);
- b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [auditable events listed in Table 3].

FAU_INV_EXT.4 Precise Location of Environmental Objects

FAU_INV_EXT.4.1

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

PLACEHOLDER Signal Library

PLACEHOLDER 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.

**FAU_INV_EXT.5 Detection of Unauthorized Connections**

**FAU_INV_EXT.5.1**
The TSF shall detect when non-whitelisted APs have a wired connection to the internal corporate network.

**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 whitelisted EUD to disconnect and promptly connects a non-whitelisted device using the MAC address of the whitelisted 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-whitelisted 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 a whitelisted EUD connecting in two distant locations.

**FAU_WIP_EXT.1 Wireless Intrusion Prevention**

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

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

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

**FPT_FLS.1 Basic Internal TSF Data Transfer Protection**

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

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

### Appendix D - Extended Component Definitions

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

#### D.1 Background and Scope

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

<table>
<thead>
<tr>
<th>Functional Class</th>
<th>Functional Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Audit</td>
<td>FAU_ARP_EXT Security Alarm Filtering</td>
</tr>
<tr>
<td></td>
<td>FAU_IDS_EXT Intrusion Detection Methods</td>
</tr>
<tr>
<td></td>
<td>FAU_INV_EXT Environmental Inventory</td>
</tr>
<tr>
<td></td>
<td>FAU_INV_EXT Characteristics of Environmental Objects</td>
</tr>
<tr>
<td></td>
<td>FAU_INV_EXT Behavior of Environmental Objects</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Malicious Environmental Objects</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Passive Information Flow Monitoring</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Denial of Service</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Unauthorized Authentication Schemes</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Unauthorized Encryption Schemes</td>
</tr>
<tr>
<td></td>
<td>FAU_WID_EXT Wireless Spectrum Monitoring</td>
</tr>
</tbody>
</table>

Security Audit (FAU)
D.2 Extended Component Definitions

FAU_ARP_EXT Security Alarm Filtering

Component Leveling
FAU.1, Security Alarm Filtering;

Management: FAU.1
Audit: FAU.1

FAU.1 Security Alarm Filtering
Hierarchical to: No other components.
Dependencies to:

FAU_ARP_EXT.2.1

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

FAU_IDS_EXT Intrusion Detection Methods

Family Behavior

FAU_IDS_EXT FAU_IDS_EXT.1

Component Leveling
FAU.1, Intrusion Detection System – Intrusion Detection and Reporting Methods;

Management: FAU.1
Audit: FAU.1

FAU.1 Intrusion Detection System – Intrusion Detection and Reporting Methods
Hierarchical to: No other components.
Dependencies to:

FAU_IDS_EXT.1.1

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

FAU_IDS_EXT.1.2
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]

FAU_IDS_EXT.1.3

The TSF shall provide the ability to import data from the system: selection: custom API, Syslog, assignment: vendor detection method (e.g. Splunk)]

FAU_INV_EXT Environmental Inventory

Family Behavior
FAU_INV_EXT FAU_INV_EXT.1 FAU_INV_EXT.2 FAU_INV_EXT.3 FAU_INV_EXT.4/CELL FAU_INV_EXT.4 FAU_INV_EXT.5

Component Leveling
FAU.1, Environmental Inventory,

Management: FAU.1

Audit: FAU.1

FAU.1 Environmental Inventory

Hierarchical to: No other components.

Dependencies to:
FAU_INV_EXT.1.1

The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

FAU_INV_EXT.1.2

The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

FAU_INV_EXT.1.3

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

Component Leveling
FAU.1, Characteristics of Environmental Objects,

Management: FAU.1

Audit: FAU.1

FAU.1 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:
FAU_INV_EXT.2.1

The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE’s wireless sensors.

FAU_INV_EXT.2.2
The TSF shall detect received signal strength and [selection: RF power levels above a predetermined threshold, no other characteristics] of hardware operating within range of the TOE’s wireless sensors.

**FAU_INV_EXT.2.3**

The TSF shall detect the

- current RF band
- current channel
- MAC Address
- 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.2.4**

The TSF shall detect the following additional details for APs:

- encryption
- number of connected EUDs.

**FAU_INV_EXT.2.5**

The TSF shall detect the following additional details for EUDs:

- SSID and BSSID of AP it is connected to.

**Component Leveling**

**FAU.1, Behavior of Environmental Objects,**

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Behavior of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.3.1**

The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An EUD establishes a peer-to-peer connection with any other EUD.

[selection:

- An EUD bridges two network interfaces,
- An EUD uses internet connection sharing,
- [assignment: other connection types],
- no other connections types]

]

**Component Leveling**

**FAU.1, Location of Environmental Objects (Cellular Devices),**

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Location of Environmental Objects (Cellular Devices)**

Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.4.1/CELL

The TSF shall detect the physical location of cellular devices to within [assignment: distance degree of accuracy] of their actual location.

Component Leveling

FAU.1, Precise Location of Environmental Objects;

Management: FAU.1

Audit: FAU.1

FAU.1 Precise Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

Component Leveling

FAU.1, Detection of Unauthorized Connections;

Management: FAU.1

Audit: FAU.1

FAU.1 Detection of Unauthorized Connections

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.5.1

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

FAU_INV_EXT Characteristics of Environmental Objects

Component Leveling

FAU.1, Environmental Inventory;

Management: FAU.1

Audit: FAU.1

FAU.1 Environmental Inventory

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.1.1

The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

FAU_INV_EXT.1.2

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

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

Component Leveling

FAU.1, Characteristics of Environmental Objects,

Management: FAU.1

Audit: FAU.1

FAU.1 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.2.1

The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE's wireless sensors.

FAU_INV_EXT.2.2

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

FAU_INV_EXT.2.3

The TSF shall detect the

- current RF band
- current channel
- MAC Address
- 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.2.4

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.5

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU.1, Behavior of Environmental Objects,

Management: FAU.1

Audit: FAU.1

FAU.1 Behavior of Environmental Objects

Hierarchical to: No other components.

Dependencies to:
The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An EUD establishes a peer-to-peer connection with any other EUD.

[selection:
  - An EUD bridges two network interfaces,
  - An EUD uses internet connection sharing,
  - [assignment: other connection types],
  - no other connections types]

Component Leveling
FAU.1, Location of Environmental Objects (Cellular Devices),

Management: FAU.1
Audit: FAU.1

FAU.1 Location of Environmental Objects (Cellular Devices)
Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.4.1/CELL

The TSF shall detect the physical location of cellular devices to within [assignment: distance degree of accuracy] of their actual location.

Component Leveling
FAU.1, Precise Location of Environmental Objects,

Management: FAU.1
Audit: FAU.1

FAU.1 Precise Location of Environmental Objects
Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.4.1

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

Component Leveling
FAU.1, Detection of Unauthorized Connections,

Management: FAU.1
Audit: FAU.1

FAU.1 Detection of Unauthorized Connections
Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.5.1
The TSF shall detect when non-whitelisted APs have a wired connection to the internal corporate network.

**FAU_INV_EXT Behavior of Environmental Objects**

**Component Leveling**

FAU.1, Environmental Inventory,

Management: FAU.1

Audit: FAU.1

**FAU.1 Environmental Inventory**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.1.1**

The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

**FAU_INV_EXT.1.2**

The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

**FAU_INV_EXT.1.3**

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

**Component Leveling**

FAU.1, Characteristics of Environmental Objects,

Management: FAU.1

Audit: FAU.1

**FAU.1 Characteristics of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.2.1**

The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE's wireless sensors.

**FAU_INV_EXT.2.2**

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

**FAU_INV_EXT.2.3**

The TSF shall detect the

- current RF band
- current channel
- MAC Address
- 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.2.4**
The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

**FAU_INV_EXT.2.5**

The TSF shall detect the follow additional details for EUDs:

- **SSID** and **BSSID** of AP it is connected to.

**Component Leveling**

FAU.1, Behavior of Environmental Objects,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Behavior of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.3.1**

The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An **EUD** establishes a peer-to-peer connection with any other **EUD**.

  **[selection:**

  - An **EUD** bridges two network interfaces,
  - An **EUD** uses internet connection sharing,
  - **[assignment: other connection types]**,
  - **[assignment: no other connection types]**
  
  **]**

**Component Leveling**

FAU.1, Location of Environmental Objects (Cellular Devices),

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Location of Environmental Objects (Cellular Devices)**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.4.1/CELL**

The TSF shall detect the physical location of detected cellular devices to within **[assignment: distance degree of accuracy]** of their actual location.

**Assurance Activity**

**TSS**

The evaluator shall verify that the **TSS** includes information on the TOE’s ability to detect the physical location of cellular devices.

**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 devices can be viewed.
Tests

The evaluator shall perform the following tests:

1. **Test 1:**
   - **Step 1:** Deploy a cellular device within range of the sensors.
   - **Step 2:** Verify that the TSF is able to track the location of the device.
   - **Step 3:** Verify the level of accuracy indicated by the TSF falls within the one indicated in the assignment.

**FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection**

This component depends upon selection in FAU_IDS_EXT.1.1.

FAU_ANO_EXT.1.1

The TSF shall support the definition of selection, at least one of baselines (expected and approved), anomaly (unexpected) traffic patterns, including the specification of selection:

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

[assignment: other methods]

and the following network protocol fields:

- **all management and control frame header elements**

Assurance Activity

**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.

Guidance

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

Tests

1. **Test 1:**
   - The evaluator shall use the instructions in the operational guidance to configure baselines or anomaly-based rules.
   - 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_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”).

Assurance Activity

**TSS**

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 perform automatic and/or manual definition of anomaly activity based on what is selected in the ST.

Tests

This test may be performed in conjunction with FAU_ANO_EXT.1.1. The evaluator shall follow the operational guidance and define anomaly activity through automated and/or manual means based on what is selected in the ST. The evaluator shall verify in each case that the anomaly activity is defined correctly by determining that anomalous traffic is identified by the TSF.
FAU_SIG_EXT.1 Signature-Based Intrusion Detection

This 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.

Assurance Activity

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 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 a whitelisted EUD
  - Step 3: Verify that the TSF triggers an alert based on the newly defined signature.

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

This component depends upon selection in FAU_ARP.1.1.
FAU_STG_EXT.1.1/PCAP
The TSF shall be able to transmit the generated packet captures to an external IT entity using a trusted channel according to FTP_ITC.1.

Application Note: FTP_ITC.1 is inherited from the NDcPP.

Assurance Activity

TSS
The evaluator shall verify that the TSS include the list of trusted channels (as specified in FTP_ITC.1) available in the TSF to transmit packet captures to an external entity. The TSS shall also include instructions on how to configure the trusted channel.

Guidance
There are no operational guidance activities for this SFR.

Tests
- Test 1: The evaluator shall configure packet captures according to the guidance specified in the TSS. 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.

FAU_STG_EXT.1.2/PCAP
The TSF shall be able to store generated packet captures on the TOE itself.

Assurance Activity

TSS
The evaluator shall verify that the TSS describes the ability of the TOE to store packet capture data within itself.

Guidance
The evaluator shall verify that the operational guidance provides information on how much storage space is available for packet capture data and where that data is stored.

Tests
- Test 1: The evaluator shall configure packet captures to be stored on the TSF according to the guidance specified in the TSS. The evaluator shall then trigger an event that starts a capture and verify that the packet capture was stored on the TSF.

FAU_STG_EXT.1.3/PCAP
The TSF shall [selection: drop new packet capture data, overwrite previous packet captures according to the following rule assignment: rule for overwriting previous packet captures]; [assignment: other action] when the local storage space for packet capture data is full.
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 behavior of the TOE when local storage space for packet capture data is exhausted is configurable, the evaluator shall verify that the operational guidance provides information on what the configurable behaviors are and how they can be set.

Tests

- **Test 1**: The evaluator shall define packet data retention and deletion rules on the TSF as specified in the TSS and test the functionality of the specified rules.

## C. Objective Requirements

This appendix includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this EP as they describe security functionality not yet widely available in commercial technology. However, these requirements may be included in the ST such that the WIDS/WIPS is still conformant to this EP. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this EP.

### FAU_INV_EXT.4 Precise Location of Environmental Objects

**FAU_INV_EXT.4.1** The TSF shall detect the physical location of APs, EUDs to within 15 feet of their actual location.

**Assurance Activity**

- **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.

**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.

**Tests**

- The evaluator shall perform the following test:
  - **Test 1:**
    - **Step 1**: Deploy an AP within range of the sensors.
    - **Step 2**: Verify the TS provides location tracking information about the AP.
    - **Step 3**: Verify the AP location presented is within 15 feet actual location.

### FAU_INV_EXT.5 Detection of Unauthorized Connections

**FAU_INV_EXT.5.1** The TSF shall detect when non-whitelisted APs as defined in FAU_INV_EXT.1 have the following connections: wired connection to the internal corporate network.

**Assurance Activity**

- **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/WIPS to detect unauthorized APs connected to the protected wired infrastructure.

**Tests**

- **Test 1:**
  - **Step 1**: The evaluator shall define packet data retention and deletion rules on the TSF as specified in the TSS and test the functionality of the specified rules.
The evaluator shall perform the following test:

- **Test 1:**
  - Step 1: Deploy a non-whitelisted AP.
  - Step 2: Connect the AP via wire to the protected network infrastructure.
  - Step 3: Check the WIDS/WIPS 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_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 whitelisted EUD to disconnect and promptly connects a non-whitelisted device using the MAC address of the whitelisted EUD.

**Assurance Activity**

**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).

**Tests**

The evaluator shall perform the following test:

- **Test 1:**
  - Step 1: Setup a whitelisted AP (Location 1).
  - Step 2: Connect a whitelisted EUD to AP.
  - Step 3: Setup a second whitelisted AP and a non-whitelisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-verlapping 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 whitelisted 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.

**FAU_MAC_EXT.1.2**

The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-whitelisted EUDs as defined in **FAU_INV_EXT.1** 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 a whitelisted EUD connecting in two distant locations.

**Assurance Activity**

There are no TSS assurance activities for this SFR.

**Guidance**

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**

The evaluator shall perform the following test:

- **Test 1:**
  - Step 1: Configure the timeframe allowed between connection of two EUDs in two separate locations (Location 1, Location 2).
  - Step 2: Setup a whitelisted AP (Location 1).
  - Step 3: Setup a second whitelisted AP and a non-whitelisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-verlapping 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 whitelisted
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_WID_EXT.7 Wireless Intrusion Detection – Proprietary Traffic Monitoring

FAU_WID_EXT.7.1
The TSF shall detect the presence of all vendor proprietary network traffic matching the [802.11 monitoring SFP] for all IEEE
802.11 a, b, g, n, ac frame types and subtypes between:

1. authorized APs and authorized EUDs.
2. authorized APs and unauthorized EUDs.
3. unauthorized APs and authorized EUDs.

Application Note: 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.1.1 and defined through FAU_WID_EXT SFRs. A
vendor does not have to formally define this policy, it only needs to comply with the SFRs.

Assurance Activity

TSS

There are no TSS assurance activities for this SFR.

Guidance

There are no operational guidance activities for this SFR.

Tests

Test 1:

Step 1: Set the WIDS sensor for a set channel.
Step 2: Start a traffic capture from the WIDS sensor.
Step 3: Send a set number of frames on the sensor’s operating channel for all IEEE 802.11 a, b, g, n, ac vendor
proprietary frame types and subtypes from/to the following:

1. authorized APs and authorized EUDs.
2. authorized APs and unauthorized EUDs.
3. unauthorized APs and authorized EUDs.
Step 4: Provide a list of the frames types and subtypes that were used for testing and verify that they were all
detected.

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, wiredside containment of an unauthorized AP connected to the internal
corporate wired network.]

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

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

Assurance Activity

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 1:

Step 1: Deploy a non-whitelisted 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 a whitelisted EUD to the AP.
Step 3: Verify that TSF generates an alert, breaks the connection of the whitelisted EUD from the rogue AP, and
contains the rogue AP.
The TSF shall be able to generate a WIDS/WIPS audit record of the following auditable events:

- a. Start-up and shutdown of the WIDS/WIPS functions;
- b. All WIDS/WIPS auditable events for the [not specified] level of audit;
- c. [Auditable events listed in Table 4;]
- d. Totals of similar events occurring within a specified time period.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU_ANO_EXT.1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ANO_EXT.1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ARP.1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_ARP_EXT.2.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_GEN.1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_IDS_EXT.1.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.1.1</td>
<td>whitelisted devices information</td>
<td>Type of device (AP or EUD), MAC Address.</td>
</tr>
<tr>
<td>FAU_INV_EXT.1.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.2.1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.2.2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.2.3</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>FAU_INV_EXT.3.1</td>
<td>Unexpected behavior by whitelisted device alert</td>
<td>Description of behavior detected (i.e., bridge, ICS connection), MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.</td>
</tr>
<tr>
<td>FAU_INV_EXT.4.1</td>
<td>Information on location of device</td>
<td>Device MAC address, device type, classification of device, sensors that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s) (in meters).</td>
</tr>
</tbody>
</table>

Component Leveling

FAU.1, Precise Location of Environmental Objects,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Precise Location of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.4.1**

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

**Component Leveling**

FAU.1, Detection of Unauthorized Connections,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Detection of Unauthorized Connections**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.5.1**

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

**FAU_WID_EXT Malicious Environmental Objects**

**Family Behavior**

FAU_WID_EXT FAU_WID_EXT.1 FAU_WID_EXT.2 FAU_WID_EXT.3 FAU_WID_EXT.4 FAU_WID_EXT.5 FAU_WID_EXT.6 FAU_WID_EXT.7

**Component Leveling**

FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects.

**Management:** FAU.1

**Audit:** FAU.1
Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.1.1

The TSF shall apply [selection: configurable, automatic] classification rules to detect rogue APs.

FAU_WID_EXT.1.2

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling

FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring

Hierarchical to: No other components.

Dependencies to:

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
- 4.9/5.0 GHz

[selection:
- channels outside regulatory domain,
- non-standard channel frequencies,
- no other domains
]

FAU_WID_EXT.2.2

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

FAU_WID_EXT.2.3

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

FAU_WID_EXT.2.4

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:

- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- NULL SSID associations
  [selection:
  - illegal state transitions,
  - protocol violations for [selection: 802.11, 802.1X],
  ]
The TSF shall perform stateful frame inspection and log attacks spanning multiple frames.

Component Leveling

FAU.1, Wireless Intrusion Detection – Denial of Service,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Denial of Service

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.3.1

The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and [selection: [assignment: other DoS methods], no other DoS methods].

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.4.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.5.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

FAU_WID_EXT.5.2

The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.
Component Leveling
FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring
Hierarchical to: None other components.
Dependencies to:
FAU_WID_EXT.6.1

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

Component Leveling
FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis
Hierarchical to: None other components.
Dependencies to:
FAU_WID_EXT.7.1

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

FAU_WID_EXT Passive Information Flow Monitoring
Component Leveling
FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects
Hierarchical to: None other components.
Dependencies to:
FAU_WID_EXT.1.1

The TSF shall apply [selection: configurable, automatic] classification rules to detect rogue APs.

FAU_WID_EXT.1.2

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling
FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring

Hierarchical to: No other components.

Dependencies to:

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
- 4.9/5.0 GHz

[selection:
- channels outside regulatory domain,
- non-standard channel frequencies,
- no other domains
]

FAU_WID_EXT.2.2

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

FAU_WID_EXT.2.3

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

FAU_WID_EXT.2.4

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:

- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- NULL SSID associations
- [selection:
  - illegal state transitions,
  - protocol violations for [selection: 802.11, 802.1X],
  - no other
  ]

FAU_WID_EXT.2.5

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

Component Leveling

FAU.1, Wireless Intrusion Detection – Denial of Service,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Denial of Service

Hierarchical to: No other components.

Dependencies to:
The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and \[ \text{selection: \text{assignment: other DoS methods}, no other DoS methods} \].

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.4.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.5.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

FAU_WID_EXT.5.2

The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

Component Leveling

FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.6.1

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

Component Leveling
FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis

Management: FAU.1
Audit: FAU.1

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.7.1**

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

**FAU_WID_EXT Denial of Service**

Component Leveling

FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects,

Management: FAU.1
Audit: FAU.1

**FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.1.1**

The TSF shall apply [selection: *configurable, automatic*] classification rules to detect rogue APs.

**FAU_WID_EXT.1.2**

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling

**FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring**

Management: FAU.1
Audit: FAU.1

Hierarchical to: No other components.

Dependencies to:

**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
- 4.9/5.0 GHz

(selection:
- *channels outside regulatory domain*,
- *non-standard channel frequencies*,
- *no other domains*)
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].

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

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:

- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- NULL SSID associations
- [selection:
  - illegal state transitions,
  - protocol violations for [selection: 802.11, 802.1X],
  - no other
  ]

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

Component Leveling

FAU.1, Wireless Intrusion Detection – Denial of Service,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Denial of Service

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.3.1

The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and [selection: [assignment: other DoS methods], no other DoS methods].

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.4.1
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

**Component Leveling**

**FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes**

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.5.1**

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

**FAU_WID_EXT.5.2**

The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

**Component Leveling**

**FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring**

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.6.1**

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

**Component Leveling**

**FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis**

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.7.1**

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

**FAU_WID_EXT Unauthorized Authentication Schemes**

**Component Leveling**

**FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects**
Management: FAU.1
Audit: FAU.1

**FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.1.1**

The TSF shall apply \[selection: configurable, automatic\] classification rules to detect rogue APs.

**FAU_WID_EXT.1.2**

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

**Component Leveling**

**FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,**

Management: FAU.1
Audit: FAU.1

**FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring**

Hierarchical to: No other components.

Dependencies to:

**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
- 4.9/5.0 GHz

\[selection:

- channels outside regulatory domain,
- non-standard channel frequencies,
- no other domains
\]

**FAU_WID_EXT.2.2**

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

**FAU_WID_EXT.2.3**

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

**FAU_WID_EXT.2.4**

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:

- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- **NULL SSID** associations
  - **selection:**
    - illegal state transitions,
    - protocol violations for **selection:** 802.11, 802.1X,
    - no other

**FAU_WID_EXT.2.5**

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

**Component Leveling**

FAU.1, Wireless Intrusion Detection – Denial of Service,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Denial of Service**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.3.1**

The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and **selection:** **assignment:** other DoS methods, no other DoS methods.

**Component Leveling**

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.4.1**

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

**Component Leveling**

FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes**

Hierarchical to: No other components.

Dependencies to:

**FAU_WID_EXT.5.1**

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

**FAU_WID_EXT.5.2**
The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

Component Leveling
FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring
Hierarchical to: No other components.
Dependencies to:
FAU_WID_EXT.6.1

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

Component Leveling
FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis
Hierarchical to: No other components.
Dependencies to:
FAU_WID_EXT.7.1

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

FAU_WID_EXT Unauthorized Encryption Schemes
Component Leveling
FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects
Hierarchical to: No other components.
Dependencies to:
FAU_WID_EXT.1.1

The TSF shall apply [selection: configurable, automatic] classification rules to detect rogue APs.

FAU_WID_EXT.1.2

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling
FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring
Hierarchical to: No other components.
Dependencies to:
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
- 4.9/5.0 GHz

[selection:
- channels outside regulatory domain,
- non-standard channel frequencies,
- no other domains
]

FAU_WID_EXT.2.2

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

FAU_WID_EXT.2.3

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

FAU_WID_EXT.2.4

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:
- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- NULL SSID associations
- [selection:
  - illegal state transitions,
  - protocol violations for [selection: 802.11, 802.1X],
  - no other
  ]

FAU_WID_EXT.2.5

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

Component Leveling
FAU.1, Wireless Intrusion Detection – Denial of Service,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Denial of Service
Hierarchical to: No other components.
The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and [selection: assignment: other DoS methods, no other DoS methods].

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.4.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.5.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

FAU_WID_EXT.5.2

The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

Component Leveling

FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.6.1

The TSF shall detect the presence of network devices that operate in the following RF bands: [selection: 3.6 GHz, 60 GHz, sub-GHz (0-900 MHz), all cellular bands]
Component Leveling
FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis
Hierarchical to: No other components.
Dependencies to:

FAU_WID_EXT.7.1

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

FAU_WID_EXT Wireless Spectrum Monitoring

Component Leveling
FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects
Hierarchical to: No other components.
Dependencies to:

FAU_WID_EXT.1.1

The TSF shall apply [selection: configurable, automatic] classification rules to detect rogue APs.

FAU_WID_EXT.1.2

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling
FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring
Hierarchical to: No other components.
Dependencies to:

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
- 4.9/5.0 GHz

[selection:
- channels outside regulatory domain,
- non-standard channel frequencies,
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].

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

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:

- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
- unauthorized point to point wireless bridges by whitelisted APs
- active probing
- NULL SSID associations
- [selection: illegal state transitions, protocol violations for [selection: 802.11, 802.1X], no other]

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

Component Leveling

FAU.1 Wireless Intrusion Detection – Denial of Service,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Denial of Service
Hierarchical to: No other components.
Dependencies to:

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes,
Management: FAU.1
Audit: FAU.1
FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes
Hierarchical to: No other components.
Dependencies to:
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

Component Leveling


Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.5.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.

FAU_WID_EXT.5.2

The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

Component Leveling


Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.6.1

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

Component Leveling

FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis;

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.7.1

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

FAU_WID_EXT Wireless Spectrum Monitoring

Component Leveling
FAU.1, Wireless Intrusion Detection – Malicious Environmental Objects

Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Malicious Environmental Objects
Hierarchical to: No other components.
Dependencies to:

**FAU_WID_EXT.1.1**

The TSF shall apply [selection: configurable, automatic] classification rules to detect rogue APs.

**FAU_WID_EXT.1.2**

The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.

Component Leveling

FAU.1, Wireless Intrusion Detection – Passive Information Flow Monitoring,

Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Passive Information Flow Monitoring
Hierarchical to: No other components.
Dependencies to:

**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
- 4.9/5.0 GHz

[selection:
- channels outside regulatory domain,
- non-standard channel frequencies,
- no other domains
]

**FAU_WID_EXT.2.2**

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

**FAU_WID_EXT.2.3**

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

**FAU_WID_EXT.2.4**

The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic:
- unauthorized APs broadcasting authorized SSIDs
- APs and EUDs spoofing the MAC address of whitelisted APs and EUDs
- authorized EUDs associating to unauthorized SSIDs
- unauthorized EUDs associating to authorized APs
• unauthorized point to point wireless bridges by whitelisted APs
• active probing
• NULL SSID associations
• [selection:
  ○ illegal state transitions,
  ○ protocol violations for [selection: 802.11, 802.1X],
  ○ no other
]

FAU_WID_EXT.2.5

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

Component Leveling

FAU.1, Wireless Intrusion Detection – Denial of Service,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Denial of Service

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.3.1

The TSF shall detect RF-based denial of service, deauthentication flooding, disassociation flooding, request-to-send/clear-to-send abuse, and [selection: [assignment: other DoS methods], no other DoS methods].

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Authentication Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.4.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.

Component Leveling

FAU.1, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Unauthorized Encryption Schemes

Hierarchical to: No other components.

Dependencies to:

FAU_WID_EXT.5.1

The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.
The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.

Component Leveling
FAU.1, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring
Hierarchical to: No other components.
Dependencies to:

FAU_WID_EXT.6.1

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

Component Leveling
FAU.1, Wireless Intrusion Detection – Wireless Spectrum Analysis,
Management: FAU.1
Audit: FAU.1

FAU.1 Wireless Intrusion Detection – Wireless Spectrum Analysis
Hierarchical to: No other components.
Dependencies to:

FAU_WID_EXT.7.1

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

FAU_ANO_EXT Anomaly-Based Intrusion Detection

Family Behavior
FAU_ANO_EXT FAU_ANO_EXT.1

Component Leveling
FAU.1, Anomaly-Based Intrusion Detection,
Management: FAU.1
Audit: FAU.1

FAU.1 Anomaly-Based Intrusion Detection
Hierarchical to: No other components.
Dependencies to:

FAU_ANO_EXT.1.1

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

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

] and the following network protocol fields:

• all management and control frame header elements.

FAU_ANO_EXT.1.2

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

FAU_INV_EXT Location of Environmental Objects (Cellular Devices)

Component Leveling

FAU.1, Environmental Inventory;

Management: FAU.1

Audit: FAU.1

FAU.1 Environmental Inventory

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.1.1

The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

FAU_INV_EXT.1.2

The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

FAU_INV_EXT.1.3

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

Component Leveling

FAU.1, Characteristics of Environmental Objects;

Management: FAU.1

Audit: FAU.1

FAU.1 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.2.1

The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE’s wireless sensors.

FAU_INV_EXT.2.2

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

FAU_INV_EXT.2.3
The TSF shall detect the
- current RF band
- current channel
- MAC Address
- 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.2.4

The TSF shall detect the follow additional details for APs:
- encryption
- number of connected EUDs.

FAU_INV_EXT.2.5

The TSF shall detect the follow additional details for EUDs:
- SSID and BSSID of AP it is connected to.

Component Leveling

FAU.1, Behavior of Environmental Objects,

Management: FAU.1

Audit: FAU.1

FAU.1 Behavior of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.3.1

The TSF shall detect when inventoried EUDs exhibit the following behavior:
- An EUD establishes a peer-to-peer connection with any other EUD.
  [selection:
  - An EUD bridges two network interfaces,
  - An EUD uses internet connection sharing,
  - [assignment: other connection types],
  - no other connections types]

Component Leveling

FAU.1, Location of Environmental Objects (Cellular Devices),

Management: FAU.1

Audit: FAU.1

FAU.1 Location of Environmental Objects (Cellular Devices)

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1/CELL

Information on location of device, device MAC address, device type, classification of device, sensors that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s) (in meters).
The TSF shall detect the physical location of cellular devices to within assignment: distance degree of accuracy] of their actual location.

**Component Leveling**

FAU.1, Precise Location of Environmental Objects;

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Precise Location of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.

4.1

Alert generated by detection of rogue device. Description of alert, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue, IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP).

FAU_MAC_EXT.1.1

Alert generated by detection of mac spoofing. Description of alert, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue, IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP).

FAU_MAC_EXT.1.2

Alert generated by detection of mac spoofing. Description of alert, location as labeled by administrator, time elapsed between connection in different locations, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue, IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP).

FAU_SAA.1.1

None

None

FAU_SAA.1.2

None

None

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

**Component Leveling**

FAU.1, Detection of Unauthorized Connections;

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Detection of Unauthorized Connections**

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.5.1

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

**FAU_SIG_EXT Signature-Based Intrusion Detection**

**Family Behavior**

FAU_SIG_EXT FAU_SIG_EXT.1

**Component Leveling**

FAU.1, Signature-Based Intrusion Detection,

**Management:** FAU.1

**Audit:** FAU.1

**FAU.1 Signature-Based Intrusion Detection**

Hierarchical to: No other components.
Dependencies to:

FAU_SIG_EXT.1.1

Alert generated by violation of user defined signature
Name of alert being triggered (as provided when creating the signature),
description of alert (as provided when creating the signature), MAC address of devices involved.
FAU_STG_EXT.1.1/PCAP None None

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

FAU_STG_EXT Protected Audit Event Storage (Packet Captures)

Family Behavior

FAU_STG_EXT FAU_STG_EXT.1/PCAP

Component Leveling

FAU.1, Protected Audit Event Storage (Packet Captures),
Management: FAU.1
Audit: FAU.1

Hierarchical to: No other components.

Dependencies to:

FAU_STG_EXT.1.

The TSF shall be able to transmit the generated packet captures to an external IT entity using a trusted channel according to
FTP_ITC.1.

FAU_STG_EXT.1.2/pcap None None

PCAP

The TSF shall be able to store generated packet captures on the TOE itself.

FAU_STG_EXT.1.3/PCAP

None None

FAU_WID_EXT.1.1 None None

Details about what SSIDs are set as authorized
SSIDs set by administrator as authorized.
FAU_WID_EXT.2 None None

Unauthorized activity description of violation (i.e. whitelisted EUD connected to unauthorized
SSID), identity information of the devices involved.
FAU_WID_EXT.3.1 None None

Alert generated for DoS
MAC Address, device type, and classification AP or EUD attacked.
DoS details (RF or injection based), for injection based, indicate type (i.e., deauth flood).
FAU_WID_EXT.4.1 None None

Information about devices and unauthorized authentication methods
MAC Address, device type, and classification of devices involved, authentication method used.
FAU_WID_EXT.5.1 None None

Information about devices and unauthorized encryption methods
MAC Address, device type, and classification of devices involved, encryption method used.
FAU_WID_EXT.6.1 None None

Information about detected devices
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.6.2 None None

Information about action taken description of violation. the type of containment used, was containment triggered manually or automatically, sensor performing the containment (if wireless), details about the device(s) being contained (classification, device type, MAC address).
FDP_IFC.1.1 None None
FMT_SMF.1.1 None None

Table 4: WIDS/WIPS Auditable Events

Application Note: The auditable events table contains the audit message that for WIDS/WIPS alerts. The Auditable Events table includes optional and objective requirements. The auditing of optional and objective requirements is only required if the vendor chooses to have the requirement evaluated by NIAP. With regards to ‘similar’ type events, ‘similar’ events are multiple occurrences of the same auditable event within some time period where the only significant difference between these events is the timestamp. For example, it is not expected that the TOE generate an individual audit message for every event of the same
kind that occurs within a reasonable time period.

**TSS**

There are no TSS assurance activities for this SFR.

**Guidance**

There are no operational guidance activities for this SFR.

**Tests**

The evaluator shall perform the following test:

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this EP. 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_GEN.2.2/WIDS**

The TSF shall record within each WIDS/WIPS auditable event as [selection: comma separated values (CSV), common log format (CLF), JavaScript Object Notation (JSON), syslog] at least the following information:

- Date and time of the event, type of event, and subject identity (if applicable).
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [auditable events listed in Table 4].

**TSS**

There are no TSS assurance activities for this SFR.

**Guidance**

The evaluator shall verify that the operational guidance describes how to configure the TOE to result in applicable WIDS/WIPS data logging. The evaluator shall verify that the operational guidance provides instructions for any configuration that may be done in regard to logging similar events (e.g., setting thresholds, defining time windows, etc.).

**Tests**

The evaluator shall perform the following test:

The evaluator shall test that the alerts yield the expected WIDS/WIPS audit data in the format selected in the ST for each WIDS/WIPS auditable event in table 4. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

**FPT_FLS.1 Basic Internal TSF Data Transfer Protection**

**FPT_FLS.1.1**

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

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

**Assurance Activity**

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 1:** For each failure mode specified in the ST, the evaluator shall ensure that the TOE attains a secure state after
The TSF shall initiate each failure mode type.

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

FAU_INV_EXT Precise Location of Environmental Objects

Component Leveling
FAU.1, Environmental Inventory,

Management: FAU.1
Audit: FAU.1

FAU.1 Environmental Inventory
Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.1.1
The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

FAU_INV_EXT.1.2
The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

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

Component Leveling
FAU.1, Characteristics of Environmental Objects;

Management: FAU.1
Audit: FAU.1

FAU.1 Characteristics of Environmental Objects
Hierarchical to: No other components.
Dependencies to:

FAU_INV_EXT.2.1
The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE’s wireless sensors.

FAU_INV_EXT.2.2
The TSF shall detect received signal strength and [selection: RF power levels above a predetermined threshold, no other characteristics] of hardware operating within range of the TOE’s wireless sensors.

FAU_INV_EXT.2.3
The TSF shall detect the
- current RF band
- current channel
- MAC Address
- 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.2.4**

The TSF shall detect the following additional details for APs:

- encryption
- number of connected EUDs.

**FAU_INV_EXT.2.5**

The TSF shall detect the following additional details for EUDs:

- **SSID** and **BSSID** of AP it is connected to.

**Component Leveling**

FAU.1, Behavior of Environmental Objects,

**Management: FAU.1**

**Audit: FAU.1**

**FAU.1 Behavior of Environmental Objects**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.3.1**

The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An **EUD** establishes a peer-to-peer connection with any other **EUD**.

[selection:]

- An **EUD** bridges two network interfaces,
- An **EUD** uses internet connection sharing,
- [assignment: other connection types],
- no other connections types

**Component Leveling**

FAU.1, Location of Environmental Objects (Cellular Devices),

**Management: FAU.1**

**Audit: FAU.1**

**FAU.1 Location of Environmental Objects (Cellular Devices)**

Hierarchical to: No other components.

Dependencies to:

**FAU_INV_EXT.4.1/CELL**

The TSF shall detect the physical location of cellular devices to within [assignment: distance degree of accuracy] of their actual location.

**Component Leveling**

FAU.1, Precise Location of Environmental Objects,

**Management: FAU.1**
Audit: FAU.1

FAU.1 Precise Location of Environmental Objects
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.4.1

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

Component Leveling
FAU.1, Detection of Unauthorized Connections,

Management: FAU.1

Audit: FAU.1

FAU.1 Detection of Unauthorized Connections
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.5.1

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

PLACEHOLDER Signal Library

FAU_INV_EXT Detection of Unauthorized Connections
Component Leveling
FAU.1, Environmental Inventory,

Management: FAU.1

Audit: FAU.1

FAU.1 Environmental Inventory
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.1.1

The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.

FAU_INV_EXT.1.2

The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.

FAU_INV_EXT.1.3

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

Component Leveling
FAU.1, Characteristics of Environmental Objects,

Management: FAU.1
Audit: FAU.1

FAU.1 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.2.1

The TSF shall detect information on the current physical location of EUDs and APs within range of the TOE’s wireless sensors.

FAU_INV_EXT.2.2

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

FAU_INV_EXT.2.3

The TSF shall detect the

- current RF band
- current channel
- MAC Address
- 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.2.4

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.5

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU.1, Behavior of Environmental Objects,

Management: FAU.1

Audit: FAU.1

FAU.1 Behavior of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.3.1

The TSF shall detect when inventoried EUDs exhibit the following behavior:

- An EUD establishes a peer-to-peer connection with any other EUD.

[selection:

- An EUD bridges two network interfaces,
- An EUD uses internet connection sharing,
- [assignment: other connection types]
no other connections types

Component Leveling
FAU.1, Location of Environmental Objects (Cellular Devices),
Management: FAU.1
Audit: FAU.1
FAU.1 Location of Environmental Objects (Cellular Devices)
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.4.1/CELL

The TSF shall detect the physical location of cellular devices to within [assignment: distance degree of accuracy] of their actual location.

Component Leveling
FAU.1, Precise Location of Environmental Objects,
Management: FAU.1
Audit: FAU.1
FAU.1 Precise Location of Environmental Objects
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.4.1

The TSF shall detect the physical location of APs and EUDs to within 15 feet of their actual location.

Component Leveling
FAU.1, Detection of Unauthorized Connections,
Management: FAU.1
Audit: FAU.1
FAU.1 Detection of Unauthorized Connections
Hierarchical to: No other components.
Dependencies to:
FAU_INV_EXT.5.1

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

FAU_MAC_EXT Device Impersonation
Family Behavior
FAU_MAC_EXT FAU_MAC_EXT.1
Component Leveling
FAU.1, Device Impersonation;
Management: FAU.1

Audit: FAU.1

FAU.1 Device Impersonation

Hierarchical to: No other components.

Dependencies to:

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-whitelisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors.

FAU_WIP_EXT Wireless Intrusion Prevention

Family Behavior

FAU_WIP_EXT FAU_WIP_EXT.1

Component Leveling

FAU.1, Wireless Intrusion Prevention.

Management: FAU.1

Audit: FAU.1

FAU.1 Wireless Intrusion Prevention

Hierarchical to: No other components.

Dependencies to:

FAU_WIP_EXT.1.1

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

Appendix E - Bibliography

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Part 2: Security Functional Components, CCMB-2017-04-005</td>
</tr>
</tbody>
</table>

80
Appendix F - Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EP</td>
<td>Extended Package</td>
</tr>
<tr>
<td>EUD</td>
<td>End User Device</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>NIAP</td>
<td>National Information Assurance Partnership</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Protocol</td>
</tr>
<tr>
<td>WIDS</td>
<td>Wireless Intrusion Intrusion Detection System</td>
</tr>
<tr>
<td>WIPS</td>
<td>Wireless Intrusion Prevention System</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
</tbody>
</table>