

# PP-Module for Widgets



Version: 1.0  
2020-01-16

**National Information Assurance Partnership**

## Revision History

Version	Date	Comment
1.0	2016-10-06	Initial Release

## Contents

1	Introduction
1.1	Overview
1.2	Terms
1.2.1	Common Criteria Terms
1.2.2	Technical Terms
1.3	Compliant Targets of Evaluation
1.3.1	TOE Boundary
1.4	Use Cases
2	Conformance Claims
3	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
4.3	Security Objectives Rationale
5	Security Requirements
5.0.0.1	Protection of the TSF (FPT)
5.0.0.2	Trusted Paths/Channels (FTP)
5.0.1	Security Audit (FAU)
5.0.2	User Data Protection (FDP)
5.0.3	Security Management (FMT)
5.0.4	Security Audit (FAU)
5.0.5	Security Audit (FAU)
5.0.6	Security Audit (FAU)
5.0.7	Protection of the TSF (FPT)
	Appendix A - An Example Appendix

1.0 National Information Assurance Partnership 2020-01-16 widgets 1.0 2016-10-06 Initial Release

## 1 Introduction

### 1.1 Overview

This Protection Profile Module (PP-Module) describes security requirements for Widgets. This PP-Module is intended to provide a minimal baseline set of requirements that are targeted at mitigating well defined and described threats.

The following content should be included if:

- the TOE implements ""

*This is content that is only applicable to Modules that extend the ND pp.*

This PP-Module contains optional requirements for Widgets, a security product that provides something.

### 1.2 Terms

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

#### 1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs <a href="#">[CC]</a> .
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology	Common Evaluation Methodology for Information Technology Security Evaluation.

(CEM)	
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

## 1.2.2 Technical Terms

Access Point (AP)	A device that provides the network interface that enables wireless client hosts to access a wired network.
End User Device (EUD)	A device that has the ability to process, transmit, and/or store information.
Service Set Identifier (SSID)	The primary name associated with an 802.11 wireless local area network (WLAN).
Wireless Intrusion Detection System (WIDS)	A security product that provides network security administrators with the ability to monitor, collect, and log real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Intrusion Prevention System (WIPS)	A security product that provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Local Area Network (WLAN)	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 widgets. Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS).

The following content should be included if:

- the TOE implements ""  
*Text specific to widgets when Newtork Device is the base.*

A conformant WIDS is a product that can monitor, collect, inspect, and analyze real-time network traffic and alert the administrator of policy violations. WIPS functionality is not required to conform to this PP-Module,

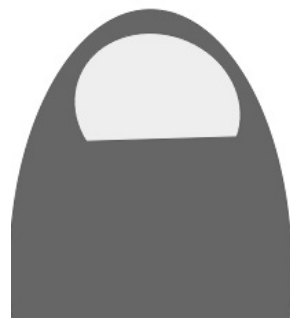
and it is optional for the TOE to have the additional ability to react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.

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

A WIDS/WIPS can be Integrated (be part of the WLAN infrastructure) or Overlay (independent from WLAN) architecture depending on vendor implementation. The two different architectures are illustrated in the [Figure 1](#) figure below.

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

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



Replace this image with a diagram of the Target of Evaluation.

**Figure 1: General TOE**

## 1.4 Use Cases

### [USE CASE 1] Use Case 1

A great use case

## 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.

- , [version](#)

### CC Conformance Claims

This Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5.

### PP Claim

This Module does not claim conformance to any Protection Profile.

### Package Claim

This Module does not claim conformance to any packages.

## 3 Security Problem Description

---

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

### 3.1 Threats

#### T.UNAUTHORIZED\_DISCLOSURE\_OF\_INFORMATION

Unintended/unauthorized disclosure of sensitive information on a protected WLAN, such as sending unencrypted sensitive data. The WIDS will be capable of collecting and analyzing WLAN data to detect unauthorized disclosure of information.

#### T.UNAUTHORIZED\_ACCESS

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

devices may be susceptible to the unauthorized disclosure of information.

**T.DISRUPTION**

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

**3.2 Assumptions**

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

**A.CONNECTIONS**

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

**A.PROPER\_ADMIN**

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

**3.3 Organizational Security Policies**

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

**P.ANALYZE**

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

**4 Security Objectives**

**4.1 Security Objectives for the TOE**

This document does not define any additional SOs.

**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 the assumptions about the environment.

**OE.CONNECTIONS**

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

**OE.PROPER\_ADMIN**

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

**4.3 Security Objectives Rationale**

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

**Table 1: Security Objectives Rationale**

Threat, Assumption, or OSP	Security Objectives	Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	O.SYSTEM_MONITORING	The threat T.Unauthorized_Disclosure_of_Inform is countered by O.SYSTEM_MONITC as this provides for visibility into the network which enables detection of network violations.
	O.WIDS_ANALYZE	The threat T.Unauthorized_Disclosure_of_Inform is countered by O.WIDS_ANALYZE a provides detection of potential violat of approved network usage.
	O.WIPS_REACT	The threat T.Unauthorized_Disclosure_of_Inform is countered by O.WIPS_REACT as tl provides containment of unauthorize and EUDs.
T.UNAUTHORIZED_ACCESS	O.SYSTEM_MONITORING	The threat T.UNAUTHORIZED_ACC countered by O.SYSTEM_MONITOR as this provides for visibility into the

		network which enables detection of unauthorized APs and EUDs.
	O.WIDS_ANALYZE	The threat <a href="#">T.UNAUTHORIZED_ACCESS</a> countered by O.WIDS_ANALYZE as this provides detection of potential violations of approved network usage.
	O.WIPS_REACT	The threat <a href="#">T.UNAUTHORIZED_ACCESS</a> countered by O.WIPS_REACT as this provides containment of unauthorized APs and EUDs.
	O.TOE_ADMINISTRATION	The threat <a href="#">T.UNAUTHORIZED_ACCESS</a> countered by O.TOE_ADMINISTRATION.
<a href="#">T.DISRUPTION</a>	O.SYSTEM_MONITORING	The threat <a href="#">T.DISRUPTION</a> is countered by O.SYSTEM_MONITORING as this provides for visibility into the network which enables detection of DoS attacks.
	O.WIDS_ANALYZE	The threat <a href="#">T.DISRUPTION</a> is countered by O.WIDS_ANALYZE as this provides for detection of potential violations of approved network usage.
	O.WIPS_REACT	The threat <a href="#">T.DISRUPTION</a> is countered by O.WIPS_REACT as this provides containment of unauthorized APs and EUDs.
<a href="#">A.CONNECTIONS</a>	<a href="#">OE.CONNECTIONS</a>	The operational environment object <a href="#">OE.CONNECTIONS</a> is realized through <a href="#">A.CONNECTIONS</a> .
<a href="#">A.PROPER_ADMIN</a>	<a href="#">OE.PROPER_ADMIN</a>	The operational environment object <a href="#">OE.PROPER_ADMIN</a> is realized through <a href="#">A.PROPER_ADMIN</a> .
<a href="#">A.PHYSICAL_PROTECTION</a>	O.WIDS_ANALYZE	Case I wanted to show an example.
<a href="#">P.ANALYZE</a>	O.WIDS_ANALYZE	The organizational security policy <a href="#">P.ANALYZE</a> is facilitated through O.WIDS_ANALYZE.

## 5 Security Requirements

<https://www.niap-ccevs.org/Profile/Info.cfm?PPID=440&id=440>

### 5.0.0.1 Protection of the TSF (FPT)

#### FPT\_ITT.1 Basic Internal TSF Data Transfer Protection

FPT\_ITT.1.1

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

#### Evaluation Activities ▼

[FPT\\_ITT.1:](#)

The evaluator shall perform the evaluation activity specified in NDcPP for this SFR.

### 5.0.0.2 Trusted Paths/Channels (FTP)

#### FTP\_ITC.1 Inter-TSF trusted channel

FTP\_ITC.1.1

The TSF shall **be capable of using** [selection: *IPsec, SSH, TLS, 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 be 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.

## Evaluation Activities ▼

### *FTP\_ITC.1:*

*The evaluator shall perform the evaluation activity specified in NDcPP for this SFR, with the inclusion of test 4, which is objective in NDcPP.*

When this PP-Module extends the Network Device cPP, the TOE type for the overall TOE is still WIDS/WIPS products. HHHHHHHHYYY. Specific to the ND base. FTP base reasons

## 5.0.1 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.

## Evaluation Activities ▼

### *FAU\_ARP.1:*

#### **TSS**

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

#### **Guidance**

*The evaluator shall use the operational guidance for instructions on where the alerts generated are displayed within the WIDS interface. If 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**

- **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:** *[conditional] If capturing of raw frames was selected, verify that the packet capture was triggered and stored as appropriate.*

### FAU\_ARP\_EXT.2 Security Alarm Filtering

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

## Evaluation Activities ▼

### [FAU\\_ARP\\_EXT.2:](#)

#### **TSS**

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

#### **Guidance**

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

#### **Tests**

##### • **Test 1:**

- The evaluator shall use the operational guidance to enable/disable detection of available detection capabilities through the WIDS administrator interface. The evaluator shall then generate traffic that would successfully trigger the alert. The evaluator should verify that the TOE generated the alert. 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.1.1/WIDS

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

- a. Start-up and shutdown of the audit functions;
- b. All auditable events for the [not specified] level of audit;
- c. [Auditable events listed in [Table 2](#);
- d. Failure of wireless sensor communication].

**Table 2: Auditable Events**

Requirement	Auditable Events	Additional Audit Record Contents
<a href="#">FAU_ANO_EXT.1</a>	None	None
<a href="#">FAU_ARP.1</a>	Actions taken due to potential security violations	None
<a href="#">FAU_ARP_EXT.2</a>	None	None
<a href="#">FAU_GEN.1/WIDS</a>	None	None
<a href="#">FAU_IDS_EXT.1</a>	None	None
<a href="#">FAU_INV_EXT.1</a>	Presence of whitelisted device	Type of device (AP or EUD), MAC Address
<a href="#">FAU_INV_EXT.2</a>	None	None
<a href="#">FAU_INV_EXT.3</a>	None	None
<a href="#">FAU_INV_EXT.4</a>	Location of AP or EUD	MAC Address, device type, classification of device, sensor(s) that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s)
<a href="#">FAU_INV_EXT.5</a>	None	None
<a href="#">FAU_MAC_EXT.1</a>	None	None
<a href="#">FAU_SAA.1</a>	None	None
<a href="#">FAU_SIG_EXT.1</a>	None	None
<a href="#">FAU_STG_EXT.1/PCAP</a>	None	None
<a href="#">FAU_WID_EXT.1</a>	Detection of rogue AP or EUD	None



	Detection of unauthorized SSID	None
FAU_WID_EXT.2	Sensor wireless transmissions capabilities.	Wireless transmission capabilities are turned on.
FAU_WID_EXT.3	None	None
FAU_WID_EXT.4	Use of an unauthorized authentication schemes	MAC Address, device type, classification of the device, authentication method used
FAU_WID_EXT.5	Use of an unauthorized encryption schemes	MAC Address, device type, classification of the device, encryption method used
FAU_WID_EXT.6	Detection of network devices operating in selected RF bands	Frequency band, channel used within frequency band, identification information (MAC address if applicable or other similar unique ID), device technology (i.e., cellular), sensor(s) that detected devices
FAU_WID_EXT.7	None	None
FAU_WID_EXT.8	None	None
FAU_WIP_EXT.1	Isolation of AP or EUD	Description of violation, type of containment used, was containment triggered manually or automatically, sensor performing the containment (if wireless), details about the device (s) being contained (classification, device type, MAC address).
FDP_IFC.1	None	None
FMT_SMF.1/WIDS	None	None
FPT_FLS.1	Information about failure.	Indication that there was a failure, type of failure, device that failed, and time of failure.
FPT_ITT.1	None	None
FTP_ITC.1	None	None

**Application Note:** The auditable events defined in [Table 2](#) are for the SFRs that are explicitly defined in this PP-Module and are intended to extend FAU\_GEN.1 in the Base-PP. The events in the [Table 2](#) should be combined with those of the ND cPP in the context of a conforming Security Target.

#### FAU\_GEN.1.2/WIDS

The TSF shall record within each audit record 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 2](#)*].

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

## Evaluation Activities ▼

### [FAU\\_GEN.1/WIDS:](#)

#### **TSS**

*There are no TSS assurance activities for this SFR.*

#### **Guidance**

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

#### **Tests**

*The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this PP-Module. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide,*

and that the fields in each audit record have the proper entries.

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

## FAU\_GEN\_EXT.1 Intrusion Detection System - Reporting Methods

### FAU\_GEN\_EXT.1.1

The TSF shall provide [**selection:**

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

].

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

### FAU\_GEN\_EXT.1.2

The TSF shall provide the ability to import data from the system: [**selection:** custom API, Syslog, common log format, CSV, [**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.

## Evaluation Activities ▼

### FAU\_GEN\_EXT.1:

#### TSS

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

#### Guidance

#### Tests

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

#### • Test 1:

- **Step 1:** Deploy a whitelisted AP and connect it to the protected wired infrastructure via wire.
- **Step 2:** Confirm that the TSF can observe and capture traffic and events generated by the AP.
- **Step 3:** Confirm that the TSF can utilize SNMP and Syslog reporting mechanisms.
- **Step 4:** Verify that the TSF can import and export observable event data in any of the following formats:
  - comma separated values (CSV)
  - common log format (CLF)
  - JavaScript Object Notation (JSON)
  - syslog

## FAU\_IDS\_EXT.1 Intrusion Detection System - Intrusion Detection Methods

### FAU\_IDS\_EXT.1.1

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

**Application Note:** At least one detection method must be selected. If multiple detection methods are supported, each method supported shall be selected.

If anomaly-based detection is selected, then FAU\_ANO\_EXT.1 shall be included in the ST. If signature-based detection is selected, then FAU\_SIG\_EXT.1 shall be included in the ST.

## Evaluation Activities ▼

### FAU\_IDS\_EXT.1:

#### TSS

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

#### Guidance

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

#### Tests

Depending on the detection technique used by the TOE, the evaluator shall confirm and note the

## FAU\_INV\_EXT.1 Environmental Inventory

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.

**Application Note:** 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.

## Evaluation Activities ▼

[FAU\\_INV\\_EXT.1:](#)

### TSS

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

### Guidance

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

### Tests

#### • Test 1:

- **Step 1:** Per guidance in FMT\_SMF.1, add MAC Addresses for an AP and EUD to the whitelist.
- **Step 2:** Deploy the AP and EUD that were added to whitelist within the range of the TOE's sensors.
- **Step 3:** Verify that the devices are classified as authorized.
- **Step 4:** Remove the EUD from the whitelist.
- **Step 5:** Verify that the EUD is classified as unauthorized.
- **Step 6:** Remove the AP from the whitelist.
- **Step 7:** Verify that the AP is classified as unauthorized.

#### • Test 2:

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

#### • Test 3:

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

## FAU\_INV\_EXT.2 Characteristics of Environmental Objects

FAU\_INV\_EXT.2.1

The TSF shall detect the

- current RF band
- current channel
- MAC Address
- classification of APs and EUDs
- **[selection: [assignment: other details], no other details]**

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

FAU\_INV\_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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

FAU\_INV\_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

## Evaluation Activities ▼

[FAU\\_INV\\_EXT.2:](#)

### TSS

*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

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

## 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,
- An EUD uses internet connection sharing,
- [assignment: other connection types],
- no other connections types

].

**Application Note:** For this requirement, it is acceptable for the WIDS to use a generic terms 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 type of connection does not have to be specific.

## Evaluation Activities ▼

[FAU\\_INV\\_EXT.3:](#)

### 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

- **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\_INV\_EXT.4 Location of Environmental Objects

FAU\_INV\_EXT.4.1

The TSF shall detect information on the current physical location of EUDs and 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.

FAU\_INV\_EXT.4.2

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.4.3

The TSF shall detect the physical location of APs and EUDs to within [**assignment:** *value equal or less than 15*] feet of their actual location.

#### Evaluation Activities ▼

[FAU\\_INV\\_EXT.4:](#)

BBBB

##### TSS

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

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

##### Guidance

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

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

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

###### • 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.

###### • Test 2:

- **Step 1:** Deploy an AP within range of the sensors.
- **Step 2:** Check the WIDS user interface for a list of detected APs and EUDs.
- **Step 3:** Verify that the current received signal strength is part of the information presented on the WIDS user interface about the APs and EUDs.

###### • Test 3:

- **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\_SAA.1 Potential Violation Analysis

FAU\_SAA.1.1

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

FAU\_SAA.1.2

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

- Accumulation or combination of [**assignment:** *subset of defined auditable events*] known to indicate a potential security violation;
- [*other potential security violations as defined by Table 3*].

Potential Security Violation	Additional Information
Detection of authorized EUD establishing peer-to-peer connection with any other EUD.	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.
Detection of EUD bridging two network interfaces.	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.
Detection of packet flooding/DoS/DDoS.	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.
Detection of ICS connection.	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.
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).
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), location as labeled by administrator.
Alert generated by violaton 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.
Detection of rogue AP.	Identity information of the devices involved.
Detection of malicious EUD.	Identity information of the devices involved.
Detection of traffic with excessive transmit power level.	Identity information of the devices involved.
Detection of active probing.	Identity information of the devices involved.
Detection of MAC spoofing.	Identity information of the devices involved.
Detection of RF-based denial of service.	MAC Address, device type, classification AP or EUD attacked.
Detection of deauthentication flooding.	MAC Address, device type, and classification AP or EUD attacked.
Detection of disassociation flooding.	MAC Address, device type, and classification AP or EUD attacked.
Detection of request-to-send/clear-to-send abuse.	MAC Address, device type, and classification AP or EUD attacked.
Detection of unauthorized authentication scheme use.	
Detection of unauthorized encryption scheme use.	

Table 3: Potential Security Violations

## Evaluation Activities ▼

### [FAU\\_SAA.1:](#)

#### **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 and detection of potential malicious events is tested through the ability to detect intrusions in other SFRs.*

## **FAU\_WID\_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects**

### FAU\_WID\_EXT.1.1

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

**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.

### FAU\_WID\_EXT.1.3

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

**Application Note:** FMT\_SMF.1 defines the subset of authorized SSID(s).

## Evaluation Activities ▼

### [FAU\\_WID\\_EXT.1:](#)

#### **TSS**

*The evaluator shall verify that the TSS describes how the TOE can detect rogue APs and whether the classification rules are configurable. The evaluator shall verify that the TSS includes how the TOE determines if a given SSID is authorized.*

#### **Guidance**

*If classification rules for rogue APs are configurable, the evaluator shall verify that the operational guidance contains instructions for configuring the classification rules. The evaluator shall verify that the operational guidance provides instructions on how to configure SSIDs as authorized.*

#### **Tests**

- **Test 1:**
  - **Step 1:** The evaluator shall configure the AP classification rules, if supported.
  - **Step 2:** Deploy an AP that would be detected as rogue by the classification rules.
  - **Step 3:** Verify that the AP gets correctly classified.
- **Test 2:** For each test below the evaluator shall verify that the TOE detects and appropriately classifies the APs and EUDs.
  - **Test 2.1:** Deploy a non-whitelisted AP in the area of the WIDS sensor, but take no action against the network.
  - **Test 2.2:** Deploy a non-whitelisted AP in the area of the WIDS sensor and connect it to the internal wired infrastructure (optional for overlay WIDS).
  - **Test 2.3:** Connect a whitelisted EUD to a non-whitelisted AP.
  - **Test 2.4:** Connect a non-whitelisted EUD to a whitelisted AP.
  - **Test 2.5:** Launch an attack against authorized AP with an unauthorized EUD.

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

- **Test 3: Unauthorized SSID, Unauthorized Connections - 2.4 GHz band**
  - **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.
- **Test 4: Unauthorized SSID, Unauthorized Connections - 5 GHz band**



- **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.

## FAU\_WID\_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring

### FAU\_WID\_EXT.2.1

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

- 2.4 GHz
- 4.9/5.0 GHz

[**selection:**

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

].

**Application Note:** If "nonsimultaneously" is selected, then "Define the amount of time sensor monitors a specific channel" 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 the FAU\_WID\_EXT SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

### FAU\_WID\_EXT.2.2

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

**Application Note:** If "can be configured to prevent transmission of data" is selected then "Enable/Disable transmission of data by wireless sensor" shall be selected in FMT\_SMF.1.

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

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP\_IFC.1> and defined through the FAU\_WID\_EXT SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

### FAU\_WID\_EXT.2.3

The TSF shall 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*

].

**Application Note:** "Authorized" EUDs/APs are those that are assigned to the whitelist as defined by FMT\_SMF.1.

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.2.4

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



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

## Evaluation Activities ▼

### [FAU\\_WID\\_EXT.2:](#)

#### **TSS**

*The evaluator shall verify that the TSS includes which channels the TOE can detect and monitor. Additionally, the TSS shall include whether the TOE simultaneously or nonsimultaneously monitors network traffic across these channels. The evaluator shall verify that the TSS includes information on if the sensors are completely passive, by default, or if the sensors ability to transmit data is configurable. 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 review the operational guidance for how to configure the TOE to monitor the channels as selected in the SFR. If the sensor ability to transmits data is configurable, the evaluator shall review the operational guidance for how to disable wireless transmissions from the sensor. The TOE shall have the ability to perform stateful frame inspection and log attacks spanning multiple frames. The evaluator shall verify that the operational guidance provides instructions on how to specify and confirm that stateful frame capture and inspection is being performed.*

#### **Tests**

##### **Channels Monitored**

- **Test 1:** Channels on On 5GHz band
  - **Step 1:** Configure the TSF to monitor the channels as selected in the SFR.
  - **Step 2:** Deploy an AP on at least 2 different channels within the regulatory domain on 5GHz band.
  - **Step 3:** Deploy an 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.

##### **Wireless Sensor Transmission of Data**

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

- **Test 1:**
  - **Step 1:** Boot a sensor and using the signal analyzer observe to check if any emanations are coming from the sensor.
  - **Step 2:** Verify that the signal analyzer does not pick up emanations from the sensor.
- **Test 2:**
  - **Step 1:** During normal sensor operations, observe the analyzer for about 10 minutes to check if any emanations are coming from the sensor.
  - **Step 2:** Verify that the signal analyzer does not pick up emanations from the sensor.
- **Test 1: MAC Spoofing**
  - **Step 1:** Spoof mac address of whitelist EUD connected to a whitelisted AP on a second EUD.
  - **Step 2:** Connect EUD with spoofed MAC address to another whitelisted AP while the valid EUD it is spoofing is connected to the first AP.
  - **Step 3:** Verify that the TSF detected the MAC spoofing.
- **Test 2: MAC Spoofing**
  - **Step 1:** Spoof mac address of whitelist AP on a second AP.
  - **Step 2:** Verify that the TSF detected the MAC spoofing.
- **Test 3: Active Probing**
  - **Step 1:** Perform an active scan on the subnet of the WLAN.
  - **Step 2:** Record tools used and type of scan performed.
  - **Step 3:** Verify that the TSF detects the active probing.

- **Test 4: Point-to-Point Wireless Bridges**
  - **Step 1:** Setup a point-to-point wireless bridge using whitelisted APs in the range of the wireless sensors.
  - **Step 2:** Verify that the TSF detects the bridge.
- **Test 5: NULL Client Associations**
  - **Step 1:** Deploy whitelisted AP.
  - **Step 2:** Configure the AP to have null SSID.
  - **Step 3:** Attempt to connect a whitelisted EUD to the AP without supplying the correct AP SSID.
  - **Step 4:** Verify that the AP does not permit the EUD to complete an association by returning a Probe Request.
  - **Step 5:** If an association does occur, confirm that an alert is triggered due to a violation of policy.

#### Stateful Frame Inspection

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

### FAU\_WID\_EXT.3 Wireless Intrusion Detection - Denial of Service

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].

#### Evaluation Activities ▼

[FAU\\_WID\\_EXT.3:](#)

##### 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

- **Test 1: RF-based DoS**
  - **Step 1:** Deploy a whitelisted AP and configure to stay in a particular channel.
  - **Step 2:** Connect a whitelisted EUD to the AP.
  - **Step 3:** Use an RF Jammer or signal generator on the same frequency as the AP and EUD to create a RF-based DoS.
  - **Step 4:** Verify that the TOE detects the RF-based DoS.
- **Test 2: Deauthentication Flood**
  - **Step 1:** Deploy whitelisted AP and configure to a set channel.
  - **Step 2:** Connect a whitelisted EUD to the AP.
  - **Step 3:** Send an flood of deauthentication frames to the EUD using the MAC address of whitelisted AP it is connected to.
  - **Step 4:** Verify that the TSF detects the deauthentication flood.
- **Test 3: Deauthentication Flood**
  - **Step 1:** Deploy whitelisted AP and configure to a set channel.
  - **Step 2:** Connect a whitelisted EUD to the AP.
  - **Step 3:** Send an flood of deauthentication frames with the MAC address of whitelisted AP as the source and destination as a broadcast.
  - **Step 4:** Verify that the TSF detects the deauthentication flood.
- **Test 4: Dissasociation Flood**
  - **Step 1:** Deploy whitelisted AP and configure to a set channel.
  - **Step 2:** Connect two whitelisted EUDs to the AP.
  - **Step 3:** Send an flood of CTS frames to reserve RF medium.
  - **Step 4:** Verify that the TSF detects the CTS abuse.

### 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.4:](#)**TSS**

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

**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 TOE, per FMT\_SMF.1, with 802.1x authentication as the only mode of authorized WLAN authentication scheme.

- **Test 1:**
  - **Step 1:** Deploy a whitelisted AP with open authentication.
  - **Step 2:** Connect a whitelisted EUD to AP.
  - **Step 3:** Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.
- **Test 2:**
  - **Step 1:** Deploy a whitelisted AP that uses pre-shared key authentication.
  - **Step 2:** Connect a whitelisted EUD to AP.
  - **Step 3:** 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 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.

[FAU\\_WID\\_EXT.5:](#)**TSS**

The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized WLAN encryption schemes are used. The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized APs and EUDs send or receive unencrypted data.

**Guidance**

There are no operational guidance activities.

**Tests**

- **Test 1:**
  - **Step 1:** Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.
  - **Step 2:** Deploy a whitelisted AP with no encryption.
  - **Step 3:** Connect a whitelisted EUD to AP.
  - **Step 4:** Verify that the TOE detects the AP and the EUD using unauthorized encryption schemes.
- **Test 2:**
  - **Step 1:** Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.
  - **Step 2:** Deploy a whitelisted AP that uses TKIP encryption only.
  - **Step 3:** Connect a whitelisted EUD to AP.
  - **Step 4:** Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.
- **Test 3:**
  - **Step 1:** Deploy a whitelisted AP with no encryption.
  - **Step 2:** Connect a whitelisted EUD to AP and generate traffic.
  - **Step 3:** Verify that the TOE detects unencrypted data frames being sent between the whitelisted AP and EUD.
  - **Step 4:** Connect a non-whitelisted EUD to AP and generate traffic.
  - **Step 5:** Verify that the TSF detects unencrypted data frames being sent between the

whitelisted AP and non-whitelisted EUD.

- **Test 4:**
  - **Step 1:** Deploy a non-whitelisted AP with no encryption.
  - **Step 2:** Connect a whitelisted EUD to AP and generate traffic.
  - **Step 3:** Verify that the TSF detects unencrypted data frames being between the non-whitelisted AP and whitelisted EUD.

## 5.0.2 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 the FAU\_WID\_EXT SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

### Evaluation Activities ▼

*FDP\_IFC.1:*

#### **TSS**

*There are no TSS 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 sensor's operating channel for all IEEE 802.11 a, b, g, n, ac frame types and subtypes from/to the following:
    - authorized APs and authorized EUDs
    - authorized APs and unauthorized EUDs
    - unauthorized APs and authorized EUDs
  - Verify that there are frames from all the types and subtypes in the capture.

## 5.0.3 Security Management (FMT)

### FMT\_SMF.1/WIDS Specification of Management Functions (WIDS)

FMT\_SMF.1.1/WIDS

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

- Define an inventory of authorized APs based on 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 anomaly activity,
  - Define classification rules to detect rogue APs,
  - **[selection:** Enable, Disable] transmission of data by wireless sensor,
  - Define attack signatures,
  - Define rules for overwriting previous packet captures,
  - Define the amount of time sensor monitors a specific **[selection:** frequency, channel],
  - 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](#), then "Definition of anomaly activity" shall be selected.

If "can be configured to prevent transmission of data" is selected in [FAU\\_WID\\_EXT.2](#) then "Enable/Disable transmission of data by wireless sensor" shall be selected.

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

#### Evaluation Activities ▼

[FMT\\_SMF.1/WIDS](#):

##### **TSS**

*The evaluator shall 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**

- **Test 1:**
  - **Step 1:** Deploy a whitelisted AP and connect it to the protected wired infrastructure via wire.
  - **Step 2:** Confirm that the TSF can observe and capture traffic and events generated by the AP.
  - **Step 3:** Verify that the TSF can be configured to capture traffic on a specific channel for specific interval of time, and assign a specified frequency and time interval.
  - **Step 4:** Confirm that the TSF" /> remains on the frequency and channel for the time period specified.

### 5.0.4 Security Audit (FAU)

#### **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](#) must be included in the ST.

#### Evaluation Activities ▼

[FAU\\_WID\\_EXT.6](#):

##### **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.7 Wireless Intrusion Detection - Wireless Spectrum Analysis**

FAU\_WID\_EXT.7.1

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

#### Evaluation Activities ▼

[FAU\\_WID\\_EXT.7:](#)

#### **TSS**

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

#### **Guidance**

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

#### **Tests**

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

## 5.0.5 Security Audit (FAU)

### FAU\_ANO\_EXT.1 Anomaly-Based Intrusion Detection

FAU\_ANO\_EXT.1.1

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

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

] and the following network protocol fields:

- all management and control frame header elements.

FAU\_ANO\_EXT.1.2

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

**Application Note:** The "baseline" and "anomaly" can be something manually defined/configured by a TOE administrator (or importing definitions), or something that the TOE is able to automatically define/create by inspecting network traffic over a period of time (a.k.a. "profiling").

### Evaluation Activities ▼

[FAU\\_ANO\\_EXT.1:](#)

#### **TSS**

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

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

#### **Guidance**

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

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

#### **Tests**

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

### FAU\_SIG\_EXT.1 Signature-Based Intrusion Detection

FAU\_SIG\_EXT.1.1

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

### Evaluation Activities ▼

[FAU\\_SIG\\_EXT.1:](#)

#### **TSS**

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

#### **Guidance**

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



customization options that are available.

#### Tests

- **Test 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)

#### 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.

#### Evaluation Activities ▼

##### [FAU\\_STG\\_EXT.1/PCAP:](#)

###### TSS

The evaluator shall verify that the TSS includes the list of trusted channels (as specified in [FTP\\_ITC.1](#)) available in the TSF to transmit packet captures to an external entity. The evaluator shall verify that the TSS describes the ability of the TOE to store packet capture data within itself, how much storage space is available for packet capture data and where that data is stored. 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

The evaluator shall verify that the operational guidance provides instructions on how to configure the trusted channel. 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 configure packet captures according to the guidance specified. The evaluator shall then trigger an event that starts a capture and verify through the tests in [FTP\\_ITC.1](#) that the captured traffic being sent to the external device is being sent through a trusted channel.
- **Test 2:** The evaluator shall configure packet captures to be stored on the TSF according to the guidance specified. The evaluator shall then trigger an event that starts a capture and verify that the packet capture was stored on the TSF.
- **Test 3:** The evaluator shall define packet data retention and deletion rules on the TSF according to the guidance specified and test the functionality of the specified rules.

## 5.0.6 Security Audit (FAU)

### 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.

#### Evaluation Activities ▼

##### [FAU\\_INV\\_EXT.5:](#)

###### TSS

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

###### Guidance

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

## Tests

- **Test 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 user interface for a list of detected APs and EUDs.
  - **Step 4:** Verify that the rogue AP is detected and an alert generated on the detection of an AP connected to the protected wired infrastructure.

## FAU\_INV\_EXT.6 Signal Library

FAU\_INV\_EXT.6.1

The TSF shall include a signal library.

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

## Evaluation Activities ▼

[FAU\\_INV\\_EXT.6:](#)

### TSS

*There are no TSS assurance activities for this SFR.*

### Guidance

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

### Tests

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

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

## FAU\_MAC\_EXT.1 Device Impersonation

FAU\_MAC\_EXT.1.1

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

**Application Note:** The intent of this SFR is to detect MAC spoofing where an attacker is able to cause the 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.

## Evaluation Activities ▼

[FAU\\_MAC\\_EXT.1:](#)

### TSS

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

### Guidance

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

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

### Tests

- **Test 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-overlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).
  - **Step 4:** Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the 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.
- **Test 2:**
- **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:** Connect a whitelisted EUD to AP.
  - **Step 4:** 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-overlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).
  - **Step 5:** Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the 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\_WIP\_EXT.1 Wireless Intrusion Prevention

### FAU\_WIP\_EXT.1.1

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

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

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

## Evaluation Activities ▼

### FAU\_WIP\_EXT.1:

#### TSS

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

#### Guidance

There are no operational guidance activities for this SFR.

#### Tests

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

- **Test 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.

## 5.0.7 Protection of the TSF (FPT)

### 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.

## Evaluation Activities ▼

### FPT\_FLS.1:

#### TSS

The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall examine the TSS section to ensure that all failure modes specified in the ST are described.

**Guidance**

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

**Tests**

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

# Appendix A - An Example Appendix

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. [CC] Common Criteria for Information Technology Security Evaluation -

- [Part 1: Introduction and General Model](#), CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- [Part 2: Security Functional Components](#), CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- [Part 3: Security Assurance Components](#), CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.