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

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

(TOE)	

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 Intrustion Detection System (WIDS)	A security product that provides network security administrators with the ability to monitor, collect, and log real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Intrustion Prevention System (WIPS)	A security product that provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Local Area Network (WLAN)	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 Network Device is a Base-PP:
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.

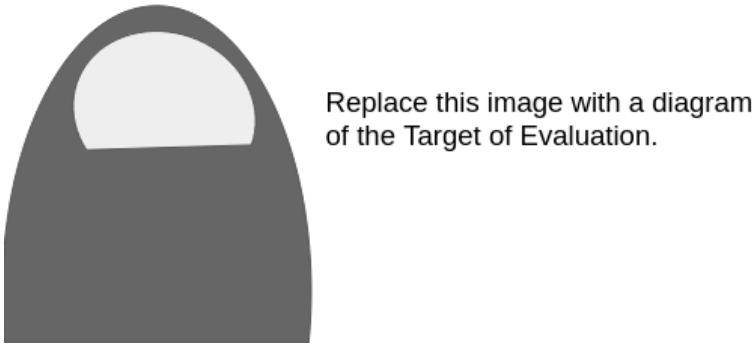

Figure 1: General TOE

1.4 Use Cases

[USE CASE 1] Use Case 1

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this , as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

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

PP Claim

This does not claim conformance to any Protection Profile.

Package Claim

This does not claim conformance to any packages.

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 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

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

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

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.

O.TOE_ADMINISTRATION
To address the threat of unauthorized administrator access that is defined in the base PP, Conformant TOEs will provide the functions necessary for an administrator to configure the WIDS Capabilities of the TOE.

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 log or produce an alert upon discovery of a problem reported via the self-test mechanism.

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.

4.2 Security Objectives for the Operational Environment

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

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

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

4.3 Security Objectives Rationale

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

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_Informati is countered by O.SYSTEM_MONITORING as this provides for visibility into the network which enables detection of network violations.
	O.WIDS_ANALYZE	The threat T.Unauthorized_Disclosure_of_Informati is countered by O.WIDS_ANALYZE as tl provides detection of potential violations approved network usage.
	O.WIPS_REACT	The threat T.Unauthorized_Disclosure_of_Informati

		is countered by O.WIPS_REACT as this provides containment of unauthorized AP and EUDs.
T.UNAUTHORIZED_ACCESS	O.SYSTEM_MONITORING	The threat T.UNAUTHORIZED_ACCESS is countered by O.SYSTEM_MONITORING as this provides for visibility into the network which enables detection of unauthorized APs and EUDs.
	O.WIDS_ANALYZE	The threat T.UNAUTHORIZED_ACCESS is countered by O.WIDS_ANALYZE as th provides detection of potential violations approved network usage.
	O.WIPS_REACT	The threat T.UNAUTHORIZED_ACCESS is countered by O.WIPS_REACT as this provides containment of unauthorized AP and EUDs.
	O.TOE_ADMINISTRATION	The threat T.UNAUTHORIZED_ACCESS is countered by O.TOE_ADMINISTRATION.
T.DISRUPTION	O.SYSTEM_MONITORING	The threat T.DISRUPTION is countered O.SYSTEM_MONITORING as this provides for visibility into the network which enables detection of DoS attacks.
	O.WIDS_ANALYZE	The threat T.DISRUPTION is countered O.WIDS_ANALYZE as this provides for detection of potential violations of approved network usage.
	O.WIPS_REACT	The threat T.DISRUPTION is countered O.WIPS_REACT as this provides containment of unauthorized APs and EUDs.
A.CONNECTIONS	OE.CONNECTIONS	The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.
A.PROPER_ADMIN	OE.PROPER_ADMIN	The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.
A.PHYSICAL_PROTECTION (from Network Device)	O.WIDS_ANALYZE	Cuase I wanted to show an example.
P.ANALYZE	O.WIDS_ANALYZE	The organizational security policy P.ANALYZE is facilitated through O.WIDS_ANALYZE.

5 Security_Requirements

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

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

5.1 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 following sections describe any modifications that the ST author must make to the SFRs defined in the ND PP in addition to what is mandated by Section 5.4 TOE Security Functional Requirements.

5.1.1 Modified SFRs

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

5.2 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 Activity

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

5.3 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 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 Activity

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

5.4 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.

5.5 TOE Security Functional Requirements Rationale

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

Table 2: SFR Rationale

OBJECTIVE	ADDRESSED BY	RATIONALE
O.SYSTEM_MONITORING	FAU_GEN.1/WIDS	Good reasons
	FAU_STG_EXT.1/PCAP	Good reasons
O.WIDS_ANALYZE	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(OPTIONAL), FAU_INV_EXT.4(OPTIONAL), FAU_INV_EXT.5(OPTIONAL), FAU_MAC_EXT.1(OPTIONAL), FAU_SIG_EXT.1(OPTIONAL), FAU_WID_EXT.6(OPTIONAL), FAU_WID_EXT.7(OPTIONAL), FAU_WID_EXT.8(OPTIONAL)	Good reasons
O.WIPS_REACT	FAU_WIP_EXT.1 (OPTIONAL)	Good reasons
O.TOE_ADMINISTRATION	FMT_SMF.1/WIDS	Good reasons
O.INSECURE_OPERATIONS	FPT_FLS.1(Optional)	Good reasons
O.TRUSTED_COMMUNICATIONS	FPT_ITT.1, FTP_ITC.1	Good reasons

6 Consistency Rationale

6.1 Protection Profile for Network Devices

6.1.1 Consistency of TOE Type

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

6.1.2 Consistency of Security Problem Definition

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

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	This threat is consistent with ND
T.UNAUTHORIZED_ACCESS	HHHHHHHHYYY.
T.DISRUPTION	This threat is consistent with ND
A.CONNECTIONS	This assumption is consistent with ND
A.PROPER_ADMIN	This assumption is consistent with ND
P.ANALYZE	Just because ND

6.1.3 Consistency of Objectives

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

PP-Module TOE Objective	Consistency Rationale
O.SYSTEM_MONITORING	Just because ND
O.WIDS_ANALYZE	Just because ND
O.WIPS_REACT	Just because ND
O.TOE_ADMINISTRATION	Just because ND
O.INSECURE_OPERATIONS	Just because ND
O.TRUSTED_COMMUNICATIONS	Just because ND

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

PP-Module Operational Environment Objective	Consistency Rationale
OE.CONNECTIONS	Just because ND
OE.PROPER_ADMIN	Just because ND

6.1.4 Consistency of Requirements

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

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FPT_ITT.1	Some really good reasons
FTP_ITC.1	FTP base reasons
Mandatory SFRs	
FAU_ARP.1	
FAU_ARP_EXT.2	

FAU_GEN.1/WIDS	Specific to the ND base.
FAU_GEN_EXT.1	
FAU_IDS_EXT.1	
FAU_INV_EXT.1	
FAU_INV_EXT.2	
FAU_INV_EXT.3	
FAU_INV_EXT.4	
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/WIDS	
Optional SFRs	
FAU_WID_EXT.6	
FAU_WID_EXT.7	
Selection-based SFRs	
FAU_ANO_EXT.1	
FAU_SIG_EXT.1	
FAU_STG_EXT.1/PCAP	
Objective SFRs	
FAU_INV_EXT.5	
FAU_INV_EXT.6	
FAU_MAC_EXT.1	
FAU_WIP_EXT.1	
FPT_FLS.1	

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

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 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 theTSF 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 Activity

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

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

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

A.2 Objective Requirements

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 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 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 exisiting signal library.

Evaluation Activity

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 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).

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-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.*
- ***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-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_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.

Evaluation 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.*

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 Activity

TSS
The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall 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.*

A.3 Objective Requirements

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 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 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 exisiting signal library.

Evaluation Activity

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 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).

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-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.*
- ***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-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_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.

Evaluation 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.*

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 Activity

TSS
The evaluator shall review the TSS section to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator shall 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 B - Selection-based SFRs

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

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

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

] and the following network protocol fields:

- all management and control frame header elements.

FAU_ANO_EXT.1.2 The TSF shall support the definition of anomaly activity through [**selection**: *manual configuration by administrators*, *automated configuration*].

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

Evaluation 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.

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 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 theTSS.*
  - ***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 theTOE 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 Activity

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 theTSF 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.*

Appendix C - 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.

C.1 Background and Scope

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

Functional Class	Functional Components

C.2 Extended Component Definitions

FAU_ARP_EXT Security Alarm Filtering

Component Leveling

FAU_ARP_EXT.2, Security Alarm Filtering,

Management: FAU_ARP_EXT.2

Audit: FAU_ARP_EXT.2

FAU_ARP_EXT.2 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_GEN_EXT Reporting Methods

Component Leveling

FAU_GEN_EXT.1, Intrusion Detection System – Reporting Methods,

Management: FAU_GEN_EXT.1

Audit: FAU_GEN_EXT.1

FAU_GEN_EXT.1 Intrusion Detection System – Reporting Methods

Hierarchical to: No other components.

Dependencies to:

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]]*

].

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)]*]

FAU_IDS_EXT Intrusion Detection Methods

Family Behavior

Component Leveling

FAU_IDS_EXT.1, Intrusion Detection System – Intrusion Detection Methods,

Management: FAU_IDS_EXT.1

Audit: FAU_IDS_EXT.1

FAU_IDS_EXT.1 Intrusion Detection System – Intrusion Detection Methods
Hierarchical to: No other components.

Dependencies to:

FAU_IDS_EXT.1.1

The TSF shall provide the following methods of intrusion detection [**assignment**: *detection methods*].

FAU_INV_EXT Environmental Inventory

Family Behavior

Component Leveling
FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects
Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

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

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1

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

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 theTOE'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.

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_INV_EXT Characteristics of Environmental Objects

Component Leveling

FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1

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

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 theTOE'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.

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_INV_EXT Behavior of Environmental Objects

Component Leveling

FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1

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

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 theTOE's wireless sensors.

FAU_INV_EXT.4.3

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

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_INV_EXT Location of Environmental Objects

Component Leveling

FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

FAU_INV_EXT.4.1

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

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 theTOE's wireless sensors.

FAU_INV_EXT.4.3

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

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_WID_EXT Malicious Environmental Objects

Family Behavior

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

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling
FAU_WID_EXT.2, Wireless Intrusion Detection – Passive Information Flow Monitoring,

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling

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

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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 Passive Information Flow Monitoring

Component Leveling

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

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling

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

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling
FAU_WID_EXT.7, Wireless Intrusion Detection – Wireless Spectrum Analysis,

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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 Denial of Service

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

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling
FAU_WID_EXT.2, Wireless Intrusion Detection – Passive Information Flow Monitoring,

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling
FAU_WID_EXT.7, Wireless Intrusion Detection – Wireless Spectrum Analysis,

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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_WID_EXT.1, Wireless Intrusion Detection – Malicious Environmental Objects,

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling

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

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling
FAU_WID_EXT.5, Wireless Intrusion Detection – Unauthorized Encryption Schemes,

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling
FAU_WID_EXT.7, Wireless Intrusion Detection – Wireless Spectrum Analysis,

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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_WID_EXT.1, Wireless Intrusion Detection – Malicious Environmental Objects,

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling

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

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling

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

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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_WID_EXT.1, Wireless Intrusion Detection – Malicious Environmental Objects,

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling

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

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling

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

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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_WID_EXT.1, Wireless Intrusion Detection – Malicious Environmental Objects,

Management: FAU_WID_EXT.1

Audit: FAU_WID_EXT.1

FAU_WID_EXT.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.

FAU_WID_EXT.1.3

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

Component Leveling

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

Management: FAU_WID_EXT.2

Audit: FAU_WID_EXT.2

FAU_WID_EXT.2 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 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.2.4

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

Component Leveling

FAU_WID_EXT.3, Wireless Intrusion Detection – Denial of Service,

Management: FAU_WID_EXT.3

Audit: FAU_WID_EXT.3

FAU_WID_EXT.3 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_WID_EXT.4, Wireless Intrusion Detection – Unauthorized Authentication Schemes,

Management: FAU_WID_EXT.4

Audit: FAU_WID_EXT.4

FAU_WID_EXT.4 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 useWLAN authentication schemes that are not authorized.

Component Leveling

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

Management: FAU_WID_EXT.5

Audit: FAU_WID_EXT.5

FAU_WID_EXT.5 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 useWLAN 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_WID_EXT.6, Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring,

Management: FAU_WID_EXT.6

Audit: FAU_WID_EXT.6

FAU_WID_EXT.6 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: [**assignment**: *some bands*].

Component Leveling
FAU_WID_EXT.7, Wireless Intrusion Detection – Wireless Spectrum Analysis,

Management: FAU_WID_EXT.7

Audit: FAU_WID_EXT.7

FAU_WID_EXT.7 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

Component Leveling
FAU_ANO_EXT.1, Anomaly-Based Intrusion Detection,

Management: FAU_ANO_EXT.1

Audit: FAU_ANO_EXT.1

FAU_ANO_EXT.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_SIG_EXT Signature-Based Intrusion Detection

Family Behavior

Component Leveling
FAU_SIG_EXT.1, Signature-Based Intrusion Detection,

Management: FAU_SIG_EXT.1

Audit: FAU_SIG_EXT.1

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

Dependencies to:

FAU_SIG_EXT.1.1

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

FAU_STG_EXT Protected Audit Event Storage (Packet Captures)

Family Behavior

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

Management: FAU_STG_EXT.1/PCAP

Audit: FAU_STG_EXT.1/PCAP

FAU_STG_EXT.1/PCAP Protected Audit Event Storage (Packet Captures)
Hierarchical to: No other components.

Dependencies to:

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.

FAU_STG_EXT.1.2/PCAP

The TSF shall be able to store generated packet captures on theTOE 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.

FAU_INV_EXT Detection of Unauthorized Connections

Component Leveling
FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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.

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 a [**assignment**: *value equal or less than 15*] feet of their actual location.

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_INV_EXT Signal Library

Component Leveling

FAU_INV_EXT.1, Environmental Inventory,

Management: FAU_INV_EXT.1

Audit: FAU_INV_EXT.1

FAU_INV_EXT.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_INV_EXT.2, Characteristics of Environmental Objects,

Management: FAU_INV_EXT.2

Audit: FAU_INV_EXT.2

FAU_INV_EXT.2 Characteristics of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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 theTOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

Component Leveling

FAU_INV_EXT.3, Behavior of Environmental Objects,

Management: FAU_INV_EXT.3

Audit: FAU_INV_EXT.3

FAU_INV_EXT.3 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 otherEUD,

[**selection**:

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

].

Component Leveling

FAU_INV_EXT.4, Location of Environmental Objects,

Management: FAU_INV_EXT.4

Audit: FAU_INV_EXT.4

FAU_INV_EXT.4 Location of Environmental Objects

Hierarchical to: No other components.

Dependencies to:

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.

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.

Component Leveling

FAU_INV_EXT.5, Detection of Unauthorized Connections,

Management: FAU_INV_EXT.5

Audit: FAU_INV_EXT.5

FAU_INV_EXT.5 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.

Component Leveling

FAU_INV_EXT.6, Signal Library,

Management: FAU_INV_EXT.6

There are no management functions foreseen.

Audit: FAU_INV_EXT.6

There are no audit events foreseen.

FAU_INV_EXT.6 Signal Library

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_INV_EXT.6.1

The TSF shall include a signal library.

FAU_MAC_EXT Device Impersonation

Family Behavior

Component Leveling

FAU_MAC_EXT.1, Device Impersonation,

Management: FAU_MAC_EXT.1

Audit: FAU_MAC_EXT.1

FAU_MAC_EXT.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

Component Leveling

FAU_WIP_EXT.1, Wireless Intrusion Prevention,

Management: FAU_WIP_EXT.1

Audit: FAU_WIP_EXT.1

FAU_WIP_EXT.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 wirelessAP or EUD from the network monitored by the TSF using the following methods: [**selection**: *wireless containment*, *wire-side containment of an unauthorizedAP connected to the internal corporate wired network*.]

Appendix D - 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.

Appendix E - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.

Appendix F - Acronyms

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