first Daisy Diff compare report. last

Click on the changed parts for a detailed description. Use the left and right arrow keys to walk through the modifications.

PP-Module for WIDS/WIPS

This page is best viewed with JavaScript enabled!

Version: 1.0

~~2019~~2020-~~11~~01-~~07~~16

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2016-10-06	Initial Release - EP for NDcPP

Contents

1 Introduction

1.1 Overview

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

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

This PP-Module extends the collaborative Protection Profile for Network Devices (NDcPP).

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].
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
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	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 a ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

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

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

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

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

A WIDS/WIPS can be Integrated (be part of the WLAN infrastructure) or ~~Overlay~~ Standalone (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 mode, 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.

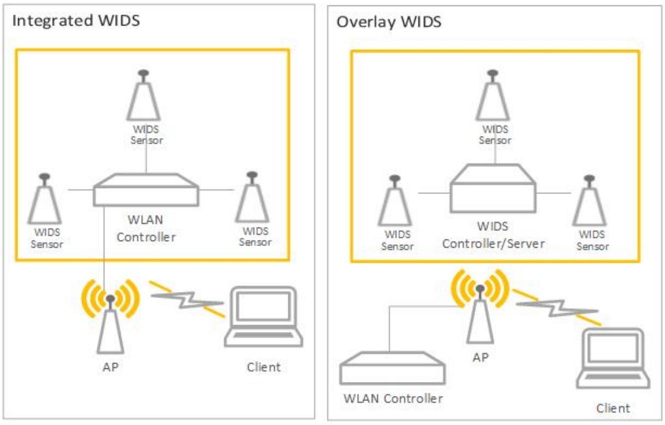

Figure 1: General TOE

1.4 Use Cases

[USE CASE 1] Use Case 1

2 Conformance Claims

Conformance Statement

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.

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

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

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

3.1 Threats

T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION

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.

~~Addressed by: FAU_GEN.1/WIDS, FAU_STG_EXT.1/PCAP~~

O.WIDS_ANALYZE

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

~~Addressed by: FAU_ARP.1, FAU_ARP_EXT.2, FAU_IDS_EXT.1, FAU_INV_EXT.1, FAU_INV_EXT.2, FAU_INV_EXT.3, FAU_SAA.1, FAU_WID_EXT.1, FAU_WID_EXT.2, FAU_WID_EXT.3, FAU_WID_EXT.4, FAU_WID_EXT.5, FDP_IFC.1, FAU_ANO_EXT.1(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)~~

O.WIPS_REACT

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

~~Addressed by: FAU_WIP_EXT.1 (OPTIONAL)~~

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.

~~Addressed by: FMT_SMF.1/WIDS~~

O.INSECURE_OPERATIONS

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

~~Addressed by: FPT_FLS.1(Optional)~~

O.TRUSTED_COMMUNICATIONS

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

~~Addressed by: FPT_ITT.1, FTP_ITC.1~~

4.2 Security Objectives for the Operational Environment

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

OE.CONNECTIONS

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

OE.PROPER_ADMIN

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

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives. ~~, O.WIDS_ANALYZE, O.WIPS_REACT, O.WIDS_ANALYZE, O.WIPS_REACT, O.TOE_ADMINISTRATION, O.WIDS_ANALYZE, O.WIPS_REACT~~

Threat, Assumption, or OSP	Security Objectives	Rationale
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	O.SYSTEM_MONITORING	The threat T.Unauthorized_Disclosure_of_Information 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_Information is countered by O.WIDS_ANALYZE as this provides detection of potential violations of approved network usage.
O.WIPS_REACT	The threat T.Unauthorized_Disclosure_of_Information is countered by O.WIPS_REACT as this provides containment of unauthorized APs 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 this provides detection of potential violations of approved network usage.
	O.WIPS_REACT	The threat T.UNAUTHORIZED_ACCESS is countered by O.WIPS_REACT as this provides containment of unauthorized APs 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 by 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 by O.WIDS_ANALYZE as this provides for detection of potential violations of approved network usage.
O.WIPS_REACT	The threat T.DISRUPTION is countered by 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.
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 notations are used:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by italicized text): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: 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 5.2 TOE Security Functional Requirements.

5.1.1 Modified SFRs

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

5.1.1.1 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1
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.

5.1.1.2 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1
The TSF shall **be capable of using [selection: *IPsec*, *SSH*, *TLS*, *HTTPS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [selection: *database server*, *[assignment: other capabilities]*, *no other capabilities*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**
FTP_ITC.1.2
The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.
FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [**assignment**: list of services for which the TSF is able to initiate communications].
Application Note: The intent of the above requirement is to provide a means by which a cryptographic protocol may be used to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. The TOE uses at least one of the listed protocols for communications with the server that collects the audit information.

If the TSF uses a separate database server, the database server selection must included in the ST.

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

5.2 TOE Security Functional Requirements

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

5.2.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

FAU_ARP.1.1
The TSF shall *display an alert to Authorized Administrator in sufficient detail to include identity of APs and EUDs involved, description of alert and severity level and* [**selection**: *capture raw frame traffic that triggered the violation*, *no other actions*] upon detection of a potential security violation.
Application Note: If "capture raw frame traffic that triggers the violation" is selected then FAU_STG_EXT.1/PCAP shall be included in the ST.

FAU_ARP_EXT.2 Security Alarm Filtering

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

FAU_GEN.1/WIDS Audit Data Generation

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

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

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ANO_EXT.1 (OPTIONAL)	None	None
FAU_ARP.1	Actions taken due to potential security violations	None
FAU_ARP_EXT.2	None	None
FAU_GEN.1/WIDS	None	None
FAU_IDS_EXT.1	None	None
FAU_INV_EXT.1	Presence of whitelisted device	Type of device (AP or EUD), MAC Address
FAU_INV_EXT.2	None	None
FAU_INV_EXT.3	None	None
FAU_INV_EXT.4	Location of AP or EUD	MAC Address, device type, classification of device, sensor(s) that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s)
FAU_INV_EXT.5 (OPTIONAL)	None	None
FAU_INV_EXT.6 (OPTIONAL)	None	None
FAU_MAC_EXT.1 (OPTIONAL)	None	None

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

~~: Auditable Events~~Table 1: Auditable Events

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

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

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

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

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

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

FAU_GEN_EXT.1 Intrusion Detection System – Reporting Methods

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

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

].
Application Note: Syslog and/or SNMP trap reporting can be used. At least one reporting method must be selected.
FAU_GEN_EXT.1.2
The TSF shall provide the ability to import data from the system: [**selection**: *custom API*, *Syslog*, *common log format*, *CSV*, [**assignment**: *vendor detection method ~~(e.g. Splunk)~~*]]
Application Note: The system shall provide the ability to interact with an extensible interface to a third party wireless monitoring system for the purposes of importing data from the wireless system.

FAU_IDS_EXT.1 Intrusion Detection System – Intrusion Detection Methods

FAU_IDS_EXT.1.1
The TSF shall provide the following methods of intrusion detection [**selection**: *anomaly-based*, *signature-based*, *behavior-based*, [**assignment**: *other detection method*]].
Application Note: At least one detection method must be selected. If multiple detection methods are supported, each method supported shall be selected.

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

FAU_INV_EXT.1 Environmental Inventory

FAU_INV_EXT.1.1
The TSF shall determine if a given AP or EUD is authorized based on MAC addresses.
FAU_INV_EXT.1.2
The TSF shall detect the presence of whitelisted EUDs and APs in the Operational Environment.
FAU_INV_EXT.1.3
The TSF shall detect the presence of non-whitelisted EUDs and APs in the Operational Environment.
Application Note: The inventory of authorized APs and EUDs is defined by FMT_SMF.1/WIDS.

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

FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.2.1
The TSF shall detect the

- current RF band
- current channel
- MAC Address
- classification of APs and EUDs

- [**selection**: [***assignment****: other details*], *no other details*]

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

- encryption
- number of connected EUDs.

Application Note: For detection of encryption type, the TSF should be able to differentiate between the differentWLAN encryption methods and when no encryption is in use.
FAU_INV_EXT.2.3
The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

FAU_INV_EXT.3 Behavior of Environmental Objects

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

- An EUD establishes a peer-to-peer connection with any otherEUD,

[**selection**:

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

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

FAU_INV_EXT.4 Location of Environmental Objects

FAU_INV_EXT.4.1
The TSF shall detect ~~information on~~ the ~~current~~ physical location of APs and EUDs ~~and APs within range of the TOE's wireless sensors. Application Note: This SFR only checks for the ability of the WIDS to track the location of APs and EUDs either by placing them on a map or providing the distance of theAP or EUD from the sensor but does not mandate a certain degree of accuracy~~to within [**assignment**: value equal or less than 15] feet of their actual location.
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.~~

~~FAU_~~SAA.1 Potential Violation Analysis

FAU_SAA.1.1
The TSF shall be able to apply a set of rules for monitoring**the wireless traffic** and based upon these rules indicate a potential**malicious action**.
FAU_SAA.1.2
The TSF shall enforce the following rules for monitoring**wireless traffic:**

a. Accumulation or combination of [**assignment**: subset of defined auditable events] known to indicate a potential security violation;
b. ~~*[other potential security violations as defined by: Potential Security Violations2].*~~

~~Potential Security ViolationAdditional Information~~

a. *Detection of authorized EUD establishing peer-to-peer connection with any otherEUD*

~~.Description of behavior detected (i.e., bridge, ICS connection),MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.~~

a. ;
b. *Detection of EUD bridging two network interfaces*

~~.Description of behavior detected (i.e., bridge, ICS connection),MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.~~

a. ;
b. *Detection of packet flooding/DoS/DDoS*

~~.Description of behavior detected (i.e., bridge, ICS connection),MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.~~

a. ;
b. *Detection of ICS connection*

~~.Description of behavior detected (i.e., bridge, ICS connection),MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.~~

a. ;
b. *Detection of rogue device*

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

a. ;
b. *Detection of mac spoofing*

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

a. ;
b. *Alert generated by violaton of user defined signature*

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

a. ;
b. *Detection of rogue AP*

~~.Identity information of the devices involved.~~

a. ;
b. *Detection of malicious EUD*

~~.Identity information of the devices involved.~~

a. ;
b. *Detection of traffic with excessive transmit power level*

~~.Identity information of the devices involved~~.

a. ;
b. *Detection of active probing*

~~.Identity information of the devices involved~~.

a. ;
b. *Detection of MAC spoofing*

~~.Identity information of the devices involved~~.

a. ;
b. *Whitelisted EUD connected to unauthorized SSID*;
c. *Detection of RF-based denial of service*

~~.MAC Address, device type, classification AP or EUD attacked.~~

a. ;
b. *Detection of deauthentication flooding*

~~.MAC Address, device type, and classification AP or EUD attacked.~~

a. ;
b. *Detection of disassociation flooding*

~~.MAC Address, device type, and classification AP or EUD attacked.~~

a. ;
b. *Detection of request-to-send/clear-to-send abuse*

~~.MAC Address, device type, and classification AP or EUD attacked.~~

a. ;
b. *Detection of unauthorized authentication scheme use*

~~.~~

a. ;
b. *Detection of unauthorized encryption scheme use*

~~.~~

a. ;
b. *Detection of unencrypted traffic*;
c. [**assignment**: any other rules].

~~: Potential Security Violations~~Table 2: Potential Security Violations

FAU_WID_EXT.1 Wireless Intrusion Detection – Malicious Environmental Objects

FAU_WID_EXT.1.1
The TSF shall apply [**selection**: *configurable*, *automatic*] classification rules to detect rogue APs.
Application Note: If "configurable" is selected then, "Define classification rules to detect rogue APs" shall be selected in FMT_SMF.1/WIDS.
FAU_WID_EXT.1.2
The TSF shall distinguish between benign and malicious APs and EUDs based on automatic detection metrics.
FAU_WID_EXT.1.3
The TSF shall provide the ability to determine if a given SSID is authorized.
Application Note: FMT_SMF.1/WIDS defines the subset of authorized SSID(s).

FAU_WID_EXT.2 Wireless Intrusion Detection – Passive Information Flow Monitoring

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

- 2.4 GHz
- 4.9/5.0 GHz

[**selection**:

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

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

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1~~>~~ and defined through ~~the~~ FAU_WID_EXT.1, FAU_WID_EXT.2, FAU_WID_EXT.3, FAU_WID_EXT.4 and FAU_WID_EXT.5, in addition to optional SFRs FAU_WID_EXT.6 and FAU_WID_EXT.7. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.
FAU_WID_EXT.2.2
The TSF shall provide wireless sensors to detect network traffic matching the 802.11 monitoring SFP that [**selection**: *can be configured to prevent transmission of data*, *does not transmit data*].
Application Note: If "can be configured to prevent transmission of data" is selected then "Enable/Disable transmission of data by wireless sensor" shall be selected in FMT_SMF.1/WIDS.

The intent of this SFR is to employ WIDS sensors that can have all wireless transmission capabilities disabled for instances where a site wishes to implement a no wireless policy.
The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1~~>~~ and defined through ~~the~~ FAU_WID_EXT~~ SFRs. A vendor does not have to formally define this policy, it only needs to comply with the SFRs~~.1, FAU_WID_EXT.2
~~.3~~
~~The TSF shall detect the presence of the following unauthorized connections and unauthorized network traffic~~:

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

  ~~].~~

~~Application Note: “Authorized” EUDs/APs are those that are assigned to the whitelist as defined by FMT_SMF.1.~~

~~The 802.11 standard allows APs to beacon with the SSID field set to null. This is referred to as a hidden or cloaked SSID. The client seeking to associate with an AP using a hidden SSID must first send out a Probe Request that contains the SSID of that network, then the AP will return with a Probe Request of its own. The TSF needs to be able to detect if an AP is allowing clients to associate without providing the valid SSID of the AP~~, FAU_WID_EXT.3, FAU_WID_EXT.4 and FAU_WID_EXT.5, in addition to optional SFRs FAU_WID_EXT.6 and FAU_WID_EXT.7. A vendor does not have to formally define this policy, it only needs to comply with the SFRs
FAU_WID_EXT.2.
~~4~~
3
The TSF shall perform stateful frame inspection and log attacks spanning multiple frames.
Application Note: Attackers possess the capability to distribute an attack across multiple frames in an attempt to avoid traditional detection measures that solely focus on packet headers. Stateful frame inspection will allow for the identification of obfuscation techniques centered around spreading an attack across multiple frames.

FAU_WID_EXT.3 Wireless Intrusion Detection – Denial of Service

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

FAU_WID_EXT.4 Wireless Intrusion Detection – Unauthorized Authentication Schemes

FAU_WID_EXT.4.1
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN authentication schemes that are not authorized.
Application Note: Whitelisted APs and EUDs are defined in FMT_SMF.1/WIDS.

FAU_WID_EXT.5 Wireless Intrusion Detection – Unauthorized Encryption Schemes

FAU_WID_EXT.5.1
The TSF shall detect when whitelisted APs and EUDs attempt to use WLAN encryption schemes that are not authorized.
Application Note: Whitelisted APs and EUDs are defined in FMT_SMF.1/WIDS.
FAU_WID_EXT.5.2
The TSF shall detect when whitelisted APs and EUDs send or receive unencrypted data.
Application Note: Whitelisted APs and EUDs are defined in FMT_SMF.1/WIDS. When referring to unencrypted data being received by a whitelisted AP or EUD it refers to unencrypted data being sent to a whitelisted AP or EUD from either a non-whitelisted or whitelisted AP or EUD.

5.2.2 User Data Protection (FDP)

FDP_IFC.1 Information Flow Control Policy

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

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

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

The "802.11 monitoring SFP" is a security function policy and the SFRs that reference this policy describe what the policy does. The "802.11 monitoring SFP" is established in FDP_IFC.1 and defined through ~~the~~ FAU_WID_EXT.1, FAU_WID_EXT.2, FAU_WID_EXT.3, FAU_WID_EXT.4 and FAU_WID_EXT.5, in addition to optional SFRs FAU_WID_EXT.6 and FAU_WID_EXT.7. A vendor does not have to formally define this policy, it only needs to comply with the SFRs.

5.2.3 Security Management (FMT)

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

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

- Define an inventory of authorized APs based on MAC addresses,
- Define an inventory of authorized EUDs based on MAC addresses,
- Define rules for monitoring and alerting on the wireless traffic,
- Define authorized SSID(s),
- Define authorized WLAN authentication schemes,
- Define authorized WLAN encryption schemes,
- [**selection**:
  - *Specification of periods of network activity that constitute baseline of expected behavior*,
  - *Definition of anomaly activity*,
  - *Define classification rules to detect rogue APs*,
  - *[**selection**: Enable, Disable] transmission of data by wireless sensor*,
  - *Define attack signatures*,
  - *Define rules for overwriting previous packet captures*,
  - *Define the amount of time sensor monitors a specific [**selection**: frequency, channel]*,
  - *no other capabilities*

  ].

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

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

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

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

5.3 TOE Security Functional Requirements Rationale

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

OBJECTIVE	ADDRESSED BY	RATIONALE
O.SYSTEM_MONITORING	FAU_GEN.1/WIDS, FAU_STG_EXT.1/PCAP	
O.WIDS_ANALYZE	FAU_ARP.1, FAU_ARP_EXT.2, FAU_ANO_EXT.1 (OPTIONAL), FAU_IDS_EXT.1, FAU_INV_EXT.1, FAU_INV_EXT.2, FAU_INV_EXT.3, FAU_INV_EXT.4 (OPTIONAL), FAU_INV_EXT.5 (OPTIONAL), FAU_INV_EXT.6 (OPTIONAL), FAU_MAC_EXT.1 (OPTIONAL), FAU_SAA.1, FAU_SIG_EXT.1 (OPTIONAL), FAU_WID_EXT.1, FAU_WID_EXT.2, FAU_WID_EXT.3, FAU_WID_EXT.4, FAU_WID_EXT.5, FAU_WID_EXT.6 (OPTIONAL), FAU_WID_EXT.7 (OPTIONAL), FDP_IFC.1	
O.WIPS_REACT	FAU_WIP_EXT.1 (OPTIONAL)	
O.TOE_ADMINISTRATION	FMT_SMF.1/WIDS	
O.INSECURE_OPERATIONS	FPT_FLS.1 (OPTIONAL)	
O.TRUSTED_COMMUNICATIONS	FPT_ITT.1, FTP_ITC.1	

6 Consistency Rationale

6.1 Network Device Protection Profile

6.1.1 Consistency of TOE Type

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

6.1.2 Consistency of Security Problem Definition

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

PP-Module Threat	**Consistency Rationale**	~~T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION~~	~~T.UNAUTHORIZED_ACCESS~~	~~T.DISRUPTION~~

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~~	~~O.WIDS_ANALYZE~~	~~O.WIPS_REACT~~	~~O.TOE_ADMINISTRATION~~	~~O.INSECURE_OPERATIONS~~	~~O.TRUSTED_COMMUNICATIONS~~

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

PP-Module Operational Environment Objective	**Consistency Rationale**	~~OE.CONNECTIONS~~	~~OE.PROPER_ADMIN~~

6.1.4 Consistency of Requirements

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

PP-Module Requirement	**Consistency Rationale**
Modified SFRs	
FPT_ITT.1	
FTP_ITC.1	
Mandatory SFRs	
FAU_ARP.1	
FAU_ARP_EXT.2	
FAU_GEN.1/WIDS	
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

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~~ WLAN (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.

FAU_WID_EXT.7 Wireless Intrusion Detection – Wireless Spectrum Analysis

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

Appendix B - Selection-based SFRs

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

This is a selection-based component. Its inclusion depends upon selection from FAU_IDS_EXT.1.1.
FAU_ANO_EXT.1.1
The TSF shall support the definition of [**selection**: *baselines ('expected and approved')*, *anomaly ('unexpected') traffic patterns*] including the specification of [**selection**:

- *throughput (data elements (e.g. bytes, packets, etc.) per time period (e.g. minutes, hours, days))*

- *time of day*,
- *frequency*,
- *thresholds*,
- *[**assignment**: other methods]*

] and the following network protocol fields:

- all management and control frame header elements.

FAU_ANO_EXT.1.2
The TSF shall support the definition of anomaly activity through [**selection**: *manual configuration by administrators*, *automated configuration*].
Application Note: The "baseline" and "anomaly" can be something manually defined/configured by a TOE administrator (or importing definitions), or something that the TOE is able to automatically define/create by inspecting network traffic over a period of time (a.k.a. "profiling").

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

This is a selection-based component. Its inclusion depends upon selection from FAU_IDS_EXT.1.1.
FAU_SIG_EXT.1.1
The TSF shall support user-defined and customizable attack signatures.

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

This is a selection-based component. Its inclusion depends upon selection from FAU_ARP.1.1.
FAU_STG_EXT.1.1/PCAP
The TSF shall be able to transmit the generated packet captures to an external IT entity using a trusted channel according to FTP_ITC.1.
Application Note: Per FAU_STG_EXT.1 in the Base-PP, the TOE must support transfer of the audit data to an external IT entity using a trusted channel per FTP_ITC.1. Note that this PP-Module modifies FTP_ITC.1 from the Base-PP. If "capture raw frame traffic that triggers the violation" is selected in FAU_ARP.1, then this SFR shall be included in the ST, and this iteration is for the PCAPs generated as a selectable action completed upon detection of a potential security violation in FAU_ARP.1.
FAU_STG_EXT.1.2/PCAP
The TSF shall be able to store generated packet captures on the TOE itself.
FAU_STG_EXT.1.3/PCAP
The TSF shall [**selection**: *drop new packet capture data*, *overwrite previous packet captures according to the following rule: [**assignment**: rule for overwriting previous packet captures]* , *[**assignment**: other action]*] when the local storage space for packet capture data is full.

Appendix C - Objective SFRs

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

FAU_INV_EXT.5 Detection of Unauthorized Connections

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

FAU_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.

FAU_MAC_EXT.1 Device Impersonation

FAU_MAC_EXT.1.1
The TSF shall detect when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously.
Application Note: The intent of this SFR is to detect MAC spoofing where an attacker is able to cause the whitelisted EUD to disconnect and promptly connects a non-whitelisted device using the MAC address of the whitelisted EUD.
FAU_MAC_EXT.1.2
The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-whitelisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors.
Application Note: The intent of this SFR is to allow the administrator to determine the time that should be allowed between a whitelisted EUD connecting in two distant locations.

FAU_WIP_EXT.1 Wireless Intrusion Prevention

FAU_WIP_EXT.1.1
The TSF shall allow an Authorized Administrator to isolate a wireless AP or EUD from the network monitored by the TSF using the following methods: [**selection**: *wireless containment*, *wire-side containment of an unauthorized AP connected to the internal corporate wired network*]
Application Note: It is expected that an Authorized Administrator will be responsible for confirming the AP or EUD as a rogue AP or EUD to initiate wireless containment.

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

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*sensor functionality failure, potential compromise of the TSF*].
Application Note: At minimum, the preservation of a secure state requires the generation of audit records when the defined failure conditions occur.

Appendix D - Extended Component Definitions

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

D.1 Background and Scope

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

Functional Class	Functional Components
Security Audit (FAU)	FAU_ARP_EXT Security Alarm Filtering FAU_GEN_EXT Reporting Methods FAU_IDS_EXT Intrusion Detection Methods FAU_INV_EXT Environmental Inventory FAU_INV_EXT Characteristics of Environmental Objects FAU_INV_EXT Behavior of Environmental Objects FAU_INV_EXT Location of Environmental Objects FAU_WID_EXT Malicious Environmental Objects FAU_WID_EXT Passive Information Flow Monitoring FAU_WID_EXT Denial of Service FAU_WID_EXT Unauthorized Authentication Schemes FAU_WID_EXT Unauthorized Encryption Schemes
Security Audit (FAU)	FAU_WID_EXT Wireless Spectrum Monitoring FAU_WID_EXT Wireless Spectrum Monitoring
	FAU_ANO_EXT Anomaly-Based Intrusion Detection

Security Audit (FAU)	FAU_SIG_EXT Signature-Based Intrusion Detection FAU_STG_EXT Protected Audit Event Storage (Packet Captures)
Security Audit (FAU)	FAU_INV_EXT Detection of Unauthorized Connections FAU_INV_EXT Signal Library FAU_MAC_EXT Device Impersonation FAU_WIP_EXT Wireless Intrusion Prevention

D.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 [**selection**: *anomaly-based*, *signature-based*, *behavior-based*, [***assignment****: other detection method*]].

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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 other EUD,

[**selection**:

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

].

Component Leveling

FAU_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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~ to within [**assignment**: value equal or less than 15] feet of their actual location.

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_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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~to within [**assignment**: value equal or less than 15] feet of their actual location.

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_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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~to within [**assignment**: value equal or less than 15] feet of their actual location.

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_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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 other EUD,

[**selection**:

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

].

Component Leveling

FAU_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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~ to within [**assignment**: value equal or less than 15] feet of their actual location.

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_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 use WLAN 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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: [**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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 theMAC 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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:[**selection**: *3.6 GHz*, *60 GHz*, *sub-GHz (0-900 MHz)*, *all cellular 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 the TOE itself.

FAU_STG_EXT.1.3/PCAP

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

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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~to within [**assignment**: value equal or less than 15] feet of their actual location.

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_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 the TOE's wireless sensors.

FAU_INV_EXT.2.2

The TSF shall detect the follow additional details for APs:

- encryption
- number of connected EUDs.

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 APs and EUDs ~~and APs within range of the TOE's wireless sensors~~to within [**assignment**: value equal or less than 15] feet of their actual location.

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 sameMAC address simultaneously.

FAU_MAC_EXT.1.2

The TSF shall detect when two sensors in non-overlapping locations receive traffic from theMAC 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 theTSF using the following methods: [**selection**: *wireless containment*, *wire-side containment of an unauthorizedAP connected to the internal corporate wired network*]

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
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-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
SSID	Service Set Identifier
ST	Security Target
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
WEP	Wired Equivalent Protocol
WIDS	Wireless Intrustion Detection System
WIPS	Wireless Intrustion Prevention System
WLAN	Wireless Local Area Network
WPA	~~Wi-Fi~~ WLAN Protected Access