PP-Module for Widgets

Version: 1.0
2020-01-16
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2016-10-06	Initial Release

Contents

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

1 Introduction

1.1 Overview

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

The following content should be included if:

- the TOE implements ""

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

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

1.2 Terms

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

1.2.1 Common Criteria Terms

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

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

1.2.2 Technical Terms

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

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

This PP-Module specifically addresses widgets. Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS).

The following content should be included if:

- the TOE implements ""

Text specific to widgets when Newtork Device is the base.

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

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

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

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

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

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

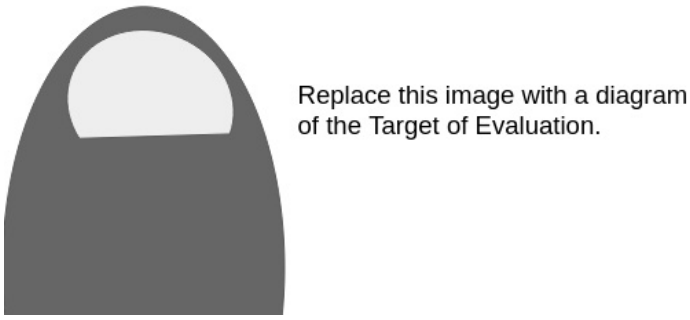

Figure 1: General TOE

1.4 Use Cases

[USE CASE 1] Use Case 1
A great use case

2 Conformance Claims

Conformance Statement

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

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

- , version

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

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

Package Claim
This Module does not claim conformance to any packages.

3 Security Problem Description

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

3.1 Threats

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

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

devices may be susceptible to the unauthorized disclosure of information.

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

3.2 Assumptions

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

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

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

3.3 Organizational Security Policies

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

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

4 Security Objectives

4.1 Security Objectives for the TOE

This document does not define any additional SOs.

4.2 Security Objectives for the Operational Environment

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

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

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

4.3 Security Objectives Rationale

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

Table 1: Security Objectives Rationale

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

		network which enables detection of unauthorized APs and EUDs.
	O.WIDS_ANALYZE	The threat T.UNAUTHORIZED_ACC countered by O.WIDS_ANALYZE as t provides detection of potential violat of approved network usage.
	O.WIPS_REACT	The threat T.UNAUTHORIZED_ACC countered by O.WIPS_REACT as this provides containment of unauthorize and EUDs.
	O.TOE_ADMINISTRATION	The threat T.UNAUTHORIZED_ACC countered by O.TOE_ADMINISTRAT
T.DISRUPTION	O.SYSTEM_MONITORING	The threat T.DISRUPTION is counte O.SYSTEM_MONITORING as this provides for visibility into the netwo which enables detection of DoS atta
	O.WIDS_ANALYZE	The threat T.DISRUPTION is counte O.WIDS_ANALYZE as this provides f detection of potential violations of approved network usage.
	O.WIPS_REACT	The threat T.DISRUPTION is counte O.WIPS_REACT as this provides containment of unauthorized APs an EUDs.
A.CONNECTIONS	OE.CONNECTIONS	The operational environment objecti OE.CONNECTIONS is realized throu A.CONNECTIONS.
A.PROPER_ADMIN	OE.PROPER_ADMIN	The operational environment objecti OE.PROPER_ADMIN is realized thro A.PROPER_ADMIN.
A.PHYSICAL_PROTECTION	O.WIDS_ANALYZE	Cuase I wanted to show an example.
P.ANALYZE	O.WIDS_ANALYZE	The organizational security policy P.ANALYZE is facilitated through O.WIDS_ANALYZE.

5 Security Requirements

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

5.0.0.1 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1

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

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

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

5.0.0.2 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1

The TSF shall **be capable of using [selection: *IPsec*, *SSH*, *TLS*, *HTTPS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [selection: *database server*, *[assignment: other capabilities]*, *no other capabilities*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2

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

FTP_ITC.1.3

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

Application Note: The intent of the above requirement is to provide a means by which a cryptographic protocol may be used to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. The TOE uses at least one of the listed protocols for communications with the server that collects the audit information.

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

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

5.0.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

FAU_ARP.1.1

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

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

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 Table 2;*
d. *Failure of wireless sensor communication].*

Table 2: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ANO_EXT.1	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	None	None
FAU_MAC_EXT.1	None	None
FAU_SAA.1	None	None
FAU_SIG_EXT.1	None	None
FAU_STG_EXT.1/PCAP	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	Detection of network devices operating in selected RF bands	Frequency band, channel used within frequency band, identification information (MAC address if applicable or other similar unique ID), device technology (i.e., cellular), sensor(s) that detected devices
FAU_WID_EXT.7	None	None
FAU_WID_EXT.8	None	None
FAU_WIP_EXT.1	Isolation of AP or EUD	Description of violation, type of containment used, was containment triggered manually or automatically, sensor performing the containment (if wireless), details about the device (s) being contained (classification, device type, MAC address).
FDP_IFC.1	None	None
FMT_SMF.1/WIDS	None	None
FPT_FLS.1	Information about failure.	Indication that there was a failure, type of failure, device that failed, and time of failure.
FPT_ITT.1	None	None
FTP_ITC.1	None	None

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

FAU_GEN.1.2/WIDS

The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, and subject identity (if applicable);
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*auditable events listed in Table 2*].

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.

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 different WLAN encryption methods and when no encryption is in use.

FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for EUDs:

- SSID and BSSID of AP it is connected to.

FAU_INV_EXT.3 Behavior of Environmental Objects

FAU_INV_EXT.3.1

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

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

[**selection**:

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

].

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

FAU_INV_EXT.4 Location of Environmental Objects

FAU_INV_EXT.4.1

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

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

FAU_INV_EXT.4.2

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

FAU_INV_EXT.4.3

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

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 Table 3].*

Potential Security Violation	Additional Information
Detection of authorized EUD establishing peer-to-peer connection with any other EUD.	Description of behavior detected (i.e., bridge, ICS connection), MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.
Detection of EUD bridging two network interfaces.	Description of behavior detected (i.e., bridge, ICS connection), MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.
Detection of packet flooding/DoS/DDoS.	Description of behavior detected (i.e., bridge, ICS connection), MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.
Detection of ICS connection.	Description of behavior detected (i.e., bridge, ICS connection), MAC address of whitelisted device, MAC address of the device that the whitelisted device made a connection with, connection start and end.
Detection of rogue device.	Description of alert, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue, IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP).
Detection of mac spoofing.	Description of alert, type of device (AP or EUD), MAC Address, associations made between authorized devices (which APs are EUDs connected to), channel detected on, RF Band detected on, encryption type used by rogue,

	IEEE 802.11 standard used (a, b, g, n, ac), SSID (if AP), location as labeled by administrator,.
Alert generated by violaton of user defined signature.	Name of alert being triggered (as provided when creating the signature), description of alert (as provided when creating the signature), MAC address of devices involved.
Detection of rogue AP.	Identity information of the devices involved.
Detection of malicious EUD.	Identity information of the devices involved.
Detection of traffic with excessive transmit power level.	Identity information of the devices involved.
Detection of active probing.	Identity information of the devices involved.
Detection of MAC spoofing.	Identity information of the devices involved.
Detection of RF-based denial of service.	MAC Address, device type, classification AP or EUD attacked.
Detection of deauthentication flooding.	MAC Address, device type, and classification AP or EUD attacked.
Detection of disassociation flooding.	MAC Address, device type, and classification AP or EUD attacked.
Detection of request-to-send/clear-to-send abuse.	MAC Address, device type, and classification AP or EUD attacked.
Detection of unauthorized authentication scheme use.	
Detection of unauthorized encryption scheme use.	
Detection of unencrypted traffic.	

Table 3: 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

FAU_WID_EXT.1.2

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

FAU_WID_EXT.1.3

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

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

FAU_WID_EXT.2 Wireless Intrusion Detection – Passive Information Flow Monitoring

FAU_WID_EXT.2.1

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

- 2.4 GHz
- 4.9/5.0 GHz

[**selection**:

- *channels outside regulatory domain*,

- *non-standard channel frequencies*,
- *no other domains*

].

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

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

FAU_WID_EXT.2.2

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

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

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

FAU_WID_EXT.2.3

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

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

  ].

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

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

FAU_WID_EXT.2.4

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

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

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.

FAU_WID_EXT.5 Wireless Intrusion Detection – Unauthorized Encryption Schemes

FAU_WID_EXT.5.1

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

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

FAU_WID_EXT.5.2

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

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

5.0.2 User Data Protection (FDP)

FDP_IFC.1 Information Flow Control Policy

FDP_IFC.1.1

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

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

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

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

5.0.3 Security Management (FMT)

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

FMT_SMF.1.1/WIDS

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

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

  ].

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

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

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

It is expected that an Authorized Administrator will be responsible for configuring the AP to operate on a specific frequency 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.

5.0.4 Security Audit (FAU)

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

FAU_WID_EXT.6.1

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

Application Note: This SFR refers to Non-Wi-Fi (IEEE 802.11 a, b, g, n, and ac) network devices that operate in the specified frequencies. If the ST author selects detection of devices in the cellular bands, FAU_INV_EXT.4 must be included in the ST.

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.

5.0.5 Security Audit (FAU)

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

FAU_ANO_EXT.1.1

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

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

] and the following network protocol fields:

- all management and control frame header elements.

FAU_ANO_EXT.1.2

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

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

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

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)

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.

5.0.6 Security Audit (FAU)

FAU_INV_EXT.5 Detection of Unauthorized Connections

FAU_INV_EXT.5.1

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

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.

5.0.7 Protection of the TSF (FPT)

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

FPT_FLS.1.1

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

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

Appendix A - An Example Appendix

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

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