Supporting Document
Mandatory Technical Document

PP-Module for WIDS/WIPS

Version: 1.0

2020-01-16

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

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

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of 802.11 Wireless Intrusion Detection/Prevention Systems products.

Acknowledgements:
This SD was developed with support from NIAP WIDS/WIPS Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the WIDS/WIPS PP-Module is to describe the security functionality of 802.11 Wireless Intrusion Detection/Prevention Systems products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the Network Device Protection Profile.

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for WIDS/WIPS, Version 1.0. Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs .
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.

1.3.2 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)	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)	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.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM work units that are performed in Section 6 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the cPP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Network Device Protection Profile

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the ND PP.

2.1.1 Modified SFRs

2.1.1.1 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

2.1.1.2 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

2.1.2 TOE SFR Evaluation Activities

2.1.3 Security Audit (FAU)

FAU_ARP.1 Security Alarms

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

Guidance
The evaluator shall use the operational guidance for instructions on where the alerts generated are displayed within the WIDS interface. If the objective requirement to capture the raw frame that triggered an alert is selected, the evaluator must also test for corresponding selection-based requirements. The evaluator shall use the operational guidance to configure the traffic capture capabilities.

Tests

- **Test 1:** The evaluator shall perform a series of events or generate traffic that would successfully trigger an alert. The evaluator should verify and record whether the TOE generated the alert. The evaluator should also record the events or traffic that was generated and what alert was attempted to be triggered and record the details provided by the TOE in the alert.
- **Test 2:** *[conditional]* If capturing of raw frames was selected, verify that the packet capture was triggered and stored as appropriate.

FAU_ARP_EXT.2 Security Alarm Filtering

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

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

Tests

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

FAU_GEN.1/WIDS Audit Data Generation

TSS
There are no TSS assurance activities for this SFR.

Guidance
There are no operational guidance activities for this SFR.

Tests
The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in

accordance with the assurance activities associated with the functional requirements in this PP-Module. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

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

FAU_GEN_EXT.1 Intrusion Detection System – Reporting Methods

TSS
The evaluator shall verify that the TSS includes which method the TOE utilizes.
Guidance
Tests
Depending on the detection technique used by the TOE, the evaluator shall confirm and note the existence of the capability, and test for the appropriate selection-based requirements.

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

FAU_IDS_EXT.1 Intrusion Detection System – Intrusion Detection Methods

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

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

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

FAU_INV_EXT.1 Environmental Inventory

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

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

Tests

- **Test 1:**
  - **Step 1:** Per guidance in FMT_SMF.1/WIDS, add MAC Addresses for an AP and EUD to the whitelist.
  - **Step 2:** Deploy the AP and EUD that were added to whitelist within the range of the TOE's sensors.
  - **Step 3:** Verify that the devices are classified as authorized.
  - **Step 4:** Remove the EUD from the whitelist.
  - **Step 5:** Verify that the EUD is classified as unauthorized.
  - **Step 6:** Remove the AP from the whitelist.
  - **Step 7:** Verify that the AP is classified as unauthorized.
- **Test 2:**
  - **Step 1:** Deploy a whitelisted AP and EUD, and connect the EUD to the AP.
  - **Step 2:** Verify that the list of detected APs and EUDs contains the whitelisted AP and EUD that were just deployed.
  - **Step 3:** If the AP and EUD are detected verify that they are classified as whitelisted devices.
- **Test 3:**
  - **Step 1:** Deploy a non-whitelisted AP and EUD and connect the EUD to the AP.
  - **Step 2:** Verify that the list of detected APs and EUDs contains the non-whitelisted AP and EUD that were just deployed.
  - **Step 3:** If the AP and EUD are detected verify that they are not classified as whitelisted devices.

FAU_INV_EXT.2 Characteristics of Environmental Objects

TSS
The evaluator shall verify that the TSS explains the capability of detecting the current RF band, current channel, MAC Address, classification of APs and EUDs within the TOE's wireless range.

Guidance
The evaluator shall review the operational guidance in order to verify that there are instructions that show how to locate the device inventory mentioned above.

Tests

- **Test 1:**
  - **Step 1:** Deploy a whitelisted AP, non-whitelisted AP and two whitelisted EUDs.
  - **Step 2:** Connect one whitelisted EUD to the whitelisted AP and one to the non-whitelisted AP.
  - **Step 3:** Check the WIDS user interface for a list of detected APs and EUDs.
  - **Step 4:** Verify that current RF band, current channel, MAC Address, classification of device, are part of the information presented on the WIDS user interface for all the APs and EUDs detected. For APs verify that encryption, number of connected EUDs is presented. For EUDs verify that the SSID and BSSID of AP it is connected is presented.

FAU_INV_EXT.3 Behavior of Environmental Objects

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

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

Tests

- **Test 1:** Create the following connections between two whitelisted EUDs.
  - Windows Ad Hoc Connection
  - Mac OS Ad Hoc
  - Linux Ad Hoc
  - Wi-Fi Direct
- **Test 2:** Create the following connections between one whitelisted EUD and a non-whitelisted EUD
  - Windows Ad Hoc Connection
  - Mac OS Ad Hoc
  - Linux Ad Hoc
  - Wi-Fi Direct
- **Test 3:** (optional) Bridge two network interfaces on a whitelisted EUD (one must be the wireless card listed as whitelisted).
- **Test 4:**
  - Create a Windows Hosted Network with a whitelisted EUD.
  - Connect a different whitelisted EUD to the network.

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

FAU_INV_EXT.4 Location of Environmental Objects

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

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

Guidance
The evaluator shall review the operational guidance for instructions on how to configure location tracking, how to load a location map (if applicable), and where in the TSF administrator interface the location of APs and EUDs can be viewed.

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

Tests

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

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

FAU_SAA.1 Potential Violation Analysis

TSS
There are no TSS assurance activities for this SFR.

Guidance
There are no operational guidance activities for this SFR.

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

FAU_WID_EXT.1 Wireless Intrusion Detection – Malicious Environmental Objects

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

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

Tests

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

  The evaluator shall configure the TSF with a set of authorized SSIDs and perform the following tests:
- **Test 3: Unauthorized SSID, Unauthorized Connections - 2.4 GHz band**
  - **Step 1:** Configure a whitelisted AP to operate on a set channel on the 2.4 GHz band with an authorized SSID.
  - **Step 2:** Connect a non-whitelisted EUD to AP.
  - **Step 3:** Verify that the TSF detects the non-whitelisted EUD connecting to the whitelisted AP.
  - **Step 4:** Change the AP's SSID to one not on the authorized list.
  - **Step 5:** Connect a whitelisted EUD to AP.
  - **Step 6:** Verify that the TSF detects the whitelisted AP using unauthorized SSID and the EUD associating to an unauthorized SSID.
- **Test 4: Unauthorized SSID, Unauthorized Connections - 5 GHz band**
  - **Step 1:** Configure a whitelisted AP to operate on a set channel on the 5 GHz band with an authorized SSID.
  - **Step 2:** Connect a non-whitelisted EUD to AP.
  - **Step 3:** Verify that the TSF detects the non-whitelisted EUD connecting to the whitelisted AP.
  - **Step 4:** hange the AP's SSID to one not on the authorized list.
  - **Step 5:** Connect a whitelisted EUD to AP.
  - **Step 6:** Verify that the TSF detects the whitelisted AP using unauthorized SSID and the EUD associating to an unauthorized SSID.

FAU_WID_EXT.2 Wireless Intrusion Detection – Passive Information Flow Monitoring

TSS
The evaluator shall verify that the TSS includes which channels the TOE can detect and monitor. Additionally, the TSS shall include whether the TOE simultaneously or nonsimultaneously monitors network traffic across these channels. The evaluator shall verify that the TSS includes information on if the sensors are completely passive, by default, or if the sensors ability to transmit data is configurable. The evaluator shall verify that the TSS describes the methods that the TOE uses to detect the presence of unauthorized connections and unauthorized network traffic.

Guidance
The evaluator shall review the operational guidance for how to configure the TOE to monitor the channels as selected in the

SFR. If the sensor ability to transmits data is configurable, the evaluator shall review the operational guidance for how to disable wireless transmissions from the sensor. The TOE shall have the ability to perform stateful frame inspection and log attacks spanning multiple frames. The evaluator shall verify that the operational guidance provides instructions on how to specify and confirm that stateful frame capture and inspection is being performed.

Tests
Channels Monitored

- **Test 1:** Channels on On 5GHz band
  - **Step 1:** Configure the TSF to monitor the channels as selected in the SFR.
  - **Step 2:** Deploy an AP on at least 2 different channels within the regulatory domain on 5GHz band.
  - **Step 3:** Deploy an AP on at least 2 different channels outside the regulatory domain on 5GHz band.
  - **Step 4:** Verify that the AP gets detected on each channel tested.
- **Test 2:** Channels on 2.4GHz band
  - **Step 1:** Configure the TSF to monitor the channels as selected in the SFR.
  - **Step 2:** Deploy AP on at least 2 different channels within the regulatory domain on 2.4GHz band.
  - **Step 3:** Deploy AP on at least 2 different channels outside the regulatory domain on 2.4GHz band.
  - **Step 4:** Verify that the AP gets detected on each channel tested.
- **Test 3:** Non-standard channel frequencies
  - **Step 1:** Configure the TSF to monitor the channels as selected in the SFR.
  - **Step 2:** Deploy AP on at least 2 different channels on non-standard channel frequencies.
  - **Step 3:** Verify that the AP gets detected on each channel tested.

Wireless Sensor Transmission of Data

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

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

- **Test 1: MAC Spoofing**
  - **Step 1:** Spoof mac address of whiteliste EUD connected to a whitelisted AP on a second EUD.
  - **Step 2:** Connect EUD with spoofed MAC address to another whitelisted AP while the valid EUD it is spoofing is connected to the first AP.
  - **Step 3:** Verify that the TSF detected the MAC spoofing.
- **Test 2: MAC Spoofing**
  - **Step 1:** Spoof mac address of whiteliste AP on a second AP.
  - **Step 2:** Verify that the TSF detected the MAC spoofing.
- **Test 3: Active Probing**
  - **Step 1:** Perform an active scan on the subnet of the WLAN.
  - **Step 2:** Record tools used and type of scan performed.
  - **Step 3:** Verify that the TSF detects the active probing.
- **Test 4: Point-to-Point Wireless Bridges**
  - **Step 1:** Setup a point-to-point wireless bridge using whitelisted APs in the range of the wireless sensors.
  - **Step 2:** Verift that the TSF detects the bridge.
- **Test 5: NULL Client Associations**
  - **Step 1:** Deploy whitelisted AP.
  - **Step 2:** Configure the AP to have null SSID.
  - **Step 3:** Attempt to connect a whitelisted EUD to the AP without supplying the correct AP SSID.
  - **Step 4:** Verify that the AP does not permit the EUD to complete an association by returning a Probe Request.
  - **Step 5:** If an association does occur, confirm that an alert is triggered due to a violation of policy.

Stateful Frame Inspection

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

FAU_WID_EXT.3 Wireless Intrusion Detection – Denial of Service

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

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

Tests

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

FAU_WID_EXT.4 Wireless Intrusion Detection – Unauthorized Authentication Schemes

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

Guidance
The evaluator shall examine the operational guidance to verify that it provides instructions on how to define a WLAN authentication scheme as authorized or unauthorized for the purposes of detection.

Tests
The evaluator shall configure the TOE, per FMT_SMF.1/WIDS, with 802.1x authentication as the only mode of authorized WLAN authentication scheme.

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

FAU_WID_EXT.5 Wireless Intrusion Detection – Unauthorized Encryption Schemes

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

Guidance
There are no operational guidance activities.

Tests

- **Test 1:**
  - **Step 1:** Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.
  - **Step 2:** Deploy a whitelisted AP with no encryption.
  - **Step 3:** Connect a whitelisted EUD to AP.

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

2.1.4 User Data Protection (FDP)

FDP_IFC.1 Information Flow Control Policy

TSS
There are no TSS assurance activities for this SFR.

Guidance
If this functionality is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure the TOE to monitor different types of IEEE 802.11 frame types and subtypes.

Tests

- **Test 1:**
    - Set the WIDS sensor for a set channel
    - Start a traffic capture from the WIDS sensor
    - Send a set number of frames on the sensor's operating channel for all IEEE 802.11 a, b, g, n, ac frame types and subtypes from/to the following:
        - *authorized APs and authorized EUDs*
        - *authorized APs and unauthorized EUDs*
        - *unauthorized APs and authorized EUDs*
    - Verify that there are frames from all the types and subtypes in the capture.

2.1.5 Security Management (FMT)

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

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

Guidance
There are no operational guidance activities for this SFR.

Tests

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

3 Evaluation Activities for Optional SFRs

3.1 Security Audit (FAU)

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

TSS
The evaluator shall verify that the TSS includes the set of RF bands and technologies that the TSF can detect the use of. The

TSS should also include instructions on how to enable and the hardware that is necessary for the additional band detection.

Guidance
The evaluator shall verify that the operational guidance describes how to enable and configure detection of the technologies included in the ST as well as the hardware that is needed to perform this function.

Tests
The evaluator shall enable and configure detection of the selected technologies.

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

FAU_WID_EXT.7 Wireless Intrusion Detection – Wireless Spectrum Analysis

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

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

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

4 Evaluation Activities for Selection-Based SFRs

4.1 Security Audit (FAU)

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

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

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

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

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

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

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

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

Guidance
The evaluator shall verify that the operational guidance provides information on how to configure user-defined and customizable attack signatures, including a description of the customization options that are available.

Tests

- **Test 1:**
  - **Step 1:** Craft a signature with the available fields indicated in the TSS.
  - **Step 2:** Send a crafted frame that matches the signature to a whitelisted EUD
  - **Step 3:** Verify that the TSF triggers an alert based on the newly defined signature.

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

TSS
The evaluator shall verify that the TSS includes the list of trusted channels (as specified in FTP_ITC.1) available in the TSF to transmit packet captures to an external entity. The evaluator shall verify that the TSS describes the ability of the TOE to store

packet capture data within itself, how much storage space is available for packet capture data and where that data is stored. The evaluator shall verify that the TSS describes the behavior of the TOE when local storage space for packet capture data is exhausted and whether this behavior is configurable.

Guidance
The evaluator shall verify that the operational guidance provides instructions on how to configure the trusted channel. If the behavior of the TOE when local storage space for packet capture data is exhausted is configurable, the evaluator shall verify that the operational guidance provides information on what the configurable behaviors are and how they can be set.

Tests

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

5 Evaluation Activities for Objective SFRs

5.1 Security Audit (FAU)

FAU_INV_EXT.5 Detection of Unauthorized Connections

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

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

Tests

- **Test 1:**
  - **Step 1:** Deploy a non-whitelisted AP.
  - **Step 2:** Connect the AP via wire to the protected network infrastructure.
  - **Step 3:** Check the WIDS user interface for a list of detected APs and EUDs.
  - **Step 4:** Verify that the rogue AP is detected and an alert generated on the detection of an AP connected to the protected wired infrastructure.

FAU_INV_EXT.6 Signal Library

TSS
There are no TSS assurance activities for this SFR.
Guidance
The evaluator shall review the operational guidance for instructions on how to locate and verify that the WIDS comes preloaded with a signal library, as well as possesses the ability to import, export, and update the existing signal library if present.

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

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

FAU_MAC_EXT.1 Device Impersonation

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

Guidance
The evaluator shall verify that the operational guidance provides instructions on how to deploy the TOE in a manner that allows the TSF to detect when two sensors in non-overlapping locations receive traffic from the same MAC address

simultaneously (i.e. information about the range and placement of sensors to ensure non-overlapping coverage).

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

Tests

- **Test 1:**
  - **Step 1:** Setup a whitelisted AP (Location 1).
  - **Step 2:** Connect a whitelisted EUD to AP.
  - **Step 3:** Setup a second whitelisted AP and a non-whitelisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-verlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).
  - **Step 4:** Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the whitelisted AP in location 2. Make sure both EUDs are connected at the same time.
  - **Step 5:** Verify that the TSF detected and generated an alert.
- **Test 2:**
  - **Step 1:** Configure the timeframe allowed between connection of two EUDs in two separate locations (Location 1, Location 2).
  - **Step 2:** Setup a whitelisted AP (Location 1).
  - **Step 3:** Connect a whitelisted EUD to AP.
  - **Step 4:** Setup a second whitelisted AP and a non-whitelisted EUD in a separate non-overlapping location where the WIDS also has sensors. Or simulate the distant non-verlapping locations by deploying the second AP in a shielded environment connected to the valid network (Location 2).
  - **Step 5:** Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the whitelisted AP in location 2. Make sure that the time between connections is shorter than the time timeframe allowed/configured.
  - **Step 6:** Verify that the TSF detected and generated an alert.

FAU_WIP_EXT.1 Wireless Intrusion Prevention

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

Guidance
There are no operational guidance activities for this SFR.

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

- **Test 1:**
  - **Step 1:** Deploy a non-whitelisted AP and connect to the protected wired infrastructure via wire (make sure it gets classified as rogue, or manually classify as such).
  - **Step 2:** Connect a whitelisted EUD to the AP.
  - **Step 3:** Verify that TSF generates an alert, breaks the connection of the whitelisted EUD from the rogue AP, and contains the rogue AP.

5.2 Protection of the TSF (FPT)

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

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

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

Tests

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

6 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the ND PP base to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The ND PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module

includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

7 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

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.