Supporting Document
Mandatory Technical Document

PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS)
Version: 1.0
2020-09-30
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	2020-09-30	Initial Release - PP-Module for NDcPP

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

Acknowledgments:
This SD was developed with support from NIAP Wireless Intrusion Detection/Prevention Systems (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
1.2 Structure of the Document
1.3 Terms
1.3.1 Common Criteria Terms
1.3.2 Technical Terms
2 Evaluation Activities for SFRs
2.1 Collaborative Protection Profile for Network Device
2.1.1 Modified SFRs
2.2 TOE SFR Evaluation Activities
2.3 Evaluation Activities for Optional SFRs
2.4 Evaluation Activities for Selection-Based SFRs
2.5 Evaluation Activities for Objective SFRs
3 Evaluation Activities for SARs
4 Required Supplementary Information

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) is to describe the security functionality of Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Network Device, version 2.2e

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

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 [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory

Testing Laboratory	Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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-PPs.
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.
Target of Evaluation (TOE)	The product under evaluation.
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.

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	A security product that provides network security administrators with the ability to

Intrustion Prevention System (WIPS)	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 workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled 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 workunit 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 PP.

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 workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled 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 workunits 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 Collaborative Protection Profile for Network Device

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

2.1.1 Modified SFRs

This PP-Module mandates the inclusion of this selection-based SFR because a TOE that conforms to this PP-Module will always be deployed in a configuration that requires this SFR to be claimed. The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component. This SFR is selection-based in the Base-PP but is mandated by this PP-Module because the ST author must claim a distributed TOE selection in FAU_STG_EXT.1.2. There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than selection-based, but there is no change to how the SFR must be implemented. This PP-Module modifies the Base-PP SFR to remove a selection that is not permitted by the TOE architecture that it specifies. The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1. The TSF shall be able to store generated audit data on the TOE itself. In addition The TOE shall be a distributed TOE that stores audit data on the following TOE components: identification of TOE components The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data . This SFR is modified from its definition in the Base-PP by removing the selection option for the TOE to be standalone. A TOE that conforms to this PP-Module is expected to be distributed. There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to remove one of the possible selection items, but there is no change to how the SFR is to be implemented. This PP-Module mandates the inclusion of this optional SFR because it is required to implement functionality required by this PP-Module. The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place. The TSF shall implement a registration process in which components establish and use a communications channel that uses A channel that meets the secure channel requirements in FTP_ITC.1 FPT_ITT.1 A channel that meets the secure registration channel requirements in FTP_TRP.1/Join No channel for at least TSF data. The TSF shall enable a Security Administrator to disable communications between any pair of TOE components. This SFR is optional in the NDcPP but is mandated by this PP-Module because the WIDS TOE is expected to be a distributed system. There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than optional, but there is no change to how the SFR is to be implemented. This PP-Module mandates the inclusion of this optional SFR because it is required to implement functionality required by this PP-Module. 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 IPsec SSH TLS DTLS HTTPS . FPT_ITT.1 is optional in NDcPP, however, since a WIDS/WIPS TOE is

distributed, FPT_ITT.1 shall be included in the ST 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. There is no change to the EAs specified for this SFR in the NDcPP SD. The PP-Module modifies this SFR to make its inclusion mandatory rather than optional, but there is no change to how the SFR is to be implemented. This PP-Module refines the Base-PP SFR to add a selection for a specific external entity that may be applicable to a TOE that conforms to this PP-Module. The TSF shall be capable of using IPsec SSH TLS DTLS HTTPS to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, authentication server database server 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. This SFR is modified from its definition in the Base-PP by adding a selection for a database server capability. If the TSF uses a separate database server to support its security-relevant functionality, this selection must be included in the ST. The intent of the database server is to store WIDS/WIPS data that must be queryable, such as events/alarms, triangulation calculations, wireless spectrum analysis (including RF jammer/Denial of Service (DoS)), and packet capture analysis. Authorized Administrators must be permitted to view alarms, raw event data, and any other data stored in the database. The Administrator must access the database through a trusted channel if done so remotely. The intent of this 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 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. There is no change to the EAs specified for this SFR in the NDcPP SD. If ‘database server’ is selected in FTP_ITC.1.1, the evaluator shall ensure that the required tests are performed on that external interface in addition to the other claimed interfaces. The evaluator shall also perform test 4 for this SFR in the NDcPP SD, which is objective in NDcPP.

2.2 TOE SFR Evaluation Activities

This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. The TSF shall display an alert to Authorized Administrator in sufficient detail to include identity of APs and EUDs involved, signal strength, accurate event timestamp, description of alert and severity level and capture raw frame traffic that triggered the violation no other actions upon detection of a potential security violation. If "capture raw frame traffic that triggers the violation" is selected then FAU_STG_EXT.1/PCAP must be included in the ST. FAU_SAA.1 defines the rules for monitoring the wireless traffic to detect for potential security violations. FAU_INV_EXT.2 defines the information the TOE needs to collect for all APs and EUDs within range of the the TOE's sensors. Device attributes can then be individually filtered and/or selected in order to be displayed as part of the alert. The evaluator shall verify that the TSS describes where to find the WIDS alerts on the Administrator console/interface. The evaluator shall use the operational guidance for instructions on where the alerts generated are displayed within the WIDS interface. If "capture raw frame traffic that triggers the violation is selected", the evaluator shall use the operational guidance to configure the traffic capture capabilities. The evaluator shall perform a series of events or generate traffic that would successfully trigger an alert for each of the rules defined in FAU_SAA.1. The evaluator should verify and record whether the TOE generated the alert for each rule, and provided sufficient details. The evaluator should also record the events or traffic that was generated as each alert was attempted to be triggered and record the details provided by the TOE in the alert. [conditional] If capturing of raw frames was selected, verify that the packet capture was triggered and stored as appropriate. This family defines requirements for suppression of audit events. It is intended to complement the FAU_ARP family already defined in CC Part 2. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to implement a filtering mechanism to selectively suppress the generation of security alarms. No specific management functions have been identified. There are no auditable events foreseen. FAU_ARP.1 Security Alarms The TSF shall provide the ability to apply methods of selection to selectively exclude alerts from being generated. The evaluator shall verify that the TSS describes the ability of the TOE to filter WIDS/WIPS alerts. The evaluator shall verify that the operational guidance includes instructions on enabling and disabling alerts. 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 disable the alert. The evaluator shall then generate events as in previous test that should successfully trigger the alert. The evaluator shall verify that the TOE did not generate an alert. This SFR iterates the FAU_GEN.1 SFR defined in the Base-PP to define auditable events for the functionality that is specific to this PP-Module. The TSF shall be able to generate an audit record of the following auditable events: Start-up and shutdown of the audit functions; All auditable events for the [not specified] level of audit; [Auditable events listed in the Auditable Events table (); Failure of wireless sensor communication]. RequirementAuditable EventsAdditional Audit Record Contents FAU_ANO_EXT.1 (selection-based)NoneNone FAU_ARP.1Actions taken due to potential security violationsNone FAU_ARP_EXT.1NoneNone FAU_GEN.1/WIDSNoneNone FAU_IDS_EXT.1NoneNone FAU_INV_EXT.1Presence of allowedlisted deviceType of device (AP or EUD), MAC Address FAU_INV_EXT.2NoneNone

FAU_INV_EXT.3Location of AP or EUDMAC 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.4 (objective)NoneNone FAU_INV_EXT.5 (objective)NoneNone FAU_MAC_EXT.1 (objective)NoneNone FAU_RPT_EXT.1NoneNone FAU_SAA.1NoneNone FAU_SIG_EXT.1 (selection-based)NoneNone FAU_STG_EXT.1/PCAP (selection-based)NoneNone FAU_WID_EXT.1Detection of rogue AP or EUDNone Detection of unauthorized SSIDNone FAU_WID_EXT.2Sensor wireless transmission capabilitiesWireless transmission capabilities are turned on FAU_WID_EXT.3 (optional)Detection of network devices operating in selected RF bandsFrequency 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.4 (optional)NoneNone FAU_WIP_EXT.1 (objective)Isolation of AP or EUDDescription 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.1NoneNone FMT_SMF.1/WIDSNoneNone FPT_FLS.1 (objective)Information about failureIndication that there was a failure, type of failure, device that failed, and time of failure : Auditable Events The auditable events defined in 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 should be combined with those of the NDcPP in the context of a conforming Security Target. The Auditable Events () 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. The TSF shall record within each audit record at least the following information: Date and time of the event, type of event, and subject identity (if applicable); For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [auditable events listed in Auditable Events table ()]. The subject identity in this case is the allowlisted inventory item. There are no TSS evaluation activities for this SFR. There are no operational guidance activities for this SFR. The evaluator shall test the TOE’s ability to correctly generate audit records by having the TOE generate audit records in accordance with the evaluation 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. This family defines requirements for supported methods of intrusion detection. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to specify the methods of intrusion detection that it supports. No specific management functions are identified. There are no auditable events foreseen. No dependencies. The TSF shall provide the following methods of intrusion detection anomaly-based signature-based other detection method . At least one detection method must be selected. If multiple detection methods are supported, each supported method must 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. 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. The evaluator shall verify that the operational guidance provides instructions on how to configure the TOE in order for it to detect such intrusions. 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. This family defines requirements for detection and inventorying of network assets in the TOE’s operational environment. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to determine if inventoried objects are authorized or unauthorized. The following actions could be considered for the management functions in FMT: Definition of inventory of authorized APs based on MAC address Definition of inventory of authorized EUDs based on MAC address The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Presence of allowlisted device FAU_INV_EXT.2 Characteristics of Environmental Objects The TSF shall determine if a given AP is authorized based on MAC addresses other unique device identifier The TSF shall determine if a given EUD is authorized based on MAC addresses other unique device identifier The TSF shall detect the presence of non-allowlisted EUDs and APs in the Operational Environment. This inventory is used as an allowlist to indicate to the WIDS which APs and EUDs are authorized members of the wireless network. The inventory of authorized APs and EUDs is configured by FMT_SMF.1/WIDS. The terminology used to describe an inventoried or allowlisted device may vary by vendor product. This PP-Module utilizes allowlisted to describe APs and EUDs that are part of the inventory and non-allowlisted to describe APs and EUDs that are not part of the inventory. 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. 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. Per guidance in FMT_SMF.1/WIDS, add MAC Addresses or other unique device identifier for an AP and EUD to the allowlist. Deploy the AP and EUD that were added to allowlist within the range of the TOE's sensors. Verify that the devices are classified as authorized. Remove the EUD from the allowlist. Verify that the EUD is classified as unauthorized. Remove the AP from the allowlist. Verify that the AP is classified as unauthorized. Deploy an allowlisted AP and EUD, and connect the EUD to the AP. Verify that the list of detected APs and EUDs contains the allowlisted AP and EUD that were just deployed. If the AP and EUD are detected verify that they are classified as allowlisted devices. Deploy a non-allowlisted AP and EUD and connect the EUD to the AP. Verify that the list of detected APs and EUDs contains the non-allowlisted AP and EUD that were just deployed. If the AP and EUD are detected verify that they are not classified as allowlisted devices. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to discover network assets in its operational environment and maintain an inventory of them based on

collected attributes. The following actions could be considered for the management functions in FMT: Definition of classification rules to detect rogue APs There are no auditable events foreseen. No dependencies. The TSF shall detect the Current RF band Current channel MAC Address Received signal strength Device detection timestamps Classification of APs and EUDs other details no other details of all APs and EUDs within range of the TOE's wireless sensors. The TSF shall detect the following additional details for all APs within range of the TOE's wireless sensors: encryption number of connected EUDs. Received frames/packets Beacon rate SSID of AP (if not hidden). 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. The TSF shall detect the follow additional details for all EUDs within range of the TOE's wireless sensors: SSID and BSSID of AP it is connected to. DHCP configuration. The evaluator shall verify that the TSS explains the capability of detecting the information specified in the requirements for all APs and EUDs within the TOE's wireless range. 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. Deploy an allowlisted AP, non-allowlisted AP and two allowlisted EUDs. Connect one allowlisted EUD to the allowlisted AP and one to the non-allowlisted AP. Check the WIDS user interface for a list of detected APs and EUDs. Verify that current RF band, current channel, MAC Address, received signal strength, device detection timestamps, 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, SSID (if not hidden), received frames/packets and beacon rate are presented. For EUDs verify that the SSID and BSSID of AP it is connected and DHCP configuration is presented. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to approximate the physical location of network assets in its operational environment based on triangulation of wireless emissions. No specific management functions are identified. The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Physical location and identification of AP or EUD FAU_INV_EXT.2 Characteristics of Environmental Objects The TSF shall detect the physical location of APs and EUDs to within value equal or less than 25 feet of their actual location. The TSF shall detect received signal strength and RF power levels above a predetermined threshold no other characteristics of hardware operating within range of the TOE’s wireless sensors. 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. 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. Deploy an AP within range of the sensors. Verify the TSF provides location tracking information about the AP. Verify the AP location presented is within 25 feet actual location. Deploy an AP within range of the sensors. Check the WIDS user interface for a list of detected APs and EUDs. Verify that the current received signal strength is part of the information presented on the WIDS user interface about the APs and EUDs. This family defines requirements for the format of generated reports. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to implement a specified reporting mechanism for collected data for compatibility with third parties that may consume this data. No specific management functions are identified. There are no auditable events foreseen. FAU_GEN.1 Audit Data Generation The TSF shall provide Syslog using defined API Syslog other detection method SNMP trap reporting using defined API Simple Network Management Protocol (SNMP) other detection method for reporting of collected data. Syslog and/or SNMP trap reporting can be used. At least one reporting method must be selected. The TSF shall provide the ability to import data, such as an allowlist of APs and EUDs, and WIDS/WIPS configuration files from the system using custom API Syslog common log format CSV vendor detection method . The system must 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. The evaluator shall verify that the TSS includes which method the TOE utilizes. There are no operational guidance activities for this SFR. Depending on the detection technique used by the TOE, the evaluator shall confirm and note the existence of the capability. Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire. Confirm that the TSF can observe and capture traffic and events generated by the AP. Confirm that the TSF can use the reporting mechanisms specified in the TSS. Verify that the TSF can import and export observable event data in each of the formats specified in the TSS. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. 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. The TSF shall enforce the following rules for monitoring wireless traffic: Accumulation or combination of subset of defined auditable events known to indicate a potential security violation, Detection of non-allowlisted AP, Detection of non-allowlisted EUD, Detection of authorized EUD establishing peer-to-peer connection with any other EUD, Detection of EUD bridging two network interfaces, Detection of unauthorized point-to-point wireless bridges by allowlisted APs, Alert generated by violation of user defined signature, Detection of ICS connection, Detection of traffic with excessive transmit power level, Detection of MAC spoofing, Detection of unauthorized AP broadcasting authorized SSIDs, Detection of authorized AP broadcasting an unauthorized SSID, Detection of allowlisted EUD connected to unauthorized SSID, Detection of NULL SSID associations, Detection of active probing, Detection of packet flooding/DoS/DDoS, Detection of RF-based denial of service, Detection of deauthentication flooding, Detection of disassociation flooding, Detection of request-to-send/clear-to-send abuse, Detection of unauthorized authentication scheme use, Detection of unauthorized encryption scheme use, Detection of unencrypted traffic, Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations, Detection of extremely high numbers of client devices using a

particular allowlisted AP, Detection of a high number of failed attempts to join the WLAN in a short period of time, Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic, such as Probes, Auths, and Assoc frames, Detection of the physical location of an identified WLAN threat by using triangulation, Detection of an SSID using weak/unsupported/disallowed encryption options, Detection of AP SSID larger than 32 bytes, any other rules. These rules are used to detect a potential security violation. Maintenance of the rules by adding, modifying or deletion of rules from the set of rules is handled by FMT_SMF.1/WIDS. If a potential security violation is detected the alert generated for the Administrator is handled by FAU_ARP.1. The evaluator shall verify that the TSS describes the ability of the TOE to detect the network behavior described by the SFR. 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. The evaluator shall examine the TSS to verify that it describes the denial of service attacks that can be detected by the TOE. The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized WLAN authentication schemes and 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. If the ability of the TSF to detect the different potential security violations is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure the TOE. Detection of non-allowlisted AP: Deploy a non-allowlisted AP. Verify that the AP is detected as a non-allowlisted AP. Detection of non-allowlisted EUD: Deploy a non-allowlisted EUD. Verify that the EUD is detected as an non-allowlisted EUD. Detection of authorized EUD establishing peer-to-peer connection with any other EUD: Create the following connections between two allowlisted EUDs. Windows Ad Hoc Connection Mac OS Ad Hoc Linux Ad Hoc Wi-Fi Direct Create the following connections between one allowlisted EUD and a non-allowlisted EUD Windows Ad Hoc Connection Mac OS Ad Hoc Linux Ad Hoc Wi-Fi Direct Verify that alerts were generated by each of the connections in each test. Detection of EUD bridging two network interfaces: Bridge two network interfaces on an allowlisted EUD (one must be the wireless card listed as allowlisted). Create a Windows Hosted Network with an allowlisted EUD. Connect a different allowlisted EUD to the network. Verify that alerts were generated by each of the connections in each test. Detection of unauthorized point to point wireless bridges by allowlisted APs: Setup a point-to-point wireless bridge using allowlisted APs in the range of the wireless sensors. Verify that the TSF detects the bridge. Alert generated by violation of user defined signature: Setup a user defined detection signature. Verify that the TSF generates an alert once the rules of signature have been violated. Detection of ICS connection: Setup an Internet Connection Sharing (ICS) connection. Verify that the TSF detects the establishment of the ICS connection. Detection of traffic with excessive transmit power level: Configure a source of network traffic that can exceed the maximum transmit power levels of 100mW on 2.4 GHz, 200mW on 5 GHz, and 250mW on 6 GHz. Configure a user defined signature to detects traffic with transmit power levels that exceed the maximum. Commence with the transmission of network traffic at excessive power levels. Collect wireless traffic with range of the TSF. Verify that the TSF detects wireless traffic that exceeds 100mW on 2.4 GHz, 200mW on 5 GHz, and 250mW on 6 GHz. Detection of MAC spoofing: Spoof mac address of allowliste EUD connected to an allowlisted AP on a second EUD. Connect EUD with spoofed MAC address to another allowlisted AP while the valid EUD it is spoofing is connected to the first AP. Verify that the TSF detected the MAC spoofing. Spoof mac address of allowliste AP on a second AP. Verify that the TSF detected the MAC spoofing. Detection of unauthorized AP broadcasting authorized SSIDs: Configure a non-allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an authorized SSID. Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID. Repeat the test utilizing the 5 GHz band. Repeat the test utilizing the 6 GHz band. Detection of authorized AP broadcasating an unathorized SSID: Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an unauthorized SSID. Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID. Repeat the test utilizing the 5 GHz band. Repeat the test utilizing the 6 GHz band. Detection of allowlisted EUD connected to unauthorized SSID: Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band with an unauthorized SSID. Connect an allowlisted EUD to the AP. Verify that the TSF detects the allowlisted EUD associated to the allowlisted AP broadcasting an unauthorized SSID. Repeat the test utilizing the 5 GHz band. Repeat the test utilizing the 6 GHz band. Detection of NULL SSID associations: Deploy allowlisted AP. Configure the AP to have null SSID. Attempt to connect an allowlisted EUD to the AP without supplying the correct AP SSID. Verify that the AP does not permit the EUD to complete an association by returning a Probe Request. If an association does occur, confirm that an alert is triggered due to a violation of policy. Detection of active probing: Perform an active scan on the subnet of the WLAN. Record tools used and type of scan performed. Verify that the TSF detects the active probing. Detection of packet flooding/DoS/DDoS: Generate a large amount of TCP and UDP traffic from a single EUD. Verify that the TSF detects the network-based DoS. Generate a large amount of TCP and UDP traffic from multiple EUDs. Verify that the TSF detects the network-based DDoS. Detection of RF-based denial of service: Deploy an allowlisted AP and configure to stay in a particular channel. Connect an allowlisted EUD to the AP. Use an RF Jammer or signal generator on the same frequency as the AP and EUD to create a RF-based DoS. Verify that the TOE detects the RF-based DoS. Detection of deauthentication flooding: Deploy allowlisted AP and configure to a set channel. Connect an allowlisted EUD to the AP. Send an flood of deauthentication frames to the EUD using the MAC address of allowlisted AP it is connected to. Verify that the TSF detects the deauthentication flood. Deploy allowlisted AP and configure to a set channel. Connect an allowlisted EUD to the AP. Send an flood of deauthentication frames with the MAC address of allowlisted AP as the source and destination as a broadcast. Verify that the TSF detects the deauthentication flood. Detection of disassociation flooding: Deploy an allowlisted AP and connect authorized EUDs. Generate disassociation frames from an unauthorized EUD. Verify that the TSF detected the disassociation flooding. Detection of request-to-send/clear-to-send abuse: Deploy allowlisted AP and configure to a set channel. Connect two allowlisted EUDs to the AP. Send an flood of CTS frames to reserve RF medium. Verify that the TSF detects the CTS abuse. Detection of unauthorized authentication scheme use: The evaluator shall configure the TOE, per FMT_SMF.1/WIDS, with 802.1x authentication as the only mode of authorized WLAN authentication scheme. Deploy an allowlisted AP with open authentication. Connect an allowlisted EUD to AP. Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes. Deploy an allowlisted AP that uses pre-shared key authentication. Connect an allowlisted EUD to AP. Verify that the TSF

detects the AP and the EUD using unauthorized authentication schemes. Detection of unauthorized encryption scheme use: Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme. Deploy an allowlisted AP with no encryption. Connect an allowlisted EUD to AP. Verify that the TOE detects the AP and the EUD using unauthorized encryption schemes. Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme. Deploy an allowlisted AP that uses TKIP encryption only. Connect an allowlisted EUD to AP. Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes. Detection of unencrypted traffic: Deploy an allowlisted AP with no encryption. Connect an allowlisted EUD to AP and generate traffic. Verify that the TOE detects unencrypted data frames being sent between the allowlisted AP and EUD. Connect a non-allowlisted EUD to AP and generate traffic. Verify that the TSF detects unencrypted data frames being sent between the allowlisted AP and non-allowlisted EUD. Deploy a non-allowlisted AP with no encryption. Connect an allowlisted EUD to AP and generate traffic. Verify that the TSF detects unencrypted data frames being between the non-allowlisted AP and allowlisted EUD. Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations: Deploy an allowlisted AP that utilizes the 802.11g or older WLAN protocol. Verify that the TSF detects the weak/outdated WLAN protocol and generates an alert. Detection of extremely high numbers of client devices using a particular allowlisted AP: Deploy an allowlisted AP. Configure a threshold amount of client devices that can use a particular AP. Connect enough client devices to the AP to purposely exceed the defined threshold. Verify that the TSF detects when the client usage exceeds the threshold. Detection of a high number of failed attempts to join the WLAN in a short period of time: Deploy an allowlisted AP. Configure a threshold amount of connection attempts that can occur in a particular timeframe. Attempt to authenticate to the AP with enough client devices to purposely exceed the defined threshold. Verify that the TSF detects when the connection attempts within the specic timeframe exceeds the threshold. Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic: Deploy an allowlisted AP. Verify that the TSF detects when WLAN scanners are the source of WLAN traffic. Detection of the physical location of an identified WLAN threat by using triangulation: Deploy a non-allowlisted AP or EUD within range of the TSF. Verify that the TSF can track and locate the AP or EUD to within 5 meters. Detection of an SSID using weak/unsupported/disallowed encryption options: Deploy an allowlisted AP and configure its encryption options. Change the encryption options the AP advertises. Verify that the TSF detects when the AP's encryption options change. Detection of AP SSID larger than 32 bytes: Deploy an allowlisted AP and configure its SSID to be larger than 32 bytes. Configure a user defined signature on the WIDS to detect when an SSID is larger than 32 bytes. Verify that the TSF detects when the AP's SSID is larger than 32 bytes. This family defines requirements for data collection of potentially malicious wireless network activity. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to implement a mechanism to distinguish between authorized and unauthorized network assets. The following actions could be considered for the management functions in FMT: Definition of authorized SSID(s) Definition of authorized WLAN authentication schemes Definition of authorized WLAN encryption schemes Definition of authorized WLAN traffic schemes The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Detection of rogue AP or EUD Detection of unauthorized SSID FAU_INV_EXT.1 Environmental Inventory The TSF shall distinguish between benign and malicious APs and EUDs based on if the APs and EUDs are authorized and automatic detection metrics no other method . FAU_INV_EXT.1 defines that an AP or EUD is authorized based on if the AP/EUD is allowlisted as configured in FMT_SMF.1. A non-allowlisted device does not always have to be conducting malicious activity. However, it is acceptable to equate an allowlisted AP/EUD as both authorized/benign and a nonallowlisted AP/EUD as both not authorized and thus malicious. If the TOE supports automatic malicious device detection, based on in-depth network traffic analysis, "automatic detection metrics" must be selected. This can be used to further distinguish if the AP/EUD is benign or malicious. If the TOE does not support automatic detection metrics, "no other method" must be selected. The TSF shall provide the ability to determine if a given SSID is authorized. FMT_SMF.1/WIDS defines the subset of authorized SSID(s). The evaluator shall verify that the TSS describes how the TOE detects malicious APs/EUDs and whether the TOE supports automatic detection. The evaluator shall verify that the TSS includes how the TOE determines if a given SSID is authorized. If TOE supports automatic detection, the evaluator shall verify that the operational guidance contains instructions for configuring the automatic detection metrics. The evaluator shall verify that the operational guidance provides instructions on how to configure SSIDs as authorized. For test 1 and 2 below the evaluator shall verify that the TOE detects and appropriately classifies the APs and EUDs. It is acceptable if the TOE uses different but equivalent descriptors for the classification. If the TOE does not support automatic detection metrics and equates a non-allowlisted AP/EUD as malicious, than it is sufficient that the the classification given to the AP/EUD in step 1 is the same as in step 2. If the TOE supports automatic detection metrics and distinguishes between a non-allowlisted AP/EUD and a malicious AP/EUD, then the classification for the AP/EUD should differ between step 1 and step 2. Deploy a non-allowlisted AP in the area of the WIDS sensor, but take no action against the network. Verify that the AP is classified as non-authorized. Deploy a non-allowlisted AP in the area of the WIDS sensor and launch an attack against the network. This can be any variation of Fake AP, Spoof AP, Flood or DoS attack. Verify that the AP is classified as malicious. Deploy a non-allowlisted EUD in the area of the WIDS sensor, but take no action against the network. Verify that the EUD is classified as non-authorized. Launch an RF Flooding, DoD/DDoS, masqueraded or spoofing attack against authorized AP with an unauthorized EUD. Verify that the EUD is classified as malicious. Deploy an AP with an unauthorized SSID in the area of the WIDS sensor. Verify that the TOE detects the unauthorized SSID. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to surveil certain wireless frequency bands and perform stateful inspection of traffic on them. The following actions could be considered for the management functions in FMT: Definition of authorized and unauthorized TCP/IP and UDP traffic Definition of known malicious activity ports Definition of the amount of time that a sensor monitors a specific frequency or channel The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Sensor wireless transmission capabilities No dependencies. The TSF shall simultaneously nonsimultaneously monitor and analyze network traffic matching

the 802.11 monitoring SFP for all channels in the following RF frequencies: 2.4 GHz 5.0 GHz 6.0 GHz and specified Wi-Fi channels in the 4.9 GHz regulatory domain channels outside regulatory domain non-standard channel frequencies no other domains . If "nonsimultaneously" is selected, then "Define the amount of time sensor monitors a specific channel" must 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 FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs. The TSF shall provide wireless sensors to detect network traffic matching the 802.11 monitoring SFP that can be configured to prevent transmission of data does not transmit data . If "can be configured to prevent transmission of data" is selected then "Enable/Disable transmission of data by wireless sensor" must 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 FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs. The TSF shall perform stateful frame inspection and log attacks spanning multiple frames. 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. 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 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 evaluator shall verify that the operational guidance provides instructions on how to specify and confirm that stateful frame capture and inspection is being performed. Channels Monitored Channels on On 5GHz band Configure the TSF to monitor the channels as selected in the SFR. Deploy an AP on at least 2 different channels within the regulatory domain on 5GHz band. Deploy an AP on at least 2 different channels outside the regulatory domain on 5GHz band. Verify that the AP gets detected on each channel tested. Channels on 2.4 GHz band Configure the TSF to monitor the channels as selected in the SFR. Deploy AP on at least 2 different channels within the regulatory domain on 2.4 GHz band. Deploy AP on at least 2 different channels outside the regulatory domain on 2.4 GHz band. Verify that the AP gets detected on each channel tested. Channels on 4.9 GHz band (if selected) Configure the TSF to monitor the channels specified in the SFR. Deploy AP and set to channels within the 4.9 GHz band outlined in the TSS. Verify that the AP gets detected on each channel tested. Channels on 6 GHz band (if selected) Configure the TSF to monitor the channels specified in the SFR. Deploy AP and set to channels within the 6 GHz band outlined in the TSS. Verify that the AP gets detected on each channel tested. Non-standard channel frequencies (if selected) Configure the TSF to monitor the channels as selected in the SFR. Deploy AP on at least 2 different channels on non-standard channel frequencies. 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 2.4 GHz, 5 GHz, and 6 GHz band. Boot a sensor and using the signal analyzer observe to check if any eminations are coming from the sensor. Verify that the signal analyzer does not pick up emanations from the sensor. During normal sensor operations, observe the analyzer for about 10 minutes to check if any eminations are coming from the sensor. Verify that the signal analyzer does not pick up emanations from the sensor. Stateful Frame Inspection Deploy allowlisted AP. Connect an allowlisted EUD to the AP. Deploy a protocol analyzer or native capability within the WIDS Controller between the AP and EUD. Verify from the network traffic packet capture that all frames are being inspected to validate their connection state from the TSF

FAU_ARP.1 Security Alarms

FAU_ARP.1
TSS
The evaluator shall verify that the TSS describes where to find the WIDS alerts on the Administrator console/interface.

Guidance
The evaluator shall use the operational guidance for instructions on where the alerts generated are displayed within the WIDS interface. If "capture raw frame traffic that triggers the violation is selected", 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 for each of the rules defined in FAU_SAA.1. The evaluator should verify and record whether the TOE generated the alert for each rule, and provided sufficient details. The evaluator should also record the events or traffic that was generated as each 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.1 Security Alarm Filtering

FAU_ARP_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to filter WIDS/WIPS alerts.

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

Tests

- **Test 1:**
  - **Step 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.
  - **Step 2:** The evaluator shall disable the alert. The evaluator shall then generate events as in previous test that should successfully trigger the alert. The evaluator shall verify that the TOE did not generate an alert.

FAU_GEN.1/WIDS Audit Data Generation (WIDS)

FAU_GEN.1/WIDS
TSS
There are no TSS evaluation 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 evaluation 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_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods

FAU_IDS_EXT.1
TSS
The evaluator shall verify that the TSS includes which intrusion detection method(s) the TOE utilizes. If multiple methods are selected, the evaluator shall confirm that the TSS describes how the different methods are incorporated.

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

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

FAU_INV_EXT.1 Environmental Inventory

FAU_INV_EXT.1
TSS
The evaluator shall verify that the TSS describes how the presence of authorized EUDs and APs is presented by the TOE. The evaluator shall verify that the TSS includes where in the WIDS interface the list of detected APs and EUDs is displayed.

Guidance
The evaluator shall verify that the operational guidance provides instructions on how to view authorized and 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 or other unique device identifier for an AP and EUD to the allowlist.
  - **Step 2:** Deploy the AP and EUD that were added to allowlist 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 allowlist.
    - **Step 5:** Verify that the EUD is classified as unauthorized.
    - **Step 6:** Remove the AP from the allowlist.
    - **Step 7:** Verify that the AP is classified as unauthorized.
- **Test 2:**
    - **Step 1:** Deploy an allowlisted AP and EUD, and connect the EUD to the AP.
    - **Step 2:** Verify that the list of detected APs and EUDs contains the allowlisted AP and EUD that were just deployed.
    - **Step 3:** If the AP and EUD are detected verify that they are classified as allowlisted devices.
- **Test 3:**
    - **Step 1:** Deploy a non-allowlisted AP and EUD and connect the EUD to the AP.
    - **Step 2:** Verify that the list of detected APs and EUDs contains the non-allowlisted AP and EUD that were just deployed.
    - **Step 3:** If the AP and EUD are detected verify that they are not classified as allowlisted devices.

FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.2
TSS
The evaluator shall verify that the TSS explains the capability of detecting the information specified in the requirements for all 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 an allowlisted AP, non-allowlisted AP and two allowlisted EUDs.
    - **Step 2:** Connect one allowlisted EUD to the allowlisted AP and one to the non-allowlisted 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, received signal strength, device detection timestamps, 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, SSID (if not hidden), received frames/packets and beacon rate are presented. For EUDs verify that the SSID and BSSID of AP it is connected and DHCP configuration is presented.

FAU_INV_EXT.3 Location of Environmental Objects

FAU_INV_EXT.3
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 TSF provides location tracking information about the AP.
    - **Step 3:** Verify the AP location presented is within 25 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_RPT_EXT.1 Intrusion Detection System - Reporting Methods

FAU_RPT_EXT.1

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

Guidance
There are no operational guidance activities for this SFR.

Tests
Depending on the detection technique used by the TOE, the evaluator shall confirm and note the existence of the capability.

- **Test 1:**
  - **Step 1:** Deploy an allowlisted 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 use the reporting mechanisms specified in the TSS.
  - **Step 4:** Verify that the TSF can import and export observable event data in each of the formats specified in the TSS.

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to detect the network behavior described by the SFR. 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. The evaluator shall examine the TSS to verify that it describes the denial of service attacks that can be detected by the TOE. The evaluator shall verify that the TSS describes the ability of the TOE to detect when unauthorized WLAN authentication schemes and 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
If the ability of the TSF to detect the different potential security violations is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure the TOE.

Tests

- **Test 1: Detection of non-allowlisted AP**:
  - **Step 1:** Deploy a non-allowlisted AP.
  - **Step 2:** Verify that the AP is detected as a non-allowlisted AP.

- **Test 2: Detection of non-allowlisted EUD**:
  - **Step 1:** Deploy a non-allowlisted EUD.
  - **Step 2:** Verify that the EUD is detected as an non-allowlisted EUD.

- **Test 3: Detection of authorized EUD establishing peer-to-peer connection with any other EUD**:
  - **Test 3.1:** Create the following connections between two allowlisted EUDs.
    - Windows Ad Hoc Connection
    - Mac OS Ad Hoc
    - Linux Ad Hoc
    - Wi-Fi Direct
  - **Test 3.2:** Create the following connections between one allowlisted EUD and a non-allowlisted EUD
    - Windows Ad Hoc Connection
    - Mac OS Ad Hoc
    - Linux Ad Hoc
    - Wi-Fi Direct

  Verify that alerts were generated by each of the connections in each test.

- **Test 4: Detection of EUD bridging two network interfaces**:
  Bridge two network interfaces on an allowlisted EUD (one must be the wireless card listed as allowlisted).
  - **Step 1:** Create a Windows Hosted Network with an allowlisted EUD.
  - **Step 2:** Connect a different allowlisted EUD to the network.

  Verify that alerts were generated by each of the connections in each test.

- **Test 5: Detection of unauthorized point to point wireless bridges by allowlisted APs**:
  - **Step 1:** Setup a point-to-point wireless bridge using allowlisted APs in the range of the wireless sensors.
  - **Step 2:** Verify that the TSF detects the bridge.

- **Test 6: Alert generated by violation of user defined signature**:
  - **Step 1:** Setup a user defined detection signature.
  - **Step 2:** Verify that the TSF generates an alert once the rules of signature have been violated.

- **Test 7: Detection of ICS connection**:
  - **Step 1:** Setup an Internet Connection Sharing (ICS) connection.

    - **Step 2:** Verify that the TSF detects the establishment of the ICS connection.

- **Test 8: Detection of traffic with excessive transmit power level**:
    - **Step 1:** Configure a source of network traffic that can exceed the maximum transmit power levels of 100mW on 2.4 GHz, 200mW on 5 GHz, and 250mW on 6 GHz.
    - **Step 2:** Configure a user defined signature to detects traffic with transmit power levels that exceed the maximum.
    - **Step 3:** Commence with the transmission of network traffic at excessive power levels.
    - **Step 4:** Collect wireless traffic with range of the TSF.
    - **Step 5:** Verify that the TSF detects wireless traffic that exceeds 100mW on 2.4 GHz, 200mW on 5 GHz, and 250mW on 6 GHz.

- **Test 9: Detection of MAC spoofing**:
    - **Test 9.1:**
        - **Step 1:** Spoof mac address of allowliste EUD connected to an allowlisted AP on a second EUD.
        - **Step 2:** Connect EUD with spoofed MAC address to another allowlisted 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 9.2:**
        - **Step 1:** Spoof mac address of allowliste AP on a second AP.
        - **Step 2:** Verify that the TSF detected the MAC spoofing.

- **Test 10: Detection of unauthorized AP broadcasting authorized SSIDs**:
    - **Step 1:** Configure a non-allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an authorized SSID.
    - **Step 2:** Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID.
    - **Step 3:** Repeat the test utilizing the 5 GHz band.
    - **Step 4:** Repeat the test utilizing the 6 GHz band.

- **Test 11: Detection of authorized AP broadcasating an unathorized SSID**:
    - **Step 1:** Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band broadcasting an unauthorized SSID.
    - **Step 2:** Verify that the TSF detects the non-allowlisted AP broadcasting an authorized SSID.
    - **Step 3:** Repeat the test utilizing the 5 GHz band.
    - **Step 4:** Repeat the test utilizing the 6 GHz band.

- **Test 12: Detection of allowlisted EUD connected to unauthorized SSID**:
    - **Step 1:** Configure an allowlisted AP to operate on a set channel on the 2.4 GHz band with an unauthorized SSID.
    - **Step 2:** Connect an allowlisted EUD to the AP.
    - **Step 3:** Verify that the TSF detects the allowlisted EUD associated to the allowlisted AP broadcasting an unauthorized SSID.
    - **Step 4:** Repeat the test utilizing the 5 GHz band.
    - **Step 5:** Repeat the test utilizing the 6 GHz band.

- **Test 13: Detection of NULL SSID associations**:
    - **Step 1:** Deploy allowlisted AP.
    - **Step 2:** Configure the AP to have null SSID.
    - **Step 3:** Attempt to connect an allowlisted 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.

- **Test 14: Detection of 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 15: Detection of packet flooding/DoS/DDoS**:
    - **Step 1:** Generate a large amount of TCP and UDP traffic from a single EUD.
    - **Step 2:** Verify that the TSF detects the network-based DoS.
    - **Step 3:** Generate a large amount of TCP and UDP traffic from multiple EUDs.
    - **Step 4:** Verify that the TSF detects the network-based DDoS.

- **Test 16: Detection of RF-based denial of service**:
    - **Step 1:** Deploy an allowlisted AP and configure to stay in a particular channel.
    - **Step 2:** Connect an allowlisted 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 17: Detection of deauthentication flooding**:

- **Test 17.1:**
  - **Step 1:** Deploy allowlisted AP and configure to a set channel.
  - **Step 2:** Connect an allowlisted EUD to the AP.
  - **Step 3:** Send an flood of deauthentication frames to the EUD using the MAC address of allowlisted AP it is connected to.
  - **Step 4:** Verify that the TSF detects the deauthentication flood.
- **Test 17.2:**
  - **Step 1:** Deploy allowlisted AP and configure to a set channel.
  - **Step 2:** Connect an allowlisted EUD to the AP.
  - **Step 3:** Send an flood of deauthentication frames with the MAC address of allowlisted AP as the source and destination as a broadcast.
  - **Step 4:** Verify that the TSF detects the deauthentication flood.

- **Test 18: Detection of disassociation flooding**:
  - **Step 1:** Deploy an allowlisted AP and connect authorized EUDs.
  - **Step 2:** Generate disassociation frames from an unauthorized EUD.
  - **Step 3:** Verify that the TSF detected the disassociation flooding.

- **Test 19: Detection of request-to-send/clear-to-send abuse**:
  - **Step 1:** Deploy allowlisted AP and configure to a set channel.
  - **Step 2:** Connect two allowlisted 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.

- **Test 20: Detection of unauthorized authentication scheme use**:
  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 20.1:**
    - **Step 1:** Deploy an allowlisted AP with open authentication.
    - **Step 2:** Connect an allowlisted EUD to AP.
    - **Step 3:** Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.
  - **Test 20.2:**
    - **Step 1:** Deploy an allowlisted AP that uses pre-shared key authentication.
    - **Step 2:** Connect an allowlisted EUD to AP.
    - **Step 3:** Verify that the TSF detects the AP and the EUD using unauthorized authentication schemes.

- **Test 21: Detection of unauthorized encryption scheme use**:
  - **Test 21.1:**
    - **Step 1:** Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.
    - **Step 2:** Deploy an allowlisted AP with no encryption.
    - **Step 3:** Connect an allowlisted EUD to AP.
    - **Step 4:** Verify that the TOE detects the AP and the EUD using unauthorized encryption schemes.
  - **Test 21.2:**
    - **Step 1:** Configure the TOE with 128 bit AES encryption type as the only allowed encryption scheme.
    - **Step 2:** Deploy an allowlisted AP that uses TKIP encryption only.
    - **Step 3:** Connect an allowlisted EUD to AP.
    - **Step 4:** Verify that the TSF detects the AP and the EUD using unauthorized encryption schemes.

- **Test 22: Detection of unencrypted traffic**:
  - **Test 22.1:**
    - **Step 1:** Deploy an allowlisted AP with no encryption.
    - **Step 2:** Connect an allowlisted EUD to AP and generate traffic.
    - **Step 3:** Verify that the TOE detects unencrypted data frames being sent between the allowlisted AP and EUD.
    - **Step 4:** Connect a non-allowlisted EUD to AP and generate traffic.
    - **Step 5:** Verify that the TSF detects unencrypted data frames being sent between the allowlisted AP and non-allowlisted EUD.
  - **Test 22.2:**
    - **Step 1:** Deploy a non-allowlisted AP with no encryption.
    - **Step 2:** Connect an allowlisted EUD to AP and generate traffic.
    - **Step 3:** Verify that the TSF detects unencrypted data frames being between the non-allowlisted AP and allowlisted EUD.

- **Test 23: Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations**:
  - **Step 1:** Deploy an allowlisted AP that utilizes the 802.11g or older WLAN protocol.

    - **Step 2:** Verify that the TSF detects the weak/outdated WLAN protocol and generates an alert.

- **Test 24: Detection of extremely high numbers of client devices using a particular allowlisted AP**:
    - **Step 1:** Deploy an allowlisted AP.
    - **Step 2:** Configure a threshold amount of client devices that can use a particular AP.
    - **Step 3:** Connect enough client devices to the AP to purposely exceed the defined threshold.
    - **Step 4:** Verify that the TSF detects when the client usage exceeds the threshold.

- **Test 25: Detection of a high number of failed attempts to join the WLAN in a short period of time**:
    - **Step 1:** Deploy an allowlisted AP.
    - **Step 2:** Configure a threshold amount of connection attempts that can occur in a particular timeframe.
    - **Step 3:** Attempt to authenticate to the AP with enough client devices to purposely exceed the defined threshold.
    - **Step 4:** Verify that the TSF detects when the connection attempts within the specic timeframe exceeds the threshold.

- **Test 26: Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic**:
    - **Step 1:** Deploy an allowlisted AP.
    - **Step 2:** Verify that the TSF detects when WLAN scanners are the source of WLAN traffic.

- **Test 27: Detection of the physical location of an identified WLAN threat by using triangulation**:
    - **Step 1:** Deploy a non-allowlisted AP or EUD within range of the TSF.
    - **Step 2:** Verify that the TSF can track and locate the AP or EUD to within 5 meters.

- **Test 28: Detection of an SSID using weak/unsupported/disallowed encryption options**:
    - **Step 1:** Deploy an allowlisted AP and configure its encryption options.
    - **Step 2:** Change the encryption options the AP advertises.
    - **Step 3:** Verify that the TSF detects when the AP's encryption options change.

- **Test 29: Detection of AP SSID larger than 32 bytes**:
    - **Step 1:** Deploy an allowlisted AP and configure its SSID to be larger than 32 bytes.
    - **Step 2:** Configure a user defined signature on the WIDS to detect when an SSID is larger than 32 bytes.
    - **Step 3:** Verify that the TSF detects when the AP's SSID is larger than 32 bytes.

FAU_WID_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects

FAU_WID_EXT.1
TSS
The evaluator shall verify that the TSS describes how the TOE detects malicious APs/EUDs and whether the TOE supports automatic detection. The evaluator shall verify that the TSS includes how the TOE determines if a given SSID is authorized.

Guidance
If TOE supports automatic detection, the evaluator shall verify that the operational guidance contains instructions for configuring the automatic detection metrics. The evaluator shall verify that the operational guidance provides instructions on how to configure SSIDs as authorized.

Tests
For test 1 and 2 below the evaluator shall verify that the TOE detects and appropriately classifies the APs and EUDs. It is acceptable if the TOE uses different but equivalent descriptors for the classification. If the TOE does not support automatic detection metrics and equates a non-allowlisted AP/EUD as malicious, than it is sufficient that the the classification given to the AP/EUD in step 1 is the same as in step 2. If the TOE supports automatic detection metrics and distinguishes between a non-allowlisted AP/EUD and a malicious AP/EUD, then the classification for the AP/EUD should differ between step 1 and step 2.

- **Test 1:**
    - **Step 1:** Deploy a non-allowlisted AP in the area of the WIDS sensor, but take no action against the network. Verify that the AP is classified as non-authorized.
    - **Step 2:** Deploy a non-allowlisted AP in the area of the WIDS sensor and launch an attack against the network. This can be any variation of Fake AP, Spoof AP, Flood or DoS attack.
    - **Step 3:** Verify that the AP is classified as malicious.
- **Test 2:**
    - **Step 1:** Deploy a non-allowlisted EUD in the area of the WIDS sensor, but take no action against the network. Verify that the EUD is classified as non-authorized.
    - **Step 2:** Launch an RF Flooding, DoD/DDoS, masqueraded or spoofing attack against authorized AP with an unauthorized EUD.
    - **Step 3:** Verify that the EUD is classified as malicious.

- **Test 3:**
  - **Step 1:** Deploy an AP with an unauthorized SSID in the area of the WIDS sensor.
  - **Step 2:** Verify that the TOE detects the unauthorized SSID.

FAU_WID_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring

FAU_WID_EXT.2
TSS
The evaluator shall verify that the TSS includes which channels the TOE can detect and monitor. Additionally, the TSS shall include whether the TOE simultaneously or nonsimultaneously monitors network traffic across these channels. The evaluator shall verify that the TSS includes information on if the sensors are completely passive, by default, or if the sensors ability to transmit data is configurable.

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 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 2.4 GHz 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 2.4 GHz band.
  - **Step 3:** Deploy AP on at least 2 different channels outside the regulatory domain on 2.4 GHz band.
  - **Step 4:** Verify that the AP gets detected on each channel tested.
- **Test 3:** Channels on 4.9 GHz band (if selected)
  - **Step 1:** Configure the TSF to monitor the channels specified in the SFR.
  - **Step 2:** Deploy AP and set to channels within the 4.9 GHz band outlined in the TSS.
  - **Step 3:** Verify that the AP gets detected on each channel tested.
- **Test 4:** Channels on 6 GHz band (if selected)
  - **Step 1:** Configure the TSF to monitor the channels specified in the SFR.
  - **Step 2:** Deploy AP and set to channels within the 6 GHz band outlined in the TSS.
  - **Step 3:** Verify that the AP gets detected on each channel tested.
- **Test 5:** Non-standard channel frequencies (if selected)
  - **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 2.4 GHz, 5 GHz, and 6 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.

Stateful Frame Inspection

- **Test 1:**
  - **Step 1:** Deploy allowlisted AP.
  - **Step 2:** Connect an allowlisted EUD to the AP.
  - **Step 3:** Deploy a protocol analyzer 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

This SFR defines operations to be performed on assets in the TOE’s operational environment, which is

behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. 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]. "Authorized" EUDs/APs are those that are assigned to the allowlist 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 FAU_WID_EXT.1, FAU_WID_EXT.2, in addition to optional SFRs FAU_WID_EXT.3 and FAU_WID_EXT.4. A vendor does not have to formally define this policy, it only needs to comply with the SFRs. There are no TSS evaluation activities for this SFR. 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. Deploy an allowlisted AP/WIDS Start a traffic capture from the AP/WIDS sensor Send a set number of frames to the sensor 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.

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1
TSS
There are no TSS evaluation 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:**
  - Deploy an allowlisted AP/WIDS
  - Start a traffic capture from the AP/WIDS sensor
  - Send a set number of frames to the sensor 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.

This SFR iterates the FMT_SMF.1 SFR defined in the Base-PP to define management functions for the functionality that is specific to this PP-Module. The TSF shall be capable of performing the following management functions for WIDS functionality: Define an inventory of authorized APs based on MAC addresses other unique device identifier , 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, Specify periods of network activity that constitute baseline of expected behavior Define anomaly activity Define classification rules to detect rogue APs 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 frequency channel Define authorized and unauthorized TCP/IP and UDP traffic Define known malicious activity ports No other capabilities . 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" must 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" must 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" must be selected. It is expected that an Authorized Administrator will be responsible for configuring the AP to operate on a specific frequency pursuant to the 802.11 standard. The TSF will have the ability to adjust the amount of time it passively monitors and captures WLAN traffic on a given frequency and channel. The evaluator shall review the TSS to verify that it includes information the ability of the TOE to define inventory of authorized APs and EUDs. The evaluator shall verify that the TSS describes the ability of the TOE to allow authorized administrators to define authorized WLAN authentication schemes. The evaluator shall review the operational guidance for instructions on how to configure and change clasification of APs and EUDs to indicate that they are part of the allowlist. The evaluator shall review the operational guidance to determine how to configure which SSIDs are permitted on the network. 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. The evaluator shall examine the operational guidance to verify that it provides instructions on how to define a WLAN encryption scheme as authorized or unauthorized for the purposes of detection. The evaluator shall define an inventory of authorized APs and EUDSs. The ability to detect allowlisted and non-allowlisted APs and EUDs will be tested in FAU_INV_EXT.1 and FAU_SAA.1. The evaluator shall define authorized SSIDs. The ability to detect authorized and unauthorized SSIDs will be tested in FAU_WID_EXT.2.3 and FAU_SAA.1. The evaluator shall configure the TSF with a set of allowed authentication and encryption schemes. The ability to detect violation of this policy will be tested in FAU_SAA.1. (conditional): If "Define the amount of time sensor monitors a specific frequency or channel" is selected: Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire. Confirm that the TSF can observe and capture traffic and events generated by the AP. 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. Confirm that the TSF remains on the frequency and channel for the time period specified.

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

FMT_SMF.1/WIDS
TSS
The evaluator shall review the TSS to verify that it includes information the ability of the TOE to define inventory of authorized APs and EUDs.

The evaluator shall verify that the TSS describes the ability of the TOE to allow authorized administrators to define authorized WLAN authentication schemes.

Guidance
The evaluator shall review the operational guidance for instructions on how to configure and change clasification of APs and EUDs to indicate that they are part of the allowlist.

The evaluator shall review the operational guidance to determine how to configure which SSIDs are permitted on the network.

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.

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

Tests

- **Test 1:** The evaluator shall define an inventory of authorized APs and EUDSs. The ability to detect allowlisted and non-allowlisted APs and EUDs will be tested in FAU_INV_EXT.1 and FAU_SAA.1.
- **Test 2:** The evaluator shall define authorized SSIDs. The ability to detect authorized and unauthorized SSIDs will be tested in FAU_WID_EXT.2.3 and FAU_SAA.1.
- **Test 3:** The evaluator shall configure the TSF with a set of allowed authentication and encryption schemes. The ability to detect violation of this policy will be tested in FAU_SAA.1.
- **Test 4:** (conditional): If "Define the amount of time sensor monitors a specific frequency or channel" is selected:
  - **Step 1:** Deploy an allowlisted 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.

2.3 Evaluation Activities for Optional SFRs

This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to surveil certain radio frequency bands that fall outside the typical wireless spectrum used by consumer-grade electronics. No specific management functions are identified. The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Detection of network devices operating in selected RF bands No dependencies. The TSF shall detect the presence of network devices that operate in the following RF bands: 3.6 GHz 60 GHz sub-GHz (0-900 MHz) all cellular bands . This SFR refers to Non-WLAN (IEEE 802.11 a, b, g, n, and ac) network devices that operate in the specified frequencies. There is an understanding that this capability requires a TOE to use specialized, licensed radio systems. This SFR will allow for the introduction of an open API, set of defined interoperability standards, or other proprietary solution(s), to allow for third-party integrations. 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. 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. The evaluator shall enable and configure detection of the selected technologies. Deploy a device within the given technology and verify that the TSF detects the device. This SFR defines an optional capability for a distributed component to be dedicated to one particular function. This function (wireless spectrum analysis) is defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to implement wireless spectrum analysis in a dedicated physical component. No specific management functions are identified. There are no auditable events foreseen. [FAU_WID_EXT.2 Wireless Intrusion Detection - Passive Information Flow Monitoring, or FAU_WID_EXT.3 Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring] The TSF shall provide a dedicated sensor for wireless spectrum analysis. The evaluator shall verify that the TSS to verify that the TOE provides a dedicated sensor for wireless spectrum analysis. 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. The evaluator shall enable and configure dedicated spectrum analysis and test the capabilities listed in the TSS.

FAU_WID_EXT.3 Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring

FAU_WID_EXT.3
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.4 Wireless Intrusion Detection - Wireless Spectrum Analysis

FAU_WID_EXT.4
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.

2.4 Evaluation Activities for Selection-Based SFRs

This family defines requirements for detection of malicious network activity based on anomalous behavior. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to define how it determines anomalous network traffic that may be indicative of malicious activity. The following actions could be considered for the management functions in FMT: Specification of periods of network activity that constitute baselines of expected behavior Definition of anomaly activity There are no auditable events foreseen. FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods The TSF shall support the definition of baselines ('expected and approved') anomaly ('unexpected') traffic patterns including the specification of throughput (data elements (e.g. bytes, packets, etc.) per time period (e.g. minutes, hours, days)) time of day frequency thresholds other methods and the following network protocol fields: all management and control frame header elements. The TSF shall support the definition of anomaly activity through manual configuration by administrators automated configuration . 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"). 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. 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. 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. This family defines requirements for detection of malicious network activity based on traffic signatures. This SFR defines operations to be performed on collected WIDS data, which is collected using an external interface defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to support the definition of traffic signatures that can be compared to observed network traffic for the purpose of identifying potential malicious activity. The following actions could be considered for the management functions in FMT: Definition of attack signatures There are no auditable events foreseen. FAU_IDS_EXT.1 Intrusion Detection System - Intrusion Detection Methods The TSF shall support user-defined and customizable attack signatures. The evaluator shall verify that the TSS describes the user-defined and customizable attack signatures that the TOE can define. 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. Craft a signature with the available fields indicated in the TSS. Send a crafted frame that matches the signature to an allowlisted EUD Verify that the TSF triggers an alert based on the newly defined signature. This SFR iterates the FAU_STG_EXT.1 SFR defined in the Base-PP for storage of audit data and applies it to storage of packet captures. The TSF shall be able to transmit the generated packet captures to an external IT entity hosting a protocol analyzer using a trusted channel according to FTP_ITC.1. 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 must 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. The TSF shall be able to store generated packet captures on the TOE itself. In addition The TOE shall be a distributed TOE that stores packet capture data on the following TOE components: identification of TOE components The TOE shall be a distributed TOE with storage of packet capture data provided externally for the following TOE components: list of TOE components that do not store packet capture data locally and the other TOE components to which they transmit their generated packet capture data . The TSF shall drop new packet capture data overwrite previous packet captures according to the following rule: rule for overwriting previous packet captures other action when the local storage space for packet capture data is full. 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. 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. 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. 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. 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.

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

FAU_ANO_EXT.1
TSS
The evaluator shall verify that the TSS describes the composition and construction of baselines or anomaly-based attributes specified in the SFR. The evaluator shall verify that the TSS provides a description of how baselines are defined and implemented by the TSF, or a description of how anomaly-based rules are defined and configured by the administrator.

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

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

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

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

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

FAU_SIG_EXT.1
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 an allowlisted EUD
  - **Step 3:** Verify that the TSF triggers an alert based on the newly defined signature.

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

FAU_STG_EXT.1/PCAP

TSS
The evaluator shall verify that the TSS includes the list of trusted channels (as specified in FTP_ITC.1) available in the TSF to transmit packet captures to an external entity. The evaluator shall verify that the TSS describes the ability of the TOE to store packet capture data within itself, how much storage space is available for packet capture data and where that data is stored. The evaluator shall verify that the TSS describes the behavior of the TOE when local storage space for packet capture data is exhausted and whether this behavior is configurable.

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

Tests

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

2.5 Evaluation Activities for Objective SFRs

This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to identify if an unauthorized network asset in its inventory is attempting to access a protected network using a wired connection. No specific management functions are identified. There are no auditable events foreseen. FAU_INV_EXT.1 Environmental Inventory The TSF shall detect when non-allowlisted APs have a wired connection to the internal corporate network. 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. 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. Deploy a non-allowlisted AP. Connect the AP via wire to the protected network infrastructure. Check the WIDS user interface for a list of detected APs and EUDs. Verify that the rogue AP is detected and an alert generated on the detection of an AP connected to the protected wired infrastructure. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to maintain a signal library. No specific management functions are identified. There are no auditable events foreseen. No dependencies. The TSF shall include a signal library. The TSF will need to have the ability to import, export, or update the exisiting signal library. There are no TSS evaluation activities for this SFR. 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. 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. Deploy an allowlisted AP and connect it to the protected wired infrastructure via wire. Confirm and note whether the TSF has an existing signal library. If existence is confirmed, verify that the TSF can import, export, and update the existing signal library. This family defines requirements for detection of potential device impersonation on the basis of MAC address spoofing. This SFR defines operations to be performed on assets in the TOE’s operational environment, which is behavior defined in this PP-Module that extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to detect possible MAC address spoofing using various methods. No specific management functions are identified. There are no auditable events foreseen. FAU_INV_EXT.2 Characteristics of Environmental Objects The TSF shall detect when two sensors in non-overlapping locations receive traffic from the same MAC address simultaneously. The intent of this SFR is to detect MAC spoofing where an attacker is able to cause the allowlisted EUD to disconnect and promptly connects a non-allowlisted device using the MAC address of the allowlisted EUD. The TSF shall detect when two sensors in non-overlapping locations receive traffic from the MAC addresses of non-allowlisted EUDs within an Authorized administrator-configurable timeframe based on distance between sensors. The intent of this SFR is to allow the administrator to determine the time that should be allowed between an allowlisted EUD connecting in two distant locations. 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. 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. Setup an allowlisted AP (Location 1). Connect an allowlisted EUD to AP. Setup a second allowlisted AP and a non-allowlisted 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). Spoof the MAC address of the EUD in location 1

with the EUD in location 2 and connect it to the allowlisted AP in location 2. Make sure both EUDs are connected at the same time. Verify that the TSF detected and generated an alert. Configure the timeframe allowed between connection of two EUDs in two separate locations (Location 1, Location 2). Setup an allowlisted AP (Location 1). Connect an allowlisted EUD to AP. Setup a second allowlisted AP and a non-allowlisted 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). Spoof the MAC address of the EUD in location 1 with the EUD in location 2 and connect it to the allowlisted AP in location 2. Make sure that the time between connections is shorter than the time timeframe allowed/configured. Verify that the TSF detected and generated an alert. This family defines requirements for wireless intrusion prevention. This SFR defines WIPS behavior in response to detection of potential malicious activity in the TOE's operational environment. This extends the logical scope of the TOE beyond what the Base-PP defines. requires the TSF to support reactive behavior if potential malicious traffic is observed to be originating from or targeted to a particular network asset. The following actions could be considered for the management functions in FMT: Enabling or disabling transmission of data by wireless sensor The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: Isolation of AP or EUD FAU_WID_EXT.1 Wireless Intrusion Detection - Malicious Environmental Objects 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: wireless containment wire-side containment of an unauthorized AP connected to the internal corporate wired network . 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. The evaluator shall verify that the TSS includes a list of available containment methods on the TSF and how to configure them. There are no operational guidance activities for this SFR. Configure the containment methods available on the TSF and perform the following test for each method. Deploy a non-allowlisted AP and connect to the protected wired infrastructure via wire (make sure it gets classified as rogue, or manually classify as such). Connect an allowlisted EUD to the AP. Verify that TSF generates an alert, breaks the connection of the allowlisted EUD from the rogue AP, and contains the rogue AP.

FAU_INV_EXT.4 Detection of Unauthorized Connections

FAU_INV_EXT.4
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-allowlisted 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.5 Signal Library

FAU_INV_EXT.5
TSS
There are no TSS evaluation 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 an allowlisted AP and connect it to the protected wired infrastructure via wire.
  - **Step 2:** Confirm and note whether the TSF has an existing signal library.
  - **Step 3:** If existence is confirmed, verify that the TSF can import, export, and update the existing signal library.

FAU_MAC_EXT.1 Device Impersonation

FAU_MAC_EXT.1

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 an allowlisted AP (Location 1).
  - **Step 2:** Connect an allowlisted EUD to AP.
  - **Step 3:** Setup a second allowlisted AP and a non-allowlisted 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 allowlisted 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 an allowlisted AP (Location 1).
  - **Step 3:** Connect an allowlisted EUD to AP.
  - **Step 4:** Setup a second allowlisted AP and a non-allowlisted 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 allowlisted AP in location 2. Make sure that the time between connections is shorter than the time timeframe allowed/configured.
  - **Step 6:** Verify that the TSF detected and generated an alert.

FAU_WIP_EXT.1 Wireless Intrusion Prevention

FAU_WIP_EXT.1
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-allowlisted 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 an allowlisted EUD to the AP.
  - **Step 3:** Verify that TSF generates an alert, breaks the connection of the allowlisted EUD from the rogue AP, and contains the rogue AP.

This SFR defines preservation of a secure state in the event that a failure condition is detected. The Base-PP does not define an SFR for this behavior but this SFR mitigates the T.SECURITY_FUNCTIONALITY_FAILURE threat defined in the Base-PP, so it is clear that this behavior is consistent with the security expectations of the Base-PP. The TSF shall preserve a secure state when the following types of failures occur: [sensor functionality failure, potential compromise of the TSF]. At minimum, the preservation of a secure state requires the generation of audit records when the defined failure conditions occur. 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. 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. 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.

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

FPT_FLS.1

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

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

Tests

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

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base NDcPP 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 NDcPP 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.

4 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.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019