Mapping Between

PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 2020-09-30

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.

- **SI-4, SI-4(14), SC-7**. The primary purpose of a WIDS/WIPS product is to monitor system activity in general, and wireless activity more specifically, which supports SI-4 and SI-4(14). The product also supports SC-7 at a high level if deployed at a wireless network boundary. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that those are all implemented in support of ensuring the proper implementation of SI-4 and SI-4(14).

- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or PP-Configuration supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.

- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

- **PP-Module.** A TOE that conforms to this PP-Module will also conform to the collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. This PP-Module refines some of the NDcPP requirements to ensure consistency between the PP and the PP-Module, but this does not affect the security controls that satisfying those requirements is intended to address.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
TOE Security Functional Requirements				
FAU_ARP.1	**Security Alarms**	SI-4(5)	**System Monitoring:** System-Generated Alerts	A conformant TOE supports this control by generating an alert when suspicious activity is detected.
		SI-4(7)	**System Monitoring:** Automated Response to Suspicious Events	A conformant TOE supports this control by generating a notification in response to detecting suspicious activity.
FAU_ARP_EXT.1	**Security Alarm Filtering**	SI-4(5)	**System Monitoring:** System-Generated Alerts	A conformant TOE supports this control by implementing a mechanism to suppress the generation of certain alerts to allow for control over the compromise indicators that trigger alerts. The control is only satisfied to the extent that the TOE can control the generated alerts to align with the organization's implementation of the control.
FAU_GEN.1/WIDS	**Audit Data Generation (WIDS)**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing. Part (b) is not satisfied by a conformant TOE because the PP-Module does not define functionality to suppress/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_IDS_EXT.1	**Intrusion Detection System - Intrusion Detection Methods**	N/A	**N/A**	This requirement is used to specify the intrusion detection methods that the TOE supports. Any relevant security controls are supported by the other SFRs that are included in the TOE boundary based on claims made here.
FAU_INV_EXT.1	**Environmental Inventory**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by implementing a mechanism to deny the flow of wireless traffic based on the legitimacy of the device from which it originates.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
		AC-18	**Wireless Access**	A conformant TOE supports this control by maintaining an allowlist of known devices, such that a device's absence from this list could prevent it from establishing a wireless connection.
		SC-43	**Usage Restrictions**	A conformant TOE supports part (b) of this control by providing a mechanism to monitor the wireless components that are connected to the system for the purpose of determining whether they are authorized.
		SI-4	**System Monitoring**	A conformant TOE supports this control by implementing a mechanism to identify connected wireless devices for the purpose of determining whether they are authorized.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control by implementing a method to detect rogue wireless devices based on their absence from the inventory of allowed devices.
FAU_INV_EXT.2	**Characteristics of Environmental Objects**	SI-4	**System Monitoring**	A conformant TOE supports this control by implementing a mechanism to identify connected wireless devices for the purpose of determining whether they are authorized.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control by collecting information about wireless devices that may be useful in determining their legitimacy.
FAU_INV_EXT.3	**Location of Environmental Objects**	SI-4	**System Monitoring**	A conformant TOE supports this control by implementing a mechanism to identify the physical

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				location of connected wireless devices for the purpose of determining whether the device is authorized for use in the detected location.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control by implementing a method to detect the physical location of wireless devices, which may aid in determining their legitimacy.
FAU_RPT_EXT.1	**Intrusion Detection System - Reporting Methods**	AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit collected record data to a logically remote location. It can be used to support the enforcement of this control if the recipient of the data is physically remote from the TOE.
		SC-16	**Transmission of Security and Privacy Attributes**	A conformant TOE supports this control by having the ability to import externally-defined configuration settings.
FAU_SAA.1	**Potential Violation Analysis**	SI-4	**System Monitoring**	A conformant TOE supports this control by having the ability to apply monitoring rules to collected traffic to determine if it represents potential misuse or a malicious use of the system.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control through its monitoring rules applying specifically to wireless network traffic.
FAU_WID_EXT.1	**Wireless Intrusion Detection - Malicious Environmental Objects**	AC-18	**Wireless Access**	A conformant TOE supports this control by maintaining an allowlist of known devices, such that a device’s absence from this list could prevent it from establishing a wireless connection.
		SC-43	**Usage Restrictions**	A conformant TOE supports part (b) of this control by

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				providing a mechanism to designate a wireless component as potentially malicious and prevent it from connecting to the network.
		SI-4	**System Monitoring**	A conformant TOE supports this control by having the ability to monitor connected devices to determine whether they should be authorized to be on the network.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control through its monitoring rules applying specifically to wireless network devices.
FAU_WID_EXT.2	**Wireless Intrusion Detection - Passive Information Flow Monitoring**	SI-4	**System Monitoring**	A conformant TOE supports this control through satisfying this requirement, which facilitates system monitoring by ensuring that certain types of traffic will be monitored.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	This SFR requires the TOE to implement sensors that can monitor certain types of wireless traffic. This supports SI-4(14) to the extent that analysis of wireless activity cannot be performed without appropriate means to collect evidence of the activity for analysis.
FDP_IFC.1	**Subset Information Flow Control**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by enforcing information control on wireless traffic based on whether or not either end of the connection (AP or EUD) is authorized.
		SI-4	**System Monitoring**	A conformant TOE supports this control through satisfying this requirement, which facilitates system monitoring by ensuring that certain types of traffic will be monitored.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	This SFR requires the TOE to monitor traffic on all 802.11 bands between APs and EUDs regardless of their authorization status. This supports SI-4(14) to the extent that analysis of wireless activity cannot be performed without appropriate means to collect evidence of the activity for analysis.
FMT_SMF.1/WIDS	**Specification of Management Functions (WIDS)**	CM-6	**Configuration Settings**	In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
Optional Requirements				
FAU_WID_EXT.3	**Wireless Intrusion Detection - Non-Wireless Spectrum Monitoring**	SI-4	**System Monitoring**	A conformant TOE supports this control through satisfying this requirement, which facilitates system monitoring by ensuring that certain types of traffic will be monitored.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	This SFR requires the TOE to monitor traffic on certain RF bands that are outside the traditional 802.11 wireless spectrum. This supports SI-4(14) to the extent that analysis of wireless activity cannot be performed without appropriate means to collect evidence of the activity for analysis.
FAU_WID_EXT.4	**Wireless Intrusion Detection - Wireless Spectrum Analysis**	N/A	**N/A**	The TOE’s claim of this SFR does not support any additional security controls; it just specifies that wireless spectrum analysis is performed by a dedicated

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				physical component if claimed.
Selection-Based Requirements				
FAU_ANO_EXT.1	**Anomaly-Based Intrusion Detection**	SI-4	**System Monitoring**	A conformant TOE supports this control through detection of potential attacks or unauthorized usage of the system by identifying anomalous usage.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control specifically because the anomalous events it detects are related to wireless network activity.
FAU_SIG_EXT.1	**Signature-Based Intrusion Detection**	SI-4	**System Monitoring**	A conformant TOE supports this control through detection of potential attacks or unauthorized usage of the system by identifying markers for attack signatures.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control specifically because the anomalous events it detects are related to wireless network activity.
FAU_STG_EXT.1/PCAP	**Protected Audit Event Storage (Packet Captures)**	AU-4	**Audit Log Storage Capacity**	A conformant TOE allocates some amount of local storage for packet capture data. It can be used to support the enforcement of this control if the amount of storage is consistent with the assignment chosen for the control.
		AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to logically transmit packet capture data to a location in its Operational Environment. While this SFR requires the TSF to store generated packet capture data on the TOE, a minimum storage size or retention period is not specified. Therefore, a TOE may not support the enforcement of this control if the local storage of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				packet capture data is limited or transitory.
		AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to react in a specific manner when the allocated packet capture storage space is full. Depending on the actions taken by the TOE when this occurs and on the assignments chosen for this control, the TOE can be used to support the enforcement of either or both parts of the control.
		AU-5(2)	**Response to Audit Logging Process Failures:** Real-Time Alerts	A conformant TOE has the ability to react in a specific manner when the allocated packet capture storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-5(4)	**Response to Audit Logging Process Failures:** Shutdown on Failure	A conformant TOE has the ability to react in a specific manner when the allocated packet capture storage space is full. A conformant TOE may support the enforcement of this control, depending on the behavior specified in the ST and the assignments chosen for this control.
		AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of packet capture records.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit packet capture data to a logically remote location. It can be used to support the enforcement of this control if the recipient of the audit data is physically remote from the TOE.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Objective Requirements				
FAU_INV_EXT.4	**Detection of Unauthorized Connections**	SC-43	**Usage Restrictions**	A conformant TOE supports this control by detecting whether an unauthorized wireless access point has been connected to the network over a wired interface, which could indicate an attempted circumvention of usage restrictions.
		SI-4	**System Monitoring**	A conformant TOE supports this control by monitoring whether an unauthorized wireless access point has been connected to the network over a wired interface.
		SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE supports this control by monitoring communications traffic for traffic that may involve an unauthorized access point using a wired connection to attempt to circumvent access restrictions.
FAU_INV_EXT.5	**Signal Library**	SI-4	**System Monitoring**	A conformant TOE supports this control through implementation of a signal library that can aid in detection of potential misuse or malicious activity.
		SI-4(14)	**System Monitoring:** Wireless Intrusion Detection	A conformant TOE supports this control specifically because the signal library is used in support of detecting potential wireless intrusion.
FAU_MAC_EXT.1	**Device Impersonation**	AC-18	**Wireless Access**	A conformant TOE supports this control by implementing a mechanism to determine whether spoofing is being used to attempt to circumvent wireless access restrictions.
		IA-3	**Device Identification and Authentication**	A conformant TOE uniquely identifies connected devices via MAC addresses such that it can assume that two devices sharing a MAC

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				address may be indicative of an attempt to circumvent access restrictions.
FAU_WIP_EXT.1	**Wireless Intrusion Prevention**	SC-7(9)	**Boundary Protection:** Restrict Threatening Outgoing Communications Traffic	A conformant TOE supports this control by implementing a mechanism that allows for suppression of a potential rogue or misused wireless network device.
FPT_FLS.1	**Basic Internal TSF Data Transfer Protection**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing in a known state such that it does not process external network traffic until it has been restored to an operational state.