Mapping Between
PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 2021-05-11
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 and 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 specific controls, but typically satisfaction also requires the implementation of operational procedures; furthermore, 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 whether the control is satisfied in the overall system context.
- **Granularity of SFRs versus controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (controls) are at completely different levels of abstraction. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the whole system, broadly across the large number of devices, components, and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way toward the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; particularly, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **IR-4.** Separate from any technical controls that a conformant product implements, the intent of deploying such a product is to support the enforcement of IR-4, both through allowing incidents to be handled and by having some direct role in the response process.
- **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. This PP-Module does not refine any NDcPP SFRs, so it does not affect any security controls in the NDcPP.

Common Criteria Version 3.1R5 SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
TOE Security Functional Requirements				
FAU_GEN.1/IPS	**Audit Data Generation (IPS)**	AU-2	**Event Logging**	A conformant TOE can generate audit records associated with IPS behavior.
		AU-3	**Content of Audit Records**	A conformant TOE can generate audit records that give details about the type of audit event that took place.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE can capture additional details about the event depending on the contents of the audit record.
		AU-12	**Audit Record Generation**	A conformant TOE can generate audit logs. 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.
FMT_SMF.1/IPS	**Specification of Management Functions (IPS)**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. 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.
		SI-4	**System Monitoring**	A conformant TOE supports this control through the implementation of its management functions because these functions directly support the TOE's

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				system monitoring function.
IPS_ABD_EXT.1	**Anomaly-Based IPS Functionality**	SI-4	**System Monitoring**	A conformant TOE supports the detection of potential malicious activities based on anomalous behavior, satisfying part (d) of the control.
		SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE is a network-based IPS that applies its monitoring capabilities to network traffic.
		SI-4(11)	**System Monitoring:** Analyze Communications Traffic Anomalies	A conformant TOE supports the enforcement of this control by detecting anomalous network traffic.
		SI-4(13)	**System Monitoring:** Analyze Traffic and Event Patterns	A conformant TOE supports the control by implementing mechanisms to analyze common traffic and event patterns such that a departure from these patterns is flagged as an anomaly for further analysis.
IPS_IPB_EXT.1	**IP Blocking**	SC-7(11)	**Boundary Protection:** Restrict Incoming Communications Traffic	A conformant TOE can restrict incoming communications traffic based on the source and destination address pairs that represent authorized or unauthorized communications.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
IPS_NTA_EXT.1	**Network Traffic Analysis**	SC-7	**Boundary Protection**	A conformant TOE partially supports part (a) of this control through its ability to monitor network traffic to detect administratively-specified violations. Part (a) of the control has both a 'monitor' and 'control' component. This SFR can be used to satisfy the 'monitor' portion of this; the 'control' portion relates to the specific actions the TSF would take in response to a detected violation, which is beyond the scope of this specific SFR.
		SI-4	**System Monitoring**	A conformant TOE can monitor and analyze network traffic to detect potential attacks, as described in part (d) of the control.
IPS_SBD_EXT.1	**Signature-Based IPS Functionality**	SI-3	**Malicious Code Protection**	A conformant TOE supports the enforcement of this control by detecting signatures of network traffic known to execute malicious code.
		SI-4	**System Monitoring**	A conformant TOE can monitor network and analysis network traffic to detect potential attacks.
		SI-4(13)	**System Monitoring:** Analyze Traffic and Event Patterns	A conformant TOE shall analyze communications traffic and event patterns for the system.
Optional Requirements				
FAU_STG.1/IPS	**Protected Audit Trail Storage (IPS Data)**	AU-9	**Protection of Audit Information**	A conformant TOE can prevent unauthorized modification and deletion of audit records.
		AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE can prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				all modification and deletion of audit records (i.e., there is no 'authorized' ability to do this), it can be used to support the enforcement of this control.
FAU_STG.4	**Prevention of Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE can react in a specific manner when the allocated audit storage space is full. This SFR does not require the TOE to generate an alert when this occurs so only part (b) of the control is satisfied.
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-7(18)	**Boundary Protection:** Fail Secure	A conformant TOE can preserve a secure state for inline interface failures.
IPS_SBD_EXT.2	**Traffic Normalization**	AC-4(24)	**Information Flow Enforcement:** Internal Normalized Format	A conformant TOE supports this control by normalizing fragmented traffic into its intended specification so that malicious actions encapsulated in a tunneling protocol do not go undetected.
		SI-4(25)	**System Monitoring:** Optimize Network Traffic Analysis	A conformant TOE supports the enforcement of this control by eliminating the potential blind spot of malicious traffic that is fragmented across multiple packets by a tunneling protocol.
Objective Requirements				
FAU_ARP.1	**Security Alarms**	SI-4	**System Monitoring**	A conformant TOE implements reactive behavior if traffic is detected that violates the configured IPS policies, which satisfies part (a) of the control. SI-4(12) may be addressed based on the specific actions the TOE takes in response to detection of a potential security violation, but the

Common Criteria Version 3.1R5 SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				assignment in the SFR is open-ended so this will not automatically be the case.
		SI-4(5)	**System Monitoring:** System-Generated Alerts	A conformant TOE supports this control by implementing a mechanism to generate an alert on detection of potential malicious activity in the form of uninspected network traffic.
		SI-4(7)	**System Monitoring:** Automated Response to Suspicious Events	A conformant TOE automatically implements a response if any traffic matching IPS triggers for potential malicious activity is detected.
FAU_SAR.1	**Audit Review**	AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE supports this control for audit records that are specifically related to IPS behavior.
		SI-4	**System Monitoring**	A conformant TOE supports part (g) of this control by implementing a mechanism that allows authorized subjects to review the IPS data that is collected by the TSF.
FAU_SAR.2	**Restricted Audit Review**	AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE supports the enforcement of this control by enforcing read-only access to IPS records to authorized subjects.
FAU_SAR.3	**Selectable Audit Review**	AU-7(1)	**Audit Record Reduction and Report Generation:** Automatic Processing	A conformant TOE supports the enforcement of this control by allowing for sorting and filtering of IPS records.
Implementation-Based Requirements				
FRU_RSA.1	**Maximum Quotas**	SC-6	**Resource Availability**	A conformant TOE supports the enforcement of this control by enforcing quotas on network traffic such that the TOE's inspection resources are always available, or that the TSF

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				can generate an alert when its resources are exhausted.
Selection-Based Requirements				
This PP-Module has no selection-based requirements.				