Mapping Between

collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.11, 15-June-2017

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.
- **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.

Common Criteria Version 3.x 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 has the ability to generate audit

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				records associated with IPS behavior.
		AU-3	**Content of Audit Records**	A conformant TOE has the ability to generate audit records that give details about the type of audit event that took place.
		AU-3(1)	**Content of Audit Records**	A conformant TOE has the ability to capture additional details about the event depending on the contents of the audit record.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to 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 system monitoring function.
IPS_ABD_EXT.1	**Anomaly-Based IPS Functionality**	SI-4	**System Monitoring**	A conformant TOE supports the detection of potential

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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 has the ability to restrict incoming communications traffic based upon the source and destination address pairs that represent authorized or unauthorized communications.
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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SI-4	**System Monitoring**	A conformant TOE has the ability to monitor network 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 has the ability to 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	**Protected Audit Trail Storage (IPS Data)**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing 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 (IPS Data)**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to 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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FMT_MOF.1/IPS	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of the TOE's IPS function unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage the TOE's IPS function.
FMT_MTD.1/IPS	**Management of IPS Data**	AC-3	**Access Enforcement**	A conformant TOE will not permit manipulation of its stored data unless proper authorization is provided.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage IPS data.
FMT_SMR.2/IPS	**Security Roles (IPS)**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE defines a role-based access model that allows individual users to be assigned to different IPS administrative roles.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE has the ability to enforce differing levels of access control to individual management roles.
FPT_FLS.1/Inline	**Failure with Preservation of Secure State**	SC-7(18)	**Boundary Protection:** Fail Secure	A conformant TOE has the capability to preserve a secure state for inline interface failures.
		SC-24	**Fail In Known State**	A conformant TOE has the capability to preserve a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				secure state for inline interface failures.
FPT_ITT.1	**Basic Internal TSF Data Transfer Protection**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between remote distributed TOE components.
		SC-8(1)	**Transmission Confidentiality and Integrity**: Cryptographic Protection	A conformant TOE will use cryptographic methods to protect data in transit between different parts of the TOE.
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 may generate an alert when its resources are exhausted.
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.
Selection-Based Requirements				
This EP has no selection-based requirements.				
Objective Requirements				
FAU_ARP.1	**Security Alarms**	SI-4	**System Monitoring**	A conformant TOE implements reactive

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				behavior in the event that 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 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 (IPS Data)**	AU-7	**Audit 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 (IPS Data)**	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 (IPS Data)**	AU-7(1)	**Audit Record Reduction and Report**	A conformant TOE supports the enforcement of this control by allowing for

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Generation: Automatic Processing	sorting and filtering of IPS records.