Mapping Between PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 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.
- **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		**Supports Enforcement of NIST SP 800-53 Revision 5 Control**		**Comments and Observations**
Mandatory Requirements				
FAU_GEN.1	**Audit Data Generation**	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.
		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 does not define functionality to suppress/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FDP_RIP.2	**Full Residual Information Protection**	SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by ensuring that memory buffers used to temporarily store network packet data cannot be used to that same data in a different packet.
		SC-8(2)	**Transmission Confidentiality and Integrity:** Pre – and - Post Transmission Handling	A conformant TOE supports this control by ensuring the confidentiality of network packet data.
FFW_RUL_EXT.1	**Stateful Traffic Filtering**	SC-7	**Boundary Protection**	A conformant TOE supports the enforcement of this control by acting as a boundary device for its managed interfaces. Note that depending on the intended usage of the TOE, one or more of control enhancements (25) through (28) may also apply.

		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports the enforcement of parts (a) and (b) of this control by enforcing traffic policy rules on managed interfaces. Part (c) is not enforced by the TOE because is it not responsible for the encryption of through traffic, and parts (d) and (e) are not enforced because these relate to organizational policies.
				Parts (f), (g) are enforced for the prevention of unauthorized of exchange of control plane traffic with external and internal networks. Part (h) is enforced to filter unauthorized control plane traffic from external networks.
		SC-7(5)	**Boundary Protection:** Deny by Default - Allow by Exception	A conformant TOE denies network communication traffic by default and allows network communication traffic by exception (i.e., deny all, permit by exception) at the managed interfaces.
		SC-7(11)	**Boundary Protection:** Restrict Incoming Communications Traffic	A conformant TOE determines that the source and destination address pairs represent authorized/allowed communications.
FMT_SMF.1/FFW	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE will satisfy this control to the extent that the TOE provides a method to configure all firewall rules.
Optional Requirements				

FFW_RUL_EXT.2	**Stateful Filtering of Dynamic Protocols**	SC-7(17)	**Boundary** A **Protection:** Automated or Enforcement of to Protocol supported	conformant TOE dynamically defines rules establishes sessions allowing network traffic Formats flow for network protocols.
Selection-Based Requirements				
This PP-Module has no selection-based requirements.				
Objective Requirements				
This PP-Module has no objective requirements.				