Mapping Between

PP-Module for Session Border Controllers, Version 1.0, 2022-12-05

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 or 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 certain controls, but typically satisfaction also requires the implementation of operational procedures. Further, given that systems are typically the product of the 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.
- **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; in particular, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **SC-7.** The primary purpose of a Session Border Controller (SBC) product is to act as a network boundary protection device between Voice and Video over IP (VVoIP) devices and communication networks. An SBC product therefore supports the enforcement of SC-7 in general at a high level. 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 SC-7 and relevant sub-controls are the behaviors that an SBC is intended to address. Note that SBC products are also generally deployed to facilitate interoperability between different communication networks (e.g. VVoIP and legacy telephone networks), but this is beyond the scope of 800-53 controls.
- **SA-4(7).** Generally, 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, if the TOE claims the optional requirement FIA_SIPS_EXT.1, it will enforce password-based authentication on SIP registration. Any password composition requirements on SIP registration will be enforced on that function and interface only. Additionally, FIA_SIPS_EXT.1 only addresses the character composition of passwords, it does not address other aspects of the control such as password history requirements. 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 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Mandatory Requirements (presented alphabetically)				
FAU_ARP_EXT.1	**Security Audit Automatic Response**	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.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses a trusted channel (SNMPv3) to transmit alarms.
FAU_GEN.1/SBC	**Audit Data Generation (Session Border Controller)**	AU-2	**Event Logging**	A conformant TOE can 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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE can 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 or enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_SAA.1	**Potential Violation Analysis**	SI-4	**System Monitoring**	A conformant TOE supports this control by having the ability to flag certain events as potential security violations.
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of this control by providing a mechanism to determine the set of auditable events that result in the generation of audit records.
FCS_SRTP_EXT.1	**Secure Real-time Transport Protocol**	SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE uses SRTP to ensure confidentiality and integrity of telecommunications traffic, which supports part (c) of this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements SRTP to ensure confidentiality and integrity of data in transit.
FDP_IFC.1	**Subset Information Flow Control**	AC-4	**Information Flow Enforcement**	A conformant TOE enforces information flow enforcement by

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				determining when a connection between remote entities is authorized.
		SC-7	**Boundary Protection**	A conformant TOE enforces an information flow control policy that determines when communications across the network boundary are authorized.
		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports part (b) of this control through its enforcement of a traffic flow policy.
FDP_IFF.1	**Simple Security Attributes**	AC-4	**Information Flow Enforcement**	A conformant TOE enforces information flow enforcement by determining when a connection between remote entities is authorized.
		SC-7	**Boundary Protection**	A conformant TOE enforces an information flow control policy that determines when communications across the network boundary are authorized.
		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports part (b) of this control through its enforcement of a traffic flow policy.
FFW_ACL_EXT.1	**Real-Time Communications 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.
		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports part (b) of this control through its enforcement of a traffic flow policy. Part (c) is enforced through other SFRs, and parts (d) and (e) are not enforced because these relate to organizational policies.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				Parts (f) and (g) are enforced for the prevention of unauthorized 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 supports this control by denying packet flow if a matching rule is not identified.
		SC-7(11)	**Boundary Protection:** Restrict Incoming Communications Traffic	A conformant TOE determines that the source and destination address pairs represent authorized and allowed communications.
FFW_ACL_EXT.2	**Stateful VVoIP Traffic Filtering**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by enforcing when an information flow is allowed or disallowed based on stateful elements of the supported protocols.
		AU-2	**Event Logging**	A conformant TOE supports this control by generating an audit record for violation of the traffic filtering rules.
		SC-7	**Boundary Protection**	A conformant TOE supports this control through enforcement of stateful traffic filtering rules.
		SC-7(4)	**Boundary Protection:** External Telecommunications Services	A conformant TOE supports part (b) of this control through its enforcement of a traffic flow policy. Part (c) is enforced through other SFRs, and parts (d) and (e) are not enforced because these relate to organizational policies. Parts (f) and (g) are enforced for the prevention of unauthorized exchange of control plane traffic with external and internal

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				networks. Part (h) is enforced to filter unauthorized control plane traffic from external networks.
		SC-7(17)	**Boundary Protection:** Automated Enforcement of Protocol Formats	A conformant TOE supports the enforcement of this control by ensuring that supported VVoIP protocols are properly formatted.
FFW_DPI_EXT.1	**Deep Packet Inspection**	SC-7(17)	**Boundary Protection:** Automated Enforcement of Protocol Formats	A conformant TOE supports the enforcement of this control by performing deep packet inspection to verify adherence to protocol formats and specifications.
FFW_NAT_EXT.1	**Topology Hiding/NAT Traversal**	SC-7(16)	**Boundary Protection:** Prevent Discovery of System Components	A conformant TOE will satisfy this control using NAT to obscure the addresses of devices residing in a protected network.
FIA_SIPT_EXT.1	**Session Initiation Protocol Trunking**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by using authentication to validate SIP trunking between the TOE and a peer device.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by ensuring the confidentiality of SIP trunk communications.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by enforcing the use of TLS to secure SIP trunk communications.
FMT_SMF.1/SBC	**Specification of Management Functions (SBC)**	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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FRU_PRS_EXT.1	**Limited Priority of Service**	SC-6	**Resource Availability**	A conformant TOE supports the enforcement of this control by assigning priority of service to network traffic.
FRU_RSA.1	**Maximum Quotas**	SC-5	**Denial-of-Service Protection**	A conformant TOE supports the enforcement of this control by ensuring that TOE resources cannot be deliberately exhausted by a subject.
		SC-6	**Resource Availability**	A conformant TOE supports the enforcement of this control through the enforcement of maximum quotas on system resources.
FTP_ITC.1/ARP	**Inter-TSF Trusted Channel (Automatic Response)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can ensure the confidentiality and integrity of security audit automatic response communications.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting security audit automatic response communications.
FTP_ITC.1/ESC	**Inter-TSF Trusted Channel (ESC Communications)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can ensure the confidentiality and integrity of signaling communications between itself and an Enterprise Session Controller (ESC).
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting signaling communications.
FTP_ITC.1/VVoIP		SC-8	**Transmission Confidentiality**	A conformant TOE can ensure the confidentiality

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
	Inter-TSF Trusted Channel (VVoIP Communications)		**and Integrity**	and integrity of VVoIP signaling and media communications between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting VVoIP signaling and media communications.
Optional Requirements (presented alphabetically)				
This PP-Module has no optional requirements.				
Objective Requirements (presented alphabetically)				
This PP-Module has no objective requirements.				
Implementation-Based Requirements (presented alphabetically)				
FIA_SIPS_EXT.1	**Session Initiation Protocol Registration**	CM-7(3)	**Least Functionality:** Registration Compliance	A conformant TOE supports this control by providing a SIP registration process.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE can enforce some minimum password complexity requirements, which supports part (h) of this control.
Selection-Based Requirements (presented alphabetically)				
FTP_ITC.1/H323	**Inter-TSF Trusted Channel (H.323 Communications)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can ensure the confidentiality and integrity of H.323 communications between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting H.323 communications.