Mapping Between
Network Device Collaborative Protection Profile (NDcPP) Extended Package Session Border Controller, Version 1.1, 2016-09-28
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.
- **SC-7.** The primary purpose of a Session Border Controller (SBC) product is to act as a network boundary protection device between Voice/Video over IP (VVoIP) devices and communications 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 communications networks (e.g. VVoIP and legacy telephone networks), but this is beyond the scope of 800-53 controls.
- **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, 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 that 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.

- **Extended Package.** A TOE that conforms to this Extended Package (EP) will also conform to the collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls through its conformance to that PP. This EP refines some of the NDcPP requirements to ensure consistency between the PP and the EP. Generally, applicable security controls do not change as a result of the modification but they have been included under “NDcPP Security Functional Requirements” below for reference. The only exception to this is that a network device product may or may not support IA-3(1) because support for mutually-authenticated communications is optional in the NDcPP, but a TOE that conforms to this EP is required to implement mutually-authenticated TLS, so this control will always be addressed by a conformant TOE.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
NDcPP Security Functional 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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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).
FCS_COP.1(1)	**Cryptographic Operation (AES Data Encryption/Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_TLSC_EXT.2	**TLS Client Protocol with Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted 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 data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLSS_EXT.2	**TLS Server Protocol with Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted 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 data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FMT_SMF.1	**Specification of Management Functions**	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.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE can generate or use time stamps to address the actions defined in this control.
		SC-45(1)	**System Time Synchronization:** Synchronization with Authoritative Time Source	A conformant TOE may have the ability to synchronize with an NTP server in its operational environment, satisfying this control.
FTP_ITC.1	**Inter-TSF Trusted Channel**	IA-3(1)	**Device Identification and Authentication:**	A conformant TOE supports the enforcement of this control through its

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Cryptographic Bidirectional Authentication	implementation of mutually-authenticated protocol(s) used to establish trusted communications.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted 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 data in transit.
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.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE uses a trusted channel (SNMPv3) to transmit alarms.
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.
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	**Information Flow Control Policy**	AC-4	**Information Flow Enforcement**	A conformant TOE enforces information flow enforcement by determining when a connection between

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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	**Information Flow Control Functions**	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. Parts (f), (g) are enforced for the prevention of unauthorized of exchange of control plane traffic with external and internal networks. Part (h)

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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/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), (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(17)	**Boundary Protection:** Automated	A conformant TOE supports the enforcement of this control by ensuring that

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Enforcement of Protocol Formats	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 through the use of NAT to obfuscate the addresses of devices residing in a protected network.
FIA_SIPT_EXT.1	**Session Initiation Protocol (SIP) 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.
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(2)	**Inter-TSF Trusted Channel**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of VVoIP signaling and

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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.
FTP_ITC.1(3)	**Inter-TSF Trusted Channel**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to 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.
Optional Requirements				
FIA_SIPS_EXT.1	**Session Initiation Protocol (SIP) 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 will have the ability to enforce some minimum password complexity requirements, which supports part (h) of this control.
Selection-Based Requirements				
FCS_DTLS_EXT.1	**Datagram Transport Layer Security**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic	The TOE supports a cryptographic method of protecting data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Protection	
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FTP_ITC.1(4)	**Inter-TSF Trusted Channel**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to 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.
Objective Requirements				
This EP has no objective requirements.				