Mapping Between

PP-Module for SSL/TLS Inspection Proxy, Version 1.0, 2019-08-23

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.
- **SI-4.** The primary purpose of a STIP product is to decrypt and re-encrypt TLS communications so that user activity can be subject to monitoring. A STIP product therefore supports the enforcement of SI-4 in general at a high level, and SI-4(4) and SI-4(10) in particular. 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 SI-4 and relevant sub-controls are the behaviors that STIP is intended to address.
- **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, the TOE's ability to implement trusted communications on its TLS proxy interfaces supports SC-8 and related controls for those interfaces only; it cannot enforce protection of data in transit for non-TLS protocols that are outside of its own boundary.
- **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.x SFR	NIST SP 800-53 Revision 5 Control Supports	Comments and Observations
TOE Security Functional Requirements		

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FAU_GCR_EXT.1.1	**Generation of Certificate Repository**	N/A	**N/A**	This SFR requires the TOE to have or make use of an environmental certificate repository. The use of a certificate repository does not satisfy any security controls on its own; other security requirements in the PP-Module are intended to satisfy security controls that relate to certificate storage.
FAU_STG.4	**Prevention of Audit Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE satisfies part b of this control by taking some action in response to unavailability of audit storage. Because the PP-Module does not require an alert mechanism; part a of the control is not necessarily addressed through the claims made to conform to this PP-Module, unless the ST makes a relevant claim in the assignment.
		AU-5(4)	**Response to Audit Logging Process Failures:** Shutdown on Failure	A conformant TOE supports this control by entering a degraded operational mode in the event that the audit trail cannot be written to.
FCS_COP.1/STIP	**Cryptographic Operation (Data Encryption/Decryption in Support of STIP)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_STG_EXT.1	**Cryptographic Key Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	Because stored key data necessarily includes private key data that can be used by the TOE to authenticate itself, a conformant TOE protects authentication

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data.
FCS_TTTC_EXT.1	**Thru-Traffic TLS Inspection Client Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, 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.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	The purpose of the thru-traffic TLS interface is to decrypt and re-encrypt user TLS traffic so that it can be visible to the organization for inspection.
FCS_TTTC_EXT.5	**Thru-Traffic TLS Inspection Client Support for Supported Groups Extension**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				additional permutations of TLS through the behavior enforced by this SFR.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	The purpose of the thru-traffic TLS interface is to decrypt and re-encrypt user TLS traffic so that it can be visible to the organization for inspection. A conformant TOE supports this by implementing a TLS interface that is capable of supporting a broad set of connection parameters.
FCS_TTTS_EXT.1	**Thru-Traffic TLS Inspection Server Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE presents a certificate to a peer before establishing trusted communications, 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.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	The purpose of the thru-traffic TLS interface is to decrypt and re-encrypt user TLS traffic so that it can be visible to the organization for inspection.
FDP_CER_EXT.1	**Certificate Profiles for Server Certificates**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the enforcement of this control by ensuring the generation of proxy TLS

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				certificates are conformant with organizational policy.
FDP_CER_EXT.2	**Certificate Request Matching of Server Certificates**	N/A	**N/A**	This requirement applies to maintaining a linkage between the certificates the TSF validates and the proxy certificates that it issues in place of these certificates. It does not directly relate to a security control; instead, it is used to maintain availability of certificates.
FDP_CER_EXT.3	**Certificate Issuance Rules for Server Certificates**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the enforcement of this control by ensuring the issuance of proxy TLS certificates are conformant with organizational policy.
FDP_CSIR_EXT.1	**Certificate Status Information Required**	N/A	**N/A**	This requirement defines whether a conformant TOE implements a certificate revocation mechanism or whether it simply issues certificates with short validity periods to prevent re-use. Any relevant security controls are supported by the other SFRs that are included in the TOE boundary based on claims made here.
FDP_PPP_EXT.1	**Plaintext Processing Policy**	SI-4	**System Monitoring**	A conformant TOE supports SI-4 at a general level by performing some action on decrypted TLS traffic, e.g. by terminating a connection that is found to be in violation of an acceptable usage policy by an external processing component.
		SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE supports this control by implementing a plaintext processing policy that determines how decrypted TLS traffic is handled.
FDP_PRC_EXT.1	**Plaintext Routing Control**	SI-4	**System Monitoring**	A conformant TOE supports SI-4 at a general level by

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				determining how decrypted TLS traffic is processed for monitoring, (e.g. by passing it to a different component outside the TOE boundary that analyzes it for potential malicious or unauthorized activity).
		SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE supports this control by implementing a plaintext processing policy that determines how decrypted TLS traffic is handled.
FDP_RIP.1	**Subset Residual Information Protection**	SC-4	**Information in Shared System Resources**	A conformant TOE supports this control ensuring that reuse of system memory does not result in unauthorized disclosure of information.
FDP_STG_EXT.1	**Certificate Data Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the certificate storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	A conformant TOE supports this control by protecting authentication data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored credential data, which includes cryptographic data.
FDP_STIP_EXT.1	**SSL/TLS Inspection Proxy Functions**	AC-8	**System Use Notification**	A conformant TOE supports this control by ensuring that users consent to their TLS activity being monitored.
		SI-4	**System Monitoring**	A conformant TOE supports SI-4 at a high level by allowing for system monitoring of user activities that would otherwise be hidden inside a TLS session.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE supports this control by implementing a function that allows network traffic to be inspected.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	A conformant TOE supports this control by implementing a function that allows for TLS traffic to be decrypted and subsequently re-encrypted so that the decrypted traffic can be inspected.
FDP_TEP_EXT.1	**SSL/TLS Inspection Proxy Policy**	SI-4(4)	**System Monitoring:** Inbound and Outbound Communications Traffic	A conformant TOE supports this control by implementing a policy that determines whether a given connection is approved without inspection, subjected to inspection, or blocked outright.
FIA_ENR_EXT.1	**Certificate Enrollment**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance, specifically the process by which the TOE obtains TLS certificates for its own use.
FIA_X509_EXT.1/STIP	**Certificate Validation (STIP)**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status, which satisfies this control.
		SC-23	**Session Authenticity**	A conformant TOE uses X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE includes the functionality needed to validate certificate authorities.
FMT_MOF.1	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit execution of management functions 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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to interact with the TOE's management functions.
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing in a known state such that it does not process external network traffic until it has been restored to an operational state.
FPT_KST_EXT.1	**No Plaintext Key Export**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key storage portion of this control by ensuring no mechanism exists to export key data in plaintext.
FPT_KST_EXT.2	**TSF Key Protection**	AC-3	**Access Enforcement**	A conformant TOE ensures protection of its key data in support of enforcing access control in general.
FPT_RCV.1	**Manual Trusted Recovery**	CP-10	**System Recovery and Reconstitution**	A conformant TOE supports this control by implementing a maintenance mode that is entered into following a failure and can be used as a starting point to restore the TOE to normal operation.
Optional Requirements				
Persistent Local Audit Storage				
FAU_SAR.1	**Audit Review**	AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE supports this control by implementing a mechanism to review audit data.
FAU_SAR.3	**Selectable Audit Review**	AU-7(1)	**Audit Record Reduction and Report Generation:** Automatic Processing	A conformant TOE supports this control by implementing a search function for stored audit data.
Certificate Pinning				
FDP_PIN_EXT.1	**Certificate Pinning**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to implement certificate pinning to determine the accepted trust anchor for a given server, which supports part b) 1) of this control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-23	**Session Authenticity**	A conformant TOE supports session authenticity by using certificate pinning to associate servers with known trusted certificates.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE supports this control by having the ability to implement certificate pinning to restrict the certificates that are considered to be acceptable for a given server.
Selection-Based Requirements				
Certificate Status Information				
FDP_CRL_EXT.1	**Certificate Revocation List Generation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to maintain certificate status information via CRL, which supports part b) 1) of this control.
		SC-23	**Session Authenticity**	A conformant TOE supports session authenticity by implementing a revocation checking mechanism that allows a client to see whether a certificate the TOE has issued is valid.
FDP_CSI_EXT.1	**Certificate Status Information**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	This SFR specifies the method by which the TOE supports revocation status (CRL or OCSP) and the security controls that relate to those are supported by the relevant SFRs for each revocation method. Separately, this SFR also identifies the management roles that are authorized to modify the revocation behavior, which supports AC-3(7).
FDP_OCSP_EXT.1	**OCSP Basic Response Generation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to maintain certificate status information via OCSP, which supports part b) 1) of this control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-23	**Session Authenticity**	A conformant TOE supports session authenticity by implementing a revocation checking mechanism that allows a client to see whether a certificate the TOE has issued is valid.
FDP_OCSPS_EXT.1	**OCSP Stapling**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to maintain certificate status information via OCSP stapling, which supports part b) 1) of this control.
		SC-23	**Session Authenticity**	A conformant TOE supports session authenticity by implementing a revocation checking mechanism that allows a client to see whether a certificate the TOE has issued is valid.
Certificate Enrollment				
FIA_ESTC_EXT.1	**Enrollment over Secure Transport (EST) Client**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.
Inspection Policy Banner				
FTA_TAB.1/TLS	**TOE Access Banner (Consent to Monitor Banners for TLS Inspection)**	AC-8	**System Use Notification**	A conformant TOE displays an advisory warning to the user prior to authentication.
Authentication of Monitored Clients				
FCS_TTTC_EXT.3	**Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE presents a client certificate before establishing trusted communications for servers that require such behavior, 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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	The purpose of the thru-traffic TLS interface is to decrypt and re-encrypt user TLS traffic so that it can be visible to the organization for inspection.
FCS_TTTS_EXT.3	**Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires the monitored client to present a valid client certificate before communications can be established, 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.
		SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	The purpose of the thru-traffic TLS interface is to decrypt and re-encrypt user TLS traffic so that it can be visible to the organization for inspection.
FDP_CER_EXT.4	**Certificate Profiles for Client Certificates**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the enforcement of this control by ensuring the generation of proxy TLS

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				certificates are conformant with organizational policy.
FDP_CER_EXT.5	**Certificate Issuance Rules for Client Certificates**	SC-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the enforcement of this control by ensuring the issuance of proxy TLS certificates are conformant with organizational policy.
FDP_CSI_EXT.2	**Certificate Status Information for Client Certificates**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	This SFR specifies the method by which the TOE supports revocation status (CRL or OCSP) and the security controls that relate to those are supported by the relevant SFRs for each revocation method. Separately, this SFR also identifies the management roles that are authorized to modify the revocation behavior, which supports AC-3(7).
FDP_STIP_EXT.2	**Mutual Authentication Inspection Operation**	SI-4(10)	**System Monitoring:** Visibility of Encrypted Communications	A conformant TOE supports this control by implementing a function that allows for TLS traffic to be decrypted and subsequently re-encrypted so that the decrypted traffic can be inspected.
Other Selection-Based SFRs				
FAU_SCR_EXT.1	**Certificate Repository Review**	N/A	**N/A**	The purpose of this requirement is for the TOE to have an option to search the certificate database for certificates that match certain values. This does not directly support any security controls; SC-17 relates to X.509 certificates but there is no behavior related to being able to search the certificate store, and controls in the AC family do not apply as the SFR does not enforce any access restrictions on the certificate search function..

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_CKM_EXT.5	**Public Key Integrity**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE implements a mechanism to protect public key data from unauthorized modification.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE supports this control by protecting the integrity of public key data at rest using a cryptographic mechanism.
FCS_TTTC_EXT.4	**STIP Client-Side Support for Renegotiation**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
FCS_TTTS_EXT.4	**STIP Server-Side Support for Renegotiation**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
Objective Requirements				
FIA_ESTC_EXT.2	**EST Client Use of TLS-Unique Value**	SC-17	**Public Key Infrastructure Certificates**	This function supports behavior related to certificate issuance.