Mapping Between

PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18-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.
- **AC-17.** The primary function of this PP-Module is to facilitate the establishment of IPsec VPN connections. A conformant TOE is therefore deployed to support the enforcement of AC-17 at a general level.
- **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				
FCS_CKM.1/IKE	**Cryptographic Key Generation (for IKE Peer Authentication)**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	A conformant TOE supports the enforcement of this control by ensuring that remote access sessions are adequately secured by sufficiently strong IKE keys.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	The specific key generation function provided by the TOE uses asymmetric keys.
FMT_SMF.1/VPN	**Specification of Management Functions (VPN Gateway)**	CM-6	**Configuration Settings**	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.
FPF_RUL_EXT.1	**Rules for Packet 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 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	A conformant TOE denies network communication

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			by Default - Allow by Exception	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.
FPT_FLS.1/SelfTest	**Fail Secure (Self-Test Failures)**	SI-6	**Security and Privacy Function Verification**	A conformant TOE has the ability to shut down in the event of a self-test failure.
FPT_TST_EXT.3	**TSF Self-Test with Defined Methods**	SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of TOE executable code when loaded for execution.
		SI-7(6)	**Software, Firmware and Information Integrity:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
		SI-7(12)	**Software, Firmware and Information Integrity:** Integrity Verification	A conformant TOE has the ability to verify the integrity of the software prior to execution.
FTP_ITC.1/VPN	**Inter-TSF Trusted Channel (VPN Communications)**	IA-3(1)	**Device Identification and Authentication**: Cryptographic Bidirectional Authentication	The use of the cryptographic protocols specified in the SFR implies that the TOE can perform mutual authentication with trusted remote entities.
		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.
Optional Requirements				

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FTA_SSL.3/VPN	**TSF-Initiated Termination (VPN Headend)**	AC-17(9)	**Remote Access:** Disconnect or Disable Access	A conformant TOE will have the ability to terminate a remote VPN client after a period of inactivity.
		SC-10	Network Disconnect	A conformant TOE will have the ability to terminate a remote VPN client after a period of inactivity.
FTA_TSE.1	**TOE Session Establishment**	AC-17(9)	**Remote Access:** Disconnect or Disable Access	A conformant TOE will have the ability to deny establishment of a remote VPN client based upon an administrator day or time.
FTA_VCM_EXT.1	**VPN Client Management**	AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE will enforce logical separation of information flows by assigning a private IP address to a connected VPN client so that it is not routable from its external network.
Selection-Based Requirements				
FIA_PSK_EXT.1	**Pre-Shared Key Composition**	IA-5	**Authenticator Management**	A conformant TOE uses pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (g) of the control.
Objective Requirements				
This PP-Module has no objective requirements.				