Mapping Between
PP-Module for VPN Gateways, Version 1.2, 2022-03-31
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 and 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 specific controls, but typically satisfaction also requires the implementation of operational procedures; furthermore, 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 whether 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; particularly, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **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.
- **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 the NDcPP. This PP-Module refines some of the NDcPP requirements to ensure consistency between the NDcPP 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
TOE Security Functional Requirements				
FAU_GEN.1/VPN	**Audit Data Generation (VPN Gateway)**	AU-2	**Event Logging**	A conformant TOE can generate audit records for various events.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data.
		AU-12	**Audit Record Generation**	The TOE can generate audit logs and control which events are logged, satisfying this control.
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.
		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**	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	**Packet Filtering Rules**	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	A conformant TOE supports the enforcement of parts (a) and (b) of this control by

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Telecommunications Services	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. 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 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 or allowed communications.
FPT_FLS.1/SelfTest	**Failure with Preservation of Secure State (Self-Test Failures)**	SI-6	**Security and Privacy Function Verification**	A conformant TOE can shut down in the event of a self-test failure.
FPT_TST_EXT.3	**Self-Test with Defined Methods**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE can verify the integrity of TOE executable code when loaded for execution.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE can implement cryptographic mechanisms to detect unauthorized change.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		SI-7(12)	**Software, Firmware, and Information Integrity:** Integrity Verification	A conformant TOE can 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 can 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				
FPF_MFA_EXT.1	**Multifactor Authentication Filtering**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports this control to the extent that the actions it requires authentication for are in alignment with the security plan for the system.
		IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE supports this control by requiring multi-factor authentication to authorize a connection attempt.
Objective Requirements				
This PP-Module has no objective requirements.				
Implementation-Based Requirements				
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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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 on 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				
FCS_EAP_EXT.1	**EAP-TLS**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can 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's use of EAP-TLS supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE supports this control if the control's assignment defines the cryptography implemented by the TSF as appropriate for the information system.
FIA_HOTP_EXT.1	**HMAC-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses hash-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.1	**Pre-Shared Key Composition**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the context in which the TOE

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				uses pre-shared keys and the types of pre-shared keys it uses.
FIA_PSK_EXT.2	**Generated Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses generated pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.3	**Password-Based Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses password-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.4	**HMAC-Based One-Time Password Pre-Shared Keys Support**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the TOE's support for HMAC-based pre-shared keys and whether the TSF verifies these keys itself or interfaces with an external authentication server to do so.
FIA_PSK_EXT.5	**Time-Based One-Time Password Pre-Shared Keys Support**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the TOE's support for time-based pre-shared keys and whether the TSF verifies these keys itself or interfaces with an external authentication server to do so.
FIA_TOTP_EXT.1	**Time-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses time-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				supports parts (c) and (h) of this control. Note also that time-based pre-shared keys implicitly support part (f) of this control since they are only valid for a given period.