Mapping Between

Extended Package for VPN Gateway, Version 2.1, 08-March-2017

and

NIST SP 800-53 Revision 4

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 4, 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.
- **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 handle administrator authentication failures only supports AC-7 to the extent that the TSF behavior in response to excessive failures as defined by FIA_AFL.1.2 is consistent with the organization-defined behavior specified in AC-7 point b. 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 4 Control Supports**		**Comments and Observations**
FCS_CKM.1/IKE	**<u>Cryptographic Key Generation</u>**: For IKE Peer Authentication	AC-17(2)	**Remote Access:** Protection of Confidentiality / Integrity Using Encryption	A conformant TOE will generate keys that are used for encryption of remote access communications.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function.
		SC-12(3)	**Cryptographic Key Establishment**	The specific key generation function

			and Management: Asymmetric Keys	provided by the TOE uses asymmetric keys.
FIA_AFL.1	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occur and take some corrective action.
FIA_X509_EXT.4	**X.509 Certificate Identity**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE has the ability to reject the establishment of an SA if the DN information is invalid, which supports part (c) of this control.
FPF_RUL_EXT.1	**Rules for Packet Filtering**	AC-4	**Information Flow Enforcement**	A conformant TOE enforces access control rules that allow or deny information flows based on characteristics of the network traffic, which may support organization-defined information flow control policies related to remote access.
		SC-7	**Boundary Protection**	A conformant TOE supports the enforcement of boundary protection by providing a mechanism to only authorize network traffic that meets certain characteristics.
		SC-7(5)	**Boundary Protection:** Deny by Default / Allow by Exception	A conformant TOE will drop all received traffic over the boundary-facing network interface unless a rule explicitly authorizes the traffic.
		SI-4	**Information System Monitoring**	A conformant TOE will support section a.2 of this control by providing the ability to monitor potentially

				unauthorized network connections.
FPT_FLS.1/SelfTest	**Fail Secure:** Self-Test Failures	SI-6	**Security Function Verification**	A conformant TOE will have the ability to shut itself down in response to a self-test failure. Note, however, that the SFR does not require the TOE to issue a notification in the event of a self-test failure and so the entirety of this control is not necessarily supported.
FPT_TST_EXT.2	**TSF Testing**	SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE will do an integrity test upon start-up.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE will use cryptographic methods to verify the integrity of its own stored executable code.
Optional Requirements				
FTA_SSL.3/VPN	**TSF-Initiated Termination**	AC-2(5)	**Account Management:** Inactivity Logout	A conformant TOE will have the ability to log out after a period of inactivity that can be configured.
FTA_TSE.1	**TOE Session Establishment**	AC-2(11)	**Account Management:** Usage Conditions	A conformant TOE will have the ability to deny remote VPN client session based on location, time, day, or other attributes configured by an administrator.
FTA_VCM_EXT.1	**VPN Client Management**	N/A	N/A	There are no security controls that apply to the ability of the TOE to assign a private IP address to connected clients.
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 h of the control.
Objective Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**