CSfC Selections for VPN Gateways

VPN Gateway product-lines used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Network Device collaborative Protection Profile (NDcPP) or Stateful Traffic Filtering Firewall collaborative Protection Profile (FWcPP) and NDcPP/FWcPP Extended Package VPN Gateway (NDcPP/FWcPP EP VPN GW). This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for NDcPP/FWcPP evaluations:

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys in accordance with at least one of the following specified cryptographic key generation algorithms: [selection:

- RSA schemes using cryptographic key sizes of **3072-bit or greater** that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [selection: **P-384**] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;

FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with at least one of the following specified cryptographic key establishment methods:

- RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services (generation and verification) in accordance with at least one of the following specified cryptographic algorithms [selection:

- RSA Digital Signature Algorithm and cryptographic key size (modulus) [assignment: **3072 bits or greater**],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: **256 bits**]

that meet the following: [selection:

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS):, Section 6 and Appendis D, Implementing "NIST curves" P-256, **P-384**, and [selection: P-521, no other curves]; ISO/IEC 14888-3, Section 6.4].

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [selection: **SHA-384**] that meet the following: ISO/IEC 10118-3:2004.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of hardware-based sources] hardware-based noise source] with a minimum of [selection: **256 bits**] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FTP_TRP.1.1 The TSF shall be capable of using [selection: **IPsec**] to provide a communication path between itself and authorized remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of communicated data from disclosure and provides detection of modification of the channel data.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on [selection:
    - number of bytes;
    - **length of time,** where the time values can be configured within [assignment: integer range including 24] hours;];
- IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection:
    - Number of bytes;
    - **Length of time,** where the time values can be configured within [assignment: integer range including 24] hours;]]

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [selection:
    - number of bytes;
    - **length of time,** where the time values can be configured within [assignment: integer range including 8] hours;];
- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [selection:
    - number of bytes;
    - **length of time,** where the time values can be configured within [assignment: integer range including 8] hours;]]

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: **(256/384 bits)** that is at least twice the security strength of the negotiated Diffie-Hellman group] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: IKEv1, IKEv2] exchanges of length [selection:

- [assignment: **security strength associated with the negotiated Diffie-Hellman group**];

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: **20 (384-bit Random ECP) or [DH Group 15 (3072-bit MODP)]**

CSfC selections for NDcPP/FWcPP EP VPN GW evaluations:

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: **tunnel mode**].