CSfC Selections for VPN Clients

VPN Client products used in CSfC solutions shall be validated by NIAP/CCVES or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile (PP) Module for VPN Client and one of the Base Protection Profiles as specified therein (i.e. General Purpose Operating System, Mobile Device Fundamentals, or Application Software). This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for VPN Client PP Module evaluations:

FCS_IPSEC_EXT.1.2 The [selection: TOE, TOE platform] shall implement [selection: **tunnel mode**, transport mode].

FCS_IPSEC_EXT.1.5 The [selection: TOE, TOE platform] shall implement the protocol: [selection:

- IKEv1, using Main Mode for Phase I exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], [selection: no other RFCs for hash functions, RFC 4868 for hash functions], and [selection: support for XAUTH, no support for XAUTH];
- **IKEv2 as defined in RFCs 7296 (with mandatory support for NAT traversal as specified in section 2.23), 4307**, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.7 The [selection: TOE, TOE platform] shall ensure that [selection: IKEv2 SA lifetimes can be configured by [selection: an Administrator, VPN Gateway] based on [selection: number of packets/number of bytes, **length of time**], IKEv1 SA lifetimes can be configured by an [selection: an Administrator, VPN Gateway] based on [selection: number of packets/number of bytes, length of time], IKEv1 SA lifetimes are fixed based on [selection: number of packets/number of bytes, length of time]]. If length of time is used, it must include at least one option that is 24 hours or less for Phase 1 SAs and 8 hours of less for Phase 2 SAs.

FCS_IPSEC_EXT.1.9 The [TOE, TOE platform] shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: (**256, 384**) number(s) of bits that is at least twice the "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management – Part 1: General] bits

FCS_IPSEC_EXT.1.10 The [selection: TOE, TOE platform] shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[assignment: (**128, 192**) "bits of security" value(s) associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management – Part 1: General].

Last Updated: November 29, 2017