Network Device Interpretation # 202404

FCS_IPSEC_EXT.1.10 Test update

Status: □ *Active* ☒ *Inactive*

Date: 9-Sep-2024

End of proposed Transition Period (to be updated after TR2TD process): 9-Oct-2024

Type of Change: □ Immediate application ☒ Minor change □ Major change

Type of Document: □ *Technical Decision* ☒ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* □ *Network iTC*

Affected Document(s): ND cPP v3.0e; ND SD v3.0

Affected Section(s): FCS_IPSEC_EXT.1.10

Superseded Interpretation(s): *None*

Issue:

Issue: IPSEC_EXT.1.10 Testing in NDcPP (NIAP#1614)

In CPP_ND_V2.2E and CPP_ND_V3.0E the tests for FCS_IPSEC_EXT.1.10 are just a copy of the TSS activities, there are no actual tests for this SFR.

Resolution:

To add add tests for FCS_IPSEC_EXT.1.10 and clarify its intent, the following changes will be made.

Changes to the cPP:

<old>

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

- according to the security strength associated with the negotiated Diffie-Hellman group;
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

  ].

Application Note 84

The ST author must select the second option for nonce lengths if IKEv2 is also selected (as this is mandated in RFC 5996). The ST author may select either option for IKEv1.

For the first option for nonce lengths, since the implementation may allow different Diffie Hellman groups to be negotiated for use in forming the SAs, the assignment in FCS_IPSEC_EXT.1.10 may contain multiple values. For each DH group supported, the ST author consults Table 2 in NIST SP 800-57 "Recommendation for Key Management –Part 1: General" to determine the security strength ("bits of security") associated with the DH group. Each unique value is then used to fill in the assignment for this element. For example, suppose the implementation supports DH group 14 (2048-bit MODP) and group 20 (ECDH using NISTcurve P-384). From Table 2, the bits of security value for group 14 is 112, and for group 20 it is 192.

Because nonces may be exchanged before the DH group is negotiated, the nonce used should be large enough to support all TOE-chosen proposals in the exchange.

</old>

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

- according to the security strength associated with the negotiated Diffie-Hellman group;
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

  ].

Application Note 84

This SFR is for the IKEv1 (phase 1 and phase 2) and IKEv2 (IKE_AUTH and CREATE_CHILD_SA) protocol exchanges.

The ST author must select the second option for nonce lengths if IKEv2 is selected (as this is mandated in RFC 7296). The ST author may select either option for IKEv1.

The security strengths of DH groups are defined in NIST SP 800-57.

Because nonces may be exchanged before the DH group is negotiated, the nonce used should be large enough to support all TOE-chosen proposals in the exchange.

</new>

<old>

FCS_IPSEC_EXT.1.10

445. Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

a. Test 1: If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.

b. Test 2: If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.

</old>

<new>

FCS_IPSEC_EXT.1.10

446. The following tests shall be performed.

a. Test 1: If IKEv1 is supported, Configure the TOE to use IKEv1:

   - Test 1.a: If "according to the security strength associated with the negotiated Diffie-Hellman group" has been selected, for each supported authentication methods and DH groups, demonstrate the TOE uses phase 1 and phase 2 nonces meeting the strength requirement defined in NIST SP 800-57 for the appropriate DH group.

   - Test 1.b: If "at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash" has been selected, for each supported authentication method and PRF hash, demonstrate the TOE uses phase 1 and phase 2 nonces suitable for the selected PRF.

b. Test 2: If IKEv2 is supported, configure the TOE to use IKEv2:

   - For each supported DH group, demonstrate the TOE uses IKE_SA_INIT and CREATE_CHILD_SA nonces suitable for the selected PRF.

</new>

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

Incorporate into next version of the cPP