Network Device Interpretation # 201707

Make CBC cipher suites optional in IPsec

Status: ☒ *Active* □ *Inactive*

Date: *10-May-2017*

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

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

Affected Document(s): *NDcPP V1.0, FWcPP V1.0, NDSD V1.0*

Affected Section(s): *FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6*

Superseded Interpretation(s): *None*

Issue:

The current NDcPP v1.0 mandates CBC (i.e. FCS_IPSEC_EXT.1.4 & FCS_IPSEC_EXT.1.6). However, the draft version 2 posted on the CC Portal has CBC and GCM as selectable and we expect it to remain this way for version 2.0 of NDcPP. We interpret this to mean that the iTC is allowing GCM for IKE & ESP going forward. Is this acceptable for evaluations against v1.0 as well?

Resolution:

The NIT acknowledges that there are some security related concerns regarding AES-CBC mode and therefore supports making AES-128-CBC and AES-256-CBC optional for IKE and ESP. FCS_IPSEC_EXT.1.4 shall therefore be modified as follows:

"**FCS_IPSEC_EXT.1.4** The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: *AES-CBC-128 (specified by RFC 3602), AES-CBC-256 (specified by RFC 3602), AES-GCM-128 (specified in RFC 4106), AES-GCM-256 (specified in RFC 4106)*] together with a Secure Hash Algorithm (SHA)-based HMAC."

FCS_IPSEC_EXT.1.6 shall be modified as follows:

"**FCS_IPSEC_EXT.1.6** The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms [selection: *AES-CBC-128 (as specified in RFC 3602), AES-CBC-256 (as specified in RFC 3602), AES-GCM-128 (as specified in RFC 5282), AES-GCM-256 (as specified in RFC 5282)*].

The TSS requirements for FCS_IPSEC_EXT.1.4 in NDSD V1.0 shall be modified as follows:

"The evaluator shall examine the TSS to verify the TSS describes all cryptographic algorithms selected in FCS_IPSEC_EXT.1.4. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(4) Cryptographic Operations (for keyed-hash message authentication)."

The TSS requirements for FCS_IPSEC_EXT.1.6 in NDSD V1.0 shall be modified as follows:

"The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that all cryptographic algorithms selected in FCS_IPSEC_EXT.1.6 are included in the TSS discussion."

The Guidance Documentation requirements for FCS_IPSEC_EXT.1.4 in NDSD V1.0 shall be modified as follows:

"The evaluator checks the guidance documentation to ensure it provides instructions on how to configure the TOE to use all the algorithms selected in FCS_IPSEC_EXT.1.4."

The Guidance Documentation requirements for FCS_IPSEC_EXT.1.6 in NDSD V1.0 shall be modified as follows:

*"*The evaluator ensures that the guidance documentation describes the configuration of all algorithms selected in FCS_IPSEC_EXT.1.6. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.*"*

The corresponding sections in the extended component definition of NDcPP V1.0 and FWcPP V1.0 need to be updated accordingly.

Rationale:

As stated in the 'Issue' section.

Further Action:

None

Action by Network iTC:

None