Network Device Interpretation # 201614

Transport mode and tunnel mode in IPsec communication

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Feb-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*

Affected Section(s): *FCS_IPSEC_EXT.1.3*

Superseded Interpretation(s): *None.*

Issue:

NDcPP V1.0 FCS_IPSEC_EXT.1.3 requires the TOE support transport mode, with tunnel mode optional.

RFC 4301 states in section 4.1 (see summary on page 16 here

https://tools.ietf.org/html/rfc4301):

- Gateways must support tunnel mode, transport mode optional.

- Host must support both transport and tunnel modes.

Therefore, the only way to be compliant with the RFC is to include the "optional" tunnel mode in the SFR. Can the group confirm that this is the intent?

Resolution:

NIT recommends to modify FCS_IPSEC_EXT.1.3 to make both, tunnel mode and transport mode selectable by introducing a corresponding selection to the SFR. The ND Supporting Document needs to be updated accordingly including the TSS section (see proposal for Application Note below).

NIT recommends to add the following Application Note:

The selection of supported modes shall be performed according to RFC 4301. The TSS shall provide details about the supported modes.

Rationale:

The recommendation is in agreement with RFC 4301, chap. 4.1.

Further Action:

- Approval by Network iTC required

- If approved, change FCS_IPSEC_EXT.1.3 and the corresponding sections in the ND Supporting Document accordingly. Add the proposed Application Note to FCS_IPSEC_EXT.1.3.

Action by Network iTC: