Network Device Interpretation # 201667

'Expected' vs. 'unexpected' DNs in certificate verification for IPsec communications

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Mar-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.1.14*

Superseded Interpretation(s): *None*

Issue:

NDcPP SFR FCS_IPSEC_EXT.1.14 states:

The TSF shall only establish a trusted channel to peers with valid certificates.

The assurance activity for this SFR reads:

The evaluator shall, if necessary, configure the expected DN according to the guidance documentation. The evaluator shall send a peer certificate signed by a trusted CA with a DN that does not match an expected DN and verify that the TOE denies the connection.

From this, it appears that there must be a mechanism within the TOE to distinguish between an "expected" DN and all others, and to reject connections from clients presenting certificates with unexpected DN's. This seems to imply that the TOE must have some form of whitelist access control, which is not explicitly required in the SFR. Can you clarify the intent of the test AA?

[Remark: This issue is related to NIAP's Technical Decision #0037 IPsec Requirement DN Verification]

Resolution:

The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).

The NIT acknowledges the issue described in the Issue section. FCS_IPSEC_EXT.1.14 shall therefore be modified as follows:

"**FCS_IPSEC_EXT.1.14** The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the

presented and reference identifiers are of the following types: [selection: IP address, Fully Qualified Domain Name (FQDN), user FQDN, Distinguished Name (DN)] and [selection: no other reference identifier type, [*assignment: other supported reference identifier types*]]."

The application note for FCS_IPSEC_EXT.1.14 shall be modified as follows:

"When using RSA or ECDSA certificates for peer authentication, the reference and presented identifiers take the form of either a DN, IP address, FQDN or user FQDN. The reference identifier is the identifier the TOE expects to receive from the peer during IKE authentication. The presented identifier is the identifier that is contained within the peer certificate body. The ST author shall select the presented and reference identifier types supported and may optionally assign additional supported identifier types in the second selection. Excluding the DN identifier type (which is necessarily the Subject DN in the peer certificate), the TOE may support the identifier in either the Common Name or Subject Alternative Name (SAN) or both.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name is required for the purposes of backwards compatibility. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented.

Supported peer certificate algorithms are the same as FCS_IPSEC_EXT.1.13."

Rationale:

As stated in the wording for the application note in the 'Resolution' section.

Further Action:

None

Action by Network iTC:

None