

Network Device Interpretation # 15

SNMPv3 Support

Status: *Active* *Inactive*

Date: 30-Jun-2016

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

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

Affected Document(s): ND cPP V1.0, FW cPP V1.0

Affected Section(s): FTP_TRP.1

Superseded Interpretation(s): None

Issue:

FTP_TRP.1 *Trusted Path*

- *FTP_TRP.1.1 The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a communication path between itself and authorized remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.*
- *FTP_TRP.1.2 The TSF shall permit remote administrators to initiate communication via the trusted path.*
- *FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.*

A number of network appliances implement SNMP v3.0 for the monitoring and administration of the device.

SNMP v3.0 is not included in the Protection Profile as an acceptable protocol for device administration.

Can you please clarify the reasons why SNMP v3.0 is not considered as an approved protocol for the monitoring and administration of a network device?

Resolution:

As of now, TOE administration must always utilize secure channel functionality as defined in FPT_TRP.1. The use of SNMPv3 protocol for administration without encapsulation is disallowed and therefore must be disabled. However, monitoring functionality, for example when SNMPv3 policy is configured for read-only mode, is outside the scope of evaluation and therefore is not explicitly disallowed in the evaluated configuration.

Support for SNMPv3 is on the Network iTC's Parking Lot list for consideration in later versions of ND cPP and FW cPP, though.

Rationale:

None

Further Action:

None

Action by Network iTC:

None