Network Device Interpretation # 1

Forwarding of audit information to external audit servers

Status: ☒ *Active* ☐ *Inactive*

Date: *25-Jan-2016*

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

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

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

Affected Section(s): *FAU_STG_EXT.1*

Superseded Interpretation(s): *None.*

Issue:

NDcPP V1.0 FAU_STG_EXT.1 requires audit forwarding, but doesn't explicitly identify a protocol.

1. *Must an NDcPP compliant device support syslog?*
2. *If the TOE transmits daily compressed log files, will this meet STG_EXT.1?*
3. *If the TOE can only transmit log files to a vendor designed audit server, does that meet STG_EXT.1?*

Resolution:

1. *Syslog is not mandated. No requirements are placed upon the format or underlying protocol of the audit being transferred. The only requirement is that it is transferred over an ITC transport.*
2. *The TOE must be capable of being configured to transfer audit data to an external IT entity without administrator intervention. Manual transfer would not meet the requirements. Transmission could be done in real-time or periodically. In case the transmission would not be done in real-time the TSS has to provide details about the possible as well as acceptable frequency for the transfer of audit data.*
3. *The audit server is not part of the TOE so there are no requirements on it except the capabilities for ITC transport for audit data.*

Rationale:

N/A

Further Action:

- Add clarification to Application Note for FAU_STG_EXT.1.

- Add requirement to TSS section of FAU_STG_EXT.1 in Supporting Document to check for details in case no real-time transfer of audit data to the external audit server.

Action by Network iTC: