Network Device Interpretation # 201658

Auditing of NTP Time Changes

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Dec-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): *FAU_GEN.1; FPT_STM.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

FAU_GEN.1 requires the old and new values of time to be logged whenever there is a time change (FPT_STM.1). A TOE might not have a manual set time function. It may always use NTP to synchronize time with NTP servers. While it records the timestamp when it is finally synced with at least one NTP server, it may not record every time its clock is adjusted.

Proposed solution:

Most NTP clients rely on slewing but not stepping for time adjustment. Logging every NTP time change would require a significant amount of engineering work but does not improve the accuracy of the timestamps.

The requirement of logging old and new time values should either be restricted to manual time changes or the requirements should be adapted to match the use cases when using NTP clients.

Resolution:

All discontinuous time changes, administrator actuated or changed via an automated process, must be audited. No audit is needed when time is changed via use of kernel or system facilities – such as adjtime(3) – that exhibit no discontinuities in time.

Rationale:

Auditing when time is stepped is meant to allow an administrator to identify and explain why there is an apparent overlap or gap in audit stream. An audit is needed whenever time jumps. When time is being slewed, all timestamps in the stream are continuous and monotonically increasing. No audit is needed.

Further Action:

V2.0 verbiage should align and clarification to Application Note 37 made.

Action by Network iTC:

None.