Network Device Interpretation # 202418

NDcPP30e FAU_STG_EXT.1 - Test 6 Unclear Testing Requirements

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Sep-2024*

End of proposed Transition Period (to be updated after TR2TD process): *27-Sep-2024*

Type of Change: ☒ Immediate application ☐ Minor change ☐ Major change

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

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

Affected Document(s): *ND SD v3.0e*

Affected Section(s): *FAU_STG_EXT.1, Test 6*

Superseded Interpretation(s): *None*

Issue:

Issue:

Both the testing activity for this test and the purpose of this test are unclear.

"Test 6 [Conditional]: In case manual export or ability to view locally is selected in FAU_STG_EXT.1.6, during interruption the evaluator shall perform a TSF-mediated action and verify the event is recorded in the audit trail."

What is the "interruption" that the activity describes? Is this the same interruption performed in FTP_ITC testing? This should be clarified. And what exactly needs to be interrupted?

The use of "TSF-mediated action" in this context isn't entirely clear. Is any administrative action that causes an audit to be generated and recorded sufficient?

Additionally, the purpose of this test isn't clear. The CCTL interprets this as verifying that a TOE continues to generate and store audits locally even if the connection to a remote syslog server is lost. But this is just an inference and would be better clarified in an App Note. There currently is no App Note for this element.

Resolution:

The following text shall be appended to ND SD v3.0e, FAU_STG_EXT.1, Tests section, definition for Test 6:

{new}

Note: The intent of the test is to ensure that the local audit TSF (as specified by FAU_STG_EXT.1.3) operates independently from the ability to transmit the generated audit data to an external audit server (as specified in FAU_STG_EXT.1.1). There are no specific requirements on the interruption of the connection between the TOE and the external audit server (as for FTP_ITC.1).

{/new}

Rationale:

see Issue and Resolution sections

This test ought to be understood as

Step 1: Set up a test system with local audit storage supported by the TOE and external audit server supported with a working connection between the TOE and the external audit server.

Step 2: Interrupt the connection between the TOE and the external audit server.

Step 3: While the connection between the TOE and the external audit server is interrupted perform a TSF-mediated action that is supposed to generate an audit event according to FAU_GEN.1.

Step 4: Confirm that the local audit TSF still functions while the connection to the external audit server is interrupted by verifying that the expected audit event that should have been generated in the previous step can be observed.

Further Action:

None

Action by Network iTC:

None