Network Device Interpretation # 202116

IPSec IKE/SA lifetimes tolerance

Status: ☒ *Active* ☐ *Inactive*

Date: *20-Dec-2021*

End of proposed Transition Period (to be updated after TR2TD process): *20-Jan-2022*

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): *NDcPP v2.2e, ND SD2.2*

Affected Section(s): *FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8*

Superseded Interpretation(s): *None*

Issue:

The tests for these requirements configure a TOE rekey limit of 24/8h on IKE/ESP SAs respectively, and ensure that the TOE negotiates a new SA on or before 24/8 hours has elapsed. The ITSEF believes that to test should accommodate some variability in the renegotiation (as historically, renegotiation was costly and preventing dual renegotiation requests from both peers was important). The security implications of an SA existing for slightly longer (say 1% longer) are negligible and worthwhile to allow for efficient renegotiation. Thus, we suggest the test wording be updated to state "... SA is negotiated after 24 hours have elapsed (for renegotiation efficiency, the TOE may renegotiate within a +/- 1% of the overall time period--e.g., renegotiate 24 hours and 14 minutes, or 23 hours and 46 minutes)."

Additionally, if schemes must rely upon the iTC for such an interpretation, the ITSEF requests that TOE allows for such +/- renegotiation variability through Administrative guidance--which could state something like "Our TOE modifies the precise renegotiation time by a variable amount to promote efficiency. An administrator who wishes to configure a maximum limit for renegotiation should reduce the configured time by <X minutes or Y%>. For example, to ensure a 24 hour limit, the administrator should configure a TOE limit of 23 hours and 55 minutes."

Resolution:

The NIT acknowledges that the definition of the currently defined evaluation activities for FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8 can be read more strictly than they are intended to be. Therefore, the following changes shall be applied.

Guidance Documentation requirements for FCS_IPSEC_EXT.1.7 shall be modified as follows:

<old>

The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, the evaluator ensures that the Administrator is able to configure Phase 1 SA values for 24 hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

</old>

<new>

The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is performed no later than 24h). The evaluator shall verify that the guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

</new>

Guidance Documentation requirements for FCS_IPSEC_EXT.1.8 shall be modified as follows:

<old>

The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, the evaluator ensures that the Administrator is able to configure Phase 2 SA values for 8 hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

</old>

<new>

The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the guidance documentation allows the Administrator to configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA

lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

</new>

Test requirements for FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8 shall be modified as follows:

Test 2 for FCS_IPSEC_EXT.1.7 shall be modified as follows:

<old>

If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a lifetime that exceeds the lifetime of the TOE.

</old>

shall be replaced by

<new>

If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 1 SA lifetime that exceeds the Phase 1 SA lifetime on the TOE.

</new>

Test 2 for FCS_IPSEC_EXT.1.8 shall be modified as follows:

<old>

If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a lifetime that exceeds the lifetime of the TOE.

</old>

shall be replaced by

<new>

If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 2 SA lifetime that exceeds the Phase 2 SA lifetime on the TOE.

</new>

Rationale:

see Resolution

Further Action:

None

Action by Network iTC:

None