Network Device Interpretation # 201624

Testing SSH 2^28 packets

Status: ☒ *Active* ☐ *Inactive*

Date: *7-Feb-2017*

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, ND SD V1.0*

Affected Section(s): *Multiple, see 'Resolution section' for details*

Superseded Interpretation(s): *RfI#24, dated 02-August-2016 (Reason: incorporating side effects of RfI#41).*

Issue:

The requirement "FCS_SSHS_EXT.1.8 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key." Has the associated test case:

"The evaluator shall configure the TOE to create a log entry when a rekey occurs. The evaluator shall connect to the TOE with an SSH client and cause 2^28 packets to be transmitted from the client to the TOE, and subsequently review the audit log to ensure that a rekey occurred."

2^28 == 268,435,456 packets sent to the TOE. While this might seem reasonable in theory (or on paper) considering GB Ethernet connections, our actual testing is showing this isn't really a practical test.

Recommendation: We think there is no practical threat scenario and suggest the test case should be dropped from the NDcPP as well as other PPs with SSHS, at least until a reasonable test method can be devised.

Resolution:

NIT recommends replacing the packet based threshold by two thresholds, one related to session time and the other related to traffic. NIT recommends the following changes:

Changes to the cPPs

<u>Rewording of SSH SFRs</u>

FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one

gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

Application Note:
This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold the total incoming and outgoing data needs to be counted. The rekey applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic.
It is acceptable for a TOE to implement lower thresholds than the maximum values defined in the SFR.
For any configurable threshold related to this requirement the guidance documentation needs to specify how the threshold can be configured. The allowed values must either be specified in the guidance documentation and must be lower or equal to the thresholds specified in this SFR or the TOE must not accept values beyond the thresholds specified in this SFR.

Modification of FMT_SMF.1
Add to the selection in FMT_SMF.1:
Ability to configure thresholds for SSH rekeying.

Add to the Application Note for FMT_SMF.1:
The selection 'Ability to configure thresholds for SSH rekeying' shall be included in the ST if the TOE supports configuration of the thresholds for the mechanisms used to fulfil FCS_SSHC_EXT.1.8 or FCS_SSHS_EXT.1.8 (such configuration then requires the inclusion of FMT_MOF.1(1)/AdminAct in the ST). If the TOE places limits on the values accepted for the thresholds then this is stated in the TSS.

Changes to the Supporting Document
Add to chap. 2.2.11.1 and 2.2.12.1
FCS_SSHC_EXT.1.8/FCS_SSHS_EXT.1.8:
The evaluator shall check the TSS to ensure that it describes how the SFR is met. This comprises checking that the TSS clarifies that both thresholds are checked by the TOE and that rekeying is performed upon reaching the threshold whichever is hit first.

Add to chap. 2.2.11.2 and 2.2.12.2
FCS_SSHC_EXT.1.8/FCS_SSHS_EXT.1.8:
If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator

shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.

Modify chap. 2.2.11.3
FCS_SSHC_EXT.1.8:
The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold.
For testing of the time-based threshold the evaluator shall use the TOE to connect to an SSH server and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and a rekey has been performed. This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events. The evaluator uses available methods and tools to demonstrate that rekeying occurs.
Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to.
For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server, and shall transmit data from and to the TOE within the active SSH session until the threshold for transmitted traffic is reached. The transmitted traffic is the total traffic comprising incoming and outgoing traffic.
The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and a rekey has been performed. This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events. The evaluator uses available methods and tools to demonstrate that rekeying occurs.
Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to.
If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1(1)/AdminAct).

Modify chap. 2.2.12.3
FCS_SSHS_EXT.1.8:
The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold.
For testing of the time-based threshold the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and a rekey has been performed.

This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events. The evaluator uses available methods and tools to demonstrate that rekeying occurs.
Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.
For testing of the traffic-based threshold the evaluator shall use an SSH client to connect to the TOE, and shall transmit data from and to the TOE within the active SSH session until the threshold for transmitted traffic is reached. The transmitted traffic is the total traffic comprising incoming and outgoing traffic.
The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and a rekey has been performed. This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events. The evaluator uses available methods and tools to demonstrate that rekeying occurs.
Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.
If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1(1)/AdminAct).

Rationale:

N/A

Further Action:

Modify ND cPP, FW cPP, and ND SD accordingly.

Action by Network iTC: