Network Device Interpretation # 201927

Firewall IPv4 & IPv6 testing by default

Status: ☒ *Active* ☐ *Inactive*

Date: *26-Feb-2020*

End of proposed Transition Period (to be updated after TR2TD process): *26-Mar-2020*

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): *FW SDv2.0e, FW MOD SDv1.3*

Affected Section(s): *FFW_RUL_EXT.1*

Superseded Interpretation(s): *None*

Issue:

Affected Document: Supporting Document Mandatory Technical Document Evaluation Activities for Stateful Traffic Filter Firewalls cPP October-2017 Version 2.0 (Note that this question applies to a number of Firewall evaluations present and future and also applies equally to the forthcoming Firewall Module).

The general question is whether, for firewall evaluations, there is some seemingly undocumented default expectation to test for both IPv4 and IPv6 rather than just testing IPv4 and/or IPv6 where specifically called out in the required test activities.

As an example, FFW_RUL_EXT.1.5 includes a test case:

"Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session." that can be contrasted with a FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 test case:

"Test 1: The evaluator shall use the instructions in the guidance documentation to test that stateful packet filter firewall rules can be created that permit, drop, and log packets for each of the following attributes:

- *ICMPv4*

    - *Type*
    - *Code*
- *ICMPv6*
    - *Type*
    - *Code*
- *IPv4*
    - *Source address*
    - *Destination Address*
    - *Transport Layer Protocol*
- *IPv6*
    - *Source address*
    - *Destination Address*
    - *Transport Layer Protocol and where defined by the ST author,*

Extension Header Type, Extension Header Fields

- *TCP*
    - *Source Port*
    - *Destination Port*
- *UDP*
    - *Source Port*
    - *Destination Port"*

While the FFW_RUL_EXT.1.5 test case seems to suggest only a single test is required and does not specifically mention IPv4 or IPv6 (instead focusing on higher level protocols and states in this case), the FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 test case is explicit about which protocols to test.

The specific question is whether the FFW_RUL_EXT.1.5 test case (and any other similar test case that is unqualified) must be tested with both IPv4 and IPv6 or not (i.e. is the default requirement to test both IPv4 and IPv6 unless otherwise specified or justified)?

Note that broad examination of previously evaluated products (based on published AARs) shows that IPv6 testing variants for FFW_RUL_EXT.1.5 and the like might have been included in only a few rare cases, but not in the majority of cases. As such, the ITSEF thinks it is not clearly expected that tests such as the FW_RUL_EXT.1.5 test case should be repeated for each lower level protocol. Regardless we think

this needs to be answered definitively to make sure it is being (and will be) applied consistently going forward.

Resolution:

In general, both IPv4 and IPv6 must be tested for all FFW_RUL_EXT.1 evaluation activities. In particular where handling of IPv4 and IPv6 is implemented separately in the TOE, both protocols need to be tested to ensure correct TOE behavior. There is no expectation, though, to test pure IPv4 features with IPv6 (or vice versa, if applicable). In particular, the following changes shall be applied:

1.) Between the headlines "FFW_RUL_EXT.1 Stateful Traffic Filtering" and "TSS" the following paragraph shall be added.

<new>

The following table provides an overview about execution of test cases regarding IPv4 and IPv6.

SFR Element/Test Case	**Test execution**
FFW_RUL_EXT.1, Tests 1-2	Both, IPv4 and IPv6.
FFW_RUL_EXT.1.2/1.3/1.4, Tests 1-2	As defined in the test description.
FFW_RUL_EXT.1.5, Tests 1-8	Both, IPv4 and IPv6.
FFW_RUL_EXT.1.6, Tests 1-2	Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element FFW_RUL_EXT.1.6. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly.
FFW_RUL_EXT.1.7, Tests 1-2	Both, IPv4 and IPv6.
FFW_RUL_EXT.1.8, Tests 1-2	Both, IPv4 and IPv6.
FFW_RUL_EXT.1.9, Test 1	As defined in the test description.
FFW_RUL_EXT.1.10, Tests 1	Both, IPv4 and IPv6.

</new>

2.) At the beginning of the Test section for FFW_RUL_EXT.1.5 (before the test definition) the following sentence shall be added:

<old>

"Tests

Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. ..."

</old>

shall be replaced by

<new>

"Tests

The following tests shall be run using IPv4 and IPv6.

Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. ..."

</new>

3.) At the beginning of the Test section for FFW_RUL_EXT.1.6 (before the test definition) the following sentence shall be added:

<old>

"Tests

Test 1: The evaluator shall test each of the conditions for automatic packet rejection in turn. ..."

</old>

shall be replaced by

<new>

"Tests

Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly.

Test 1: The evaluator shall test each of the conditions for automatic packet rejection in turn. ..."

</new>

4.) At the beginning of the Test section for FFW_RUL_EXT.1.7 (before the test definition) the following sentence shall be added:

<old>

"Tests

Test 1: The evaluator shall configure the TOE to drop and log network traffic where the source address of the packet matches that of the TOE network interface upon which the traffic was received. ..."

</old>

shall be replaced by

<new>

"Tests

The following tests shall be run using IPv4 and IPv6.

Test 1: The evaluator shall configure the TOE to drop and log network traffic where the source address of the packet matches that of the TOE network interface upon which the traffic was received. ..."

</new>

5.) At the beginning of the Test section for FFW_RUL_EXT.1.10 (before the test definition) the following sentence shall be added:

<old>

"Tests

Test 1: The evaluator shall define a TCP half-open connection limit on the TOE. The evaluator shall generate TCP SYN requests to pass through the TOE to the target system using a randomised source IP address and common destination IP address. ..."

</old>

shall be replaced by

<new>

"Tests

The following tests shall be run using IPv4 and IPv6.

Test 1: The evaluator shall define a TCP half-open connection limit on the TOE. The evaluator shall generate TCP SYN requests to pass through the TOE to the target system using a randomised source IP address and common destination IP address. ..."

</new>

Rationale:

Provided in the Resolution section.

Further Action:

None

Action by Network iTC:

None