Network Device Interpretation # 202505

FFW_RUL_EXT.1.2 Expected Rule Granularity Level

Status: ☒ *Active* □ *Inactive*

Date: *16-Jun-2025*

End of proposed Transition Period (to be updated after TR2TD process): *TBD*

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): *MOD_CPP_FW_v1.4e, MOD_FW_v1.4e-SD*

Affected Section(s): *FFW_RUL_EXT.1.2,*

Superseded Interpretation(s): *None*

Issue:

In the Stateful Firewall Module, FFW_RUL_EXT.1.2 specifies that the TSF shall allow for the definition of stateful traffic filtering rules that contain a variety of network packet fields. However, there is some ambiguity regarding the granularity of control which the Firewall can have rules written. Specifically, the PP-Module and its SD are unclear about what is expected for the ICMP[v4/v6] Type and Code values and the IPv[4/6] Transport Layer Protocol values which are intended to be configurable by the administrator of the device. Is it expected that only IANA recognized values are expected to be configurable on the TSF or is it expected that the firewall can have any arbitrary ICMP Type and/or Code value specified for a rule? Further, is it expected that only defined Transport Layer Protocol values can be configured or are arbitrary values for the Transport Layer Protocol intended to be configurable?

An example of the scenario that could be affected by this query could be in the case of ICMP. ICMP Type 8 correlates to the Echo Request message, which does not utilize the code value for the ICMP protocol and implies that the code value, while nominally '0' may not always be '0' (RFC 792) in the definition of the Identifier portion of the record. Since the Code value is not utilized by the ICMP type 8 it is ignored by the peer and is simply parroted back by to the 'client'. As the SFR is not clear as to how granular of a rule needs to be written, it is possible for a Firewall to theoretically only support the ICMP type definition and implicitly specify the code value(s) that correlate to the defined type. This would lead to a scenario where the example above would only ever hit the default rule and could not have a rule written where the type and the code are specified by the administrator.

Please provide clarity on the expected granularity that is expected to be configurable in the firewall rules for the ICMP type/code and Transport Layer Protocol values on a Stateful Firewall device claiming conformance to the PP-Module.

Resolution:

The NIT acknowledges the issue. The following changes shall be applied:

FFW_RUL_EXT.1.2 Application Note 4

{old}

This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement – the applicable interface is a property of the TOE and the rest of the identified attributes are defined in the associated RFCs. Note that the 'Transport Layer Protocol' is the IPv4/IPv6 field that identifies the applicable protocol, such as TCP, UDP, ICMP, or GRE. IPv6 extension headers are defined in RFC 2460 and the ST author may specify which fields within each supported extension header, if any may be used as attributes in the construction of an inspection rule. Also, 'Interface' identified above is the external port where the applicable network traffic was received or will be sent.

{/old}

{new}

This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement – the applicable interface is a property of the TOE and the rest of the identified attributes are defined in the associated RFCs. TOEs are encouraged to support the configuration of all possible values in the specified network protocol fields; however, TOEs are only required to support the configuration of RFC and IANA defined values. It should be noted that FFW_RUL_EXT.1.9 is applicable to any values that cannot be configured. Note that the 'Transport Layer Protocol' is the IPv4/IPv6 field that identifies the applicable protocol, such as TCP, UDP, ICMP, or GRE. IPv6 extension headers are defined in RFC 2460 and the ST author may specify which fields within each supported extension header, if any may be used as attributes in the construction of an inspection rule. Also, 'Interface' identified above is the external port where the applicable network traffic was received or will be sent.

{/new}

SD Section 2.3.2.1 Insert before Paragraph 32

{new}

If the TOE does not support the configuration of all possible values in the specified network protocol fields, the evaluator shall verify the TSS identifies which fields cannot filter all values, and for those fields which values cannot be filtered (implicitly or explicitly) by rules. For any field and value combinations that are not supported, the evaluator shall confirm the values are not IANA recognized values. If the TOE supports the implicit configuration of any values, the evaluator shall ensure the TSS identifies the specific configurations that result in the implicit configuration of a value (e.g., configuring ICMP type 8 implicitly configures ICMP code 0).

{/new}

SD Section 2.3.2.1 Insert Before Paragraph 34

{new}

If the TOE does not support the configuration of rules to filter all possible values in the fields identified in FFW_RUL_EXT.1.2, the evaluator shall verify the Guidance describes which field and value combinations are not filterable. If the TOE supports the implicit configuration of any values, the evaluator shall ensure the Guidance identifies the specific configurations that result in the implicit configuration of a value (e.g., configuring ICMP type 8 implicitly configures ICMP code 0).

{/new}

Rationale:

Not all values need to be configurable; however, TOEs are not allowed to ignore fields that are not used by a protocol. In the example provided in the issue, an organization may want to filter (or at least log) non-standard ICMP traffic (e.g., traffic with non-standard ICMP codes) as an attacker could use this as a signaling channel.

Further Action:

None

Action by Network iTC:

None