Network Device Interpretation # 201837

Conflicting FW rules cannot be configured

Status: ☒ *Active* ☐ *Inactive*

Date: *1-Apr-2019*

End of proposed Transition Period (to be updated after TR2TD process): *1-May-2019*

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 SD V2.0*

Affected Section(s): FFW_RUL_EXT.1.8*, Test 1*

Superseded Interpretation(s): *None*

Issue:

In the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0 + Errata, 14 March 2018 (FWcPP20E) we have the following SFR and test case:

FFW_RUL_EXT.1.8: The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

FFW_RUL_EXT.1.8: Test 1: The evaluator shall devise two equal stateful traffic filtering rules with alternate operations - permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.

The problem we have is that the TOE in question does not allow conflicting rules to be configured. We can test ordering for alternate rules of different scopes, but otherwise while we can devise the alternate rules we cannot actually deploy them. We have seen this behavior in other products where the FW rule API is doing sanity checks to prevent conflicts rather than dealing with that at runtime.

We think this implementation should be acceptable and suggest that Test 1 above be amended to allow either 1) deploy alternate rules to ensure they are processed in the expected order or 2) ensure that alternate (conflicting) rules cannot be configured.

Resolution:

The NIT agrees with the issue described in the Issue section. For FFW_RUL_EXT.1.8 TSS Section the following paragraph shall be added:

<new>”If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the TSS shall describe the underlying mechanism.”</new>

For FFW_RUL_EXT.1.8 Test 1 shall be modified as follows:

<old>*:* Test 1: The evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation. </old>

Shall be replaced by

<new> Test 1: If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the evaluator shall try to configure two conflicting rules and verify that the TOE rejects the conflicting rule(s). It is important to verify that the mechanism is implemented in the TOE but not in the non-TOE environment. If the TOE does not implement a mechanism that ensures that no conflicting rules can be configured, the evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation. </new>

Rationale:

See Issue section.

Further Action:

None.

Action by Network iTC:

None.