Network Device Interpretation # 202403

Behavior for FFW_RUL_EXT.1.10

Status: ☒ *Active* □ *Inactive*

Date: *17-May-2024*

End of proposed Transition Period (to be updated after TR2TD process): *17-May-2024*

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 Mod v1.4e, FW SD v1.4e*

Affected Section(s): *FFW_RUL_EXT.1.10, Test 1*

Superseded Interpretation(s): *None*

Issue:

Issue:

FFW_RUL_EXT.1.10 states: The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [counted].

The test requirement is:

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. The number of SYN requests should exceed the TCP half-open threshold defined on the TOE. TCP SYN-ACK messages should not be acknowledged. The evaluator shall verify through packet capture that once the defined TCP half-open threshold has been reached, subsequent TCP SYN packets are not transmitted to the target system. The evaluator shall verify that when the configured threshold is reached that, depending upon the selection, either a log entry is generated or a counter is incremented.

The test results demonstrate, that the TOE checks the TCP half-open connection limit once per second, so the configured threshold may be exceeded prior to packets being blocked. This is reasonable, because this a DoS threshold where precision is not that important, and the DoS protection should not contribute to consuming resources (e.g., checking every packet). The CCTL plans to observe the timestamp of the TCP SYN Packet that meets the threshold and verify TCP SYNs are blocked within one second. Please let us know if this is a reasonable approach to satisfying the intent of the test. Please confirm if this approach and expected result is acceptable.

Resolution:

According to the test requirements a compliant TOE should limit the number of half-open TCP connections passing through the TOE. A configured limit should not be surpassed and result in a denial of service due to an exceeded configured limit and maxed out connections. The activity to meet compliance should adhere to connections through the TOE. To comply with the SFR the TOE should prevent half open connections from flooding the table and preventing those connections from surpassing the limit.

Rationale:

On a typical gigabit ethernet network, well over 1,000,000 minimum length SYN packets can be sent in a single second, assuming minimum frame size and framing symbols; so, a one-second delay in detecting the DoS could already put the target device into a failing state. Even a device with only 10Mb/s interfaces could pass nearly 12,000 minimum length SYN packets in a second.

Further Action:

None

Action by Network iTC:

None