How are firewall rules evaluated in Eagle Tofino?

- 2018-02-15 - Tofino

The first firewall rule that matches a packet will determine what the firewall does with that packet, based on the 'permission' setting of the rule.

If no rule matches a packet, then the default action is to block that packet and generate an alarm.

When using Tofino CMP, firewall rules are evaluated in the following order:

(1) Rules for non-IP protocols in the firewall tab of each Tofino icon
(2) Rules for IP-based protocols in the firewall tab of each Tofino icon
(3) Rules for IP-based protocols on the firewall tab of each protected device under a Tofino ('Talker' rules)

All rules are evaluated top to bottom as displayed visually in the CMP network editor, within the groups outlined above.

Where multiple rules match the same packet, the first rule that is evaluated will determine how the packet is processed. For example, if a Tofino has a global rule that allows Modbus/TCP traffic, and there is also a Talker rule on a protected device under the same Tofino that uses the Modbus TCP Enforcer to perform content inspection on Modbus/TCP traffic, the Modbus/TCP traffic will be allowed without inspection since the global rule is evaluated before the talker rule.

Rules can be re-ordered by the user on any firewall tab, except that Global rules will always be evaluated before Talker rules (top to bottom, as described above). CMP always displays them in alphabetic order based on the device name, but devices in the network editor can be re-ordered by changing the device name to get the desired rule evaluation order.