Firewall Rule Processing Order

From PFSenseDocs

Rules in pfSense are processed in a specific order. Understanding this order is especially important when crafting more complicated sets of rules and when troubleshooting. This document is intended to give a *general* idea of how rules are processed. It can be much more complicated, especially when floating rules are involved and *out* direction rules are used. See The pfSense Book (https://www.pfsense.org/our-services/gold-membership.html) for more in-depth information.

Short Version

Rules are always processed from the top of a list down, first match wins (except for floating rules without **quick** set, see the next section).

The tl;dr version of **user-defined** rule processing is:

- Rules defined on the floating tab are processed first
- Rules defined on interface group tabs (Including OpenVPN) are processed
- Rules defined on interface tabs (WAN, LAN, OPTx, etc) are processed last

Longer Version

More accurately, the following order (still simplified) is found in the ruleset (Check */tmp/rules.debug*):

- Outbound NAT rules
- Inbound NAT rules such as Port Forwards (including rdr pass and UPnP)
- NAT rules for the Load Balancing daemon (relayd)
- Rules dynamically received from RADIUS for OpenVPN and IPsec clients
- Internal automatic rules (pass and block for various items like lockout, snort, DHCP, etc.)
- User-defined rules:
    - Rules defined on the floating tab
    - Rules defined on interface group tabs (Including OpenVPN)
    - Rules defined on interface tabs (WAN, LAN, OPTx, etc)
- Automatic VPN rules

Floating Rules notes

Floating rules without **quick** set process in a "last match wins" way instead of "first match wins" So if a floating rule is set without **quick** and it matches a packet, then a later rule also matches, the later rule will be used. This is the opposite of the other tab rules (groups, interfaces) and rules with **quick** set which stop processing as soon as a match is made. See What are Floating Rules for more details on how Floating Rules operate.

Retrieved from "https://doc.pfsense.org/index.php?title=Firewall_Rule_Processing_Order& oldid=7377"

Categories: FAQ | Firewall Rules

- This page was last modified on 18 November 2015, at 14:09.