BROCADE

Technical Bulletin

Announcement Date: May 1, 2017

Exclusions: None

Effective Date: Immediate

Expiration Date: None

Products Covered by this bulletin: vRouter 5600

Versions Covered by this bulletin: 5.1 and later

The FW behavior when stateful & stateless rules exist simultaneously with Global State Policy

---

Related to the default behavior change for “global-state-policy” from version 5.1 (for more detail please refer to “Technical_Bulletin_globalstate(IF)_E.pdf”), in case of stateful & stateless rules existing on same FW rule and deployed an IF, modifying FW rule configurations may be required.

■Normal behavior for Stateless & Stateful rules existing simultaneously

When enabling Global-State-policy, ICMP/TCP/UDP of protocols must be set as following:

CLI :

```
set security firewall global-state-policy 'icmp'
set security firewall global-state-policy 'tcp'
set security firewall global-state-policy 'udp'
```

In defining FW rules, in case not specifying “protocol” configuration, it will be treated as “protocol any” and work as Stateless.

Example)

```
set security firewall name FW-IN rule 1 action 'accept'
set security firewall name FW-IN rule 1 source address '10.0.0.0/8'      <- Stateless rule (without Protocol)
set security firewall name FW-IN rule 10 action 'accept'
set security firewall name FW-IN rule 10 protocol 'icmp'      <- ICMP Stateful rule by Global-State
set security firewall name FW-IN rule 11 action 'accept'
set security firewall name FW-IN rule 11 protocol 'tcp'        <- TCP Stateful rule by Global-State

vyatta@vyatta#sh firewall
```

```
------------------------------
Rulesets Information: Firewall
------------------------------
Firewall "FW-IN":
Active on (dp0p192p1, in)
rule    action  proto          packets        bytes
----    ------  -----         -------        -----
1       allow   any            141            15140
  condition - from 10.0.0.0/8                    <<< No ”stateful” description
10      allow   icmp           0              0
  condition - stateful proto icmp

11      allow   tcp            0              0
  condition - stateful proto tcp
```

As above, in order to work as stateful the rules requires to match the protocols specified in “global-state-policy” command. When stateless and stateful rules are in a same FW rule, **the default behavior of return traffic that matches “Stateless” rules will become the behavior dropped as well as “Stateful” traffic. Because of that,**
Return traffic for “Stateful” rule can dynamically pass through FW referring to session table,
Return traffic for “Stateless” rule requires to be set explicit allow rule.

NOTE: Prior to release 5.0, with global-state-policy, all of interfaces have auto-created allow rules working as Stateful, which allow the return traffic to pass. That is why explicit allow rules was not required like this.

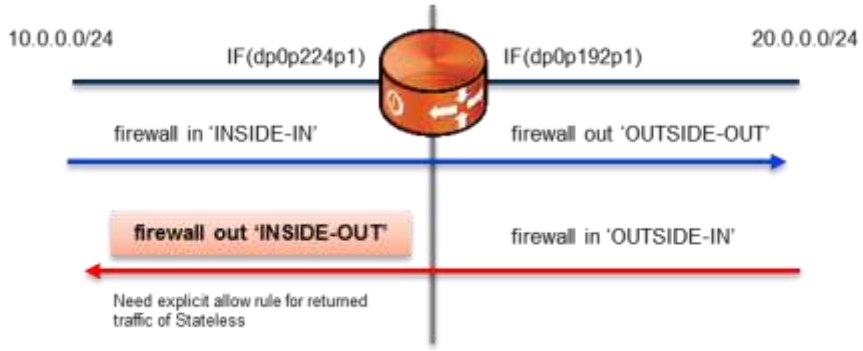
Therefore,

- Define explicit rules to pass the “Stateless” returned traffic
- Define all the rules standardized either “Stateless” or “Stateless”

It should be configured by any of the methods.

- Define explicit rules to pass the “Stateless” return traffic

  As the following example, configure outbound FW rules for returned traffic.



set security firewall name INSIDE-IN rule 1 action 'accept'

set security firewall name INSIDE-IN rule 1 source address '10.0.0.0/24' <<< Stateless rule for going traffic

set security firewall name INSIDE-IN rule 10 action 'accept'

set security firewall name INSIDE-IN rule 10 protocol 'icmp'

set security firewall name INSIDE-IN rule 11 action 'accept'

set security firewall name INSIDE-IN rule 11 protocol 'tcp'

set security firewall name INSIDE-OUT rule 1 action 'accept' >>> Required Stateless rule to pass return traffic

set security firewall name INSIDE-OUT rule 1 destination address '10.0.0.0/24'

set security firewall name OUTSIDE-OUT rule 1 action 'accept'

set security firewall name OUTSIDE-OUT rule 1 source address '10.0.0.0/8' <<< Stateless rule for going traffic

set security firewall name OUTSIDE-OUT rule 10 action 'accept'

set security firewall name OUTSIDE-OUT rule 10 protocol 'icmp'

set security firewall name OUTSIDE-OUT rule 11 action 'accept'

set security firewall name OUTSIDE-OUT rule 11 protocol 'tcp'

set security firewall name OUTSIDE-IN default-action 'drop'

set security firewall name OUTSIDE-IN rule 1 action 'accept'

set security firewall name OUTSIDE-IN rule 1 destination address '10.0.0.0/8'<<< Stateless rule for return traffic

set interfaces dataplane dp0p224p1 firewall in 'INSIDE-IN'

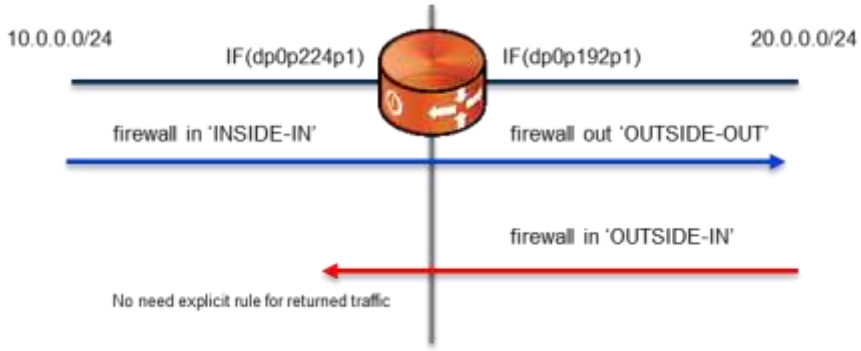
set interfaces dataplane dp0p224p1 firewall out 'INSIDE-OUT' <<<deploy Stateless rules for returned

set interfaces dataplane dp0p192p1 firewall in 'OUTSIDE-IN'

set interfaces dataplane dp0p192p1 firewall out 'OUTSIDE-OUT'

- Define all the rules standardized either “Stateless” or “Stateless”

  As following example, configure ”state enable” or ”protocol” to no protocol rules.



set security firewall name INSIDE-IN rule 1 action 'accept'
set security firewall name INSIDE-IN rule 1 source address '10.0.0.0/8'
set security firewall name INSIDE-IN rule 1 state enable
set security firewall name INSIDE-IN rule 1 protocol tcp
} Specify tcp/udp/icmp protocols or “state enable” to each rule for multiple/other protocols
set security firewall name INSIDE-IN rule 10 action 'accept'
set security firewall name INSIDE-IN rule 10 protocol 'icmp'
set security firewall name INSIDE-IN rule 11 action 'accept'
set security firewall name INSIDE-IN rule 11 protocol 'tcp'

set security firewall name OUTSIDE-OUT rule 1 action 'accept'
set security firewall name OUTSIDE-OUT rule 1 source address '10.0.0.0/8'
set security firewall name OUTSIDE-OUT rule 1 state enable
set security firewall name OUTSIDE-OUT rule 10 action 'accept'
set security firewall name OUTSIDE-OUT rule 10 protocol 'icmp'
set security firewall name OUTSIDE-OUT rule 11 action 'accept'
set security firewall name OUTSIDE-OUT rule 11 protocol 'tcp'
set security firewall name OUTSIDE-IN default-action 'drop'
~~set security firewall name OUTSIDE-IN rule 1 action 'accept'~~ <<< No Stateless rule for returned is required
~~set security firewall name OUTSIDE-IN rule 1 destination address '10.0.0.0/8'~~

set interfaces dataplane dp0p224p1 firewall in 'INSIDE-IN'
set interfaces dataplane dp0p192p1 firewall in 'OUTSIDE-IN'
set interfaces dataplane dp0p192p1 firewall out 'OUTSIDE-OUT'

For a customer who uses Stateless & Stateful rules simultaneously with “global-state-policy” in release 5.1 and later, please review firewall rules and reconfigure appropriate configurations if you are affected.