BROCADE

Technical Bulletin

Announcement Date: March 16, 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

Update to firewall section: Default behavior change for FW global state policy（Zone based FW）

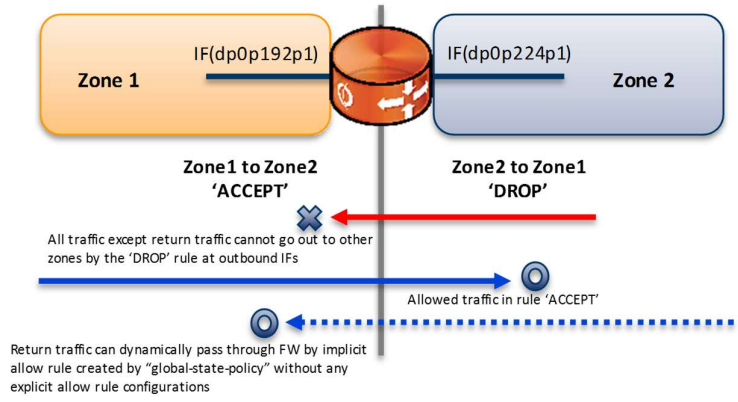
Configuration Examples / Stateful behavior/ Configuring global state policies

Notes

From release 5.1, default behavior for “global-state-policy” of Stateful FW has been changed.
Prior to Release 5.1, the vRouter will add implicit allow rules for reply traffic when global state policies of stateful FW are defined. In release 5.1 and later, an explicit group of rules needs to be created which should be applied to each interface.

■ **Prior to release 5.1**

Topology



firewall configuration （with global-state-policies defined)

```
security {
        firewall {
                global-state-policy {
                        icmp
                        tcp
                        udp
                }
```

```
                name DROP {             <- rule of DROP for all traffic
                        default-action drop
                }
                name ACCEPT {           <- rule of ACCEPT for specified traffic
                        rule 10 {
                                action accept
                                protocol icmp
                        }
                        rule 20 {
                                action accept
                                protocol tcp
                        }
                }
        }
        zone-policy {
                zone zone1 {
                        interface dp0p192p1
                        to zone2 {      <- apply ACCEPT FW policy from zone1 to zone2
                                firewall ACCEPT
                        }
                }
                zone zone2 {
                        interface dp0p224p1
                        to zone1 {      <- apply DROP FW policy from zone2 to zone1
                                firewall DROP
                        }
                }
        }
```

Check output of "show firewall"

"default_state_group" is implicitly added after all FW rules and zone policies are configured. This "default_state_group" is allow action and makes session-table without setting explicit rules on OUT direction firewall.

```
vyatta@FW-01:~$ show firewall
------------------------------------
Rulesets Information: Zone from dp0p192p1
------------------------------------
------------------------------------------------------------------------------
Firewall "ACCEPT":
Active on (dp0p224p1, out)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
10      allow   icmp            355             34790
  condition - stateful proto icmp

20      allow   tcp             16              3327
  condition - stateful proto tcp

Firewall "default_state_group":   ★THIS IS THE IMPLICIT RULE
Active on (dp0p224p1)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
100     allow   tcp             0               0
  condition - stateful proto tcp

200     allow   udp             0               0
  condition - stateful proto udp
```

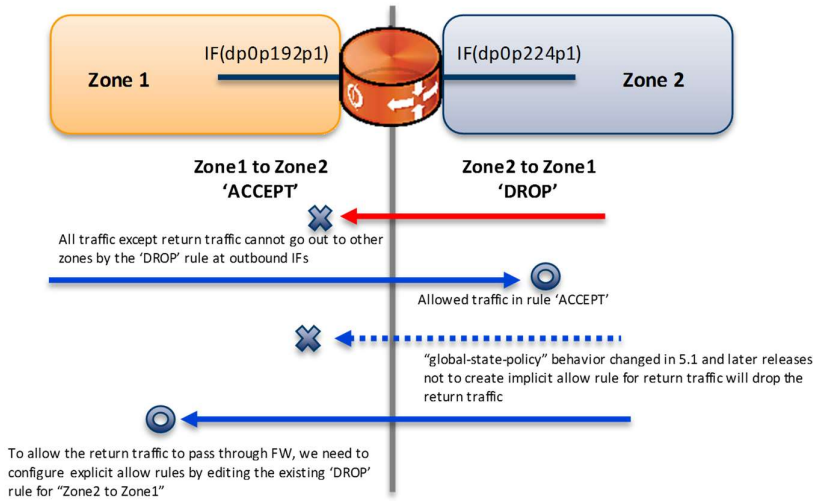
```
300     allow   icmp            0               0
  condition - stateful proto icmp

--------------------------------------
Rulesets Information: Zone from dp0p224p1
--------------------------------------
--------------------------------------------------------------------------------
Firewall "DROP":
Active on (dp0p192p1, out)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
default drop    any             0               0
  condition - all

Firewall "default_state_group":   ★THIS IS THE IMPLICIT RULE
Active on (dp0p192p1)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
100     allow   tcp             0               0
  condition - stateful proto tcp

200     allow   udp             0               0
  condition - stateful proto udp

300     allow   icmp            0               0
  condition - stateful proto icmp
```

While these auto-created “default_state_group” rules are applied to both in/out zone direction, in release 5.1 and later, this behavior has been changed to specify the FW direction and strengthen the security level as follows.

■ Release 5.1 and later

From release 5.1, adding the implicit rules no longer occurs and the explicit rule for return traffic is needed.

So, with the following rule on Zone1 from "dp0s192p1" to Zone2 of “dp0s224p1”, outgoing session is created on dp0s224p1 but reply traffic is dropped because there is no allowed FW rule for Zone2 to Zone1 on ”dp0p192p1”.




```
----------------------------------------
Rulesets Information: Zone from dp0p192p1
----------------------------------------
Firewall "ACCEPT":
Active on (dp0p224p1, out)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
10      allow   icmp            2204            215992
  condition - stateful proto icmp

20      allow   tcp             79              14257
  condition - stateful proto tcp
```

To avoid this, the explicit allow FW rule is needed in the direction from Zone2 to Zone1.

For example)

```
vyatta@FW-01# show security firewall
security {
        firewall {
                global-state-policy {
                        icmp
                        tcp
                        udp
                }
                name DROP {
                        default-action drop
                        rule 10 {       <- ★Add the explicit allow rule for return traffic
                                action accept
                                protocol icmp
                        }
                        rule 20 {       <- ★Add the explicit allow rules for return traffic
                                action accept
                                protocol tcp
                        }
```

```
        }
        name ACCEPT {          <- rule of ACCEPT for specified traffic
                rule 10 {
                        action accept
                        protocol icmp
                }
                rule 20 {
                        action accept
                        protocol tcp
                }
        }
}
zone-policy {
        zone zone1 {
                interface dp0p192p1
                to zone2 {     <- apply ACCEPT FW policy from zone1 to zone2
                        firewall ACCEPT
                }
        }
        zone zone2 {
                interface dp0p224p1
                to zone1 {       <- apply DROP FW policy from zone2 to zone1
                        firewall DROP
                }
        }
}
```

If “global-state-policy” is not configured, this behavior change is not affected.
Also, if using “state enable” option in each rule instead of global-state-policy, the behavior change is not affected.
For a customer who is using “global-state-policy” in release 5.0 and earlier and is going to upgrade to 5.1 and later, please review firewall rules and add appropriate configurations.