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

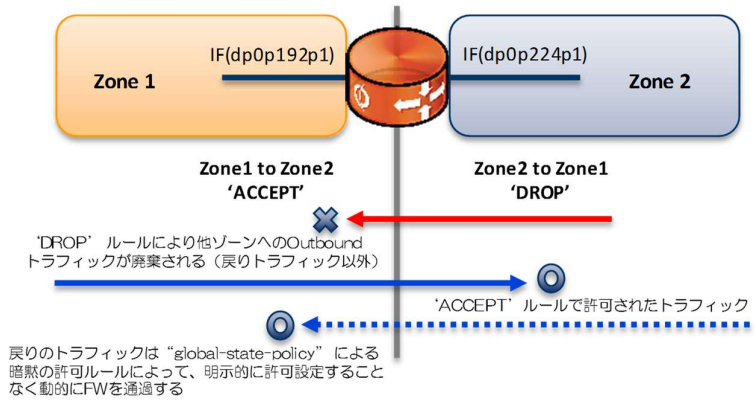
Firewall 機能のデフォルト動作変更について（Zone based FW）

コンフィグ例・ステートフル動作・global-state ポリシー設定

Notes

リリース 5.1 からステートフル FW の”global-state-policy”設定時の動作が変更されています。
リリース 5.1 より前のバージョンでは、ステートフル FW の”global-state-policy”を設定すると、vRouter がセッションの戻り通信のための暗黙の Allow ルールを自動追加していましたが、リリース 5.1 以降では明示的に Allow ルール設定を追加する必要があります。

■ リリース 5.0 より前のバージョンでの動作
例）
構成



firewall 設定例（グローバルでステートフルを有効化）

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

```
                name DROP {             ← 全トラフィックを Drop する FW ルール
                        default-action drop
                }
                name ACCEPT {           ← トラフィックを ACCEPT する FW ルール
                        rule 10 {
                                action accept
                                protocol icmp
                        }
                        rule 20 {
                                action accept
                                protocol tcp
                        }
                }
        }
        zone-policy {
                zone zone1 {
                        interface dp0p192p1
                        to zone2 {          ← zone1 から zone2 への FW ポリシーを適用
                                firewall ACCEPT
                        }
                }
                zone zone2 {
                        interface dp0p224p1
                        to zone1 {          ← zone2 から zone1 への FW ポリシーを適用
                                firewall DROP
                        }
                }
        }
```

show firewall で確認

上記設定例を適用した状態を確認すると、設定した適用したルールとは別に"default_state_group"が追加されます。このルールは allow action となり、OUT 側での FW ルールを明示的に設定しなくても、セッションテーブルが自動作成されます。

```
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":    ← 自動作成された allow ルール
Active on (dp0p224p1)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
100     allow   tcp             0               0
  condition - stateful proto tcp
```

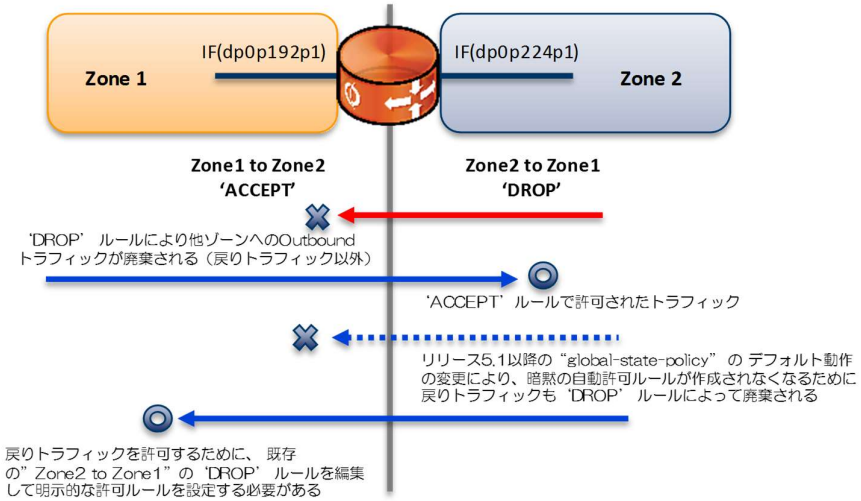
```
200     allow   udp             0               0
  condition - stateful proto udp

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":    ← 自動作成された allow ルール
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
```

この自動作成された"default_state_group"のルールは zone 間の両方向の通信に適用されますが、より方向性を限定してセキュリティを強化するために、次の通りリリース 5.1 から動作が変更されています。

■ リリース 5.1 以降の動作

5.1 以降ではこの"default_state_group" という暗黙の allow ルールの追加が廃止され、明示的に戻り通信を許可するための allow ルールを設定するように変更されています。

以下のルールで Zone1 の"dp0p192p1" から Zone2 の"dp0p224p1"へ出て行くときのルールは作られますが、戻り通信を許可するルールが自動で作られなくなるため戻りの Drop ルールで落とされることになります。




```
----------------------------------------
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
```

これを回避するために、明示的に Zone2 から Zone1 への Allow ルールを設定する必要があります。

例）

```
security {
        firewall {
                global-state-policy {
                        icmp
                        tcp
                        udp
                }
                name DROP {
                        default-action drop
                        rule 10 {       ← ★戻りトラフィックを明示的に許可するルールを追加
                                action accept
                                protocol icmp
                        }
                        rule 20 {       ← ★戻りトラフィックを明示的に許可するルールを追加
                                action accept
                                protocol tcp
                        }
                }
```

```
        name ACCEPT {          ← トラフィックを ACCEPT する FW ルール
                rule 10 {
                        action accept
                        protocol icmp
                }
                rule 20 {
                        action accept
                        protocol tcp
                }
        }
}
zone-policy {
        zone zone1 {
                interface dp0p192p1
                to zone2 {          ← zone1 から zone2 への FW ポリシーを適用
                        firewall ACCEPT
                }
        }
        zone zone2 {
                interface dp0p224p1
                to zone1 {          ← zone2 から zone1 への FW ポリシーを適用
                        firewall DROP
                }
        }
}
```

“global-state-policy”を使用していない場合の動作には変更はありません。
また、FW ルール毎に”state enable”を設定してステータス FW をご使用の場合には今回の仕様動作の影響はございません。

旧バージョンにて“global-state-policy”をご使用中でリリース 5.1 以降へ移行されるお客様へは大変お手数をおかけいたしますが、FW ルール設定にご注意いただき、該当する場合には適切に再設定いただけますようお願いいたします。

以上