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（Interface based FW）

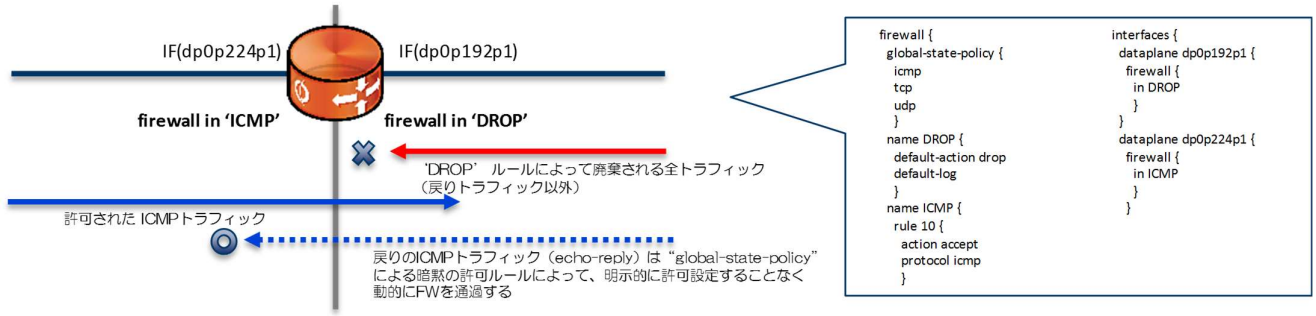
コンフィグ例・ステートフル動作・global-state ポリシー設定

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 5.1 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）

```
vyatta@FW-01# show security firewall
 firewall {
        global-state-policy {
                icmp
                tcp
                udp
        }
        name DROP {                    ← トラフィックを Drop する FW ルール
                default-action drop
```

```
                default-log
        }
        name ICMP {                ← ICMP を許可する FW ルール
                rule 10 {
                        action accept
                        protocol icmp
                }
        }

vyatta@FW-01# show interfaces
 interfaces {
        dataplane dp0p192p1 {
                address 10.0.0.1/24
                firewall {             ← ”DROP” FW ルールを IF に適用
                        in DROP
                }
        }
        dataplane dp0p224p1 {
                address 192.168.10.254/24
                firewall {              ← ”ICMP” FW ルールを IF に適用
                        in ICMP
                }
        }
```

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: Firewall
------------------------------------
-------------------------------------------------------------------------------
Firewall "DROP":
Active on (dp0p192p1, in)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
default drop    any             0               0
  condition - all apply log

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

Firewall "ICMP":
Active on (dp0p224p1, in)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
```

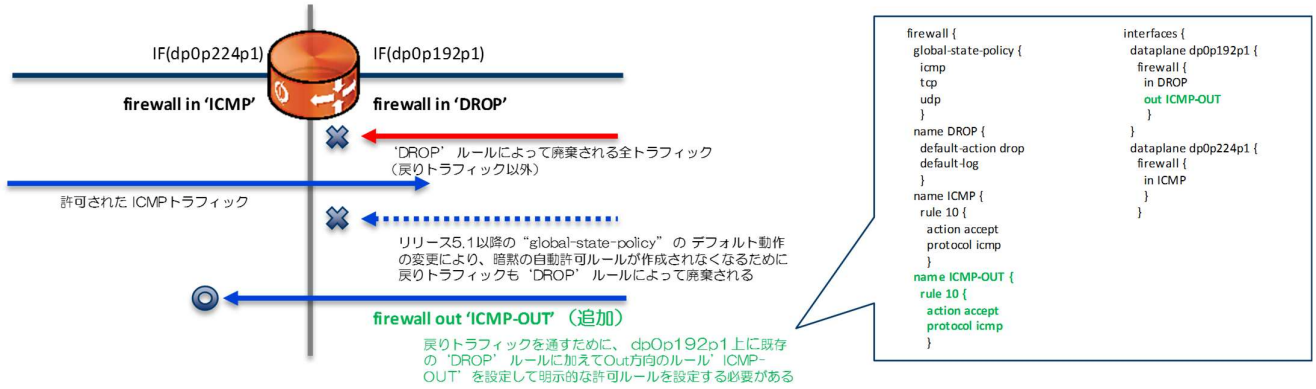
```
10      allow   icmp            0               0
  condition - stateful proto icmp

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
```

この自動作成された"default_state_group"のルールは in/out 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。

つまり、以下のルールで"dp0p224p1 から入ってきたというセッションは作られますが、dp0p192p1 から出て行った"というセッションが作られないため、戻りの Drop ルールで落とされてしまうことになります。




```
Firewall "ICMP":
Active on (dp0p224p1, in)
rule    action  proto           packets         bytes
----    ------  -----           -------         -----
10      allow   icmp            0               0
  condition - stateful proto icmp
```

これを回避するために、明示的に dp0p192p1 の OUT 側で Allow ルールを設定する必要があります。

例）

```
vyatta@FW-01# show security firewall
 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
                default-log
        }
        name ICMP {                ← ICMP を許可する FW ルール
                rule 10 {
                        action accept
                        protocol icmp
                }
        name ICMP-OUT {            <<<★ OUT 側の Allow を明示的に設定
                rule 10 {
                        action accept
                        protocol icmp
                }
   }

vyatta@FW-01# show interfaces
 interfaces {
        dataplane dp0p192p1 {
                address 10.0.0.1/24
                firewall {
                        in DROP
                        out ICMP-OUT    <<<★ OUT 側の Allow を追加
                }
        }
        dataplane dp0p224p1 {
                address 192.168.10.254/24
                firewall {
                        in ICMP
                }
        }
```

“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