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

Global State Policy 有効時の stateful ルールと stateless ルール混在時の動作について

Release5.1 以降の Global State Policy の仕様動作変更に関連して（※Technical_Bulletin_globalstate(IF)_J.pdf 参照）、同一 IF 上に Deploy する Firewall ルール設定に stateful ルールと stateless ルールが混在している場合の動作にも関係してくるため Firewall の設定内容を見直す必要がある場合があります。

■Stateless ルールと Stateful ルール混在時の仕様動作

Global-State-policy 有効時には Protocol（ICMP、TCP、UDP）のいずれかを指定します。

CLI：

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

FW ルールを定義する際に、ルール内でプロトコルを指定しない場合は”Protocol any”として扱われ、Stateful に該当する特定の Protocol のルールとはならずに Stateless ルールとなります。

出力例）

```
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 ルール（Protocol 指定なし）
set security firewall name FW-IN rule 10 action 'accept'
set security firewall name FW-IN rule 10 protocol 'icmp'      ←Global-State による Statelful ルール（icmp 指定）
set security firewall name FW-IN rule 11 action 'accept'
set security firewall name FW-IN rule 11 protocol 'tcp'       ←Global-State による Statelful ルール（tcp 指定）

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        ★"stateful"の記載がなく Stateless となっている

10      allow   icmp           0               0
  condition - stateful proto icmp

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

上述のとおり、stateful で動作するにはルールが global-state-policy で指定する protocol に match する必要があります。これら stateless と stateful ルールが同一 FW name のルール内に混在する場合、**Stateless ルールに match する戻りトラフィックのデフォルト動作が、Stateful のトラフィックと同様にドロップされる動作となります。**そのため、

Stateful ルールの戻りトラフィックはセッションテーブルを見て動的に通過しますが、

Stateless ルールの戻りトラフィックは Firewall ルールで通るように設定が必要です。

※5.0 より以前のバージョンでは、global-state-policy 有効時は全 IF に stateful の自動 allow ルールが自動作成される動作であったため、その動作に則って実際は Stateful 動作して通過させていたため、このような設定は必要ありませんでした。

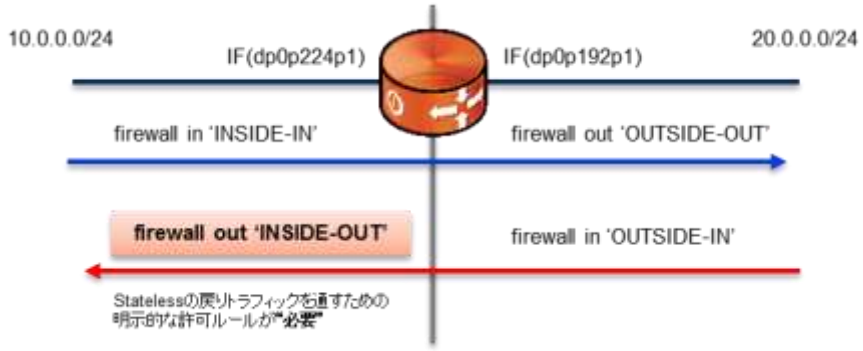
従いまして、

- Stateless の戻りトラフィックを通すルールを明示的に定義する
- 全て Stateful ルール（もしくは全て Stateless）に統一してルールを定義する

いずれかの方法でルールを設定します

■Stateless の戻りトラフィックを通すルールを明示的に定義する

以下例のように戻りトラフィックを通すための FW ルール(OUT)を設定します。



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'　★行きの Stateless ルール

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'　★Release 5.1 以降必要となる戻りトラフィックを

set security firewall name INSIDE-OUT rule 1 destination address '10.0.0.0/24'　通す Stateless ルール

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'　★行きの Stateless ルール

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'　★戻りの Stateless ルール

set interfaces dataplane dp0p224p1 firewall in 'INSIDE-IN'

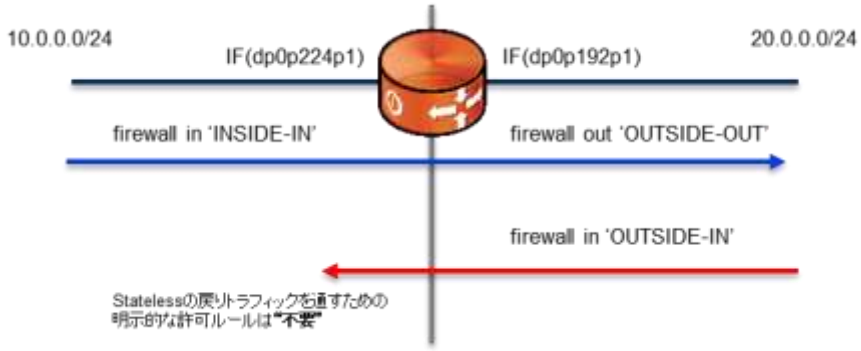
set interfaces dataplane dp0p224p1 firewall out 'INSIDE-OUT'　★戻りの Stateless ルールを適用

set interfaces dataplane dp0p192p1 firewall in 'OUTSIDE-IN'

set interfaces dataplane dp0p192p1 firewall out 'OUTSIDE-OUT'

■全て Stateful ルール（もしくは全て Stateless）に統一してルールを定義する

以下例のように、Stateless ルールになるものは”state enable”か”protocol”を設定します。



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
} tcp,udp,icmp の protocol を指定するか、複数やその他の protocol の場合は state enable を個別に設定する
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'~~ ★Stateful になるため、戻りの Stateless ルールも不要
~~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'

Stateless と Stateful のルールが混在する環境でリリース 5.1 以降をご使用になられるお客様に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設定いただけますようお願いいたします。

以上