IP　Filter設定例

2024年7月18日

株式会社ネットワークバリューコンポネンツ

NVC NETWORK VALUE COMPONENTS

IP Filter設定例

本手順は IP FilterによりGigamon管理ポートへの通信を制限する手順となります。
特定の端末からSSHを許可、それ以外は通信をブロックします。

- デフォルトでは当IP Filter機能はオフとなっております。
- 許可された通信以外はすべてブロックの挙動となりますのでご注意ください。snmpポーリングを行われている場合などは通信要件に応じてルールを追加ください。
- クラスター構成においてはノード間の通信についてもMgmtインターフェースが使用されております。このためクラスターの各ノードの管理インターフェース間につきましては全通信を明示的に許可いただくことを推奨します。
- デフォルトで内部管理通信を許可するポリシーが設定されますので、削除されませんようご注意ください。

IP Filter設定例

１．現在の設定を確認します。「 Packet filtering for IPv4」がDISABLED（無効）であることを確認します。

```
# show ip filter configured
Packet filtering for IPv4: DISABLED
Apply filters to bridges: no
IPv4 configuration (ignored until filtering is enabled):

Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
Policy: DROP

Chain 'OUTPUT'
  No rules.
Policy: ACCEPT

Chain 'FORWARD'
  No rules.
Policy: DROP
```

※初期状態で設定されている内部管理通信となります

IP Filter設定例

２．設定例：送信元(172.16.111.111）から管理ポートのアドレス(172.16.111.222)へのSSH、HTTPSの許可設定を行います

```
# ip filter chain INPUT rule append tail target ACCEPT source-addr 172.16.111.111 /32 dest-addr 172.16.111.222 /32 dest-port 22 in-intf eth0 protocol tcp
# ip filter chain INPUT rule append tail target ACCEPT source-addr 172.16.111.111 /32 dest-addr 172.16.111.222 /32 dest-port 443 in-intf eth0 protocol tcp
```

※　/32のプレフィックス前にスペースが必要
※　必要に応じてその他使用する通信を許可設定を追加してください

３．設定を確認します

```
# show ip filter configured
～中略～
Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 22,  inb eth0
  8  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 443,  inb eth0
```

←設定したルールが追加されます

４，ルールが追加されたらIP Filterを有効化します

```
# ip filter enable
```

警告が出るのでYESを入力後、Enterキーを押します

```
WARNING!! Enabling the ipv4/ipv6 filter may impact mgmt and clustering ports and operations!!.
Enter  'YES'  to confirm this operation:  YES
```

IP Filter設定例

５，有効化後の設定を確認します

```
# show ip filter configured
Packet filtering for IPv4: enabled
Apply filters to bridges: no
IPv4 configuration:

Chain 'INPUT'
  #  Target  Proto   Source              Destination         Other
  1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 22, inb eth0
  8  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 443, inb eth0
Policy: DROP

Chain 'OUTPUT'
  No rules.
Policy: ACCEPT

Chain 'FORWARD'
  No rules.
Policy: DROP
```

以上がIP Filter追加設定手順となります

IP Filter設定例（削除手順）

【設定の削除手順】

１．ルール設定を確認し、削除するルールのIDを確認します。

```
# show ip filter configured

 1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 22, inb eth0
  8  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 443, inb eth0
```

←削除したいルールIDを確認する

２．ルールID:8の設定を削除します。

```
# no ip filter chain INPUT rule 8
```

３．ルール設定を確認し、ルールが削除されたことを確認します。

```
# show ip filter configured

 1  ACCEPT  icmp    all                 all
  2  ACCEPT  igmp    all                 all
  3  ACCEPT  all     all                 all                 state ESTABLISHED,RELATED
  4  ACCEPT  all     all                 all                 inb lo
  5  ACCEPT  all     12.19.148.0/24      all
  6  ACCEPT  all     all                 12.19.148.0/24
  7  ACCEPT  tcp     172.16.111.111/32   172.16.111.222/32   dpt 22, inb eth0
```

以上がIP Filter設定削除手順となります

NVC NETWORK VALUE COMPONENTS