GigaVUE-FM IPアクセス制限設定例

2025年7月24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

GigaVUE-FM IPアクセス制限設定例

本手順は firewalldによりGigaVUE-FM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HTTPSを許可、またはブロックします。

- 不適切な設定を行った場合、FMへのリモートアクセスが不可となったり、FM機能が利用できなくなる可能性があります。ルール追加は設定内容を注意し実施してください。
- デフォルトの firewalld ルールを削除または修正しないでください。

GigaVUE-FM IPアクセス制限設定例

１．デフォルトのゾーン、ルールを確認します。

ゾーン名を確認するコマンドを入力します

```
$ sudo firewall-cmd --get-active-zones
fm
  interfaces: eth0
```

※ゾーン名がfmであることを確認します

ルールを確認するコマンドを入力します

```
$ sudo firewall-cmd --list-all
fm (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv4" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv6" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv6" source NOT address="::1" port port="8009" protocol="tcp" reject
        rule family="ipv6" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="127.0.0.1" port port="8009" protocol="tcp" reject
        rule family="ipv6" source NOT address="::1" port port="8080" protocol="tcp" reject
        rule family="ipv4" icmp-block name="timestamp-request"
        rule family="ipv6" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv4" icmp-block name="timestamp-reply"
        rule family="ipv4" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="127.0.0.1" port port="2181" protocol="tcp" reject
        rule family="ipv4" source NOT address="127.0.0.1" port port="8080" protocol="tcp" reject
```

※初期状態で設定されているルールとなります

NVC NETWORK VALUE COMPONENTS

GigaVUE-FM IPアクセス制限設定例

２．必要なルールを追加します

例 １： ソースが 10.1.8.0/24 サブネット以外の、FM への ipv4 HTTPS アクセスを制限します。
```
 sudo firewall-cmd —zone=fm —add-rich-rule='rule family="ipv4" source NOT address="10.1.8.0/24" port protocol="tcp" port="443" drop' —permanent
```

例 ２： 10.5.11.114 ホストから FM へのすべてのアクセスを制限します。
```
sudo firewall-cmd --zone=fm --add-rich-rule='rule family="ipv4" source address="10.5.11.114" reject' —permanent
```

例 ３： ソースが 10.2.3.0/22 サブネット以外の、FM への SSH アクセスを制限します。
```
sudo firewall-cmd --zone=fm --add-rich-rule='rule family="ipv4" source NOT address="10.2.3.0/22" port protocol="tcp" port="22" drop' —permanent
```

３．firewalld を再起動して変更を適用します。
```
$ sudo firewall-cmd --reload
```

NVC NETWORK VALUE COMPONENTS

GigaVUE-FM IPアクセス制限設定例

５，有効化後の設定を確認します
ルールを確認するコマンドを入力します

```
$ sudo firewall-cmd --list-all
fm (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: eth0
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
 rich rules:
        rule family="ipv4" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv4" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv6" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv6" source NOT address="::1" port port="8009" protocol="tcp" reject
        rule family="ipv6" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="10.1.8.0/24" port port="443" protocol="tcp" drop
        rule family="ipv4" source NOT address="127.0.0.1" port port="8009" protocol="tcp" reject
        rule family="ipv6" source NOT address="::1" port port="8080" protocol="tcp" reject
        rule family="ipv4" icmp-block name="timestamp-request"
        rule family="ipv6" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv4" icmp-block name="timestamp-reply"
        rule family="ipv4" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="127.0.0.1" port port="2181" protocol="tcp" reject
        rule family="ipv4" source NOT address="127.0.0.1" port port="8080" protocol="tcp" reject
```

※ルールが追加されていることを確認します

以上がfirewalldによるルール追加設定手順となります

NVC NETWORK VALUE COMPONENTS

GigaVUE-FM IPアクセス制限設定例（削除手順）

【設定の削除手順】

１．remove-rich-ruleオプションでルールを削除します。

例 １： ソースが 10.1.8.0/24 サブネット以外の、FM への ipv4 HTTPS アクセスを制限したルールを削除します

```
$ sudo firewall-cmd --zone=fm --remove-rich-rule='rule family="ipv4" source NOT address="10.1.8.0/24" port protocol="tcp" port="443" drop' --permanent
```

２．firewalld を再起動して変更を適用します。

```
$ sudo firewall-cmd --reload
```

３，有効化後の設定を確認します

ルールを確認するコマンドを入力します

```
$ sudo firewall-cmd --list-all
fm (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: eth0
  ～中略～
 rich rules:
        rule family="ipv4" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv4" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv6" forward-port port="514" protocol="udp" to-port="9514"
        rule family="ipv6" source NOT address="::1" port port="8009" protocol="tcp" reject
        rule family="ipv6" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="127.0.0.1" port port="8009" protocol="tcp" reject
        rule family="ipv6" source NOT address="::1" port port="8080" protocol="tcp" reject
        rule family="ipv4" icmp-block name="timestamp-request"
        rule family="ipv6" forward-port port="162" protocol="udp" to-port="9162"
        rule family="ipv4" icmp-block name="timestamp-reply"
        rule family="ipv4" forward-port port="514" protocol="tcp" to-port="9514"
        rule family="ipv4" source NOT address="127.0.0.1" port port="2181" protocol="tcp" reject
        rule family="ipv4" source NOT address="127.0.0.1" port port="8080" protocol="tcp" reject
```

※ルールが削除されていることを確認します

以上がfirewalldによるルール設定削除手順となります

NVC NETWORK VALUE COMPONENTS