

Juniper SRX 日本語マニュアル

Firewall Filter (ACL) の CLI 設定

JUNIPER
NETWORKS

Engineering
Simplicity

はじめに

Firewall Filter (ACL) の CLI 設定について説明します。

※手順内容は「SRX300」、JUNOS「19.4R3-S1」にて確認を実施しております。
実際の設定内容やパラメータは導入する環境や構成によって異なります。
各種設定内容の詳細は下記リンクよりご確認ください。

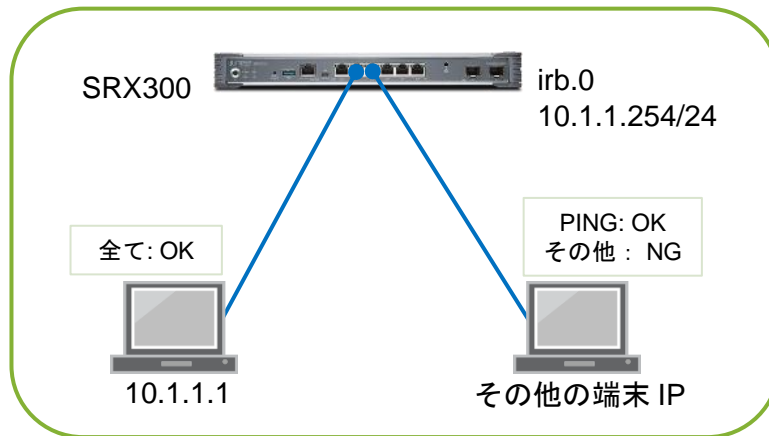
<https://www.juniper.net/documentation/>

2021年7月

Firewall Filter (ACL)

構成概要

SRX300 の irb.0 インタフェースにて、特定の端末 IP (10.1.1.1)からの全ての通信を許可し、他の端末 IP からは PING 通信のみを許可する Firewall Filter (ACL) 設定を設定します。



※機器宛の通信を使用の場合は、セキュリティゾーンでの host-inbound-traffic の許可を別途設定する必要があります。

Firewall Filter (ACL)

1. 特定の端末 IP (10.1.1.1)からの通信を許可(accept)する Firewall Filter を設定

```
user@srx# set firewall family inet filter FILTER term Allow-PC from source-address 10.1.1.1/32
user@srx# set firewall family inet filter FILTER term Allow-PC then accept
```

2. 同 Firewall Filter に PING (ICMP)を許可(accept)する term を設定

```
user@srx# set firewall family inet filter FILTER term Allow-PING from protocol icmp
user@srx# set firewall family inet filter FILTER term Allow-PING then accept
```

3. その他の通信を遮断(discard)する term を設定

```
user@srx# set firewall family inet filter FILTER term BLOCK then discard
```

4. 定義したフィルタをインタフェース(irb.0)に適用

```
user@srx# set interface irb unit 0 family inet filter input FILTER
```

5. 定義した設定内容を適用

```
user@srx# commit
commit complete
```

Firewall Filter (ACL)

設定の確認

```
user@srx# show
firewall {
  family inet {
    filter FILTER {
      term Allow-PC {
        from {
          source-address {
            10.1.1.1/32;
          }
        }
        then accept;
      }
      term Allow-PING {
        from {
          protocol icmp;
        }
        then accept;
      }
      term BLOCK {
        then {
          discard;
        }
      }
    }
  }
}
```

Firewall Filter (ACL)

設定の確認

```
interfaces {
  irb {
    unit 0 {
      family inet {
        filter {
          input FILTER;
        }
      }
    }
  }
}
```

Firewall Filter (ACL)

動作の確認

```
user@srx> show firewall ※ Firewall Filter の設定の確認
```

```
user@srx> show firewall filter {filter name} ※ Firewall Filter の確認
```

```
user@srx> show firewall log ※ Firewall Filter のログを確認
```