Juniper SRX 日本語マニュアル

管理サービスのアクセス制御設定

Juniper NETWORKS | Engineering Simplicity

はじめに

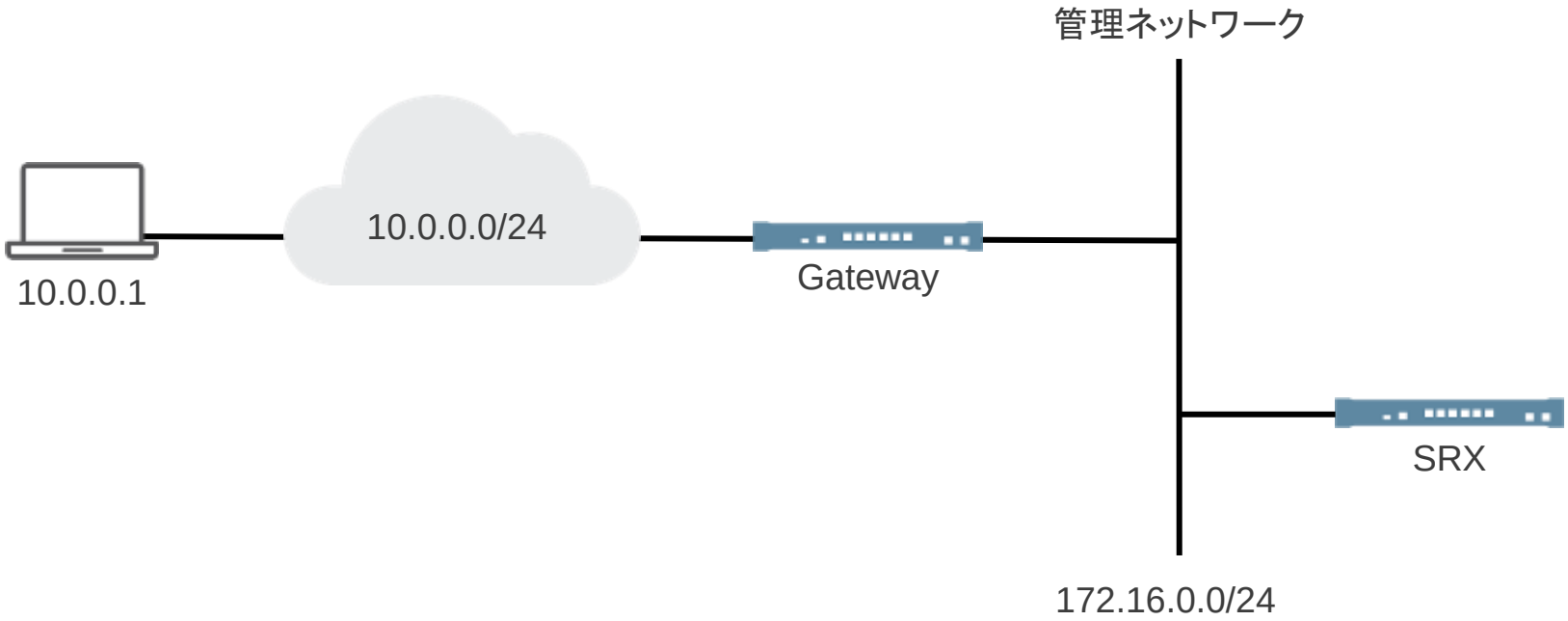
Firewall Filter(ACL) で、デバイス管理できる IP アドレスを制限する CLI 設定について説明します。

※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

管理サービスのアクセス制御設定

構成概要



管理サービスのアクセス制御設定

デバイスの管理を許可する管理ネットワーク(172.16.0.0/24)とリモート管理端末(10.0.0.1/32)をプレフィックスリストに manager-ip として設定

```
user@srx# set policy-options prefix-list manager-ip 172.16.0.0/24
user@srx# set policy-options prefix-list manager-ip 10.0.0.1/32
```

Firewall Filter を設定して、プレフィックスリストで定義されているアドレスを除くすべての IP アドレスからの Telnet および SSH トラフィックを拒否

```
user@srx# set firewall filter management term block_non_manaer from source-address 0.0.0.0/0
user@srx# set firewall filter management term block_non_manaer from source-prefix-list manager-ip except
user@srx# set firewall filter management term block_non_manaer from protocol tcp
user@srx# set firewall filter management term block_non_manaer from destination-port ssh
user@srx# set firewall filter management term block_non_manaer from destination-port telnet
user@srx# set firewall filter management term block_non_manaer then discard
```

他のすべてのトラフィックを受け入れるデフォルトの条件を設定

```
user@srx# set firewall filter manager term allow_everything_else then accept
```

ループバックインターフェースに Firewall Filter を入力フィルタとして適用

```
user@srx# set interfaces lo0 unit 0 family inet filter input management
```

管理ネットワークのアクセス制御設定

設定の確認

```
user@srx# show
interfaces {
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input management;
                }
            }
        }
    }
}
policy-options {
    prefix-list manager-ip {
        10.0.0.1/32;
        172.16.0.0/24;
    }
}
```

管理ネットワークのアクセス制御設定

```
firewall {
    filter management {
        term block_non_manager {
            from {
                source-address {
                    0.0.0.0/0;
                }
                source-prefix-list {
                    manager-ip except;
                }
                protocol tcp;
                destination-port [ ssh telnet ];
            }
            then {
                discard;
            }
        }
        term allow_everything_else {
            then accept;
        }
    }
}
```