Juniper SRX 日本語マニュアル

26. Traffic Logging の CLI 設定

はじめに

Traffic Logging の CLI 設定方法について説明します。

※手順内容は「SRX300」、JUNOS「15.1X49-D140」にて確認を実施しております。

2018年8月

Traffic Logging

2種類の収集方法から選択が可能

- Event Mode
  Default 設定（最大1500 events/sec）

- Stream Mode
  高負荷なトラフィック環境で Security Log の取得が必要な場合には推奨されるモード

ロギング設定

Traffic Log を取得したい FW ポリシーでアクションを指定

```
user@srx# set security policies from-zone trust to-zone untrust policy P1 then log session-init
user@srx# set security policies from-zone trust to-zone untrust policy P1 then log session-close
```

Traffic Logging

Event Mode

① Event Mode を宣言して、イベントレート、フォーマットなどを指定

```
user@srx# set security log mode event
user@srx# set security log event-rate 100
user@srx# set security log format sd-syslog
```

② Log を Local Storage に保存する場合は File 名を指定

Traffic Logのメッセージは“RT_FLOW”にマッチ

```
user@srx# set system syslog file TRAFFIC-LOG any any
user@srx# set system syslog file TRAFFIC-LOG match RT_FLOW
```

Syslog サーバーに送信する場合は Host を指定

Traffic Logのメッセージは“RT_FLOW”にマッチ

```
user@srx# set system syslog host 192.168.0.99 any any
user@srx# set system syslog host 192.168.0.99 match RT_FLOW
```

Traffic Logging

Stream Mode

① Stream Mode を宣言して、Source Address を指定

```
user@srx# set security log mode stream
user@srx# set security log source-address 192.168.0.254
```

② フォーマット、Syslog サーバーのターゲットを指定

```
user@srx# set security log stream TRAFFIC-LOG format sd-syslog
user@srx# set security log stream TRAFFIC-LOG host 192.168.0.99
```

Traffic Logging

設定の確認（Event Mode）

```
user@srx> show
system {
    syslog {
        host 192.168.0.99 {
            any any;
            match RT_FLOW;
        }
        file TRAFFIC-LOG {
            any any;
            match RT_FLOW;
        }
    }
}
security {
    log {
        mode event;
        event-rate 100;
        format sd-syslog;
    }
}
```

Traffic Logging

設定の確認（Stream Mode）

```
user@srx> show
security {
    log {
        mode stream;
        source-address 192.168.0.254;
        stream TRAFFIC-LOG {
            format sd-syslog;
            host {
                192.168.0.99;
            }
        }
    }
}
```