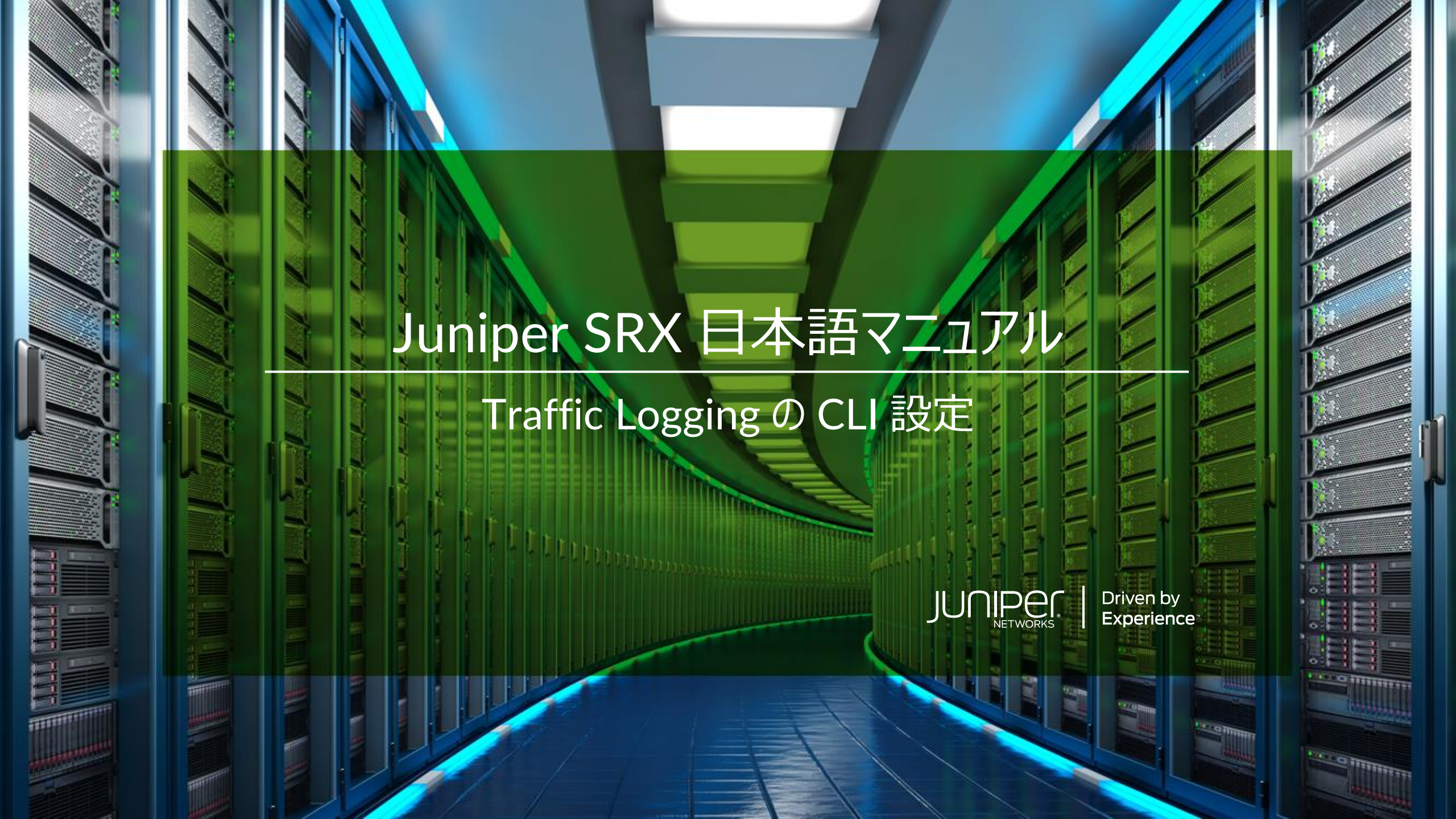


Juniper SRX 日本語マニュアル

Traffic Logging の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、Traffic Logging の CLI 設定について説明します
- 手順内容は SRX300 、Junos 21.2R3-S2 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/

- 他にも多数の SRX 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/security.html

2022 年 8 月

Traffic Logging

ログの収集方法は以下の 2 つのモードから選択可能です

- Event Mode
  - Default 設定 (最大 1500 events/sec)
  - コントロールプレーンで処理した後に Syslog サーバへ送信されるため高トラフィック環境では
    コントロールプレーンの処理負荷が増大します

- Stream Mode
  - コントロールプレーンでの処理は挟まず、データプレーンのみで処理されますので高トラフィック環境で
    Security Log の取得が必要な場合に推奨されます

Traffic Logging

ロギング設定 (Event Mode および Stream Mode 共通)

- セキュリティ ポリシーで取得したい Traffic Log のアクションを指定します

```
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

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します

```
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 名を指定します
   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
```

3. Syslog サーバーに送信する場合は Host を指定します
   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 - Event Mode

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 - Stream Mode

Stream Mode

1. Stream Mode を宣言して Source Address を指定します

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

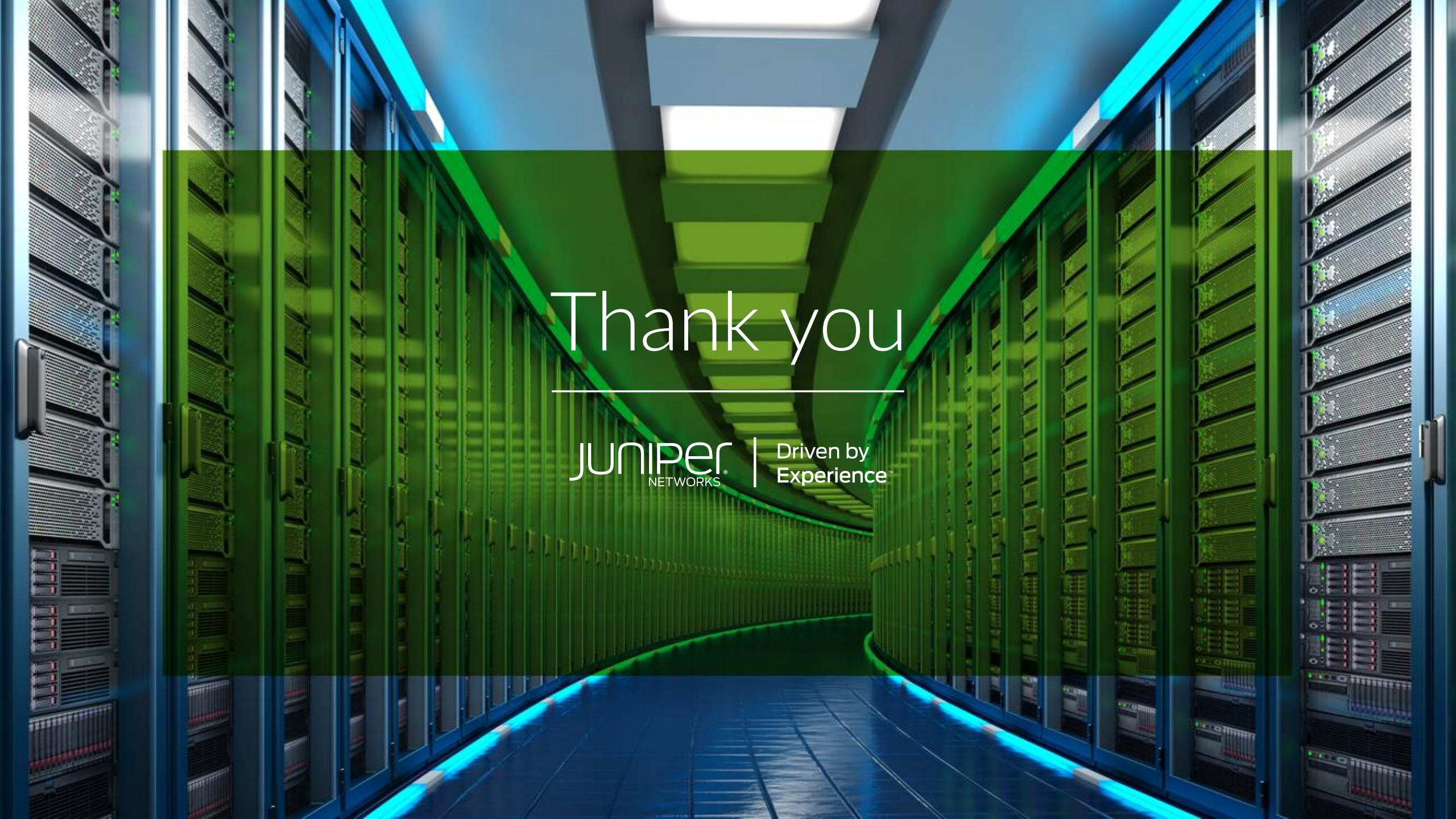
2. フォーマット、Syslog サーバーのターゲットを指定します

```
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 - Stream Mode

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;
            }
        }
    }
}
```


Thank you
JUNIPER NETWORKS
Driven by Experience™