Juniper SRX 日本語マニュアル

Application Firewall の CLI 設定

はじめに

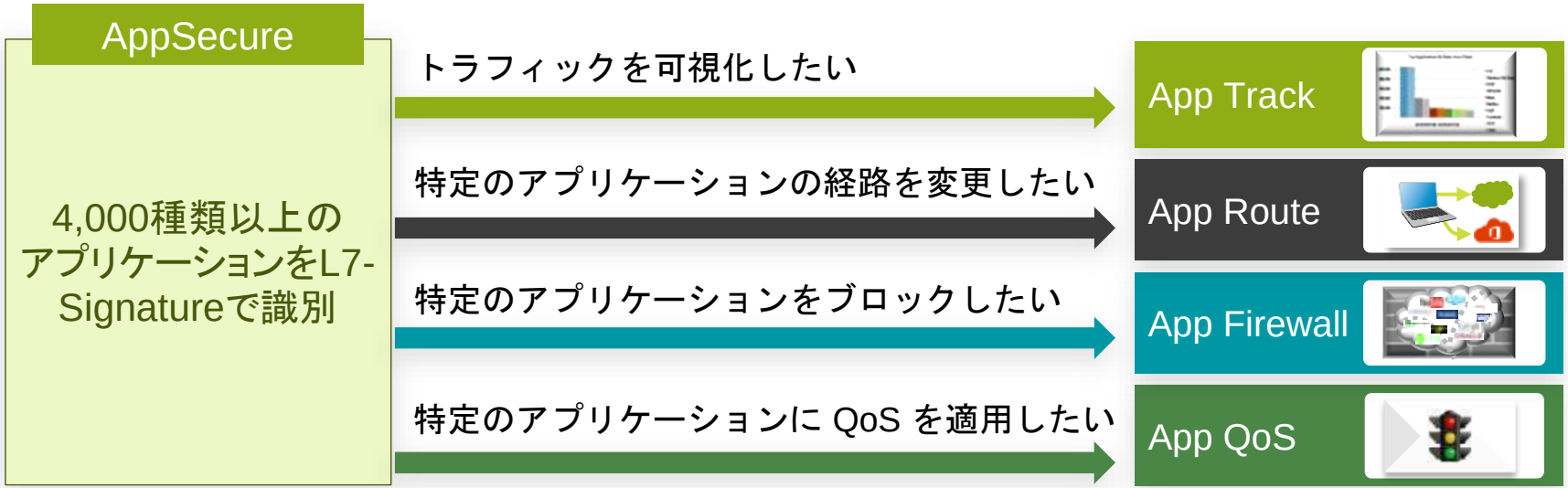
アプリケーションファイアウォールの CLI 設定について説明します。

※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

AppSecureの用途による分類

SRX は識別したアプリケーションに対して、
可視化、経路制御、ポリシー、QoS を適用させることが可能です。



Application Firewall

アプリケーションファイアウォール機能を利用するには、機器にライセンスがインストールされている必要があります。当該機能を IDP なしで使用されている場合は、application-identification (AppID シグネチャ)をダウンロードする必要があります。

下記コマンドでダウンロード

```
user@srx> request services application-identification download
```

ダウンロード状況の確認

```
user@SRX> request services application-identification download status
Downloading application package 3372 succeeded.
```

この機能を IDP とともに使用する場合、シグネチャは下記コマンドでダウンロード

```
user@srx> request security idp security-package download
```

ダウンロード状況の確認

```
user@SRX> request security idp security-package download status
Successfully retrieved from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3372(Detector=12.6.160200828, Templates=3372)
```

Application Firewall

自動更新をスケジューリングするには、次の設定を追加
例: 36 時間毎に更新

```
user@srx# set security idp security-package automatic interval 36 start-time 12-21:02:00
```

AppID シグネチャを下記コマンドでインストール

```
user@srx> request services application-identification install
```

アプリケーションファイアウォールの profile を設定し、ブロック時のメッセージを設定

```
user@srx# set security dynamic-application profile profile1 redirect-message type custom-text
content "THIS APPLICATION IS BLOCKED"
```

Application Firewall

セキュリティポリシーを設定しアプリケーションファイアウォールで YouTube をブロックし、
それ以外の通信は許可します。

例:

- 送信元ゾーン/アドレス　Trust / Any
- 宛先ゾーン/アドレス　Untrust / Any
- アプリケーション　Any
- dynamic-application　junos:YOUTUBE (reject)

```
user@srx# set security policies from-zone trust to-zone untrust policy policy1 match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy policy1 match destination-address
any
user@srx# set security policies from-zone trust to-zone untrust policy policy1 match application any
user@srx# set security policies from-zone trust to-zone untrust policy policy1 match dynamic-application
junos:YOUTUBE
user@srx# set security policies from-zone trust to-zone untrust policy policy1 then reject profile
profile1
user@srx# set security policies default-policy permit-all
```

Application Firewall

設定の確認

```
user@srx# show
security {
    dynamic-application {
        profile profile1 {
            redirect-message {
                type {
                    custom-text {
                        content "THIS APPLICATION IS BLOCKED";
                    }
                }
            }
        }
    }
```

Application Firewall

```
    policies {
        from-zone trust to-zone untrust {
            policy policy1 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                    dynamic-application junos:YOUTUBE;
                }
                then {
                    reject {
                        profile profile1;
                    }
                }
            }
        }
    }
}
```