Juniper SRX 日本語マニュアル

AppRoute（APBR） の CLI 設定

Juniper NETWORKS | Engineering Simplicity

はじめに

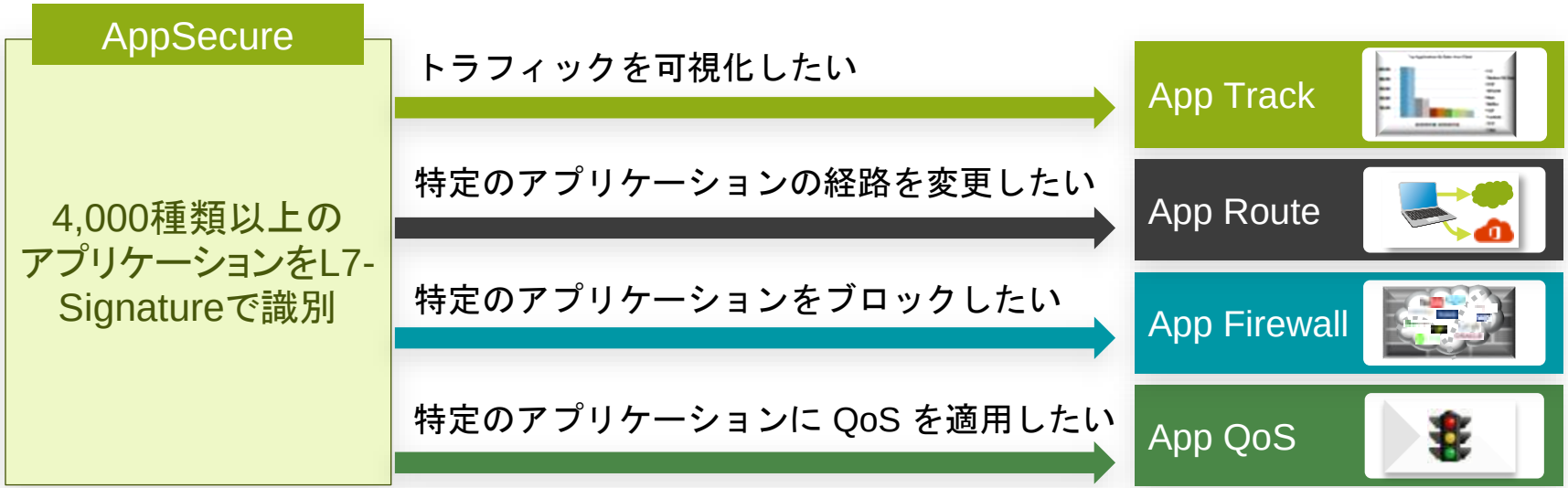
AppRoute（APBR）の CLI 設定について説明します。

※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

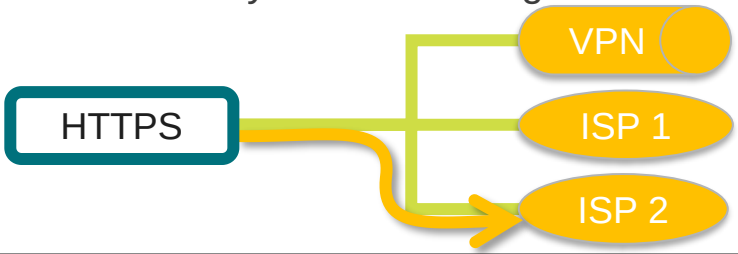
AppSecureの用途による分類

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。



AppRoute（APBR）

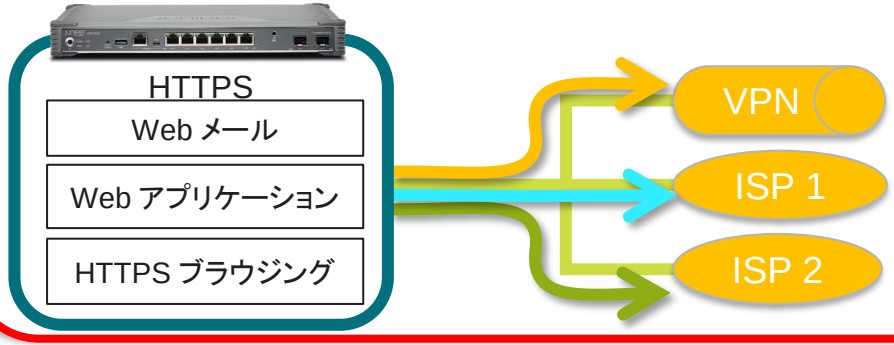
これまでの Policy-Based Routing



送信元やプロトコル/サービスによってルーティング先を指定することは可能だがアプリケーション別での制御は行えなかった

現在、多くのアプリケーションがブラウザ（HTTP / HTTPS）を介して動作するため、増加する通信量を効率的に振り分けられない

AppRoute を使用した「Advanced Policy-Based Routing」（APBR機能）



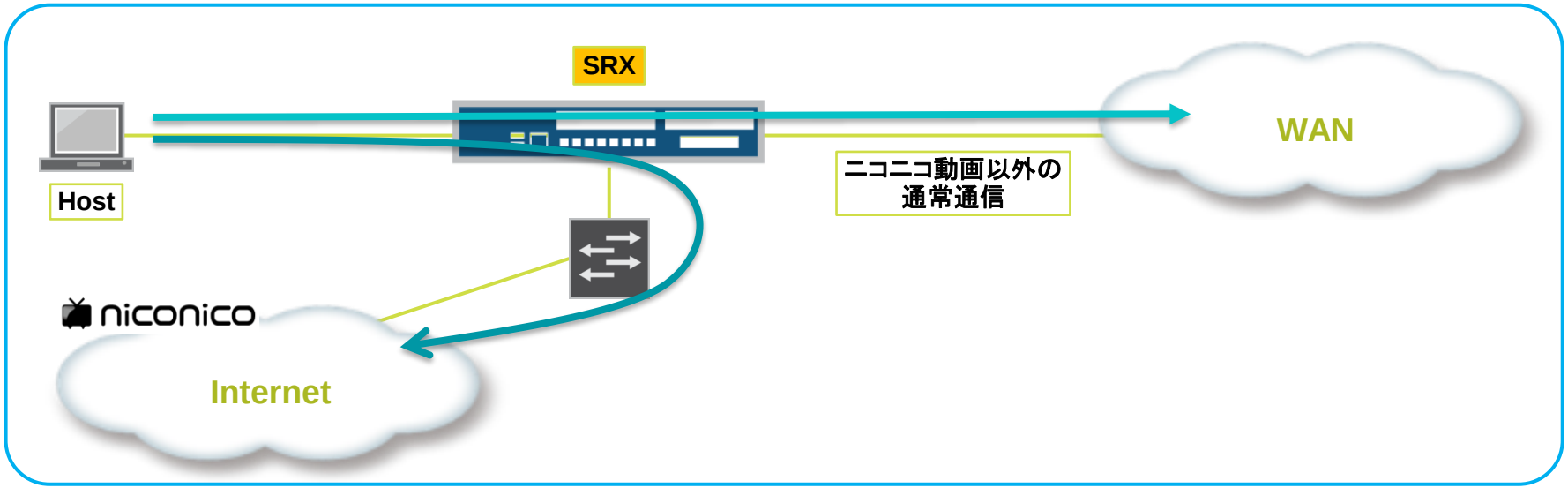
Application 識別（AppID）を利用することにより、同じウェブ通信をアプリケーション別に認識することが可能

それぞれのアプリケーションに対して、特定したルーティングを定義し、振り分けられる

AppRoute（APBR）

構成例

ニコニコ動画のみ Internet 回線側で通信を行うよう設定



AppRoute（APBR）

AppRoute（APBR）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)
```

AppRoute（APBR）

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
```

routing-instance、および routing-instance に対するルーティングを定義

```
user@SRX# set routing-instances RI-1 instance-type forwarding
user@SRX# set routing-instances RI-1 routing-options static route 0.0.0.0/0 next-hop 192.168.112.1
```

AppRoute（APBR）

APBR のプロファイルを作成し、routing-instance へ割り当て

```
user@SRX# set security advance-policy-based-routing profile PROFILE rule R1 match dynamic-application
junos:NICONICO-DOUGA
user@SRX# set security advance-policy-based-routing profile PROFILE rule R1 match dynamic-application
junos:NICONICO-DOUGA-STREAM
user@SRX# set security advance-policy-based-routing profile PROFILE rule R1 match dynamic-application
junos:NICONICO-DOUGA-UPLOAD
user@SRX# set security advance-policy-based-routing profile PROFILE rule R1 then routing-instance RI-1
```

セキュリティゾーンに作成した APBR プロファイルを割り当て

```
user@SRX# set security zones security-zone trust advance-policy-based-routing-profile PROFILE
```

デフォルトのルート情報を、routing-instance のルーティングテーブルにインポート

```
user@SRX# set routing-options interface-routes rib-group inet APBR-GROUP
user@SRX# set routing-options rib-groups APBR-GROUP import-rib RI-1.inet.0
user@SRX# set routing-options rib-groups APBR-GROUP import-rib inet.0
```

AppRoute（APBR）

設定の確認

```
user@host# show
security {
    advance-policy-based-routing {
        profile PROFILE {
            rule R1 {
                match {
                    dynamic-application [ junos:NICONICO-DOUGA junos:NICONICO-DOUGA-STREAM
junos:NICONICO-DOUGA-UPLOAD ];
                }
                then {
                    routing-instance RI-1;
                }
            }
        }
    }
    zones {
        security-zone trust {
            advance-policy-based-routing-profile {
                PROFILE;
            }
        }
```

AppRoute（APBR）

設定の確認

```
routing-options {
    interface-routes {
        rib-group inet APBR-GROUP;
    }
    rib-groups {
        APBR-GROUP {
            import-rib [ RI-1.inet.0 inet.0 ];
        }
    }
}
routing-instances {
    RI-1 {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 192.168.112.1;
            }
        }
    }
}
```

AppRoute（APBR）

ニコニコ動画のシグネチャがキャッシュされていることを確認

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: 0
IP address: 133.152.33.133                          Port: 443    Protocol: TCP
Application: SSL:NICONICO-DOUGA                     Encrypted: Yes
Classification Path: IP:TCP:SSL:NICONICO-DOUGA
```

AppRoute（APBR）

App rule hit on cache hit と Route changed on cache hits のカウンタが上昇していることを確認

```
user@host> show security advance-policy-based-routing statistics
Advance Profile Based Routing statistics:
  Sessions Processed                          1301
  App rule hit on cache hit                   37
  App rule hit on HTTP Proxy/ALG              0
  Midstream disabled rule hit on cache hit    0
  URL cat rule hit on cache hit               0
  DSCP rule hit on first packet               0
  App and DSCP hit on first packet            0
  App rule hit midstream                      10
  Midstream disabled rule hit midstream       0
  URL cat rule hit midstream                  0
  App and DSCP rule hit midstream             0
  DSCP rule hit midstream                     0
  Route changed on cache hits                 37
  Route changed on HTTP Proxy/ALG             0
  Route changed midstream                     10
  Zone mismatch                               0
  Drop on zone mismatch                       0
  Next hop not found                          0
  Application services bypass                 0
```