Juniper SRX 日本語マニュアル

AppRoute (APBR) の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

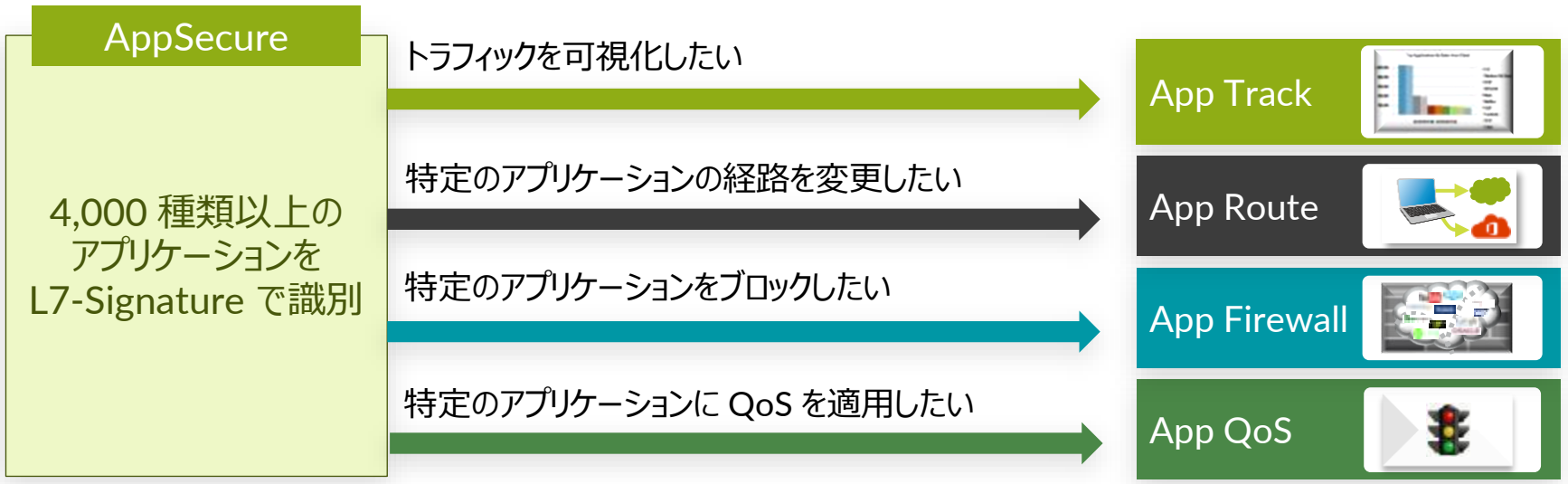
- 本マニュアルは、AppRoute (APBR) の CLI 設定について説明します
- 手順内容は SRX300 、Junos 21.2R3-S2 にて確認を実施しております
- 実際の設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.juniper.net/documentation/

- 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

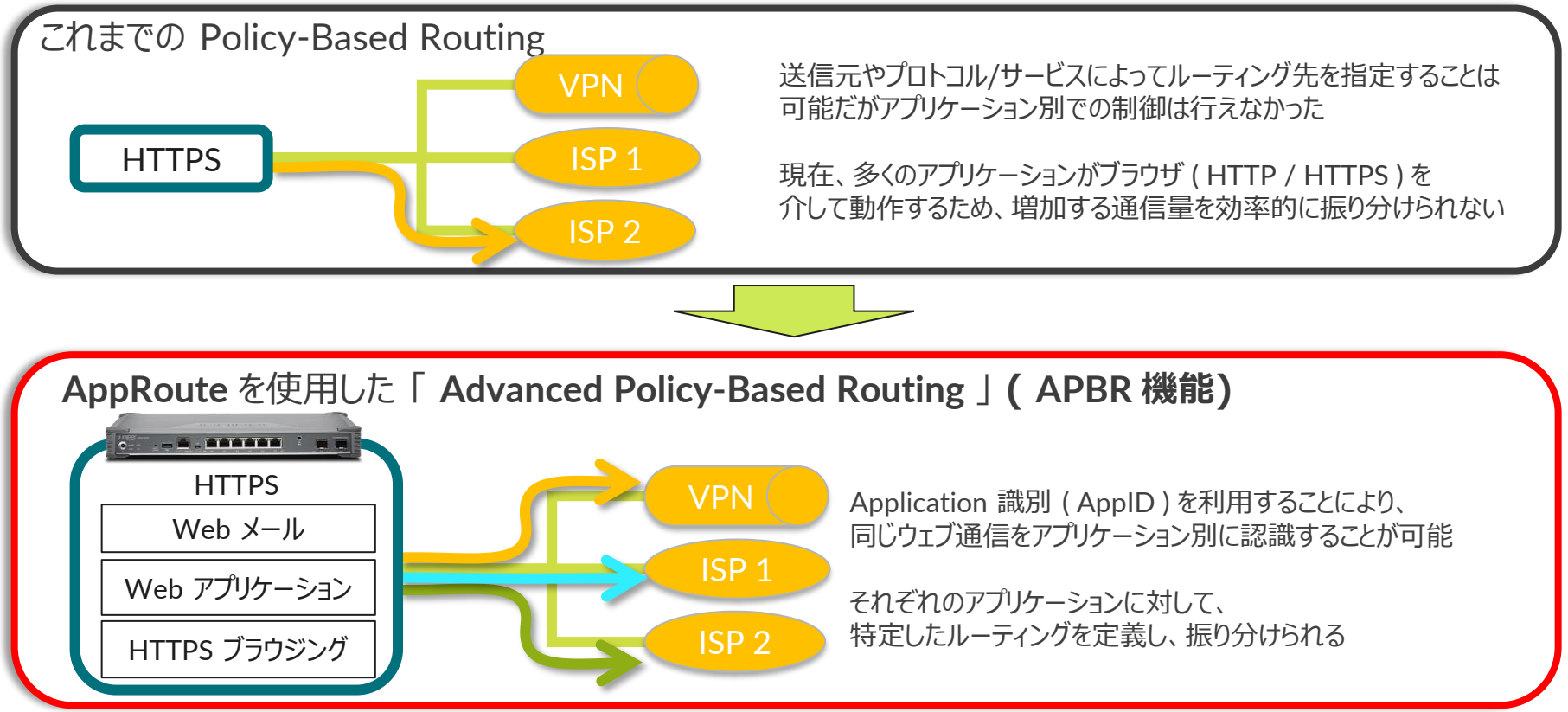
2022 年 8 月

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



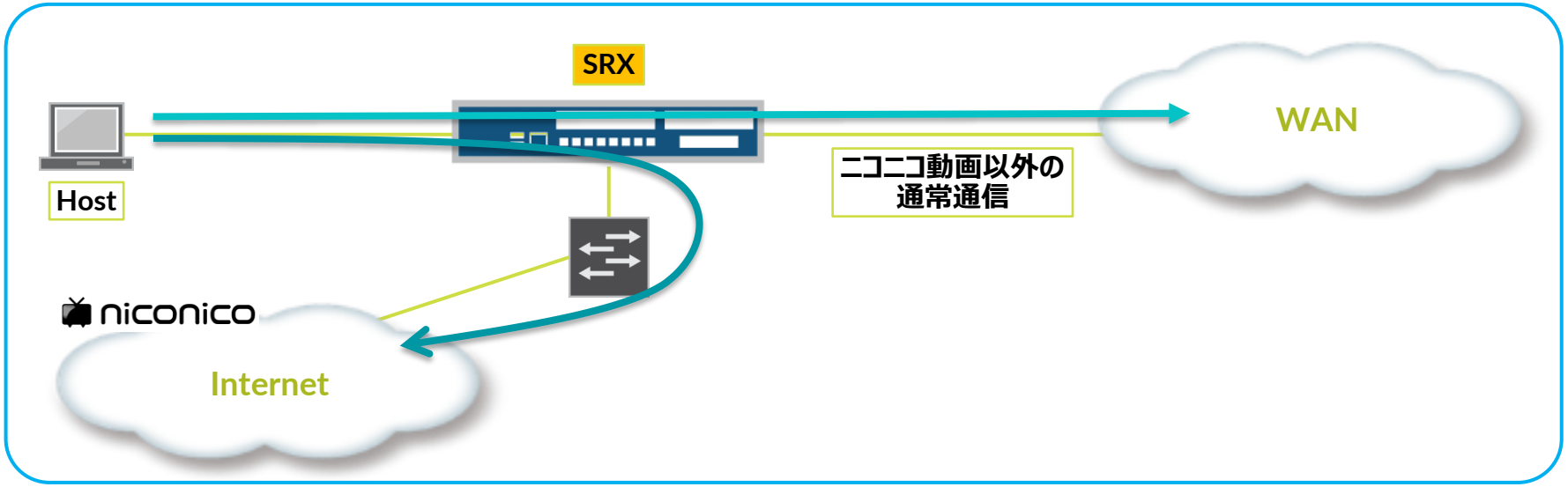
AppRoute (APBR)



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

1. 下記コマンドでダウンロードします

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

2. ダウンロード状況を確認します

```
user@srx> request services application-identification download status
Downloading application package 3505 succeeded.
```

3. 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します

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

4. ダウンロード状況を確認します

```
user@srx> request security idp security-package download status
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3505(Thu Jun 30 14:30:52 2022 UTC, Detector=12.6.160200828)
```

AppRoute (APBR)

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

```
user@srx# set security idp security-package automatic interval 36 start-time 2022-05-15.13:00:00
```

6. AppID シグネチャを下記コマンドでインストールします

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

7. インストール状況を確認します

```
user@srx> request services application-identification install status
Installed
        Application package (3505) and Protocol bundle successfully

user@srx> show services application-identification version
  Application package version: 3505
```

AppRoute (APBR)

8. routing-instance および routing-instance に対するルーティングを定義します

```
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 192.168.91.99
```

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

```
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
```

10. APBR ポリシーを作成し、プロファイルを割り当てます

```
user@srx# set security advance-policy-based-routing from-zone trust policy APBR-POLICY match source-address any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR-POLICY match destination-address any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR-POLICY match application any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR-POLICY then application-services advance-policy-
based-routing-profile PROFILE
```

11. 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します

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

AppRoute (APBR)

設定の確認 1 (security idp)

```
user@srx# show
security {
    idp {
        security-package {
            automatic {
                start-time "2022-5-15.13:00:00 +0000";
                interval 36;
            }
        }
    }
```

AppRoute (APBR)

設定の確認 2 (security advance-policy-based-routing)

```
    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;
                }
            }
        }
        from-zone trust {
            policy APBR-POLICY {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    application-services {
                        advance-policy-based-routing-profile PROFILE;
                    }
                }
            }
        }
    }
}
```

AppRoute (APBR)

設定の確認 3 (routing-instances 、routing-options)

```
routing-instances {
    RI-1 {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 192.168.91.99;
            }
        }
    }
}
routing-options {
    interface-routes {
        rib-group inet APBR-GROUP;
    }
    rib-groups {
        APBR-GROUP {
            import-rib [ inet.0 RI-1.inet.0 ];
        }
    }
}
```

AppRoute (APBR)

動作の確認 1
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します

```
user@srx> 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
  (略)
```

AppRoute (APBR)

動作の確認 2
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します

```
user@srx> show security advance-policy-based-routing statistics
Advance Profile Based Routing statistics:
  Sessions Processed                          237
  App rule hit on cache hit                   52
  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                      19
  Default rule match                          0
  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                 52
  Route changed on HTTP Proxy/ALG             0
  Route changed midstream                     19
  Default rule applied                        0
  Zone mismatch                               0
  Drop on zone mismatch                       0
  Next hop not found                          0
  Application services bypass                 0
```


Thank you
JUNIPER NETWORKS
Driven by Experience™