

Juniper SRX 日本語マニュアル

Application QoS の CLI 設定

JUNIPER
NETWORKS

Driven by
Experience™

はじめに

- ◆ 本マニュアルは、Application QoS 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

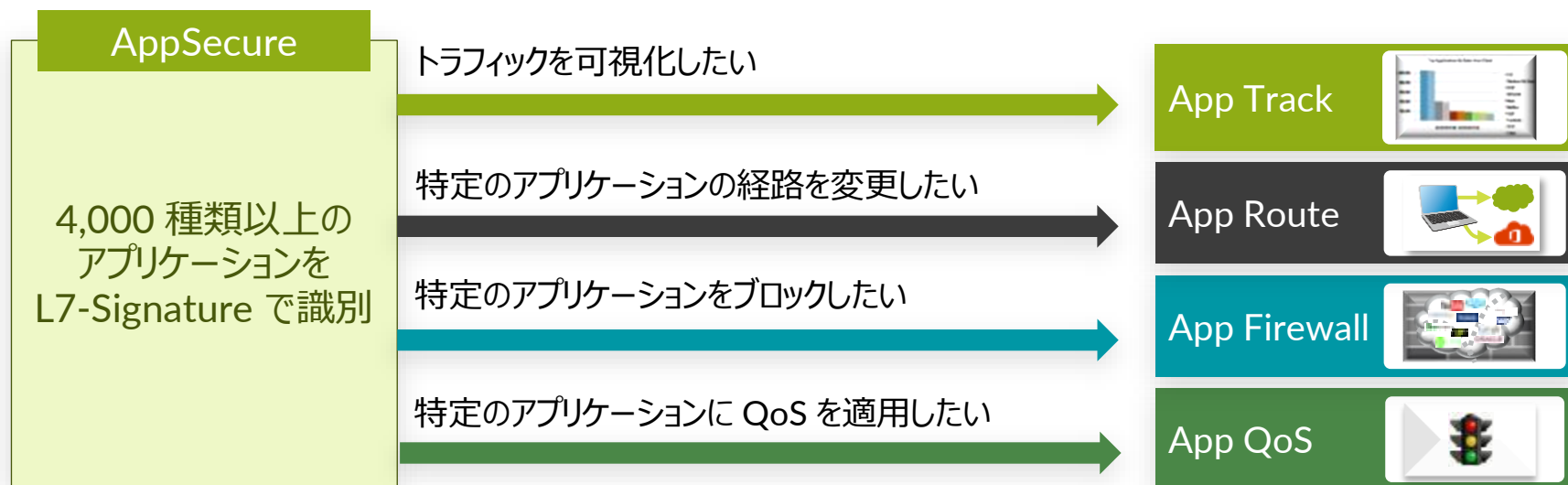
<https://www.juniper.net/documentation/>

- ◆ 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>

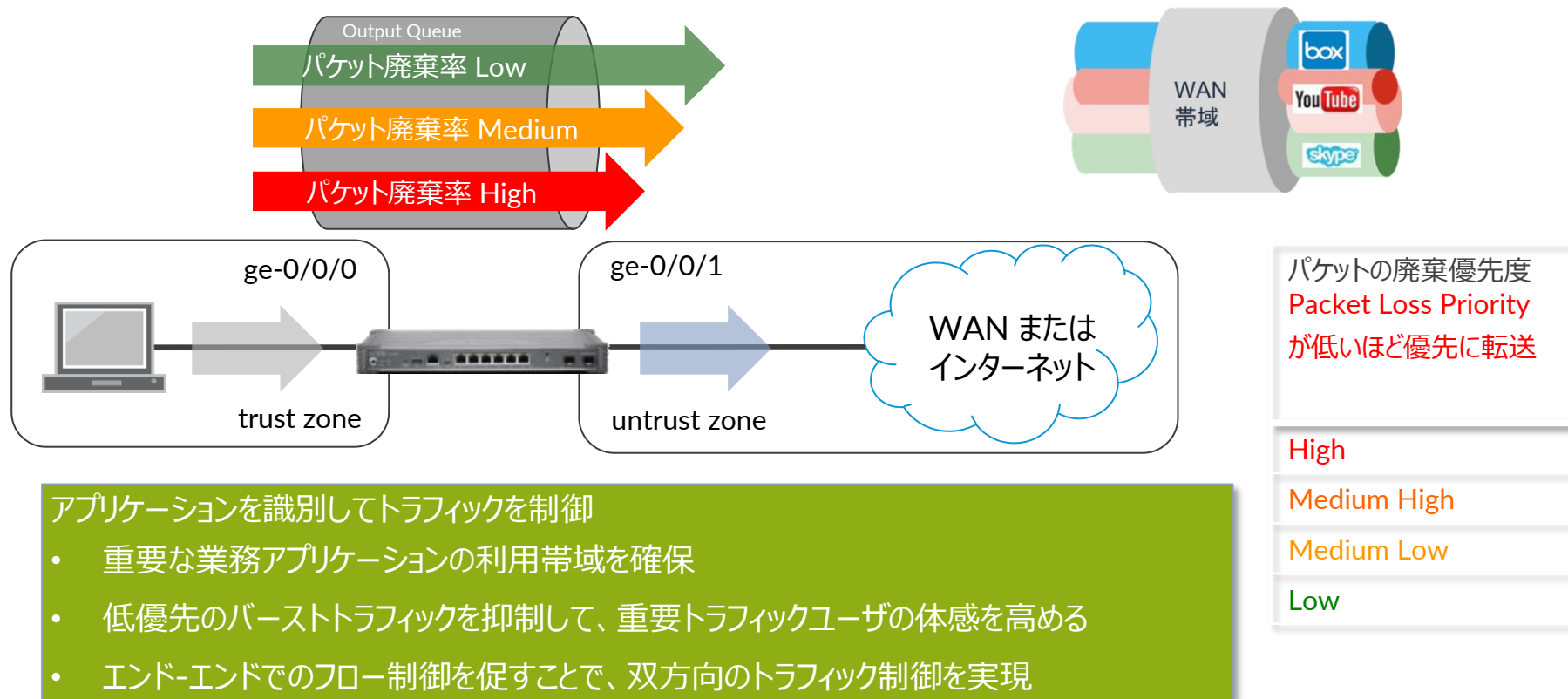
2022 年 8 月

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



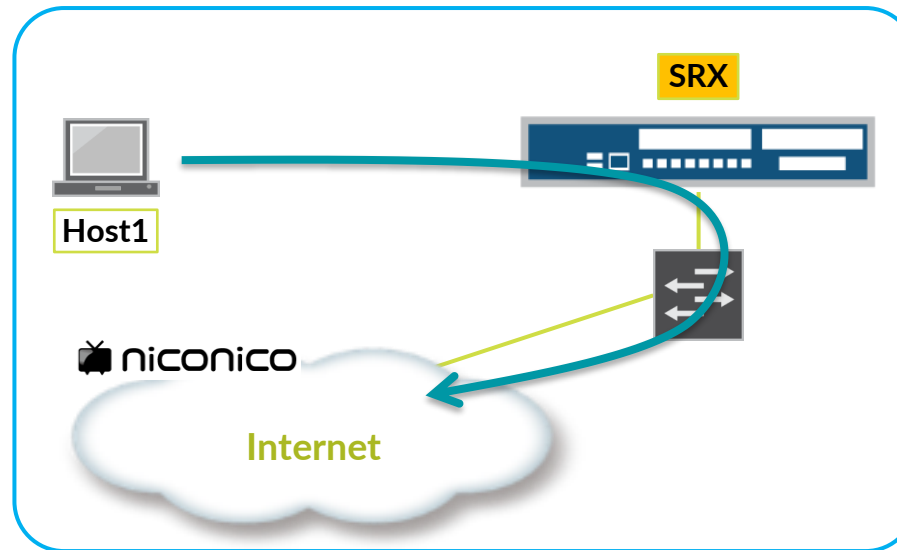
Application QoS



Application QoS

構成例

ニコニコ動画の通信へ Application QoS による帯域幅の閾値を適用
(Bandwidth Limit : 20,000 kbps)



Application QoS

Application QoS 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)
```

Application QoS

5. 自動更新をスケジュール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
```

Application QoS

8. rate-limiter を作成し bandwidth limit (kbps) を定義します

```
user@srx# set class-of-service application-traffic-control rate-limiters TEST-R1 bandwidth-limit 20000
```

9. rule-set を作成し、対象のアプリケーションへ rate-limiter を割り当てます

```
user@srx# set class-of-service application-traffic-control rule-sets R-NICONICO rule 0 match application junos:NICONICO-DOUGA
user@srx# set class-of-service application-traffic-control rule-sets R-NICONICO rule 0 match application junos:NICONICO-DOUGA-STREAM
user@srx# set class-of-service application-traffic-control rule-sets R-NICONICO rule 0 match application junos:NICONICO-DOUGA-UPLOAD
user@srx# set class-of-service application-traffic-control rule-sets R-NICONICO rule 0 then rate-limit server-to-client TEST-R1
```

10. セキュリティポリシーに rule-set を割り当てます ※セキュリティポリシーについては事前に作成

```
user@srx# set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit application-services application-traffic-control rule-set R-NICONICO
```


Application QoS

設定の確認 1

```
user@srx# show
security {
  idp {
    security-package {
      automatic {
        start-time "2022-5-15.13:00:00 +0000";
        interval 36;
      }
    }
  }
}
policies {
  from-zone trust to-zone untrust {
    policy t2u {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            application-traffic-control {
              rule-set R-NICONICO;
            }
          }
        }
      }
    }
  }
}
}
```

Application QoS

設定の確認 2

```
class-of-service {
  application-traffic-control {
    rate-limiters TEST-R1 {
      bandwidth-limit 20000;
    }
    rule-sets R-NICONICO {
      rule 0 {
        match {
          application [ junos:NICONICO-DOUGA junos:NICONICO-DOUGA-STREAM junos:NICONICO-DOUGA-UPLOAD ];
        }
        then {
          rate-limit {
            server-to-client TEST-R1;
          }
        }
      }
    }
  }
}
```

Application QoS

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)
```

Application QoS

動作の確認 2

class-of-service の application-traffic-control にて rate limited のカウンタが上昇していることを確認します

```
user@srx> show class-of-service application-traffic-control statistics rate-limiter
Logical System: root-logical-system

pic: 0/0
Ruleset           Application           Client-to-server    Rate (kbps)    Server-to-client  Rate (kbps)
R-NICONICO        junos:NICONICO-DOUGA -                    0              TEST-R1         20000

user@srx> show class-of-service application-traffic-control statistics rule
Logical System: root-logical-system

pic: 0/0
Ruleset           Rule                Hits
R-NICONICO        0                   69

user@srx> show class-of-service application-traffic-control counter
Logical System: root-logical-system

pic: 0/0
Counter type           Value
Sessions processed     465
Sessions marked        0
Sessions honored       0
Sessions rate limited  69
Client-to-server flows rate limited  0
Server-to-client flows rate limited  69
Session default ruleset hit  0
Session ignored no default ruleset  0
```



Thank you

JUNIPER
NETWORKS®

Driven by
Experience™