Juniper SRX 日本語マニュアル

Application Firewall の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

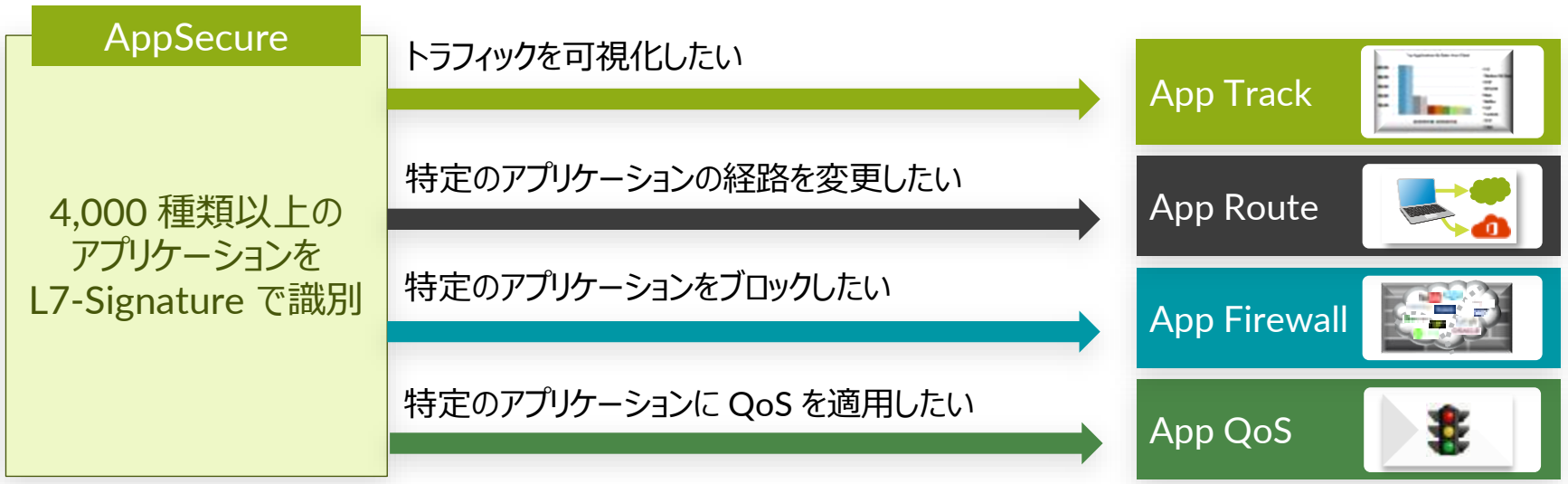
- 本マニュアルは、Application Firewall の CLI 設定について説明します
- 手順内容は SRX300 、Junos 21.2R3-S2 にて確認を実施しております
- 実際の設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.juniper.net/documentation/

- 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 Firewall

Application Firewall 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 Firewall

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
```

8. 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します

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

Application Firewall

9. 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 Yahoo のアプリケーション通信をブロックし、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:YAHOO (reject)

```
user@srx# set security policies from-zone trust to-zone untrust policy T2U match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy T2U match destination-address any
user@srx# set security policies from-zone trust to-zone untrust policy T2U match application any
user@srx# set security policies from-zone trust to-zone untrust policy T2U match dynamic-application junos:YAHOO
user@srx# set security policies from-zone trust to-zone untrust policy T2U then reject profile PROFILE
user@srx# set security policies default-policy permit-all
```

Application Firewall

設定の確認 1

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

Application Firewall

設定の確認 2

```
    policies {
        from-zone trust to-zone untrust {
            policy T2U {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                    dynamic-application junos:YAHOO;
                }
                then {
                    reject {
                        profile PROFILE;
                    }
                }
            }
        }
        default-policy {
            permit-all;
        }
    }
}
```

Application Firewall

動作の確認
セキュリティポリシーにてトラフィックログを有効に設定することにより Application Firewall 機能によってブロックされた通信が確認されます

```
user@srx> show log traffic-logging
May 15 18:45:32  srx RT_FLOW: APPTRACK_SESSION_VOL_UPDATE: AppTrack volume update: 10.91.0.99/60146->172.217.161.35/443 junos-https
SSL GCP 10.91.0.99/60146->172.217.161.35/443 N/A N/A 6 default-policy-logical-system-00 trust untrust 5857 15(2486) 15(6653) 66 N/A
N/A No ge-0/0/0.0 Web miscellaneous N/A N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60164->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5884 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60165->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5885 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60166->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5887 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60167->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5888 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60169->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5890 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:32  srx RT_FLOW: RT_FLOW_SESSION_DENY: session denied 10.91.0.99/60170->183.79.219.252/443 0x0 junos-https 6(0) T2U
trust untrust SSL YAHOO N/A(N/A) ge-0/0/1.0 No Rejected by policy 5891 Web miscellaneous 2 N/A N/A N/A
May 15 18:45:33  srx RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack session closed Closed by junos-dynapp: 10.91.0.99/60164-
>183.79.219.252/443 junos-https SSL YAHOO 10.91.0.99/60164->183.79.219.252/443 N/A N/A 6 T2U trust untrust 5884 3(649) 9(8639) 1 N/A
N/A No N/A N/A default ge-0/0/0.0  0 0 Web miscellaneous N/A N/A N/A N/A N/A N/A
May 15 18:45:33  srx RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack session closed Closed by junos-dynapp: 10.91.0.99/60165-
>183.79.219.252/443 junos-https SSL YAHOO 10.91.0.99/60165->183.79.219.252/443 N/A N/A 6 T2U trust untrust 5885 3(649) 7(7074) 1 N/A
N/A No N/A N/A default ge-0/0/0.0  0 0 Web miscellaneous N/A N/A N/A N/A N/A N/A
May 15 18:45:33  srx RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack session closed Closed by junos-dynapp: 10.91.0.99/60166-
>183.79.219.252/443 junos-https SSL YAHOO 10.91.0.99/60166->183.79.219.252/443 N/A N/A 6 T2U trust untrust 5887 3(649) 9(8639) 1 N/A
N/A No N/A N/A default ge-0/0/0.0  0 0 Web miscellaneous N/A N/A N/A N/A N/A N/A
May 15 18:45:33  srx RT_FLOW: APPTRACK_SESSION_CLOSE: AppTrack session closed Closed by junos-dynapp: 10.91.0.99/60167-
>183.79.219.252/443 junos-https SSL YAHOO 10.91.0.99/60167->183.79.219.252/443 N/A N/A 6 T2U trust untrust 5888 3(649) 9(8639) 1 N/A
N/A No N/A N/A default ge-0/0/0.0  0 0 Web miscellaneous N/A N/A N/A N/A N/A N/A
```


Thank you
JUNIPER NETWORKS
Driven by Experience™