Juniper SRX 日本語マニュアル

44. Application Tracking の CLI 設定

Juniper NETWORKS | Engineering Simplicity

はじめに

Application Tracking の CLI 設定について説明します。

※手順内容は「SRX300」、JUNOS「15.1X49-D140」にて確認を実施しております。

2018年8月

Application Tracking

以下の設定を行う場合のコマンド例となります。

Trust ゾーンで受信したトラフィックを可視化
ログを Syslog サーバ（192.168.1.2）へ転送

Application Tracking

① アプリケーショントラッキング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。
ライセンスを購入していない場合は、試験用にトライアルライセンスがあり、以下の方法でインターネット経由でのダウンロードが可能です。

```
user@SRX> request system license update trial
```

ライセンスの確認

```
user@SRX> show system license
License usage:
                Licenses    Licenses      Licenses    Expiry
Feature name      used      installed      needed
idp-sig             1           1             0         2012-02-08 00:00:00 UTC
appid-sig           0           1             0         2012-02-08 00:00:00 UTC
```

Application Tracking

② IDP なしで使用されている場合は、application-identification をダウンロードする必要があります。
これを行うには、次のコマンドを使用します。

```
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 2157 succeed
```

この機能を IDP とともに使用する場合、シグネチャは次の方法でダウンロードできます。

```
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
Done;Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:2102(Wed Jan 21 12:05:38 2011, Detector=11.6.140110920)
```

Application Tracking

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 12-21:02:00
```

AppID シグネチャを次のコマンドでインストールします。

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

Application Tracking

③ Syslog（Stream Mode）の設定

```
user@SRX# set security log mode stream
user@SRX# set security log format sd-syslog
user@SRX# set security log source-address 192.168.1.1
user@SRX# set security log stream app-track-logs host 192.168.1.2
```

④ トラフィックを受信するゾーンでアプリケーショントラッキングを有効化

```
user@SRX#  set security zones security-zone trust application-tracking
```

Application Tracking

設定の確認

```
user@host# show
security {
    log {
        mode stream;
        format sd-syslog;
        source-address 192.168.1.1;
        stream app-track-logs {
            host {
                192.168.1.2;
            }
        }
    }
    zones {
        security-zone trust {
            application-tracking;
        }
    }
}
```

Application Tracking

Application の統計確認

```
user@SRX> show services application-identification statistics applications
Last Reset: 2017-05-25 02:07:40 UTC
                     Application           Sessions              Bytes    Encrypted
                           ADOBE                  1               70577           No
     ANDROID-MARKETPLACE-DOWNLOAD                  3               19914           No
                             DNS                 75               22894           No
                          GOOGLE                 22              347154           No
            GOOGLE-ADSERVICES-SSL                28              171788           No
                   GOOGLE-STATIC                 29              105171           No
                  GOOGLE-WEBCHAT                  1                8262           No
                       MICROSOFT                 10              101416           No
    OFFICE365-CREATE-CONVERSATION                  2               21140           No
                         YOUTUBE                 60             9911994           No
```