

# Juniper SRX 日本語マニュアル

## 14. Application Firewall の CLI 設定

# はじめに

---

アプリケーションファイアウォールの CLI 設定方法を説明します。

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

2018年8月

# Application Firewall

- ① アプリケーションファイアウォール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 Firewall

- ② アプリケーションファイアウォール機能が 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、シグネチャは次のようにして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 Firewall

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
```

③ アプリケーションファイアウォールの rule-sets を設定します。

例: Facebook のチャットはブロック、その他は許可

```
user@srx# set security application-firewall rule-sets test rule 1 match dynamic-application
junos:FACEBOOK-CHAT
user@srx# set security application-firewall rule-sets test rule 1 then deny
user@srx# set security application-firewall rule-sets test default-rule permit
```

# Application Firewall

- ④ 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の rule-sets を入れます。

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

```
user@srx# set security policies from-zone trust to-zone untrust policy pol match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy pol match destination-address any
user@srx# set security policies from-zone trust to-zone untrust policy pol match application any
user@srx# set security policies from-zone trust to-zone untrust policy pol then permit application-
services application-firewall rule-set test
```

# Application Firewall

## 設定の確認①

```
user@srx# show
security {
    application-firewall {
        rule-sets test {
            rule 1 {
                match {
                    dynamic-application junos:FACEBOOK-CHAT;
                }
                then {
                    deny;
                }
            }
            default-rule {
                permit;
            }
        }
    }
}
```

# Application Firewall

## 設定の確認②

```
polices {
    from-zone trust to-zone untrust {
        policy pol {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    application-services {
                        application-firewall {
                            rule-set test;
                        }
                    }
                }
            }
        }
    }
}
```