

Juniper SRX 日本語マニュアル

11. IDP の CLI 設定

JUNIPER
NETWORKS

Engineering
Simplicity

はじめに

IDP 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

IDP

IDP シグネチャアップデートは、ライセンスが必要なサブスクリプションサービスです。シグネチャをダウンロードして使用するには、IDP ライセンスをインストールする必要があります。カスタムシグネチャのみを使用している場合は、IDP ライセンスは必要ありません。

IDP

IDP ライセンスのインストール後、次の手順を実行して IDP シグネチャデータベースをダウンロードし、インストールします。

- ① デバイスがインターネット接続が行える構成であるか確認
- ② シグネチャデータベースサーバへアクセスし、シグネチャバージョンを確認
この例でのバージョンは 2894

```
root> request security idp security-package download check-server
Successfully retrieved from(https://signatures.juniper.net/cgi-bin/index.cgi) .
Version info:2894 (Detector=12.6.160161014, Templates=2894)
```

- ③ シグネチャをダウンロード

```
root> request security idp security-package download
```

IDP

④ ダウンロードの進行状況を確認

```
root> request security idp security-package download status
In progress:SignatureUpdate_tmp.xml.gz 100 % 3822478 Bytes/ 3822478 Bytes
```

Successfully downloaded と表示されたら次の手順に進みます。

```
root> request security idp security-package download status
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:2894(Tue May 16 11:54:08 2017 UTC, Detector=12.6.160161014)
```

⑤ 次のコマンドを実行してシグネチャ DB をインストール

```
root> request security idp security-package install
```

既存の実行中のポリシーが存在する場合、実行中の既存のポリシーを再コンパイルし、コンパイルされたポリシーをデータプレーンにプッシュします。

したがって、プラットフォームとポリシーのサイズによっては、インストールに時間がかかることがあります。

IDP

⑥ インストール進行状況の確認

```
root> request security idp security-package install status
Done;Attack DB update : successful - [UpdateNumber=2894,ExportDate=Tue May 16 11:54:08 2017
UTC,Detector=12.6.160161014]
Updating control-plane with new detector : successful
Updating data-plane with new attack or detector : not performed
due to no active policy configured.
```

UpdateNumber フィールドには、更新されたバージョン、シグネチャ DB がリリースされた日付が表示されます。

⑦ インストールされているシグネチャ DB のバージョンを確認

```
root> show security idp security-package-version
Attack database version:2894(Tue May 16 11:54:08 2017 UTC)
Detector version :12.6.160161014
Policy template version :N/A
```

IDP

定義済みの IDP ポリシーテンプレートを提供しています。
まずは、Recommended という名前の定義済みポリシーを使用することをお勧めします。

① 最新の IDP ポリシーテンプレートをダウンロード

```
root> request security idp security-package download policy-templates
```

② ダウンロードの進行状況を確認

```
root> request security idp security-package download status  
In progress: Downloading ...
```

Successfully downloaded と表示されたら次の手順に進みます。

```
root> request security idp security-package download status  
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).  
Version info:2894
```

③ 次のコマンドを実行してポリシーテンプレートをインストール

```
root> request security idp security-package install policy-templates
```

IDP

④ インストール進行状況を確認

```
root> request security idp security-package install status
Done;policy-templates has been successfully updated into internal repository
(=>/var/db/scripts/commit/templates.xsl)!
```

Done と表示されたら次の手順に進みます。

⑤ ポリシーテンプレートを展開

```
root# set system scripts commit file templates.xsl
root# commit
```

⑥ Recommended をアクティブなポリシーとして設定

```
root# set security idp active-policy Recommended
root# commit
```

⑦ アクティブな IDP ポリシーが Recommended であることを確認

```
root> show security idp status
Session Statistics:
[ICMP: 0] [TCP: 0] [UDP: 0] [Other: 0]
Policy Name : Recommended
Running Detector Version : 12.6.160161014
```


IDP

⑧ セキュリティポリシーで IDP ポリシーを有効化

この例は Trust ゾーンから Trust ゾーンへのすべてのトラフィックに対して IDP のチェックを行う設定です。

```
root# set security policies from-zone trust to-zone trust policy idp-app-policy-1 match
source-address any destination-address any application any
root# set security policies from-zone trust to-zone trust policy idp-app-policy-1 then
permit application-services idp
```

IDP

設定の確認

```
root# show
security {
  policies {
    from-zone trust to-zone trust {
      policy idp-app-policy-1 {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit {
            application-services {
              idp;
            }
          }
        }
      }
    }
  }
}
```