Juniper SRX 日本語マニュアル

IDP の CLI 設定

はじめに

IDP の CLI 設定方法を説明します。

※手順内容は「SRX300」、JUNOS「19.4R3-S1」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/

2021年7月

© 2021 Juniper Networks

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。

© 2021 Juniper Networks

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。

- 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
- 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 3370

```
root> request security idp security-package download check-server
Successfully retrieved from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3370(Detector=12.6.160200828, Templates=3370)
```

- シグネチャをダウンロード

```
root> request security idp security-package download
Will be processed in async mode. Check the status using the status checking CLI
```

© 2021 Juniper Networks

IDP

- 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 % 5501078 Bytes/ 5501078 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:3370(Thu Apr  1 14:39:05 2021 UTC, Detector=12.6.160200828)
```

- 次のコマンドを実行してシグネチャデータベースをインストール

```
root> request security idp security-package install
Will be processed in async mode. Check the status using the status checking CLI
```

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。

© 2021 Juniper Networks

IDP

- 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=3370,ExportDate=Thu Apr  1 14:39:05 2021
UTC,Detector=12.6.160200828]
     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。

- インストールされているシグネチャデータベースのバージョンを確認

```
root> show security idp security-package-version
  Attack database version:3370(Thu Apr  1 14:39:05 2021 UTC)
  Detector version :12.6.160200828
  Policy template version :N/A
```

© 2021 Juniper Networks

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。

- 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
Will be processed in async mode. Check the status using the status checking CLI
```

- 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 % 5501078 Bytes/ 5501078 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:3370
```

© 2021 Juniper Networks

IDP

- 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
Will be processed in async mode. Check the status using the status checking CLI
```

- 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/run/scripts/commit/templates.xsl)!
```

Done と表示されたら次の手順に進みます。

© 2021 Juniper Networks

IDP

- ポリシーテンプレートを展開

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

- ポリシーテンプレート（Recommended）を定義し、デフォルトポリシーとして設定

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

- デフォルトポリシーが Recommended であることを確認

```
Root# show security idp default-policy
default-policy Recommended;
```

- セキュリティポリシーで IDP ポリシーを有効化する方法

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
```

© 2021 Juniper Networks

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;
                        }
                    }
                }
            }
        }
    }
}
```

© 2021 Juniper Networks