Juniper SRX 日本語マニュアル

IDP の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、IDP 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

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

1. インストールされているライセンスを確認します

```
user@srx> show system license
License usage:
                        Licenses     Licenses        Licenses    Expiry
  Feature name              used       installed        needed
  dynamic-vpn                  0               2             0      permanent

Licenses installed: none
```

2. ライセンスをインストールします
   ※ライセンスキーをコピー＆ペースト (最後に Ctrl + D を入力)

```
user@srx> request system license add terminal
```

IDP

3. インストールしたライセンスを確認します (IDP Signature)

```
user@srx> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  dynamic-vpn                           0            2           0    permanent
  idp-sig                               1            1           0    2022-07-31 09:00:00 JST

Licenses installed:
  License identifier: JUNOSXXXXXXXX
  License version: 4
  Valid for device: XXXXXXXXXXXX
  Customer ID: Juniper Internal
  Features:
    idp-sig          - IDP Signature
      date-based, 2022-05-31 09:00:00 JST - 2022-07-31 09:00:00 JST
```

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

4. 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します

5. 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します
   ※この例でのバージョンは 3505

```
user@srx> request security idp security-package download check-server
Successfully retrieved from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3505(Detector=12.6.160200828, Templates=3505)
```

6. シグネチャをダウンロードします

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

7. ダウンロードの進行状況を確認します

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

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

```
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)
```

IDP

9. シグネチャデータベースをインストールします

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

10. 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

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

11. インストール進行状況を確認します

```
user@srx> request security idp security-package install status
Done;Attack DB update : successful - [UpdateNumber=3505,ExportDate=Thu Jun 30 14:30:52 2022 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

12. 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します

```
user@srx> show security idp security-package-version
  Attack database version:3505(Thu Jun 30 14:30:52 2022 UTC)
  Detector version :12.6.160200828
  Policy template version :3495
```

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
定義済みポリシー Recommended (推奨)を使用することをお勧めします

13. 最新の IDP ポリシーテンプレートをダウンロードします

```
user@srx> request security idp security-package download policy-templates
Will be processed in async mode. Check the status using the status checking CLI
```

14. ダウンロードの進行状況を確認します

```
user@srx> request security idp security-package download status
In progress:SignatureUpdate_tmp.xml.gz                          100 % 5748254 Bytes/ 5748254 Bytes
```

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

```
user@srx> request security idp security-package download status
Done;Successfully downloaded from(https://signatures.juniper.net/cgi-bin/index.cgi).
Version info:3505
```

16. 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します

```
user@srx> request security idp security-package install policy-templates
Will be processed in async mode. Check the status using the status checking CLI
```

17. インストール進行状況を確認します

```
user@srx> 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

IDP

18. ポリシーテンプレートを展開します

```
user@srx# set system scripts commit file templates.xsl
user@srx# commit
```

19. 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します

```
user@srx# set security idp default-policy Recommended
user@srx# commit
```

20. デフォルトポリシーが Recommended であることを確認します

```
user@srx# show security idp default-policy
default-policy Recommended;
```

21. セキュリティポリシーで IDP ポリシーを有効化します
    この例は Trust ゾーンから Untrust 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

```
user@srx# set security policies from-zone trust to-zone trust policy T2U match source-address any
user@srx# set security policies from-zone trust to-zone trust policy T2U match destination-address any
user@srx# set security policies from-zone trust to-zone trust policy T2U match application any
user@srx# set security policies from-zone trust to-zone trust policy T2U then permit application-services idp
```

IDP

設定の確認 1

```
user@srx# show
system {
    scripts {
        commit {
            file templates.xsl;
        }
    }
}
security {
    idp {
  (略)

        idp-policy Recommended {
            /* This legacy template policy covers most current vulnerabilities.  This template is supported on all platforms,
including Branch devices with 1G of memory. */
            rulebase-ips {
                rule TCP/IP {
  (略)

        default-policy Recommended;
        security-package {
            automatic {
                start-time "2022-5-15.22:00:00 +0900";
                interval 36;
            }
        }
    }
```

IDP

設定の確認 2

```
    policies {
        from-zone trust to-zone untrust {
            policy T2U {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            idp;
                        }
                    }
                }
            }
        }
    }
}
```


Thank you
JUNIPER NETWORKS
Driven by Experience™