Juniper SRX 日本語マニュアル

Antivirus の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、アンチウイルスの 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

Antivirus

デフォルトの UTM ポリシー (junos-av-policy) を使用してアンチウィルス機能を設定する方法について説明します

- サポートされているプロトコル
  HTTP 、HTTPS (SSL Forward Proxy) 、FTP 、SMTP 、IMAP 、POP3

※ 19.4R1 以降では以下のプロトコルもサポート
  パッシブモード FTPS 、SMTPS 、IMAPS 、POP3S

- サポートされているファイル形式
  exe 、zip 、rar 、swf (shockwave flash) 、pdf 、ole2 (doc 、xls)

Antivirus

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
```

Antivirus

3. インストールしたライセンスを確認します (Anti Virus with Sophos Engine)

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

Licenses installed:
  License identifier: JUNOSXXXXXXXX
  License version: 4
  Valid for device: XXXXXXXXXXXX
  Customer ID: Juniper Internal
  Features:
    av_key_sophos_engine - Anti Virus with Sophos Engine
      date-based, 2022-05-31 00:00:00 UTC - 2022-07-31 00:00:00 UTC
```

Antivirus

4. anti-virus タイプを設定します

```
user@srx# set security utm default-configuration anti-virus type sophos-engine
```

5. UTM Policy を適用します

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

Antivirus

設定の確認

```
user@srx# show
security {
    utm {
        default-configuration {
            anti-virus {
                type sophos-engine;
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy T2U {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            utm-policy junos-av-policy;
                        }
                    }
                }
            }
        }
    }
}
```

Antivirus

ステータスの確認

```
user@srx> show security utm anti-virus status
 UTM anti-virus status:

    Anti-virus key expire date: 2022-07-31 09:02:33
    Update server: https://update.juniper-updates.net/SAV/
           Interval: 1440 minutes
           Pattern update status: next update in 1438 minutes
           Last result: new database downloaded
    Forwarding-mode: continuous delivery
    Scan engine type: sophos-engine
    Scan engine information: last action result: No error
    Anti-virus signature version: 1.13 (1.02)
```

Antivirus

カウンターの確認

```
user@srx> show security utm anti-virus statistics
 UTM Anti Virus statistics:

 Intelligent-prescreening passed:      0
 MIME-whitelist passed:                0
 URL-whitelist passed:                 0
 Session abort:                        0
 Scan Request:

  Total           Clean         Threat-found    Fallback
      26              14              12              0

 Fallback:
                               Log-and-Permit    Block             Permit
 Engine not ready:                 0                 0                 0
 Out of resources:                 0                 0                 0
 Timeout:                          0                 0                 0
 Maximum content size:             0                 0                 0
 Too many requests:                0                 0                 0
 Decompress error:                 0                 0                 0
 Others:                           0                 0                 0
```


Thank you
JUNIPER NETWORKS
Driven by Experience™