Juniper SRX 日本語マニュアル

SSL Forward Proxy の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、SSL Forward Proxy の CLI 設定ついて説明します
- 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/

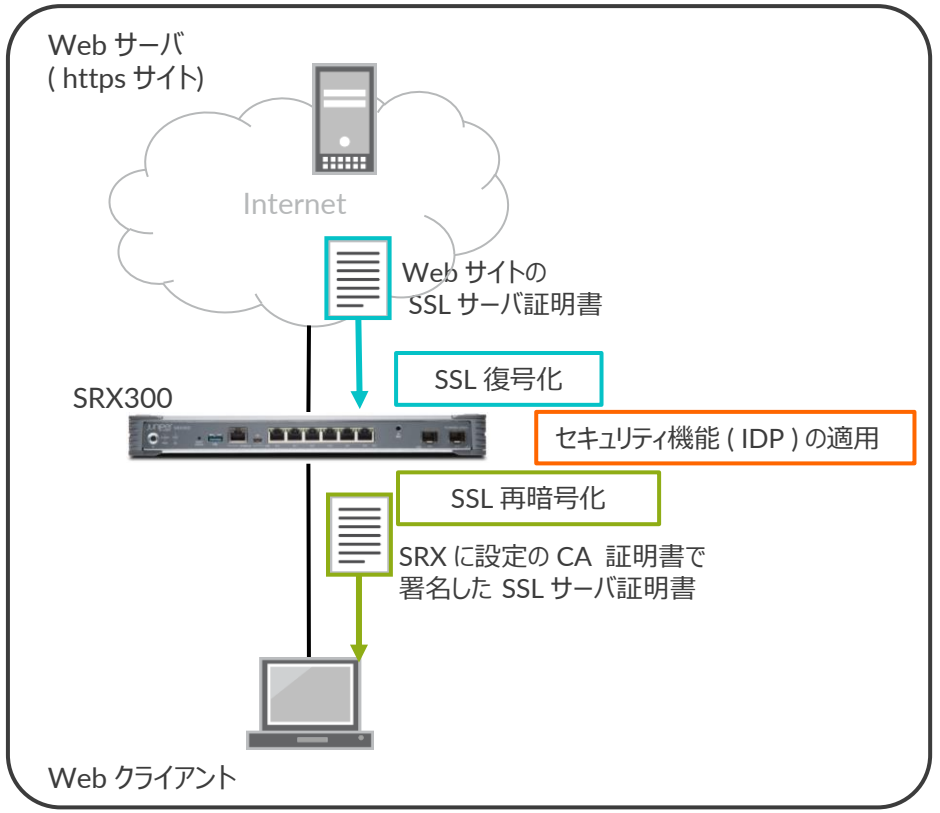
- 他にも多数の SRX 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/security.html

2022 年 8 月

SSL Forward Proxy

以下の設定を行う場合の コマンド例となります

- SSL 暗号化通信の復号化・再暗号化
- セキュリティ機能 (IDP) の適用



SSL Forward Proxy

- CA 証明書を作成します

```
user@srx> request security pki generate-key-pair certificate-id srx-cert size 2048 type rsa
                                                          ※任意の ID ( srx-cert )、鍵長を 2048 、RSA 暗号を指定

user@srx> request security pki local-certificate generate-self-signed certificate-id srx-cert domain-name srx-ca.local subject
"CN=srx-ca.local,OU=Sales,O=Juniper Networks,L=Tokyo,C=JP" email admin@srx-ca.local add-ca-constraint
                                                          ※任意のドメイン名 ( srx-ca.local )、
                                                            任意の subject 内容 "CN,OU,O,L,C"、CA 証明書オプションを適用

Self-signed certificate generated and loaded successfully    ※作成成功時の出力メッセージ
```

- Key-Pair や CA 証明書の作成のやり直しが必要となった場合は clear コマンドで作成した内容を削除します

```
user@srx> clear security pki key-pair certificate-id srx-cert                ※ Key-Pair 削除用のコマンド
Key pair deleted successfully

user@srx> clear security pki local-certificate certificate-id srx-cert       ※ CA 証明書削除用のコマンド
```

SSL Forward Proxy

- CA 証明書の確認

```
user@srx> show security pki local-certificate certificate-id srx-cert detail
LSYS: root-logical-system
Certificate identifier: srx-cert
  Certificate version: 3
  Serial number: 0xa994a22095192625347e555b4b0062c5
  Issuer:
    Organization: Juniper Networks, Organizational unit: Sales, Country: JP,
    Locality: Tokyo, Common name: srx-ca.local
  Subject:
    Organization: Juniper Networks, Organizational unit: Sales, Country: JP,
    Locality: Tokyo, Common name: srx-ca.local
  Subject string:
    CN=srx-ca.local, OU=Sales, O=Juniper Networks, L=Tokyo, C=JP
  Alternate subject: "admin@srx-ca.local", srx-ca.local, ipv4 empty, ipv6 empty
  Validity:
    Not before: 05-14-2022 00:51 UTC
    Not after: 05-13-2027 00:51 UTC
  Public key algorithm: rsaEncryption(2048 bits)
    30:82:01:0a:02:82:01:01:00:a9:12:8c:b5:23:b6:3c:04:c6:c6:cb
    09:a7:f5:54:4c:98:b2:f0:52:83:90:a6:49:27:fe:1a:e1:9b:10:b4

  (略)
```

SSL Forward Proxy

- CA リストの登録

```
user@srx> request security pki ca-certificate ca-profile-group load ca-group-name CA-group filename default
                                                                    ※ default (ファイル名)に格納される CA 情報を CA-group として登録
Do you want to load this CA certificate ? [yes,no] (no) yes

Loading 155 certificates for group 'CA-group'.
CA-group_1: Loading done.
CA-group_2: Loading done.
 (略)

CA-group_155: Loading done.
ca-profile-group 'CA-group' successfully loaded. Success[154] Skipped[1]
PKId will be un-responsive for next few minutes to set-up new Cas     ※処理に数分( 1～2 分程度)必要
```

SSL Forward Proxy

- CA リストの確認

```
user@srx> show security pki ca-certificate ca-profile-group CA-group    ※ CA 情報プロファイル CA-group の詳細を表示
Certificate identifier: CA-group_1
  Issued to: Equifax Secure Certificate Authority, Issued by: C = US, O = Equifax, OU = Equifax Secure Certificate Authority
  Validity:
    Not before: 08-22-1998 16:41 UTC
    Not after: 08-22-2018 16:41 UTC
  Public key algorithm: rsaEncryption(1024 bits)
 (略)

user@srx> show configuration security pki          ※ security pki 階層の設定内容を表示するコマンド
ca-profile CA-group_1 {
    ca-identity CA-group_1;
}
ca-profile CA-group_2 {
    ca-identity CA-group_2;
}
 (略)
```

SSL Forward Proxy

- SSL Proxy プロファイルを設定します

```
user@srx# set services ssl proxy profile SSL-Proxy root-ca srx-cert          ※ CA 証明書を指定
user@srx# set services ssl proxy profile SSL-Proxy trusted-ca CA-group       ※ CA 情報リストを指定
user@srx# set services ssl proxy profile SSL-Proxy actions ignore-server-auth-failure    ※サーバエラーを無視するオプションを指定
```

- オプション設定 (Ciphers)

```
user@srx# set services ssl proxy profile SSL-Proxy preferred-ciphers custom
user@srx# set services ssl proxy profile SSL-Proxy custom-ciphers rsa-with-aes-256-cbc-sha
```

- IDP を設定します (ライセンス等必要)

```
user@srx# set security idp idp-policy IDP rulebase-ips rule rule1 match attacks predefined-attacks HTTP:STC:DL:EICAR
user@srx# set security idp idp-policy IDP rulebase-ips rule rule1 then action drop-connection
user@srx# set security idp default-policy IDP
```

SSL Forward Proxy

- セキュリティポリシーを設定します

```
user@srx# set security policies from-zone trust to-zone untrust policy HTTPS match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy HTTPS match destination-address any
user@srx# set security policies from-zone trust to-zone untrust policy HTTPS match application junos-https
user@srx# set security policies from-zone trust to-zone untrust policy HTTPS then permit application-services idp
user@srx# set security policies from-zone trust to-zone untrust policy HTTPS then permit application-services ssl-proxy profile-name
SSL-Proxy
```

- CA 証明書をエクスポートします（ Web クライアントのブラウザなどにインポート)

```
user@srx> request security pki local-certificate export certificate-id srx-cert type pem filename /var/tmp/srx-cert.pem
```

SSL Forward Proxy

設定の確認 1

```
user@srx# show
services {
    ssl {
        proxy {
            profile SSL-Proxy {
                preferred-ciphers custom;
                custom-ciphers [ rsa-with-aes-256-cbc-sha ];
                trusted-ca CA-group;
                root-ca srx-cert;
                actions {
                    ignore-server-auth-failure;
                }
            }
        }
    }
}
```

SSL Forward Proxy

設定の確認 2

```
security {
    pki {
        ca-profile CA-group_1 {
            ca-identity CA-group_1;
        }
        ca-profile CA-group_2 {
            ca-identity CA-group_2;
        }
         (略)

    idp {
        idp-policy IDP {
            rulebase-ips {
                rule rule1 {
                    match {
                        attacks {
                            predefined-attacks HTTP:STC:DL:EICAR;
                        }
                    }
                    then {
                        action {
                            drop-connection;
                        }
                    }
                }
            }
        }
        default-policy IDP;
    }
```

SSL Forward Proxy

設定の確認 3

```
    policies {
        from-zone trust to-zone untrust {
            policy HTTPS {
                match {
                    source-address any;
                    destination-address any;
                    application junos-https;
                }
                then {
                    permit {
                        application-services {
                            idp;
                            ssl-proxy {
                                profile-name SSL-Proxy;
                            }
                        }
                    }
                }
            }
        }
    }
}
```


Thank you
JUNIPER NETWORKS
Driven by Experience™