Juniper SRX 日本語マニュアル

Secure Web Proxy の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

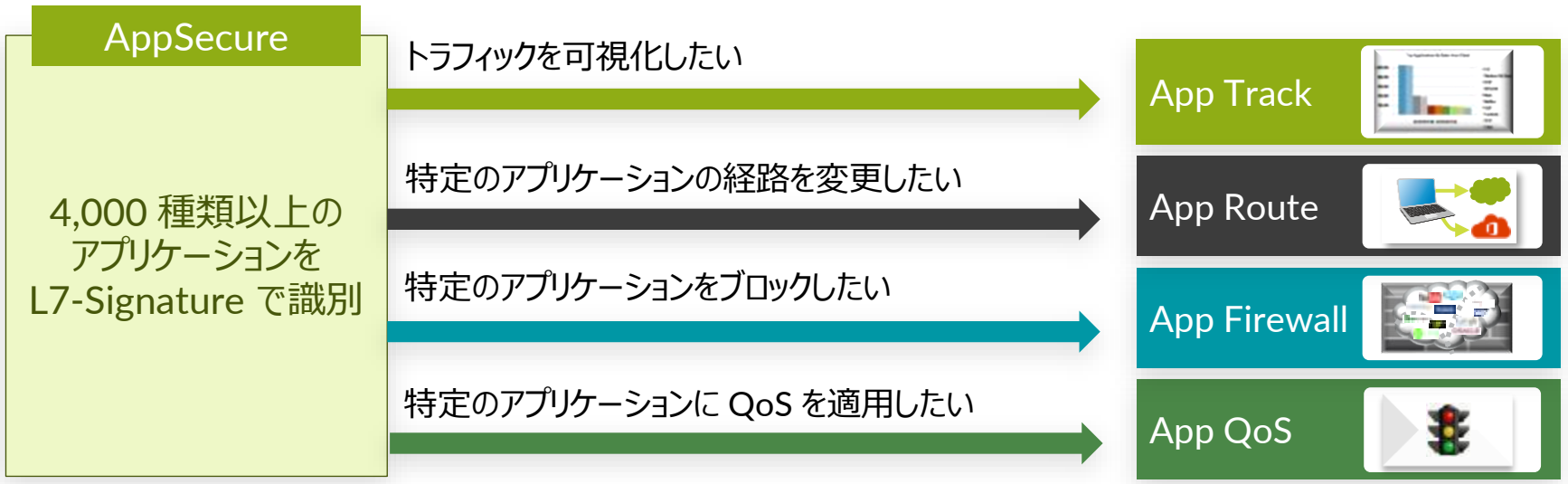
はじめに

- 本マニュアルは、Secure Web Proxy 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

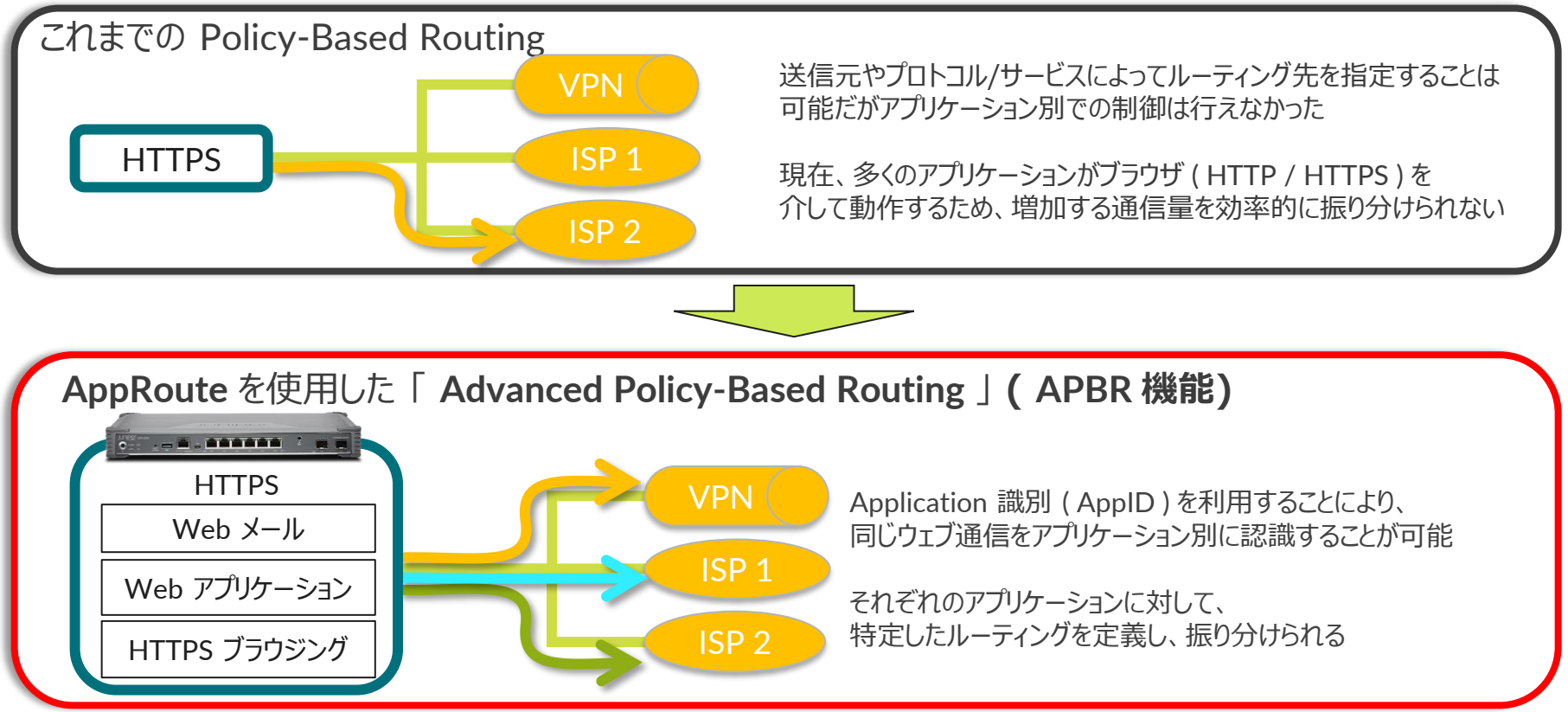
2022 年 8 月

AppSecure の用途による分類

SRX は識別したアプリケーションに対して、可視化、 経路制御、 ポリシー、 QoS を適用させることが可能です



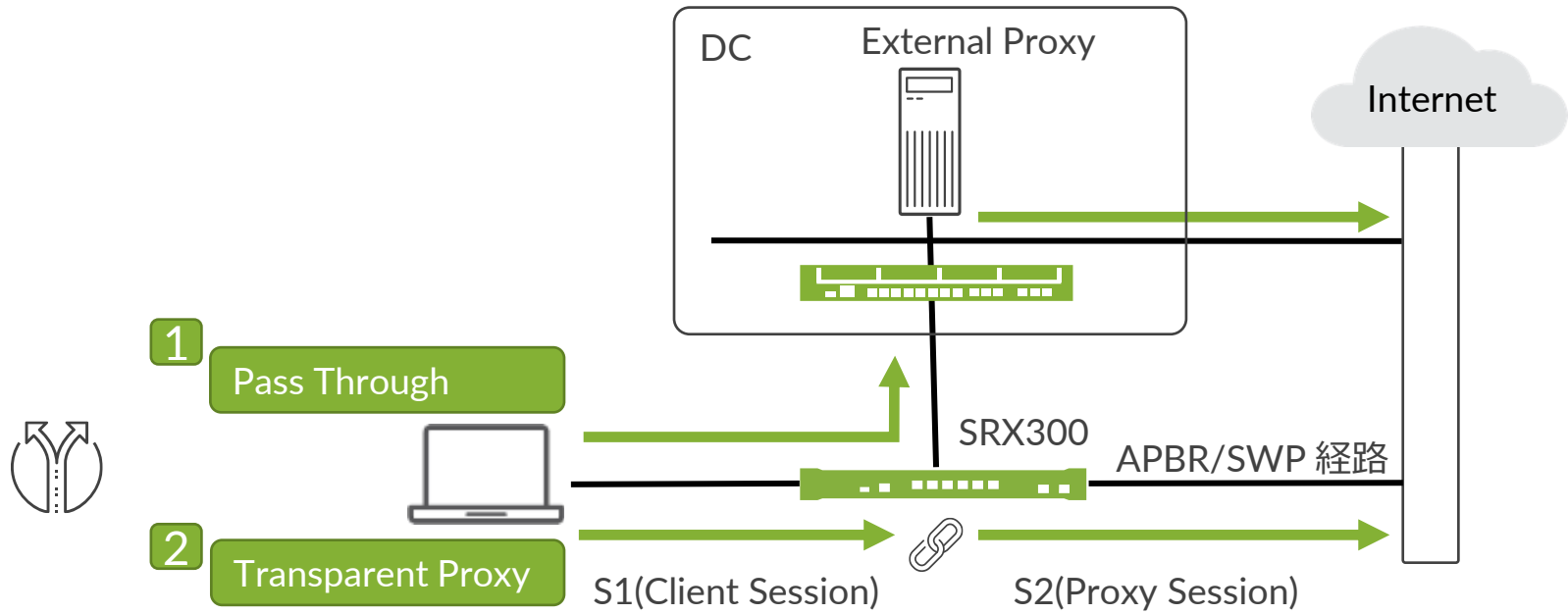
AppRoute（ APBR ）



Secure Web Proxy

構成例

DC の Proxy 経由の通信の一部、Zoom と WebEx をインターネット回線にブレイクアウトします
SRX がプロキシとして動作するため、クライアントの Proxy 設定変更は不要です



Secure Web Proxy

Secure Web Proxy 機能を利用するには機器にライセンスがインストールされている必要があります
当該機能を IDP なしで使用されている場合は application-identification (AppID シグネチャ)をダウンロードする必要があります

1. 下記コマンドでダウンロードします

```
user@srx> request services application-identification download
```

2. ダウンロード状況を確認します

```
user@srx> request services application-identification download status
Downloading application package 3505 succeeded.
```

3. この機能を IDP とともに使用する場合、シグネチャは下記コマンドでダウンロードします

```
user@srx> request security idp security-package download
```

4. ダウンロード状況を確認します

```
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)
```

Secure Web Proxy

5. 自動更新をスケジューリングするには、次の設定を追加します
   例: 36 時間毎に更新

```
user@srx# set security idp security-package automatic interval 36 start-time 2022-05-15.13:00:00
```

6. AppID シグネチャを下記コマンドでインストールします

```
user@srx> request services application-identification install
```

7. インストール状況を確認します

```
user@srx> request services application-identification install status
Installed
        Application package (3505) and Protocol bundle successfully

user@srx> show services application-identification version
  Application package version: 3505
```

Secure Web Proxy

8. APBR を設定します
   アプリケーション可視化を有効化

```
user@srx# set security zones security-zone trust application-tracking
```

9. 対象とするアプリケーションを定義します

```
user@srx# set services application-identification application-group BREAKOUT_GRP applications junos:WEBEX
user@srx# set services application-identification application-group BREAKOUT_GRP applications junos:ZOOM
```

10. APBR 用のルーティングインスタンスの作成し、APBR 経路用のデフォルトルートを設定します

```
user@SRX# set routing-instances APBR instance-type forwarding
user@SRX# set routing-instances APBR routing-options static route 0.0.0.0/0 next-hop 192.168.91.99
```

11. 経路情報を設定します
    デフォルトルート、ルーティングインスタンスの情報を APBR 用のルーティングインスタンスにインポート

```
user@srx# set routing-options static route 0.0.0.0/0 next-hop 192.168.26.99
user@srx# set routing-options interface-routes rib-group inet APBR-Group
user@srx# set routing-options rib-groups APBR-Group import-rib APBR.inet.0
user@srx# set routing-options rib-groups APBR-Group import-rib inet.0
```

Secure Web Proxy

12. APBR プロファイルを作成します

```
user@srx# set security advance-policy-based-routing tunables max-route-change 0
user@srx# set security advance-policy-based-routing profile APBR_profile rule R01 match dynamic-application-group BREAKOUT_GRP
user@srx# set security advance-policy-based-routing profile APBR_profile rule R01 then routing-instance APBR
```

13. APBR ポリシーの作成し、プロファイルを紐づけます

```
user@srx# set security advance-policy-based-routing from-zone trust policy APBR_policy match source-address any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR_policy match destination-address any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR_policy match application any
user@srx# set security advance-policy-based-routing from-zone trust policy APBR_policy then application-services advance-policy-
based-routing-profile APBR_profile
```

14. Secure Web Proxy を設定します
    Proxy サーバとブレイクアウト対象アプリを指定

```
user@srx# set services web-proxy secure-proxy profile LBO-profile proxy-address external_proxy ip 192.168.26.226/32
user@srx# set services web-proxy secure-proxy profile LBO-profile proxy-address external_proxy port 8080
user@srx# set services web-proxy secure-proxy profile LBO-profile dynamic-web-application-group BREAKOUT_GRP
```

15. Secure Web Proxy プロファイルをポリシーに紐づけます

```
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 web-proxy profile-name
LBO-profile
```

Secure Web Proxy

設定の確認 1

```
user@srx# show
services {
    application-identification {
        application-group BREAKOUT_GRP {
            applications {
                junos:WEBEX;
                junos:ZOOM;
            }
        }
    }
    web-proxy {
        secure-proxy {
            profile LBO-profile {
                proxy-address external_proxy {
                    ip 192.168.26.226/32;
                    port 8080;
                }
                dynamic-web-application-group BREAKOUT_GRP;
            }
        }
    }
}
```

Secure Web Proxy

設定の確認 2

```
security {
    idp {
        security-package {
            automatic {
                start-time "2022-5-15.13:00:00 +0900";
                interval 36;
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy T2U {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            web-proxy {
                                profile-name LBO-profile;
                            }
                        }
                    }
                }
            }
        }
    }
```

Secure Web Proxy

設定の確認 3

```
zones {
    security-zone trust {
        application-tracking;
    }
advance-policy-based-routing {
    tunables {
        max-route-change 0;
    }
    profile APBR_profile {
        rule R01 {
            match {
                dynamic-application-group BREAKOUT_GRP;
            }
            then {
                routing-instance APBR;
            }
        }
    }
    from-zone trust {
        policy APBR_policy {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                application-services {
                    advance-policy-based-routing-profile APBR_profile;
                }
```

Secure Web Proxy

設定の確認 4

```
                }
            }
        }
    }
}
routing-instances {
    APBR {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 192.168.91.99;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.168.26.99;
    }
    interface-routes {
        rib-group inet APBR-Group;
    }
    rib-groups {
        APBR-Group {
            import-rib [ inet.0 APBR.inet.0 ];
        }
    }
}
```

Secure Web Proxy

Secure Web Proxy の動作確認 (Transparent Proxy / Passthrough)

```
user@srx> show services web-proxy statistics
        Active Transparent proxy sessions              18
        Active Passthrough sessions                    9
        Active HTTP passthrough sessions               0
        Active HTTPS passthrough sessions              9
        Total Transparent proxy sessions               88
        Total Passthrough sessions                     401
        Total HTTP Passthrough sessions                2
        Total HTTPS Passthrough sessions               399
```

Transparent Proxy として動作中のセッションの確認
※ SRX が Proxy として動作するため 2 セッションを消費します

```
user@srx> show services web-proxy session summary
Web Proxy sessions:
Client Session                                                  Proxy Session
[2455] 10.91.0.99/62869 ---> 192.168.26.226/8080                      [2456] 10.91.0.99/62869 ---> 182.22.28.252/443

[2437] 10.91.0.99/62859 ---> 192.168.26.226/8080                      [2438] 10.91.0.99/62859 ---> 182.22.24.252/443

[2426] 10.91.0.99/62852 ---> 192.168.26.226/8080                      [2429] 10.91.0.99/62852 ---> 183.79.217.124/443

[2440] 10.91.0.99/62861 ---> 192.168.26.226/8080                      [2443] 10.91.0.99/62861 ---> 54.65.24.54/443

[2457] 10.91.0.99/62870 ---> 192.168.26.226/8080                      [2458] 10.91.0.99/62870 ---> 183.79.217.124/443
  (略)
```


Thank you
JUNIPER NETWORKS
Driven by Experience™