Juniper SRX 日本語マニュアル

Local Web Filter を使用した SNI ログの CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、Local Web Filter を使用した HTTPS サイトの SNI (Server Name Indication) 情報をログに出力するための 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

Local Web Filter

全ての URL を許可するローカルの Web Filter 設定をセキュリティポリシーに使用することによって、
HTTPS Web 通信の SNI (Server Name Indication) 情報を Web Filter のログに出力させる設定をします

HTTPS の Web 通信は通常 SSL 暗号化されており、SSL Proxy などの復号化機能を使用しない場合は
アクセス先の URL 情報が確認できない状態となります

通信内の SNI 情報を Web Filter 機能で記録することによって、通信先の HTTPS サイトのドメイン名情報を
ログにて確認することが可能になります

※ Web Filtering の SNI 機能は Junos 15.1X49-D80 より実装の機能です
※ Local Web Filter 機能の利用は、追加の UTM ライセンスは不要です

Local Web Filter

UTM プロファイル、 Local Web Filter 、UTM ポリシーを設定します

1. UTM の feature-profile (web-filtering) において Web Filter の type を juniper-local と指定します

```
user@srx# set security utm feature-profile web-filtering type juniper-local
```

2. juniper-local のプロファイルに、デフォルトの許可とログ（ log-and-permit ）、ブロック時の表示メッセージ
(全て許可の設定のため実際には利用されない)、フェールバック時の許可とログ（ log-and-permit ）を設定します

```
user@srx# set security utm feature-profile web-filtering juniper-local profile SNI-Profile default log-and-permit
user@srx# set security utm feature-profile web-filtering juniper-local profile SNI-Profile custom-block-message "Blocked Site"
user@srx# set security utm feature-profile web-filtering juniper-local profile SNI-Profile fallback-settings default log-and-permit
```

3. 設定した feature-profile を UTM ポリシー (Web-Filter) に指定します

```
user@srx# set security utm utm-policy Web-Filter web-filtering http-profile SNI-Profile
```

Local Web Filter

4. 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 WEB match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy WEB match destination-address any
user@srx# set security policies from-zone trust to-zone untrust policy WEB match application junos-https
user@srx# set security policies from-zone trust to-zone untrust policy WEB then permit application-services utm-policy Web-Filter
```

5. Syslog を設定します
   (Web Filter ログを記録するための Syslog 設定を指定)

```
user@srx# set system syslog file WF-log any info
user@srx# set system syslog file WF-log match WEBFILTER_
user@srx# set system syslog file WF-log archive size 1m
user@srx# set system syslog file WF-log archive files 3
```

6. System Log を設定します

```
user@arx# set security log mode event
```

Local Web Filter

設定の確認 1

```
user@srx# show
system {
    syslog {
        file WF-log {
            any info;
            match WEBFILTER_;
            archive size 1m files 3;
        }
    }
}
```

Local Web Filter

設定の確認 2

```
security {
    log {
        mode event;
    }
    utm {
        feature-profile {
            web-filtering {
                type juniper-local;
                juniper-local {
                    profile SNI-Profile {
                        default log-and-permit;
                        custom-block-message "Blocked Site";
                        fallback-settings {
                            default log-and-permit;
                        }
                    }
                }
            }
        }
        utm-policy Web-Filter {
            web-filtering {
                http-profile SNI-Profile;
            }
        }
    }
```

Local Web Filter

設定の確認 3

```
    policies {
        from-zone trust to-zone untrust {
            policy WEB {
                match {
                    source-address any;
                    destination-address any;
                    application junos-https;
                }
                then {
                    permit {
                        application-services {
                            utm-policy Web-Filter;
                        }
                    }
                }
            }
        }
    }
}
```

Local Web Filter

- Operational モードの show log コマンドより、作成したセキュリティポリシーを介した HTTPS サイトのアクセス情報（ Web Filter ログ）が確認できます

※ Web Filter ログの URL 項目に記録されたサイトの SNI 情報が出力されます
SNI が無い場合はアクセス先の IP アドレス情報が出力されます

```
user@srx> show log WF-log

May 13 18:49:44  srx RT_UTM: WEBFILTER_URL_PERMITTED: WebFilter: ACTION="URL Permitted" source-zone="trust" destination-
zone="untrust" 10.91.0.99(50129)->142.250.199.99(443) SESSION_ID=1130 APPLICATION="UNKNOWN" NESTED-APPLICATION="UNKNOWN"
CATEGORY="N/A" REASON="BY_LOCAL_DEFAULT" PROFILE="SNI-Profile" URL=www.gstatic.com OBJ=/ username N/A roles N/A application-sub-
category N/A urlcategory-risk 0
```


Thank you
JUNIPER NETWORKS
Driven by Experience™