Juniper SRX 日本語マニュアル

42. Local Web Filter を使用した SNI ログの CLI 設定

Juniper Networks | Engineering Simplicity

はじめに

Local Web Filter を使用した、HTTPS サイトの SNI（Server Name Indicater）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「15.1X49-D140」にて確認を実施しております。

2018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 Indicator）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」より実装の機能になります。
※ Local Web Filter 機能の利用は、追加の UTM ライセンスは不要になります。

Local Web Filter

① UTM プロファイル、Local Web Filter、UTM ポリシーの設定

UTM の feature-profile（web-filtering）において、Web Filter の type を juniper-local と指定

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

juniper-local のプロファイルに、デフォルトの許可とログ（log-and-pernit）、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

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

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

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

Local Web Filter

② セキュリティポリシーの設定

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

③ Syslog の設定

Web Filter ログを記録するための Syslog 設定を指定

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

④ System Log の設定

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

Local Web Filter

設定の確認

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

Local Web Filter

設定の確認

```
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;
                        }
                    }
                }
```

Local Web Filter

設定の確認

```
        utm-policy Web-Filter {
            web-filtering {
                http-profile SNI-Profile;
            }
        }
    }
    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@host> show log WF-log

May 26 16:19:15  host RT_UTM: WEBFILTER_URL_PERMITTED: WebFilter: ACTION="URL Permitted"
10.3.45.210(32314)->216.58.200.195(443) CATEGORY="N/A" REASON="BY_LOCAL_DEFAULT"
PROFILE="SNI-Profile" URL=www.google.co.jp OBJ=/ username N/A roles N/A
```