Juniper SRX 日本語マニュアル

Screen オプションの CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、Screen オプションの 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

Screen オプション

以下の設定を行う場合のコマンド例となります

- 同一宛先 IP アドレスに対するセッションを 50 に制限する Screen オプションを追加
- Untrust ゾーンに対して Screen Profile を適用

Screen オプション

1. 現在の Screen オプションを表示します

```
user@srx> show configuration security | match screen | display set
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood destination-threshold 2048
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security zones security-zone untrust screen untrust-screen
```

※上記はデフォルトの設定

2. Screen オプションを追加します

```
user@srx# set security screen ids-option untrust-screen limit-session destination-ip-based 50
```

3. Screen Profile を Security Zone に設定します

```
user@srx# set security zones security-zone untrust screen untrust-screen
```

Screen オプション

設定の確認 1

```
user@srx# show
security {
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
                land;
            }
            limit-session {
                destination-ip-based 50;
            }
        }
    }
```

Screen オプション

設定の確認 2

```
    zones {
        security-zone untrust {
            screen untrust-screen;
        }
    }
}
```

Screen オプション

カウンターの確認

```
user@srx> show security screen statistics zone untrust
Screen statistics:

IDS attack type                              Statistics
  ICMP flood                                 0
  UDP flood                                  0
  TCP winnuke                                0
  TCP port scan                              0
  （省略）

  IP block fragment                          0
  Destination session limit                  1693
  IPv6 extension header                      0
  （省略）
```

Screen オプション

ロギングの設定

- Syslog を設定

```
user@srx# set system syslog file messages any any
```

- Syslog を表示

```
user@srx> show log messages

May 13 16:54:25  srx RT_IDS: RT_SCREEN_SESSION_LIMIT: Dst IP session limit! source: 192.168.26.226:undefined, destination:
192.168.1.1:undefined, protocol-id: 1, zone name: untrust, interface name: ge-0/0/0.0, action: drop
```


Thank you
JUNIPER NETWORKS
Driven by Experience™