Juniper SRX 日本語マニュアル

Screen オプションの CLI 設定

JUNIPER NETWORKS | Engineering Simplicity

はじめに

Screen オプションの CLI 設定方法について説明します。

※手順内容は「SRX300」、JUNOS「19.4R3-S1」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/

2021年7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 zone に対して screen profile を適用

Screen オプション

- 現在の screen オプションを表示

```
user@host> 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

Screen オプション

- screen オプションを追加

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

- screen profile を security zone に設定

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

Screen オプション

設定の確認

```
user@host> 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;
            }
```

Screen オプション

設定の確認

```
            limit-session {
                destination-ip-based 50;
            }
        }
    }
    zones {
        security-zone untrust {
            screen untrust-screen;
        }
    }
}
```

Screen オプション

カウンターの確認

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

IDS attack type                              Statistics
  ICMP flood                                 0
  UDP flood                                  0
  （略）
  TCP FIN no ACK                             0
  Source session limit                       0
  TCP SYN-ACK-ACK proxy                      0
  IP block fragment                          0
  Destination session limit                  13507
  IPv6 extension header                      0
  （略）
```

Screen オプション

ロギングの設定

- syslog を設定

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

- syslog を表示

```
user@host> show log messages

May 16 14:45:55  SRX300 RT_IDS: RT_SCREEN_SESSION_LIMIT: Dst IP session limit!      source:
198.51.100.228:45688, destination: 203.0.113.198:45688, protocol-id: 17,       zone name:
untrust, interface name: ge-0/0/0.0, action: drop
```