

On-box logging and reporting CSB statistics in J-web

Version 1.1
Ricardo Garcia
Date: April 23rd, 2020

Intellectual Property Rights

This document contains valuable trade secrets and confidential information of Juniper Networks Ltd. and its suppliers, and shall not be disclosed to any person, organization, or entity unless such disclosure is subject to the provisions of a written non-disclosure and proprietary rights agreement or intellectual property license agreement approved by Juniper Networks Ltd. The distribution of this document does not grant any license in or rights, in whole or in part, to the content, the product(s), technology, or intellectual property described herein.

Contents

Overview	3
Description	3
Syntax	3
Heirarchy Level	3
Options	4

Overview

During IBM Cloud deployment and provisioning of the vSRX, basic settings for the gateway are set, which do not include on-box reporting configuration. You can enable the on-box reporting feature by configuring the `set security log report` CLI command at `edit security log hierarchy`.

Description

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action.

Syntax

```
report {
  logs-per-table {
    idp log-number;
    ipsec-vpn log-number;
    screen log-number;
    session-all log-number;
    sky log-number;
    utm log-number;
  }
  table-lifetime table-lifetime;
}
table-mode {
  dense;
}
```

Heirarchy Level

```
[edit security log (Security)]
[edit logical-systems name security log (Security)]
[edit tenants tenant-name security log (Security)]
```

Options

report—Enable log report.

logs-per-table—Log number for each table.

idp—Log number of idp.

Range: vSRX: 40000 through 80000

ipsec-vpn—Log number of IPsec-VPN.

Range: vSRX: 26666 through 26666

screen—Log number of screen.

Range: vSRX: 40000 through 80000

session-all—Log number of session.

Range: vSRX: 80000 through 800000

sky—Log number of SKY.

Range: vSRX: 40000 through 80000

utm—Log number of UTM.

Range: vSRX: 40000 through 80000

table-lifetime—Table lifetime days.

Default: 90

Range: 0 through 365

table-mode—Enable table dense mode.

Database File Size Capacity

Devices	Session	Screen	IDP	UTM	IPsec-VPN	SKY
vSRX	1.8G	0.18G	0.18G	0.18G	0.06G	0.18G

Note:

You must configure security policy for the session using the set security policies from-zone zone-name to-zone zone-name policy *policy-name* then log session-close command to list all the applications and nested applications in Application Tracking on J-Web using the on-box reporting feature.

For more information about on-box Security logging please visit:

https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-edit-log-security-logging.html