

Check Point Log Export

Solution

Check Point "**Log Exporter**" is an easy and secure method for exporting Check Point logs over the syslog protocol. It is integrated in Version R80.20 or higher.

Example

Basic Log Export to another syslog Server

```
cp_log_export add name SyslogToSplunk target-server <ip|hostname> target-port <port> protocol
tcp format splunk
```

Show existing config

```
cp_log_export show

name: SyslogToSplunk
  enabled: true
  target-server: 1.2.3.4
  target-port: 8514
  protocol: tcp
  format: splunk
  read-mode: semi-unified
  export-attachment-ids: false
  export-link: false
  export-attachment-link: false
  time-in-milli: false
  export-log-position: Not configured, using default
  encrypted: true
  reconnect-interval: Not configured, using default
```

Filter example (Log only drop and reject messages)

```
cp_log_export set name SyslogToSplunk filter-action-in "drop,reject"
```

Link

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323

Revision #1

Created 28 February 2023 08:49:24 by Peter Baumann

Updated 28 February 2023 08:59:12 by Peter Baumann