

Operation

- [Useful CLI Commands Check Point](#)
- [Export/Import Policy Package](#)
- [Useful Smartlog Queries](#)
- [Useful SNMP OIDs \(VSX\)](#)
- [Threat Prevention API](#)
- [GAIA - Easy execute CLI commands on all gateways simultaneously](#)
- [Threat Prevention Cyber Attacks Dashboard Template](#)
- [DOS & DDOS Prevention, Mitigation](#)
- [Export Syslog Messages](#)
- [Missing feature - Global search across multiple CMA](#)
- [Show logging using the web interface](#)
- [Managing partition sizes via LVM manager on Gaia OS](#)
- [SmartConsole cli parameters](#)
- [Jump to Rule Number or UID](#)
- [SmartConsole: Clear disconnected sessions](#)
- [Initiating manual cluster failover](#)
- [How to migrate Custom Queries from one SmartView Tracker to another](#)
- [Check Point Log Export](#)

Useful CLI Commands Check Point

Cheatsheets

- Check Point CLI Reference Card (https://www.roesen.org/files/cp_cli_ref_card.pdf)
- FW Monitor (https://www.roesen.org/files/fw_monitor.pdf)
- R80 Cheat Sheet FW-Monitor (<https://www.ankenbrand24.de/index.php/articles/check-point-articel/cheat-sheets/r80-cheat-sheet-fw-monitor/>)
- ClusterXL Cheat Sheet (<https://www.ankenbrand24.de/index.php/articles/check-point-articel/cheat-sheets/r80-cheat-sheet-clusterxl/>)

CLISH Commands

To start a transaction in CLISH use **start transaction**.

Commands - **commit**, or **rollback** to be used to end the transaction mode. All changes made using commands in transaction mode are applied at once or none of the changes are applied based on the way transaction mode is terminated.

Show Commands

save config	save the current configuration
show commands	shows all commands
show allowed-client all	show allowed clients
show arp dynamic all	displays the dynamic arp entries
show arp proxy all	shows proxy arp
show arp static all	displays all the static arp entry
show as	displays autonomous system number
show assets all	display hardware information

show bgp stats	shows bgp statistics
show bgp summary	shows summary information about bgp
show vrrp stats	show vrrp statistics
show bootp stats	shows bootp/dhcp relay statistics
show bootp interface	show all bootp/dhcp relay interfaces
show bonding groups	show all bonding groups
show bridging groups	show all bridging groups
show backups	shows a list of local backups
show backup status	show the status of a backup or restore operation being performed
show backup last-successful	show the latest successful backup
show backup logs	show the logs of the recent backups/restores performed
show clock	show current clock
show configuration	show configuration
show-config state	shows the state of configuration either saved or unsaved
show date	shows date
show dns primary	shows primary dns server
show dns secondary	shows secondary dns server
show extended commands	shows all extended commands
show groups	shows all user groups
show hostname	show host name
show inactivity-timeout	shows inactivity-timeout settings
show interfaces	shows all interfaces
show interfaces ethx	shows settings related to an interface “x
show interfaces	show detailed information about all interfaces
show ipv6-state	shows ipv6 status as enabled or disabled
show management interface	shows management interface configuration
show ntp active	shows ntp status as enabled or disabled
show ntp servers	shows ntp servers
show ospf database	shows ospf database information
show ospf neighbors	shows ospf neighbors information
show ospf summary	shows ospf summary information
show pbr rules	shows policy based routing rules

show pbr summary	shows policy based routing summary information
show pbr tables	show pbr tables
show route	shows routing table
show routed version	shows information about routed version
show snapshots	shows a list of local snapshots
show snmp agent-version	shows whether the version is v1/v2/v3
show snmp interfaces	shows snmp agent interface
show snmp traps receivers	shows snmp trap receivers
show time	shows local machine time
show timezone	show configured timezone
show uptime	show system uptime
show users	show configured users and their homedir, uid/gid and shell
show user <username>	shows settings related to a particular user
show version all	shows version related to os edition, kernel version, product version etc
show virtual-system all	show virtual-systems configured
show vpn tunnels	use to show the vpn tunnels
show vrrp stats	shows vrrp status
show vrrp interfaces	shows vrrp enabled interfaces

Set Commands

add allowed-client host any-host / add allowed-client host <ip address>	add any host to the allowed clients list/ add allowed client by ipv4 address
add backup local	create and store a backup file in /var/cpbackups/backups/(on open servers) or /var/log/cpbackup/backups/ (on checkpoint appliances)
add backup scp ip value path value username value	adds backup to scp server
add backup tftp ip value [interactive]	adds backup to tftp server
add snapshot	create snapshots which backs up everything like os configuration, checkpoint configuration, versions, patch level), including the drivers
add syslog log-remote-address <ip address> level <emerg/alert/crit/err/warning/notice/info/debug/all>	specifies syslog parameters
add user <username> uid <user-id-value> homedir	creates a user
expert	executes system shell

halt	put system to halt
history	shows command history
lock database override	overrides the config-lock settings
quit	exits out of a shell
reboot	reboots a system
restore backup local [value]	restores local backup interactively
rollback	ends the transaction mode by reverting the changes made during transaction
save config	save the current configuration
set backup restore local <filename>	restores a local backup
set cluster member admin {down up}	initiating manual cluster failover
set core-dump <enable/disable>	enable/disable core dumps
set date yyyy-mm-dd	sets system date
set dhcp server enable	enable dhcp server
set dns primary <x.x.x.x>	sets primary dns ip address
set dns secondary <x.x.x.x>	sets secondary dns ip address
set expert-password	set or change password for entering into expert mode
set edition default <value>	set the default edition to 32-bit or 64-bit
set hostname <value>	sets system hostname
set inactivity-timeout <value>	sets the inactivity timeout
set interface ethx ipv4-address x.x.x.x mask-length 24	adds ip address to an interface
set ipv6-state on/off	sets ipv6 status as on or off
set kernel-routes on/off	sets kernel routes to on/off state
set management interface <interface name>	sets an interface as management interface
set message motd value	sets message of the day
set ntp active on/off	activates ntp on/off
set ntp server primary x.x.x.x version <1/2/3/4>	sets primary ntp server
set ntp server secondary x.x.x.x version <1/2/3/4>	sets secondary ntp server
set snapshot revert<filename>	revert the machine to the selected snapshot
set snmp agent on/off	sets the snmp agent daemon on/off
set snmp agent-version <value>	sets snmp agent version
set snmp community <value> read-only	sets snmp readonly community string

add snmp interface <interface name>	sets snmp agent interface
set snmp traps receiver <ip address> version v1 community value	specifies trap receiver
set snmp traps trap <value>	set snmp traps
set static-route x.x.x.x/xx nexthop gateway address x.x.x.x on set static-route x.x.x.x/xx comment "{comment}"	adds specific static route comment static route
set static-route <i>NETWORK_ADDRESS/MASK_LENGTH</i> nexthop gateway address <i>GATEWAY_IP_ADDRESS</i> off set static-route <Destination IP address> off set static-route default nexthop gateway address <i>GATEWAY_IP_ADDRESS</i> off	Delete Routes
set time <value>	sets system time
set time zone <time-zone>	sets the time zone
set vsx off	sets vsx mode on
set vsx on	sets vsx mode off
set user <username> password	sets users password
set web session-timeout <value>	sets web configuration session time-out in minutes
set web ssl-port <value>	sets the web ssl-port for the system

Generic Commands

The commands below have to be used in expert mode and NOT in clish.

Action	Use on	Command
--------	--------	---------

SIC Reset	GW / MGMT	<ol style="list-style-type: none"> 1. <i>cpconfig</i> 2. <i>Secure Internal Communication</i> 3. <i>re-initialize communication</i> 4. <i>Enter activation key</i> <p><i>On MGMT goto GW settings - General Properties - Communication and re-initialize the SIC with the provided activation key</i></p> <p><i>More information:</i></p> <p><i><u>How to reset SIC</u></i></p> <p><i><u>How to troubleshoot SIC</u></i></p> <p><i><u>How to reset SIC on a VSX Gateway for a specific Virtual System</u></i></p>
Show licenses	MGMT / GW	<i>cplic print -x</i> (-x print signatures)
Remove Evaluation License	GW	<i>cplic eval_disable</i> You have disabled Check Point evaluation period For activation you need to restart ALL Check Point modules (performing cpstop & cpstart)
Get licenses from management system on gateway	GW	<i>contract_util mgmt</i>
Show enabled blades Example: <div># enabled_blades</div> <div>fw ips ThreatEmulation Scrub</div>	GW	<i>enabled_blades</i>
ClusterXL Switch over (disable ClusterXL state)	GW	<i>clusterXL_admin down</i> Note: The [-p] is an optional flag (stands for "permanent") - the Critical Device called "admin_down" will be automatically added to the \$FWDIR/conf/cphaprob.conf file, so that this configuration survives the reboot.
Show Cluster status	GW	<i>cphaprob stat</i>
Show Virtual Cluster Interfaces	GW	<i>cphaprob -a if</i>

Debug to see all dropped connections	GW	<i>fw ctl zdebug drop</i> <i>fw ctl zdebug -h (help)</i>
Debug to see all NAT informations	GW	<i>fw ctl zdebug + xlat</i>
Debug to get a fast packet trace	GW	<i>fw ctl zdebug + packet grep -B 1 TCP grep -B 1 "(SYN)"</i>
See stats of number of connections	GW	<i>cpstat fw</i>
Connections load on the fw	GW	<i>fw tab -s -t connections</i>
Clear ALL connections on fw from the table (CAUTION!)	GW	<i>fw tab -t connections -x</i>
ClusterXL sync statistics to R80.10 (sk34476) ClusterXL sync statistics for R80.20 and higher (sk34475)	GW GW	<i>fw ctl pstat</i> CLISH: show cluster statistics sync Expert: cphaprob syncstat
Show connected SmartConsole clients	MGMT	<i>cpstat mg</i>
Manage the GUI clients that can use SmartConsoles to connect to the Security Management Server	MGMT	<i>cp_conf client get</i> # Get the GUI clients list <i>cp_conf client add <GUI client></i> # Add one GUI Client <i>cp_conf client del < GUI client 1> < GUI client 2>...</i> # Delete GUI Clients <i>cp_conf client createlist < GUI client 1> < GUI client 2>...</i> # Create new list.
Show sync details	GW	<i>fw ha -f all</i>
Shows packets accepted, dropped, peak connections, and top rule hits	GW	<i>cpstat blades</i>

Use CLI commands over SIC from MGMT without password, used as example for "last chance" configs.	MGMT	<i>cprid_util (--help)</i> <div> <p>Example Reset admin password without access to GW:</p> <pre> /sbin/grub-md5-crypt cprid_util -server <IP_of_Gateway> -verbose rexec -rcmd /bin/clish -s -c \ 'set config-lock on override' # Ensure clish db is unlocked cprid_util -server <IP_of_Gateway> -verbose rexec -rcmd /bin/clish -s -c \ 'set user admin password-hash <Password_Hash_from_Step_ab ove>' # Set admin user pw hash cprid_util -server <IP_of_Gateway> -verbose rexec -rcmd /bin/clish -s -c \ 'set expert-password-hash <Password_Hash_from_Step_ab ove>' # change expert pw hash </pre> </div>
Show interfaces, ip-addresses and subnet mask, used for a very good interface-overview.	MGMT/GW	<i>fw getifs</i>
Show installed hotfixes and releases	GW	<i>cpinfo -y all</i>
Create cpinfo file for sending to the support. Included are log files and fw table dump. The resulting file is compressed	MGMT / GW	<i>cpinfo -Ddlzk -o /var/tmp/\$HOSTNAME</i>

Show statistics about accelerated traffic	GW	<i>fwaccel stats -s</i>
This command will list what interface is connected to what IRQ to what core.	GW	<i>fw ctl affinity -l -v -r</i> <i>fw ctl affinity -s</i> will subsequently allow you to set the values.
UNDOCUMENTED Show state and timeline of ClusterXL events in CLISH	GW	<i>CLISH:</i> <i>show routed cluster-state detailed</i>
Top 10 Source-IPs in connection table. You need to manual convert hex in ascii to get the ip, like so: 0a1f0af2 = 10.31.10.242. For the top 10 destinations, substitute \$4 for \$2 in the awk command.	GW	<i>fw tab -u -t connections awk '{ print \$2 }' sort -n uniq -c sort -nr head -10</i>
Log Diagnostic Report It will analyze the logs and give you a brief output of your Current Logging and Daily Average Logging rates. It will also produce a detailed output at <i>/tmp/sme-diag/results/detailed_diag_report.txt</i> https://community.checkpoint.com/t5/Logging-and-Reporting/R80-xx-equivalent-of-CPLogInvestigator-for-Log-Volume-and/td-p/46792	LOG	<i>\$RTDIR/scripts/doctor_log.sh</i>

VPN Commands

The commands below have to be used in expert mode and NOT in clish.

To view informations about VPN Tunnels

In R80+:

- Open SmartConsole > Logs & Monitor.
- Open the catalog (new tab).
- Click Tunnel & User Monitoring.

See also: [Logging and Monitoring R80.10 \(Part of Check Point Infinity\)](#)

Action	Use on	Command
VPN statistics	GW	<i>cpstat -f all vpn</i>
VPN Tunnel manipulation	GW	<i>vpn tu</i> Interactive usage (better): <i>vpn shell</i>
VPN Remote Access specific	GW	<i>pep show user all</i>
Check VPN-1 major and minor version as well as build number and latest hotfix. Use -k for kernel version	GW	<i>vpn ver [-k]</i>
Show, if any, overlapping VPN domains	GW	<i>vpn overlap_encdom</i>
VPN IKE Debugging (P1 and P2 Communication) The resulting \$FWDIR/log/ike.elg and/or \$FWDIR/log/ikev2.xml can be used in the "IKEView" Utility from Check Point, see here: sk30994	GW	<i>vpn debug ikeon</i> (enable IKE debug) <i>vpn debug ikeoff</i> (disable IKE debug)

VSX specific

The commands below have to be used in expert mode and NOT in clish

Action	Use on	Command
Show VSX status. Verbose with -v, interface list with -l or status of single VS with VS ID <id>.	VSX / VS	<i>vsx stat [-v] [-l] [id]</i>

<p>Show connections stats</p> <div> <p>Example:</p> <pre># vsx stat -v -l</pre> <p>VSID: 0 VRID: 0 Type: VSX Gateway Name: fwvsx01 Security Policy: fwvsx01_VSX Installed at: 21Nov2019 10:30:11 SIC Status: Trust Connections number: 66 Connections peak: 765 Connections limit: 14900 <p>VSID: 1 VRID: 1 Type: Virtual System Name: fw01p Security Policy: FW_01 Installed at: 25Nov2019 11:30:39 SIC Status: Trust Connections number: 30628 Connections peak: 90464 Connections limit: 119900</p> </p></div>	VSX	vsx stat -v -l
View current shell context.	VSX	vsenv
Set context to VS ID <id>	VSX	vsenv <id>
Reset SIC for VS	VSX	vsenv <id>; fw vsx sicreset
View state tables for virtual system <id>.	VSX	vsenv <id>; fw tab -t <table>
<p>View traffic for virtual system with ID <id>.</p> <p>Attention: with fw monitor use -v instead of -vs.</p>	VSX	fw monitor -v <id> -e 'accept;'

View HA state of all configured Virtual Systems.	VSX	cphaprob state
View HA state for Virtual System ID <id>.	VSX	cphaprob -vs <id> state
Show all bond interfaces and Cluster state	VSX	cphaprob show_bond -a
Check VS bit state	VSX	vs_bits -stat All VSs are at 64 bits (R80.20 default, R80.10 need upgrade)
Show virtual devices memory usage	VSX	cpstat -f memory vsx
<p>Traffic statistic per virtual system</p> <p>See sk90860</p> <p>More information: Check Point Useful SNMP OIDs (VSX)</p>	VSX	snmpwalk -v 2c -c community 127.0.0.1 .1.3.6.1.4.1.2620.1.16.22.3 (vsxStatusMemoryUsage) SNMPv2- SMI::enterprises.2620.1.16.22.3.1.1.1. 0 = INTEGER: 0 SNMPv2- SMI::enterprises.2620.1.16.22.3.1.1.2. 0 = INTEGER: 1 SNMPv2- SMI::enterprises.2620.1.16.22.3.1.1.3. 0 = INTEGER: 2 SNMPv2- SMI::enterprises.2620.1.16.22.3.1.1.4. 0 = INTEGER: 3 SNMPv2- SMI::enterprises.2620.1.16.22.3.1.2.1. 0 = STRING: "vs0" SNMPv2- SMI::enterprises.2620.1.16.22.3.1.2.2. 0 = STRING: "vs1" SNMPv2- SMI::enterprises.2620.1.16.22.3.1.2.3. 0 = STRING: "vs2" SNMPv2- SMI::enterprises.2620.1.16.22.3.1.2.4. 0 = STRING: "vs3" SNMPv2- SMI::enterprises.2620.1.16.22.3.1.3.1. 0 = Gauge32: 0 help SNMPv2- SMI::enterprises.2620.1.16.22.3.1.3.2. 0 = Gauge32: 0 help SNMPv2- SMI::enterprises.2620.1.16.22.3.1.3.3. 0 = Gauge32: 0 help SNMPv2- SMI::enterprises.2620.1.16.22.3.1.3.4. 0 = Gauge32: 0 help

To enable monitoring CPU per-VS with OID .1.3.6.1.4.1.2620.1.16.22.4	VSX	fw vsx resctrl monitor enable
To enable monitoring memory per-VS with OID .1.3.6.1.4.1.2620.1.16.22.3 Needs a reboot!	VSX	vsx mstat enable

API specific (mgmt_cli)

API Manual: <https://sc1.checkpoint.com/documents/latest/APIs/index.html>

The mgmt_cli tool is installed as part of Gaia on all R80 gateways and can be used in scripts running in expert mode.

The mgmt_cli.exe tool is installed as part of the R80 SmartConsole installation (typically under C:\Program Files (x86)\CheckPoint\SmartConsole\R80\PROGRAM\) and can be copied to run on any Windows machine.

On Windows you cannot login with a certificate since the mgmt_cli_login is missing, you need to login with user/password or use the mgmt_cli tool on the management server.

To use the actual ssh login with mgmt_cli use the undocumented feature

```
mgmt_cli -r true
```

If your mgmt server is running on another port (ex. 8443) use

```
mgmt_cli --port 8443
```

Show api-settings

Check if clients are allowed to connect to the api and check all the api-settings.

```
mgmt_cli -r true --domain 'System Data' show api-settings
```

```
...
```

```
accepted-api-calls-from: "all ip addresses"
```

```
...
```

API Status

To confirm that the API is usable and available remotely, run the api status command. If Accessibility shows “Require all granted” it means that any system can access the API (on R80 this will show “Allow all”).

[Expert@awsmgmt:0]# api status

API Settings:

Accessibility: Require all granted
Automatic Start: Enabled

Processes:

Name	State	PID	More Information

API	Started	14472	
CPM	Started	14350	Check Point Security Management Server is running and ready
FWM	Started	13807	

Port Details:

JETTY Internal Port: 50276
APACHE Gaia Port: 443

Overall API Status: Started

API readiness test SUCCESSFUL. The server is up and ready to receive connections

Notes:

To collect troubleshooting data, please run 'api status -s <comment>'

API Status Troubleshooting data

To create a <comment>.tgz file with troubleshooting data start

```
api status -s <comment>
```

API restart

To restart the api process use the following

```
api restart
2024-Jun-21 11:59:04 - Stopping API ...
2024-Jun-21 11:59:06 - API stopped successfully.
2024-Jun-21 11:59:06 - Starting API ...
2024-Jun-21 11:59:08 - API started successfully.
```

logging in

First create a session into a file and reuse it:

```
mgmt_cli login user admin > id.txt
```

With read-only access:

```
mgmt_cli login user admin read-only true > id.txt
```

Search object in database

search objects by IP, return all objects that contain the ip explicitly or within a network address space/range.

```
mgmt_cli -s id.txt show objects filter "192.168.1.1" ip-only true --format json | jq '.objects[] | {name: .name, subnet: .subnet4, mask: ."mask-length4"}'
```

Show Hosts

```
mgmt_cli -s id.txt show hosts --format json
```

Show access layers

```
mgmt_cli show access-layers limit 500 -s id.txt --format json | jq '"access-layers"[].name'
```

Output:

```
"Layer1"
```

```
"Layer2"
```

```
...
```

Show number of rules in policy

```
mgmt_cli show access-rulebase name "<layer>" -s id.txt --format json limit 1 | jq '.total'
```


Show access rule base

```
mgmt_cli show access-rulebase offset 0 limit 20 name "Network" details-level "standard" use-object-dictionary true show-hits true hits-settings.from-date "2020-01-01" hits-settings.to-date "2020-12-31T23:59" hits-settings.target "corporate-gw" --format json
```

Display rule with explicit uid

```
mgmt_cli -s id.txt show access-rule layer "My_policy Network" uid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

Show unused objects in objects-db

```
mgmt_cli show unused-objects offset 0 limit 50 details-level "standard" -s id.txt --format json
```

Show changes from who and when in objects-db

```
mgmt_cli show changes from-date "2019-04-11T08:20:50" to-date "2019-04-15" -s id.txt --format json
```

Run script on firewall

<https://sc1.checkpoint.com/documents/latest/APIs/index.html#web/run-script~v1.6%20>

```
mgmt_cli run-script script-name "ifconfig" script "ifconfig" targets.1 "corporate-gateway" -s id.txt --format json
```

Show application-site URLs

```
mgmt_cli show application-site name "HTTPS Pass Through Global" details-level "standard" -s id.txt --version 1.2 --format json
```

Show VPN communities

```
mgmt_cli -r true show vpn-communities-star details-level full -s id.txt --format json
```

```
mgmt_cli -r true show vpn-communities-meshed details-level full -s id.txt --format json
```

Count and show access-layers (Inline Layers)

```
mgmt_cli show access-layers limit 500 --format json
```

Output:

```
.  
.br/>} 1,  
"from" : 1,  
"to" : 260,  
"total" : 260  
}
```

Links

<http://sicuriconnoi.blogspot.com/2017/11/top-checkpoint-cli-commands.html>

Check Point stattest Utility for OID Troubleshooting on GW

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_CLI_ReferenceGuide/Content/Topics-CLIG/FWG/stattest.htm

Export/Import Policy Package

Check Point ExportImportPolicyPackage tool enables you to export a policy package from a Management database to a .tar.gz file, which can then be imported into any other Management database. The tool is supported for version R80.10 and above.

This tool can be used for backups, database transfers, testing, and more.

Link: <https://github.com/CheckPointSW/ExportImportPolicyPackage>

Useful Smartlog Queries

Generic Queries

Research	SmartLog Query
Search for E-Mail Subject Note: Search without quotation marks and wildcard works for email_subject	<i>email_subject:*TEXT*</i>
Application Control Proxy Log	<i>blade:"Application Control" AND appi_name:"Web Surfen" AND *part-of-hostname*</i>
Every logs of a specific rule	<i>{ABC12345-ABC1-ABC1-ABC1-ABC123ABC12}</i>
Security Management Log Server : when logs were not able to be sent to it	<i>"were not sent to log server"</i>
Filter Logs by Geo-Location	<i>src_country:"Germany" AND src:<ip-address></i>
Alert on GW	<i>type:Alert AND origin:<fw-gwname></i>
FW Control Messages (Failover etc.)	<i>type:Control</i>
ClusterXL Control Messages, Cluster Switch over Messages	<i>type:Control ClusterXL</i>
DHCP Messages	<i>service:dhcp</i>
Address Spoofing	<i>address spoofing</i>
Find aggressive aging events	<i>aggressive aging</i>
Any TCP state errors listed in sk101221	<i>tcp (fin OR syn) NOT "both fin" NOT "established"</i> In the query field, type " tcp state " (without quotes) or any relevant text (e.g., " syn_sent ", " both fin ")
Global Broadcast	<i>dst:255.255.255.255</i>
HTTPS Inspection CRL or OCSP errors	<i>blade:"HTTPS Inspection" crl OR ocsp</i>
Certificates: any alert regarding crl (Certification Revocation List) or certificates (see sk104400 for more details)	<i>type:alert (certificate or CRL)</i>
Potential network configuration problem messages in log - See SK63160	<i>"Engine Settings - TCP"</i>
IPS Bypass Messages See discussion here: Checkmates: IPS bypass	<i>blade:IPS NOT(action: (prevent OR block)) OR "IPS Bypass Engaged" OR "IPS Bypass Disengaged"</i>

Threat Extraction / Emulation

Research	SmartLog Query
Threat Extraction	<i>blade:"Threat Extraction" AND action:Extract</i>
Threat Extraction Search for E-Mail Subject	<i>blade:"Threat Extraction" OR blade:"Threat Emulation" AND email_subject:" TTTT" OR email_subject:"TTTT"</i>
Threat Extraction show last activity	<i>blade:"Threat Extraction" AND "Content Removal" OR "Conversion to PDF"</i>
Threat Emulation show errors	<i>blade:"Threat Emulation" *"ended with verdict Error"*</i>
Threat Emulation show found threats	<i>blade:"Threat Emulation" AND severity:Critical NOT type:Correlated</i>

Endpoint Security & Remote Access

Research	SmartLog Query
Seeing tunnels activities	<i>tunnel_test or action:"Key Install" or action:"Failed Log In" OR action:"Log In" OR action:"Log Out" OR action:reject OR action:Update</i>
Connection Errors	<i>blade:vpn AND action:Reject ("endpoint" OR "user" OR "Office Mode")</i>
Errors Authenticating Users	<i>"Could not obtain user object" "IKE failure"</i>

Useful SNMP OIDs (VSX)

Check Point and SNMP

Monitoring for a Firewall is important, you need to make sure that you see the baseline of your environment and that you can see when some value will go up too high.

The following guide is showing some of the most used SNMP OID for monitoring generic HW Appliances and VSX Clusters.

To Browse the Check Point MIBS use: <https://mibs.observium.org/mib/CHECKPOINT-MIB/> or <http://oidref.com/1.3.6.1.4.1.2620>

Activate SNMP

To enable SNMP on a Check Point FW checkout the [sk90860](#)

Check Point MIB Files

MIB Files can be found in [sk90470](#)

SNMP OIDs

OIDs: Hardware Status

Hardware sensors (fans, power supplies, temperatures and raid state)

Fan status	fanSpeedSensorStatus	.1.3.6.1.4.1.2620.1.6.7.8.2.1.6
Power Supply status	powerSupplyStatus	.1.3.6.1.4.1.2620.1.6.7.9.1.1.2

Raid status	raidDiskState	.1.3.6.1.4.1.2620.1.6.7.7.2.1.9
Temperature status	tempertureSensorTable	.1.3.6.1.4.1.2620.1.6.7.8.1

```
snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 CHECKPOINT-MIB::fanSpeedSensorStatus
CHECKPOINT-MIB::fanSpeedSensorStatus.1.0 = INTEGER: 0
CHECKPOINT-MIB::fanSpeedSensorStatus.2.0 = INTEGER: 0
CHECKPOINT-MIB::fanSpeedSensorStatus.3.0 = INTEGER: 0
CHECKPOINT-MIB::fanSpeedSensorStatus.4.0 = INTEGER: 0
```

```
snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 CHECKPOINT-MIB::powerSupplyStatus
CHECKPOINT-MIB::powerSupplyStatus.1.0 = STRING: Up
CHECKPOINT-MIB::powerSupplyStatus.2.0 = STRING: Up
```

```
snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 CHECKPOINT-MIB::tempertureSensorTable
CHECKPOINT-MIB::tempertureSensorIndex.1.0 = INTEGER: 1
CHECKPOINT-MIB::tempertureSensorIndex.2.0 = INTEGER: 2
CHECKPOINT-MIB::tempertureSensorIndex.3.0 = INTEGER: 3
CHECKPOINT-MIB::tempertureSensorIndex.4.0 = INTEGER: 4
CHECKPOINT-MIB::tempertureSensorName.1.0 = STRING: CPU0 Temp
CHECKPOINT-MIB::tempertureSensorName.2.0 = STRING: CPU1 Temp
CHECKPOINT-MIB::tempertureSensorName.3.0 = STRING: Intake Temp
CHECKPOINT-MIB::tempertureSensorName.4.0 = STRING: Outlet Temp
CHECKPOINT-MIB::tempertureSensorValue.1.0 = STRING: 65.50
CHECKPOINT-MIB::tempertureSensorValue.2.0 = STRING: 65.00
CHECKPOINT-MIB::tempertureSensorValue.3.0 = STRING: 30.38
CHECKPOINT-MIB::tempertureSensorValue.4.0 = STRING: 31.50
CHECKPOINT-MIB::tempertureSensorUnit.1.0 = STRING: Celsius
CHECKPOINT-MIB::tempertureSensorUnit.2.0 = STRING: Celsius
CHECKPOINT-MIB::tempertureSensorUnit.3.0 = STRING: Celsius
CHECKPOINT-MIB::tempertureSensorUnit.4.0 = STRING: Celsius
CHECKPOINT-MIB::tempertureSensorType.1.0 = STRING: Temperature
CHECKPOINT-MIB::tempertureSensorType.2.0 = STRING: Temperature
CHECKPOINT-MIB::tempertureSensorType.3.0 = STRING: Temperature
CHECKPOINT-MIB::tempertureSensorType.4.0 = STRING: Temperature
CHECKPOINT-MIB::tempertureSensorStatus.1.0 = INTEGER: 0
CHECKPOINT-MIB::tempertureSensorStatus.2.0 = INTEGER: 0
CHECKPOINT-MIB::tempertureSensorStatus.3.0 = INTEGER: 0
CHECKPOINT-MIB::tempertureSensorStatus.4.0 = INTEGER: 0
```

```
snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 CHECKPOINT-MIB::raidDiskState
CHECKPOINT-MIB::raidDiskState.1.0 = INTEGER: 0
CHECKPOINT-MIB::raidDiskState.2.0 = INTEGER: 0
```

OIDs: Connections

Current connections in certain virtual system and the configured limit.

This limit is configured in the virtual system properties, Optimization section (Capacity Optimization)

<https://somoit.net/wp-content/uploads/2019/05/checkpoint-useful-snmp-oids-to-monitor-1.png>

Connections	fwNumConn.0	.1.3.6.1.4.1.2620.1.1.25.3.0
Connections limit	fwConnTableLimit.0	.1.3.6.1.4.1.2620.1.1.25.10.0

```
snmpwalk -v 3 -l authNoPriv -u user -A pass -n ctxname_vsid2 vsx1 CHECKPOINT-  
MIB::fwNumConn.0  
CHECKPOINT-MIB::fwNumConn.0 = Gauge32: 64121
```

```
snmpwalk -v 3 -l authNoPriv -u user -A pass -n ctxname_vsid2 vsx1 CHECKPOINT-  
MIB::fwConnTableLimit.0  
CHECKPOINT-MIB::fwConnTableLimit.0 = Gauge32: 199900
```

OIDs: ClusterXL state

If you manage a Checkpoint ClusterXL, I suppose you use quite a lot the “cphaprob state” command.

ClusterXLState	haState	.1.3.6.1.4.1.2620.1.5.6.0
----------------	---------	---------------------------

```
snmpwalk -v 3 -l authNoPriv -u user -A pass -n ctxname_vsid2 vsx1 CHECKPOINT-MIB::haState.0  
CHECKPOINT-MIB::haState.0 = STRING: standby
```

OIDs: CPU

Monitor each of the CPUs

CPUCores	multiProcUsage	.1.3.6.1.4.1.2620.1.6.7.5.1.5
----------	----------------	-------------------------------

```
/usr/bin/snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 CHECKPOINT-MIB::multiProcUsage  
CHECKPOINT-MIB::multiProcUsage.1.0 = Gauge32: 7  
CHECKPOINT-MIB::multiProcUsage.2.0 = Gauge32: 2  
CHECKPOINT-MIB::multiProcUsage.3.0 = Gauge32: 8
```


CHECKPOINT-MIB::multiProcUsage.4.0 = Gauge32: 8
CHECKPOINT-MIB::multiProcUsage.5.0 = Gauge32: 7
CHECKPOINT-MIB::multiProcUsage.6.0 = Gauge32: 7
CHECKPOINT-MIB::multiProcUsage.7.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.8.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.9.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.10.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.11.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.12.0 = Gauge32: 6
CHECKPOINT-MIB::multiProcUsage.13.0 = Gauge32: 5
CHECKPOINT-MIB::multiProcUsage.14.0 = Gauge32: 5
CHECKPOINT-MIB::multiProcUsage.15.0 = Gauge32: 5

OIDs: Memory

Counters

RAM - Real Total	memTotalReal64	.1.3.6.1.4.1.2620.1.6.7.4.3
RAM - Real Active	memActiveReal64	.1.3.6.1.4.1.2620.1.6.7.4.4
RAM - Real Free	memFreeReal64	.1.3.6.1.4.1.2620.1.6.7.4.5
RAM - Virtual Total	memTotalVirtual64	.1.3.6.1.4.1.2620.1.6.7.4.1
RAM - Virtual Active	memActiveVirtual64	.1.3.6.1.4.1.2620.1.6.7.4.2
Hmem fails	fwHmem-failed-alloc	.1.3.6.1.4.1.2620.1.1.26.1.21
System Kmem fails	fwKmem-failed-alloc	.1.3.6.1.4.1.2620.1.1.26.2.15

Traps

Swap memory utilization alert	chkpntSwapMemoryTrap	.1.3.6.1.4.1.2620.1.2000.4.1
Real memory utilization alert	chkpntRealMemoryTrap	.1.3.6.1.4.1.2620.1.2000.4.2

OIDs: Memory VSX

The following SNMP queries have to be done on the VSX Host.

RAM - Memory Usage VS ID	vsxStatusMemoryUsageVSId	.1.3.6.1.4.1.2620.1.16.22.3.1.1
--------------------------	--------------------------	---------------------------------

RAM - Memory Usage VS Name	vsxStatusMemoryUsageVSName	.1.3.6.1.4.1.2620.1.16.22.3.1.2
RAM - Memory Usage per VS	vsxStatusMemoryUsage	.1.3.6.1.4.1.2620.1.16.22.3.1.3

```
/usr/bin/snmpwalk -v 3 -l authNoPriv -u user -A pass vsx1 SNMPv2-SMI::enterprises.2620.1.16.22.3
```

```
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.1.0 = INTEGER: 0
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.2.0 = INTEGER: 1
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.3.0 = INTEGER: 2
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.4.0 = INTEGER: 3
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.5.0 = INTEGER: 4
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.6.0 = INTEGER: 5
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.1.7.0 = INTEGER: 6
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.1.0 = STRING: "fwvsx01"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.2.0 = STRING: "fw01"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.3.0 = STRING: "fw02"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.4.0 = STRING: "swi01"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.5.0 = STRING: "swi02"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.6.0 = STRING: "fw03"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.2.7.0 = STRING: "fw04"
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.1.0 = Gauge32: 1995131
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.2.0 = Gauge32: 335056
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.3.0 = Gauge32: 1126517
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.4.0 = Gauge32: 98547
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.5.0 = Gauge32: 64391
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.6.0 = Gauge32: 103978
SNMPv2-SMI::enterprises.2620.1.16.22.3.1.3.7.0 = Gauge32: 86436
```

Links

Thank you for this BLOG entry somoit.net:

<https://somoit.net/checkpoint-fw/useful-snmp-oids-monitor-vsx>

Threat Prevention API

Threat Prevention APIs

Take control of the Threat Prevention APIs powered by the largest Threat Cloud in the industry

URL Reputation – for a domain/URL returns the classification and risk in accessing the resource

File Reputation – for a file digest (md5/sha1/sha256/sha512) returns the risk in downloading the file without the need to scan it

IP Reputation – for an IP address returns it's classification and risk in accessing a resource hosted on it

Mail Security – upload an email for scanning against malware and phishing attacks, based on award winning Sandblast engines

All APIs are RESTful, simple to use and can be integrated as part of a SOAR application, home-made application and more!

Detailed API instructions including samples in Java/Python can now be found in the GitHub repository.

Check it out here - <https://github.com/CheckPointSW/reputation-service-api>

Swagger UI to explore the API

<https://app.swaggerhub.com/apis-docs/cp-devops-cloud/reputation-service>

GAIA - Easy execute CLI commands on all gateways simultaneously

Link

<https://community.checkpoint.com/t5/Enterprise-Appliances-and-Gaia/GAIA-Easy-execute-CLI-commands-on-all-gateways-simultaneously/m-p/50883>

Threat Prevention Cyber Attacks Dashboard Template

If you have Anti-Bot, Anti-Virus, IPS, Threat Emulation Blades active and a SmartLog License, you're maybe interested to see the following Dashboard:

image-1604935138774.png

image-1604935159991.png

image-1604935178173.png

Description and Download of the Template here:

<https://community.checkpoint.com/community/management/visibility-monitoring/blog/2018/04/04/threat-prevention-cyber-attacks-dashboard>

DOS & DDOS Prevention, Mitigation

Preface

Since R80.20 DOS/DDOS Prevention changed in Check Point.

The following is a summary how you can setup and mitigate DOS & DDOS attacks.

SYN Defender since R80.20

Important changes in IPS "SYN Attack" (SYN Defender) protection for R80.20 and above

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120476

How to configure Rate Limiting rules for DoS Mitigation (R80.20 and newer)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112454

Mitigation

How to configure Security Gateway to detect and prevent port scan

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110873&partition=Advanced&product=Security

How to create and view Suspicious Activity Monitoring (SAM) Rules

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112061

Best practice

- Set "Host Scan" and "Sweep Scan" in IPS Policy to "User Alert 1".
- In Global Settings on Smartcenter at "User Alert 1" 120 seconds blocking of source ip run via script

```
sam_alert -t 120 -l -src
```

Export Syslog Messages

Export Syslog Messages

How to export syslog messages from Gaia Security Gateway to a Log Server and view them in SmartView Tracker

https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk102995

Syslog from LOM Interface

At the moment it seems that syslog cannot be sent from Check Point LOM Interface.

Missing feature - Global search across multiple CMA

Preface

Before R80.x in a MDM (Multi Domain Management) you could do a search where an object is used in all the CMA's.

Until now (R80.30) this feature is not included in SmartConsole anymore.

Script solution

- <https://github.com/WadesWeaponShed/Global-IP-Search-MDS>
- <https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/MDS-Global-search-across-CMAs-by-IP/m-p/75906>
- <https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Search-multiple-CMA/m-p/35237>

The Script

```
#!/bin/sh

JQ=${CPDIR}/jq/jq

OBJECT_NAME=$1
DOMAINS_FILE="domains.json"
PACKAGES_FILE="packages.json"
PACKAGE_FILE="package.json"

echo 'Getting a list of domains...'
mgmt_cli -r true -d MDS show domains limit 500 --format json > $DOMAINS_FILE
if [ $? -eq 1 ]; then
    echo "Error getting list of domains. Aborting!"
    exit 1
fi
```

```
DOMAINS_NAMES=$(($JQ -r ".objects[] | .name" $DOMAINS_FILE))
```

```
echo 'Searching for object "'$OBJECT_NAME'" in all domains...'
```

```
FOUND=0
```

```
OBJECT_UID=""
```

```
for DOMAIN in ${DOMAINS_NAMES[@]}
```

```
do
```

```
  echo 'Searching in domain "'$DOMAIN'..."'
```

```
  mgmt_cli -r true -d "$DOMAIN" show objects offset 0 limit 1 in.1 name in.2 "$OBJECT_NAME" --format json >
```

```
$OBJECT_NAME.json
```

```
  if [ $? -ne 1 ]; then
```

```
    OBJECT_COUNT=$(($JQ -r ".total" $OBJECT_NAME.json)
```

```
    if [ $OBJECT_COUNT -ne 0 ]; then
```

```
      FOUND=1
```

```
      OBJECT_UID=$(($JQ -r ".objects[0].uid" $OBJECT_NAME.json)
```

```
      echo 'Found in domain "'$DOMAIN'!!!'
```

```
      break
```

```
    fi
```

```
  fi
```

```
done
```

```
if [ $FOUND -ne 1 ]; then
```

```
  echo 'Object "'$OBJECT_NAME'" does not exist. Aborting!'
```

```
  exit 1
```

```
fi
```

```
echo 'Searching for object "'$OBJECT_NAME'" usages in all policy packages in all domains...'
```

```
for DOMAIN in ${DOMAINS_NAMES[@]}
```

```
do
```

```
  echo 'Searching in domain "'$DOMAIN'..."'
```

```
  mgmt_cli -r true -d "$DOMAIN" show packages limit 500 --format json > $PACKAGES_FILE
```

```
  if [ $? -ne 1 ]; then
```

```
    PACKAGES_NAMES=$(($JQ -r ".packages[] | .name" $PACKAGES_FILE))
```

```
    for PACKAGE in ${PACKAGES_NAMES[@]}
```

```
    do
```

```
      echo 'Searching in package "'$PACKAGE'..."'
```

```
      mgmt_cli -r true -d "$DOMAIN" show-package name $PACKAGE --format json > $PACKAGE_FILE
```

```
      if [ $? -ne 1 ]; then
```

```
ACCESS_LAYERS=$(($JQ '["access-layers"][] | .name' -r $PACKAGE_FILE))
for LAYER in ${ACCESS_LAYERS[@]}
do
    mgmt_cli -r true -d "$DOMAIN" show access-rulebase package "$PACKAGE" name "$LAYER" offset 0 limit 1
filter $OBJECT_UID --format json > $OBJECT_NAME.json
    if [ $? -ne 1 ]; then
        OBJECT_COUNT=$(($JQ -r ".total" $OBJECT_NAME.json)
        if [ $OBJECT_COUNT -ne 0 ]; then
            echo 'The requested object is used in policy package "'$PACKAGE'"
            break
        fi
    fi
done
fi
done
fi
done
echo 'Done!'
```

Show logging using the web interface

If you need to view Logs over the Web in Check Point you can use SmartView.

Available since R80 but not enabled per default. In R80.10 it is enabled per default and you can access it with your SmartConsole Credentials.

It looks like this in the Browser:

image-1604935250608.png

Also see here: <https://community.checkpoint.com/thread/5212-smartview-accessing-check-point-logs-from-web>

Managing partition sizes via LVM manager on Gaia OS

Partition Resize

Since R77.30 *lvm_manager* is included in Gaia OS and can be used to resize logical volumes on the system.

Check [Managing partition sizes via LVM manager on Gaia OS \(sk95566\)](#) for more information.

Partition Sizes when installing Gaia OS

When installing Gaia OS there is an option to change the partition sizes.
Don't use default sizes as they are for minimal usage.

Screenshot:

<https://sc1.checkpoint.com/sc//SolutionsStatics/sk92303/R801905210741.30-gaia.png>

Check this Link: [How to configure partition sizes during Gaia installation \(sk92303\)](#)

SmartConsole cli parameters

In R77.30 you could use command line parameters to specify username/password like this:

```
FwPolicy.exe connect %Hostname% %Username%
```

Since R80.10 you need to do the following:

```
SmartConsole.exe -p SmartConsole.LoginParams
```

Here is the SmartConsole.LoginParams example file:

```
<RemoteLaunchParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Username>admin</Username>
  <Password>password</Password>
  <ServerIP>1.2.3.4</ServerIP>
  <DomainName>LocationDomain</DomainName>
  <ReadOnly>False</ReadOnly>
  <CloudDemoMode>False</CloudDemoMode>
</RemoteLaunchParameters>
```

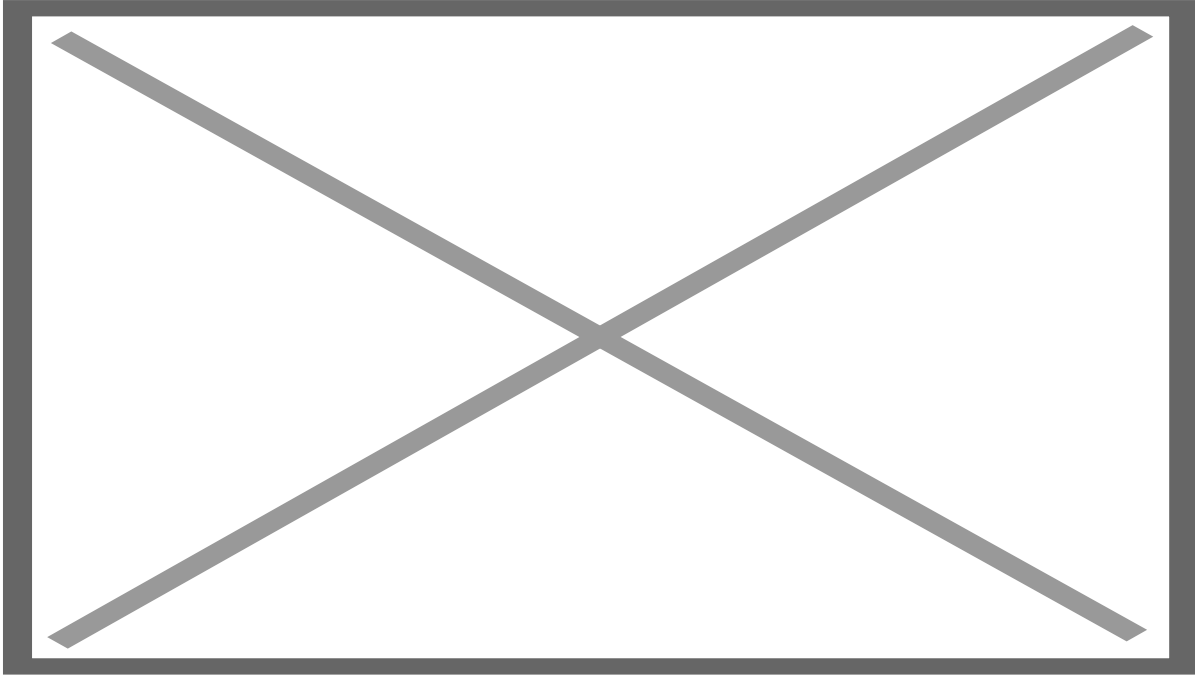
For non-mds connection you need to leave "DomainName" field empty.

Link: <https://community.checkpoint.com/thread/6432-command-line-arguments-to-r8010-smartconsoleexe>

Jump to Rule Number or UID

In R80.10 you can jump directly to a rule number or a rule-UID.

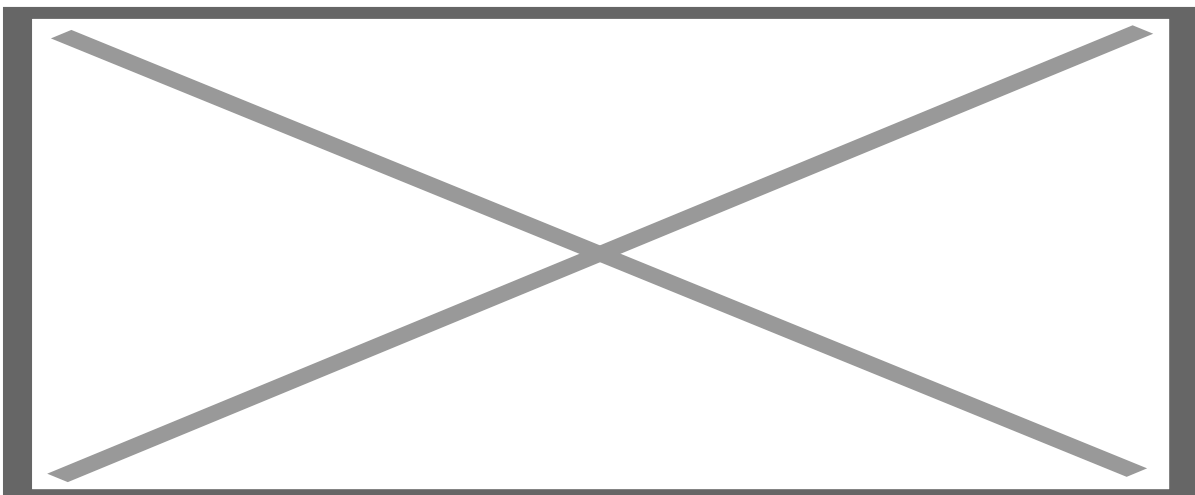
With Ctrl-G you get the following:



You can copy the UID from a rule:



Or search for an rule-UID:



Perfect to use in documentations, just use the rule-UID or sometimes I also use the
<FW_RuleName: FW_RuleName> Tag for documentation.

SmartConsole: Clear disconnected sessions

Howto clear disconnected sessions

If several SmartConsole disconnected (stale) sessions that cannot be discarded, see this here:

<https://community.checkpoint.com/t5/General-Management-Topics/clear-disconnected-sessions/td-p/33027>

Postgresql Queries

View

```
psql_client cpm postgres -c "select  
applicationname,objid,creator,state,numberoflocks,numberofoperations,creationtime,lastmodifytime  
from worksession  
where state = 'OPEN'  
and (numberoflocks != '0'  
or numberofoperations != '0');"
```

Clear

```
mgmt_cli discard --port 4434 uid 4b2ac7a8-9b0b-4e39-a3f0-4c065d631cdf  
Username: admin  
Password:  
number-of-discarded-changes: 2  
message: "OK"
```

Initiating manual cluster failover

This command lets you initiate a manual cluster failover (see [sk55081](#)).

Syntax

Shell	Command
Gaia Clish	<code>set cluster member admin {down up}</code>
Expert mode	<code>clusterXL_admin {down up}</code>

Example

```
[Expert@Member1:0]# cphaprob state
```

```
Cluster Mode:  High Availability (Active Up) with IGMP Membership
```

ID	Unique Address	Assigned Load	State	Name
1 (local)	11.22.33.245	100%	ACTIVE	Member1
2	11.22.33.246	0%	STANDBY	Member2

```
Active PNOTEs: None
```

```
... ..
```

```
[Expert@Member1:0]#
```

```
[Expert@Member1:0]# clusterXL_admin down
```

This command does not survive reboot. To make the change permanent, please run 'set cluster member admin down/up permanent' in clish or add '-p' at the end of the command in expert mode

Setting member to administratively down state ...

Member current state is DOWN

[Expert@Member1:0]#

[Expert@Member1:0]# cphaprob state

Cluster Mode: High Availability (Active Up) with IGMP Membership

ID	Unique Address	Assigned Load	State	Name
1 (local)	11.22.33.245	0%	DOWN	Member1
2	11.22.33.246	100%	ACTIVE	Member2

Active PNOTEs: ADMIN

Last member state change event:

Event Code: CLUS-111400
State change: ACTIVE -> DOWN
Reason for state change: ADMIN_DOWN PNOTE
Event time: Sun Sep 8 19:35:06 2019

Last cluster failover event:

Transition to new ACTIVE: Member 1 -> Member 2
Reason: ADMIN_DOWN PNOTE
Event time: Sun Sep 8 19:35:06 2019

Cluster failover count:

Failover counter: 2
Time of counter reset: Sun Sep 8 16:08:34 2019 (reboot)

[Expert@Member1:0]#

[Expert@Member1:0]# clusterXL_admin up

This command does not survive reboot. To make the change permanent, please run 'set cluster member admin down/up permanent' in clish or add '-p' at the end of the command in expert mode

Setting member to normal operation ...

Member current state is STANDBY

[Expert@Member1:0]#

[Expert@Member1:0]# cphaprob state

Cluster Mode: High Availability (Active Up) with IGMP Membership

ID	Unique Address	Assigned Load	State	Name
1 (local)	11.22.33.245	0%	STANDBY	Member1
2	11.22.33.246	100%	ACTIVE	Member2

Active PNOTEs: None

Last member state change event:

Event Code: CLUS-114802

State change: DOWN -> STANDBY

Reason for state change: There is already an ACTIVE member in the cluster (member 2)

Event time: Sun Sep 8 19:37:03 2019

Last cluster failover event:

Transition to new ACTIVE: Member 1 -> Member 2

Reason: ADMIN_DOWN PNOTE

Event time: Sun Sep 8 19:35:06 2019

Cluster failover count:

Failover counter: 2

Time of counter reset: Sun Sep 8 16:08:34 2019 (reboot)

[Expert@Member1:0]#

How to migrate Custom Queries from one SmartView Tracker to another

Problem

To do administration of IPS and other modules of the check point firewall, you often need to check logs with smartlog queries.

These queries are saved then to favorites for later use.

image.png

Migration

To migrate these queries to a new user account on the same management server or to another smartview tracker you need to know where this data is stored.

The favorites queries data is stored here:

```
$SMARTLOGDIR/data/users_settings/<username>/Bookmarks_Custom.xml
```

The file Bookmarks_Custom.xml can just be copied to the location of the new user.
After a restart of the smartconsole the favorite queries are visible again.

Links

More info also here in [sk39268](#)

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"
```

```
cp_log_export restart
```

Link

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