Check Point CHECKMATES
Learn. Share. Inspire.

Best of Code Hub Contributions

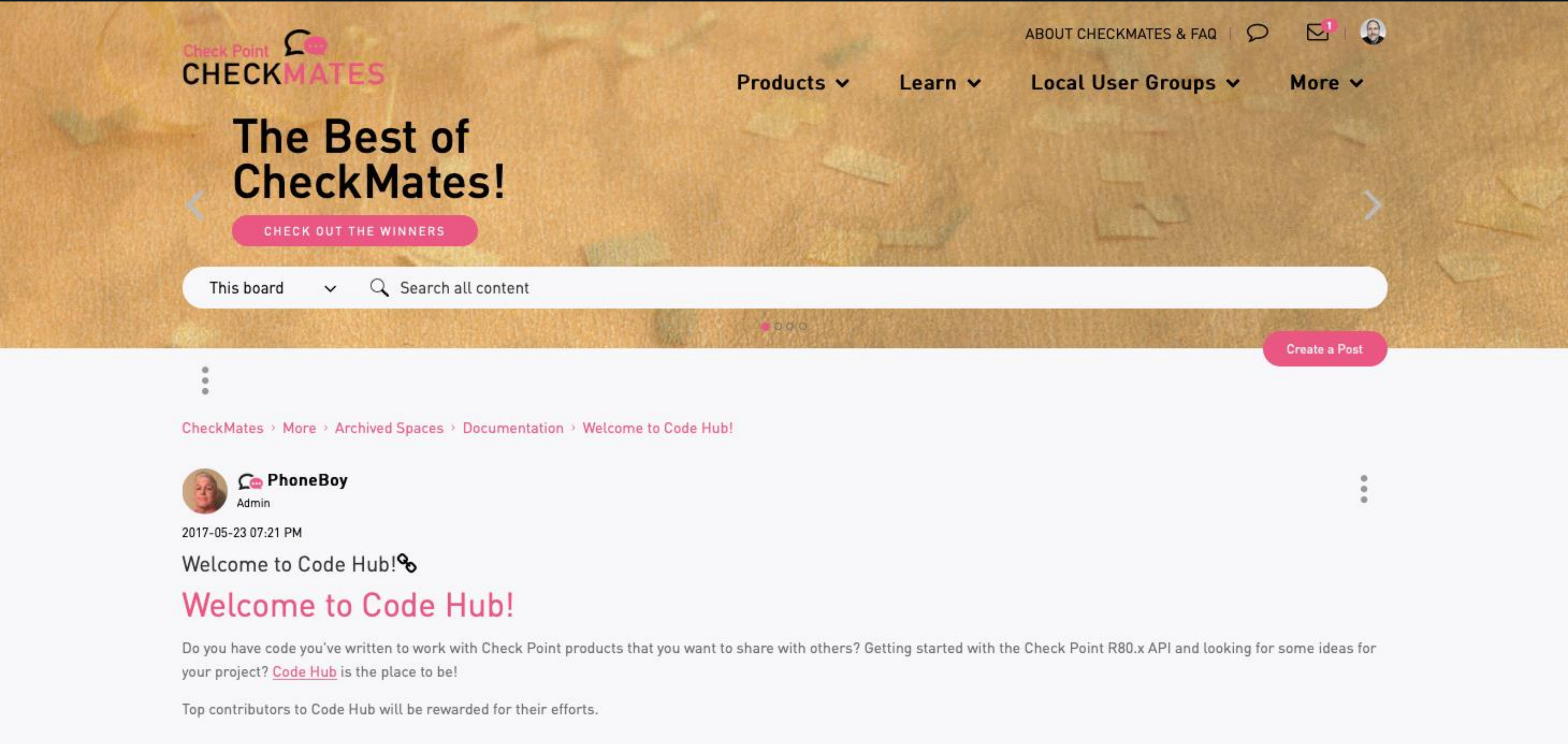
Danny Jung

Code Hub Contribution Winner 2018 / 2019

ESC.de

Check Point CHECKMATES

Learn. Share. Inspire.



PhoneBoy
Admin

2017-05-23 07:21 PM

Welcome to Code Hub!

Welcome to Code Hub!

Do you have code you've written to work with Check Point products that you want to share with others? Getting started with the Check Point R80.x API and looking for some ideas for your project? Code Hub is the place to be!

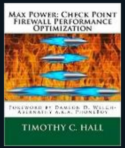
Top contributors to Code Hub will be rewarded for their efforts.

CHECKMATES

Common Check Point Commands

by **Danny Jung**

https://community.checkpoint.com/t5/General-Topics/Common-Check-Point-Commands-ccc/m-p/38488



CHECKMATES Winner 2018

Environment:

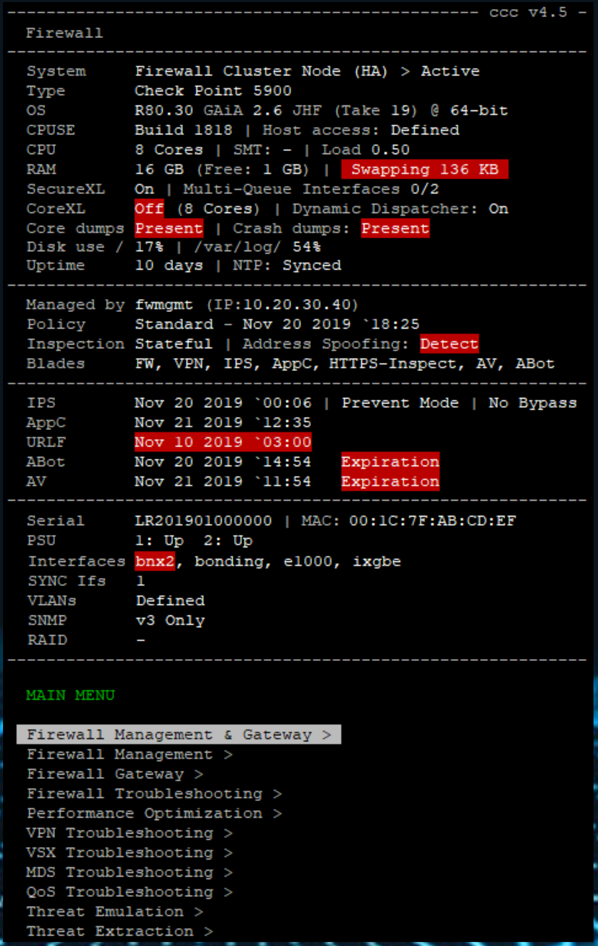
GAiA

Runs at:

Bash (Expert mode)

Result:

System info + Interactive CLI



```
---------------------------------------------- ccc v4.5 -
 Firewall
---------------------------------------------------------
 System     Firewall Cluster Node (HA) > Active
 Type       Check Point 5900
 OS         R80.30 GAiA 2.6 JHF (Take 19) @ 64-bit
 CPUSE      Build 1818 | Host access: Defined
 CPU        8 Cores | SMT: - | Load 0.50
 RAM        16 GB (Free: 1 GB) |  Swapping 136 KB
 SecureXL   On | Multi-Queue Interfaces 0/2
 CoreXL     Off (8 Cores) | Dynamic Dispatcher: On
 Core dumps Present | Crash dumps: Present
 Disk use / 17% | /var/log/ 54%
 Uptime     10 days | NTP: Synced
---------------------------------------------------------
 Managed by fwmgmt (IP:10.20.30.40)
 Policy     Standard - Nov 20 2019 `18:25
 Inspection Stateful | Address Spoofing: Detect
 Blades     FW, VPN, IPS, AppC, HTTPS-Inspect, AV, ABot
---------------------------------------------------------
 IPS        Nov 20 2019 `00:06 | Prevent Mode | No Bypass
 AppC       Nov 21 2019 `12:35
 URLF       Nov 10 2019 `03:00
 ABot       Nov 20 2019 `14:54   Expiration
 AV         Nov 21 2019 `11:54   Expiration
---------------------------------------------------------
 Serial     LR201901000000 | MAC: 00:1C:7F:AB:CD:EF
 PSU        1: Up  2: Up
 Interfaces bnx2, bonding, e1000, ixgbe
 SYNC Ifs   1
 VLANs      Defined
 SNMP       v3 Only
 RAID       -
---------------------------------------------------------

 MAIN MENU

 Firewall Management & Gateway >
 Firewall Management >
 Firewall Gateway >
 Firewall Troubleshooting >
 Performance Optimization >
 VPN Troubleshooting >
 VSX Troubleshooting >
 MDS Troubleshooting >
 QoS Troubleshooting >
 Threat Emulation >
 Threat Extraction >
```

Benefits:

System-aware info screen, menu-driven navigation through available commands, hosts other Code Hub solutions, supports VSX environments

Intended for:

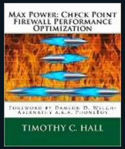
All

CHECKMATES

Common Check Point Commands

by **Danny Jung**

https://community.checkpoint.com/t5/General-Topics/Common-Check-Point-Commands-ccc/m-p/38488



CHECKMATES Winner 2018

Environment:

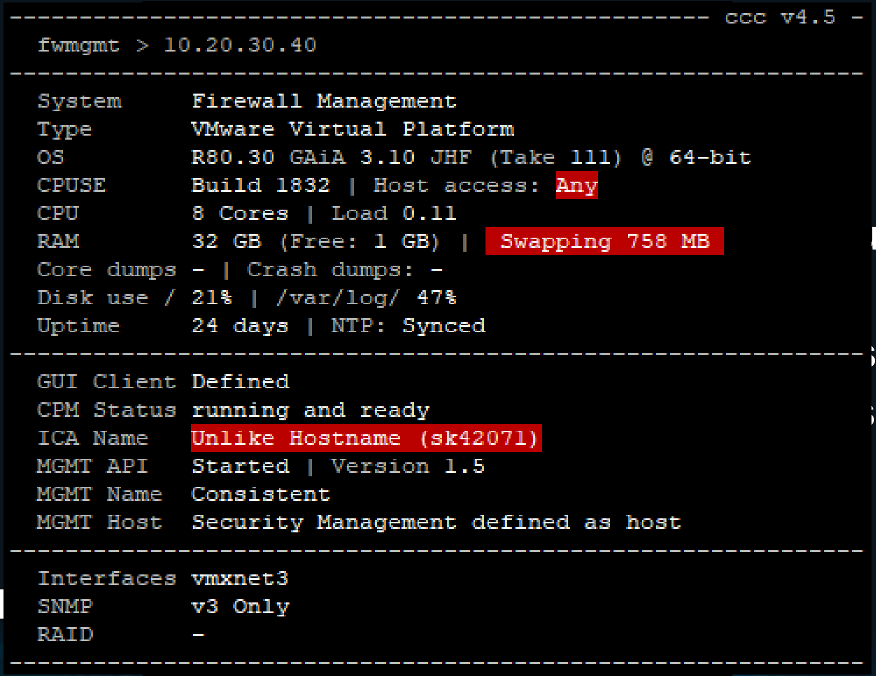
GAiA

Runs at:

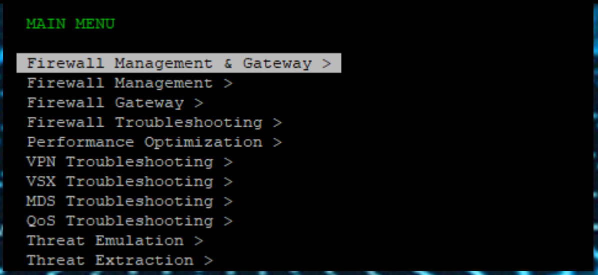
Bash **(Expert mode)**

Result:

System info + Interactive Cl



```
----------------------------------------------------- ccc v4.5 -
  fwmgmt > 10.20.30.40
-----------------------------------------------------------------
  System      Firewall Management
  Type        VMware Virtual Platform
  OS          R80.30 GAiA 3.10 JHF (Take 111) @ 64-bit
  CPUSE       Build 1832 | Host access: Any
  CPU         8 Cores | Load 0.11
  RAM         32 GB (Free: 1 GB) |  Swapping 758 MB
  Core dumps  - | Crash dumps: -
  Disk use /  21% | /var/log/ 47%
  Uptime      24 days | NTP: Synced
-----------------------------------------------------------------
  GUI Client  Defined
  CPM Status  running and ready
  ICA Name    Unlike Hostname (sk42071)
  MGMT API    Started | Version 1.5
  MGMT Name   Consistent
  MGMT Host   Security Management defined as host
-----------------------------------------------------------------
  Interfaces  vmxnet3
  SNMP        v3 Only
  RAID        -
-----------------------------------------------------------------
```



```
MAIN MENU

Firewall Management & Gateway >
Firewall Management >
Firewall Gateway >
Firewall Troubleshooting >
Performance Optimization >
VPN Troubleshooting >
VSX Troubleshooting >
MDS Troubleshooting >
QoS Troubleshooting >
Threat Emulation >
Threat Extraction >
```

Benefits:

System-aware info screen,
-driven navigation through
available commands,
other Code Hub solutions,
upports VSX environments

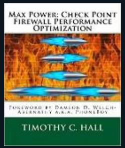
Intended for:

All

Common Check Point Commands

by **Danny Jung**

https://community.checkpoint.com/t5/General-Topics/Common-Check-Point-Commands-ccc/m-p/38488


MAX POWER: CHECK POINT FIREWALL PERFORMANCE OPTIMIZATION

TIMOTHY C. HALL

Environment:

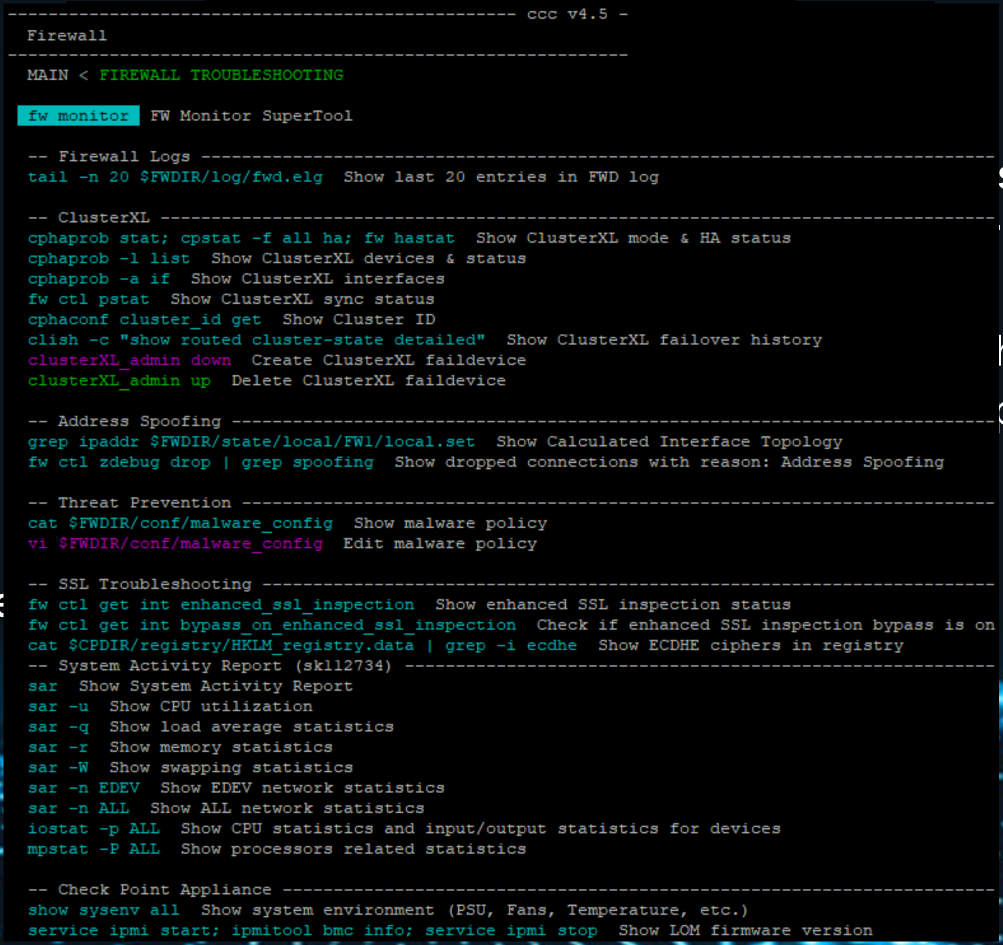
GAiA

Runs at:

Bash (Expert mode)

Result:

System info + Interactive



```
------------------------------------------------- ccc v4.5 -
  Firewall
-------------------------------------------------------------
  MAIN < FIREWALL TROUBLESHOOTING

  fw monitor  FW Monitor SuperTool

  -- Firewall Logs ------------------------------------------------------------------
  tail -n 20 $FWDIR/log/fwd.elg  Show last 20 entries in FWD log

  -- ClusterXL ----------------------------------------------------------------------
  cphaprob stat; cpstat -f all ha; fw hastat  Show ClusterXL mode & HA status
  cphaprob -l list  Show ClusterXL devices & status
  cphaprob -a if  Show ClusterXL interfaces
  fw ctl pstat  Show ClusterXL sync status
  cphaconf cluster_id get  Show Cluster ID
  clish -c "show routed cluster-state detailed"  Show ClusterXL failover history
  clusterXL_admin down  Create ClusterXL faildevice
  clusterXL_admin up  Delete ClusterXL faildevice

  -- Address Spoofing ---------------------------------------------------------------
  grep ipaddr $FWDIR/state/local/FW1/local.set  Show Calculated Interface Topology
  fw ctl zdebug drop | grep spoofing  Show dropped connections with reason: Address Spoofing

  -- Threat Prevention --------------------------------------------------------------
  cat $FWDIR/conf/malware_config  Show malware policy
  vi $FWDIR/conf/malware_config  Edit malware policy

  -- SSL Troubleshooting ------------------------------------------------------------
  fw ctl get int enhanced_ssl_inspection  Show enhanced SSL inspection status
  fw ctl get int bypass_on_enhanced_ssl_inspection  Check if enhanced SSL inspection bypass is on
  cat $CPDIR/registry/HKLM_registry.data | grep -i ecdhe  Show ECDHE ciphers in registry
  -- System Activity Report (sk112734) ----------------------------------------------
  sar  Show System Activity Report
  sar -u  Show CPU utilization
  sar -q  Show load average statistics
  sar -r  Show memory statistics
  sar -W  Show swapping statistics
  sar -n EDEV  Show EDEV network statistics
  sar -n ALL  Show ALL network statistics
  iostat -p ALL  Show CPU statistics and input/output statistics for devices
  mpstat -P ALL  Show processors related statistics

  -- Check Point Appliance ----------------------------------------------------------
  show sysenv all  Show system environment (PSU, Fans, Temperature, etc.)
  service ipmi start; ipmitool bmc info; service ipmi stop  Show LOM firmware version
```

Benefits:

stem-aware info screen,
iven navigation through
available commands,
her Code Hub solutions,
ports VSX environments

Intended for:

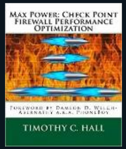
All

CHECKMATES

Comm nds

by **Danny Jung**

https://community.checkpoint.co


Max Power: Check Point Firewall Performance Optimization
Foreword by Dameon D. Welch-Abernathy a.k.a. PhoneBoy
Timothy C. Hall

CHECKMATES Winner 2018

Environment:

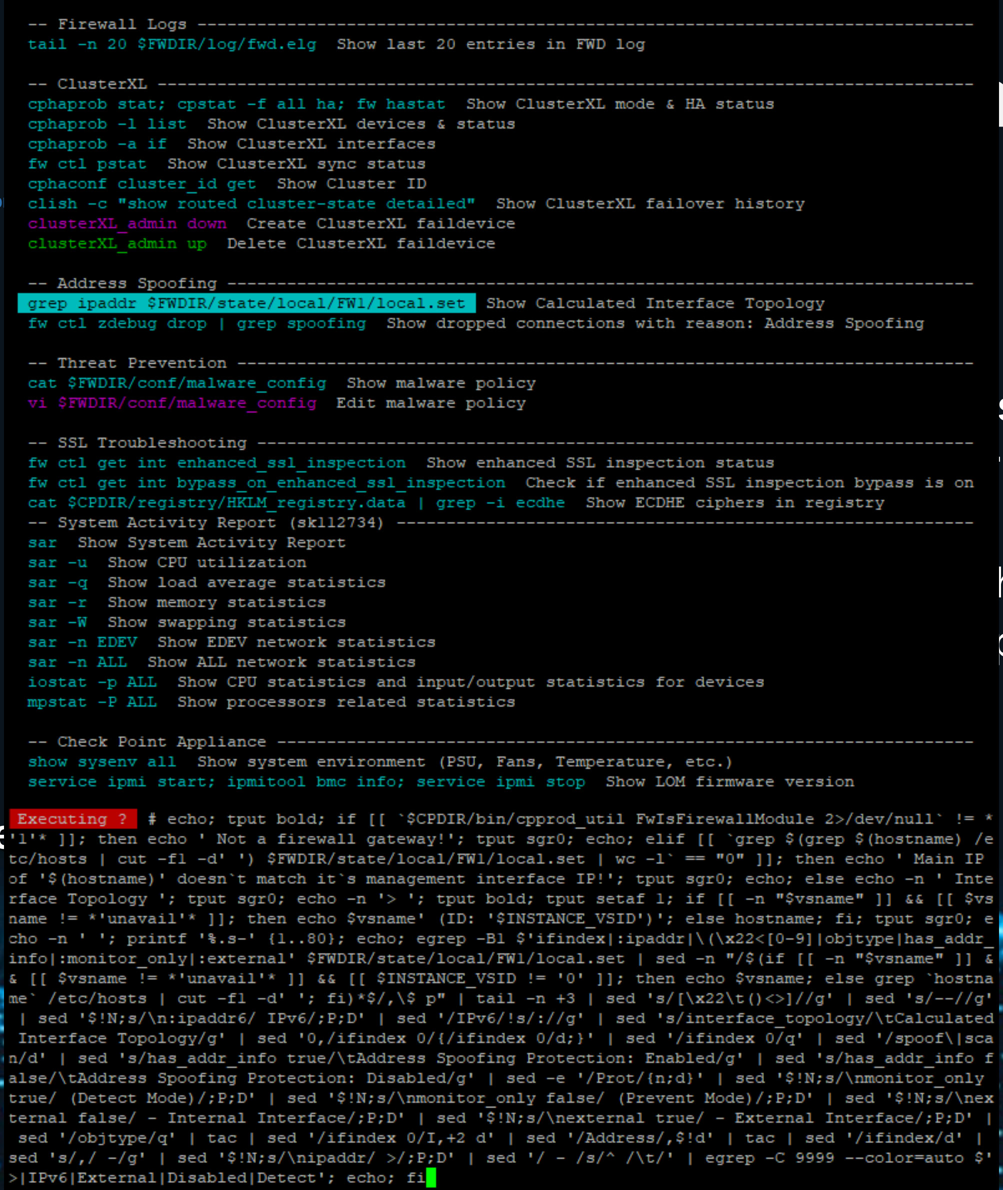
GAiA

Runs at:

Bash (Expert mode)

Result:

System info + Interactive



```
-- Firewall Logs ------------------------------------------------------------------------
tail -n 20 $FWDIR/log/fwd.elg  Show last 20 entries in FWD log

-- ClusterXL ----------------------------------------------------------------------------
cphaprob stat; cpstat -f all ha; fw hastat  Show ClusterXL mode & HA status
cphaprob -l list  Show ClusterXL devices & status
cphaprob -a if  Show ClusterXL interfaces
fw ctl pstat  Show ClusterXL sync status
cphaconf cluster_id get  Show Cluster ID
clish -c "show routed cluster-state detailed"  Show ClusterXL failover history
clusterXL_admin down  Create ClusterXL faildevice
clusterXL_admin up  Delete ClusterXL faildevice

-- Address Spoofing ---------------------------------------------------------------------
grep ipaddr $FWDIR/state/local/FW1/local.set  Show Calculated Interface Topology
fw ctl zdebug drop | grep spoofing  Show dropped connections with reason: Address Spoofing

-- Threat Prevention --------------------------------------------------------------------
cat $FWDIR/conf/malware_config  Show malware policy
vi $FWDIR/conf/malware_config  Edit malware policy

-- SSL Troubleshooting ------------------------------------------------------------------
fw ctl get int enhanced_ssl_inspection  Show enhanced SSL inspection status
fw ctl get int bypass_on_enhanced_ssl_inspection  Check if enhanced SSL inspection bypass is on
cat $CPDIR/registry/HKLM_registry.data | grep -i ecdhe  Show ECDHE ciphers in registry
-- System Activity Report (sk112734) ----------------------------------------------------
sar  Show System Activity Report
sar -u  Show CPU utilization
sar -q  Show load average statistics
sar -r  Show memory statistics
sar -W  Show swapping statistics
sar -n EDEV  Show EDEV network statistics
sar -n ALL  Show ALL network statistics
iostat -p ALL  Show CPU statistics and input/output statistics for devices
mpstat -P ALL  Show processors related statistics

-- Check Point Appliance ----------------------------------------------------------------
show sysenv all  Show system environment (PSU, Fans, Temperature, etc.)
service ipmi start; ipmitool bmc info; service ipmi stop  Show LOM firmware version

Executing ?  # echo; tput bold; if [[ `$CPDIR/bin/cpprod_util FwIsFirewallModule 2>/dev/null` != *
'1'* ]]; then echo ' Not a firewall gateway!'; tput sgr0; echo; elif [[ `grep $(grep $(hostname) /e
tc/hosts | cut -f1 -d' ') $FWDIR/state/local/FW1/local.set | wc -l` == "0" ]]; then echo ' Main IP
of '$(hostname)' doesn`t match it`s management interface IP!'; tput sgr0; echo; else echo -n ' Inte
rface Topology '; tput sgr0; echo -n '> '; tput bold; tput setaf 1; if [[ -n "$vsname" ]] && [[ $vs
name != *'unavail'* ]]; then echo $vsname' (ID: '$INSTANCE_VSID')'; else hostname; fi; tput sgr0; e
cho -n ' '; printf '%.s-' {1..80}; echo; egrep -B1 $'ifindex|:ipaddr|\(\x22<[0-9]|objtype|has_addr_
info|:monitor_only|:external' $FWDIR/state/local/FW1/local.set | sed -n "/$(if [[ -n "$vsname" ]] &
& [[ $vsname != *'unavail'* ]] && [[ $INSTANCE_VSID != '0' ]]; then echo $vsname; else grep `hostna
me` /etc/hosts | cut -f1 -d' '; fi)*$/,\$ p" | tail -n +3 | sed 's/[\x22\t()<>]//g' | sed 's/--//g'
 | sed '$!N;s/\n:ipaddr6/ IPv6/;P;D' | sed '/IPv6/!s/://g' | sed 's/interface_topology/\tCalculated
 Interface Topology/g' | sed '0,/ifindex 0/{/ifindex 0/d;}' | sed '/ifindex 0/q' | sed '/spoof\|sca
n/d' | sed 's/has_addr_info true/\tAddress Spoofing Protection: Enabled/g' | sed 's/has_addr_info f
alse/\tAddress Spoofing Protection: Disabled/g' | sed -e '/Prot/{n;d}' | sed '$!N;s/\nmonitor_only
true/ (Detect Mode)/;P;D' | sed '$!N;s/\nmonitor_only false/ (Prevent Mode)/;P;D' | sed '$!N;s/\nex
ternal false/ - Internal Interface/;P;D' | sed '$!N;s/\nexternal true/ - External Interface/;P;D' |
 sed '/objtype/q' | tac | sed '/ifindex 0/I,+2 d' | sed '/Address/,$!d' | tac | sed '/ifindex/d' |
sed 's/,/ -/g' | sed '$!N;s/\nipaddr/ >/;P;D' | sed '/ - /s/^ /\t/' | egrep -C 9999 --color=auto $'
>|IPv6|External|Disabled|Detect'; echo; fi
```

Benefits:

stem-aware info screen,
iven navigation through
available commands,
her Code Hub solutions,
ports VSX environments

Intended for:

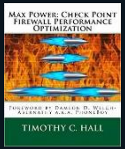
All

CHECKMATES

One-liner(s) for Troubleshooting

by **Danny Jung**

https://community.checkpoint.com/t5/Enterprise-Appliances-and-Gaia/One-liner-for-Address-Spoofing-Troubleshooting/m-p/33204


MAX POWER: CHECK POINT FIREWALL PERFORMANCE OPTIMIZATION
FOREWORD BY DAMEON D. WELCH-ABERNATHY A.K.A. PHONEBOY
TIMOTHY C. HALL

CHECKMATES Winner 2019

Environment:

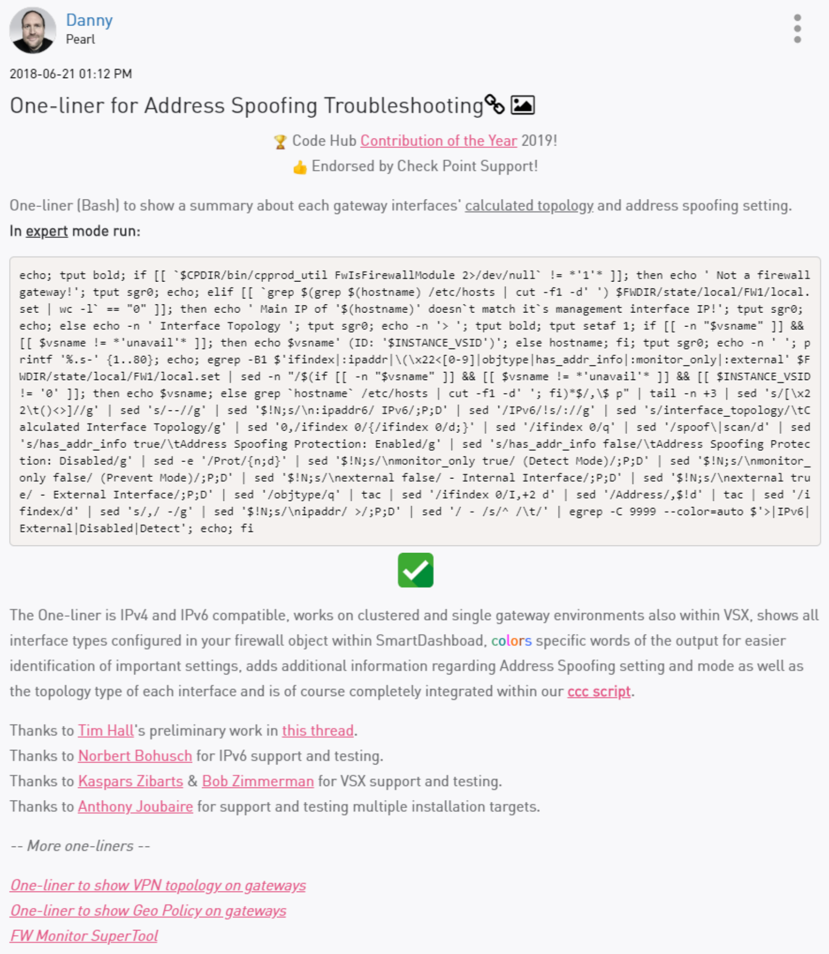
GAiA

Runs at:

Bash (Expert mode)

Result:

CLI output



Danny
Pearl

2018-06-21 01:12 PM

One-liner for Address Spoofing Troubleshooting

🏆 Code Hub Contribution of the Year 2019!
👍 Endorsed by Check Point Support!

One-liner (Bash) to show a summary about each gateway interfaces' calculated topology and address spoofing setting.

In expert mode run:

```
echo; tput bold; if [[ `$CPDIR/bin/cpprod_util FwIsFirewallModule 2>/dev/null` != *'1'* ]]; then echo ' Not a firewall
gateway!'; tput sgr0; echo; elif [[ `grep $(grep $(hostname) /etc/hosts | cut -f1 -d' ') $FWDIR/state/local/FW1/local.
set | wc -l` == "0" ]]; then echo ' Main IP of '$(hostname)' doesn`t match it`s management interface IP!'; tput sgr0;
echo; else echo -n ' Interface Topology '; tput sgr0; echo -n '> '; tput bold; tput setaf 1; if [[ -n "$vsname" ]] &&
[[ $vsname != *'unavail'* ]]; then echo $vsname' (ID: '$INSTANCE_VSID')'; else hostname; fi; tput sgr0; echo -n ' '; p
rintf '%.s-' {1..80}; echo; egrep -B1 $'ifindex|:ipaddr|\(\x22<[0-9]|objtype|has_addr_info|:monitor_only|:external' $F
WDIR/state/local/FW1/local.set | sed -n "/$(if [[ -n "$vsname" ]] && [[ $vsname != *'unavail'* ]] && [[ $INSTANCE_VSID
!= '0' ]]; then echo $vsname; else grep `hostname` /etc/hosts | cut -f1 -d' '; fi)*$/,\$ p" | tail -n +3 | sed 's/[\x2
2\t()<>]//g' | sed 's/--//g' | sed '$!N;s/\n:ipaddr6/ IPv6/;P;D' | sed '/IPv6/!s/://g' | sed 's/interface_topology/\tC
alculated Interface Topology/g' | sed '0,/ifindex 0/{/ifindex 0/d;}' | sed '/ifindex 0/q' | sed '/spoof\|scan/d' | sed
's/has_addr_info true/\tAddress Spoofing Protection: Enabled/g' | sed 's/has_addr_info false/\tAddress Spoofing Protec
tion: Disabled/g' | sed -e '/Prot/{n;d}' | sed '$!N;s/\nmonitor_only true/ (Detect Mode)/;P;D' | sed '$!N;s/\nmonitor_
only false/ (Prevent Mode)/;P;D' | sed '$!N;s/\nexternal false/ - Internal Interface/;P;D' | sed '$!N;s/\nexternal tru
e/ - External Interface/;P;D' | sed '/objtype/q' | tac | sed '/ifindex 0/I,+2 d' | sed '/Address/,$!d' | tac | sed '/i
findex/d' | sed 's/,/ -/g' | sed '$!N;s/\nipaddr/ >/;P;D' | sed '/ - /s/^ /\t/' | egrep -C 9999 --color=auto $'>|IPv6|
External|Disabled|Detect'; echo; fi
```

✓

The One-liner is IPv4 and IPv6 compatible, works on clustered and single gateway environments also within VSX, shows all interface types configured in your firewall object within SmartDashboad, colors specific words of the output for easier identification of important settings, adds additional information regarding Address Spoofing setting and mode as well as the topology type of each interface and is of course completely integrated within our ccc script.

Thanks to Tim Hall's preliminary work in this thread.
Thanks to Norbert Bohusch for IPv6 support and testing.
Thanks to Kaspars Zibarts & Bob Zimmerman for VSX support and testing.
Thanks to Anthony Joubaire for support and testing multiple installation targets.

-- More one-liners --

One-liner to show VPN topology on gateways
One-liner to show Geo Policy on gateways
FW Monitor SuperTool

Benefits:

Simply copy & paste to your GAiA CLI to receive detailed information

Easier troubleshooting

Intended for:

All

Run a command across all VS

by **Petr Hantak**

https://community.checkpoint.com/t5/Enterprise-Appliances-and-Gaia/Show-bgp-peers-across-VSX-in-CLI/m-p/39929

Environment:

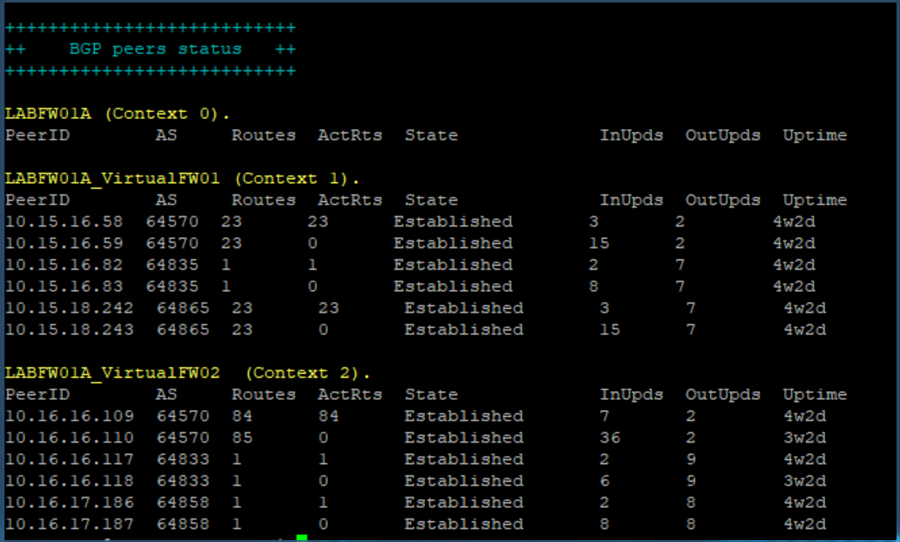
VSX GAiA

Runs at:

Bash (Expert mode)

Result:

CLI output



```
++++++++++++++++++++++++++++
++    BGP peers status   ++
++++++++++++++++++++++++++++

LABFW01A (Context 0).
PeerID         AS     Routes  ActRts  State             InUpds  OutUpds  Uptime

LABFW01A_VirtualFW01 (Context 1).
PeerID         AS     Routes  ActRts  State             InUpds  OutUpds  Uptime
10.15.16.58  64570  23       23      Established       3       2        4w2d
10.15.16.59  64570  23       0       Established       15      2        4w2d
10.15.16.82  64835  1        1       Established       2       7        4w2d
10.15.16.83  64835  1        0       Established       8       7        4w2d
10.15.18.242  64865  23       23      Established       3       7        4w2d
10.15.18.243  64865  23       0       Established       15      7        4w2d

LABFW01A_VirtualFW02  (Context 2).
PeerID         AS     Routes  ActRts  State             InUpds  OutUpds  Uptime
10.16.16.109  64570  84       84      Established       7       2        4w2d
10.16.16.110  64570  85       0       Established       36      2        3w2d
10.16.16.117  64833  1        1       Established       2       9        4w2d
10.16.16.118  64833  1        0       Established       6       9        3w2d
10.16.17.186  64858  1        1       Established       2       8        4w2d
10.16.17.187  64858  1        0       Established       8       8        4w2d
```

```
echo -e "\e[36m++++++++++++++++++++++++++++\n++    BGP peers status   ++\n++++++++++++++++++++++++++++\n"; for i in /proc/vrf/*; do
i=${i#*vrf/}; echo -n -e "\e[93m"; vsenv $i | grep  -e "Contex" | sed 's/^Context is set to Virtual Device //' | sed 's/ID/Context/'; echo -n
-e "\e[0m"; echo "set virtual-system" $i > /tmp/clishcmd; echo "show bgp peers" >> /tmp/clishcmd; clish -i -f /tmp/clishcmd | grep -vi -e
"contex" -e "show" -e "done" -e "flag" -e"^$"; echo; done
```

Benefits:

Easily run a command across all VSs on a VSX system simultaneously

Intended for:

Check Point SEs, Partners

(Available to customers)

Run a command across all gateways

by **Heiko Ankenbrand**

https://community.checkpoint.com/t5/Enterprise-Appliances-and-Gaia/GAIA-Easy-execute-CLI-commands-on-all-gateways-simultaneously/m-p/50971

Environment:

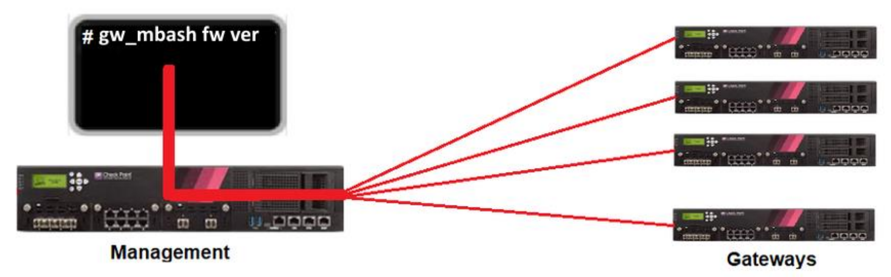
SMS GAiA

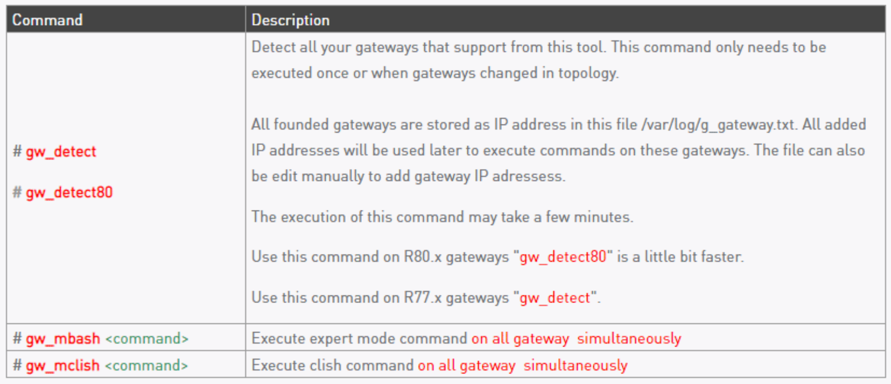
Runs at:

Bash (Expert mode)

Result:

CLI output





Command	Description
# gw_detect # gw_detect80	Detect all your gateways that support from this tool. This command only needs to be executed once or when gateways changed in topology. All founded gateways are stored as IP address in this file /var/log/g_gateway.txt. All added IP addresses will be used later to execute commands on these gateways. The file can also be edit manually to add gateway IP adressess. The execution of this command may take a few minutes. Use this command on R80.x gateways "gw_detect80" is a little bit faster. Use this command on R77.x gateways "gw_detect".
# gw_mbash <command>	Execute expert mode command on all gateway simultaneously
# gw_mclish <command>	Execute clish command on all gateway simultaneously

Benefits:

Easily run a command across all gateways managed by a SMS simultaneously

Intended for:

Check Point SEs, Partners

(Available to customers)

CP Viewer

by **Petar Markota**

https://community.checkpoint.com/t5/Visibility-Analytics/CPViewer-visualize-your-cpview-cpinfo-files-in-5-minutes/m-p/71345

Environment:

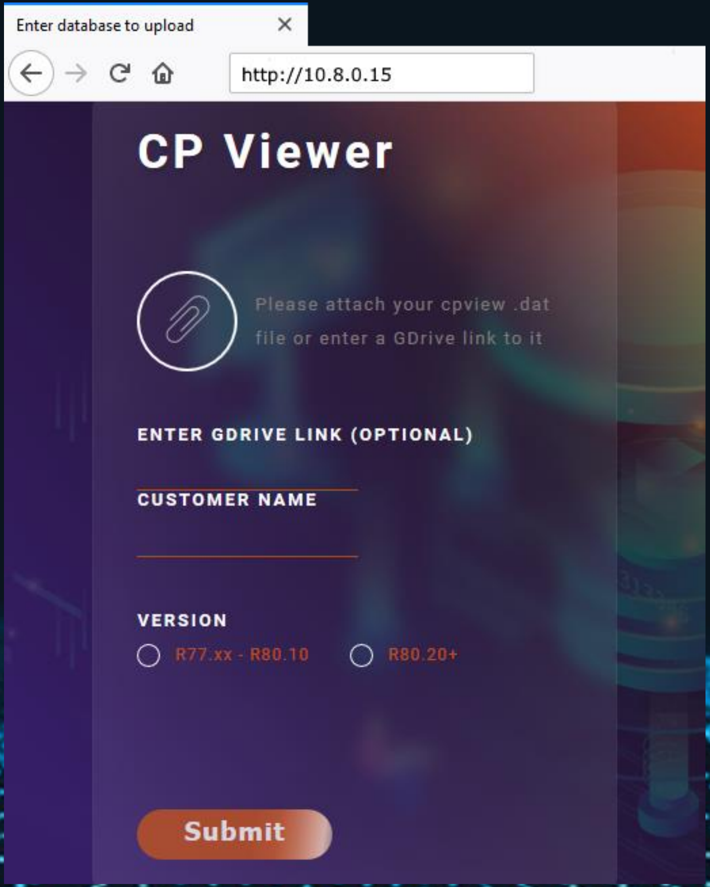
Ubuntu VM

Runs at:

Web browser

Result:

CPinfo, CPview database visualization and GAiA health check



Enter database to upload

http://10.8.0.15

CP Viewer

Please attach your cpview .dat file or enter a GDrive link to it

ENTER GDRIVE LINK (OPTIONAL)

CUSTOMER NAME

VERSION

○ R77.xx - R80.10 ○ R80.20+

Benefits:

Easily analyze Check Point system data to identify issues

Supports troubleshooting by visualization

Intended for:

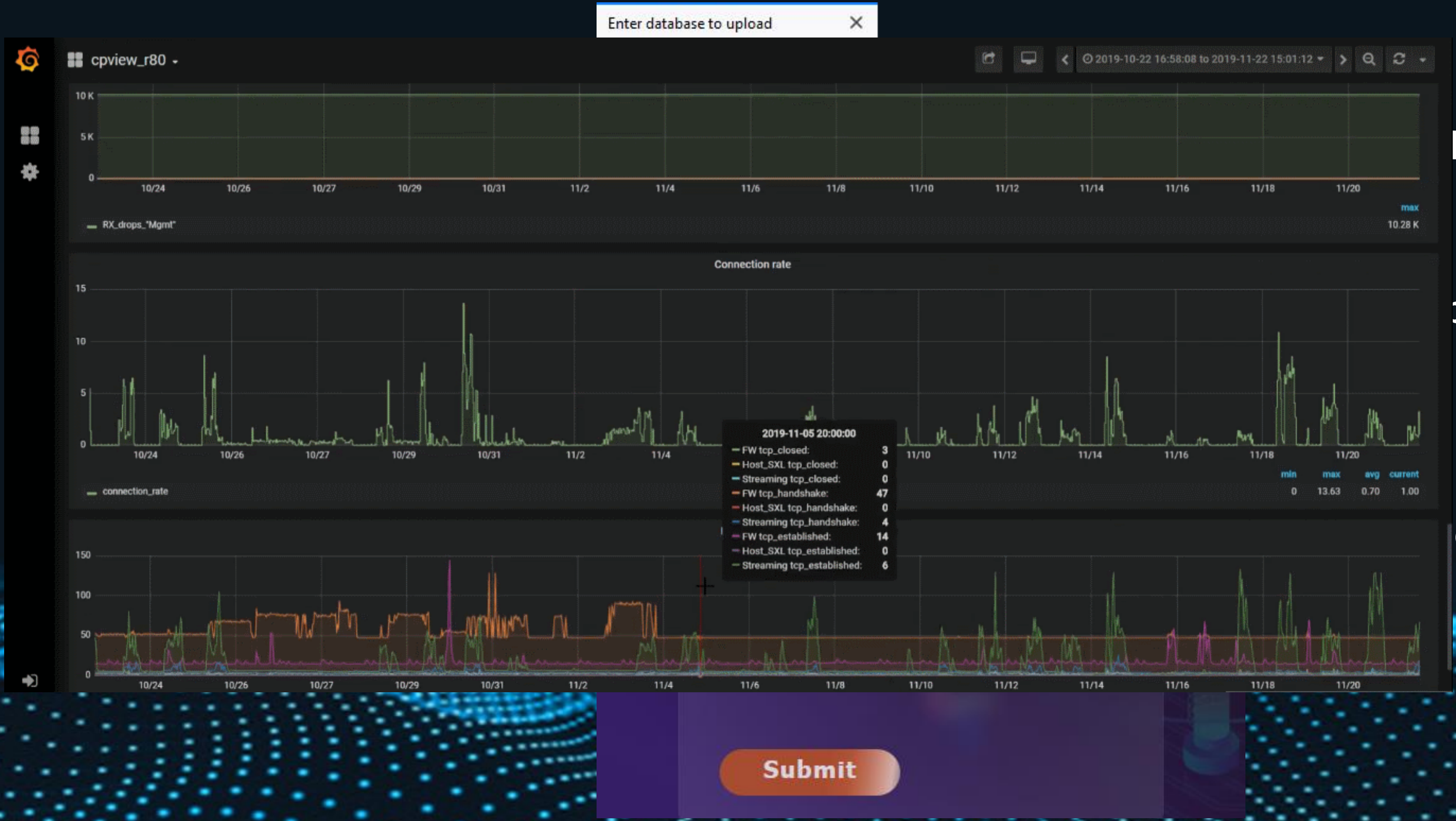
Check Point SEs, Partners

(Available to customers)

CP Viewer

by **Petar Markota**

https://community.checkpoint.com/t5/Visibility-Analytics/CPViewer-visualize-your-cpview-cpinfo-files-in-5-minutes/m-p/71345



Enter database to upload

2019-11-05 20:00:00

FW tcp_closed:	3
Host_SXL tcp_closed:	0
Streaming tcp_closed:	0
FW tcp_handshake:	47
Host_SXL tcp_handshake:	0
Streaming tcp_handshake:	4
FW tcp_established:	14
Host_SXL tcp_established:	0
Streaming tcp_established:	6

Benefits:

ly analyze Check Point data to identify issues

pports troubleshooting by visualization

Intended for:

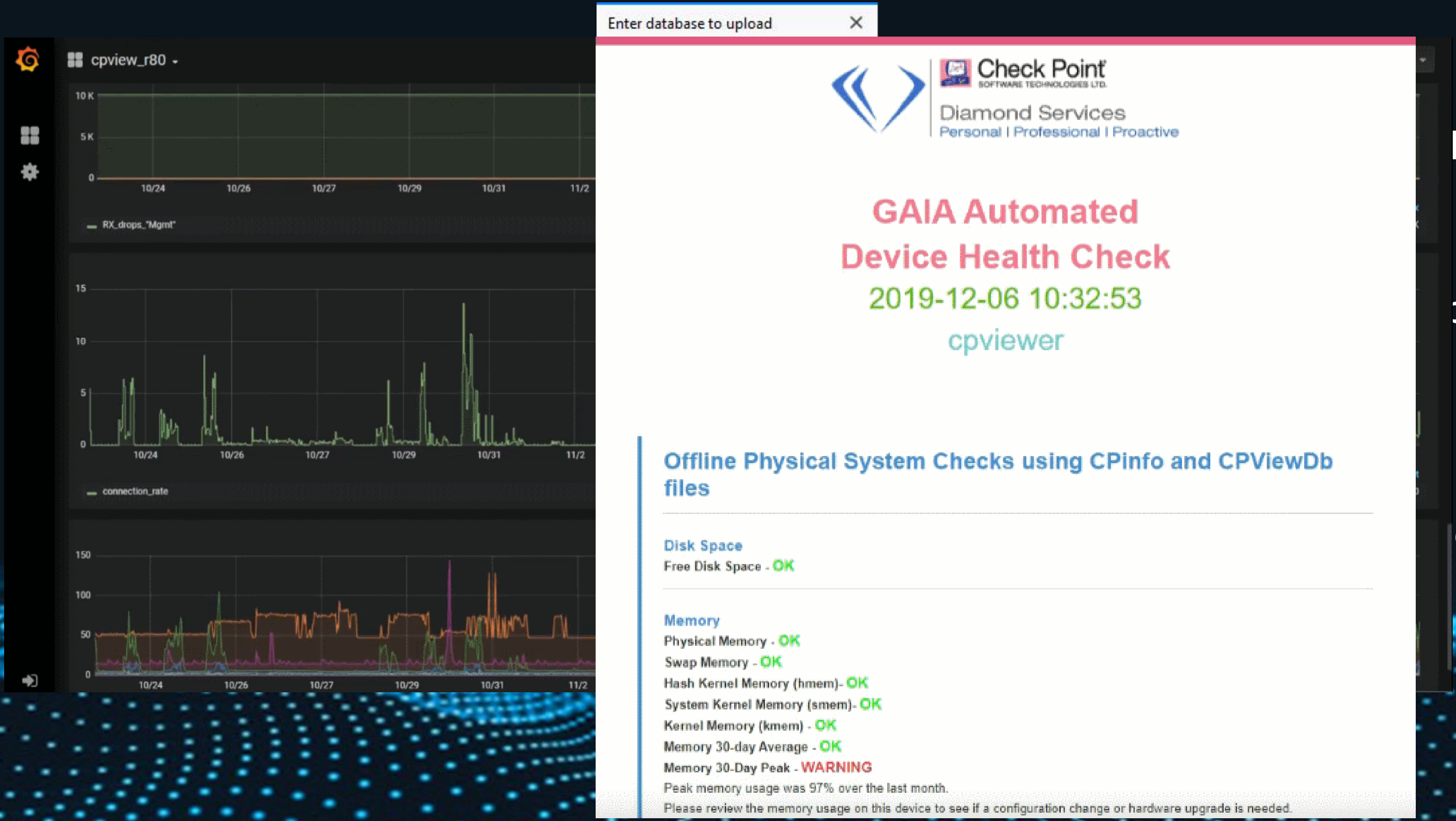
ck Point SEs, Partners

(Available to customers)

CP Viewer

by **Petar Markota**

https://community.checkpoint.com/t5/Visibility-Analytics/CPViewer-visualize-your-cpview-cpinfo-files-in-5-minutes/m-p/71345



GAIA Automated
Device Health Check
2019-12-06 10:32:53
cpviewer

Offline Physical System Checks using CPinfo and CPViewDb files

Disk Space
Free Disk Space - OK

Memory
Physical Memory - OK
Swap Memory - OK
Hash Kernel Memory (hmem)- OK
System Kernel Memory (smem)- OK
Kernel Memory (kmem) - OK
Memory 30-day Average - OK
Memory 30-Day Peak - WARNING
Peak memory usage was 97% over the last month.
Please review the memory usage on this device to see if a configuration change or hardware upgrade is needed.

Benefits:

ly analyze Check Point data to identify issues

pports troubleshooting by visualization

Intended for:

ck Point SEs, Partners

(Available to customers)

Security Gateway Inventory

by **Kaspars Zibarts**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Security-Gateway-Inventory/m-p/32547

Environment:

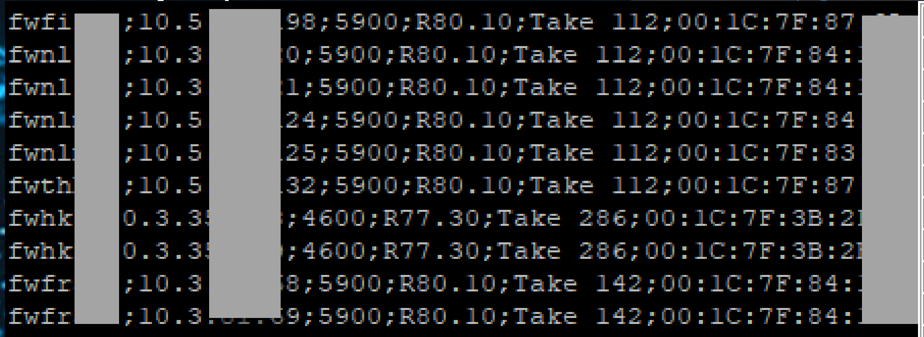
MDS GAiA

Runs at:

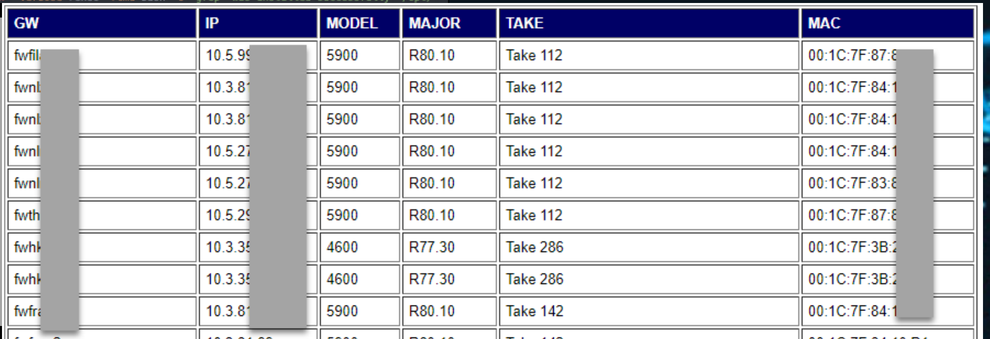
Bash (Expert mode)

Result:

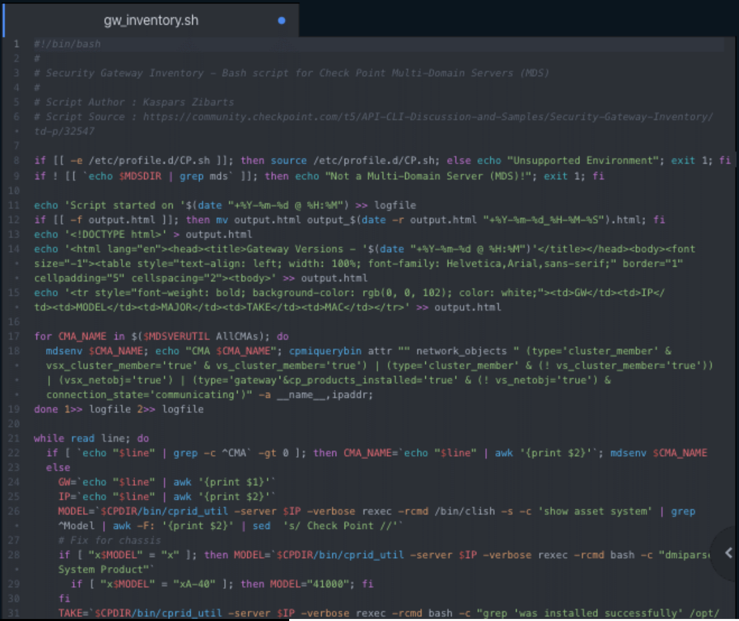
CLI output, HTML file



```
fwfi[redacted];10.5[redacted]98;5900;R80.10;Take 112;00:1C:7F:87[redacted]
fwnl[redacted];10.3[redacted]0;5900;R80.10;Take 112;00:1C:7F:84:[redacted]
fwnl[redacted];10.3[redacted]1;5900;R80.10;Take 112;00:1C:7F:84:[redacted]
fwnl[redacted];10.5[redacted]24;5900;R80.10;Take 112;00:1C:7F:84[redacted]
fwnl[redacted];10.5[redacted]25;5900;R80.10;Take 112;00:1C:7F:83[redacted]
fwth[redacted];10.5[redacted]32;5900;R80.10;Take 112;00:1C:7F:87[redacted]
fwhk[redacted]0.3.35[redacted];4600;R77.30;Take 286;00:1C:7F:3B:2[redacted]
fwhk[redacted]0.3.35[redacted];4600;R77.30;Take 286;00:1C:7F:3B:2[redacted]
fwfr[redacted];10.3[redacted]8;5900;R80.10;Take 142;00:1C:7F:84:[redacted]
fwfr[redacted];10.3[redacted]9;5900;R80.10;Take 142;00:1C:7F:84:[redacted]
```



GW	IP	MODEL	MAJOR	TAKE	MAC
fwfil[redacted]	10.5.9[redacted]	5900	R80.10	Take 112	00:1C:7F:87:[redacted]
fwn[redacted]	10.3.8[redacted]	5900	R80.10	Take 112	00:1C:7F:84:1[redacted]
fwn[redacted]	10.3.8[redacted]	5900	R80.10	Take 112	00:1C:7F:84:1[redacted]
fwnl[redacted]	10.5.2[redacted]	5900	R80.10	Take 112	00:1C:7F:84:1[redacted]
fwnl[redacted]	10.5.2[redacted]	5900	R80.10	Take 112	00:1C:7F:83:[redacted]
fwth[redacted]	10.5.2[redacted]	5900	R80.10	Take 112	00:1C:7F:87:[redacted]
fwh[redacted]	10.3.35[redacted]	4600	R77.30	Take 286	00:1C:7F:3B:[redacted]
fwh[redacted]	10.3.35[redacted]	4600	R77.30	Take 286	00:1C:7F:3B:[redacted]
fwfr[redacted]	10.3.8[redacted]	5900	R80.10	Take 142	00:1C:7F:84:1[redacted]



```bash
#!/bin/bash
#
# Security Gateway Inventory - Bash script for Check Point Multi-Domain Servers (MDS)
#
# Script Author : Kaspars Zibarts
# Script Source : https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Security-Gateway-Inventory/
td-p/32547

if [[ -e /etc/profile.d/CP.sh ]]; then source /etc/profile.d/CP.sh; else echo "Unsupported Environment"; exit 1; fi
if ! [[ `echo $MDSDIR | grep mds` ]]; then echo "Not a Multi-Domain Server (MDS)!"; exit 1; fi

echo 'Script started on '$(date "+%Y-%m-%d @ %H:%M") >> logfile
if [[ -f output.html ]]; then mv output.html output_$(date -r output.html "+%Y-%m-%d_%H-%M-%S").html; fi
echo '<!DOCTYPE html>' > output.html
echo '<html lang="en"><head><title>Gateway Versions - '$(date "+%Y-%m-%d @ %H:%M")'</title></head><body><font
size="-1"><table style="text-align: left; width: 100%; font-family: Helvetica,Arial,sans-serif;" border="1"
cellpadding="5" cellspacing="2"><tbody>' >> output.html
echo '<tr style="font-weight: bold; background-color: rgb(0, 0, 102); color: white;"><td>GW</td><td>IP</
td><td>MODEL</td><td>MAJOR</td><td>TAKE</td><td>MAC</td></tr>' >> output.html

for CMA_NAME in $($MDSVERUTIL AllCMAs); do
  mdsenv $CMA_NAME; echo "CMA $CMA_NAME"; cpmiquerybin attr "" network_objects " (type='cluster_member' &
  vsx_cluster_member='true' & vs_cluster_member='true') | (type='cluster_member' & (! vs_cluster_member='true'))
  | (vsx_netobj='true') | (type='gateway'&cp_products_installed='true' & (! vs_netobj='true') &
  connection_state='communicating')" -a __name__,ipaddr;
done 1>> logfile 2>> logfile

while read line; do
  if [ `echo "$line" | grep -c ^CMA` -gt 0 ]; then CMA_NAME=`echo "$line" | awk '{print $2}'`; mdsenv $CMA_NAME
  else
    GW=`echo "$line" | awk '{print $1}'`
    IP=`echo "$line" | awk '{print $2}'`
    MODEL=`$CPDIR/bin/cprid_util -server $IP -verbose rexec -rcmd /bin/clish -s -c 'show asset system' | grep
    ^Model | awk -F: '{print $2}' | sed  's/ Check Point //'`
    # Fix for chassis
    if [ "x$MODEL" = "x" ]; then MODEL=`$CPDIR/bin/cprid_util -server $IP -verbose rexec -rcmd bash -c "dmipars
    System Product"`
      if [ "x$MODEL" = "xA-40" ]; then MODEL="41000"; fi
    fi
    TAKE=`$CPDIR/bin/cprid_util -server $IP -verbose rexec -rcmd bash -c "grep 'was installed successfully' /opt/
```

Benefits:

Live inventory listing of all CP gateways managed by a MDS

Output easily modifiable

Intended for:

Check Point SEs, Partners

(Available to customers)

Office 365 Object Creation

by **Stuart Green** (Python) / **Daniel Meier** (Bash)

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Can-we-create-custom-updatable-objects-in-R80-20/m-p/47914/highlight/true#M3190
https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Basic-script-for-importing-IP-Address-objects-from-feed-here/m-p/40842/highlight/true#M2759

Environment:

Management API

Runs at:

Bash (Expert mode)

Result:

O365 object group

Benefits:

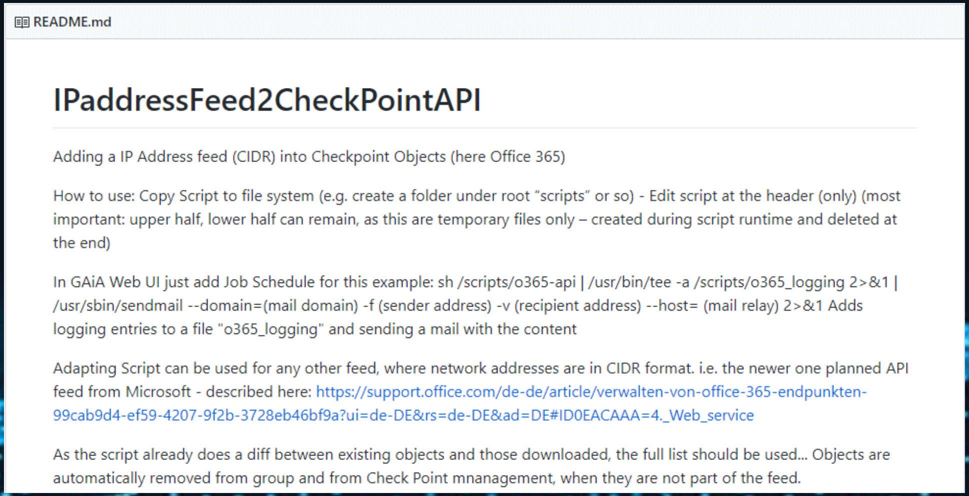
Alternative to MS Office 365 object

Overcomes R80.20 limitation *(sk131852)*

Can be re-used for similar needs

Intended for:

All



README.md

IPaddressFeed2CheckPointAPI

Adding a IP Address feed (CIDR) into Checkpoint Objects (here Office 365)

How to use: Copy Script to file system (e.g. create a folder under root "scripts" or so) - Edit script at the header (only) (most important: upper half, lower half can remain, as this are temporary files only – created during script runtime and deleted at the end)

In GAiA Web UI just add Job Schedule for this example: sh /scripts/o365-api | /usr/bin/tee -a /scripts/o365_logging 2>&1 | /usr/sbin/sendmail --domain=(mail domain) -f (sender address) -v (recipient address) --host= (mail relay) 2>&1 Adds logging entries to a file "o365_logging" and sending a mail with the content

Adapting Script can be used for any other feed, where network addresses are in CIDR format. i.e. the newer one planned API feed from Microsoft - described here: https://support.office.com/de-de/article/verwalten-von-office-365-endpunkten-99cab9d4-ef59-4207-9f2b-3728eb46bf9a?ui=de-DE&rs=de-DE&ad=DE#ID0EACAAA=4._Web_service

As the script already does a diff between existing objects and those downloaded, the full list should be used... Objects are automatically removed from group and from Check Point mnanagement, when they are not part of the feed.

Automatic hosts discovery and creation

by **Nicolas Boissé**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/R80-10-Hosts-Discovery-and-creation/m-p/38708

Environment:

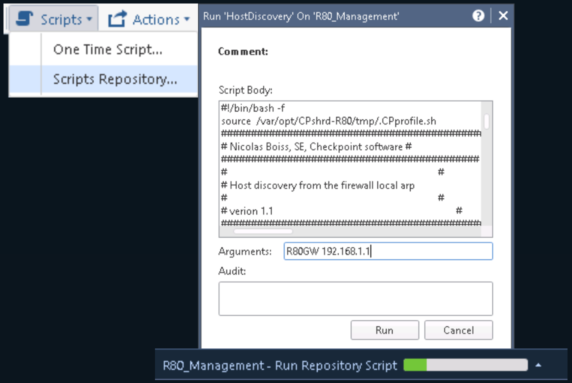
SMS GAiA / SmartConsole

Runs at:

Bash (Expert Mode) / Scripts repository

Result:

Hosts within group objects



Run 'HostDiscovery' On 'R80_Management'

Comment:

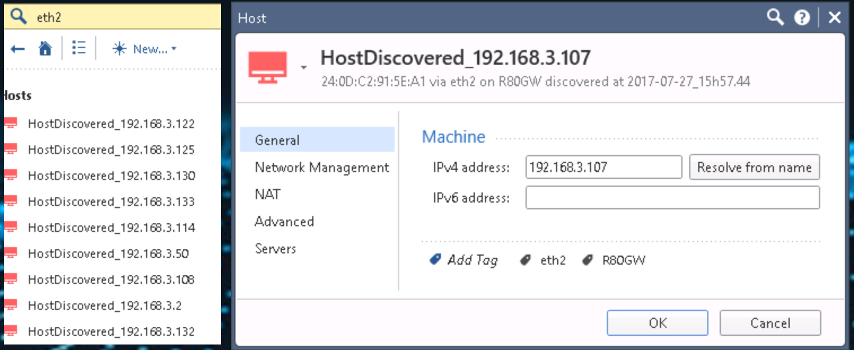
Script Body:

```
#!/bin/bash -f
source  /var/opt/CPshrd-R80/tmp/.CPprofile.sh
##################################################
# Nicolas Boiss, SE, Checkpoint software #
##################################################
#                                             #
# Host discovery from the firewall local arp
#                                             #
# verion 1.1                                      #
##################################################
```

Arguments: R80GW 192.168.1.1

Audit:

R80_Management - Run Repository Script



Hosts

- HostDiscovered_192.168.3.122
- HostDiscovered_192.168.3.125
- HostDiscovered_192.168.3.130
- HostDiscovered_192.168.3.133
- HostDiscovered_192.168.3.114
- HostDiscovered_192.168.3.50
- HostDiscovered_192.168.3.108
- HostDiscovered_192.168.3.2
- HostDiscovered_192.168.3.132

Host

HostDiscovered_192.168.3.107

24:0D:C2:91:5E:A1 via eth2 on R80GW discovered at 2017-07-27_15h57.44

Machine

IPv4 address: 192.168.3.107

IPv6 address:

Tags: eth2, R80GW

Benefits:

Easy hosts discovery and creation during initial setup of Security Mangement configuration

Intended for:

All

Automatic objects tagging

by **Jozko Mrkvicka**

https://community.checkpoint.com/t5/General-Management-Topics/How-to-count-objects-of-a-group/m-p/21558/highlight/true#M4185

Environment:

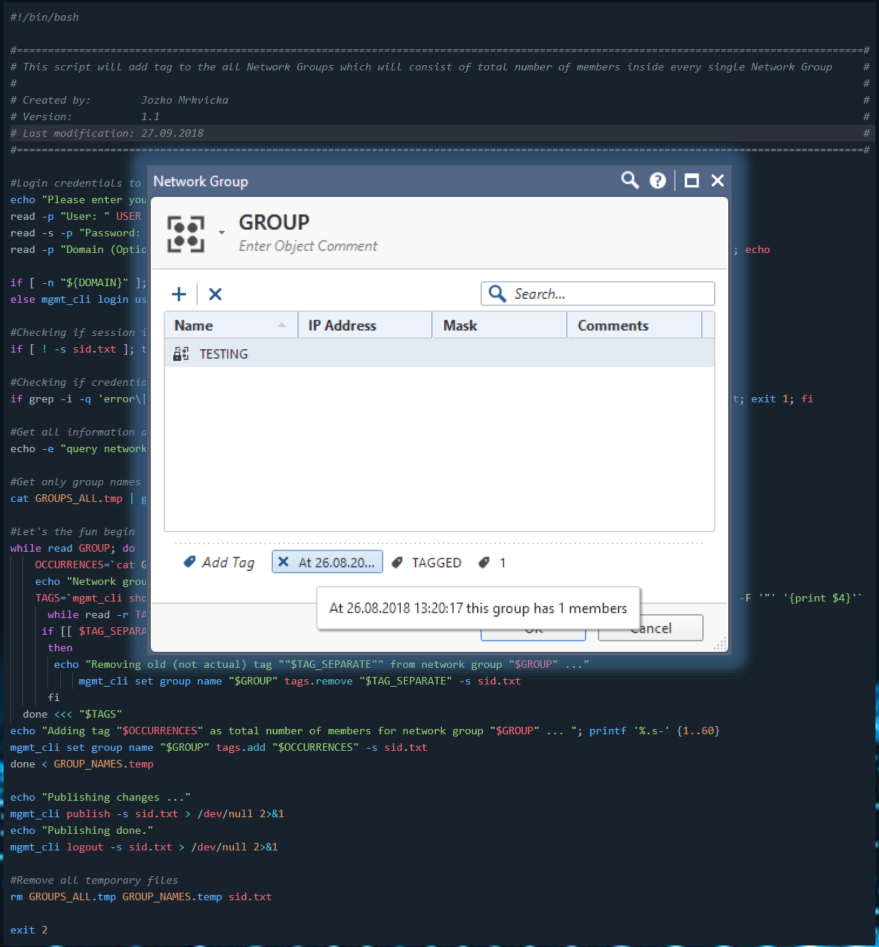
SMS GAiA / SmartConsole

Runs at:

Bash (Expert Mode) / Scripts repository

Result:

Tagged group objects



```
#!/bin/bash

#====================================================================================================#
# This script will add tag to the all Network Groups which will consist of total number of members inside every single Network Group     #
#                                                                                                    #
# Created by:        Jozko Mrkvicka                                                                  #
# Version:           1.1                                                                             #
# Last modification: 27.09.2018                                                                      #
#====================================================================================================#

#Login credentials to
echo "Please enter you
read -p "User: " USER
read -s -p "Password:
read -p "Domain (Optio                                                          ; echo

if [ -n "${DOMAIN}" ];
else mgmt_cli login us

#Checking if session i
if [ ! -s sid.txt ]; t

#Checking if credentia
if grep -i -q 'error\|                                                          t; exit 1; fi

#Get all information a
echo -e "query network

#Get only group names
cat GROUPS_ALL.tmp | g

#Let's the fun begin
while read GROUP; do
    OCCURRENCES=`cat G
    echo "Network grou
    TAGS=`mgmt_cli sho                                                          -F '"' '{print $4}'`
     while read -r TA
    if [[ $TAG_SEPARA
     then
      echo "Removing old (not actual) tag ""$TAG_SEPARATE"" from network group "$GROUP" ..."
        mgmt_cli set group name "$GROUP" tags.remove "$TAG_SEPARATE" -s sid.txt
     fi
  done <<< "$TAGS"
echo "Adding tag "$OCCURRENCES" as total number of members for network group "$GROUP" ... "; printf '%.s-' {1..60}
mgmt_cli set group name "$GROUP" tags.add "$OCCURRENCES" -s sid.txt
done < GROUP_NAMES.temp

echo "Publishing changes ..."
mgmt_cli publish -s sid.txt > /dev/null 2>&1
echo "Publishing done."
mgmt_cli logout -s sid.txt > /dev/null 2>&1

#Remove all temporary files
rm GROUPS_ALL.tmp GROUP_NAMES.temp sid.txt

exit 2
```

Network Group

GROUP

Enter Object Comment

+ ✕ Search...

Name	IP Address	Mask	Comments
TESTING			

Add Tag ✕ At 26.08.20... TAGGED 1

At 26.08.2018 13:20:17 this group has 1 members

Benefits:

Easy tagging of groups for various needs. Here: Adding the number of grouped hosts

Intended for:

All

MDSM Demo Environment

by **Jim Öqvist**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Sample-batch-script-to-deply-MDSM-environment-for-lab-purposes/td-p/39874

Environment:

Multi-Domain Security Management

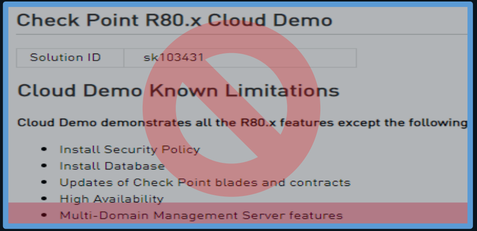
Runs as:

Windows Batch script

Result:

MDSM demo environment

single / redundant



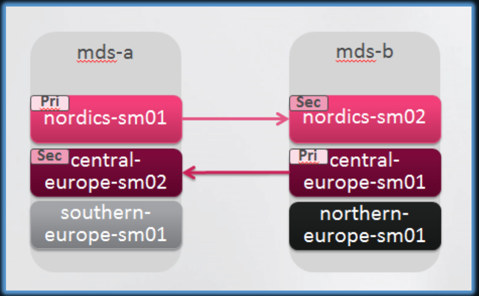
Check Point R80.x Cloud Demo

Solution ID	sk103431

Cloud Demo Known Limitations

Cloud Demo demonstrates all the R80.x features except the following

- Install Security Policy
- Install Database
- Updates of Check Point blades and contracts
- High Availability
- Multi-Domain Management Server features



Benefits:

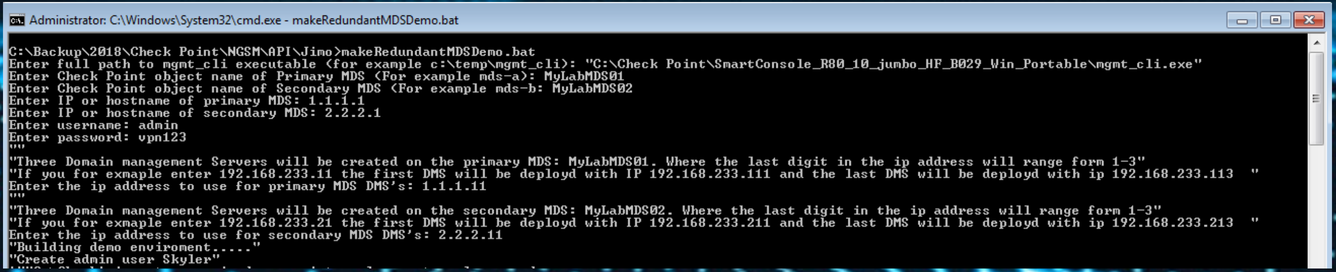
Overcome DemoPoint limitation

Save time setting up MDSM lab environment

Intended for:

Check Point SEs, Partners

(Available to customers)



Administrator: C:\Windows\System32\cmd.exe - makeRedundantMDSDemo.bat

```
C:\Backup\2018\Check Point\NGSM\API\Jimo>makeRedundantMDSDemo.bat
Enter full path to mgmt_cli executable (for example c:\temp\mgmt_cli): "C:\Check Point\SmartConsole_R80_10_jumbo_HF_B029_Win_Portable\mgmt_cli.exe"
Enter Check Point object name of Primary MDS (For example mds-a): MyLabMDS01
Enter Check Point object name of Secondary MDS (For example mds-b: MyLabMDS02
Enter IP or hostname of primary MDS: 1.1.1.1
Enter IP or hostname of secondary MDS: 2.2.2.1
Enter username: admin
Enter password: vpn123
""
"Three Domain management Servers will be created on the primary MDS: MyLabMDS01. Where the last digit in the ip address will range form 1-3"
"If you for exmaple enter 192.168.233.11 the first DMS will be deployd with IP 192.168.233.111 and the last DMS will be deployd with ip 192.168.233.113  "
Enter the ip address to use for primary MDS DMS's: 1.1.1.11
""
"Three Domain management Servers will be created on the secondary MDS: MyLabMDS02. Where the last digit in the ip address will range form 1-3"
"If you for exmaple enter 192.168.233.21 the first DMS will be deployd with IP 192.168.233.211 and the last DMS will be deployd with ip 192.168.233.213  "
Enter the ip address to use for secondary MDS DMS's: 2.2.2.11
"Building demo enviroment....."
"Create admin user Skyler"
```

Apple Siri Shortcuts + MGMT API

by **Adam Forester**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/iOS12-Siri-Shortcuts-and-MGMT-API/m-p/40448

Environment:

Apple iOS + Shortcuts App

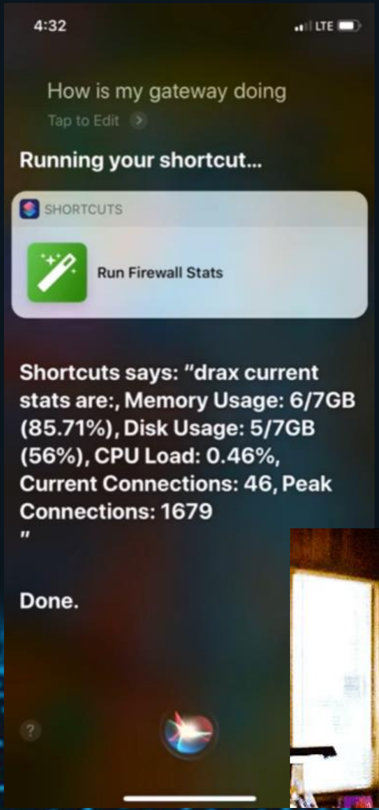
SMS GAiA

Runs as:

Siri command, Bash script

Result:

Output on iPhone screen



How is my gateway doing

Running your shortcut...

Shortcuts says: "drax current stats are:, Memory Usage: 6/7GB (85.71%), Disk Usage: 5/7GB (56%), CPU Load: 0.46%, Current Connections: 46, Peak Connections: 1679
"

Done.

Benefits:

Voice control of your firewall

Quick checks on your mobile

Intended for:

Testing purposes

Multi-Factor Auth w/ Google Authenticator

by **Vladimir Yakovlev**

https://community.checkpoint.com/t5/General-Topics/MFA-with-Google-Autheticator/m-p/55703

Alternative: MFA with Microsoft Authenticator by Rodrigo Silva

Environment:

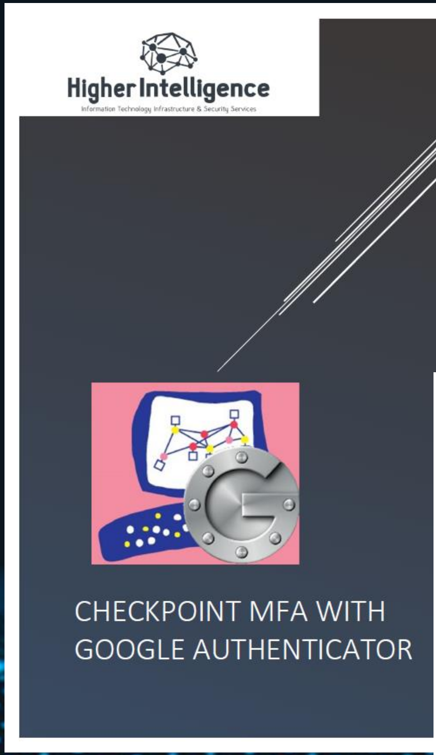
Android Phone with Google Auth App / Radius

Provided as:

PDF tech doc

Result:

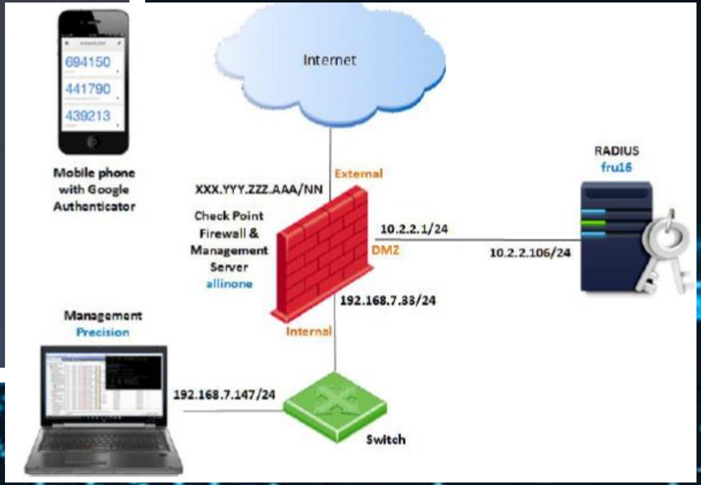
Step-by-step guide for all required commands and settings



Higher Intelligence

Information Technology Infrastructure & Security Services

CHECKPOINT MFA WITH GOOGLE AUTHENTICATOR



Benefits:

Google MFA usage with CP

Intended for:

All

Access rule creation via HTML

by **Charles Currier**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/What-the-Management-API-can-do-for-you/m-p/44420

Environment:

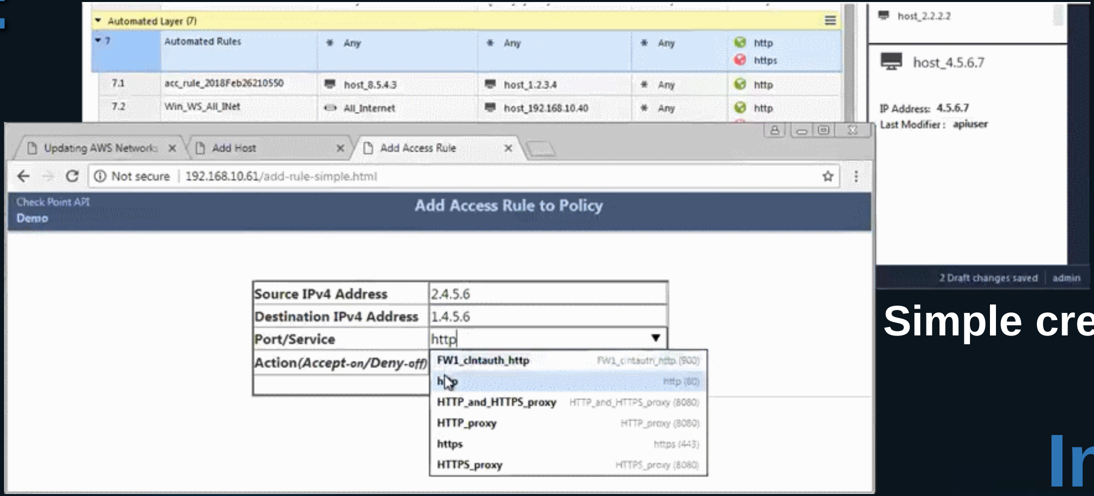
Management API

Runs as:

Python script

Result:

HTML-based access rule creation



Automated Layer (7)

7	Automated Rules	Any	Any	Any	http https
7.1	acc_rule_2018Feb26210550	host_8.5.4.3	host_1.2.3.4	Any	http
7.2	Win_WS_All_INet	All_Internet	host_192.168.10.40	Any	http

host_2.2.2.2

host_4.5.6.7

IP Address: 4.5.6.7
Last Modifier : apiuser

2 Draft changes saved | admin

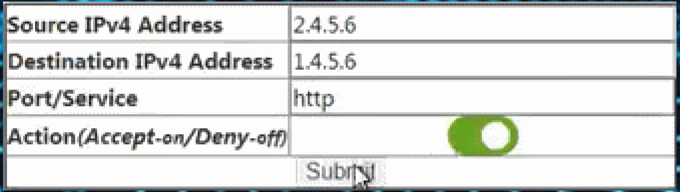
Not secure | 192.168.10.61/add-rule-simple.html

Check Point API
Demo

Add Access Rule to Policy

Source IPv4 Address	2.4.5.6
Destination IPv4 Address	1.4.5.6
Port/Service	http
Action*(Accept-on/Deny-off)*	

Updating AWS Networks
Add Host
Add Access Rule
FW1_clntauth_http FW1_clntauth_http (900)
http http (80)
HTTP_and_HTTPS_proxy HTTP_and_HTTPS_proxy (8080)
HTTP_proxy HTTP_proxy (8080)
https https (443)
HTTPS_proxy HTTPS_proxy (8080)



Source IPv4 Address	2.4.5.6
Destination IPv4 Address	1.4.5.6
Port/Service	http
Action*(Accept-on/Deny-off)*	

Benefits:

Simple creation of rules within your web browser

Intended for:

Testing purposes

DAIP VPN IP Change Tracker

by **Daniel Sceberra**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/CheckPoint-DAIP-VPN-get-Peer-Names/m-p/35633/highlight/true#M2197

Environment:

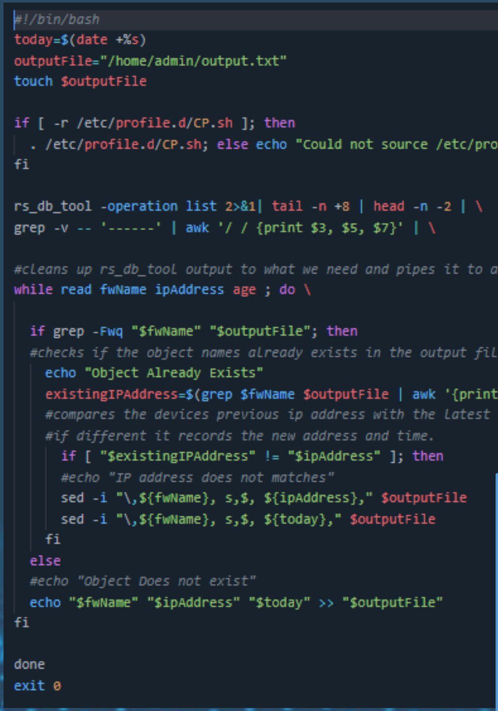
MGMT GAiA

Runs as:

Bash (Expert mode)

Result:

output.txt with all IP changes



```bash
#!/bin/bash
today=$(date +%s)
outputFile="/home/admin/output.txt"
touch $outputFile

if [ -r /etc/profile.d/CP.sh ]; then
  . /etc/profile.d/CP.sh; else echo "Could not source /etc/profile.d/CP.sh"; exit 1
fi

rs_db_tool -operation list 2>&1| tail -n +8 | head -n -2 | \
grep -v -- '------' | awk '/ / {print $3, $5, $7}' | \

#cleans up rs_db_tool output to what we need and pipes it to awk
while read fwName ipAddress age ; do \

  if grep -Fwq "$fwName" "$outputFile"; then
  #checks if the object names already exists in the output file
    echo "Object Already Exists"
    existingIPAddress=$(grep $fwName $outputFile | awk '{print $(NF-1)}')
    #compares the devices previous ip address with the latest checked IP address,
    #if different it records the new address and time.
      if [ "$existingIPAddress" != "$ipAddress" ]; then
      #echo "IP address does not matches"
      sed -i "\,${fwName}, s,$, ${ipAddress}," $outputFile
      sed -i "\,${fwName}, s,$, ${today}," $outputFile
    fi
  else
  #echo "Object Does not exist"
  echo "$fwName" "$ipAddress" "$today" >> "$outputFile"
fi

done
exit 0
```

Benefits:

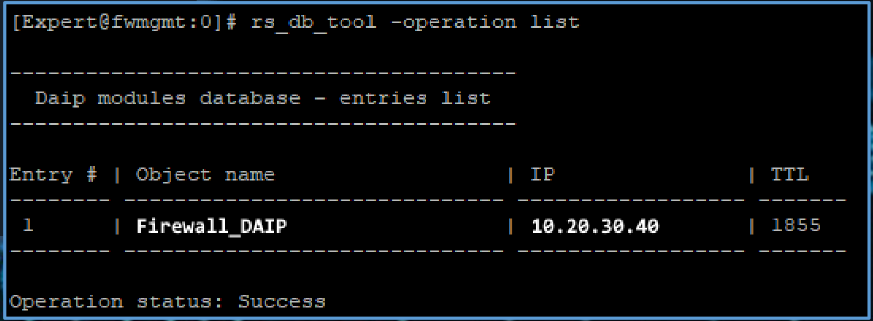
Scripted use of

rs_db_tool -operation list

for easy tracking of IP changes

Intended for:

All



```
[Expert@fwmgmt:0]# rs_db_tool -operation list

-----------------------------------------
  Daip modules database - entries list
-----------------------------------------

Entry # | Object name                      | IP                  | TTL
-------- ---------------------------------- ------------------- -------
 1       | Firewall_DAIP                    | 10.20.30.40         | 1855
-------- ---------------------------------- ------------------- -------

Operation status: Success
```

ESC.de

VPN IPsec Tunnel w/ Raspberry Pi WiFi AP

by **Stuart Green**

https://community.checkpoint.com/t5/CloudGuard-SaaS/CloudGuard-Connect-Demo-with-Raspberry-Pi/m-p/71571

Environment:

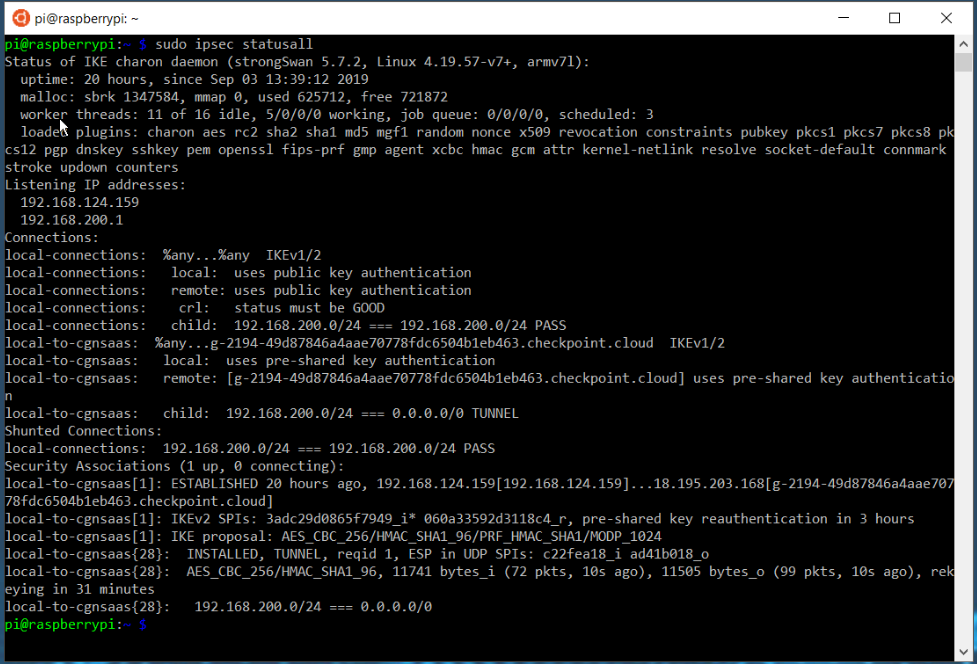
Raspbian OS

Runs as:

Bash, Python script

Result:

NSaaS CloudGuard Demo for VPN IPsec tunnel with Raspberry Pi



pi@raspberrypi: ~

```
pi@raspberrypi:~ $ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.7.2, Linux 4.19.57-v7+, armv7l):
  uptime: 20 hours, since Sep 03 13:39:12 2019
  malloc: sbrk 1347584, mmap 0, used 625712, free 721872
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pk
cs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark
stroke updown counters
Listening IP addresses:
  192.168.124.159
  192.168.200.1
Connections:
local-connections:  %any...%any  IKEv1/2
local-connections:   local:  uses public key authentication
local-connections:   remote: uses public key authentication
local-connections:    crl:   status must be GOOD
local-connections:   child:  192.168.200.0/24 === 192.168.200.0/24 PASS
local-to-cgnsaas:  %any...g-2194-49d87846a4aae70778fdc6504b1eb463.checkpoint.cloud  IKEv1/2
local-to-cgnsaas:   local:  uses pre-shared key authentication
local-to-cgnsaas:   remote: [g-2194-49d87846a4aae70778fdc6504b1eb463.checkpoint.cloud] uses pre-shared key authenticatio
n
local-to-cgnsaas:   child:  192.168.200.0/24 === 0.0.0.0/0 TUNNEL
Shunted Connections:
local-connections:  192.168.200.0/24 === 192.168.200.0/24 PASS
Security Associations (1 up, 0 connecting):
local-to-cgnsaas[1]: ESTABLISHED 20 hours ago, 192.168.124.159[192.168.124.159]...18.195.203.168[g-2194-49d87846a4aae707
78fdc6504b1eb463.checkpoint.cloud]
local-to-cgnsaas[1]: IKEv2 SPIs: 3adc29d0865f7949_i* 060a33592d3118c4_r, pre-shared key reauthentication in 3 hours
local-to-cgnsaas[1]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
local-to-cgnsaas{28}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c22fea18_i ad41b018_o
local-to-cgnsaas{28}:  AES_CBC_256/HMAC_SHA1_96, 11741 bytes_i (72 pkts, 10s ago), 11505 bytes_o (99 pkts, 10s ago), rek
eying in 31 minutes
local-to-cgnsaas{28}:   192.168.200.0/24 === 0.0.0.0/0
pi@raspberrypi:~ $
```

Benefits:

Step-by-step Raspi config and VPN setup guide

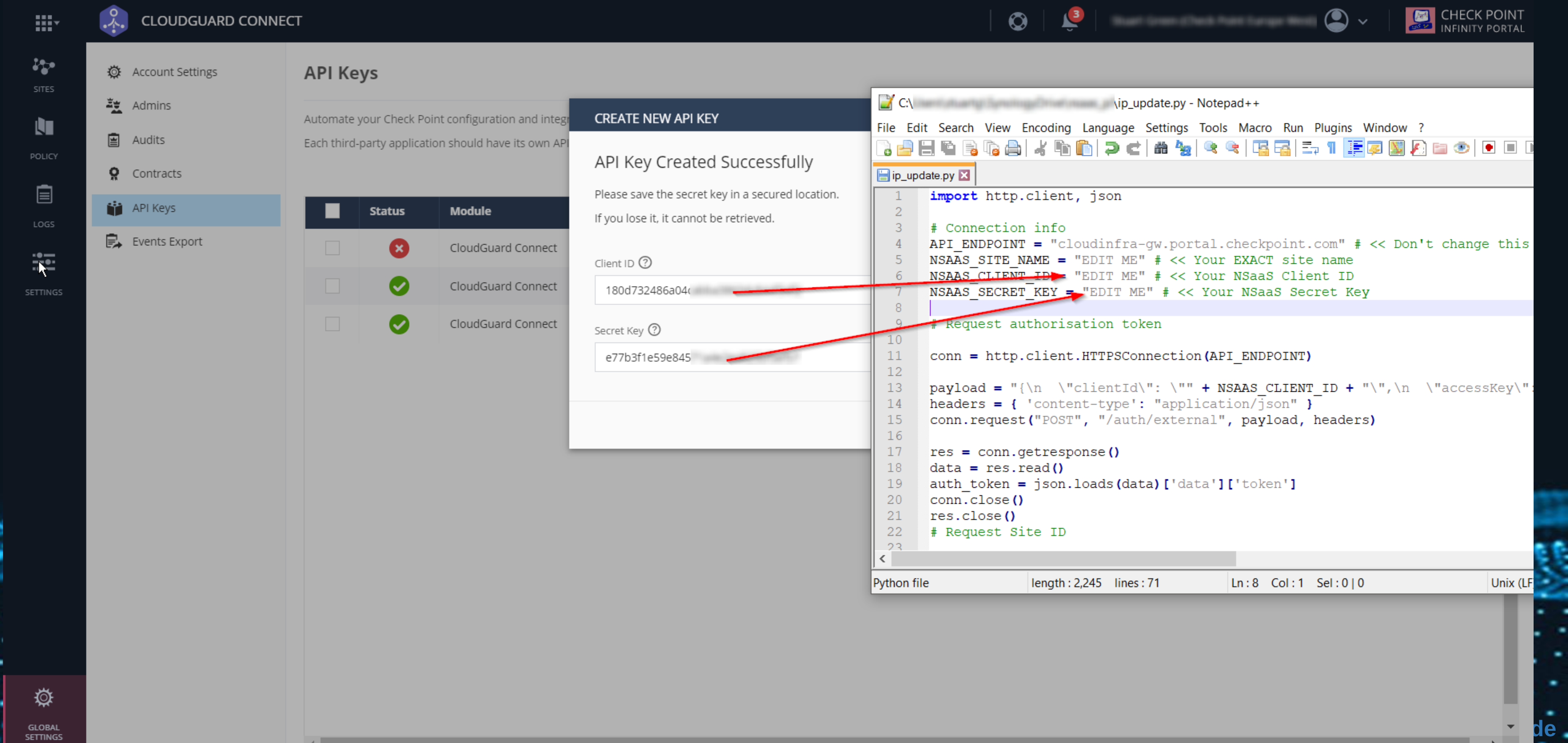
Purpose:

Demo

VPN IPsec Tunnel w/ Raspberry Pi WiFi AP

by **Stuart Green**

https://community.checkpoint.com/t5/CloudGuard-SaaS/CloudGuard-Connect-Demo-with-Raspberry-Pi/m-p/71571



API Keys

Automate your Check Point configuration and integ

Each third-party application should have its own API

□	Status	Module
□	☒	CloudGuard Connect
□	✓	CloudGuard Connect
□	✓	CloudGuard Connect

CREATE NEW API KEY

API Key Created Successfully

Please save the secret key in a secured location.

If you lose it, it cannot be retrieved.

Client ID ⓘ

180d732486a04[redacted]

Secret Key ⓘ

e77b3f1e59e845[redacted]

C:\[redacted]\ip_update.py - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
ip_update.py

```
import http.client, json

# Connection info
API_ENDPOINT = "cloudinfra-gw.portal.checkpoint.com" # << Don't change this
NSAAS_SITE_NAME = "EDIT ME" # << Your EXACT site name
NSAAS_CLIENT_ID = "EDIT ME" # << Your NSaaS Client ID
NSAAS_SECRET_KEY = "EDIT ME" # << Your NSaaS Secret Key

# Request authorisation token

conn = http.client.HTTPSConnection(API_ENDPOINT)

payload = "{\n  \"clientId\": \"" + NSAAS_CLIENT_ID + "\",\n  \"accessKey\":
headers = { 'content-type': "application/json" }
conn.request("POST", "/auth/external", payload, headers)

res = conn.getresponse()
data = res.read()
auth_token = json.loads(data)['data']['token']
conn.close()
res.close()
# Request Site ID
```

Python file | length : 2,245 lines : 71 | Ln : 8 Col : 1 Sel : 0 | 0 | Unix (LF

Update Dynamic IP via Management API

by **Luca Famà**

https://community.checkpoint.com/t5/API-CLI-Discussion-and-Samples/Using-R80-10-APIs-to-update-dynamic-public-IP-address/td-p/39413

Environment:

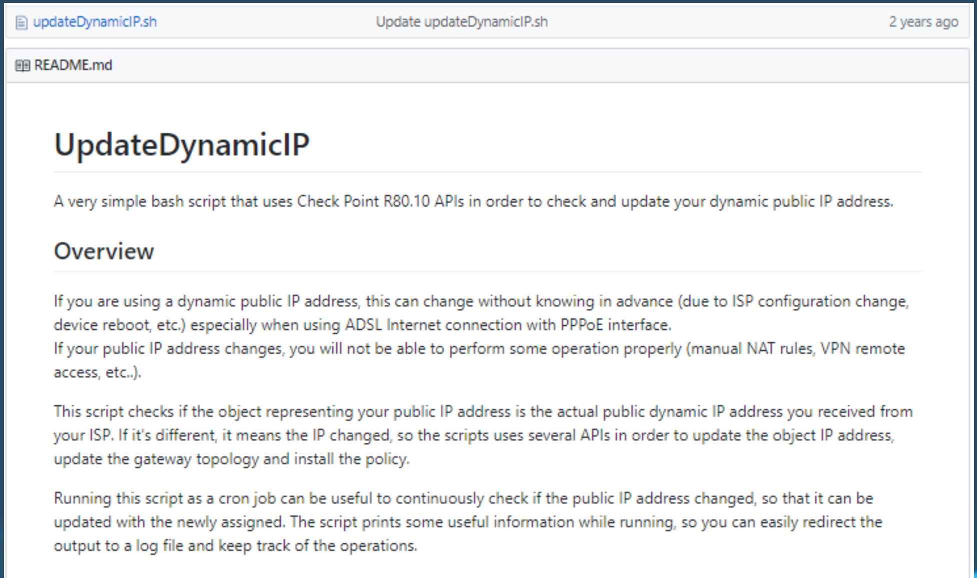
SMS GAiA

Runs as:

Bash (Expert mode)

Result:

Auto-updated IP and topology of gateway object



updateDynamicIP.sh — Update updateDynamicIP.sh — 2 years ago

README.md

UpdateDynamicIP

A very simple bash script that uses Check Point R80.10 APIs in order to check and update your dynamic public IP address.

Overview

If you are using a dynamic public IP address, this can change without knowing in advance (due to ISP configuration change, device reboot, etc.) especially when using ADSL Internet connection with PPPoE interface.
If your public IP address changes, you will not be able to perform some operation properly (manual NAT rules, VPN remote access, etc..).

This script checks if the object representing your public IP address is the actual public dynamic IP address you received from your ISP. If it's different, it means the IP changed, so the scripts uses several APIs in order to update the object IP address, update the gateway topology and install the policy.

Running this script as a cron job can be useful to continuously check if the public IP address changed, so that it can be updated with the newly assigned. The script prints some useful information while running, so you can easily redirect the output to a log file and keep track of the operations.

Benefits:

Removes many annoyances that are caused by dyn. GW IPs

Purpose:

Branch / Home offices

Check Point CHECKMATES
Learn. Share. Inspire.

Thank YOU!

Danny Jung

CTO at Check Point 4-Star Partner ESC

ESC.de