CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

NEW QUESTION 1
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Answer: A

NEW QUESTION 2
Check Point Access Control Daemons contains several daemons for Software Blades and features. Which Daemon is used for Application & Control Filtering?

A. rad
B. cprad
C. pepd
D. pdpd

Answer: A

NEW QUESTION 3
James is using the same filter expression in fw monitor for CITRIX very often and instead of typing this all the time he wants to add it as a macro to the fw monitor definition file. What's the name and location of this file?

A. $FWDIR/lib/fwmonltor.def
B. $FWDIR/conf/fwmonltor.def
C. $FWDIR/lib/tcpip.def
D. $FWDIR/lib/fw.monitor

Answer: A

NEW QUESTION 4
Which command is most useful for debugging the fwaccel module?

A. fw zdebug
B. securexl debug
C. fwaccel dbg
D. fw debug

Answer: C

NEW QUESTION 5
How many tiers of pattern matching can a packet pass through during IPS inspection?

A. 2
B. 1
C. 5
D. 9

Answer: A

NEW QUESTION 6
You have configured IPS Bypass Under Load function with additional kernel parameters ids_tolerance_no_stress=15 and ids_tolerance_stress-15 For configuration you used the *fw ctl set' command After reboot you noticed that these parameters returned to their default values What do you need to do to make this configuration work immediately and stay permanent?

A. Set these parameters again with "fw ctl set" and edit appropriate parameters in $FWDIR/boot/modules/ fwkern.conf
B. Use script $FWDIR/bin IpsSetBypass.sh to set these parameters
C. Set these parameters again with "fw ctl set" and save configuration with "save config"
D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Answer: A

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

NEW QUESTION 7
What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Answer: C

NEW QUESTION 8
What is the difference in debugging a S2S or C2S (using Check Point VPN Client) VPN?

A. there is no difference
B. the C2S VPN uses a different VPN daemon and there a second VPN debug
C. the C2S VPN can not be debugged as it uses different protocols for the key exchange
D. the C2S client uses Browser based SSL vpn and can't be debugged

Answer: D

NEW QUESTION 9
What does SIM handle?

A. Accelerating packets
B. FW kernel to SXL kernel hand off
C. OPSEC connects to SecureXL
D. Hardware communication to the accelerator

Answer: D

NEW QUESTION 10
What is connect about the Resource Advisor (RAD) service on the Security Gateways?

A. RAD has a kernel module that looks up the kernel cache, notifies client about hits and misses and forwards a-sync requests to RAD user space module which is responsible for online categorization
B. RAD is completely loaded as a kernel module that looks up URL in cache and if not found connects online for categorization There is no user space involvement in this process
C. RAD functions completely in user space The Pattern Matter (PM) module of the CMI looks up for URLs in the cache and if not found, contact the RAD process in user space to do online categorization
D. RAD is not a separate module, it is an integrated function of the 'fw1 kernel module and does all operations in the kernel space

Answer: C

NEW QUESTION 10
Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS. and compiles them together into unified Pattern Matchers?

A. CMI Loader
B. cpas
C. PSL - Passive Signature Loader
D. Context Loader

Answer: A

NEW QUESTION 15
Jenna has to create a VPN tunnel to a CISCO ASA but has to set special property to renegotiate the Phase 2 tunnel after 10 MB of transferee1 data. This can not be configured in the smartconsole, so how can she modify this property?

A. using GUIDBEDIT located in same directory as Smartconsole on the Windows client
B. she need to install GUIDBEDIT which can be downloaded from the Usercenter
C. she need to run GUIDBEDIT from CLISH which opens a graphical window on the smartcenter
D. this cant be done anymore as GUIDBEDIT is not supported in R80 anymore

Answer: C

NEW QUESTION 16
Which command is used to write a kernel debug to a file?

A. fw ctl debug -T -f > debug.txt
B. fw ctl kdebug -T -l > debug.txt
C. fw ctl debug -S -t > debug.txt
D. fw ctl kdebug -T -f > debug.txt

Answer: D

NEW QUESTION 21
Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Answer: B

NEW QUESTION 24
If you run the command "fw monitor -e accept src=10.1.1.201 or src=172.21.101.10 or src=192.0.2.10;" from the cli sh What will be captured?

A. Packets from 10 1 1 201 going to 192.0 2.10
B. Packets destined to 172 21 101 10 from 10.1.1.101
C. Only packet going to 192.0.2.10
D. fw monitor only works in expert mode so no packets will be captured

Answer: C

NEW QUESTION 26
You are trying to establish a VPN tunnel between two Security Gateways but fail. What initial steps will you make to troubleshoot the issue

A. capture traffic on both tunnel members and collect debug of IKE and VPND daemon
B. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags, then collect debug of IKE and VPND daemon
C. collect debug of IKE and VPND daemon and collect kernel debug for fw module with vm, crypt, conn and drop flags
D. capture traffic on both tunnel members and collect kernel debug for fw module with vm, crypt, conn and drop flags

Answer: A

NEW QUESTION 27
What is NOT a benefit of the fw ctl zdebug command?

A. Cannot be used to debug additional modules
B. Collect debug messages from the kernel
C. Clean the buffer
D. Automatically allocate a 1MB buffer

Answer: A

NEW QUESTION 31
Troubleshooting issues with Mobile Access requires the following:

A. Standard VPN debugs, packet captures, and debugs of cvpnd' process on Security Gateway
B. Standard VPN debugs and packet captures on Security Gateway, debugs of "cvpnd' process on Security Management
C. 'ma_vpnd' process on Secunty Gateway
D. Debug logs of FWD captured with the command - 'fw debug fwd on TDERROR_MOBILE_ACCESS=5'

Answer: A

NEW QUESTION 36
Which of the following is NOT a valid "fwaccel" parameter?

A. stat
B. stats
C. templates
D. packets

Answer: D

NEW QUESTION 41
You are running R80.XX on an open server and you see a high CPU utilization on your 12 CPU cores You now want to enable Hyperthreading to get more cores to gain some performance. What is the correct way to achieve this?

A. Hyperthreading is not supported on open servers, on on Check Point Appliances
B. just turn on HAT in the bios of the server and boot it
C. just turn on HAT in the bios of the server and after it has booted enable it in cpconfig
D. in dish run set HAT on

Answer: A

NEW QUESTION 44
Which Threat Prevention daemon is the core Threat Emulator, engine and responsible for emulation files and communications with Threat Cloud?

A. ctasd
B. inmsd
C. ted
D. scrub

Answer: C

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

NEW QUESTION 47
Check Point Threat Prevention policies can contain multiple policy layers and each layer consists of its own Rule Base Which Threat Prevention daemon is used for Anti-virus?

A. in.emaild.mta
B. in.msd
C. ctasd
D. in emaild

Answer: D

NEW QUESTION 52
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump
B. CPMIL dump
C. fw monitor
D. tcpdump

Answer: A

NEW QUESTION 54
Where will the usermode core files be located?

A. /var/log/dump/usermode
B. /var/suroot
C. SFWDIR/var'log/dump/usermode
D. SCPDIR/var/log/dump/usermode

Answer: A

NEW QUESTION 56
What command is usually used for general firewall kernel debugging and what is the size of the buffer that is automatically enabled when using the command?

A. fw ctl debug, buffer size is 1024 KB
B. fw ell zdebu
C. buffer size is 32768 KB
D. fw dl zdebug, buffer size is 1 MB
E. fw ctl kdeou
F. buffer size is 32000 KB

Answer: D

NEW QUESTION 58
Which command do you need to execute to insert fw monitor after TCP streaming (out) in the outbound chain using absolute position? Given the chain was 1ffffe0, choose the correct answer.

A. fw monitor –po -0x1ffffe0
B. fw monitor –p0 ox1ffffe0
C. fw monitor –po 1ffffe0
D. fw monitor –p0 –ox1ffffe0

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG

NEW QUESTION 60
Which command can be run in Expert mode to verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep $FWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm.conf

Answer: C

NEW QUESTION 65
What is the simplest and most efficient way to check all dropped packets in real time?

A. fw ctl zdebug * drop in expert mode
B. Smartlog
C. cat /dev/fwTlog in expert mode
D. tail -f SFWDIR/log/fw log |grep drop in expert mode

Answer: D

NEW QUESTION 68
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required"

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Answer: B

NEW QUESTION 72
The two procedures available for debugging in the firewall kernel are
i fw ctl zdebug
ii fw ctl debug/kdebug
Choose the correct statement explaining the differences in the two

A. (i) Is used for general debugging, has a small buffer and is a quick way to set kernel debug flags to get an output via command linewhereas (11) is useful when there is a need for detailed debugging and requires additional steps to set the buffer and get an output via command line
B. (i) is used to debug the access control policy only, however (n) can be used to debug a unified policy
C. (i) is used to debug only issues related to dropping of traffic, however (n) can be used for any firewall issue including NATing, clustering etc.
D. (i) is used on a Security Gateway, whereas (11) is used on a Security Management Server

Answer: C

NEW QUESTION 76
What command sets a specific interface as not accelerated?

A. noaccel-s<interface1>
B. fwaccel exempt state <interface1>
C. nonaccel -s <interface1>
D. fwaccel -n <intetface1 >

Answer: C

NEW QUESTION 77
To check the current status of hyper-threading, which command would you execute in expert mode?

A. cat /proc/hypert_status
B. cat /proc/smt_status
C. cat /proc/hypert_stat
D. cat /proc/smt_stat

Answer: B

NEW QUESTION 78
Which of the following inputs is suitable for debugging HTTPS inspection issues?

A. vpn debug cptls on
B. fw ctl debug –m fw + conn drop cptls
C. fw diag debug tls enable
D. fw debug tls on TDERROR_ALL_ALL=5

Answer: B

NEW QUESTION 81
What is the main SecureXL database for tracking acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: B

NEW QUESTION 86
An administrator receives reports about issues with log indexing and text searching regarding an existing Management Server. In trying to find a solution she wants to check if the process responsible for this feature is running correctly. What is true about the related process?

A. fwm manages this database after initialization of the ICA
B. cpd needs to be restarted manual to show in the list
C. fwssd crashes can affect therefore not show in the list
D. solr is a child process of cpm

Answer: D

NEW QUESTION 89
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-585 Practice Exam Features:

* 156-585 Questions and Answers Updated Frequently

* 156-585 Practice Questions Verified by Expert Senior Certified Staff

* 156-585 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-585 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year