CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
How can you start debug of the Unified Policy with all possible flags turned on?

A. fw ctl debug -m UP all
B. fw ctl debug -m UnifiedPolicy all
C. fw ctl debug -m fw + UP
D. fw ctl debug -m UP *

Answer: D

NEW QUESTION 3
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Answer: A

NEW QUESTION 4
When a User Mode process suddenly crashes it may create a core dump file. Which of the following information is available in the core dump and may be used to identify the root cause of the crash?
i Program Counter ii Stack Pointer
ii. Memory management information
iv Other Processor and OS flags / information

A. i, ii, lii and iv
B. i and n only
C. iii and iv only
D. D Only iii

Answer: C

NEW QUESTION 5
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 6
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 7
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 8
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 9
What components make up the Context Management Infrastructure?

A. CMI Loader and Pattern Matcher
B. CPMI and FW Loader
C. CPX and FWM
D. CPM and SOLR

Answer: A

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 10
Which Daemon should be debugged for HTTPS Inspection related issues?

A. FWD
B. HTTPD
C. WSTLSO
D. VPND

Answer: C

NEW QUESTION 12
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
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore you need to add a timestamp to the kernel debug and write the output to a file What is the correct syntax for this?

A. fw ctl kdebug -T -f > filename.debug
B. fw ctl kdebug -T > filename.debug
C. fw ctl debug -T -f > filename.debug
D. fw ctl kdebug -T -f -o filename.debug

Answer: C

NEW QUESTION 19
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 24
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 25
What are four main database domains?

A. System, Global, Log, Event
B. System, User, Host, Network
C. Local, Global, User, VPN
D. System, User, Global, Log

Answer: D

NEW QUESTION 30
If IPS protections that prevent SecureXL from accelerating traffic, such as Network Quota, Fingerprint Scrambling. TTL Masking etc, have to be used, what is a recommended practice to enhance the performance of the gateway?

A. Use the IPS exception mechanism
B. Disable all such protections
C. Disable SecureXL and use CoreXL
D. Upgrade the hardware to include more Cores and Memory

Answer: C

NEW QUESTION 31
Some users from your organization have been reporting some connection problems with CIFS since this morning You suspect an IPS issue after an automatic IPS update last night. So you want to perform a packet capture on uppercase I only directly after the IPS chain module (position 4 in the chain) to check If the packets pass the IPS. What command do you need to run?

A. fw monitor -ml -pi 5 -e <filterexperession>
B. fw monitor -pi 5 -e <filterexptession>
C. tcpdump -eni any <filterexpression>
D. fw monitor -pi asm <filtefexpfession>

Answer: C

NEW QUESTION 32
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
What is the correct syntax to set all debug flags for Unified Policy related issues?

A. fw ctl debug -m UP all
B. fw ctl debug -m up all
C. fw ctl kdebug -m UP all
D. fw ctl debug -m fw all

Answer: A

NEW QUESTION 41
What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap
B. .exe
C. .tgz
D. .pcap

Answer: A

NEW QUESTION 43

The management configuration stored in the Postgres database is partitioned into several relational database Domains, like - System, User, Global and Log Domains. The User Domain stores the network objects and security policies. Which of the following is stored in the Log Domain?

A. Configuration data of Log Servers and saved queries for applications
B. Active Logs received from Security Gateways and Management Servers
C. Active and past logs received from Gateways and Servers
D. Log Domain is not stored in Postgres database, it is part of Solr indexer only

Answer: D

NEW QUESTION 45
If the cpsemd process of SmartEvent has crashed or is having trouble coming up. then it usually indicates that .

A. Postgres database ts down
B. Cpd daemon is unable to connect to the log server
C. The SmartEvent core on the Solr mdexer has been deleted
D. The logged in administrator does not have permissions to run SmartEvent

Answer: C

NEW QUESTION 46
What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gatewa
C. Multi-Domain Server, SmartEvent Server
D. Management Serve
E. Log Serve
F. LDAP Server, Web Server
G. Management server Log server, Gateway serve
H. Security server

Answer: A

NEW QUESTION 48
Which of the following is NOT a valid "fwaccel" parameter?

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

Answer: D

NEW QUESTION 50
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 53
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file but you can’t afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

A. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
B. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
C. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
D. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Answer: D

NEW QUESTION 54
PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?

A. psql_client cpm postgres
B. mysql_client cpm postgres
C. psql_c!ieni postgres cpm
D. mysql -u root

Answer: A

NEW QUESTION 59
In Security Management High Availability, if the primary and secondary managements, running the same version of R80.x, are in a state of 'Collision', how can this be resolved?

A. Administrator should manually synchronize the servers using SmartConsole
B. The Collision state does not happen in R80.x as the synchronizing automatically on every publish action
C. Reset the SIC of the secondary management server
D. Run the command 'fw send synch force' on the primary server and 'fw get sync quiet' on the secondary server

Answer: A

NEW QUESTION 60
When a User process or program suddenly crashes, a core dump is often used to examine the problem. Which command is used to enable the core-dumping via GAIA dish?

A. set core-dump enable
B. set core-dump per_process
C. set user-dump enable
D. set core-dump total

Answer: A

NEW QUESTION 64
You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy After the upgrade you can't connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

A. new new console port is 19009 and a access rule ts missing
B. the license became invalig and the firewall does not start anymore
C. the upgrade process changed the interfaces and IP adresses and you have to switch cables
D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Answer: D

NEW QUESTION 65
Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
B. run vpn debug truncon
C. run fw ctl zdebug -m sslvpn all
D. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart

Answer: A

NEW QUESTION 68
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 71
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 76
What acceleration mode utlizes multi-core processing to assist with traffic processing?

A. CoreXL
B. SecureXL
C. HyperThreading
D. Traffic Warping

Answer: C

NEW QUESTION 80
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 84
Which of the following is contained in the System Domain of the Postgres database?

A. Saved queries for applications
B. Configuration data of log servers
C. Trusted GUI clients
D. User modified configurations such as network objects

Answer: C

NEW QUESTION 89
What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis
B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Answer: B

NEW QUESTION 93
Joey is configuring a site-to-site VPN with his business partner. On Joey’s site he has a Check Point R80.10 Gateway and his partner uses Cisco ASA 5540 as a gateway.
Joey’s VPN domain on the Check Point Gateway object is manually configured with a group object that contains two network objects:
VPN_Domain3 = 192.168.14.0/24 VPN_Domain4 = 192.168.15.0/24
Partner’s site ACL as viewed from “show run”
access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.14.0 255.255.255.0
access-list JOEY-VPN extended permit ip 172.26.251.0 255.255.255.0 192.168.15.0 255.255.255.0 When they try to establish VPN tunnel, it fails. What is the most likely cause of the failure given the
information provided?

A. Tunnel falls on partner sit
B. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/24 and 192.168.15.0/24, but the peer expects the one network 192.168.14.0/23
C. Tunnel fails on partner sit
D. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation.Check Point continues to present its own encryption domain as 192.168.14.0/23, but the peer expects the two distinct networks 192.168.14.0/24 and 192.168.15.0/24.
E. Tunnel fails on Joey’s site, because he misconfigured IP address of VPN peer.
F. Tunnel falls on partner sit
G. It is likely that the Cisco ASA 5540 will reject the Phase 2 negotiation due to the algorithm mismatch.

Answer: B

NEW QUESTION 97
Which command(s) will turn off all vpn debug collection?

A. vpn debug off
B. vpn debug -a off
C. vpn debug off and vpn debug ikeoff
D. fw ctl debug 0

Answer: C

NEW QUESTION 99
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 103
What process is responsible for sending and receiving logs in the management server?

A. FWD
B. CPM
C. FWM
D. CPD

Answer: A

NEW QUESTION 104
What is the best way to resolve an issue caused by a frozen process?

A. Reboot the machine
B. Restart the process
C. Kill the process
D. Power off the machine

Answer: B

NEW QUESTION 109
For TCP connections, when a packet arrives at the Firewall Kernel out of sequence or fragmented, which layer of IPS corrects this to allow for proper inspection?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Answer: A

NEW QUESTION 114
After kernel debug with "fw ctl debug" you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.

A. Use "fw ctl zdebug' because of 1024KB buffer size
B. Divide debug information into smaller files Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
C. Reduce debug buffer to 1024KB and run debug for several times
D. Use Check Point InfoView utility to analyze debug output

Answer: C

NEW QUESTION 117
What is the purpose of the Hardware Diagnostics Tool?

A. Verifying that Check Point Appliance hardware is functioning correctly
B. Verifying the Security Management Server hardware is functioning correctly
C. Verifying that Security Gateway hardware is functioning correctly
D. Verifying that Check Point Appliance hardware is actually broken

Answer: B

NEW QUESTION 119
How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Answer: A

NEW QUESTION 124
Which situation triggers an IPS bypass under load on a 24-core Check Point appliance?

A. any of the CPU cores is above the threshold for more than 10 seconds
B. all CPU core most be above the threshold for more than 10 seconds
C. a single CPU core must be above the threshold for more than 10 seconds, but is must be the same core during this time
D. the average cpu utilization over all cores must be above the threshold for 1 second

Answer: A

NEW QUESTION 126
What is the correct syntax to turn a VPN debug on and create new empty debug files?

A. vpn debug truncon

B. vpndebug trunc on
C. vpn kdebug on
D. vpn debug trunkon

Answer: D

NEW QUESTION 131
Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is used for Application & Control URL Filtering?

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

Answer: C

NEW QUESTION 132
What are the four ways to insert an FW Monitor into the firewall kernel chain?

A. Relative position using location, relative position using alias, absolute position, all positions
B. Absolute position using location, absolute position using alias, relative position, all positions
C. Absolute position using location, relative position using alias, general position, all positions
D. Relative position using geolocation, relative position using inertial navigation, absolute position, all positions

Answer: D

NEW QUESTION 136
What file contains the RAD proxy settings?

A. rad_settings.C
B. rad_services.C
C. rad_scheme.C
D. rad_control.C

Answer: A

NEW QUESTION 138
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 142
Which one of the following is NOT considered a Solr core partition:

A. CPM_0_Revisions
B. CPM_Global_A
C. CPM_Gtobal_R
D. CPM_0_Disabled

Answer: D

NEW QUESTION 147
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 151
John works for ABC Corporation. They have enabled CoreXL on their firewall John would like to identify the cores on which the SND runs and the cores on which the firewall instance is running. Which command should John run to view the CPU role allocation?

A. fw ctl affinity -v
B. fwaccel stat -I
C. fw ctl affinity -I
D. fw ctl cores

Answer: C

NEW QUESTION 155

.....

Relate Links

100% Pass Your 156-585 Exam with Exambible Prep Materials

https://www.exambible.com/156-585-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/