CheckPoint

Exam Questions 156-587

Check Point Certified Troubleshooting Expert - R81.20 (CCTE)

NEW QUESTION 1
You need to monitor traffic pre-inbound and before the VPN module in a Security Gateway. How would you achieve this using fw monitor?

A. fw monitor -p all
B. fw monitor -pi -vpn
C. fw monitor -pi +vpn
D. fw monitor -pi +vpn

Answer: B

NEW QUESTION 2
What is the proper command for allowing the system to create core files?

A. service core-dump start
B. SFWDIR/scripts/core-dump-enable.sh
C. set core-dump enable>save config
D. # set core-dump enable# save config

Answer: C

NEW QUESTION 3
You modified kernel parameters and after rebooting the gateway, a lot of production traffic gets dropped and the gateway acts strangely What should you do"?

A. Run command fw ctl set int fw1_kernel_all_disable=1
B. Restore fwkem.conf from backup and reboot the gateway
C. run fw unloadlocal to remove parameters from kernel
D. Remove all kernel parameters from fwkem.conf and reboot

Answer: B

NEW QUESTION 4
Which of the following is contained in the System Domain of the Postgres database?

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

Answer: A

NEW QUESTION 5
What is the best way to resolve an issue caused by a frozen process?

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

Answer: D

NEW QUESTION 6
What is the most efficient way to read an IKEv2 Debug?

A. IKEview
B. vi on the cti
C. notepad++
D. any xml editor

Answer: A

NEW QUESTION 7
The Check Point Watch Daemon (CPWD) monitors critical Check Point processes, terminating them or restarting them as needed to maintain consistent, stable operating conditions. When checking the status/output of CPWD you are able to see some columns like APP, PID, STAT, START, etc. What is the column "STAT" used for?

A. Shows the Watch Dog name of the monitored process
B. Shows the status of the monitored process
C. Shows how many times the Watch Dog started the monitored process
D. Shows what monitoring method Watch Dog is using to track the process

Answer: B

NEW QUESTION 8

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

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

Answer: B

NEW QUESTION 9
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 debug -T -f > filename debug
B. fw ctl kdebug -T -f -o filename debug
C. fw ell kdebug -T > filename debug
D. fw ctl kdebug -T -f > filename.debug

Answer: B

NEW QUESTION 10
Like a Site-to-Site VPN between two Security Gateways, a Remote Access VPN relies on the Internet Key Exchange (IKE) what types of keys are generated by IKE during negotiation?

A. Produce a symmetric key on both sides
B. Produce an asymmetric key on both sides
C. Symmetric keys based on pre-shared secret
D. Produce a pair of public and private keys

Answer: D

NEW QUESTION 10
The management configuration stored in the Postgres database is partitioned into several relational database domains. What is the purpose of the Global Domain?

A. Global Domains is used by the IPS software blade to map the IDs to the corresponding countries according to the IpToCountry.csv file.
B. This domain is used as the global database to back up the objects referencing the corresponding object attributes from the System Domain.
C. This domain is used as the global database to track the changes made by multiple administrators on the same objects prior to publishing.
D. This domain is used as the global database for MDSM and contains global objects and policies.

Answer: D

NEW QUESTION 11
In Check Point's Packet Processing Infrastructure what is the role of Observers?

A. Observers attach object IDs to traffic
B. They store Rule Base matching state related information
C. Observers monitor the state of Check Point gateways and report it to the security manager
D. Observers decide whether or not to publish a CLOB to the Security Policy

Answer: C

NEW QUESTION 12
When viewing data for CPMI objects in the Postgres database, what table column should be selected to query for the object instance?

A. CpmiHostCkp
B. fwset
C. CPM Global M
D. GuiDBedit

Answer: A

NEW QUESTION 17
How does Identity Collector connect to Windows Server?

A. ADQuery is needed for connection
B. LDAP connection
C. It uses a PDP demon to connect
D. via Windows API

Answer: D

NEW QUESTION 18
Where do you enable log indexing on the SMS?

A. SMS object under "Other"

B. SMS object under "Advanced"
C. SMS object under "Logs"
D. SMS object under "General Properties"

Answer: C

NEW QUESTION 21
Which Daemon should be debugged for HTTPS inspection related issues?

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

Answer: B

NEW QUESTION 22
What is the benefit of fw ctl debug over fw ctl zdebug?

A. There is no difference Both are used for debugging kernel
B. You don't need timestamps
C. It allows you to debug multiple modules at the same time
D. You only need 1MB buffer

Answer: C

NEW QUESTION 24
What cli command is run on the GW to verify communication to the identity Collector?

A. pdp connections idc
B. pep connections idc
C. show idc connections
D. fwd connected

Answer: A

NEW QUESTION 26
In the Security Management Architecture, what port and process does SmartConsole use to communicate with the Security Management Server?

A. CPM and 18190
B. FWM and 19009
C. CPM and 19009
D. CPM, 19009, and 18191

Answer: A

NEW QUESTION 30
When URL category is not found in the kernel cache, what action will GW do?

A. RAD In user space will forward request to the cloud
B. GW will update kernel cache during next policy install
C. RAD in kernel space will forward request to the cloud
D. RAD forwards this request to CMI which is the brain of inspection

Answer: A

NEW QUESTION 34
You found out that $FWDIR/log/fw.log is constantly growing in size at a Security Gateway, what is the reason?

A. TCP state logging is enabled
B. Its not a problem the gateways is logging connections and also sessions
C. fw.log can grow when GW does not have space in logging directory
D. The GW is logging locally

Answer: B

NEW QUESTION 38
In some scenarios it is very helpful to use advanced Linux commands for troubleshooting purposes. Which command displays information about resource utilization for running processes and shows additional information for core utilization and memory?

A. top
B. vmstat
C. cptop
D. mpstat

Answer: A

NEW QUESTION 41
When a user space process or program suddenly crashes, what type of file is created for analysis

A. core dump
B. kernel_memory_dump dbg
C. core analyzer
D. coredebug

Answer: A

NEW QUESTION 46
What does CMI stand for in relation to the Access Control Policy?

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

Answer: B

NEW QUESTION 47
What component is NOT part of Unified policy manager?

A. Classifier
B. CMI
C. Handle
D. Observer

Answer: D

NEW QUESTION 50
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?

A. Program Counteri
B. Stack Pointerii
C. Memory management informationi
D. Other Processor and OS flags / information
E. iii and iv only
F. i and ii only
G. i, ii, iii and iv
H. Only lii

Answer: C

NEW QUESTION 55
The Check Point Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process. There are two procedures available for debugging the firewall kernel. Which procedure/command is used for troubleshooting packet drops and other kernel activities while using minimal resources (1 MB buffer)?

A. fw ctl zdebug
B. fwk ell debug
C. fw debug ctl
D. fw ctl debug/kdebug

Answer: A

NEW QUESTION 56
SmartEvent utilizes the Log Server, Correlation Unit and SmartEvent Server to aggregate logs and identify security events. The three main processes that govern these SmartEvent components are:

A. cpcu, cplog, cpse
B. eventiasv, eventiarp,eventiacu
C. cpsemd, cpsead, and DBSync
D. fwd, secu, sesrv

Answer: B

NEW QUESTION 61
VPN issues may result from misconfiguration communication failure, or incompatible default configurations between peers. Which basic command syntax needs to be used for troubleshooting Site-toSite VPN Issues?

A. vpn truncon debug

B. cp debug truncon
C. fw debug truncon
D. vpn debug truncon

Answer: D

NEW QUESTION 65
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. Context Loader
B. PSL - Passive Signature Loader
C. cpas
D. CMI Loader

Answer: B

NEW QUESTION 70
You receive complains that Guest Users cannot login and use the Guest Network which is configured with Access Role of Guest Users. You need to verity the Captive Portal configuration. Where can
you find the config file?

A. on the gateway at $NACPORTAL_ HOME/conf/httpd_ nac.conf
B. on the management at SCPNAC_ HOME/conf/httpd_ nac.conf
C. on the management at SNACPORTAL_ HOME/conf/httpd_ nac.conf
D. on the gateway at $CPNAC_ HOME/conf/httpd_ nac.conf

Answer: A

NEW QUESTION 71
How many packets are needed to establish IKEv1?

A. Only three packets for main mode
B. 8
C. 5
D. 6

Answer: D

NEW QUESTION 73
Your users have some issues connecting with Mobile Access VPN to your gateway. How can you debug the tunnel establishment?

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

Answer: C

NEW QUESTION 78
.....

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

156-587 Practice Exam Features:

* 156-587 Questions and Answers Updated Frequently

* 156-587 Practice Questions Verified by Expert Senior Certified Staff

* 156-587 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-587 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year