156-115.80 Q&As

Check Point Certified Security Master - R80

Pass CheckPoint 156-115.80 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/156-115-80.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

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

Correct Answer: C

Reference: https://community.checkpoint.com/thread/6199-classifying-traffic-to-match-unified-policycolumn-objects

QUESTION 2

What command, when combined with IPS traffic, will give you information that can be used to determine if adjustments can be made to improve performance and security?

A. # fw ctl ips stats

B. # $FWDIR/bin/get_ips_statistics.sh

C. # $FWDIR/scripts/get_ips_statistics.sh

D. > show ips all statistics

Correct Answer: C

QUESTION 3

Where does the translation occur with Hide NAT?

A. The destination translation occurs at the client side

B. The source translation occurs at the server side

C. The source translation occurs at the client side

D. The destination translation occurs at the server side

Correct Answer: B

QUESTION 4

What process(es) should be checked if there is high I/O and you suspect it may be related to the Antivirus Software Blade?

A. avsp

B. dlpu and rad processes

C. cpta

D. cpm and fwm

Correct Answer: B

QUESTION 5

What is true about ike.elg file?

A. It contains the name of the VPN communities on the local security gateway

B. ike.elg is only present on the security manager

C. It is a debug file that contains information relevant to IKE phase 1 and phase 2 exchange

D. It is a binary file and needs a special app to open it.

Correct Answer: C

QUESTION 6

Which database domain stores URL filtering updates?

A. Threat Prevention Domain

B. Application Control domain

C. IPS Domain

D. Check Point Data Domain

Correct Answer: B

QUESTION 7

You have configured SecureXL NAT templates with the "fw ctl set" command. You check configuration and ensure that NAT templates were enabled. After an accidental reboot, you issue "fwaccel stat" and noticed that NAT Templates are not enabled. You need to permanently enable SecureXL NAT templates. What should you do?

A. Set NAT Templates with "fwaccel templates NAT" command and save configuration with "save config"

B. Enable NAT Templates again with "fw ctl set" and save configuration with "save config"

C. Enable NAT Templates again with "fw ctl set" and edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

D. Edit appropriate parameters in $FWDIR/boot/modules/fwkern.conf

Correct Answer: B

QUESTION 8

On a production Check Point Gateway that is running Check Point Acceleration features, is it possible to reset SIC without affecting the production machines?

A. Yes, use the cp_conf command

B. No, Reset SIC using cpconfig during a change window

C. Yes, use the vi utility to edit CP HKLM_registry.data Registry File

D. No, Reset SIC on the Gateway first and then in SmartConsole

Correct Answer: A

Reference: https://securityguy225.wordpress.com/2015/06/11/how-to-reset-sic-without-restarting-allcheckpoint-process/

QUESTION 9

What must be done for the "fw monitor" command to capture packets through the firewall kernel?

A. SecureXL must be disabled

B. ClusterXL must be temporarily disabled

C. Firewall policy must be re-installed

D. The output file must be transferred to a machine with WireShark

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk30583

QUESTION 10

The fw monitor output file type is?

A. Binary

B. ASCII text

C. ZIP

D. tar.gzip

Correct Answer: B

QUESTION 11

Which kernel table stores information about NAT connections?

A. connections

B. tab_nat_conn

C. xlate

D. fwx_alloc

Correct Answer: D

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk32224

QUESTION 12

Which IPS command debug tool can you use for troubleshooting IPS traffic?

A. ips debug traffic –o IPSdebug

B. ips debug –f /var/log/IPSdebug.txt

C. debug ips enable –o IPSdebug

D. ips debug –o IPSdebug

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/84627.htm#o84632

QUESTION 13

Which daemon would you debug if you have issues acquiring identities via identity sharing and identities with other gateways?

A. pdpd

B. wstlsd

C. iad

D. pepd

Correct Answer: A

Reference: https://sc1.checkpoint.com/documents/R76/ CP_R76_IdentityAwareness_AdminGuide/66477.htm

QUESTION 14

You suspect that IPS protections may be dropping legitimate traffic by mistake. To reduce the false positives, what GuiDBedit parameter could you enable to work with fw ctl zdebug drop to generate a more elaborate drop message for these packets?

A. enable_inspect_debug_ips_compilation

B. inspect_ips_debug_inspection

C. enable_inspect_debug_compilation

D. enable_inspect_debug_ips

Correct Answer: C

QUESTION 15

Which command(s) can be used to set up 5 core files per process?

A. set core-dump per_process 5 save config

B. set core-dump per_process amount = 5 save config

C. set core-dump per_process 5

D. add core-dump per_process 5 save config

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk92764