156-315.80^{Q&As}

Check Point Certified Security Expert (CCSE) R80

Pass CheckPoint 156-315.80 Exam with 100% Guarantee

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

https://www.certbus.com/156-315-80.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Address

B. Destination Address

C. TCP Acknowledgement Number

D. Source Port

Correct Answer: C

Connections are identified by the 5 tuple attributes: source address, destination address, source port, destination port, protocol. When the packets in a connection match all the 5 tuple attributes, the traffic flow can be processed on the accelerated path.

QUESTION 2

View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)
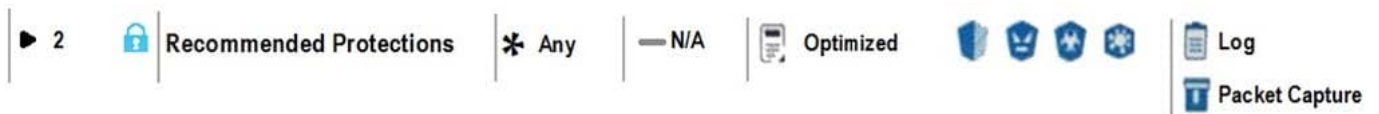
A. The current administrator has read-only permissions to Threat Prevention Policy.

B. Another user has locked the rule for editing.

C. Configuration lock is present. Click the lock symbol to gain read-write access.

D. The current administrator is logged in as read-only because someone else is editing the policy.

Correct Answer: B

https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265

QUESTION 3

SmartEvent uses it\\'s event policy to identify events. How can this be customized?

A. By modifying the firewall rulebase

B. By creating event candidates

C. By matching logs against exclusions

D. By matching logs against event rules

Correct Answer: D

QUESTION 4

You plan to automate creating new objects using new R80 Management API. You decide to use GAIA CLI for this task.

What is the first step to run management API commands on GAIA\\\'s shell?

A. mgmt_admin@teabag > id.txt

B. mgmt_login

C. login user admin password teabag

D. mgmt_cli login user "admin" password "teabag" > id.txt

Correct Answer: B

QUESTION 5

SandBlast offers businesses flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Service

B. Any Cloud Service

C. Threat Agent Service

D. Public Cloud Service

Correct Answer: A

QUESTION 6

SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic.

B. This statement is false because SecureXL does not improve this traffic but CoreXL does.

C. This statement is true because SecureXL does improve this traffic.

D. This statement is false because encrypted traffic cannot be inspected.

Correct Answer: C

SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

Reference: https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/10001/FILE/ SecureXL_and_Nokia_IPSO_White_Paper_20080401.pdf

QUESTION 7

Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

A. 50%

B. 75%

C. 80%

D. 15%

Correct Answer: D

QUESTION 8

What is the purpose of the CPCA process?

A. Monitoring the status of processes.

B. Sending and receiving logs.

C. Communication between GUI clients and the SmartCenter server.

D. Generating and modifying certificates.

Correct Answer: D

Reference: https://supportcenter.checkpoint.com/supportcenter/portal? eventSubmit_doGoviewsolutiondetails=andsolutionid=sk97638

QUESTION 9

In R80, where do you manage your Mobile Access Policy?

A. Access Control Policy

B. Through the Mobile Console

C. Shared Gateways Policy

D. From the Dedicated Mobility Tab

Correct Answer: A

QUESTION 10

What is the command used to activated Multi-Version Cluster mode?

A. set cluster member mvc on in Clish

B. set mvc on on Clish

C. set cluster MVC on in Expert Mode

D. set cluster mvc on in Expert Mode

Correct Answer: A

Reference: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ClusterXL_AdminGuide/ Topics-CXLG/Configuring-Multi-Version-Cluster-Mechanism.htm

QUESTION 11

What Factor preclude Secure XL Templating?

A. Source Port Ranges/Encrypted Connections

B. IPS

C. ClusterXL in load sharing Mode

D. CoreXL

Correct Answer: A

QUESTION 12

What needs to be configured if the NAT property `Translate destination or client side\' is not enabled in Global Properties?

A. A host route to route to the destination IP.

B. Use the file local.arp to add the ARP entries for NAT to work.

C. Nothing, the Gateway takes care of all details necessary.

D. Enabling `Allow bi-directional NAT\' for NAT to work correctly.

Correct Answer: C

QUESTION 13

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R80.10. Company\'s Developer Team is having random access issue to newly deployed Application Server in DMZ\'s Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela\'s desk for an investigation. Pamela decides to use Check Point\'s Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.

What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it\'s turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.

B. Pamela should check SecureXL status on DMZ Security Gateway and if it\'s turned OFF. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.

C. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.

D. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Correct Answer: A

QUESTION 14

Which method below is NOT one of the ways to communicate using the Management API\'s?

A. Typing API commands using the "mgmt_cli" command

B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Typing API commands using Gaia\'s secure shell(clish)19+

D. Sending API commands over an http connection using web-services

Correct Answer: D

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction%20

QUESTION 15

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?

A. Slow Path

B. Medium Path

C. Fast Path

D. Accelerated Path

Correct Answer: A