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.leads4pass.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

QUESTION 1

Which of the following is NOT an alert option?

A. SNMP

B. High alert

C. Mail

D. User defined alert

Correct Answer: B

Reference: https://sc1.checkpoint.com/documents/R77/ CP_R77_SmartViewMonitor_AdminGuide/101104.htm

QUESTION 2

What is the base level encryption key used by Capsule Docs?

A. RSA 2048

B. RSA 1024

C. SHA-256

D. AES

Correct Answer: A

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=andsolutionid=sk103706

QUESTION 3

When using CPSTAT, what is the default port used by the AMON server?

A. 18191

B. 18192

C. 18194

D. 18190

Correct Answer: B

Reference: https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/
CP_R80.20_M1_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R80.20_M1/ WebAdminGuides/EN/
CP_R80.20_M1_CLI_ReferenceGuide/162534

QUESTION 4

SandBlast agent extends 0 day prevention to what part of the network?

A. Web Browsers and user devices

B. DMZ server

C. Cloud

D. Email servers

Correct Answer: A

QUESTION 5

Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

A. Block Port Overflow

B. Local Interface Spoofing

C. Suspicious Activity Monitoring

D. Adaptive Threat Prevention

Correct Answer: C

Suspicious Activity Rules Solution Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access). The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

Reference: https://sc1.checkpoint.com/documents/R76/ CP_R76_SmartViewMonitor_AdminGuide/17670.htm