

CheckPoint

156-215.81.20

Check Point Certified Security Administrator (CCSA) R81.20

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

<https://www.testsexpert.com/>

- **Product Version**

Latest Version: 6.0

Question: 1

What is the most recommended installation method for Check Point appliances?

Response:

- A. USB media created with Check Point ISOMorphic.
- B. DVD media created with Check Point ISOMorphic.
- C. SmartUpdate installation.
- D. Cloud based installation.

Answer: A

Question: 2

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

Response:

- A. Interoperable Device
- B. Network Node
- C. Externally managed gateway
- D. Gateway

Answer: A

Question: 3

According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A(n):

Response:

- A. Gateway
- B. Interoperable Device
- C. Externally managed gateway
- D. Network Node

Answer: C

Question: 4

What is the difference between an event and a log?

Response:

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow from Trouble Ticket systems
- D. Logs and Events are synonyms

Answer: B

Question: 5

Using R81 Smart Console, what does a “pencil icon” in a rule mean?

Response:

- A. This rule is managed by check point’s SOC
- B. Someone else has changed this rule
- C. I have changed this rule
- D. This rule can’t be changed as it’s an implied rule

Answer: C

Question: 6

Which icon indicates that read/write access is enabled?

Response:

- A. Pencil
- B. Padlock
- C. Book
- D. Eyeglasses

Answer: A

Question: 7

What is true about the IPS-Blade?

Response:

-
- A. in R81, IPS is managed by the Threat Prevention Policy
 - B. in R81, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
 - C. in R81, IPS Exceptions cannot be attached to “all rules”
 - D. in R81, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

Question: 8

On R81.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

Response:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

Question: 9

What are the three authentication methods for SIC?

Response:

- A. Passwords, Users, and standards-based SSL for the creation of secure channels
- B. Certificates, standards-based SSL for the creation of secure channels, and 3DES or AES128 for encryption
- C. Packet Filtering, certificates, and 3DES or AES128 for encryption
- D. Certificates, Passwords, and Tokens

Answer: B

Question: 10

How is communication between different Check Point components secured in R81?

As with all questions, select the best answer.

Response:

- A. By using IPSEC
- B. By using SIC

-
- C. By using ICA
 - D. By using 3DES

Answer: B

For More Information – Visit link below:
<https://www.testsexpert.com/>

16\$ Discount Coupon: **9M2GK4NW**

Features:

■ Money Back Guarantee.....



■ 100% Course Coverage.....



■ 90 Days Free Updates.....



■ Instant Email Delivery after Order.....

