

CheckPoint

156-915.80 Exam

Check Point Certified Security Expert Update - R80.10

**Questions & Answers
Demo**

Version: 11.0

Topic 1, Main Questions

Question: 1

What is the port used for SmartConsole to connect to the Security Management Server:

- A. CPMI port 18191/TCP
- B. CPM port / TCP port 19009
- C. SIC port 18191/TCP
- D. https port 4434/TCP

Answer: A

Question: 2

Which is the correct order of a log flow processed by SmartEvents components:

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

Question: 3

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

These are the types of Automatic Reactions:

Mail - tell an administrator by email that the event occurred. See Create a Mail Reaction.

Block Source - instruct the Security Gateway to block the source IP address from which this event was

detected for a configurable period of time . Select a period of time from one minute to more than three weeks. See Create a Block Source Reaction

Block Event activity - instruct the Security Gateway to block a distributed attack that emanates from multiple sources, or attacks multiple destinations for a configurable period of time. Select a period of time from one minute to more than three weeks). See Create a Block Event Activity Reaction.

External Script - run a script that you provide. See Creating an External Script Automatic Reaction to write a script that can exploit SmartEvent data.

SNMP Trap - generate an SNMP Trap. See Create an SNMP Trap Reaction.

Question: 4

Which components allow you to reset a VPN tunnel?

- A. vpn tu command or SmartView monitor
- B. delete vpn ike sa or vpn she11 command
- C. vpn tunnelutil or delete vpn ike sa command
- D. SmartView monitor only

Answer: D

Question: 5

When synchronizing clusters, which of the following statements is FALSE?

- A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
- B. Only cluster members running on the same OS platform can be synchronized.
- C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
- D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D
