Checkpoint

Exam 156-315.77

Check Point Certified Security Expert

Version: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Check Point Technology Overview	3
Topic 5: User Management and Authentication	1
Topic 8: Configuring VPN tunnels	1
Topic 10: Mixed questions Set A	1
Topic 11: Mixed Questions Set B	3
Topic 12: Mixed Questions Set C	1

Topic 1, Check Point Technology Overview

Question No : 1 - (Topic 1)

A tracked SmartEvent Candidate in a Candidate Pool becomes an Event. What does NOT happen in the Analyzer Server?

A. SmartEvent provides the beginning and end time of the Event.
B. The Event is kept open, but condenses many instances into one Event.
C. The Correlation Unit keeps adding matching logs to the Event.
D. SmartEvent stops tracking logs related to the Candidate.

Answer: D

Question No : 2 - (Topic 1)

If ClusterXL Load Sharing is enabled with state synchronization enabled, what will happen if one member goes down?

A. The processing of all connections handled by the faulty machine is immediately taken over by the other member(s).
B. The processing of all connections handled by the faulty machine is dropped, so all connections need to be re-established through the other machine(s).
C. There is no state synchronization on Load Sharing, only on High Availability.
D. The connections are dropped as Load Sharing does not support High Availability.

Answer: A

Question No : 3 - (Topic 1)

In a UNIX environment, SmartReporter Data Base settings could be modified in:

A. $CPDIR/Database/conf/conf.C
B. $RTDIR/Database/conf/my.cnf
C. $ERDIR/conf/my.cnf
D. $FWDIR/Eventia/conf/ini.C

Answer: B

Topic 5, User Management and Authentication

Question No : 4 - (Topic 5)

When an Endpoint user is able to authenticate but receives a message from the client that it is unable to enforce the desktop policy, what is the most likely scenario?

A. The gateway could not locate the user in SmartDirectory and is allowing the connection with limitations based on a generic profile.
B. The user's rights prevent access to the protected network.
C. A Desktop Policy is not configured.
D. The user is attempting to connect with the wrong Endpoint client.

Answer: D

Topic 8, Configuring VPN tunnels

Question No : 5 - (Topic 8)

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

A. VTIs are assigned only local addresses, not remote addresses
B. VTIs cannot share IP addresses
C. VTIs are only supported on IPSO
D. VTIs cannot use an already existing physical-interface IP address

Answer: D

Topic 10, Mixed questions Set A

Question No : 6 - (Topic 10)

Using SmartProvisioning Profiles, which of the following could be configured for both Secure Platform and UTM-1 Edge devices?

(i) Backup

(ii) Routing

(iii) Interfaces

(iv) Hosts

(v) NTP server

(vi) DNS

A. (ii), (iii), (iv) and (vi)
B. (i), (iii), (iv) and (vi)
C. none of these options are available for both.
D. (i), (ii) and (iv)

Answer: C

Topic 11, Mixed Questions Set B

Question No : 7 - (Topic 11)

Your company is planning on moving their server farm to a new datacenter which requires IP changes to important network services including DNS, DHCP, and TFTP. Rather than manually logging in to all your firewalls and modifying the settings individually, you decide to purchase and enable SmartProvisioning. Assuming all your firewalls are on SPLAT, what is the minimum version required to update the firewalls' DNS and backup settings via SmartProvisioning?

A. R62
B. R60 HFA 02
C. R65 HFA 40
D. R71

Answer: C

Question No : 8 - (Topic 11)

Which is the BEST configuration option to protect internal users from malicious Java code, without stripping Java scripts?

A. Use the URI resource to block Java code
B. Use CVP in the URI resource to block Java code
C. Use the URI resource to strip applet tags
D. Use the URI resource to strip ActiveX tags

Answer: A

Question No : 9 - (Topic 11)

Which of the following is supported with Office Mode?

A. Secure mote
B. Secure Client
C. SSL Network Extender
D. Connect Mode

Answer: A

Topic 12, Mixed Questions Set C

Question No : 10 - (Topic 12)

Which of the following statements about the Port Scanning feature of IPS is TRUE?

A. The default scan detection is when more than 500 open inactive ports are open for a period of 120 seconds.
B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. Port Scanning does not block scanning; it detects port scans with one of three levels of detection sensitivity.
D. When a port scan is detected, only a log is issued, never an alert.

Answer: C