

Section: 313 Questions

QUESTION NO: 1

Which SmartEvent, what is the Correlation Unit's function?

- A. Invoke and define automatic reactions and add events to the database
- B. Assign severity levels to events
- C. Display received threats and tune the Events Policy
- D. Analyze log entries, looking for Event Policy patterns

Answer: D

QUESTION NO: 2

How do you verify the Check Point kernel running on a firewall?

- A. fw ctrl get kernel
- B. fw ctrl pstat
- C. fw kernel
- D. fw ver -k

Answer: D

QUESTION NO: 3

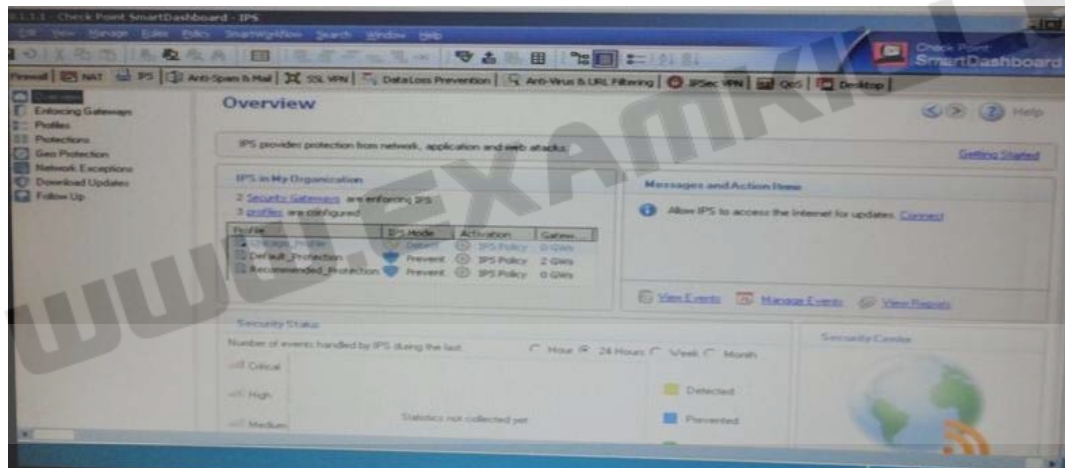
After repairing a Smart Workflow session:

- A. The session moves to status Repaired and a new session can be started
- B. The session moves to status Awaiting Repair and must be resubmitted
- C. The session is continued with status Not approved and a new session must be started
- D. The session is discarded and a new session is automatically started

Answer: B

QUESTION NO: 4

TotallyCoolSecurity Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-Chicago using Detect mode. After reviewing Matt noticed that fw-Chicago is not detecting any of the IPS protections that Bob had previously setup. Analyze the output below and determine how Matt corrects the problem.



- A. Matt should assign the fw-Chicago Security Gateway to the Chicago_Profile.
- B. Matt should the Chicago_Profile to use Protect mode because Detect mode
- C. Matt should re-create the Chicago_Profile and select Active protections manually instead of per the IPS Policy.
- D. Matt should activate the Chicago_Profile as it is currently not activated.

Answer: A

QUESTION NO: 5

Which Remote Desktop protocols are supported natively in SSL VPN?

- A. Microsoft RDP only
- B. AT&T VNC and Microsoft RDP
- C. Citrix ICA and Microsoft RDP
- D. AT&T VNC, Citrix ICA and Microsoft RDP

Answer: D

QUESTION NO: 6

To force clients to use integrity Security Workspace when accessing sensitive applications, the Administrator can configure Connectra:

- A. Via protection levels
- B. To implement integrity Clientless Security
- C. To force the user to re-authenticate at login
- D. Without a special setting. Secure Workspace is automatically configured.

Answer: A

QUESTION NO: 7

The default port for browser access to the Management Portal is

- A. 4433
- B. 4343
- C. 8080
- D. 443

Answer: A

QUESTION NO: 8

In which case is a Sticky Decision Function relevant?

- A. Load Sharing - Unicast
- B. Load Balancing - Forward
- C. High Availability
- D. Load Sharing - Multicast

Answer: D

QUESTION NO: 9

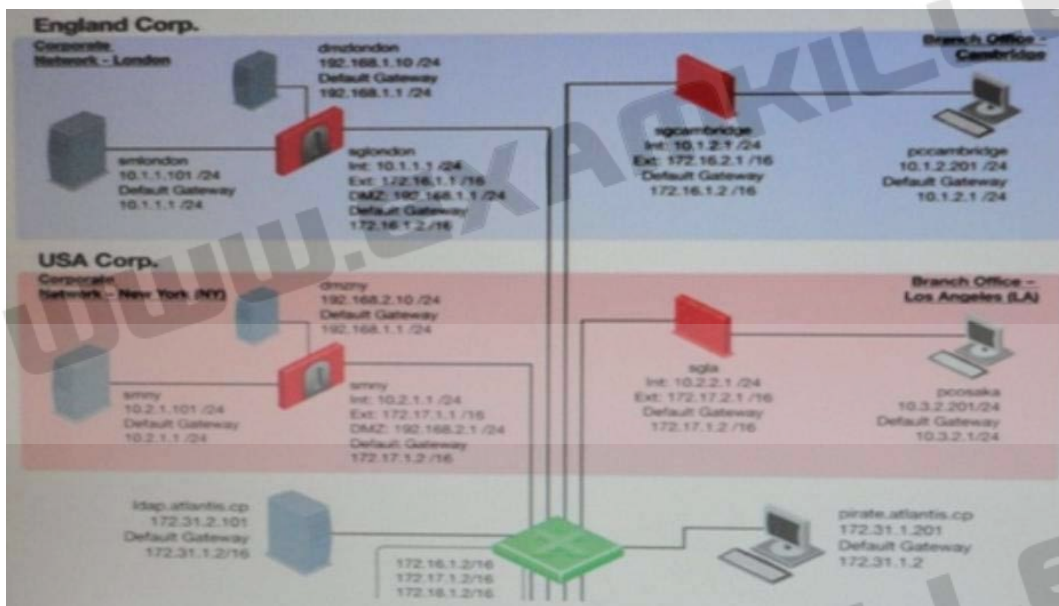
You just upgraded to R71 and are using the IPS Software Blade You want to enable all critical protections while keeping the rate of false positives very low. How can you achieve this?

- A. The new IPS system is based on policies, but it has no ability to calculate or change the confidence level, so it always has a high rate of false positives.
- B. This can't be achieved; activating any IPS system always causes a high rate of false positives.
- C. The new IPS system is based on policies and gives you the ability to activate all checks with critical severity and a high confidence level.
- D. As in SmartDefense, this can be achieved by activating all the critical checks manually.

Answer: C

QUESTION NO: 10

Refer to the network topology below. You have IPS Software Blades active on the Security Gateways sglondon, sgl, and sgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?



- A. All of these options are possible.
- B. The attacker may have used a bunch of evasion techniques like using escape sequence instead of cleartext commands. It is also possible that there are entry points not shown in the network layout, like rogue access points.
- C. Since other Gateways do not have IPS activated, attacks may originate from their network without anyone noticing.

D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-tuned anomaly algorithms. Even if this is accomplished, no technology can offer 100 % protection.

Answer: C

QUESTION NO: 11

Which of the following is NOT an Smartevent event-triggered Automatic Reaction?

- A. Mail
- B. Block Access
- C. External Script
- D. SNMP Trap

Answer: B

QUESTION NO: 12

Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?

- i Use same hard drive for database directory, log files and temporary directory
- ii Use Consolidation Rules
- iii Limit logging to blocked traffic only
- iv Using Multiple Database Tables

- A. (i), (ii) and (iv)
- B. (i), (iii), (iv)
- C. (ii) and (iv)
- D. (i) and (ii)

Answer: C

QUESTION NO: 13

What SmartConsole application allows you to change the Log Consolidation Policy?