

Exam Number/Code : 156-915.71

Exam Name : Check Point Certified
Security Expert R71
Update

Version : Demo

<http://cert24.com/>

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

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

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

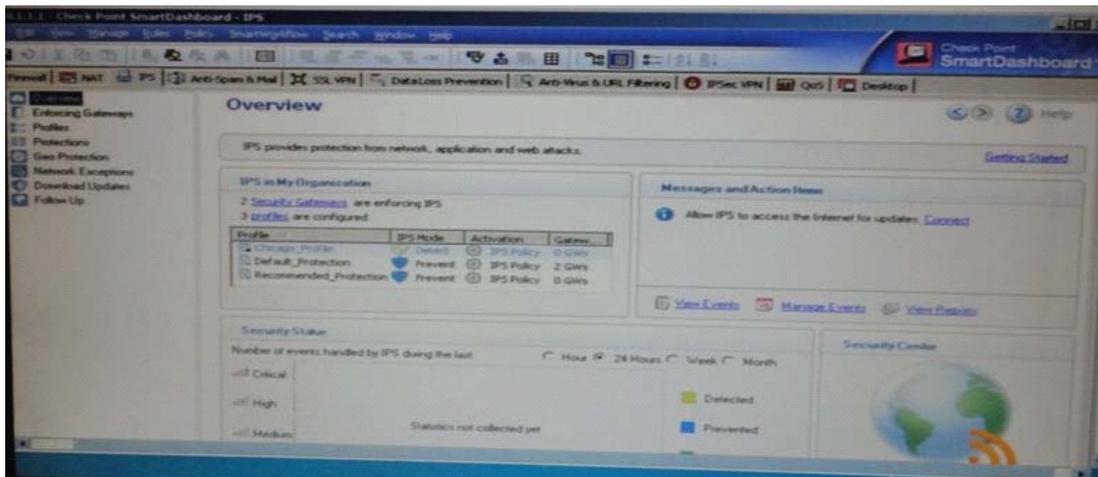
Answer: D

3. After repairing a SmartWorkflow 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

4. TotallyCoolSecurity Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-Chicagousing 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-ChicagoSecurity Gateway to theChicago_Profile.
- B. Matt should theChicago_Profile to useProtect mode because Detect mode
- C. Matt should re-create theChicago_Profile and select Activeprotections manually instead of per theIPSPolicy.

D. Matt should activate the Chicago_Profile as it is currently not activated.

Answer: A

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

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

7. The default port for browser access to the Management Portal is

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

Answer: A

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

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 cannot be achieved; activating any IPS system always causes a high rate of false

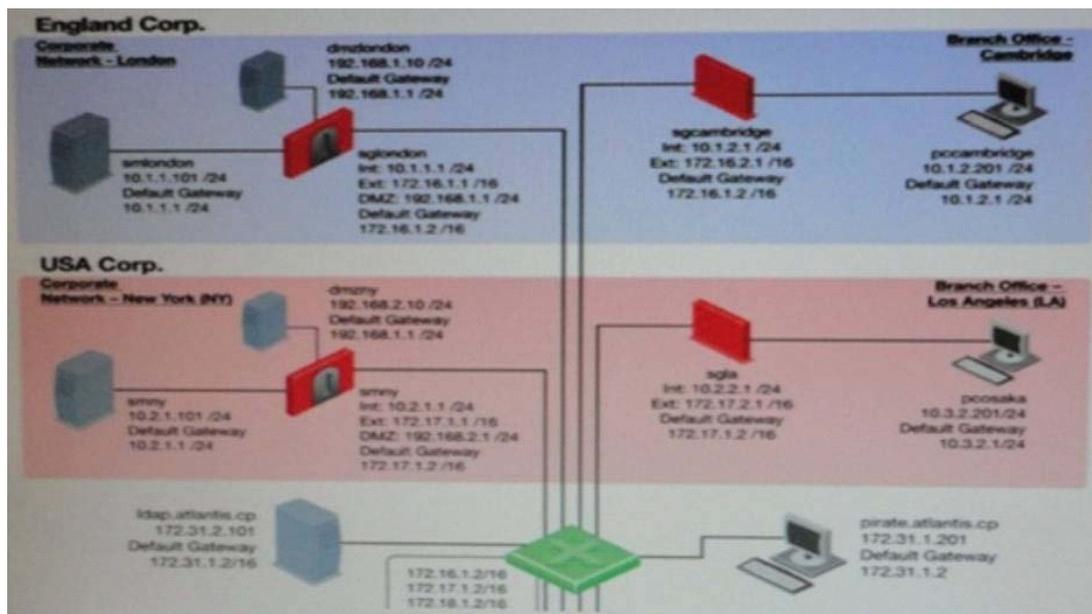
positives.

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

10. Refer to the network topology below. You have IPS Software Blades active on the Security Gateways *sglondon*, *sgla*, 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, network technology can offer 100% protection.

Answer: C

11. Which of the following is NOT a SmartEvent event-triggered Automatic Reaction?

A. Mail

B. Block Access

C. External Script

D. SNMP Trap

Answer: B

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?

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

Answer: C

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

- A. SmartReporter
- B. SmartUpdate
- C. SmartEvent Server
- D. Smart Dashboard

Answer: A

14. In configure a client to properly log in to the user portal using a certificate, the Administrator MUST:

- A. Create an internal user in the admin portal.
- B. Install an R71 internal Certificate Authority certificate.
- C. Create a client certificate from Smart Dashboard
- D. Store the client certificate on the SSL VPN Gateway

Answer: C

15. What process manages the dynamic routing protocols (ospf, RIP, etc) on SecurePlatform Pro?

- A. gated
- B. arouted
- C. routerd
- D. There is no separate process, but the Linux default router can take care of that.

Answer: A

16. To change the default port of the Management Portal,

- A. Edit the masters.conf file on the Portal server.
- B. Modify the file cp_httpd_admin.conf.
- C. Run sysconfig and change the management interface
- D. Re-initialize SIC.

Answer: C

17. Where do Gateways managed by SmartProvisioning fetch their assigned profiles?

- A. The Smartview Monitor
- B. The standalone SmartProvisioning server
- C. The Security Management server or CMA
- D. They are fetched locally from the individual device

Answer: C

18. When synchronizing clusters, which of the following statements is NOT true?

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

Answer: D

19. What command will allow you to disable sync on a cluster firewall member?

- A. `fw ctl setaync 0`
- B. `fw ctl syncstat stop`
- C. `fw ctl syncstat off`
- D. `fw ctl setsync off`

Answer: D

20. By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:

- A. The Security Policy is saved.
- B. The Security Policy is installed.
- C. The user database is installed.
- D. The standby Security Management Server starts for the first time.

Answer: A