

ACCA 7032 Sample Questions

1. Which default Gaia user has full read/write access?

- A. superuser
- B. monitor
- C. altuser
- D. admin

2. Which SmartConsole tab is used to monitor network and security performance?

- A. Logs Monitor
- B. Manage Settings
- C. Security Policies
- D. Gateway Servers

3. In SmartConsole, on which tab are Permissions and Administrators defined?

- A. MANAGE & SETTINGS
- B. SECURITY POLICIES
- C. GATEWAYS & SERVERS
- D. LOGS & MONITOR

4. In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server?

- A. Verify and compile Security Policies.
- B. Display policies and logs on the administrator's workstation.
- C. Store firewall logs to hard drive storage.
- D. Manage the object database.

5. True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

- A. True, every administrator works on a different database that is independent of the other administrators
- B. False, only one administrator can login with write permission
- C. True, every administrator works in a session that is independent of the other administrators
- D. False, this feature has to be enabled in the Global Properties

6.If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

- A. Delete older versions of database.
- B. Publish or discard the session.
- C. Revert the session.
- D. Save and install the Policy.

7.Which two statements are characteristics of a virus? (Choose two.)

- A. A virus typically requires end-user activation.
- B.A virus has an enabling vulnerability, a propagation mechanism, and a payload.
- C. A virus replicates itself by independently exploiting vulnerabilities in networks.
- D. A virus provides the attacker with sensitive data, such as passwords.
- E. A virus can be dormant and then activate at a specific time or date.

8.What are the two deployment options available for a security gateway?

- A. Bridge and Switch
- B. Local and Remote
- C. Cloud and Router
- D. Standalone and Distributed

9.One of major features in SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

- A. AdminB sees a pencil icon next the rule that AdminB is currently editing.
- B. AdminA, AdminB and AdminC are editing three different rules at the same time.
- C. AdminA and AdminB are editing the same rule at the same time.
- D. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.

10.Which one of the following is the preferred licensing model? Select the BEST answer.

- A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.

- **B.** Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
- **C.** Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency on the gateway.
- **D.** Central licensing because it ties the package license to the MAC-address of the Security Management Server's Mgmt-interface and has no dependency on the gateway.

11.A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _____.

- **A.** Two; Security Management and Endpoint Security
- **B.** Three; Security Management, Security Gateway, and Endpoint Security
- **C.** Three; Security Gateway, Endpoint Security, and Gateway Management
- **D.** Two; Endpoint Security and Security Gateway

12.Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

- **A.** Formal
- **B.** Central
- **C.** Local
- **D.** Corporate

13.Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

- **A.** Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- **B.** Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
- **C.** Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
- **D.** Tom's changes will be lost since he lost connectivity and he will have to start again.

14. In which deployment is the security management server and Security Gateway installed on the same appliance?

- **A.** Switch

- B. Standalone
- C. Distributed
- D. Remote

15. What is the default shell of Gaia CLI?

- A. Read-only
- B. Expert
- C. Clish
- D. Bash

16. What are two basic rules Check Point recommends for building an effective security policy?

- A. Accept Rule and Drop Rule
- B. Explicit Rule and Implied Rule
- C. Cleanup Rule and Stealth Rule
- D. NAT Rule and Reject Rule

17. When dealing with policy layers, what two layer types can be utilized?

- A. Inbound Layers and Outbound Layers
- B. Ordered Layers and Inline Layers
- C. Structured Layers and Overlap Layers
- D. R81.X does not support Layers

18. What are the three main components of Check Point security management architecture?

- A. Smart Console, Standalone, Security Management Server
- B. Policy-Client, Security Management Server, Security Gateway
- C. SmartConsole, Security Policy Server, Logs & Monitoring
- D. SmartConsole, Security Management Server, Security Gateway

19. Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Threat Extraction
- B. Threat Emulation
- C. Firewall
- D. Application Control

20.By default, which port is used to connect to the GAIa Portal?

- A. 4434
- B. 80
- C. 8080
- D. 443

21.What is a characteristic of a Trojan Horse ?

A.A Trojan Horse can be carried in a virus or worm

B. A proxy Trojan Horse opens port 21 on the target system.

C.A FTP Trojan Horse stops anti-virus programs or firewalls from functioning.

D.A Trojan Horse can be hard to detect because it closes when the application that launches it closes

22.Choose what BEST describes a Session.

- A. Sessions ends when policy is pushed to the Security Gateway.
- B. Sessions locks the policy package for editing.
- C. Starts when an Administrator logs in through SmartConsole and ends when the Administrator logs out.
- D. Starts when an Administrator publishes all the changes made on SmartConsole.

23.Which of the following is a valid deployment option?

- A. CloudSec deployment
- B. Disliked deployment
- C. Router only deployment
- D. Standalone deployment

24. occurs during a spoofing attack?

A.One device falsifies data to gain access to privileged information.

B. Large amounts of network traffic are sent to a target device to make resources unavailable to intended users.

C. Improperly formatted packets are forwarded to a target device to cause the target system to crash.

D.A program writes data beyond the allocated memory to enable the execution of malicious code.

25 In the SmartConsole, which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Read Only All
- B. Full Access
- C. Editor
- D. Super User

26 Which type of Check Point license ties the package license to the IP address of the Security Management Server?

- A. Formal
- B. Corporate
- C. Central
- D. Local

27 Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? Choose the BEST answer.

- A. Anti-Malware
- B. Content Awareness
- C. Anti-Virus
- D. IPS

28. URL Filtering cannot be used to:

- A. Control Data Security
- B. Decrease legal liability
- C. Improve organizational security
- D. Control Bandwidth issues

29. Which one of the following is TRUE?

- A. One policy can be either inline or ordered, but not both.
- B. Inline layer can be defined as a rule action.
- C. Ordered policy is a sub-policy within another policy.
- D. Pre-R80 Gateways do not support ordered layers.

30. Fill in the blanks: A Check Point software license consists of a _____ and _____.

- A. Software container; software package
- B. Software package; signature
- C. Signature; software blade
- D. Software blade; software container

31. Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

- A. 192.168.1.1 AND 172.26.1.1 AND drop
- B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
- C. 192.168.1.1 OR 172.26.1.1 AND action:Drop
- D. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop

32. Fill in the blanks: The _____ collects logs and sends them to the _____.

- A. Log server; Security Gateway
- B. Security Gateways; log server
- C. Log server; security management server
- D. Security management server; Security Gateway

33. What is the main objective when using Application Control?

- A. To see what users are doing.
- B. Ensure security and privacy of information.
- C. To filter out specific content.
- D. To assist the firewall blade with handling traffic.

34. Fill in the blanks: In _____ NAT, Only the _____ is translated.

- A. Hide; source
- B. Simple; source
- C. Static; source
- D. Hide; destination

Application Control/URL filtering database library is known as:

- A. AppWiki
- B. Application-Forensic Database
- C. Application Library
- D. Application database

35. Which of the following technologies extracts detailed information from packets and stores that information in different tables?

- A. Application Layer Firewall
- B. Packet Filtering
- C. Next-Generation Firewall
- D. Stateful Inspection

36. A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

- A. Security Zones are not supported by Check Point firewalls.
- B. The firewall rule can be configured to include one or more subnets in a zone.
- C. The zone is based on the network topology and determined according to where the interface leads to.
- D. The local directly connected subnet defined by the subnet IP and subnet mask.

37. Which encryption algorithm is the least secured?

- A. 3DES
- B. AES-128
- C. DES
- D. AES-256

38. What is the default tracking option of a rule?

- A. None
- B. Alert
- C. Log
- D. Tracking

39. Which of the following situations would not require a new license to be generated and installed?

- A. The existing license expires.
- B. The Security Gateway is upgraded.
- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

40. Fill in the blank: In order to install a license, it must first be added to the _____.

- A. Package repository

- B. Download Center Web site
- C. License and Contract repository
- D. User Center

41. Which is a main component of the Check Point security management architecture?

- A. Proxy Server
- B. Endpoint VPN client
- C. Identity Collector
- D. SmartConsole

42. An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this?

A. Trust exploitation

B. Buffer overflow

C. Man in the middle

D. Port redirection

43. What are the two types of NAT supported by the Security Gateway?

- A. Destination and Hide
- B. Source and Destination
- C. Static and Source
- D. Hide and Static

44. Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Anti-spam and Email Security
- B. Anti-Virus
- C. Firewall
- D. Application Control

45. Why is a Central License the preferred and recommended method of licensing?

- **A.** Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.
- **B.** Central Licensing actually not supported with Gaia.
- **C.** Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
- **D.** Central Licensing is the only option when deploying Gaia.

46. In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

- **A.** Install policy
- **B.** Publish changes
- **C.** Install database
- **D.** Save changes

47. A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe?

- A. Denial of Service
- B. Port redirection
- C. Reconnaissance
- D. Trust exploitation

48. A layer can support different combinations of blades. What are the supported blades:

- **A.** Firewall, NAT, Content Awareness and Mobile Access
- **B.** Firewall, URLF, Content Awareness and Mobile Access
- **C.** Firewall (Network Access Control), Application & URL Filtering and Content Awareness
- **D.** Firewall (Network Access Control), Application & URL Filtering, Content Awareness and Mobile Access

49. What licensing feature automatically verifies current licenses and activates new licenses added to the License and Contracts repository?

- **A.** Automatic Licensing and Verification tool
- **B.** Verification licensing

- C. Verification tool
- D. Automatic licensing

50. Which option in tracking allows you to see the amount of data passed in the connection?

- A. Advanced
- B. Accounting
- C. Data
- D. Logs

51. Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

- A. Manual NAT can offer more flexibility than Automatic NAT.
- B. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
- C. Automatic NAT can offer more flexibility than Manual NAT.
- D. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.

52. Which one is not a primary goal of network security?

- A. Confidentiality
- B. Redundancy
- C. Integrity
- D. Availability

53. Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

- A. Threat Emulation
- B. Anti-Virus
- C. Advanced Networking Blade
- D. Application Control

54. What is the main difference between Static NAT and Hide NAT?

- A. Static NAT only allows outgoing connections. Hide NAT allows incoming and outgoing connections.
- B. Hide NAT only allows incoming connections to protect your network.
- C. Static NAT allow incoming and outgoing connections. Hide NAT only allows outgoing connections.

- D. Static NAT only allows incoming connections to protect your network.

55. What default layers are included when creating a new policy layer?

- A. Application Control, URL Filtering and Threat Prevention
- B. Firewall, Application Control and IPSec VPN
- C. Firewall, Application Control and IPS
- D. Access Control, Threat Prevention and HTTPS Inspe

56. What are the types of Software Containers?

- A. Smart Console, Security Management, and Security Gateway
- B. Security Management, Security Gateway, and Endpoint Security
- C. Security Management, Standalone, and Security Gateway
- D. Security Management, Log & Monitoring, and Security Policy

57. In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

- A. The installation can be done on virtual machines only, but not on appliances and not in mixed environments.
- B. The installation is done on different computers or appliances.
- C. The installation is done on the same computer or appliance.
- D. The installation is allowed in Azure only but not in AWS cloud environments.

58. Fill in the blanks: Gaia can be configured using the _____ or _____.

- A. GaiaUI; command line interface (serial console only)
- B. Gaia Interface; Gaia Ultimate Shell
- C. Command line interface; GAiA Portal
- D. Web Ultimate Interface; Gaia Interface (SSH)

59. How many users can have read/write access in Gaia Operating System at one time?

- A. One
- B. Two
- C. Three
- D. Infinite

60. Which part of SmartConsole allows administrators to add, edit, delete, and clone objects?

- A. Object Explorer
- B. Object Navigator
- C. Object Editor

- D. Object Browser

61. True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.

- A. True, Central Licenses can be installed with CPLIC command on a Security Gateway
- B. True, CLI is the preferred method for Licensing
- C. False, Central Licenses are installed via Gaia on Security Gateways
- D. False, Central Licenses are handled via Security Management Server

62. What is the purpose of the Stealth Rule?

- A. To reduce the amount of logs for performance issues.
- B. To reduce the number of rules in the database.
- C. To prevent users from directly connecting to a Security Gateway.
- D. To make the gateway visible to the Internet.

63. Which policy type is used to enforce bandwidth and traffic control rules?

- A. Threat Prevention
- B. QoS
- C. Threat Emulation
- D. Access Control

64. What type of NAT is a one-to-one relationship where each host is translated to a unique address?

- A. Source
- B. Destination
- C. Hide
- D. Static

65. Which Autonomous Threat Prevention profile uses sanitization technology?

- A. Cloud/data Center
- B. Guest Network
- C. Sandbox
- D. Perimeter

66. In the Check Point Security Management Architecture, which component(s) can store logs?

- A. Security Management Server and Security Gateway

- B. SmartConsole
- C. SmartConsole and Security Management Server
- D. Security Management Server

67. Which of the following is NOT a tracking log option in R81.x?

- A. Full Log
- B. Log
- C. Detailed Log
- D. Extended Log

68. Which information is included in the "Extended Log" tracking option, but is not included in the "Log" tracking option?

- A. data type information
- B. application information
- C. file attributes
- D. destination port

69. How many layers make up the TCP/IP model?

- A. 6
- B. 4
- C. 7
- D. 2

70. Which two statements describe access attacks? (Choose two.)

A. Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.

B. Password attacks can be implemented using brute-force attack methods, Trojan Horses, or packet sniffers.

C. Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or exploit systems to execute malicious code. .

D. Port scanning attacks scan a range of TCP or UDP port numbers on a host to detect listening services.