KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **156-536**

Title : Check Point Certified Harmony Endpoint Specialist - R81.20

Version : DEMO

1.What communication protocol does Harmony Endpoint management use to communicate with the management server?
A. SIC
B. CPCOM
C. TCP
D. UDP
Answer: A
Explanation:
To determine the correct communication protocol used by Harmony Endpoint management to communicate with the management server, we need to clarify what "Harmony Endpoint management" refers to in the context of Check Point's Harmony Endpoint solution. The provided document, "CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf," offers detailed insights into the architecture and communication protocols used within this ecosystem. Let’s break this down step-by-step based on the official documentation.
Step 1: Understanding "Harmony Endpoint Management"
Harmony Endpoint is Check Point’s endpoint security solution, encompassing both client-side components (Endpoint Security Clients) and management-side components (SmartEndpoint console and Endpoint Security Management Server). The phrase "Harmony Endpoint management" in the question is ambiguous—it could refer to the management console (SmartEndpoint), the management server itself, or even the client-side management components communicating with the server. However, in security contexts, "management" typically implies the administrative or console component responsible for overseeing the system, which in this case aligns with the SmartEndpoint console.
The document outlines the architecture on page 23 under "Endpoint Security Architecture":
SmartEndpoint: "A Check Point SmartConsole application to deploy, monitor and configure Endpoint Security clients and policies."
Endpoint Security Management Server: "Includes the Endpoint Security policy management and databases. It communicates with endpoint clients to update their components, policies, and protection data."
Endpoint Security Clients: "Application installed on end-user computers to monitor security status and enforce security policies."
Given the question asks about communication "with the management server," it suggests that "Harmony Endpoint management" refers to the SmartEndpoint console communicating with the Endpoint Security Management Server, rather than the clients or the server communicating with itself.
Step 2: Identifying Communication Protocols
The document specifies communication protocols under "Endpoint Security Server and Client Communication" starting on page 26. It distinguishes between two key types of communication relevant to this query:
SmartEndpoint Console and Server to Server Communication (page 26):
"Communication between these elements uses the Check Point Secure Internal Communication (SIC) service."
"Service (Protocol/Port): SIC (TCP/18190 - 18193)"
This applies to communication between the SmartEndpoint console and the Endpoint Security Management Servers, as well as between Endpoint Policy Servers and Management Servers. Client to Server Communication (page 27):

"Most communication is over HTTPS TLSv1.2 encryption."
"Service (Protocol/Port): HTTPS (TCP/443)"
This covers communication from Endpoint Security Clients to the Management Server or Policy Servers.
The options provided are:
A . SIC: Secure Internal Communication, a Check Point proprietary protocol for secure inter-component communication.
B . CPCOM: Not explicitly mentioned in the document; likely a distractor or typo.
C . TCP: Transmission Control Protocol, a general transport protocol underlying many applications.
D . UDP: User Datagram Protocol, another transport protocol, less reliable than TCP.
Step 3: Analyzing the Options in Context
SIC: The document explicitly states on page 26 that SIC is used for "SmartEndpoint console to Endpoint Security Management Servers" communication, operating over TCP ports 18190–18193. SIC is a specific, secure protocol designed by Check Point for internal communications between management components, making it a strong candidate if "Harmony Endpoint management" refers to the SmartEndpoint console.
CPCOM: This term does not appear in the provided document. It may be a misnomer or confusion with another protocol, but without evidence, it’s not a valid option.
TCP: While TCP is the underlying transport protocol for both SIC (TCP/18190–18193) and HTTPS (TCP/443), it’s too generic. The question likely seeks a specific protocol, not the transport layer. UDP: The document does not mention UDP for management-to-server communication. It’s used in other contexts (e.g., RADIUS authentication on port 1812, page 431), but not here. Step 4: Interpreting "Harmony Endpoint Management"
If "Harmony Endpoint management" refers to the SmartEndpoint console, the protocol is SIC, as per page 26: "Communication between these elements uses the Check Point Secure Internal Communication (SIC) service." This aligns with the management console’s role in administering the Endpoint Security Management Server.
If it referred to the clients (less likely, as "management" typically denotes administrative components), the protocol would be HTTPS over TCP/443 (page 27). However, HTTPS is not an option, and TCP alone is too broad. The inclusion of SIC in the options strongly suggests the question targets management-side communication, not client-side.
The introduction on page 19 supports this: "The entire endpoint security suite can be managed centrally using a single management console," referring to SmartEndpoint. Thus, "Harmony Endpoint management" most logically means the SmartEndpoint console, which uses SIC to communicate with the management server.
Step 5: Conclusion
Based on the exact extract from page 26, "SmartEndpoint Console and Server to Server Communication" uses SIC (TCP/18190–18193). This matches option
A. SIC is a specific, Check Point-defined protocol, fitting the question’s intent over the generic TCP or irrelevant UDP and CPCOM options.
Final **Answer** A
Reference: "CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf," Page 19: Introduction to Endpoint Security
"CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf," Page 23: Endpoint Security Architecture
"CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf," Page 26: SmartEndpoint Console and

Server to Server Communication

2."Heartbeat" refers to what?
A. A periodic client connection to the server
B. A client connection that happens every 60 seconds
C. A server connection that happens every 5 minutes
D. A random server connection
Answer: A
Explanation:
In Check Point's Harmony Endpoint, the "heartbeat" refers to a periodic connection initiated by the endpoint client to the Endpoint Security Management Server. This mechanism ensures ongoing communication and allows the client to report its status and receive updates. The documentation states, "Endpoint clients send 'heartbeat' messages to the Endpoint Security Management Server to check the connectivity status and report updates" (page 28). The heartbeat is configurable, with a default interval of 60 seconds, but its defining characteristic is its periodic nature rather than a fixed timing, making option A the most accurate.
Option B is overly specific by locking the interval at 60 seconds, while option C incorrectly suggests a server-initiated connection every 5 minutes.
Option D is incorrect, as the heartbeat is not random but scheduled. This periodic connection is vital for maintaining compliance and monitoring endpoint security.
Reference: "CP_R81.20_Harmony_Endpoint_Server_AdminGuide.pdf," Page 28: The Heartbeat Interval

3.What are the benefits of the Check Point Consolidated Cyber Security Architecture?
A. Consolidated network functions
B. Single policy
C. Decentralized management
D. Consolidated security functions
Answer: D
Explanation:
The Check Point Consolidated Cyber Security Architecture is designed to integrate multiple security functions into a unified platform. This architecture provides "consolidated security functions," which is its primary benefit. This means it combines endpoint protection, data security, and threat prevention into a single, manageable system, improving efficiency and simplifying security administration for organizations. While "Consolidated network functions" (A) might sound similar, it’s too vague and not the focus of the architecture. "Single policy" (B) is not highlighted as a standalone benefit, and "Decentralized management" (C) contradicts the centralized approach of this architecture. Thus, "Consolidated security functions" (D) is the correct answer, as it aligns directly with the documented advantages.

4.What is the time interval of heartbeat messages between Harmony Endpoint Security clients and Harmony Endpoint Security Management?
A. 60 milli-seconds
B. 60 minutes
C. 60 seconds

D. 30 seconds
Answer: C
Explanation:
In Harmony Endpoint, heartbeat messages are periodic signals sent from endpoint clients to the Endpoint Security Management Server to report their status and check for updates. The default time interval for these messages is 60 seconds. This interval ensures timely communication between clients and the management server without overwhelming the network. While the interval can be adjusted, the question refers to the standard setting, making 60 seconds (C) the correct choice. 60 milliseconds (A) is far too short for practical use, 60 minutes (B) is excessively long and would delay updates, and 30 seconds (D) is not the default value specified in the documentation.

5.Which of the following is TRUE about the functions of Harmony Endpoint components?
A. SmartEndpoint connects to the Check Point Security Management Server (SMS)
B. SmartEndpoint Console connects to and manages the Endpoint Management Server (EMS)
C. SmartConsole connects to and manages the Endpoint Management Server (EMS)
D. Web Management Console for Endpoint connects to the Check Point Security Management Server (SMS)
Answer: B
Explanation:
The SmartEndpoint Console is a key component in the Harmony Endpoint architecture, specifically designed to connect to and manage the Endpoint Management Server (EMS). It is a Check Point SmartConsole application used to deploy, monitor, and configure endpoint security clients and policies, communicating directly with the EMS. In contrast, SmartEndpoint does not connect to the Security Management Server (SMS) as stated in option A. SmartConsole (C) is a broader management tool for Check Point gateways, not specifically for the EMS.
Option D, regarding the Web Management Console, is not supported by the documentation as connecting to the SMS. Therefore, "SmartEndpoint Console connects to and manages the Endpoint Management Server (EMS)" (B) is the true statement.