Check Point Certified Security Expert Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn’t just about memorization, it’s about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you’re preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You’ll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it’s correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It’s ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn’t about getting every question right the first time, it’s about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let’s begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Don't worry about getting everything right, your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations, and take breaks to retain information better.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning.

7. Use Other Tools

Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly — adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **During the Check Point Stateful Inspection Process, what happens to packets that do not pass Firewall Kernel Inspection?**

    A. Dropped without sending a negative acknowledgment

    B. Dropped without logs and without sending a negative acknowledgment

    C. Dropped with negative acknowledgment

    D. Dropped with logs and without sending a negative acknowledgment

2. **In the context of Check Point, what does the term “Rule Base” refer to?**

    A. A sequence of access rules for network traffic

    B. A database of all user accounts

    C. A backup mechanism for configurations

    D. A report generation feature

3. **In a Management HA setup, which Smartcenter should John connect to for making changes?**

    A. active Smartcenter

    B. secondary Smartcenter

    C. connect virtual IP of Smartcenter HA

    D. primary Smartcenter

4. **On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API), the default Log Server uses port:**

    A. 18210

    B. 18184

    C. 257

    D. 18191

5. **What does SandBlast Threat Emulation primarily focus on?**

    A. Delivering original files to the end user

    B. Monitoring user activity for potential threats

    C. Identifying zero-day vulnerabilities in files

    D. Ensuring safe downloads from external sources

6. **Which type of licenses are required for running a Check Point Security Gateway?**

    A. Basic licenses only

    B. Premium licenses only

    C. Standard licenses only

    D. All types of licenses can be applied

7. **What is the primary service of the INSPECT Engine in a firewall?**

    A. To provide authentication

    B. To perform packet inspection

    C. To manage licenses

    D. To configure NAT

8. **What is the primary purpose of anti-spoofing in a firewall architecture?**

    A. To prevent unauthorized access

    B. To control outgoing traffic

    C. To manage inbound traffic

    D. To prevent IP address spoofing

9. **Which command is used to show the installed licenses on a Check Point device?**

    A. cplic print

    B. print cplic

    C. fwlic print

    D. show licenses

10. **Which command is used to set the CCP protocol to Multicast?**

    A. cphaprob set_ccp multicast

    B. cphaconf set_ccp multicast

    C. cphaconf set_ccp no_broadcast

    D. cphaprob set_ccp no_broadcast

Answers

1. C
2. A
3. B
4. B
5. C
6. D
7. B
8. D
9. A
10. B

Explanations

1. During the Check Point Stateful Inspection Process, what happens to packets that do not pass Firewall Kernel Inspection?

A. Dropped without sending a negative acknowledgment

B. Dropped without logs and without sending a negative acknowledgment

C. Dropped with negative acknowledgment

D. Dropped with logs and without sending a negative acknowledgment

In the Check Point Stateful Inspection Process, when a packet does not pass the Firewall Kernel Inspection, it is classified as potentially harmful or non-compliant with the established security policies. Consequently, the packet is dropped, meaning it is not allowed to proceed further in the network. When a packet is dropped due to failing inspection, it generates a negative acknowledgment back to the sender. This serves as an indication that the packet was not accepted, allowing for protocol management and ensuring that the sender is aware that their packet did not make it to the intended destination. Negative acknowledgments are crucial for certain connection-oriented protocols, as they prompt the sender to take corrective actions, like retransmitting the packet. While logs may be kept for various events and actions within the firewall, in this specific scenario, the emphasis is on the fact that the packet is dropped with a negative acknowledgment. This provides feedback to the sender about the status of their transmission, enhancing overall network communication integrity and security.

2. In the context of Check Point, what does the term “Rule Base” refer to?

A. A sequence of access rules for network traffic

B. A database of all user accounts

C. A backup mechanism for configurations

D. A report generation feature

The term "Rule Base" in the context of Check Point refers to a sequence of access rules that govern the flow of network traffic through the security infrastructure. This foundational component of Check Point's security management system details how data packets are treated based on predefined conditions, ensuring that legitimate traffic is allowed while unauthorized access is blocked. The Rule Base determines the criteria for allowing or denying traffic based on various attributes such as source and destination IP addresses, ports, and protocols. This hierarchical set of rules is essential for maintaining network security, as it enables administrators to enforce policies that protect sensitive data and resources. Understanding the Rule Base is fundamental for effectively managing and troubleshooting network security policies, which in turn helps in securing the overall network architecture from threats.

3. In a Management HA setup, which Smartcenter should John connect to for making changes?

A. active Smartcenter

B. secondary Smartcenter

C. connect virtual IP of Smartcenter HA

D. primary Smartcenter

In a Management High Availability (HA) setup, the secondary SmartCenter is the appropriate choice for making changes, especially during maintenance or when the active SmartCenter is unavailable. When managing Security Management Servers in an HA configuration, the primary or active SmartCenter typically handles all management tasks and is responsible for the management of the firewalls and other gateways. However, connecting to the secondary SmartCenter allows administrators to perform necessary changes without disrupting the primary operations. This practice is critical for maintaining high availability and ensuring that management capabilities are not hampered during failover situations. The virtual IP of the SmartCenter HA can be used for connecting seamlessly to either SmartCenter without needing to specify which one is active. Therefore, while the virtual IP might provide convenience, connecting directly to the secondary SmartCenter ensures that tasks can be executed smoothly without dependence on the state of the primary SmartCenter.

4. On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API), the default Log Server uses port:

A. 18210

B. 18184

C. 257

D. 18191

In R80.10, when setting up third-party devices to read logs using the Log Export API (LEA), the default log server utilizes port 18184. This port is specifically designated for the LEA service within the Check Point architecture, allowing external systems to securely access logs generated by the Check Point security management and enforcement points. Understanding the importance of port 18184 in the context of LEA is crucial, as it facilitates communication between Check Point devices and third-party log analysis tools, ensuring that logs can be seamlessly exported and utilized for monitoring and compliance purposes. The selection of different ports in the remaining options does not align with the LEA configuration for log reading. Each of those ports is used for other services within the Check Point ecosystem or are not standard configurations for logging purposes. For example, 18210 is commonly associated with communication between the management server and gateways, while 257 is not a recognized port for Check Point logging services. Port 18191 may also serve a different function and is not utilized for LEA log exports. Understanding the specific roles of these ports emphasizes the importance of the default port utilized by the Log Export API for effective log management and analysis.

5. What does SandBlast Threat Emulation primarily focus on?

A. Delivering original files to the end user

B. Monitoring user activity for potential threats

C. Identifying zero-day vulnerabilities in files

D. Ensuring safe downloads from external sources

SandBlast Threat Emulation is primarily designed to identify zero-day vulnerabilities in files. This technology analyzes files in a secure environment to detect malicious content that traditional antivirus programs may miss, especially threats that exploit unknown vulnerabilities. By executing files in a virtual sandbox, SandBlast can observe their behavior without risking the endpoint or network, leading to the early detection of sophisticated attacks that utilize zero-day exploits. This proactive assessment helps organizations defend against files that appear benign but may contain harmful codes, such as malware or ransomware. The other options, while they address important aspects of cybersecurity, do not capture the primary focus of SandBlast Threat Emulation. Delivering original files to the end user does not align with the purpose of threat emulation, which is concerned with analyzing files rather than just passing them through. Monitoring user activity focuses more on behavior analytics than on file vulnerability detection, and ensuring safe downloads is more about filtering and validating files before they reach the user, rather than examining them for hidden threats.

6. Which type of licenses are required for running a Check Point Security Gateway?

A. Basic licenses only

B. Premium licenses only

C. Standard licenses only

D. All types of licenses can be applied

To run a Check Point Security Gateway, all types of licenses can be applied, making it possible to match the licensing to the specific needs of the organization. This flexibility allows organizations to choose the license that fits their requirements, whether they need basic features for a smaller environment or more advanced functionalities provided by premium or standard licenses. Basic licenses typically cover essential firewall and traffic control features, which may be sufficient for smaller setups or businesses with minimal security requirements. Standard licenses are designed for organizations that require additional capabilities such as intrusion prevention, application control, and more comprehensive reporting. Premium licenses offer the most extensive feature set, including advanced threat protection and advanced security management solutions. This variability ensures that businesses of different sizes and with different security needs can effectively implement Check Point Security Gateways without being locked into a single licensing model, thereby promoting scalability and customization. This approach to licensing supports a wide range of operational requirements and enhances the security posture based on specific organizational needs.

7. What is the primary service of the INSPECT Engine in a firewall?

A. To provide authentication

B. To perform packet inspection

C. To manage licenses

D. To configure NAT

The primary service of the INSPECT Engine in a firewall is to perform packet inspection. This engine is integral to the firewall's ability to analyze and filter traffic based on predefined security policies. It examines both the header and payload of packets, allowing the firewall to make informed decisions about whether to allow or block incoming and outgoing traffic. Packet inspection is crucial for identifying threats such as malware, unauthorized access attempts, and other malicious activities that might be concealed within legitimate traffic. By inspecting the data packets, the INSPECT Engine can enforce security measures effectively and maintain the integrity and confidentiality of the network. Understanding the role of the INSPECT Engine highlights its fundamental importance in network security, as it serves as the first line of defense against a variety of network threats. This capability distinguishes it from other functions such as user authentication, license management, and NAT configuration, which, while important, do not directly pertain to the core function of traffic inspection and filtering used to maintain network security.

8. What is the primary purpose of anti-spoofing in a firewall architecture?

A. To prevent unauthorized access

B. To control outgoing traffic

C. To manage inbound traffic

D. To prevent IP address spoofing

The primary purpose of anti-spoofing in a firewall architecture is to prevent IP address spoofing. Spoofing occurs when an attacker sends packets from a falsified source address, potentially allowing them to bypass security measures or gain unauthorized access to resources. Anti-spoofing techniques help to ensure that only legitimate source addresses are allowed, which enhances the overall security of the network. By implementing anti-spoofing measures, the firewall can verify that incoming packets originate from valid sources. This is critical in maintaining the integrity of network communications and protecting against various types of attacks that exploit packet manipulation. For instance, an anti-spoofing feature may block packets whose source IP addresses do not match any expected interfaces or internal network configurations. While the features to prevent unauthorized access, manage inbound traffic, and control outgoing traffic all contribute to the firewall's overall security posture, the specific role of anti-spoofing is focused on addressing the threats associated with creating deceptive packets that do not originate from legitimate sources.

9. Which command is used to show the installed licenses on a Check Point device?

A. cplic print

B. print cplic

C. fwlic print

D. show licenses

The command used to show the installed licenses on a Check Point device is "cplic print." This command retrieves and displays the current license information, including the types of licenses installed, their expiration dates, and the number of devices or users they cover. It is a crucial tool for administrators to ensure that their Check Point solutions are compliant and fully operational. Having detailed access to licensing information helps in proper management and maintaining the effectiveness of security protocols. The other alternatives do not represent valid commands for checking license information on Check Point devices. For instance, "print cplic" and "fwlic print" do not exist in the Check Point command lexicon or function as intended. "Show licenses" also does not correspond to a recognized command within the Check Point environment. Understanding the correct command is essential for effective system management and compliance with licensing agreements.

10. Which command is used to set the CCP protocol to Multicast?

A. cphaprob set_ccp multicast

B. cphaconf set_ccp multicast

C. cphaconf set_ccp no_broadcast

D. cphaprob set_ccp no_broadcast

The command to set the CCP (Cluster Control Protocol) to Multicast is indeed found in the context of managing cluster configurations. The correct choice emphasizes the appropriate utility for cluster management, which is `cphaconf`. Using `cphaconf set_ccp multicast` allows an administrator to configure the cluster to utilize Multicast for its CCP communications. This configuration is essential in environments where efficient data transfer and network resource optimization are priorities, as Multicast reduces the overhead on the network compared to other communication methods, such as Unicast. When configuring cluster settings, it's crucial to select the right command depending on the context. The `cphaprob` command is primarily used for checking cluster status and operational states rather than setting configurations. Therefore, while it's involved in cluster management, it does not serve the purpose of establishing the CCP protocol mode. The focus on the `cphaconf` command makes choice B the appropriate answer when aiming to set the CCP to Multicast.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we’d love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://checkpointsecurityexpert.examzify.com

We wish you the very best on your exam journey. You've got this!