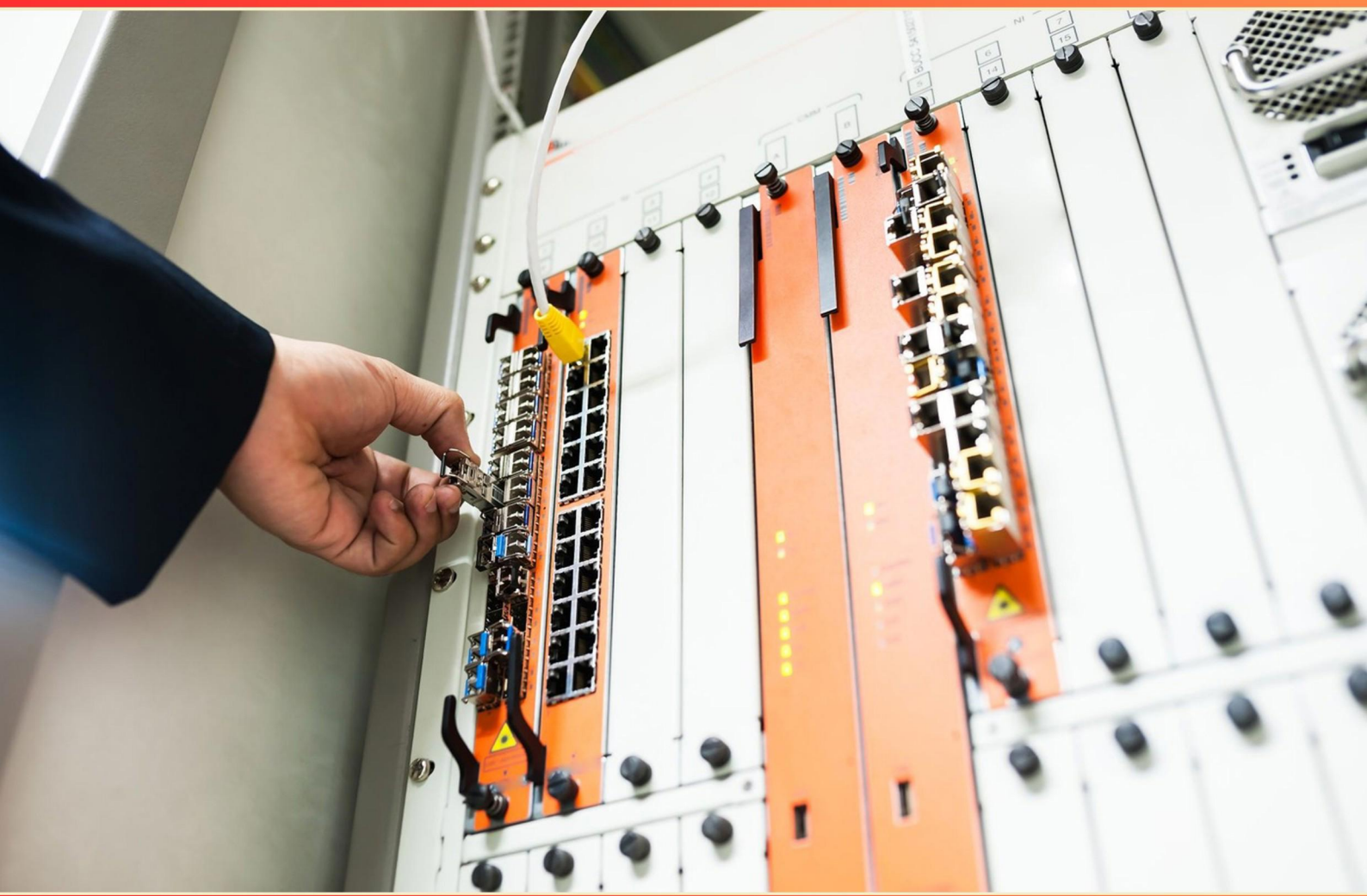
CHECK POINT CERTIFIED SECURITY EXPERT PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://checkpointsecurityexpert.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1
Table of Contents 2
Introduction 3
How to Use This Guide 4
Questions 5
Answers 8
Explanations 10
Next Steps 16

SAMPLE

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.

SAMPLE

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. 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.

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. 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!

SAMPLE

Questions

SAMPLE

1. **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

2. **Which Threat Prevention Profile is NOT included by default in R80 Management?**

   A. Basic - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

   B. Optimized - Provides excellent protection for common network products and protocols against recent or popular attacks

   C. Strict - Provides a wide coverage for all products and protocols, with impact on network performance

   D. Recommended - Provides all protection for all common network products and servers, with impact on network performance

3. **Which component of Check Point is tasked with correlating and consolidating events?**

   A. SmartEvent Policy

   B. Correlation Unit

   C. Consolidation Policy

   D. Log Server

4. **Which command is used to re-establish the Check Point configuration to a previous state?**

   A. config revert

   B. restore_config

   C. cp_merge

   D. backup_restore

5. **Which of the following is not a feature of the Check Point R80 architecture?**

   A. Single Point of Management

   B. Built-in compliance reporting

   C. Real-time threat intelligence

   D. Integrated VPN services

SAMPLE

6. What is the recommended sync method in a ClusterXL deployment?

A. Use 1 cluster + 1st sync

B. Use 1 dedicated sync interface

C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

D. Use multiple clusters with separate sync interfaces

7. What command do you use to enable Priorities Queues and Dynamic Dispatcher to optimize CPU core utilization?

A. fw ctl multik dynamic_dispatching on

B. fw ctl multik dynamic_dispatching set_mode 9

C. fw ctl multik set_mode 9

D. fw ctl multik pq enable

8. What protocol does the Check Point user authentication process primarily rely on?

A. HTTPS

B. RADIUS

C. LDAP

D. SSH

9. Can a Check Point gateway translate both source IP address and destination IP address in a packet?

A. Yes

B. No

C. Yes, but only when using Automatic NAT

D. Yes, but only when using Manual NAT

10. CoreXL is supported when which feature is enabled?

A. Route-based VPN

B. IPS

C. IPv6

D. Overlapping NAT

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. 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.

2. Which Threat Prevention Profile is NOT included by default in R80 Management?

A. Basic - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

B. Optimized - Provides excellent protection for common network products and protocols against recent or popular attacks

C. Strict - Provides a wide coverage for all products and protocols, with impact on network performance

D. Recommended - Provides all protection for all common network products and servers, with impact on network performance

The correct answer is the "Recommended" Threat Prevention Profile, which is not included by default in R80 Management. In R80, the default profiles available typically aim to balance security and performance, which is essential for most enterprise environments. The existing profiles, like Basic, Optimized, and Strict, cater to various needs based on performance impact and the extent of protection required. The Basic profile is designed specifically for environments where minimal performance impact is needed while still offering reliable protection for non-HTTP protocols. The Optimized profile strikes a balance, providing substantial protection against prevalent attacks while also maintaining desirable performance levels for common products and protocols. The Strict profile ensures extensive coverage across all products and protocols but does have a notable impact on network performance, making it suitable for situations where maximizing security is prioritized over performance. On the other hand, the Recommended profile is typically understood to be a preset that may include various levels of protection but isn't specifically set as a default option in R80. By not including it by default, R80 emphasizes the need for administrators to evaluate their specific security requirements and choose a profile that fits their operational characteristics and risk tolerance effectively. Having a wide array of specialized profiles allows for tailored security measures that align more closely with the specific needs of

SAMPLE

3. Which component of Check Point is tasked with correlating and consolidating events?

A. SmartEvent Policy

B. Correlation Unit

C. Consolidation Policy

D. Log Server

The component responsible for correlating and consolidating events within the Check Point ecosystem is the Correlation Unit. This unit plays a critical role in security event management by analyzing data collected from various sources, such as firewalls, intrusion prevention systems, and other security technologies. Its primary function is to identify patterns, anomalies, and relationships among the events that occur in the network. By performing this correlation, the Correlation Unit enables security teams to better understand and respond to potential threats more effectively. In addition to event correlation, the Correlation Unit can prioritize alerts based on risk levels, leading to more efficient management of security incidents. This enhances the overall visibility and control that security teams have over their environments, allowing them to make informed decisions when it comes to incident response and proactive threat detection. Other options, while related to event management and analysis, do not specifically focus on the task of correlating and consolidating events. For instance, SmartEvent Policy pertains to the configuration aspect of event management, focusing on defining what events to monitor and the actions to take, rather than performing the actual correlation. The Consolidation Policy, similarly, deals with how data is organized and displayed but does not engage in the analytical process itself. The Log Server is tasked

4. Which command is used to re-establish the Check Point configuration to a previous state?

A. config revert

B. restore_config

C. cp_merge

D. backup_restore

The command used to re-establish the Check Point configuration to a previous state is cp_merge. This command plays a crucial role in managing configurations, particularly when you want to revert to an earlier saved configuration after changes have been made. When you utilize cp_merge, it allows you to merge a previously saved configuration file into the current configuration, effectively restoring settings to that prior state. This is particularly useful when configurations have been altered and you need to backtrack to a time when the setup was optimal or functioning correctly. In the context of configuration management within Check Point systems, having the ability to revert to a specific state helps maintain network security and stability, especially when unexpected changes lead to issues. While there are other commands listed that might suggest similar functionalities, cp_merge is the accurate command for this particular action of restoring a previous state within the Check Point environment.

SAMPLE

5. Which of the following is not a feature of the Check Point R80 architecture?

A. Single Point of Management

B. Built-in compliance reporting

C. Real-time threat intelligence

D. Integrated VPN services

The Check Point R80 architecture is designed to streamline security management and improve operational efficiency through various integrated features. One of its key characteristics is the Single Point of Management, which allows administrators to manage multiple security gateways from a centralized console, thus simplifying policy management and enhancing visibility across the network. Built-in compliance reporting is another important feature, enabling organizations to generate reports that assist in meeting regulatory requirements, thereby ensuring compliance with various standards and frameworks relevant to cybersecurity. Real-time threat intelligence is also integrated within the R80 architecture. This feature allows organizations to benefit from automatically updated threat feeds that provide insights to quickly address emerging threats, improving the overall security posture. Integrated VPN services, while crucial in many security architectures, are not specifically highlighted as a feature of the Check Point R80 architecture. Instead, R80 focuses more on centralizing the management of security policies, visibility, and compliance rather than just VPN services. As such, it is the integrated VPN services that stand out as not being a defining feature of the R80 architecture specifically.

6. What is the recommended sync method in a ClusterXL deployment?

A. Use 1 cluster + 1st sync

B. Use 1 dedicated sync interface

C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

D. Use multiple clusters with separate sync interfaces

In a ClusterXL deployment, utilizing a dedicated sync interface is the recommended synchronization method. This approach enhances the reliability and efficiency of the synchronization process between cluster members. By isolating the sync traffic on a dedicated interface, the synchronization of essential data—such as security policies, connection states, and sessions—occurs without competing for bandwidth with other types of traffic. This ensures that the synchronization process remains unaffected by other network activities, leading to reduced latency and higher reliability in maintaining consistent configurations and state information across all cluster members. Hence, using a dedicated sync interface contributes to improved overall performance and stability of the ClusterXL setup. Other options, while they might involve synchronization, do not provide the same level of dedicated resource allocation and operational efficiency that a single dedicated sync interface guarantees.

SAMPLE

7. What command do you use to enable Priorities Queues and Dynamic Dispatcher to optimize CPU core utilization?

A. fw ctl multik dynamic_dispatching on

B. fw ctl multik dynamic_dispatching set_mode 9

C. fw ctl multik set_mode 9

D. fw ctl multik pq enable

To optimize CPU core utilization by enabling Priority Queues and the Dynamic Dispatcher, the command utilized is specifically designed to activate the Dynamic Dispatcher feature. The command "fw ctl multik dynamic_dispatching on" directly enables this feature, which allows for dynamic load balancing across CPU cores. When Dynamic Dispatcher is enabled, it actively manages packet processing distribution based on the current load, thus helping to optimize performance by efficiently utilizing all available CPU cores. This is crucial in high-throughput environments where traffic levels can vary substantially, and balancing the load can significantly impact overall system efficiency. Other commands may modify modes or specific configurations, but they do not enable the Dynamic Dispatcher functionality itself. The detailed and specific nature of the correct command focuses on essentially switching the feature to an active state, which is key for optimizing core utilization within the system. This understanding is vital for effectively configuring Check Point security solutions to handle varying network loads efficiently.

8. What protocol does the Check Point user authentication process primarily rely on?

A. HTTPS

B. RADIUS

C. LDAP

D. SSH

The Check Point user authentication process primarily relies on the RADIUS protocol due to its widespread use for network access control and its ability to provide centralized authentication, authorization, and accounting (AAA) services. RADIUS operates as a client-server protocol where the Check Point security gateway acts as a client and communicates with a RADIUS server to authenticate users attempting to access the network. This ensures that user credentials are handled securely and efficiently. While other protocols like LDAP and SSH are often used in various contexts, such as directory services and secure access, respectively, they are not the primary means of user authentication in Check Point environments. LDAP may be used for retrieving user information or for integrating with directory services, but it does not provide the complete AAA framework that RADIUS does. Similarly, SSH is designed for secure shell access to devices rather than user authentication in a network access context. HTTPS is mainly used for securing web traffic and is not related to user authentication processes directly. Thus, RADIUS stands out as the key protocol in facilitating secure and effective user authentication in Check Point systems.

SAMPLE

9. Can a Check Point gateway translate both source IP address and destination IP address in a packet?

A. Yes

B. No

C. Yes, but only when using Automatic NAT

D. Yes, but only when using Manual NAT

The capability of a Check Point gateway to translate both the source IP address and the destination IP address in a packet falls under the functionality of Manual NAT (Network Address Translation). In Manual NAT, the administrator has full control over the mappings, allowing the configuration of both source and destination addresses explicitly. This is particularly useful in scenarios where specific IP addresses need to be translated in a custom way that aligns with network requirements or policies. On the other hand, Automatic NAT is primarily designed for easier management, automatically assigning translations without detailed configuration for each specific case. While Automatic NAT provides flexibility, it does not support translating both source and destination addresses in the same context as Manual NAT; it is typically aimed at translating just source addresses or simplifying outbound NAT for internal IPs. Thus, the correct answer reflects the functionality provided by Manual NAT, which allows for the simultaneous translation of both source and destination IPs, enabling more precise control over traffic management and security policies.

10. CoreXL is supported when which feature is enabled?

A. Route-based VPN

B. IPS

C. IPv6

D. Overlapping NAT

CoreXL is a technology designed to enhance the performance of Check Point firewalls by leveraging the capabilities of multiple CPU cores to process network traffic more efficiently. This technology allows for increased throughput and improved scalability. When it comes to the context of the question, CoreXL is specifically supported when the Intrusion Prevention System (IPS) feature is enabled. The integration of CoreXL with IPS provides significant performance benefits, allowing the system to process IPS traffic across multiple cores, thus facilitating higher traffic loads while maintaining security measures. In scenarios where IPS is enabled, CoreXL can distribute the processing of traffic to multiple cores, which is crucial for high-throughput environments. This setup not only enhances performance but also ensures that security functions can keep pace with network traffic demands. Other features such as Route-based VPN, IPv6, and Overlapping NAT do not specifically trigger the support for CoreXL in the same way that enabling IPS does, as they operate independently of the core processing architecture designed to optimize traffic flow for security functions like IPS.

SAMPLE

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!

SAMPLE