FCSS FORTISASE 24 ADMINISTRATOR (FCSS_SASE_AD-24) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fcssfortisase24admin.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. How does FortiSASE ensure that only compliant devices access the network?

A. By allowing all devices access regardless of compliance

B. By evaluating the security posture of endpoints against established security policies

C. By limiting access to only mobile devices

D. By requiring physical inspections of devices

2. What endpoint functionality can be configured using FortiSASE?

A. Enable and push web filter to FortiClient endpoints

B. Automatically patch operating systems on endpoints

C. Provide remote desktop access to endpoints

D. Deploy antivirus software across all endpoints

3. What does BGP enable between FortiSASE and the FortiGate SD-WAN hub?

A. Encryption of all data packets

B. The exchange of routing information to ensure optimal routing paths and efficient traffic management

C. The monitoring of network performance

D. The establishment of a VPN connection

4. What action is necessary to ensure proper functioning of the antivirus profile?

A. Regularly revise the allowed application list

B. Ensure continuous updates and correct configuration

C. Limit access to necessary user groups only

D. Implement additional firewalls for protection

5. Why is it important for FortiGate to inspect all TCP traffic?

A. To reduce network latency

B. To ensure security and compliance

C. To prioritize traffic for faster connections

D. To ensure user privacy is maintained

SAMPLE

6. How does hashing with salt contribute to data security?

A. It prevents the data from being accessed

B. It makes the data unidentifiable after storage

C. It protects against dictionary and rainbow table attacks

D. It speeds up the data retrieval process

7. What advantage does multi-tenancy provide in FortiSASE for MSSPs?

A. It allows multiple service providers to operate from a single account

B. It allows MSSPs to manage multiple customer environments from a single FortiSASE instance

C. It mandates the use of identical security protocols for all tenants

D. It prevents any client access if one user is compromised

8. What functionality does a next-generation firewall provide in relation to IPSec VPN hubs?

A. It optimizes web traffic

B. It establishes and manages VPN connections

C. It caches frequently accessed data

D. It enforces compliance policies

9. What is the primary function of a secure web gateway (SWG)?

A. To enhance internet speed and connectivity

B. To protect users from web-based threats and enforce security policies

C. To provide unrestricted access to any website

D. To serve as a backup for all web traffic

10. What is a key benefit of ZTNA in terms of access control?

A. It allows unlimited access to all applications

B. It enforces granular access control policies

C. It eliminates the need for user credentials

D. It simplifies the authentication process

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How does FortiSASE ensure that only compliant devices access the network?

A. By allowing all devices access regardless of compliance

B. By evaluating the security posture of endpoints against established security policies

C. By limiting access to only mobile devices

D. By requiring physical inspections of devices

FortiSASE employs a method of evaluating the security posture of endpoints against established security policies to ensure that only compliant devices can access the network. This process typically involves assessing various security attributes of devices, such as operating system updates, antivirus software presence, and adherence to configuration guidelines. By performing this evaluation, FortiSASE can determine whether a device meets the required compliance standards before granting access to the network. This approach is important because it helps protect the network from threats posed by non-compliant or vulnerable devices that could potentially introduce security risks. By ensuring that only devices that satisfy specific security requirements can connect, FortiSASE enhances the overall security posture of the organization. The other responses present methods that would not effectively manage network access based on compliance. For example, allowing all devices access regardless of compliance ignores potential security threats. Limiting access to only mobile devices does not accommodate the diverse range of endpoints that may be necessary for an organization. Requiring physical inspections of devices is impractical for large-scale or remote environments and would not scale well to modern network demands.

2. What endpoint functionality can be configured using FortiSASE?

A. Enable and push web filter to FortiClient endpoints

B. Automatically patch operating systems on endpoints

C. Provide remote desktop access to endpoints

D. Deploy antivirus software across all endpoints

The functionality of enabling and pushing a web filter to FortiClient endpoints through FortiSASE is significant for organizations looking to enhance their security posture. This capability allows network administrators to implement web filtering policies that help protect endpoints from malicious websites and content. By controlling which websites users can access based on predefined rules, organizations can mitigate risks associated with web-based threats, ensuring that users only interact with safe and approved sites. Moreover, web filtering can help enhance productivity by restricting access to non-work-related or harmful content, thereby allowing organizations to manage bandwidth effectively and reduce the likelihood of endpoints being infected by malware via harmful sites. This aspect of endpoint management is particularly crucial in today's environment, where remote work and endpoint diversity demand robust security measures. The other functionalities presented are important but do not fall under the specific capabilities provided by FortiSASE. For instance, automatic operating system patching, remote desktop access provision, and antivirus software deployment generally fall under different management or security solutions rather than the specific endpoint functionality offered by FortiSASE.

SAMPLE

3. What does BGP enable between FortiSASE and the FortiGate SD-WAN hub?

A. Encryption of all data packets

B. The exchange of routing information to ensure optimal routing paths and efficient traffic management

C. The monitoring of network performance

D. The establishment of a VPN connection

BGP, or Border Gateway Protocol, is instrumental in facilitating the exchange of routing information between networks. In the context of FortiSASE and the FortiGate SD-WAN hub, BGP plays a crucial role in ensuring that routing paths remain optimal and traffic is managed efficiently across the network. By leveraging BGP, these systems can dynamically communicate about network changes and the availability of different paths, allowing for adaptive routing that can respond to network fluctuations. This capability supports load balancing, failover solutions, and overall enhanced performance for the SD-WAN infrastructure. The primary purpose of BGP in this scenario is not focused on encrypting data packets, monitoring network performance, or establishing VPN connections—areas that are covered by other protocols and technologies. While encryption is vital for data security, it is not a function of BGP itself; instead, this is typically managed by protocols designed specifically for secure communication. Similarly, monitoring tools or solutions separately manage performance analytics, and VPNs use other tunneling protocols to establish secure connections. Thus, the focus of BGP's functionality is very much aligned with routing and traffic management, making it the best answer in this context.

4. What action is necessary to ensure proper functioning of the antivirus profile?

A. Regularly revise the allowed application list

B. Ensure continuous updates and correct configuration

C. Limit access to necessary user groups only

D. Implement additional firewalls for protection

Ensuring continuous updates and correct configuration of the antivirus profile is crucial for its effective functioning. Antivirus software relies on regular updates to its virus definitions and threat intelligence to protect against the latest malware and vulnerabilities. These updates help to identify and mitigate new threats as they emerge, which is essential for maintaining security in an ever-evolving threat landscape. Correctly configuring the antivirus settings optimizes its performance and effectiveness, tailoring its operation to the specific environment and needs of the organization. This includes setting up scan schedules, defining objects for monitoring, adjusting sensitivity levels, and integrating it with other security measures in place. Without timely updates and proper configuration, the antivirus profile may fail to detect threats, leading to potential security breaches. In contrast, revising the allowed application list, while important for application control strategies, does not directly address the functionality of the antivirus profile itself. Limiting access to specific user groups contributes to securing the environment, but it does not influence how the antivirus functions. Similarly, adding additional firewalls may enhance overall network security but does not directly affect the operation of the antivirus profile. Focusing on updates and configuration is the foundational aspect necessary for the antivirus to function properly.

SAMPLE

5. Why is it important for FortiGate to inspect all TCP traffic?

A. To reduce network latency

B. To ensure security and compliance

C. To prioritize traffic for faster connections

D. To ensure user privacy is maintained

Inspecting all TCP traffic is vital for ensuring security and compliance. By thoroughly analyzing this traffic, FortiGate can identify and mitigate potential threats such as malware, data breaches, and unauthorized access attempts. This proactive stance helps organizations enforce security policies and regulatory requirements, which are increasingly critical in today's digital landscape where cyber threats are ubiquitous. Additionally, comprehensive traffic inspection assists in ensuring that sensitive data is not being transmitted insecurely or in violation of compliance regulations. By not inspecting all TCP traffic, there remains a risk that harmful traffic could pass through undetected, leading to security incidents that might compromise sensitive information or the organization's overall security posture. While reducing network latency, prioritizing traffic, and maintaining user privacy are important aspects of network management and security, they are secondary to the core need for thorough inspection of traffic to uphold security and compliance standards.

6. How does hashing with salt contribute to data security?

A. It prevents the data from being accessed

B. It makes the data unidentifiable after storage

C. It protects against dictionary and rainbow table attacks

D. It speeds up the data retrieval process

Hashing with salt is a crucial practice in securing sensitive data, especially passwords, by adding a unique value (the salt) to the input data before it is hashed. This process significantly enhances security by providing multiple layers of protection against specific attack methods. The primary benefit of incorporating salt into hashing is its effectiveness against dictionary and rainbow table attacks. In these types of attacks, hackers utilize precomputed tables containing hashes of common passwords to quickly determine the original input. By adding a unique salt for each password before hashing, even if two users have the same password, the resulting hashes will be different. This randomness disrupts the usefulness of precomputed tables, requiring attackers to generate new hash tables for each unique salt, making it computationally intensive and time-consuming. Other choices like preventing access to data or making data unidentifiable do not accurately describe the function of hashing with salt. While salting adds complexity to the process, it does not inherently speed up data retrieval, as the focus is on security instead of performance. Thus, the correct answer focuses on the enhanced protection against specific types of threats that salted hashes effectively mitigate.

SAMPLE

7. What advantage does multi-tenancy provide in FortiSASE for MSSPs?

A. It allows multiple service providers to operate from a single account

B. It allows MSSPs to manage multiple customer environments from a single FortiSASE instance

C. It mandates the use of identical security protocols for all tenants

D. It prevents any client access if one user is compromised

The advantage of multi-tenancy in FortiSASE for Managed Security Service Providers (MSSPs) primarily lies in its ability to enable the management of multiple customer environments from a single FortiSASE instance. This architecture allows MSSPs to efficiently allocate resources, streamline management tasks, and provide tailored security services to different clients without the need for separate instances for each customer. By using a single platform to oversee various customer environments, MSSPs can enhance operational efficiency, reduce costs, and improve their ability to respond to security incidents or changes in customer needs. Multi-tenancy facilitates a shared infrastructure while maintaining data isolation and security for each tenant, ensuring that customers' data remains confidential and protected from one another. This is crucial for MSSPs that serve multiple clients, as it allows them to efficiently scale their operations while still providing robust security measures specific to each client's requirements.

8. What functionality does a next-generation firewall provide in relation to IPSec VPN hubs?

A. It optimizes web traffic

B. It establishes and manages VPN connections

C. It caches frequently accessed data

D. It enforces compliance policies

A next-generation firewall is designed to enhance security at various levels, including network, application, and content levels. In the context of IPSec VPN hubs, its primary functionality revolves around establishing and managing VPN connections. This includes the capability to create secure tunnels between sites or remote users and the central hub, ensuring that data transmitted over these connections remains confidential and secure. By managing the IPSec VPN connections, the next-generation firewall can also provide additional security features such as traffic inspection, intrusion prevention, and even application control. This means that not only can it facilitate the creation of secure connections, but it can also monitor and enforce security policies on the traffic flowing through those connections. In contrast, other functionalities mentioned do not directly relate to the specific role of managing IPSec VPN hubs: - Optimizing web traffic typically involves performance enhancements and caching mechanisms rather than direct VPN management. - Caching frequently accessed data is more aligned with content delivery networks or proxy servers, aimed at improving access speed rather than VPN connection security. - Enforcing compliance policies generally pertains to overall network security strategies and regulatory requirements that can run parallel to VPN usage but are not a core function of managing those connections specifically. Thus, establishing and managing VPN connections is the definitive role of a next

SAMPLE

9. What is the primary function of a secure web gateway (SWG)?

A. To enhance internet speed and connectivity

B. To protect users from web-based threats and enforce security policies

C. To provide unrestricted access to any website

D. To serve as a backup for all web traffic

The primary function of a secure web gateway (SWG) is to protect users from web-based threats and enforce security policies. This security device acts as a filter between users and the internet, ensuring that malicious content, such as malware or phishing attempts, is blocked before it can reach users. By analyzing web traffic in real-time, a SWG can enforce organizational policies regarding acceptable internet usage and provide comprehensive protection against various threats. The implementation of security features within a SWG includes URL filtering, malware scanning, and data loss prevention, which collectively enhance the overall safety of web interactions for users. By focusing on both threat mitigation and policy enforcement, a SWG plays a crucial role in maintaining a secure network environment for both remote and on-premises users. Other options misrepresent the primary role of an SWG. While enhancing internet speed could be a secondary benefit due to optimizations, it is not the main purpose. Providing unrestricted access contradicts the very reason SWGs exist, as they are designed to impose controls and maintain secure browsing. Lastly, serving as a backup for all web traffic does not capture the essential function of a secure web gateway, which focuses instead on inspection and protection rather than data redundancy.

10. What is a key benefit of ZTNA in terms of access control?

A. It allows unlimited access to all applications

B. It enforces granular access control policies

C. It eliminates the need for user credentials

D. It simplifies the authentication process

The benefit of ZTNA (Zero Trust Network Access) that stands out is its ability to enforce granular access control policies. This approach is fundamental to the zero-trust security model, which assumes that no user or device should be trusted by default, regardless of whether they are inside or outside the network perimeter. With granular access control, ZTNA allows organizations to define specific access policies based on various factors such as user role, device health, location, and application sensitivity. This level of specificity ensures that users are granted access only to the resources they need to perform their job functions, significantly reducing the risk of unauthorized access and data breaches. By implementing such precise controls, organizations can also respond more effectively to security incidents by quickly adjusting access permissions as needed. In comparison, options suggesting unlimited access, the elimination of user credentials, or simplification of the authentication process do not reflect the core principles of ZTNA. Unlimited access contradicts the zero-trust model by undermining its primary objective of limiting access. Eliminating credentials would pose significant security risks, as verification of identity is crucial in any access control framework. Simplifying authentication might improve user experience but does not inherently address the fundamental purpose of ZTNA—enhancing security through controlled access.

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://fcssfortisase24admin.examzify.com

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

SAMPLE