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

STUDY GUIDE

Prepare with structure. Pass with confidence

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

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. 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!

Questions

1. Which feature is common in both ZTNA and traditional VPN?

A. Access control based on user roles

B. Use of encryption for data transmission

C. User-friendly access interfaces

D. Limiting access to company personnel only

2. How does FortiSASE improve administration for multiple branch offices?

A. By providing decentralized management systems

B. By offering onsite technical support

C. By providing a centralized management platform for security policies

D. By eliminating the need for internet access

3. What does the term 'routing adjacency' refer to in the context of FortiSASE and FortiGate?

A. The established connection for exchanging routing information between the two systems

B. A method to store routing information locally

C. A type of network redundancy feature

D. The protocol used for classifying data packets

4. What does the FortiSASE secure web gateway (SWG) do?

A. It accelerates web browsing speed

B. It provides secure access to the web and protects users from web-based threats

C. It filters advertisements from websites

D. It manages user identities for web applications

5. What FortiSASE feature allows monitoring of SaaS applications and health-check metrics?

A. Vulnerability Management

B. Endpoint Detection and Response (EDR)

C. Digital Experience Monitoring (DEM)

D. Data Loss Prevention (DLP)

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 are the required setups for implementing device posture checks for remote endpoints through FortiGate?

A. Define user roles and access rights

B. Configure ZTNA tags, as a ZTNA access proxy, and ZTNA policies

C. Set firewall rules and VPN connections

D. Create user accounts and passwords

8. What are the three setups required for implementing device posture checks for remote endpoints accessing a protected server?

A. Set up access control, configure user authentication, and enable logging

B. Configure ZTNA tags, set up FortiGate as a ZTNA access proxy, and implement ZTNA policies

C. Design network architecture, optimize bandwidth, and set firewall rules

D. Establish user roles, configure device settings, and enable alerting

9. What is a significant advantage of using FortiSASE for network security?

A. It relies solely on traditional VPNs

B. It offers on-premises only deployment options

C. It integrates cloud capabilities with local security measures

D. It requires no user authentication

10. What does SD-WAN stand for and how is it related to FortiSASE?

A. Secure Digital Wide Area Network; enhancing data protection

B. Software-Defined Wide Area Network; for enhanced network management

C. Single Device Wide Area Network; simplifying local connections

D. Standard Data Wide Area Network; optimizing internet speeds

Answers

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

Explanations

1. Which feature is common in both ZTNA and traditional VPN?

A. Access control based on user roles

B. Use of encryption for data transmission

C. User-friendly access interfaces

D. Limiting access to company personnel only

The feature shared by both Zero Trust Network Access (ZTNA) and traditional VPN is the use of encryption for data transmission. Encryption is essential in both frameworks as it secures data being transmitted over the internet, ensuring that unauthorized users cannot easily intercept or read sensitive information. Both ZTNA and traditional VPNs recognize the importance of maintaining data confidentiality and integrity during communication, making encryption a fundamental aspect of their design. In ZTNA, encryption helps to protect data by establishing secure connections between users and applications, ensuring that only those with appropriate access can view the data. Similarly, traditional VPNs create encrypted tunnels that safeguard the data as it travels between a remote user and the corporate network. This commonality highlights how both approaches prioritize secure data transmission as a critical element of their functionality.

2. How does FortiSASE improve administration for multiple branch offices?

A. By providing decentralized management systems

B. By offering onsite technical support

C. By providing a centralized management platform for security policies

D. By eliminating the need for internet access

FortiSASE enhances administration for multiple branch offices primarily through the provision of a centralized management platform for security policies. This centralized approach allows administrators to manage and enforce security protocols uniformly across all locations, which simplifies oversight and ensures consistency in security measures. Centralized management enables IT teams to quickly deploy policies, monitor security events, and respond to incidents from a single interface. This is especially vital for organizations with multiple branch offices, as it streamlines operations, reduces the likelihood of configuration errors that can arise from decentralized systems, and allows for better visibility into the security posture across the enterprise. In contrast, decentralization, which could involve having separate management systems for each branch, could lead to inconsistencies and challenges in enforcing a cohesive security strategy. Onsite technical support is beneficial but does not address the overarching challenge of coordinating security measures across multiple locations. Lastly, eliminating the need for internet access is not a viable management strategy for modern organizations, as connectivity is essential for remote offices to operate and communicate effectively.

3. What does the term 'routing adjacency' refer to in the context of FortiSASE and FortiGate?

A. The established connection for exchanging routing information between the two systems

B. A method to store routing information locally

C. A type of network redundancy feature

D. The protocol used for classifying data packets

'Routing adjacency' in the context of FortiSASE and FortiGate specifically refers to the established connection for exchanging routing information between the two systems. This concept is crucial for enabling communication and the efficient forwarding of data packets across a network. Establishing routing adjacency allows the systems to share updates about network topology and routing paths. This is fundamental in a dynamic environment where network changes occur frequently, as it ensures that both FortiSASE and FortiGate are aware of the best routes to take for data transmission. The successful exchange of this routing information helps maintain network performance and resilience. The other options do not encapsulate the definition of routing adjacency. For example, storing routing information locally pertains more to static routing tables rather than the dynamic exchange facilitated through adjacency. Network redundancy features typically deal with pathways or failover mechanisms rather than the exchange of routing data. Lastly, data packet classification is more related to how packets are prioritized or treated within the network rather than the connection for sharing routing information.

4. What does the FortiSASE secure web gateway (SWG) do?

A. It accelerates web browsing speed

B. It provides secure access to the web and protects users from web-based threats

C. It filters advertisements from websites

D. It manages user identities for web applications

The FortiSASE secure web gateway (SWG) primarily functions to provide secure access to the web and protect users from web-based threats. This is achieved through several layers of security protocols that monitor and filter internet traffic, thereby blocking malicious content such as malware, phishing attempts, and other cyber threats. The SWG ensures that data transmitted over the internet is secure by inspecting it for potential risks before allowing users to access websites or applications. The primary role of an SWG is not just about enabling safe browsing but also enhancing security postures by enforcing policies that manage what content is accessible to users based on predefined parameters. This means that security measures are integrated into the user experience, which is essential in today's digital landscape where threats are becoming increasingly sophisticated. While accelerating web browsing speed or managing identities for web applications might be beneficial features, they do not align with the core purpose of a secure web gateway. Similarly, filtering advertisements, while a common feature in some web privacy tools, is not the main function of an SWG. Thus, option B accurately captures the critical function of a FortiSASE secure web gateway by highlighting its dual role of secure access and protection against web-based threats.

5. What FortiSASE feature allows monitoring of SaaS applications and health-check metrics?

A. Vulnerability Management

B. Endpoint Detection and Response (EDR)

C. Digital Experience Monitoring (DEM)

D. Data Loss Prevention (DLP)

The feature that enables the monitoring of SaaS applications and health-check metrics is Digital Experience Monitoring (DEM). This functionality is designed to provide insights into the performance and reliability of cloud services and applications. DEM allows organizations to track user experiences and performance metrics, which can help identify issues affecting the accessibility or functionality of SaaS applications. By utilizing DEM, administrators can gain visibility into how applications perform from various locations, analyze response times, and assess overall user experience. This information is crucial for optimizing cloud application use and ensuring that users are not facing disruptions, which can impact productivity. In contrast, Vulnerability Management focuses on identifying and addressing security vulnerabilities within an organization's systems and applications but does not include monitoring of application performance. Endpoint Detection and Response (EDR) is concerned with detecting and responding to threats on endpoint devices rather than application-level performance. Data Loss Prevention (DLP) is primarily aimed at protecting sensitive information from unintended exposure or exfiltration and does not encompass performance tracking. Therefore, Digital Experience Monitoring is the correct feature that ties directly to the monitoring of SaaS applications and their health-check metrics.

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.

7. What are the required setups for implementing device posture checks for remote endpoints through FortiGate?

A. Define user roles and access rights

B. Configure ZTNA tags, as a ZTNA access proxy, and ZTNA policies

C. Set firewall rules and VPN connections

D. Create user accounts and passwords

The implementation of device posture checks for remote endpoints through FortiGate heavily relies on the configuration of Zero Trust Network Access (ZTNA) elements. The correct approach is to configure ZTNA tags, set up a ZTNA access proxy, and establish ZTNA policies. ZTNA tags help in classifying devices based on their security posture and compliance status. By applying these tags, FortiGate can make informed decisions on whether to grant access to specific resources based on the security posture of the remote endpoints. The ZTNA access proxy facilitates the secure connection and authentication of these devices, ensuring that only compliant and trusted devices are allowed access. Finally, ZTNA policies are crucial as they dictate the rules and conditions under which devices can access network resources, effectively implementing the principle of least privilege. By combining these elements, an organization can maintain a strong security posture while granting remote access, ensuring that only devices meeting the defined security criteria can connect to the network. In contrast, defining user roles and access rights, setting firewall rules and VPN connections, or creating user accounts and passwords do not directly address device posture checks. While these configurations are important for overall network security and user management, they do not fulfill the specific requirements for implementing device posture checks

8. What are the three setups required for implementing device posture checks for remote endpoints accessing a protected server?

A. Set up access control, configure user authentication, and enable logging

B. Configure ZTNA tags, set up FortiGate as a ZTNA access proxy, and implement ZTNA policies

C. Design network architecture, optimize bandwidth, and set firewall rules

D. Establish user roles, configure device settings, and enable alerting

Implementing device posture checks for remote endpoints accessing a protected server is essential for ensuring that only compliant devices are allowed access. The correct answer focuses specifically on the necessary setups related to Zero Trust Network Access (ZTNA), which enhances security by verifying user and device identity before granting access. Configuring ZTNA tags allows the organization to categorize devices based on their compliance status and other criteria. These tags play a crucial role in ensuring that only devices meeting specific security requirements are allowed to access sensitive resources. Setting up FortiGate as a ZTNA access proxy involves routing the traffic from remote endpoints through the FortiGate firewall. This configuration helps enforce security policies and conduct the necessary posture checks on devices before granting them access to the protected server. Implementing ZTNA policies is vital for defining how access is controlled based on the device's posture. These policies determine what type of access a device receives, depending on its compliance state, and can restrict access to certain applications or data if a device does not meet the necessary security posture. Other choices do not encompass all three critical elements specifically related to ZTNA and device posture checks. While access control, user authentication, and logging are important for overall security, they do not directly implement posture checks in the

9. What is a significant advantage of using FortiSASE for network security?

A. It relies solely on traditional VPNs

B. It offers on-premises only deployment options

C. It integrates cloud capabilities with local security measures

D. It requires no user authentication

Utilizing FortiSASE for network security significantly enhances an organization's capabilities by integrating cloud capabilities with local security measures. This hybrid approach allows for flexible security solutions that can adapt to various environments, whether users are accessing resources from the office or remotely. By leveraging the cloud, FortiSASE ensures that security policies are consistently applied regardless of the user's location, enabling real-time threat detection and response. This integration also allows organizations to benefit from advanced security features that may not be possible with traditional on-premises systems alone. The cloud capabilities enable scalability and ease of management, as updates and new threats can be promptly addressed without the extensive overhead associated with maintaining solely on-premises systems. Moreover, this model supports the ongoing trend towards more decentralized work environments, where employees may work from home, public spaces, or branches across different locations. By combining local security measures with cloud capabilities, organizations can better secure their network and data, adapting swiftly to changing security needs.

10. What does SD-WAN stand for and how is it related to FortiSASE?

A. Secure Digital Wide Area Network; enhancing data protection

B. Software-Defined Wide Area Network; for enhanced network management

C. Single Device Wide Area Network; simplifying local connections

D. Standard Data Wide Area Network; optimizing internet speeds

The term SD-WAN stands for Software-Defined Wide Area Network. This technology represents a significant evolution in wide area networking, focusing on the ability to manage and optimize network connections over various types of transport, such as MPLS, LTE, or broadband internet. In the context of FortiSASE (Secure Access Service Edge), SD-WAN plays a crucial role as it enhances network management by intelligently directing traffic based on real-time conditions and policies that improve performance, reduce costs, and increase agility. FortiSASE integrates SD-WAN capabilities to provide secure and reliable connectivity across the WAN while effectively supporting cloud applications and services. Through SD-WAN, FortiSASE facilitates efficient routing, bandwidth management, and ensures Quality of Service (QoS) for critical applications. This technology allows organizations to leverage cloud resources without compromising on security or performance, thus aligning with the overarching goals of FortiSASE in delivering a secure, scalable, and responsive networking solution. This emphasis on software-defined management and the ability to dynamically steer network traffic based on various conditions is what makes the second choice particularly relevant and applicable. Other definitions presented do not accurately capture the primary functions or implications of SD-WAN technology, such as data protection, simplifying local connections, or

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!