FORTINET NETWORK SECURITY EXPERT (NSE) 4 CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fortinetnetsecurityexpert4.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. What is the default administrative login for a new FortiGate unit?

A. Username "admin" with no password

B. Username "root" with password "fortinet"

C. Username "admin" with password "admin"

D. Username "administrator" with no password

2. How does FortiGate's application control feature function?

A. It identifies applications based on their IP addresses

B. It controls applications based on ports and protocols exclusively

C. It identifies and controls applications regardless of the ports and protocols used

D. It restricts all applications by default

3. What occurs when configuring multiple static routes with identical metrics?

A. FortiGate will randomly select one of the routes.

B. Both routes will be utilized, allowing for load balancing.

C. Conflicts will prevent any of the routes from functioning.

D. Static routes must be manually configured to avoid conflicting metrics.

4. Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used with user authentication

B. They can only be applied to wireless interfaces

C. Users must accept the disclaimer to continue

D. The disclaimer page is customizable

5. What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

A. Conditional-forward

B. Forward-only

C. Non-recursive

D. Recursive

SAMPLE

6. What is the main outcome of using SSL inspection on a FortiGate device?

A. To increase internet speed for users

B. To enable secure communication channels for all users

C. To identify and address potential threats within encrypted traffic

D. To isolate network segments for additional security

7. In FortiGate, what is 'Fabric Connector'?

A. A mechanism for high-speed internet connections

B. A feature that allows integration with third-party security solutions to enhance overall security

C. A command line interface tool for configuration

D. A built-in network diagnostic tool

8. In traffic shaping, what is typically adjusted to manage network load?

A. Bandwidth limits

B. Packet sizes

C. Routing metrics

D. Connection limits

9. Which statements are true regarding IPv6 anycast addresses?

A. Multiple interfaces can share the same anycast address.

B. They are allocated from the multicast address space.

C. Different nodes cannot share the same anycast address.

D. An anycast packet is routed to the nearest interface.

10. What types of authentication can be configured for FortiGate firewall users?

A. Local user accounts, RADIUS, LDAP, and TACACS+

B. Windows authentication only

C. Single Sign-On (SSO) exclusively

D. Only local user accounts

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the default administrative login for a new FortiGate unit?

A. Username "admin" with no password

B. Username "root" with password "fortinet"

C. Username "admin" with password "admin"

D. Username "administrator" with no password

The default administrative login for a new FortiGate unit is indeed the username "admin" with no password. This setup allows for immediate access to the FortiGate firewall upon initial configuration. Having no password set by default is a common practice in many networking devices to facilitate initial setup and configuration. However, it is crucial to change this default setting promptly during the initial configuration process to ensure security. By not requiring a password, it allows administrators to log in quickly and start configuring the device without the hindrance of needing to remember or input a password at that stage. The other options provided do not represent the default settings for a new FortiGate device. Using "root" and "fortinet" is incorrect as this is not the standard format for administration on FortiGate units. Similarly, "admin" with "admin" or "administrator" with no password do not reflect the default configurations. Understanding this default administrative login is essential for anyone working with FortiGate devices, as it sets the stage for their secure deployment and management.

2. How does FortiGate's application control feature function?

A. It identifies applications based on their IP addresses

B. It controls applications based on ports and protocols exclusively

C. It identifies and controls applications regardless of the ports and protocols used

D. It restricts all applications by default

FortiGate's application control feature is designed to identify and manage applications based on a combination of factors, which includes deep packet inspection and application signatures, rather than solely relying on ports and protocols. This means it can recognize applications even when they use non-standard ports or employ encryption technologies to obscure their traffic patterns. By identifying applications regardless of the ports and protocols they use, FortiGate can enforce more granular policies, allowing or blocking specific applications based on their behavior, risk assessment, or other defined criteria. This capability enhances network security by providing visibility into application usage and ensuring only authorized applications operate within the network, even if they don't adhere to typical port assignments. This contrasts with options suggesting application identification based solely on IP addresses, ports, or a blanket restriction of all applications, which would not provide the nuanced control and visibility that FortiGate's application control feature is designed to offer.

SAMPLE

3. What occurs when configuring multiple static routes with identical metrics?

A. FortiGate will randomly select one of the routes.

B. Both routes will be utilized, allowing for load balancing.

C. Conflicts will prevent any of the routes from functioning.

D. Static routes must be manually configured to avoid conflicting metrics.

When configuring multiple static routes with identical metrics, both routes will be utilized, allowing for load balancing. This means that when traffic is sent out, the FortiGate will distribute the traffic between the routes that share the same metric. This results in efficient use of available paths and increased redundancy. Load balancing improves performance by spreading the traffic load over multiple links, which can prevent any single route from becoming a bottleneck. In this scenario, the FortiGate will use equal-cost multi-path (ECMP) routing to manage the outgoing packets efficiently, ensuring that network resources are optimized. Other choices present misconceptions about static route behavior. Randomly selecting one of the routes would not take full advantage of the available bandwidth. Furthermore, conflicts do not inherently prevent routes from functioning; rather, the FortiGate is designed to handle multiple routes with the same metrics simultaneously, rather than requiring manual intervention to manage potential conflicts.

4. Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used with user authentication

B. They can only be applied to wireless interfaces

C. Users must accept the disclaimer to continue

D. The disclaimer page is customizable

In the context of firewall policy disclaimers, the correct statement is that users must accept the disclaimer to continue. This is a fundamental aspect of how disclaimers operate within a firewall or network security framework. The purpose of a disclaimer is to inform users of the policies they must abide by while using the network. By requiring users to accept the disclaimer, the system ensures that individuals are aware of and acknowledge the terms of usage before proceeding, which can help in compliance and governance. Additionally, it's worth noting that in some cases, a disclaimer may need to be displayed to users before they gain access to certain network resources. This not only serves a legal purpose but also acts as an important component in informing users about acceptable use policies, security measures, and potential risks involved in using the network. The appreciation of these disclaimers highlights their role as part of a broader security policy integrated into network management practices. Customization and application of disclaimers can vary, but the acceptance mechanism is central to their functionality.

SAMPLE

5. What are valid options for handling DNS requests sent directly to a FortiGate's interface IP? (Choose three.)

A. Conditional-forward

B. Forward-only

C. Non-recursive

D. Recursive

Handling DNS requests directly sent to a FortiGate's interface IP involves determining how the FortiGate processes such requests. The correct approach for this scenario includes using DNS options that control how queries are resolved and forwarded. One valid option is non-recursive DNS handling. In a non-recursive configuration, when a DNS query is received, the FortiGate will provide responses from its own DNS cache, if available, or will forward the query to an external DNS server without looking up the answer itself. This approach is useful when the goal is to minimize the load on the FortiGate device while still allowing for DNS query handling. Conditional-forwarding and forward-only are not typical responses directly associated with handling incoming DNS queries in this context. Conditional-forwarding applies when specific criteria are used to determine which DNS server a request should be sent to based on the domain queried. Forward-only implies that the FortiGate device will only forward DNS queries to designated servers without querying its cache or handling any local resolution. Both options focus more on operational directives for queries rather than handling incoming requests specifically. Recursive DNS, on the other hand, typically entails the device being responsible for resolving the DNS request itself, querying other DNS servers on behalf of the client. In the case

6. What is the main outcome of using SSL inspection on a FortiGate device?

A. To increase internet speed for users

B. To enable secure communication channels for all users

C. To identify and address potential threats within encrypted traffic

D. To isolate network segments for additional security

Using SSL inspection on a FortiGate device primarily serves to identify and address potential threats within encrypted traffic. This is particularly crucial as a significant amount of internet traffic is now encrypted through protocols like SSL/TLS, making it difficult for traditional security measures to inspect, analyze, or apply security policies to that traffic. By implementing SSL inspection, the FortiGate device can decrypt the encrypted traffic, allowing it to conduct a thorough examination for potential threats, such as malware or data leaks, before re-encrypting the traffic and sending it to its destination. The ability to inspect this encrypted traffic helps organizations maintain a more secure network, as unknown or malicious content can be detected and dealt with proactively. This process enhances overall network security while ensuring compliance with policies that govern data privacy and protection.

SAMPLE

7. In FortiGate, what is 'Fabric Connector'?

A. A mechanism for high-speed internet connections

B. A feature that allows integration with third-party security solutions to enhance overall security

C. A command line interface tool for configuration

D. A built-in network diagnostic tool

Fabric Connector is a feature within FortiGate that facilitates seamless integration with third-party security solutions. This capability enhances the overall security posture of the organization by allowing FortiGate devices to communicate and share intelligence with various tools and applications outside of Fortinet's ecosystem. By utilizing Fabric Connector, organizations can implement advanced security measures, orchestrate responses to threats, and leverage additional functionality from integrated services such as endpoint protection solutions, threat intelligence feeds, and security information and event management (SIEM) systems. This integration helps create a more cohesive security framework that enhances visibility and response capabilities. The other options do not align with the primary function of Fabric Connector. High-speed internet connections pertain more to network connectivity rather than security integration. A command line interface tool is focused on configuration management rather than integration with external solutions. Lastly, a built-in network diagnostic tool would relate more to troubleshooting and monitoring network performance rather than enhancing security via third-party integrations.

8. In traffic shaping, what is typically adjusted to manage network load?

A. Bandwidth limits

B. Packet sizes

C. Routing metrics

D. Connection limits

In traffic shaping, bandwidth limits are adjusted to manage network load effectively. This technique involves controlling the amount of data that can flow through the network at any given time, which helps to prevent congestion and ensures optimal performance for critical applications. By setting specific bandwidth limits for different types of traffic or users, organizations can prioritize important data transmission while reducing the impact of less critical traffic, leading to a more balanced and efficient use of network resources. This approach helps maintain the quality of service and ensures that no single user or application consumes all available bandwidth, which can degrade performance for others. Traffic shaping is particularly useful in environments where bandwidth is limited or where different services have varying needs for data transmission speed and reliability.

SAMPLE

9. Which statements are true regarding IPv6 anycast addresses?

A. Multiple interfaces can share the same anycast address.

B. They are allocated from the multicast address space.

C. Different nodes cannot share the same anycast address.

D. An anycast packet is routed to the nearest interface.

In the context of IPv6 anycast addresses, the statement highlighting that multiple interfaces can share the same anycast address is accurate. Anycast addressing is designed so that a single IP address is assigned to multiple interfaces, usually on different devices. When a packet is sent to an anycast address, it is ultimately delivered to the nearest interface (in terms of routing distance) that is configured with that anycast address. This allows for efficient routing and resource utilization, as it enables load balancing and redundancy. While some of the other statements address characteristics of anycast, they do not accurately reflect its nature. For example, anycast addresses are not allocated from the multicast address space; they have their own designation within the IPv6 addressing framework. Additionally, it is indeed possible for different nodes to share the same anycast address, which directly supports load balancing and failover configurations. Thus, A stands out as a correct statement regarding IPv6 anycast addresses.

10. What types of authentication can be configured for FortiGate firewall users?

A. Local user accounts, RADIUS, LDAP, and TACACS+

B. Windows authentication only

C. Single Sign-On (SSO) exclusively

D. Only local user accounts

The correct answer encompasses a wide range of authentication methods available for FortiGate firewall users, which allows for greater flexibility and security in user management. FortiGate firewalls can indeed be configured to use local user accounts, RADIUS, LDAP, and TACACS+. Local user accounts are used for straightforward access control within the FortiGate itself. RADIUS and TACACS+ are both protocols that support centralized authentication for network access, making them ideal for organizations that want to manage user credentials in a single location. LDAP can also be employed for directory services integration, allowing FortiGate devices to leverage existing user databases for authentication, which streamlines user management. By supporting these various methods, FortiGate enables organizations to select the best authentication strategy that aligns with their security policies and infrastructure, ensuring that both operational efficiency and security are maintained. This flexibility is crucial for adapting to different environments and user management needs.

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://fortinetnetsecurityexpert4.examzify.com

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

SAMPLE