FORTINET CERTIFIED PROFESSIONAL (FCP) FORTIGATE 7.4 ADMINISTRATOR (FCP_FGT_AD-7.4) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fcpfortigate7point4admin.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 two statements are true about the routing entries in a FortiGate routing database?**

   A. Both default routes have different administrative distances.

   B. The default route on port2 is marked as the standby route.

   C. Routing entries can only be modified by an administrator.

   D. All routes have the same administrative distance.

2. **How does a FortiGate unit typically categorize incoming traffic?**

   A. Based on user authentication

   B. Through predefined service categories

   C. Using session tracking and configured rules

   D. By the source and destination IP addresses

3. **What does UTM stand for in the context of Fortinet?**

   A. Unified Technology Management

   B. Universal Threat Module

   C. Unified Threat Management

   D. Universal Transmission Medium

4. **What does the NetSessionEnum function achieve in the context of NetAPI polling?**

   A. Tracks user logouts

   B. Authenticates user sessions

   C. Manages firewall policies dynamically

   D. Encrypts session data for security

5. **Which three strategies are valid SD-WAN rule strategies for member selection?**

   A. Manual with load balancing

   B. Lowest Cost (SLA) with load balancing

   C. Lowest Cost (SLA) without load balancing

   D. Round Robin with load balancing

SAMPLE

6. What is preventing the administrator from enabling DHCP service on FortiGate's GUI?

A. The role of the interface is restrictive

B. The GUI is not functioning properly

C. DHCP can only be enabled via CLI

D. The interface is operating in monitoring mode

7. What configuration must be ensuring for SSL inspection to function properly on FortiGate?

A. The firewall must be configured without policies

B. The firewall needs to adjust NAT settings

C. SSL certificates must be distributed to users' browsers

D. The firewall should operate in transparent mode

8. When a FortiGate firewall policy is configured with active authentication, which protocol must be allowed for user access even if authentication fails?

A. HTTP

B. DNS

C. HTTPS

D. FTP

9. What does a successful SSL VPN connection require from the client-side configuration?

A. The correct SSL VPN port to be configured

B. An active firewall rule permitting VPN connections

C. User credentials associated with the VPN configuration

D. A properly configured VPN gateway address

10. Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. All VDOMs are displayed in the topology

B. VDOMs without ports with connected devices are not displayed in the topology

C. VDOMs require additional licensing to display

D. VDOMs can only communicate with each other through a direct link

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which two statements are true about the routing entries in a FortiGate routing database?

A. Both default routes have different administrative distances.

B. The default route on port2 is marked as the standby route.

C. Routing entries can only be modified by an administrator.

D. All routes have the same administrative distance.

The correct response highlights that both default routes have different administrative distances. In FortiGate's routing database, administrative distance is a significant factor that determines which route is preferred when multiple routes to the same destination exist. By assigning different administrative distances to default routes, the FortiGate can effectively prioritize one route over another based on the value assigned. This allows for more complex routing scenarios, such as failing over to a secondary route when the primary one is unavailable or less favorable, thereby enhancing the overall reliability and performance of network routing. On the other hand, considerations about the other statements can further clarify why they do not hold true. The notion of the default route on port2 being marked as the standby route may not accurately represent the variable nature of routing configurations in FortiGate, where standby versus active routes depend significantly on administrative distances and specific configurations. The assertion that routing entries can only be modified by an administrator fails to consider the influence of dynamic routing protocols, which can also update the routing database autonomously. Lastly, the notion that all routes have the same administrative distance contradicts the fundamental principle of route selection, where different routes available for the same network or host can indeed have various administrative distances assigned.

2. How does a FortiGate unit typically categorize incoming traffic?

A. Based on user authentication

B. Through predefined service categories

C. Using session tracking and configured rules

D. By the source and destination IP addresses

A FortiGate unit categorizes incoming traffic through session tracking and configured rules, which is fundamental to its operation as a next-generation firewall (NGFW). Session tracking allows the FortiGate to monitor active sessions and manage traffics based on the established context alongside various parameters such as source, destination, and protocols. Configured rules are essential as they define how the FortiGate should handle different types of traffic. These rules can include policies for traffic inspection, security actions, and routing decisions that determine whether traffic should be permitted or denied based on predefined criteria. When a packet is received, the FortiGate evaluates it against the configured policies to correctly categorize and manage the traffic throughout its network. This capability to use session tracking in conjunction with rules enables the FortiGate to effectively apply security measures, optimize performance, and provide visibility into the network traffic, ensuring that incoming data is correctly identified and processed according to the network's security posture. While user authentication, predefined service categories, and source/destination IP addresses play a role in traffic management, they are all aspects of the broader session tracking and rules configuration mechanism that the FortiGate employs to categorize incoming traffic accurately.

SAMPLE

3. What does UTM stand for in the context of Fortinet?

A. Unified Technology Management

B. Universal Threat Module

C. Unified Threat Management

D. Universal Transmission Medium

Unified Threat Management (UTM) refers to a comprehensive cybersecurity strategy that integrates multiple security features and functions into a single platform. In the context of Fortinet, UTM encompasses various security services such as firewall protection, intrusion prevention, antivirus, web filtering, and application control, among others. The purpose of UTM is to simplify the management of security and provide a streamlined way to protect networks against a wide range of threats. Fortinet's FortiGate devices are well-known for their UTM capabilities, allowing organizations to reduce complexity while maintaining effective security measures. The other options do not accurately reflect the established term used in the context of cybersecurity and Fortinet's offerings. For instance, the concept of "Unified Technology Management" does not specifically pertain to security functions, "Universal Threat Module" is not a recognized term in cybersecurity frameworks, and "Universal Transmission Medium" refers to a communication technology concept, which is unrelated to threat management. Thus, the correct definition is Unified Threat Management, emphasizing the integrated nature of security solutions provided by Fortinet.

4. What does the NetSessionEnum function achieve in the context of NetAPI polling?

A. Tracks user logouts

B. Authenticates user sessions

C. Manages firewall policies dynamically

D. Encrypts session data for security

The NetSessionEnum function is used in the context of NetAPI polling to retrieve information about active network sessions connected to a server, typically within a Windows environment. Specifically, it provides details about user sessions, including their connection status. Therefore, it is instrumental in tracking user logouts because when a session is no longer active, the function can identify this change. The function does not handle user authentication directly; it simply enumerates existing sessions, meaning it will provide data on who is connected, their session state, and related details. Similarly, managing firewall policies or encrypting session data are not functions associated with NetSessionEnum. This function focuses primarily on obtaining session information, making it capable of identifying when users disconnect or log out from the network.

SAMPLE

5. Which three strategies are valid SD-WAN rule strategies for member selection?

A. Manual with load balancing

B. Lowest Cost (SLA) with load balancing

C. Lowest Cost (SLA) without load balancing

D. Round Robin with load balancing

The correct strategy involves using a "Manual with load balancing" approach for member selection in an SD-WAN configuration. This strategy allows administrators to set specific member gateways based on their preferences and objectives, while also enabling the load to be distributed evenly across those selected members. Manual member selection gives precise control to the administrator on which WAN links to utilize based on the network's needs, such as prioritizing certain connections due to their reliability or speed. The load balancing feature ensures that traffic is evenly distributed among the chosen members, enhancing performance and redundancy. This is crucial in SD-WAN scenarios where traffic needs to be optimized in real time across multiple paths. In contrast, other strategies may not provide the same level of flexibility or control. For instance, the "Lowest Cost (SLA)" strategies focus primarily on selecting paths based on cost-effectiveness or service level agreements, which may not meet specific network traffic requirements. Additionally, "Round Robin" methods, while useful for distributing traffic, lack manual input or controls, potentially leading to less optimal performance under certain conditions. By selecting the "Manual with load balancing" strategy, organizations can ensure that their SD-WAN operates in alignment with their specific operational priorities and performance goals.

6. What is preventing the administrator from enabling DHCP service on FortiGate's GUI?

A. The role of the interface is restrictive

B. The GUI is not functioning properly

C. DHCP can only be enabled via CLI

D. The interface is operating in monitoring mode

Enabling the DHCP service on a FortiGate device requires the interface to have the appropriate role and configuration. If the role of the interface is restrictive, it means that the settings or permissions associated with that interface do not allow for DHCP services to be activated. For example, an interface set to a role that restricts traffic management or denies service configuration would prevent an administrator from enabling DHCP. In this context, the interface's designated role must permit DHCP functionality. If the role is not configured correctly or is too restrictive, DHCP services will not be available in the GUI, making it impossible for the administrator to enable it through that interface. The other options provide scenarios that, while plausible, do not specifically address the core issue at hand. If the GUI were malfunctioning or if DHCP could only be enabled via CLI, these would not directly involve the interface's role. Similarly, operation in monitoring mode typically implies a lack of ability to change configurations, but the primary determinant for enabling DHCP service is the assigned role of the interface.

SAMPLE

7. What configuration must be ensuring for SSL inspection to function properly on FortiGate?

A. The firewall must be configured without policies

B. The firewall needs to adjust NAT settings

C. SSL certificates must be distributed to users' browsers

D. The firewall should operate in transparent mode

For SSL inspection to function properly on FortiGate, it is essential to distribute SSL certificates to users' browsers. This step is critical because SSL inspection involves the FortiGate device acting as a proxy and decrypting the SSL traffic for inspection. To achieve this without generating security warnings or trust issues in the users' browsers, the device's SSL certificate must be trusted by the client systems. When the browser encounters an SSL certificate from the FortiGate device during inspection, it needs to recognize that certificate as valid. By distributing the appropriate SSL certificate to users' browsers, the firewall can create a trusted relationship, ensuring seamless SSL inspection without interruptions. This configuration helps to maintain security compliance as browsers will not flag the certificate as untrusted, thus allowing for effective visibility into the encrypted traffic that would otherwise be inaccessible.

8. When a FortiGate firewall policy is configured with active authentication, which protocol must be allowed for user access even if authentication fails?

A. HTTP

B. DNS

C. HTTPS

D. FTP

The correct choice is DNS because, in scenarios involving active authentication on a FortiGate firewall, it's essential for the firewall to maintain basic network services even when user authentication fails. DNS (Domain Name System) is crucial for name resolution, which allows users to access websites and services using domain names instead of IP addresses. If DNS is blocked and a user's authentication fails, they may not be able to resolve the names of the sites they want to visit, effectively causing a communication breakdown. In contrast, protocols like HTTP, HTTPS, and FTP rely on successfully establishing sessions after authentication. Allowing DNS ensures that clients can still resolve domain names to access services, which is an important functional requirement even when user access is restricted. This consideration is critical in maintaining a certain level of connectivity for users while adhering to security policies.

SAMPLE

9. What does a successful SSL VPN connection require from the client-side configuration?

A. The correct SSL VPN port to be configured

B. An active firewall rule permitting VPN connections

C. User credentials associated with the VPN configuration

D. A properly configured VPN gateway address

A successful SSL VPN connection indeed requires the correct SSL VPN port to be configured on the client-side. The SSL VPN typically operates over standard ports such as 443 for HTTPS; thus, ensuring that the client is attempting to connect through the correct port is crucial for successfully establishing the connection. If the port is not correctly identified, the connection attempt can fail regardless of other configurations. While an active firewall rule permitting VPN connections is necessary, this relates more to the server-side configuration and does not directly affect the client's ability to reach the VPN. Similarly, user credentials associated with the VPN configuration are critical for authentication post-connection but do not influence the establishment of the SSL tunnel itself from the client-side perspective. Lastly, a properly configured VPN gateway address is fundamental; however, it pertains more to ensuring the client can point to the correct server, rather than the specific configurations on the client side required for the SSL establishment process. Thus, the most directly relevant requirement from a client-side configuration view is indeed having the correct SSL VPN port configured.

10. Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. All VDOMs are displayed in the topology

B. VDOMs without ports with connected devices are not displayed in the topology

C. VDOMs require additional licensing to display

D. VDOMs can only communicate with each other through a direct link

In a multi-VDOM (Virtual Domain) environment, the accurate statement regarding the deployment of the Security Fabric is that VDOMs without ports with connected devices are not displayed in the topology. This is because the Security Fabric topology is designed to show the various devices and connections that are actively involved in the security posture of the network. VDOMs that do not have any interfaces or ports linked to devices are not contributing to the overall network topology and thus are not shown. This approach helps simplify the visualization of the network's security landscape, focusing on the elements that are actually communicating and requiring monitoring. The other statements do not hold true within the context of VDOM deployments. For instance, the idea that all VDOMs appear on the topology would clutter the view with inactive components, while suggesting that additional licensing is needed to display VDOMs fails to recognize that the ability to visualize is typically part of the standard capabilities of FortiGate with VDOMs. Lastly, the notion that VDOMs can only communicate via a direct link misrepresents the more flexible communication methodologies available within Fortinet's architecture, which may include methods such as through shared resources or other configurational capabilities.

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://fcpfortigate7point4admin.examzify.com

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

SAMPLE