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

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 are two potential reasons for failed virus detection on HTTPS downloads in FortiGate? (Choose two)**

   A. The selected SSL inspection profile has certificate inspection enabled

   B. FortiGate's firewall policy is misconfigured

   C. The website is exempted from SSL inspection

   D. The antivirus engine is outdated

2. **Which FortiGate setting helps prevent the risk of unauthorized device access?**

   A. VLAN tagging

   B. IPsec encryption

   C. Active authentication

   D. Firewall policy restriction

3. **What is the correct order followed during the HTTP inspection process in web filtering when multiple features are enabled?**

   A. Static URL filter, FortiGuard category filter, and advanced filters

   B. FortiGuard category filter, static URL filter, and advanced filters

   C. Advanced filters, static URL filter, and FortiGuard category filter

   D. Advanced filters, FortiGuard category filter, and static URL filter

4. **What action can FortiGate take when detecting a blocked application?**

   A. It can log the event and notify the user

   B. It can log the event and either drop or reset the session

   C. It can temporarily block all traffic

   D. It can send an alert to the administrator

5. **What is the function of a "link control protocol (LCP)" in FortiGate's WAN Optimization?**

   A. To establish VPN connections

   B. To manage and maintain a connection between devices over a link

   C. To provide bandwidth monitoring

   D. To encrypt data transmitted over the WAN

SAMPLE

6. Which two statements are true about the requirements of connected physical interfaces on FortiGate operating in NAT mode? (Choose two)

A. Only one interface needs an IP address assigned

B. Both interfaces must have directly connected routes on the routing table

C. Both interfaces must have IP addresses assigned

D. Only the DMZ interface needs to have a route

7. What information does FortiGate use to identify the hostname of the SSL server during SSL certificate inspection?

A. The server name indication (SNI) extension in the client hello message.

B. The subject field in the user access request.

C. The SSL version supported by the server.

D. The cipher suite used for the SSL connection.

8. Which algorithm does SD-WAN use for traffic distribution that doesn't match any established rules?

A. All traffic from a source IP to a destination IP is sent to a different interface each time.

B. Traffic is evenly distributed across all available interfaces.

C. All traffic from a source IP to a destination IP is sent to the same interface.

D. Traffic is load balanced using round-robin scheduling.

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. What is the purpose of fabric-object-unification in FortiGate's security fabric?

A. Simplifying address object management

B. Enforcing compliance policies across units

C. Increasing throughput between FortiGates

D. Coordinating firmware updates across devices

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What are two potential reasons for failed virus detection on HTTPS downloads in FortiGate? (Choose two)

A. The selected SSL inspection profile has certificate inspection enabled

B. FortiGate's firewall policy is misconfigured

C. The website is exempted from SSL inspection

D. The antivirus engine is outdated

The correct choice highlights a significant aspect of how SSL inspection interacts with virus detection processes on HTTPS downloads. When the selected SSL inspection profile has certificate inspection enabled, it may not be adequately inspecting the traffic for malware or viruses because the inspection could be terminating the secure session before it is analyzed. In cases where certificate inspection is applied, FortiGate might not fully decrypt and analyze the content if it doesn't trust the certificates involved or if there are issues in the SSL handshake process. This can lead to a failure in detecting viruses that could otherwise be captured during a complete inspection of the decrypted traffic. FortiGate's antivirus engine being outdated is another plausible reason for detection failure. An outdated antivirus engine may not have the latest signatures, which could prevent the device from identifying new or evolving threats that are penetrating through HTTPS traffic. Keeping the antivirus definitions current is critical for effective threat detection, as new malware is constantly emerging. The remaining options may contribute to detection issues as well but are not as directly related to the failure in virus detection as the choices identified. Issues arising from firewall policy misconfiguration may not directly correlate to HTTPS download analysis and inspection capabilities. Similarly, if a website is exempted from SSL inspection, it may still undergo scanning by other protocols; thus

2. Which FortiGate setting helps prevent the risk of unauthorized device access?

A. VLAN tagging

B. IPsec encryption

C. Active authentication

D. Firewall policy restriction

Active authentication is a FortiGate setting designed to enhance security by validating the identity of devices attempting to access the network. This process ensures that only authorized users can connect to the system, thereby preventing unauthorized device access. Active authentication methods can include various forms of user credentials, such as usernames and passwords, digital certificates, or other validation methods that verify the identity before granting access. VLAN tagging primarily relates to network segmentation rather than directly preventing unauthorized access. It helps in organizing and managing traffic among different virtual networks but does not validate the identity of users or devices. IPsec encryption secures data in transit by establishing encrypted tunnels between devices or networks. While this is crucial for protecting data from interception, it does not directly address the need for identifying or authorizing devices before they join the network. Firewall policy restriction focuses on controlling incoming and outgoing traffic based on predetermined security rules. While effective in managing traffic flow, it does not inherently assess whether a device is authorized, making it less effective as a standalone approach to prevent unauthorized access compared to active authentication. Therefore, active authentication stands out as the most appropriate setting for preventing unauthorized device access.

SAMPLE

3. What is the correct order followed during the HTTP inspection process in web filtering when multiple features are enabled?

A. Static URL filter, FortiGuard category filter, and advanced filters

B. FortiGuard category filter, static URL filter, and advanced filters

C. Advanced filters, static URL filter, and FortiGuard category filter

D. Advanced filters, FortiGuard category filter, and static URL filter

The correct order, which is represented by the first choice, follows the established sequence of processing during the HTTP inspection process in web filtering when multiple features are enabled. Starting with the static URL filter, this initial step involves checking the requests against a defined list of URLs that are either allowed or blocked. This is a basic but effective filtering mechanism to manage access to websites based on predefined criteria. Next, the FortiGuard category filter comes into play, where the requests are further evaluated against the FortiGuard categorization service. This service classifies web content into various categories like social media, news, or adult content, allowing for more dynamic and context-based filtering decisions based on the nature of the site being accessed. Finally, advanced filters are applied, which can include more complex rules and criteria that involve additional parameters such as content type, application control, and specific user or device policies. This layer provides flexibility to accommodate nuanced security policies tailored to the organization's needs. This sequence ensures a comprehensive approach to web filtering, effectively combining both static and dynamic methods for optimal traffic management.

4. What action can FortiGate take when detecting a blocked application?

A. It can log the event and notify the user

B. It can log the event and either drop or reset the session

C. It can temporarily block all traffic

D. It can send an alert to the administrator

When FortiGate detects a blocked application, it can log the event and then take action on the session associated with that application. Specifically, the system has the ability to either drop the session, which means the data packets associated with that session are discarded, or reset the session, which involves terminating the connection and signaling the endpoints that the session has been interrupted. This dual capability allows for effective management of potentially harmful traffic while ensuring that the network remains secure. Logging the event is crucial for keeping track of what types of applications are being monitored and blocked, helping administrators to analyze traffic patterns and potential threats. The option to drop or reset the session provides immediate action against unwanted or malicious activity, protecting the network in real-time. The other options either do not encompass the full range of actions available (such as notifying users or temporarily blocking all traffic) or do not reflect the specific capabilities of FortiGate in handling blocked applications, which specifically includes managing the session itself.

SAMPLE

5. What is the function of a "link control protocol (LCP)" in FortiGate's WAN Optimization?

A. To establish VPN connections

B. To manage and maintain a connection between devices over a link

C. To provide bandwidth monitoring

D. To encrypt data transmitted over the WAN

The function of a link control protocol (LCP) in FortiGate's WAN Optimization is primarily to manage and maintain a connection between devices over a link. LCP is part of the Point-to-Point Protocol (PPP) suite and is responsible for establishing, configuring, and testing the data link connection. It plays a crucial role in ensuring that the connection remains active and is capable of handling data transfers effectively by managing options such as link quality monitoring, including negotiating link parameters and options during the connection's setup. This functionality is essential for optimizing persistent connections in WAN settings, as it helps ensure that data packets are correctly transmitted and received, without interruptions that could lead to reduced performance. Maintaining a reliable connection contributes significantly to the overall efficiency of WAN optimization efforts, minimizing latency and maximizing throughput. While other options reference important network functions—such as establishing VPN connections, providing bandwidth monitoring, and encrypting data—none of them accurately describe the specific role LCP plays in the context of link management and maintenance within WAN Optimization.

6. Which two statements are true about the requirements of connected physical interfaces on FortiGate operating in NAT mode? (Choose two)

A. Only one interface needs an IP address assigned

B. Both interfaces must have directly connected routes on the routing table

C. Both interfaces must have IP addresses assigned

D. Only the DMZ interface needs to have a route

In NAT mode, FortiGate devices manage traffic in a way that requires certain configurations for connected physical interfaces. The correct choice, stating that both interfaces must have directly connected routes on the routing table, underlines a crucial aspect of routing and communication within NAT environments. When operating in NAT mode, the FortiGate device often connects multiple interfaces—commonly a trusted internal interface (such as LAN) and an untrusted external interface (like WAN). For effective packet routing and communication between these interfaces, it is essential that both have routes in the routing table that directly connect them to each other. This ensures that the FortiGate can correctly process and forward packets between the different networks represented by these interfaces. The requirement for connected routes is critical because without them, the device may lack the necessary information to send traffic to the appropriate destination, potentially resulting in communication failures or interruptions in connectivity. In contrast, the other options lack the essential routing requirements or impose unnecessary restrictions. For instance, there is no mandate that every interface must have an IP address assigned or that only one interface should have a route. Such misconceptions could lead to misconfigured devices, affecting their performance in a live network environment.

SAMPLE

7. What information does FortiGate use to identify the hostname of the SSL server during SSL certificate inspection?

A. The server name indication (SNI) extension in the client hello message.

B. The subject field in the user access request.

C. The SSL version supported by the server.

D. The cipher suite used for the SSL connection.

The identification of the hostname of the SSL server during SSL certificate inspection primarily relies on the server name indication (SNI) extension found in the client hello message. SNI is an extension to the SSL/TLS protocols that allows the client to specify the hostname they are trying to connect to at the start of the handshake process. This is particularly useful in shared hosting environments where multiple domains are served from a single IP address. By examining the SNI, FortiGate can determine which hostname the client is attempting to reach, which is essential for SSL inspection because it allows the firewall to present the correct certificate and correctly validate the connection. This is crucial for ensuring that secure connections are appropriately filtered and monitored. Other options, while related to SSL connections, do not provide the hostname information needed for this process. The subject field in the user access request pertains more to the identity of the user rather than the server. The SSL version and cipher suite relate to the protocol and encryption methods being used but do not contain hostname information. Thus, the SNI extension is the vital piece of information used in identifying the hostname during SSL certificate inspection.

8. Which algorithm does SD-WAN use for traffic distribution that doesn't match any established rules?

A. All traffic from a source IP to a destination IP is sent to a different interface each time.

B. Traffic is evenly distributed across all available interfaces.

C. All traffic from a source IP to a destination IP is sent to the same interface.

D. Traffic is load balanced using round-robin scheduling.

In SD-WAN, when traffic doesn't match any established rules, the default behavior is to ensure that all traffic from a specific source IP to a specific destination IP is consistently directed to the same interface. This method helps maintain session persistence and integrity, ensuring that packets belonging to the same connection are sent over the same path. This behavior aids in minimizing disruptions that could occur with the reordering of packets, which is crucial for applications that are sensitive to latency and jitter. By funneling all traffic for a particular session through the same interface, the network provides a more stable experience for end users, particularly for time-sensitive applications like VoIP or video conferencing. Other methods like round-robin scheduling or even distribution can lead to packet sequencing issues and connection drops if packets are delivered over multiple paths. Therefore, maintaining a consistent path for traffic flows that do not have explicit rules is the reason behind the choice being correct.

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. What is the purpose of fabric-object-unification in FortiGate's security fabric?

A. Simplifying address object management

B. Enforcing compliance policies across units

C. Increasing throughput between FortiGates

D. Coordinating firmware updates across devices

The purpose of fabric-object-unification in FortiGate's security fabric primarily revolves around simplifying address object management. This feature allows for a centralized and cohesive way to manage and standardize address objects across all devices within the security fabric. By unifying these objects, administrators can efficiently organize, edit, and apply security policies related to these addresses without needing to replicate efforts across multiple devices or configurations. This not only improves the consistency of network policies but also reduces the potential for errors and simplifies overall management. The other choices focus on aspects that are not directly related to fabric-object-unification. While enforcing compliance policies and coordinating firmware updates are essential functions within a security fabric, they do not specifically pertain to the management and organization of address objects. Similarly, increasing throughput between FortiGates relates more to performance optimizations and network efficiency rather than the specific organizational capabilities that fabric-object-unification provides.

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