SOPHOS FIREWALL ADMINISTRATOR PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sophosfirewalladministrator.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. TRUE or FALSE: Applications discovered via synchronized application control can be added as a traffic selector under SD WAN routing.

A. True

B. False

C. Only if they are prioritized

D. Only for specific applications

2. Which of the following DoS and spoof protection modes will drop packets if the source IP address does not match an entry on the firewall's routing table?

A. IP-Spoofing

B. Flood Protection

C. HTTP Flood

D. Rate Limiting

3. When evaluating a risk score, which group should be involved in assessing the implications?

A. IT support team only

B. End users exclusively

C. Security, IT, and management teams

D. External contractors only

4. What is a key characteristic of Session persistence in SD-WAN settings?

A. Maintains user sessions across multiple connections

B. Balances traffic equally across all paths

C. Traffic is routed based on user location

D. Uses the fastest path available at all times

5. True or False: NAT rules are processed in order from top to bottom.

A. True

B. False

C. Depends on configuration

D. Not specified

SAMPLE

6. Which of the following is an attack using a spoof email to persuade users to provide sensitive information or credentials?

A. Phishing

B. Malware

C. DDoS

D. Keylogging

7. Which of the following best describes the Bridge to VLAN security mode for wireless networks?

A. Isolates wireless clients from each other

B. Allows the wireless network to extend the VLAN

C. Restricts wireless access to a specific network

D. Connects wireless devices to multiple VLANs

8. If synchronized application control is not working across your network after enabling active-active high availability, what could be the reason?

A. Synchronized Application Control is not supported in this deployment scenario

B. Firewall settings are incorrect

C. All connections are using the same IP

D. Application control is not enabled

9. Why is it important to monitor user actions in relation to the application risk meter?

A. To ensure all applications run without issues

B. To enhance network speed

C. To identify and mitigate security risks

D. To reward high-performing users

10. How can you register Sophos Firewall with your Sophos Central account?

A. Through email confirmation

B. By using OTP or credentials

C. Via a mobile app

D. Automatically during setup

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. TRUE or FALSE: Applications discovered via synchronized application control can be added as a traffic selector under SD WAN routing.

A. True

B. False

C. Only if they are prioritized

D. Only for specific applications

The statement is true because applications that are discovered through synchronized application control can indeed be utilized as traffic selectors in SD-WAN routing. This feature enhances the firewall's capabilities by allowing it to make smarter routing decisions based on real-time application data. By integrating application awareness into SD-WAN routing, administrators have the ability to create more granular and effective policies, ensuring optimal performance for critical applications and improved bandwidth management. The ability to add applications as traffic selectors means that specific applications can be identified and prioritized based on their needs, routing criteria, and the overall goals of the organization. This aligns with optimal SD-WAN management, enabling organizations to dynamically adapt their traffic flow in response to application behavior and requirements, thereby improving user experience and network efficiency.

2. Which of the following DoS and spoof protection modes will drop packets if the source IP address does not match an entry on the firewall's routing table?

A. IP-Spoofing

B. Flood Protection

C. HTTP Flood

D. Rate Limiting

The choice of IP-Spoofing is accurate in this context because this protection mode specifically helps to prevent unauthorized access and mitigate denial of service (DoS) attacks by checking the source IP address against the routing table on the firewall. If a packet arrives with a source IP address that doesn't correspond to a valid entry in the routing table, the firewall recognizes that the packet may be spoofed—meaning it's trying to masquerade as a trusted source. As a result, the packet is dropped to prevent potential malicious traffic from entering the network. The IP-Spoofing protection mode plays a pivotal role in demonstrating the security functionality of a firewall, ensuring only legitimate traffic with valid source IPs is allowed. This is particularly crucial in maintaining the integrity and security of the network against impersonation attacks. The other listed options typically do not focus on checking the source IP against the routing table in this specific manner. For example, Flood Protection primarily works to identify and mitigate traffic surges from legitimate sources, whereas HTTP Flood targets HTTP traffic specifically and manages requests to prevent overloading a web server. Rate Limiting regulates the number of packets or connections and is more about managing traffic flows than explicitly validating source IPs against the routing table.

SAMPLE

3. When evaluating a risk score, which group should be involved in assessing the implications?

A. IT support team only

B. End users exclusively

C. Security, IT, and management teams

D. External contractors only

In assessing the implications of a risk score, including the security, IT, and management teams is crucial for a comprehensive evaluation. Each of these groups brings specific expertise and perspective needed for thorough risk assessment. The security team has the specialized knowledge of potential threats and vulnerabilities, which is essential in understanding the implications of various risks. Meanwhile, the IT team has a deep understanding of the technical infrastructure and can evaluate how risks might impact system operations and data integrity. Management teams contribute a broader organizational perspective, including insights into strategic priorities and resource allocation. Their involvement ensures that the implications of the risk score are considered in the context of overall business objectives and compliance requirements. Collaborating among these groups helps ensure that the assessment is well-rounded and facilitates informed decision-making regarding risk mitigation strategies. This collaboration is ineffective if isolated to just one group, as it would lack the diverse knowledge necessary for understanding the multifaceted nature of risk in an organization.

4. What is a key characteristic of Session persistence in SD-WAN settings?

A. Maintains user sessions across multiple connections

B. Balances traffic equally across all paths

C. Traffic is routed based on user location

D. Uses the fastest path available at all times

Session persistence in SD-WAN settings is primarily about maintaining user sessions across multiple connections. This characteristic ensures that once a session is established, it remains uninterrupted and consistent even if the underlying network paths change. This is critical for applications that rely on stable connections, such as VoIP or video conferencing, where any disruption can lead to degraded performance or loss of connectivity. Maintaining session persistence allows for efficient use of available bandwidth while ensuring that end-users experience a seamless service. User sessions can be maintained without requiring re-establishment of sessions, which can introduce latency or other issues. The other options relate to different aspects of traffic management and routing but do not capture the essence of session persistence. While balancing traffic, routing based on location, and using the fastest path are important for overall network efficiency and performance, they do not guarantee that active user sessions remain stable during path changes, which is the crux of session persistence.

SAMPLE

5. True or False: NAT rules are processed in order from top to bottom.

A. True

B. False

C. Depends on configuration

D. Not specified

NAT (Network Address Translation) rules are indeed processed in order from top to bottom. This sequential processing means that when a packet matches the condition of a NAT rule, that rule is applied, and no further rules are evaluated for that packet. This approach allows administrators to establish precedence among rules by placing more specific rules higher in the list, directing how IP addresses should be translated. For example, if you have multiple rules that affect the same traffic, the first matching rule will take effect. This ordered processing is crucial for correctly managing how traffic flows in and out of the network, ensuring that the desired translations occur as intended. The idea that it is false or context-dependent would indicate either a misunderstanding of NAT processing or suggest that configurations can override the standard processing order, which is not the case in this scenario. Thus, the correct understanding is that NAT rules always follow the top-to-bottom processing order.

6. Which of the following is an attack using a spoof email to persuade users to provide sensitive information or credentials?

A. Phishing

B. Malware

C. DDoS

D. Keylogging

Phishing is a cyberattack that typically involves the use of spoofed emails designed to trick users into divulging sensitive information, such as usernames, passwords, or financial data. The attacker often masquerades as a trustworthy entity, such as a bank or a recognizable service, to gain the victim's confidence. These emails usually contain urgent requests or enticing links that lead to fake websites, where the unsuspecting user is prompted to enter their credentials. This method leverages social engineering techniques to manipulate individuals. It exploits emotional responses, creating a false sense of urgency or security that compels recipients to act without critically evaluating the information presented. Due to its effectiveness and widespread use, phishing remains a significant threat in the cybersecurity landscape. In contrast, malware refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. DDoS (Distributed Denial of Service) attacks aim to overwhelm a network or service with traffic, rendering it unusable. Keylogging involves capturing the keystrokes of a user, which can be a consequence of malware but is not directly related to the act of soliciting information via spoofed communications.

SAMPLE

7. Which of the following best describes the Bridge to VLAN security mode for wireless networks?

A. Isolates wireless clients from each other

B. Allows the wireless network to extend the VLAN

C. Restricts wireless access to a specific network

D. Connects wireless devices to multiple VLANs

Bridge to VLAN security mode for wireless networks primarily functions to extend VLANs (Virtual Local Area Networks) to wireless clients. This mode allows the wireless access points to bridge the wireless clients directly to the specified VLAN on the wired network. As a result, wireless clients can communicate as if they are plugged into that VLAN's wired segment, receiving the same policies and access rights as wired devices on that VLAN. This approach enhances the network's flexibility, as it permits seamless integration of wireless devices into existing VLAN architecture, thus maintaining consistent security policies and improving device management. By extending VLANs wirelessly, devices can interact with the broader network while benefiting from VLAN segmentation and its advantages, such as traffic management and improved security. Other options do not accurately capture the specific function of Bridge to VLAN mode. While isolating clients, restricting access, and connecting devices to multiple VLANs are important aspects of network security and functionality, they do not pertain to the primary purpose of this mode, which is to create an extended architecture for managing wireless traffic within a designated VLAN.

8. If synchronized application control is not working across your network after enabling active-active high availability, what could be the reason?

A. Synchronized Application Control is not supported in this deployment scenario

B. Firewall settings are incorrect

C. All connections are using the same IP

D. Application control is not enabled

Synchronized Application Control is designed to provide a unified view and management of applications across a network. In the context of active-active high availability (HA) deployments, certain features may be limited or unsupported to ensure optimal performance and functionality. In the specific case where Synchronized Application Control is not functional after setting up an active-active HA configuration, the primary reason may stem from the inherent limitations of the technology in this deployment scenario. It is vital for administrators to understand that not all features available in a single instance of the firewall will translate seamlessly to a multi-unit high-availability setting, especially in configurations designed to handle simultaneous traffic across multiple devices. Both the limitations of application synchronization and the complexities introduced by maintaining state across multiple active devices make it clear that administrators should verify the compatibility of specific features when configuring HA settings. This means recognizing that Synchronized Application Control may not be supported within this specific scenario, guiding users towards alternative methods or configurations that ensure effective application management in high-availability environments.

SAMPLE

9. Why is it important to monitor user actions in relation to the application risk meter?

A. To ensure all applications run without issues

B. To enhance network speed

C. To identify and mitigate security risks

D. To reward high-performing users

Monitoring user actions in relation to the application risk meter is crucial for identifying and mitigating security risks. The application risk meter is a tool that assesses the security posture of applications used within a network, categorizing them based on their potential risk to the organization. By closely observing how users interact with these applications, administrators can detect unusual or potentially harmful behaviors that may indicate a security threat, such as data breaches or unauthorized access. This monitoring enables organizations to proactively manage risks by allowing them to take appropriate actions—such as restricting access to high-risk applications or implementing stricter security measures. In doing so, it ultimately helps in protecting sensitive data and maintaining the integrity of the network. While ensuring applications run without issues and enhancing network speed are important in their own right, they do not directly relate to the critical need for security oversight. Rewarding high-performing users also does not align with the primary goal of monitoring user actions concerning the application's inherent risks. Thus, focusing on security risk mitigation is the most relevant and vital reason for such monitoring.

10. How can you register Sophos Firewall with your Sophos Central account?

A. Through email confirmation

B. By using OTP or credentials

C. Via a mobile app

D. Automatically during setup

Registering Sophos Firewall with your Sophos Central account typically involves using one-time passwords (OTP) or credentials associated with your Sophos Central account. This process ensures that the firewall can securely connect and communicate with the Sophos Central management platform, allowing for centralized management of security policies, monitoring, and reporting. Using OTP or credentials is a common method to establish a secure connection, as it verifies the identity and authorization of the device being registered. This step is crucial for ensuring that only authenticated and authorized devices can access the central management services. The other methods listed, such as email confirmation, using a mobile app, or automatic registration during setup, can be part of adjacent processes but may not directly apply to the secure registration of the firewall in this context. For example, email confirmation typically deals with verifying account ownership rather than registering devices, while mobile apps may facilitate account management rather than the direct registration of hardware like firewalls. Automatic registration could occur in some cases, but it generally requires prior authorization through user credentials to ensure security compliance.

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://sophosfirewalladministrator.examzify.com

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

SAMPLE