Sophos Firewall Administrator Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
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

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 must you choose if you want a certificate to be signed by a third-party company?

A. Generate Key

B. Request Signing

C. Generate CSR

D. Import Certificate

2. When installing STAS on a single domain controller, which installation type should you select?

A. Standard Installation

B. SSO Suite

C. Basic Configuration

D. Enterprise Suite

3. What is the purpose of configuring syslog servers on Sophos Firewall?

A. To enhance firewall security

B. To send logs for external monitoring

C. To block unauthorized access

D. To recover deleted files

4. You are checking the application risk meter which is reporting a risk score of 4.2. What does this indicate about user behavior on the network?

A. Users are completely safe from threats

B. Users are performing risky actions on the network

C. No users are accessing the network

D. Users are following security protocols

5. How should users be informed about the risks associated with a score of 4.2?

A. Through automated alerts and training sessions

B. By ignoring the risk score

C. Only during annual security audits

D. Through general announcements only

SAMPLE

6. Which two VPN protocols are supported by Sophos Firewall for Site to Site connections?

A. PPTP and L2TP

B. SSL and IPSEC

C. GRE and OpenVPN

D. SSH and ICMP

7. What does the term "malicious traffic" refer to in DoS Protection?

A. Unauthorized access attempts

B. Traffic intending to disrupt services

C. Regular traffic spikes

D. Internal network traffic

8. What limit is imposed on the configuration of static DNS servers in Sophos Firewall?

A. 4 servers

B. 3 servers

C. 2 servers

D. 1 server

9. True or False: RED connections are automatically added to the VPN Zone.

A. True

B. False

C. Only in certain cases

D. Depends on configuration

10. True or False: Web protection exceptions apply to all web protection policies regardless of when they are applied in the Sophos Firewall.

A. True

B. False

C. Depends on configuration

D. Only applies for HTTPS traffic

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What must you choose if you want a certificate to be signed by a third-party company?

A. Generate Key

B. Request Signing

C. Generate CSR

D. Import Certificate

When you want a certificate to be signed by a third-party company, the correct step is to generate a Certificate Signing Request (CSR). A CSR is essentially a message sent from an applicant to a certificate authority (CA) to apply for a digital certificate. This request contains information including the public key that will be included in the certificate, along with the details of the organization requesting the certificate. Generating a CSR is crucial because it contains the necessary information that the CA needs to verify your identity and then cryptographically sign your public key, thereby giving you a trusted certificate. This certificate can then be used to establish secure communications, authenticate a website, or sign documents. The process typically follows these steps: first, you generate a private key on your server, which remains confidential; then, you create a CSR using that key. Finally, you send the CSR to the CA, who verifies your information and issues the signed certificate. In contrast, generating a key only creates a private key without initiating the signing process, while requesting signing does not generate the required CSR. Importing a certificate is for bringing an already signed certificate into your system, which doesn't apply when you're starting the signing process with a third-party company.

2. When installing STAS on a single domain controller, which installation type should you select?

A. Standard Installation

B. SSO Suite

C. Basic Configuration

D. Enterprise Suite

When installing the Sophos Transparent Authentication Suite (STAS) on a single domain controller, selecting the SSO Suite as the installation type is appropriate because it is specifically designed to facilitate single sign-on (SSO) capabilities. This suite streamlines the authentication process by allowing users to access network resources without needing to re-enter their credentials, leveraging the single domain controller's capabilities to provide seamless access. In cases where small to medium environments are involved, the SSO Suite is optimal because it incorporates the functions necessary for transparent authentication while simplifying configuration for a single server scenario. It allows for efficient management of user login sessions, monitoring activity, and ensuring secure access to resources across the network. Other installation types might be intended for larger or more complex environments, where additional features or components would be necessary. For instance, the Standard Installation often provides a more straightforward deployment without the full suite of SSO capabilities. The Basic Configuration may limit functionality and would not fully leverage the advantages of using STAS on a domain controller. Meanwhile, the Enterprise Suite is aimed at larger organizations where multiple servers and advanced setups are required, which isn't necessary for a single domain installation. Thus, the SSO Suite is tailored for the context presented and optimally supports the functionalities needed in

SAMPLE

3. What is the purpose of configuring syslog servers on Sophos Firewall?

A. To enhance firewall security

B. To send logs for external monitoring

C. To block unauthorized access

D. To recover deleted files

Configuring syslog servers on Sophos Firewall primarily serves the purpose of sending logs for external monitoring. This functionality allows administrators to centralize their log management by forwarding logs to a dedicated syslog server, which can then analyze, store, and visualize this data comprehensively. By using external monitoring solutions, organizations can enhance their ability to audit network activities, track potential security incidents, and ensure compliance with regulatory requirements. This centralized logging can facilitate better analysis and quicker response to incidents, as well as offer insights into network performance and health. The other options do not accurately reflect the function of syslog server configuration. While enhancing firewall security and blocking unauthorized access are important aspects of firewall management, these are more about the core features and functionalities of the Sophos Firewall itself. Recovering deleted files is outside the scope of syslog usage, as syslog primarily deals with logging events and not file recovery processes.

4. You are checking the application risk meter which is reporting a risk score of 4.2. What does this indicate about user behavior on the network?

A. Users are completely safe from threats

B. Users are performing risky actions on the network

C. No users are accessing the network

D. Users are following security protocols

A risk score of 4.2 on the application risk meter indicates that users are engaging in activities that are considered to be risky on the network. This score reflects a considerable level of potential risk which could include unsafe behaviors such as accessing untrusted applications, visiting sites known for malicious content, or interacting with high-risk online services. In a security context, a higher risk score often highlights user actions that could lead to data breaches, malware infections, or other cybersecurity threats. Organizations typically use such risk assessments to identify and mitigate vulnerabilities in user behavior, deploying security measures or policies to minimize exposure to threats. By understanding the significance of a score like 4.2, network administrators can take proactive steps to educate users about safe practices, implement stricter access controls, and enhance monitoring to ensure a safer computing environment. This proactive approach aims not just to respond to threats but to foster a culture of security awareness among users.

SAMPLE

5. How should users be informed about the risks associated with a score of 4.2?

A. Through automated alerts and training sessions

B. By ignoring the risk score

C. Only during annual security audits

D. Through general announcements only

Users should be informed about the risks associated with a score of 4.2 through automated alerts and training sessions because this approach ensures that individuals receive timely and relevant information about potential security threats. Automated alerts can provide immediate notifications when a risk is identified, allowing users to respond quickly and effectively. Training sessions further enhance understanding by educating users on how to mitigate these risks and recognize their implications. This combination of proactive communication and education equips users with the knowledge necessary to maintain a secure environment and fosters a culture of security awareness within the organization. In contrast, ignoring the risk score would leave users unprepared to handle potential threats, while relying solely on annual security audits would mean that users are not kept informed throughout the year. General announcements do not provide the detailed context necessary for users to comprehend the specific implications of a 4.2 score, which diminishes the effectiveness of the notification.

6. Which two VPN protocols are supported by Sophos Firewall for Site to Site connections?

A. PPTP and L2TP

B. SSL and IPSEC

C. GRE and OpenVPN

D. SSH and ICMP

Sophos Firewall supports both SSL and IPsec protocols for Site to Site connections, making this choice correct. SSL (Secure Sockets Layer) VPN provides a secure and encrypted tunnel between two endpoints and is particularly useful for remote access as well as site-to-site connections when enhanced security is required. It uses the SSL protocol, which is widely recognized for its encryption capabilities. IPsec (Internet Protocol Security) is another prevalent protocol used for establishing secure connections over IP networks. It operates at the network layer and secures IP communications by authenticating and encrypting each IP packet in a communication session. IPsec is often preferred for Site to Site connections due to its robustness and compatibility across multiple types of devices and environments. The combination of these two protocols allows for flexible deployment options depending on the specific network needs and security requirements. Other options mentioned do not provide the same level of support or security features for Site to Site connections through the Sophos Firewall.

SAMPLE

7. What does the term "malicious traffic" refer to in DoS Protection?

A. Unauthorized access attempts

B. Traffic intending to disrupt services

C. Regular traffic spikes

D. Internal network traffic

The term "malicious traffic" in the context of DoS (Denial of Service) Protection specifically refers to traffic that is purposefully generated with the intent to disrupt services. This type of traffic is often overwhelming to the target system, aiming to consume network resources, bandwidth, or server capabilities, thus rendering those services unavailable to legitimate users. The primary goal of such traffic is to cause harm by interrupting normal operations, which aligns directly with the definition of malicious activity in the realm of network security. Other options do not accurately capture this concept. Unauthorized access attempts are related to security breaches but do not necessarily contribute to service disruption in the same manner. Regular traffic spikes can occur due to legitimate usage patterns and do not imply malicious intent. Internal network traffic is part of normal operations within an organization and typically does not fall under the category of malicious unless specifically crafted to compromise the network from within.

8. What limit is imposed on the configuration of static DNS servers in Sophos Firewall?

A. 4 servers

B. 3 servers

C. 2 servers

D. 1 server

In Sophos Firewall, the configuration of static DNS servers is limited to a maximum of three servers. This allows organizations to provide redundancy and failover capabilities in their DNS resolution process. When specifying multiple DNS servers, the firewall will query them in order until it receives a response, which enhances the reliability and performance of network communications. The choice to allow three static DNS servers strikes a balance between simplicity and increased resiliency. It accommodates different scenarios where additional DNS servers may be necessary, such as when using both internal and external DNS services or when an organization employs multiple DNS providers for fault tolerance. This limitation of three servers ensures that configurations remain manageable while still providing the necessary level of redundancy for effective network operations.

SAMPLE

9. True or False: RED connections are automatically added to the VPN Zone.

A. True

B. False

C. Only in certain cases

D. Depends on configuration

RED (Remote Ethernet Device) connections are not automatically added to the VPN Zone in a Sophos Firewall environment. Instead, RED operates independently of the VPN configurations. When a RED device is deployed, it creates a secure connection to the Sophos Firewall, but that connection is mainly used to tunnel traffic from remote Ethernet devices to the central site without being part of the actual VPN zone. The misunderstanding may arise from the fact that while the RED connection does facilitate secure communication similar to a VPN, it uses its own mechanisms and settings distinct from standard VPN zones. This isolation ensures that network administrators have clear control over which devices and traffic patterns are integrated into the VPN zone versus those that are managed by the RED mechanism. Thus, the statement that RED connections are automatically added to the VPN Zone is false.

10. True or False: Web protection exceptions apply to all web protection policies regardless of when they are applied in the Sophos Firewall.

A. True

B. False

C. Depends on configuration

D. Only applies for HTTPS traffic

The statement is true because web protection exceptions are designed to be universally applicable across all web protection policies implemented within the Sophos Firewall. This means that once an exception is established, it takes precedence over the specific settings of any subsequent web protection policies, regardless of the order in which they are applied. This functionality ensures that particular websites, categories, or user groups can be consistently managed, allowing for flexible control over web traffic while maintaining security protocols. Therefore, any exception defined will automatically influence the behavior of the web protection policies that are in place, independent of their sequence or settings. In this context, other options like false or conditional statements might suggest limitations or exceptions that do not reflect the comprehensive nature of how web protection exceptions are designed to operate within the firewall system. This reinforces the understanding that exceptions serve as a high-level control mechanism, streamlining administrative tasks and enhancing overall web security management.

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