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

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 2 actions are required to utilize IPS policies on the Sophos Firewall?**

   A. Select an IPS policy in a firewall rule; Enable IPS with a switch

   B. Select an IPS policy; Enable logging

   C. Allow IPS from the dashboard; Set alerts

   D. Configure firewall rules; Set network zones

2. **Under what conditions can non-administrative users log in to the Web Admin of Sophos Firewall?**

   A. They can log in during maintenance hours

   B. They cannot log in

   C. They can log in for monitoring purposes

   D. They can log in with special permissions

3. **What is the maximum number of external syslog servers you can configure on Sophos Firewall?**

   A. 3

   B. 5

   C. 10

   D. 15

4. **Which of the following is a potential consequence of a risk score indicating risky user actions?**

   A. Increased system performance

   B. Higher chances of security breaches

   C. Improved user compliance

   D. Guaranteed data integrity

5. **What is the consequence when a user logs in to the Sophos Firewall as part of multiple groups?**

   A. All groups are active

   B. The first matched group is active

   C. Only the highest priority group is active

   D. No groups will be active

SAMPLE

6. Which three actions are necessary for Synchronized User ID to work?

A. Configure an AD authentication server on the Sophos Firewall

B. Enable AD server in the Firewall authentication methods

C. Import groups from AD into the Sophos firewall

D. Enable VPN authentication

7. Which option is supported when using the DPI Engine?

A. Custom DNS settings

B. Configure quota time

C. Bandwidth limit per user

D. IP address exclusion

8. Which aspect of security does hotspot creation aim to improve in a network?

A. Traffic management

B. Authorization of guest access

C. Full visibility into internal traffic

D. Access to restricted websites

9. What is the primary benefit of using the Sophos Web Filter?

A. Content filtering and malware protection

B. Improved network speed

C. Redundant internet connections

D. Increased bandwidth

10. Which protocols are supported by clientless SSL VPN access?

A. SSH, HTTP, FTP, RDP

B. SSH, VNC, FTP, RDP, SMB

C. SSH, VNC, HTTPS, Telnet, SMB

D. HTTP, FTP, VNC, RDP, SMB

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What 2 actions are required to utilize IPS policies on the Sophos Firewall?

A. Select an IPS policy in a firewall rule; Enable IPS with a switch

B. Select an IPS policy; Enable logging

C. Allow IPS from the dashboard; Set alerts

D. Configure firewall rules; Set network zones

To utilize Intrusion Prevention System (IPS) policies on the Sophos Firewall, it is essential to select an IPS policy in a firewall rule and enable IPS. This is fundamental because the IPS functions as a protective measure that actively monitors network traffic for potentially malicious activity, so its configuration must be explicitly associated with a firewall rule to ensure it is applied correctly. Enabling IPS with a switch in the configuration confirms that the firewall will process incoming and outgoing traffic through the defined IPS policy. Selecting an IPS policy is a crucial step as it specifies which set of rules the firewall will enforce to identify and block threats. Additionally, enabling IPS is necessary to activate the feature, meaning that simply having an IPS policy defined is not sufficient; it must be actively applied to the traffic being managed by the firewall. This makes the combination of selecting an IPS policy in a firewall rule and enabling IPS essential for effective operation of the system.

2. Under what conditions can non-administrative users log in to the Web Admin of Sophos Firewall?

A. They can log in during maintenance hours

B. They cannot log in

C. They can log in for monitoring purposes

D. They can log in with special permissions

Non-administrative users are not permitted to log in to the Web Admin interface of the Sophos Firewall, which includes restrictions on access to the administrative functionalities of the system. This limitation is in place primarily due to security considerations, as allowing unauthorized or non-authorized users to access the Web Admin could lead to unintended changes or potential breaches. Typically, only users with administrative privileges are granted access to the administrative interface, ensuring that configurations, monitoring, and critical settings can be managed exclusively by those with the correct permissions. Non-admin users may have access to other aspects of the network or device, but their inability to log in to the Web Admin secures the administrative controls from risks associated with wider user access. This principle is aligned with best practices in cybersecurity, emphasizing the importance of controlling administrative access to sensitive systems. While other conditions listed may seem plausible, non-administrative users logging in at any time or with any permissions still would present security risks that the firewall's design aims to mitigate.

SAMPLE

3. What is the maximum number of external syslog servers you can configure on Sophos Firewall?

A. 3

B. 5

C. 10

D. 15

The maximum number of external syslog servers that can be configured on Sophos Firewall is five. This capability allows users to centralize logs and monitor them from multiple devices, improving the management of security events and compliance reporting. By supporting five syslog servers, Sophos Firewall provides flexibility for organizations that may want to send logs to different logging solutions or services for redundancy and event correlation. This setup can be particularly useful in environments where multiple branches or systems need to maintain central visibility into logs for security analysis or audits. The choice of this specific number reflects a balance between usability and the complexity of managing log data across various external systems.

4. Which of the following is a potential consequence of a risk score indicating risky user actions?

A. Increased system performance

B. Higher chances of security breaches

C. Improved user compliance

D. Guaranteed data integrity

A risk score indicating risky user actions is a critical assessment used to evaluate the likelihood of potential security threats posed by user behavior. When users engage in actions that are deemed risky, such as accessing sensitive data without proper authorization or bypassing security protocols, this can significantly increase the likelihood of security breaches occurring. Higher chances of security breaches stem from the fact that risky behaviors can expose vulnerabilities within the system, allowing malicious actors to take advantage of these weaknesses. For example, if a user frequently accesses or shares sensitive information without appropriate safeguards, this creates pathways for unauthorized access, data leaks, or other forms of cyberattacks. In contrast, the other options do not align with the implications of risky user actions. Increased system performance is unrelated to user risk behavior, and improved user compliance would be the opposite of what is expected with risky actions. Additionally, guaranteed data integrity is not achievable in environments where user behaviors are risky, as such actions compromise the security and reliability of the data. Thus, the correlation between a high-risk score and the heightened potential for security breaches is evident and underscores the importance of monitoring and addressing risky user actions effectively.

SAMPLE

5. What is the consequence when a user logs in to the Sophos Firewall as part of multiple groups?

A. All groups are active

B. The first matched group is active

C. Only the highest priority group is active

D. No groups will be active

When a user logs into the Sophos Firewall and is a member of multiple groups, the pivotal factor is how the system determines which group is considered active. In this scenario, the firewall evaluates the groups and identifies the first matched group that aligns with the user's attributes and permissions. This means that as soon as it identifies a matching group during its process, it will activate that group, thereby overriding the potential activation of any subsequent groups the user may belong to. This behavior is essential for ensuring that the firewall can efficiently apply the correct policies and configurations to the user's session based on their initial match, providing a streamlined and effective security posture. Consequently, it helps in managing access rights and permissions without the complexity of handling multiple group effects simultaneously, which could lead to conflicts or confusion regarding user privileges. Understanding this mechanism is crucial for administrators when designing group policies and determining how they interact with user logins and access controls.

6. Which three actions are necessary for Synchronized User ID to work?

A. Configure an AD authentication server on the Sophos Firewall

B. Enable AD server in the Firewall authentication methods

C. Import groups from AD into the Sophos firewall

D. Enable VPN authentication

For Synchronized User ID to function correctly, it requires several key components to be properly set up. Configuring an Active Directory (AD) authentication server on the Sophos Firewall is fundamental because this establishes the connection between the firewall and the AD environment. This connection facilitates the firewall's ability to authenticate users based on their AD credentials. When the Sophos Firewall is linked to Active Directory, it can communicate with the directory services to retrieve user information, including group memberships and user identities. Without this configuration, the firewall would not be able to verify user identities, which is crucial for implementing user-based policies and controls. In addition to setting up an AD authentication server, other actions are necessary for full functionality of Synchronized User ID. For instance, enabling the AD server in the firewall authentication methods and importing groups from AD into the Sophos firewall are also critical steps that support user identification and policy application based on group memberships. However, the foundational step of configuring the AD authentication server is what allows the firewall to establish the necessary connection to the user directory for synchronization.

SAMPLE

7. Which option is supported when using the DPI Engine?

A. Custom DNS settings

B. Configure quota time

C. Bandwidth limit per user

D. IP address exclusion

The recognition of the ability to configure quota time within the DPI (Deep Packet Inspection) Engine highlights one of its fundamental functionalities. The DPI Engine is designed to analyze and manage network traffic deeply, allowing for precise control over how long users can consume bandwidth. By implementing quota time, network administrators can establish specific limits for user activity, ensuring that no single user monopolizes bandwidth resources and that network performance remains optimal for all. This capability supports fair usage policies, enhances user experience by preventing lag caused by excessive bandwidth consumption, and helps in maintaining an overall balanced network load. Additionally, it can enforce compliance with organizational policies around internet usage, making it a vital feature when managing large or diverse user groups. While other options might seem relevant, they do not align with the primary functions of the DPI Engine in terms of traffic analysis and management. The DPI Engine focuses on inspecting and regulating traffic rather than configuring settings like DNS or applying exclusions based on IP addresses.

8. Which aspect of security does hotspot creation aim to improve in a network?

A. Traffic management

B. Authorization of guest access

C. Full visibility into internal traffic

D. Access to restricted websites

Hotspot creation is primarily designed to enhance the authorization of guest access within a network. By implementing hotspot functionality, organizations can set up a controlled and secure environment for temporary users—such as visitors or clients—allowing them to access the network under specific conditions. This process involves providing a means for guests to authenticate themselves before gaining internet access. Often, guests may be required to enter credentials, accept terms of service, or enter a code to gain entry. This helps ensure that the network is protected against unauthorized usage, as it allows the organization to control who accesses the network and under what terms. While traffic management, visibility into internal traffic, and access to restricted websites are important aspects of network security, they do not directly relate to the primary purpose of hotspot creation. The main focus of hotspot functionality is to establish a secure and manageable gateway for guests, making sure that while they can connect to the internet, their access is monitored and regulated according to organizational policies.

SAMPLE

9. What is the primary benefit of using the Sophos Web Filter?

A. Content filtering and malware protection

B. Improved network speed

C. Redundant internet connections

D. Increased bandwidth

The primary benefit of using the Sophos Web Filter is content filtering and malware protection. This feature is crucial for organizations seeking to enforce acceptable use policies and protect their network from harmful websites. By controlling and monitoring access to web content, the Sophos Web Filter helps to block inappropriate or malicious sites, thereby reducing the risk of malware infections and compromising sensitive data. Moreover, effective content filtering contributes to enhanced productivity by preventing employees from accessing distracting or non-work-related websites. It also minimizes the chances of falling victim to phishing attacks or other online threats. Overall, the Sophos Web Filter serves as a robust security measure that works to safeguard the network while also aligning internet use with company policies.

10. Which protocols are supported by clientless SSL VPN access?

A. SSH, HTTP, FTP, RDP

B. SSH, VNC, FTP, RDP, SMB

C. SSH, VNC, HTTPS, Telnet, SMB

D. HTTP, FTP, VNC, RDP, SMB

Clientless SSL VPN access is designed to allow users to access services without needing to install additional client software on their devices. In this context, the supported protocols must be those that can be operated entirely within a web browser or through native remote desktop functionalities. The correct option includes protocols that allow secure access to various types of remote services. SSH (Secure Shell) is widely used for secure command-line access to servers, VNC (Virtual Network Computing) enables remote desktop access, FTP (File Transfer Protocol) is used for file transfers, RDP (Remote Desktop Protocol) permits users to connect to remote Windows computers, and SMB (Server Message Block) facilitates file sharing and printer access on Windows networks. These protocols collectively satisfy the requirements for clientless access, as they can be managed through browser-based interfaces or remote connections that do not necessitate separate client software installations. This ensures that users can maintain secure and convenient access to resources across different services while leveraging the flexibility of SSL VPN technology.

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