

# SonicWall Network Security Administrator (SNSA) Practice Test (Sample)

## Study Guide



**Everything you need from our exam experts!**

**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

<b>Copyright</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>How to Use This Guide</b> .....	<b>4</b>
<b>Questions</b> .....	<b>5</b>
<b>Answers</b> .....	<b>8</b>
<b>Explanations</b> .....	<b>10</b>
<b>Next Steps</b> .....	<b>16</b>

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.

# 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!**

## **Questions**

SAMPLE

- 1. Which best practices should be implemented before updating the firmware on SonicWall devices?**
  - A. Create a backup and Download a settings file locally**
  - B. Update all licenses and Restart the device**
  - C. Reconfigure all settings and Check for compatibility**
  - D. Notify users and Log changes**
- 2. What is split horizon in relation to RIP?**
  - A. It sends learned routes to all adjacent routers**
  - B. It allows the use of multiple routing protocols simultaneously**
  - C. It suppresses learned routes in updates to prevent routing loops**
  - D. It enhances bandwidth by reducing unnecessary updates**
- 3. What is a primary function of the Neighbor Discovery protocol?**
  - A. It provides network address translation**
  - B. It helps discover other devices on the local network**
  - C. It establishes VPN connections**
  - D. It manages firewall traffic**
- 4. True or False: The firewall can perform a rolling analysis of event logs for web site access and bandwidth use.**
  - A. True**
  - B. False**
  - C. Only under specific conditions**
  - D. Requires a separate license**
- 5. True or False: Static Routes by default take precedence over VPN traffic.**
  - A. True**
  - B. False**
  - C. Depends on the configuration**
  - D. Only for specific types of traffic**

**6. What sorts of data does the App Flow Monitor specifically track?**

- A. Only firewall breach attempts**
- B. Incoming and outgoing data packets**
- C. Administrative login attempts**
- D. SonicWall configuration changes**

**7. What is a method to replicate settings or configurations across tenants?**

- A. Templates**
- B. Custom scripts**
- C. Manual configuration**
- D. Policy export**

**8. How many web proxy servers can be configured on a SonicWall?**

- A. 16**
- B. 32**
- C. 64**
- D. 128**

**9. Next Generation Antivirus powered by Sentinel One is associated with which feature of SonicWall?**

- A. Threat Intelligence**
- B. Endpoint Protection**
- C. Email Security**
- D. Network Monitoring**

**10. Which of the following is NOT a method for exporting a packet capture?**

- A. PCapNG**
- B. JSON**
- C. HTML**
- D. Text**

## **Answers**

SAMPLE

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

SAMPLE

## **Explanations**

SAMPLE

## 1. Which best practices should be implemented before updating the firmware on SonicWall devices?

- A. Create a backup and Download a settings file locally**
- B. Update all licenses and Restart the device**
- C. Reconfigure all settings and Check for compatibility**
- D. Notify users and Log changes**

Creating a backup and downloading a settings file locally before updating the firmware on SonicWall devices is crucial for several reasons. Firstly, having a backup ensures that you can restore the device to its previous configuration if the update leads to unexpected issues or if there is a failure during the update process. This step minimizes the risk of data loss or downtime, which can be critical for network stability and security.

Downloading a settings file locally provides an additional layer of security, as it allows administrators to maintain an offline copy of the configuration that can be quickly restored if necessary. This practice is particularly important because firmware updates can sometimes reset settings or lead to configuration changes that may not be immediately apparent. This proactive approach contributes significantly to operational resilience, allowing administrators to manage updates confidently while ensuring that recovery options are readily available.

## 2. What is split horizon in relation to RIP?

- A. It sends learned routes to all adjacent routers**
- B. It allows the use of multiple routing protocols simultaneously**
- C. It suppresses learned routes in updates to prevent routing loops**
- D. It enhances bandwidth by reducing unnecessary updates**

In the context of the Routing Information Protocol (RIP), split horizon is a technique used to prevent routing loops, which are problematic in distance-vector routing protocols. When a router learns about a route from one of its neighbors, split horizon prohibits the router from sending that same route information back to the neighbor from which it was learned. This mechanism helps to ensure that incorrect routing information does not circulate indefinitely, which can lead to loops and ultimately degrade network performance. By implementing split horizon, each router can build a more accurate topology and routing table, reducing the chances of routing information becoming stale or causing the network to become unstable. This method is crucial for maintaining efficient and reliable routing within a network that employs RIP, contributing to overall stability and efficiency. The other options describe different aspects of routing behavior or features that do not directly pertain to the concept of split horizon. For example, sending learned routes to all adjacent routers would lead to potential routing loops rather than preventing them. The simultaneous use of multiple routing protocols is a separate topic altogether, and enhancing bandwidth through reduced updates refers more to overall optimization strategies rather than the specific mechanism of split horizon.

### 3. What is a primary function of the Neighbor Discovery protocol?

- A. It provides network address translation**
- B. It helps discover other devices on the local network**
- C. It establishes VPN connections**
- D. It manages firewall traffic**

The primary function of the Neighbor Discovery protocol is to help discover other devices on the local network. This protocol facilitates the communication and interaction among devices within a local area network (LAN) by enabling devices to identify each other, determine their link-layer addresses, and maintain reachability information. Essentially, it allows devices to find out about their neighbors in the network, which is crucial for IPv6 operations as it replaces the Address Resolution Protocol (ARP) used in IPv4. Neighbor Discovery is important for several reasons, such as allowing devices to efficiently communicate without manual configuration of each device and supporting functions like router discovery, address autoconfiguration, and maintaining a list of reachable neighbors. This native ability to discover neighboring devices enhances the overall functionality and connectivity within a network. The other options listed do not directly relate to the responsibilities of the Neighbor Discovery protocol, focusing instead on different aspects of networking such as address translation, VPN setup, and traffic management.

### 4. True or False: The firewall can perform a rolling analysis of event logs for web site access and bandwidth use.

- A. True**
- B. False**
- C. Only under specific conditions**
- D. Requires a separate license**

The statement is true because firewalls, particularly those like SonicWall, have advanced logging and analysis features. They are capable of monitoring and analyzing event logs related to website access and bandwidth usage. This functionality allows network administrators to gain insights into user behavior, identify traffic patterns, and detect potential security threats. The rolling analysis capability means that the firewall can continuously review and process these logs in real-time or near-real-time, providing ongoing visibility into network activity. This feature is invaluable for maintaining security posture, optimizing bandwidth utilization, and ensuring compliance with organizational policies. The other options, while they might seem plausible, do not fully capture the broad capabilities of modern firewalls regarding log analysis. Some may suggest limitations or specific conditions that are not inherent to the general functionality of the firewalls discussed.

**5. True or False: Static Routes by default take precedence over VPN traffic.**

- A. True**
- B. False**
- C. Depends on the configuration**
- D. Only for specific types of traffic**

Static routes are used to define a fixed path that network traffic should follow to reach a destination. By default, static routes take precedence over dynamic routing protocols and VPN traffic because they provide a direct and defined route to the destination. This means that if a static route is configured for a specific destination, any traffic directed towards that destination will utilize the static route instead of being routed over a VPN, unless specifically configured otherwise. This precedence is integral for network efficiency and control, ensuring that important or critical traffic follows the intended path as defined by the network administrator. In scenarios where there might be both static routes and VPN configurations, the existence of a static route that matches the traffic's destination ensures that the traffic will not be encapsulated in a VPN tunnel unless the administrator has set up exceptions or overrides in the routing configuration. Thus, the statement that static routes by default take precedence over VPN traffic is accurate.

**6. What sorts of data does the App Flow Monitor specifically track?**

- A. Only firewall breach attempts**
- B. Incoming and outgoing data packets**
- C. Administrative login attempts**
- D. SonicWall configuration changes**

The App Flow Monitor is designed to track incoming and outgoing data packets associated with applications traversing the network. This tool provides valuable insights into application performance, bandwidth consumption, user behavior, and overall network traffic patterns. By monitoring data packets, the App Flow Monitor can help identify issues such as bandwidth hogs or applications that may be misconfigured or generating excessive traffic. The other options involve specific categories of data that the App Flow Monitor is not specifically intended to track, making the focus on data packets particularly relevant. For instance, while firewall breach attempts and administrative login attempts pertain to security monitoring, those would typically be managed by a different set of tools aimed at intrusion detection or access control auditing. Configuration changes are important for device management but again fall outside the scope of what the App Flow Monitor is set up to analyze. Therefore, the ability to monitor incoming and outgoing data packets is the core function of the App Flow Monitor, making it the correct choice.

## 7. What is a method to replicate settings or configurations across tenants?

- A. Templates**
- B. Custom scripts**
- C. Manual configuration**
- D. Policy export**

Using templates is an efficient method to replicate settings or configurations across tenants. Templates allow administrators to define a standard set of configurations that can be easily applied to multiple tenants, ensuring consistency and reducing the potential for errors that may arise from manual input. This approach streamlines the process of managing multiple tenants, particularly in environments where similar configurations are required. Templates can encapsulate a wide range of settings, including network configurations, security policies, and user permissions. Once a template is created, it can be cloned or applied to other tenants, which not only saves time but also ensures that updates to the template can be propagated across all tenants that utilize it. Other methods, such as custom scripts and policy export, may also be viable approaches, but they require a greater level of technical expertise and may not guarantee the same level of ease in ensuring uniformity across tenants. Manual configuration is typically the least efficient method, as it is prone to human error and significantly more time-consuming compared to the use of templates.

## 8. How many web proxy servers can be configured on a SonicWall?

- A. 16**
- B. 32**
- C. 64**
- D. 128**

The correct answer is 32, reflecting SonicWall's capability to manage multiple web proxy servers efficiently. This function is crucial for organizations that need to optimize traffic management, load balancing, and enhanced security for web traffic. By supporting 32 web proxy servers, SonicWall enables improved performance and redundancy, allowing for a scalable architecture that can cater to a variety of network demands. This design is particularly beneficial for environments where bandwidth might be limited, or where there's a high volume of simultaneous connections to the internet, as it can distribute traffic loads effectively across the available proxy servers. Furthermore, employing multiple proxy servers can enhance privacy and security by allowing for segmented traffic management and providing additional layers of content filtering and inspection. Each of the other numbers of proxy servers listed in the options would exceed the designed capacity, making them unfeasible within the SonicWall operating framework. This capacity understanding is essential for network administrators to configure the systems optimally and ensure reliable network performance.

**9. Next Generation Antivirus powered by Sentinel One is associated with which feature of SonicWall?**

- A. Threat Intelligence**
- B. Endpoint Protection**
- C. Email Security**
- D. Network Monitoring**

Next Generation Antivirus powered by Sentinel One directly relates to the feature of Endpoint Protection within SonicWall's suite of security offerings. This feature is designed to provide advanced protection against a wide array of threats that target end-user devices, such as laptops and desktops. Endpoint Protection employs sophisticated algorithms and machine learning techniques to identify and mitigate potential threats before they can cause harm to the device or the network. By leveraging Sentinel One's technology, SonicWall enhances its capability to detect and respond to malware, ransomware, and other endpoint-based attacks effectively. This focus on safeguarding endpoints is critical, as these devices are often the most vulnerable to cyber threats and can serve as entry points for attacks on broader network infrastructure. By ensuring robust Endpoint Protection, SonicWall helps organizations maintain a secure environment, manage risks, and adhere to security best practices. Other options like Threat Intelligence could complement the security strategy, but they do not directly pertain to the advanced antivirus features provided by Sentinel One. Email Security and Network Monitoring are important aspects of a comprehensive security framework, but they focus on different areas of vulnerability compared to the specific protection offered through effective endpoint solutions.

**10. Which of the following is NOT a method for exporting a packet capture?**

- A. PCapNG**
- B. JSON**
- C. HTML**
- D. Text**

In the context of exporting packet captures, the correct answer is based on the common formats used in packet analysis. PCapNG is a well-known format specifically designed for network packet captures, allowing for detailed information storage. HTML can be utilized to present captured data in a web browser, while Text format allows the export of raw data in a readable form. However, JSON, while a widely used format in data interchange, is not typically associated with exporting packet captures from network analysis tools. It is primarily designed for structuring data in a way that is easy for machines to parse and generate, especially in web applications. Thus, it is not a standard export format for packet captures, making it the correct response to the question.

# 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](mailto:hello@examzify.com).**

**Or visit your dedicated course page for more study tools and resources:**

**<https://sonicwallnetworksecurityadministrator.examzify.com>**

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

**SAMPLE**