NSE7 ENTERPRISE FIREWALL PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nse7enterprisefirewall.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. What session flag signifies that the traffic will be checked by an IPS signature?

A. ndr

B. nds

C. npu

D. log

2. Which command summarizes the FortiGuard configuration?

A. diagnose system status

B. diagnose autoupdate status

C. get fortiguard config

D. show autoupdate summary

3. Which command displays the current statistics on a HA pair?

A. get router info ospf database brief

B. diagnose sys ha status

C. diagnose sys ha dump-by vlcuster

D. get router info ospf interface

4. Which command would provide current statistics about OSPF in the FortiGate?

A. get router info ospf status

B. diagnose sys ha status

C. get router info ospf interface

D. get router info ospf database brief

5. What is the function of the command 'diagnose test application ipsmonitor 1'?

A. It displays the IPS engine information

B. It toggles the IPS engine enable/disable status

C. It restarts all IP engines

D. It configures IPS monitoring parameters

SAMPLE

6. Which protocol is characterized by having no state, as indicated by its protocol state?

A. TCP

B. ICMP

C. UDP

D. SCTP

7. What protocol and port does ESP traffic primarily use?

A. TCP protocol 53

B. IP protocol 50

C. UDP protocol 80

D. HTTP protocol 443

8. What must be true for FortiGate to add a static route to the routing table?

A. The outgoing interface is down

B. Another route exists for the same destination

C. The link health monitor is configured

D. The outgoing interface is up

9. Which command displays the processes with the highest resource usage?

A. diagnose sys high-usage

B. diagnose sys processes

C. diagnose sys top

D. diagnose sys active

10. What ports does IKE traffic primarily use?

A. TCP 80 and 443

B. UDP 500 and UDP 4500

C. UDP 9999 and TCP 22

D. TCP 23 and 53

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What session flag signifies that the traffic will be checked by an IPS signature?

A. ndr

B. nds

C. npu

D. log

The session flag "ndr" indicates that the traffic will be checked by an Intrusion Prevention System (IPS) signature. When this flag is set, it tells the firewall that the corresponding session should undergo inspection for any potentially malicious activity, utilizing the IPS capabilities to analyze the traffic against its defined signatures and rules. This proactive measure helps in identifying and mitigating threats in real time, ensuring that only legitimate traffic is allowed while potentially harmful traffic is blocked. The other options do not specifically relate to the IPS signature checking process. For instance, "nds" typically indicates that a session has been identified but does not explicitly relate to IPS checks. "npu" is likely indicative of sessions that utilize certain processing units but is unrelated to the IPS functionality. Lastly, "log" is associated with logging traffic for audit or monitoring purposes rather than actively checking traffic against IPS signatures. Thus, "ndr" is the definitive flag that signifies IPS inspection of the traffic, marking it as critical for threat management.

2. Which command summarizes the FortiGuard configuration?

A. diagnose system status

B. diagnose autoupdate status

C. get fortiguard config

D. show autoupdate summary

The command that summarizes the FortiGuard configuration is significant because it provides real-time information regarding the status of automatic updates for FortiGuard services. This service is crucial for the operation of a Fortinet device, as it enables features like antivirus, IPS, web filtering, and more by ensuring the device is up-to-date with the latest security definitions and data. When using the command to diagnose autoupdate status, you can view details such as the last update time, the current status of the update process, and any errors that may have occurred during recent updates. This visibility is important for troubleshooting and maintaining the effectiveness of security measures applied through FortiGuard services. In contrast, other options either provide generic system status information, details about the autoupdate process, or simply display configuration details but not specifically focused on the FortiGuard configuration. Thus, the correct command specifically caters to giving detailed insight into how the FortiGuard services are configured and functioning, making it the most relevant choice for summarizing FortiGuard configuration.

SAMPLE

3. Which command displays the current statistics on a HA pair?

A. get router info ospf database brief

B. diagnose sys ha status

C. diagnose sys ha dump-by vlcuster

D. get router info ospf interface

The command that displays the current statistics on a High Availability (HA) pair is "diagnose sys ha status." This command provides detailed information about the HA configuration, including the roles of the devices in the pair, their operational status, synchronization information, and other relevant statistics that help administrators monitor the health and performance of the HA setup. Using this command is crucial in a maintenance or troubleshooting scenario because it aids in understanding how well the HA devices are functioning together and if there are any issues that need to be addressed. Information obtained from this command can help in assessing whether the primary and secondary devices are synchronized, which is a critical aspect of ensuring high availability. The other commands focus on different aspects of the network: - The command that retrieves OSPF database information provides insight into OSPF routing information, which is unrelated to the HA status. - A command that dumps HA information by cluster also provides HA information but may not summarize the current operational state as directly as the "diagnose sys ha status." - The command that displays OSPF interface information is more geared towards understanding the status of OSPF-enabled interfaces rather than HA settings. Therefore, "diagnose sys ha status" is specifically designed for reviewing the current HA statistics, making it

4. Which command would provide current statistics about OSPF in the FortiGate?

A. get router info ospf status

B. diagnose sys ha status

C. get router info ospf interface

D. get router info ospf database brief

The command that provides current statistics about OSPF (Open Shortest Path First) in the FortiGate is the one that queries the OSPF status directly. This command gives you a broad overview of OSPF, including information such as the OSPF router ID, the OSPF state, and various metrics that help in monitoring the OSPF process. By using this command, network administrators can assess the overall health and performance of their OSPF configuration, making it a vital tool in troubleshooting and optimizing OSPF implementations. The OSPF status information is essential for understanding not just how well the OSPF protocol is functioning, but also how efficiently data is being routed through the network. Other commands listed serve different purposes: one checks HA status, which is unrelated to OSPF statistics, while another focuses specifically on OSPF interface details rather than the overall OSPF process. The command that retrieves OSPF database information, while insightful, does not communicate the real-time status or performance metrics of the OSPF process itself. Therefore, querying the status directly provides the necessary insights for effective OSPF management.

SAMPLE

5. What is the function of the command 'diagnose test application ipsmonitor 1'?

A. It displays the IPS engine information

B. It toggles the IPS engine enable/disable status

C. It restarts all IP engines

D. It configures IPS monitoring parameters

The command 'diagnose test application ipsmonitor 1' is specifically designed to provide information about the Intrusion Prevention System (IPS) engine. When executed, it retrieves and displays the operational state and statistics associated with the IPS engine, allowing network administrators to monitor its performance and health. This includes information such as enabled features, statistics on detected threats, and the effectiveness of the IPS in real-time threat mitigation. In a practical scenario, being able to access this detailed engine information is crucial for diagnosing issues, optimizing performance, and ensuring the overall security posture of the network is being effectively upheld. Understanding the operational metrics through this command helps administrators determine if any adjustments or troubleshooting steps are needed for the IPS deployment. The other choices, while related to IPS functionality, do not accurately describe the specific outcome of the command in question.

6. Which protocol is characterized by having no state, as indicated by its protocol state?

A. TCP

B. ICMP

C. UDP

D. SCTP

The correct answer is ICMP, which stands for Internet Control Message Protocol. ICMP is characterized by being a stateless protocol, primarily used for sending control messages and error messages in network communications, rather than for establishing connections or maintaining sessions. Unlike stateful protocols, ICMP does not maintain context about the communication state between sender and receiver, which makes it inherently stateless. This means that each ICMP message is independent, and the protocol does not keep track of whether a message was sent or received. For example, when a host sends an ICMP Echo Request, it does not expect to memorably track the state or history of that request. As a result, ICMP is utilized primarily for diagnostic purposes, such as pinging devices to check for their availability on a network. In contrast, other protocols listed, such as TCP and SCTP, are stateful because they establish connections and maintain state for the duration of those connections, keeping track of the session information. UDP, while also a connectionless protocol like ICMP, is still considered stateful in TCP/IP communication context due to its relationship to sessions. However, ICMP uniquely fulfills its role without maintaining any state information, focusing solely on sending error reports and other network status messages

SAMPLE

7. What protocol and port does ESP traffic primarily use?

A. TCP protocol 53

B. IP protocol 50

C. UDP protocol 80

D. HTTP protocol 443

ESP, which stands for Encapsulating Security Payload, is a protocol used in the context of IPsec (Internet Protocol Security) to provide confidentiality, integrity, and authentication to IP packets. It primarily operates on a specific protocol number rather than within the framework of typical transport layer protocols like TCP or UDP. The correct answer highlights that ESP traffic primarily uses IP protocol number 50. This protocol is part of the IP layer, directly communicating with IP and is not dependent on a port number as seen in TCP and UDP communications. This means ESP traffic is not referenced or routed through ports such as those specified in alternative options, like TCP port 53 or HTTP port 443. Understanding this distinction is crucial for firewall configurations, network security management, and troubleshooting, where knowing how IPsec operates—including the role of ESP—can significantly impact the effective implementation of secure communications.

8. What must be true for FortiGate to add a static route to the routing table?

A. The outgoing interface is down

B. Another route exists for the same destination

C. The link health monitor is configured

D. The outgoing interface is up

For FortiGate to successfully add a static route to the routing table, it is essential that the outgoing interface is up. This means that the interface designated for forwarding traffic must be operational and able to send and receive packets. If the outgoing interface is down, the device cannot use this route for traffic, making it impossible to add to the routing table since it would be ineffective for network communication. This requirement highlights the importance of interface status in routing decisions. A static route without an active outgoing interface cannot function properly, as there will be no path for the traffic to travel through. Thus, having the outgoing interface up ensures that the routing entry is valid and can be utilized for directing packets to the respective destination.

9. Which command displays the processes with the highest resource usage?

A. diagnose sys high-usage

B. diagnose sys processes

C. diagnose sys top

D. diagnose sys active

The command that displays the processes with the highest resource usage is 'diagnose sys top'. This command provides a real-time overview of active processes, sorted by their resource consumption, allowing you to quickly identify which processes are using the most CPU and memory. This is particularly useful for troubleshooting performance issues, as it enables administrators to monitor the impact of various processes on system resources continuously. By using this command, users are presented with a similar interface to the top command found in other operating systems, allowing for easy interpretation of resource usage statistics. This clarity and accessibility make it an effective tool for managing system performance. Other commands might provide useful information about system processes or general statistics, but they do not focus exclusively on the highest resource consumers in a way that 'diagnose sys top' does. This specialized information is crucial for efficient troubleshooting and performance optimization on Fortinet devices.

SAMPLE

10. What ports does IKE traffic primarily use?

A. TCP 80 and 443

B. UDP 500 and UDP 4500

C. UDP 9999 and TCP 22

D. TCP 23 and 53

IKE (Internet Key Exchange) is an essential component of establishing secure communication through VPNs. It is primarily responsible for setting up the security associations and exchanging keys, which are vital for initiating a Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) tunnel. The primary ports used by IKE traffic are UDP 500 and UDP 4500. UDP 500 is specifically used for IKE phase 1, where the initial negotiation and establishment of the security parameters take place. Once the IKE negotiation is complete, and if NAT (Network Address Translation) is involved, UDP 4500 may also be used for encapsulating IKE packets to ensure they can traverse NAT devices without issues. This utilization of UDP is crucial since it is a connectionless protocol, which is ideal for the quick exchanges required for session setup, unlike TCP that requires a connection establishment handshake. Thus, understanding the specific ports used by IKE is important for configuring firewalls and ensuring proper traffic can flow for successful VPN establishment.

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://nse7enterprisefirewall.examzify.com

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

SAMPLE