NSE7 Enterprise Firewall Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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

1. **Which TCP protocol state is associated with an established connection?**

   A. Proto_state=02

   B. Proto_state=04

   C. Proto_state=01

   D. Proto_state=03

2. **What command set is used to enable/disable longer than screen outputs?**

   A. config system console

   B. config output settings

   C. diagnose output console

   D. set output display options

3. **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

4. **Which command shows the details of the prefix advertised by a neighbor?**

   A. get router info bgp neighbors xx.xx.xx.xx advertise

   B. get bgp neighbor info

   C. show neighbor prefixes

   D. display prefix details

5. **What command would you use to list OSPF adjacency information?**

   A. get router info bgp neighbors

   B. get router info ospf database router lsa

   C. config system fortiguard

   D. diagnose ip router ospf all enable

6. What is the TCP state associated with closing a connection waiting for an acknowledgment?

A. LAST_ACK

B. CLOSE_WAIT

C. FIN_WAIT

D. TIME_WAIT

7. Which command displays current IPsec SA information for active tunnels?

A. diagnose vpn tunnel list

B. show ipsec tunnels

C. get sa information

D. display active sa

8. What command lists the LSAs originated on the local FortiGate?

A. get router info ospf database self-originate

B. execute ha manage <HA_unit_index> <Admin_Username>

C. diagnose sys ha status

D. get router info ospf neighbor

9. What debug flow blocking message indicates a packet was dropped due to exceeding traffic shaping policy?

A. Traffic shaping policy error

B. Exceeded shaper limit, drop

C. Packet limit reached

D. Shaping policy violation

10. What is the process name used for FortiGuard updates?

A. scanunitd

B. wad

C. iked

D. updated

Answers

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

Explanations

1. Which TCP protocol state is associated with an established connection?

A. Proto_state=02

B. Proto_state=04

C. Proto_state=01

D. Proto_state=03

An established connection in TCP is represented by a specific protocol state that indicates a successful three-way handshake has occurred, allowing for data transmission between the two endpoints. In the context of TCP, each state corresponds to a part of the connection lifecycle. The associated state for an established TCP connection is characterized by the system being in a state where packets can be sent and received between the communicating devices. When considering the protocol states, the value corresponding to an established connection is indicative of the 'ESTABLISHED' state in the TCP connection management process. Therefore, the designation "Proto_state=01" aligns with this established state, confirming that there is an active communication link. This state allows both sides to send and receive data freely, which is fundamental for reliable communication in TCP. Recognizing the correct state helps in understanding the behavior of TCP connections and their management in networking.

2. What command set is used to enable/disable longer than screen outputs?

A. config system console

B. config output settings

C. diagnose output console

D. set output display options

The command set used to enable or disable longer than screen outputs in the Fortinet command line interface is associated with configuring the system console settings. By using the command that relates to 'config system console,' you can adjust how output is displayed in the console, including whether or not outputs longer than the screen will be truncated or allow scrolling. This capability is particularly useful during debugging or monitoring sessions, as it ensures that users can view all necessary information without losing any output due to screen limitations. Adjusting these console settings can enhance the user experience by providing greater control over output visibility and making it easier to manage longer outputs.

3. 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.

4. Which command shows the details of the prefix advertised by a neighbor?

A. get router info bgp neighbors xx.xx.xx.xx advertise

B. get bgp neighbor info

C. show neighbor prefixes

D. display prefix details

The command that shows the details of the prefix advertised by a neighbor is indeed the command to retrieve specific information about BGP neighbors and their advertised prefixes. This command provides valuable insights into the routing information shared between BGP peers. When you use the command that specifies the neighbor's IP address along with the "advertise" argument, you are effectively asking the router to display the prefixes that this particular neighbor has advertised to it. This is crucial for network operators who need to understand which routes are being received from their BGP peers and to diagnose routing issues. The other options do not specifically target the advertised prefixes from a neighbor in such a direct manner. Instead, they may provide more general information or not include the necessary detail about specific prefixes, which makes the correct command the most effective choice for this inquiry.

5. What command would you use to list OSPF adjacency information?

A. get router info bgp neighbors

B. get router info ospf database router lsa

C. config system fortiguard

D. diagnose ip router ospf all enable

The correct command to list OSPF adjacency information is particularly focused on retrieving the OSPF protocol data directly relating to router link-state advertisements. The command retrieves information about the OSPF router link-state advertisement (LSA) database, which contains details regarding the OSPF topology, including neighboring routers' states and their link information. When examining the OSPF process, understanding the link-state database is crucial because it allows you to analyze and confirm existing OSPF adjacencies or the state of the OSPF network. By detailing router LSAs, this command provides insights into both the OSPF neighbors and their statuses, thereby confirming adjacency setups. In contrast, the command that relates to BGP neighbors focuses on the Border Gateway Protocol (not OSPF), thus making it irrelevant for OSPF adjacency checks. The command to configure Fortiguard is entirely unrelated to OSPF functionality. Lastly, while the diagnostic command provided does pertain to OSPF, it is aimed more at enabling additional diagnostic features rather than directly listing the adjacency information that you would find in the OSPF LSA database. This specificity in data retrieval is what identifies the correct command for the task at hand.

6. What is the TCP state associated with closing a connection waiting for an acknowledgment?

A. LAST_ACK

B. CLOSE_WAIT

C. FIN_WAIT

D. TIME_WAIT

The TCP state associated with closing a connection while waiting for an acknowledgment is LAST_ACK. In this state, the connection has already sent a final acknowledgment indicating that it is ready to close, and it is now waiting for the acknowledgment of that final segment from the other side before fully terminating the connection. When a connection is in LAST_ACK, it means the endpoint has transmitted a FIN segment and is essentially waiting for the peer to acknowledge that FIN. This state is important because it ensures that both sides of the connection have a clear agreement on closing the session, preventing any loss of data that could occur if one side were to terminate the connection prematurely. Understanding the nuances of the TCP connection states, especially in the context of closing mechanisms, helps ensure robust and reliable network communication. Other states, such as CLOSE_WAIT, FIN_WAIT, and TIME_WAIT, serve different roles in the TCP connection lifecycle, dealing with aspects like waiting for the application to close the connection, actively waiting for a remote connection closure, and ensuring that all data has been properly transmitted and received before fully closing, respectively. However, LAST_ACK specifically encapsulates the idea of waiting for acknowledgment as part of the closing process.

7. Which command displays current IPsec SA information for active tunnels?

A. diagnose vpn tunnel list

B. show ipsec tunnels

C. get sa information

D. display active sa

The command that displays current IPsec Security Association (SA) information for active tunnels is "diagnose vpn tunnel list." This command is specifically designed to provide detailed information regarding the established VPN tunnels, including their status and configuration. When executed, it reveals active tunnels, their encryption and integrity settings, and can indicate issues or statuses related to those tunnels. The focused utility of this command in managing and troubleshooting IPsec tunnels makes it an essential tool for administrators. It helps to ascertain whether the tunnels are up and running as expected, providing vital information that can assist in monitoring and ensuring the reliability of VPN connections.

8. What command lists the LSAs originated on the local FortiGate?

A. get router info ospf database self-originate

B. execute ha manage <HA_unit_index> <Admin_Username>

C. diagnose sys ha status

D. get router info ospf neighbor

The command that lists the Link State Advertisements (LSAs) originated on the local FortiGate is "get router info ospf database self-originate." This command provides a focused view of the LSAs that the FortiGate device itself has generated and is advertising to other OSPF neighbors. When using this command, network administrators can quickly verify what information the local device has shared about its own routing capabilities, which is critical for troubleshooting OSPF-related issues and ensuring proper route dissemination within an OSPF domain. It helps in confirming that the device is correctly representing its routes to other routers in the network. The other options pertain to different functionalities that do not directly provide the list of locally originated LSAs. For instance, managing a high-availability unit or checking neighbor relationships with OSPF does not give insight into the LSAs that the device originated. Therefore, the correct choice stands out as the most relevant command for the task.

9. What debug flow blocking message indicates a packet was dropped due to exceeding traffic shaping policy?

A. Traffic shaping policy error

B. Exceeded shaper limit, drop

C. Packet limit reached

D. Shaping policy violation

The debug flow blocking message that indicates a packet was dropped due to exceeding traffic shaping policy is "Exceeded shaper limit, drop." This message specifically indicates that the traffic shaping policy in place has defined a maximum bandwidth or packet rate that was surpassed, leading the firewall to drop the excess packets to adhere to the defined limits. This behavior is a critical element of traffic management, designed to ensure that network resources are used efficiently and to prevent any single type of traffic from consuming all available bandwidth. Recognizing this message can help network administrators troubleshoot and fine-tune their traffic shaping policies, ensuring optimal performance and compliance with organizational traffic management strategies. The other options do not accurately capture the specific reasoning behind the dropped packet in relation to traffic shaping policy limits. While they may suggest that there was some form of limitation or violation, they do not explicitly state that the packet was dropped due to exceeding the specified shaper limits, which is the key aspect of identifying the issue.

10. What is the process name used for FortiGuard updates?

A. scanunitd

B. wad

C. iked

D. updated

The process responsible for FortiGuard updates is known as "updated." This process is crucial for maintaining the security and effectiveness of FortiGate devices, as it is responsible for automatically downloading and applying the latest threat intelligence and product updates provided by FortiGuard. Regular updates are essential to protect the network against emerging threats and ensure optimal performance of security features. The other processes mentioned have distinct roles; for instance, "scanunitd" is involved in handling antivirus scanning operations, "wad" is related to the web filter's operations, and "iked" is responsible for handling Internet Key Exchange (IKE) for VPN connections. Each of these processes contributes to the overall functionality of FortiGate devices, but none specifically pertains to the task of updating FortiGuard services.

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!