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

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

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

1. What is the correct proto_state value for the CLOSE_WAIT state?

A. Proto_state=01

B. Proto_state=06

C. Proto_state=02

D. Proto_state=07

2. Which command is used to restart a BGP session between two peers?

A. execute router clear bgp ?

B. diagnose debug enable

C. config system fortiguard

D. diagnose webfilter fortiguard statistic list

3. What is contained in Type 3 LSA Summary Link Advertisements?

A. Specific router configurations

B. Detailed error statistics

C. Summarized link state information

D. Real-time performance data

4. What command lists options for testing the IPS monitor?

A. diagnose test application ipsmonitor ?

B. show ips test options

C. get ips monitor configuration

D. display ips test details

5. In FortiGate's route selection process, which is considered first?

A. Lowest metric

B. Lowest distance

C. Most specific route

D. Lowest priority

6. Which command provides information on the current status of BGP neighbors?

A. get router info bgp neighbors

B. show bgp neighbor status

C. get bgp neighbor info

D. display neighbor status

7. What does the process name 'hasync' relate to?

A. File synchronization

B. HA protocol

C. URL filtering

D. Traffic analysis

8. What is the state representation for UDP traffic in both directions?

A. proto_state=00

B. proto_state=01

C. proto_state=10

D. proto_state=11

9. What command displays FQDN and IP addresses of FortiGuard antivirus and IPS update servers?

A. diagnose test application dnsproxy 7

B. diagnose fortiguard update servers

C. show ip fortiguard

D. get fortiguard server info

10. What is the command to set the output method for screen outputs?

A. set output {standard | more}

B. set output {default | extended}

C. set console output {normal | verbose}

D. config system console outputs

Answers

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

Explanations

1. What is the correct proto_state value for the CLOSE_WAIT state?

A. Proto_state=01

B. Proto_state=06

C. Proto_state=02

D. Proto_state=07

The CLOSE_WAIT state is an important part of the TCP connection lifecycle, indicating that the local end of the connection has received a connection termination request from the remote side (a FIN segment) but has not yet sent its own FIN to confirm the closure of the connection. In the context of proto_state values, each state in the TCP connection lifecycle is assigned a specific numerical code. The value associated with the CLOSE_WAIT state is 06. This numerical representation helps in identifying and managing TCP states programmatically within firewall and networking software. Understanding the role of the CLOSE_WAIT state clarifies why the proto_state value of 06 is the correct answer; it accurately represents the state in which the local application is still processing the connection and has yet to fully close it. This distinguishes it from the other states, each of which corresponds to different stages in the life of a TCP connection.

2. Which command is used to restart a BGP session between two peers?

A. execute router clear bgp ?

B. diagnose debug enable

C. config system fortiguard

D. diagnose webfilter fortiguard statistic list

The command to restart a BGP session between two peers is "execute router clear bgp ?". This command is specifically designed for managing the Border Gateway Protocol (BGP) sessions. When you run this command, it allows the user to clear specific BGP sessions or all BGP sessions, which effectively restarts them and can help in resolving issues such as session hangs or route updates not propagating as expected. The BGP protocol relies on maintaining a stable connection between peers for route exchange, and clearing the session can force a fresh connection, helping to re-establish the communication necessary for routing information. This command can be used in various contexts, whether to clear a specific BGP peer or all peers connected to the router, making it a versatile tool for network administrators dealing with BGP configurations. The other options listed do not pertain to managing BGP sessions. For instance, commands related to debug or Fortiguard services are unrelated to BGP session management, making them unsuitable for restarting BGP peer connections. This specificity in purpose and functionality is what establishes the chosen command as the correct answer.

3. What is contained in Type 3 LSA Summary Link Advertisements?

A. Specific router configurations

B. Detailed error statistics

C. Summarized link state information

D. Real-time performance data

Type 3 LSA, or Summary Link Advertisements, play a crucial role in OSPF (Open Shortest Path First) routing protocol. These LSAs are used to summarize routes that exist within an area and are then advertised to other areas. By containing summarized link state information, Type 3 LSAs enable routers in different areas to learn about networks without requiring them to know all the detailed route information within that area. This summarization helps reduce the amount of routing information that needs to be processed and communicated, thus optimizing network performance and efficiency. Type 3 LSAs are especially beneficial in large-scale OSPF networks, as they assist in minimizing the size of routing tables and reducing the overall complexity of the routing domain. Instead of every router in the area sharing all its routing details, Type 3 LSAs allow for more concise communication between areas, ensuring that routers can still make informed routing decisions based on summarized information.

4. What command lists options for testing the IPS monitor?

A. diagnose test application ipsmonitor ?

B. show ips test options

C. get ips monitor configuration

D. display ips test details

The command that lists options for testing the IPS monitor is "diagnose test application ipsmonitor ?". This command is specifically designed to provide a way to interactively see the various options available for testing the IPS (Intrusion Prevention System) monitor. When executed, the question mark at the end serves as a wildcard, prompting the system to return a list of possible parameters or actions that can be taken within the context of the IPS monitor testing. This is a common syntax in command-line interfaces, allowing administrators to quickly understand what commands or options are available without needing to refer to external documentation. Understanding how to use this syntax is critical for effective management and troubleshooting within a Fortinet environment, as it helps users to navigate the various commands and functionalities offered by the IPS system. Having access to testing options is essential for ensuring that the IPS is adequately configured and operational, thus protecting the network from potential threats.

5. In FortiGate's route selection process, which is considered first?

A. Lowest metric

B. Lowest distance

C. Most specific route

D. Lowest priority

In the FortiGate route selection process, the most specific route is indeed the first criterion considered during routing decisions. This principle stems from the idea that a more specific route, typically defined by a longer subnet mask, has precedence over less specific routes. For example, if there are routes for both 192.168.1.0/24 and 192.168.0.0/16, the route for 192.168.1.0/24 is more specific and will be selected for traffic destined to that subnet. Focusing on the specifics allows for more precise routing control and effective handling of network traffic, ensuring that data packets are routed efficiently based on detailed criteria rather than more general route definitions. Thus, when multiple possible routes exist for a destination, the system prioritizes the one that can narrow down the possibilities more accurately. Other factors like metric, distance, and priority may come into play subsequently, but the initial step emphasizes the specificity of the route, making it the critical factor in selecting the appropriate path for traffic within FortiGate's routing architecture.

6. Which command provides information on the current status of BGP neighbors?

A. get router info bgp neighbors

B. show bgp neighbor status

C. get bgp neighbor info

D. display neighbor status

The command that provides information on the current status of BGP neighbors is indeed "get router info bgp neighbors." This command is specific to Fortinet devices running FortiOS and allows administrators to retrieve detailed information about the status and characteristics of each BGP neighbor directly from the command line interface. Using this command, you can check aspects such as the current state of the BGP session (whether it's established or down), the number of prefixes received from the neighbor, and other important parameters. This is crucial for troubleshooting and ensuring that the BGP configuration is functioning as intended. Other commands listed may not directly correspond to the expected output for BGP neighbor statuses in Fortinet's command set. For example, "show bgp neighbor status" and "display neighbor status" are not applicable to FortiOS syntax. Meanwhile, "get bgp neighbor info" may either be an incorrect command or not yield the specific output needed for BGP neighbor status inquiry. Understanding the correct command syntax is essential for effective network management in Fortinet environments, especially when dealing with BGP configurations.

7. What does the process name 'hasync' relate to?

A. File synchronization

B. HA protocol

C. URL filtering

D. Traffic analysis

The process name 'hasync' is associated with the high availability (HA) protocol, which is used in network environments to ensure that services remain available in the event of a failure or disruption. The HA protocol facilitates the synchronization of session state and configuration information between primary and secondary devices. This allows for seamless failover, ensuring that there are no interruptions in service for users. In the context of network security devices, like next-generation firewalls, maintaining high availability is crucial for ensuring continuous protection against threats, as well as maintaining network performance. The 'hasync' process helps keep the systems in sync with the latest configuration and state information, essential for a reliable and redundant infrastructure. The other options, while related to networking and security, do not align with the 'hasync' process. File synchronization pertains to keeping files up-to-date across different locations, and URL filtering involves inspecting and controlling access to web content. Traffic analysis relates to monitoring and analyzing data flow in the network to identify patterns or issues. None of these processes specifically refer to the actions performed by 'hasync' in managing HA configurations.

8. What is the state representation for UDP traffic in both directions?

A. proto_state=00

B. proto_state=01

C. proto_state=10

D. proto_state=11

The representation for UDP traffic in both directions is indicated as proto_state=01. In network protocols, the state representation often indicates whether the traffic is considered established or not. For UDP, which is a connectionless protocol, the state representation signifies the presence of bidirectional traffic without requiring a session establishment like TCP. The "01" state specifically indicates traffic is flowing in both the incoming and outgoing directions. This is important for firewall configurations, as it allows for the proper handling of UDP packets that may not maintain a session state, yet still need to be processed for valid communication between endpoints. Understanding this state representation is crucial in configurations that rely on stateful inspection methods, particularly in environments that leverage firewalls to monitor and filter network traffic. In contrast, other state representations like "00", "10", and "11" do not apply to the condition of bidirectional UDP traffic, as these would either denote different states of traffic (like one-directional or inactive states).

9. What command displays FQDN and IP addresses of FortiGuard antivirus and IPS update servers?

A. diagnose test application dnsproxy 7

B. diagnose fortiguard update servers

C. show ip fortiguard

D. get fortiguard server info

The command that displays the Fully Qualified Domain Names (FQDN) and IP addresses of FortiGuard antivirus and IPS update servers is "diagnose test application dnsproxy 7." This command is specifically designed to query the DNS proxy service of the FortiGate device and retrieve the relevant information related to FortiGuard update servers. Using this command allows administrators to effectively test and troubleshoot DNS resolution issues that may affect the connectivity to FortiGuard services. It provides insight into how the FortiGate device is resolving the FQDNs associated with the update servers, which is crucial for ensuring that the device can receive timely updates for antivirus and IPS signatures. In the context of network security operations, establishing a reliable connection to FortiGuard servers is pivotal for maintaining updated protection against threats. The other commands listed may serve different purposes but do not provide the same specific output regarding the FQDN and IP addresses of the update servers. Therefore, utilizing this command ensures that all necessary information for managing updates is accessible.

10. What is the command to set the output method for screen outputs?

A. set output {standard | more}

B. set output {default | extended}

C. set console output {normal | verbose}

D. config system console outputs

The command to set the output method for screen outputs is correctly identified as "set output {standard | more}." This command allows you to configure how output messages are displayed on the screen when using the console interface. By using this command, you can choose between two output modes: 'standard,' which will display the information continuously on the screen, and 'more,' which provides paginated output, allowing you to view the data in stages. This is particularly useful in scenarios where large amounts of data are generated, as it helps manage screen clutter and makes it easier for users to read the output incrementally. The other options do not pertain directly to configuring screen output methods. They may be related to output configurations, but they serve different specific functions or contexts that do not align with the prompt regarding screen output methods.

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!