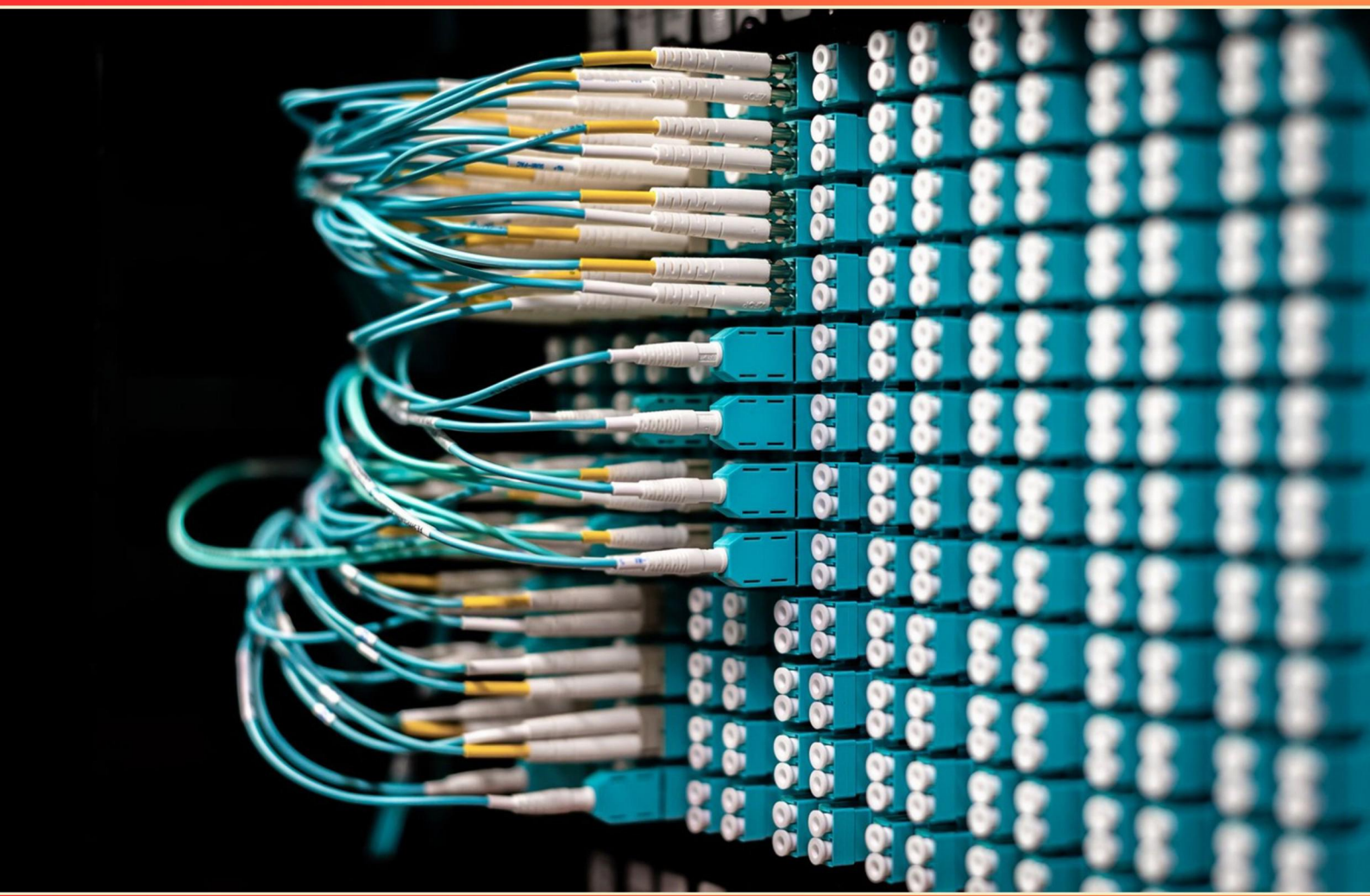
PALO ALTO NETWORKS (PANW) CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://panw-certifiednetworksecurityadministrator.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 is the primary purpose of a security profile in Palo Alto?

A. To report security incidents

B. To apply additional security measures to a security policy rule

C. To configure the network topology

D. To create user accounts for firewall access

2. What does a "Security Zone" allow a Palo Alto Networks firewall to enforce?

A. It allows encryption of all network traffic.

B. It allows segmentation of network traffic for granular security policy enforcement.

C. It simplifies user access management.

D. It enhances the speed of data transfer.

3. What is the primary purpose of a firewall in network security?

A. To encrypt outgoing network traffic

B. To control incoming and outgoing network traffic based on predetermined security rules

C. To log network activity for security analysis

D. To provide a backup for network data

4. In Palo Alto Networks firewalls, what does "User-ID Agent" do?

A. It provides user information to the firewall for controlling network access based on identity

B. It generates reports on user activities

C. It encrypts user data packets

D. It sets user priorities for network access

5. When the Content-ID engine detects a virus and the decoder action is set to "block", what happens to the client's file download?

A. The download completes successfully

B. The file download is terminated

C. The client is notified to proceed with the download

D. The firewall sends a warning email to the administrator

SAMPLE

6. What is the function of configuration logs in PANW?

A. To log user activity

B. To track changes made to the firewall configuration

C. To monitor network traffic throughput

D. To inspect incoming email attachments

7. What capability can be used when running PA-200 firewalls in HA active/passive mode using HA-Lite?

A. Session Synchronization

B. Configuration Sync

C. Shared Addressing

D. Stateful Failover

8. What does SSL Decryption enable in PAN firewalls?

A. Visibility into encrypted traffic for security inspection

B. Blocking of all encrypted traffic without inspection

C. Improved performance of non-encrypted traffic

D. Encryption of all outgoing traffic

9. Which feature of PAN firewalls refers to the capability to partition firewall resources?

A. Security Profiles

B. Network Segmentation

C. Network Virtualization

D. Traffic Filtering

10. What is the default setting for application-default security rules in Palo Alto Networks firewalls?

A. To block all unknown application traffic

B. To allow only application traffic that is known to the firewall

C. To allow all application traffic by default

D. To encrypt application traffic

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary purpose of a security profile in Palo Alto?

A. To report security incidents

B. To apply additional security measures to a security policy rule

C. To configure the network topology

D. To create user accounts for firewall access

The primary purpose of a security profile in Palo Alto is to apply additional security measures to a security policy rule. Security profiles enhance the protection offered by security policies by providing various mechanisms for threat prevention, such as antivirus, anti-spyware, vulnerability protection, URL filtering, and others. By associating a security profile with a specific security policy rule, organizations can better tailor their security posture to meet specific risks and compliance requirements. This ensures that traffic that passes through a policy rule is not only allowed or denied based on basic criteria but is also scrutinized for threats using the enhanced capabilities offered by the security profile. This layered security approach is essential for effectively managing and mitigating potential threats. The focus of security profiles on strengthening the enforcement of security policies makes them a critical component in a comprehensive security strategy.

2. What does a "Security Zone" allow a Palo Alto Networks firewall to enforce?

A. It allows encryption of all network traffic.

B. It allows segmentation of network traffic for granular security policy enforcement.

C. It simplifies user access management.

D. It enhances the speed of data transfer.

A "Security Zone" is a key concept within the Palo Alto Networks firewall architecture that enables the segmentation of network traffic. This segmentation is essential for enforcing granular security policies. By categorizing interfaces into distinct security zones, administrators can apply specific security policies tailored to the requirements of each zone. For instance, you might have a 'Trust' zone for internal network traffic that requires different security measures than a 'Guest' zone, where external users connect. These policies may include rules for allowing or denying traffic, logging activities, and applying inspection strategies. By enforcing policies based on the security zones, organizations can enhance their overall security posture and ensure that only the necessary traffic is allowed between different parts of the network. In contrast, the other options do not accurately describe the function of security zones. Encryption of network traffic pertains to securing data in transit rather than segmenting it. User access management focuses on who can connect to the network and their permissions, which is not directly related to the concept of security zones. Finally, while segmentation can impact performance, the primary purpose of security zones is not to enhance the speed of data transfer but to ensure that security policies are enforced effectively.

SAMPLE

3. What is the primary purpose of a firewall in network security?

A. To encrypt outgoing network traffic

B. To control incoming and outgoing network traffic based on predetermined security rules

C. To log network activity for security analysis

D. To provide a backup for network data

The primary purpose of a firewall in network security is to control incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between trusted and untrusted networks, making decisions on whether to allow or block specific traffic based on policies established by the network administrator. This capability is crucial for protecting internal networks from unauthorized access and securing data from external threats. By filtering packets and managing connections, firewalls help prevent malicious traffic, such as attacks or unauthorized access attempts, from infiltrating the network while also controlling what sensitive data can be sent out. This functionality is essential in maintaining the confidentiality, integrity, and availability of networked systems and data. While other options mention important functions such as encryption, logging, and backup, they do not represent the core role of a firewall. Encryption focuses on securing data in transit, logging pertains to monitoring activity for analysis, and backup deals with data preservation, none of which encapsulate the fundamental objective of a firewall within the context of network security.

4. In Palo Alto Networks firewalls, what does "User-ID Agent" do?

A. It provides user information to the firewall for controlling network access based on identity

B. It generates reports on user activities

C. It encrypts user data packets

D. It sets user priorities for network access

The User-ID Agent plays a vital role in Palo Alto Networks firewalls by facilitating user identification within the network. When users attempt to access network resources, the User-ID Agent collects and forwards user IP address and identity information to the firewall. This allows the firewall to implement policies based on user identity rather than just IP address, enhancing security control by associating network activity with specific users. By using the User-ID Agent, organizations can assign access privileges based on user roles, allowing the firewall to apply policies that better reflect the organization's security posture and compliance requirements. This mechanism is integral as it aids in enforcing user-specific policies, managing access controls, and monitoring user activities in a more granular way. The other options describe functions that are not the primary focus of the User-ID Agent. Generating reports on user activities, encrypting data packets, or setting user priorities for network access are tasks that do not align with the core function of the User-ID Agent, which is primarily concerned with providing user identity information for effective security policy application.

SAMPLE

5. When the Content-ID engine detects a virus and the decoder action is set to "block", what happens to the client's file download?

A. The download completes successfully

B. The file download is terminated

C. The client is notified to proceed with the download

D. The firewall sends a warning email to the administrator

When the Content-ID engine detects a virus and the decoder action is set to "block," the file download is terminated. This action is part of the security measures implemented by the Palo Alto Networks firewall to prevent the spread of malware and protect the network from potentially harmful files. Once the Content-ID engine identifies a file that is malicious based on predefined signatures or heuristical analysis, it intervenes by immediately stopping the transmission of the file. This ensures that the client does not receive any infected files that could compromise the security of their system or the broader network. By blocking the file download, the firewall effectively prevents the threat from entering the client's environment, thereby maintaining a secure network posture. This proactive approach is a fundamental aspect of how network security policies are enforced using Palo Alto Networks security appliances.

6. What is the function of configuration logs in PANW?

A. To log user activity

B. To track changes made to the firewall configuration

C. To monitor network traffic throughput

D. To inspect incoming email attachments

Configuration logs in Palo Alto Networks (PANW) play a crucial role in tracking changes made to the firewall configuration. These logs provide a detailed history of every modification made to the device's settings, including who made the change, what was changed, when it occurred, and the source of the change. This is vital for maintaining the integrity of the firewall and ensuring accountability, as any unauthorized or erroneous modifications can be identified and addressed promptly. The capability to review configuration logs helps organizations adhere to compliance requirements and internal policies by providing visibility into how the security posture has evolved over time. For example, if a network administrator mistakenly changes a policy that impacts security, the configuration logs allow for easy backtracking to understand what happened and when, facilitating swift corrective action. By ensuring that all changes are logged comprehensively, the firewall management can better evaluate the security implications of each change, thus supporting proactive security measures and enhancing overall network security management.

SAMPLE

7. What capability can be used when running PA-200 firewalls in HA active/passive mode using HA-Lite?

A. Session Synchronization

B. Configuration Sync

C. Shared Addressing

D. Stateful Failover

In an HA active/passive setup using HA-Lite with PA-200 firewalls, the functionality of Configuration Sync is essential. Configuration Sync allows the primary (active) firewall to synchronize its configuration settings with the secondary (passive) firewall. This ensures that both firewalls have the same configuration, allowing for a seamless transition should a failover occur. When one firewall takes over as the active unit, it can do so without the need for manual intervention to replicate the configuration settings. This is vital for maintaining continuity in network security policies and rules, as well as ensuring that the correct set of configurations is applied during an active failover event. In the context of HA-Lite, which is a simplified version of High Availability, some advanced features like Session Synchronization or Stateful Failover are not available, focusing instead on providing essential redundancy via configuration consistency. Thus, Configuration Sync is indeed the right capability in this scenario.

8. What does SSL Decryption enable in PAN firewalls?

A. Visibility into encrypted traffic for security inspection

B. Blocking of all encrypted traffic without inspection

C. Improved performance of non-encrypted traffic

D. Encryption of all outgoing traffic

SSL Decryption enhances the ability of Palo Alto Networks firewalls to monitor and analyze encrypted traffic, which is crucial for effective security management. When SSL Decryption is enabled, the firewall can identify and inspect the data contained within encrypted streams, allowing it to detect potential threats hiding within the encryption. This is particularly important since a significant amount of internet traffic is encrypted, making it a common vector for malware and other illicit activities. By decrypting this traffic, the firewall can apply the same security policies and protections it uses for unencrypted traffic, thus maintaining the integrity and security of the network. The option that states blocking all encrypted traffic without inspection does not enable the firewall's security capabilities since it would prevent the analysis of potentially harmful data. Improved performance of non-encrypted traffic while significant is not a direct function of SSL Decryption, as this feature primarily focuses on security rather than performance enhancements. Lastly, the option regarding the encryption of outgoing traffic is unrelated to the decryption function, as SSL Decryption pertains to inspecting, rather than encrypting, traffic flows. Therefore, the correct choice emphasizes the core benefit of SSL Decryption: enabling thorough visibility into encrypted traffic for security inspection.

SAMPLE

9. Which feature of PAN firewalls refers to the capability to partition firewall resources?

A. Security Profiles

B. Network Segmentation

C. Network Virtualization

D. Traffic Filtering

The capability to partition firewall resources within Palo Alto Networks firewalls is best described by network virtualization. This feature allows the creation of multiple virtual firewalls on a single physical hardware platform. Each virtual firewall can operate independently with its own security policies, routing configurations, and resources, effectively allowing segmentation and allocation of resources based on different organizational needs. This is particularly useful for environments where different departments or business units require isolated security policies or where resources need to be efficiently allocated to various functions. The other options do not encompass the full functionality of resource partitioning in the way network virtualization does. Security profiles refer to specific configurations around threat prevention, like antivirus and anti-spyware, which don't inherently partition resources. Network segmentation usually refers to dividing a network into segments for better traffic management and security but does not directly address the partitioning of firewall resources. Traffic filtering pertains to the process of allowing or blocking specific traffic based on a defined rule set, which, while an important aspect of firewall functionality, does not encapsulate the idea of partitioning resources.

10. What is the default setting for application-default security rules in Palo Alto Networks firewalls?

A. To block all unknown application traffic

B. To allow only application traffic that is known to the firewall

C. To allow all application traffic by default

D. To encrypt application traffic

The default setting for application-default security rules in Palo Alto Networks firewalls is to allow only application traffic that is known to the firewall. This means that the firewall uses its application identification capabilities to classify and manage traffic based on a set of predefined known applications. By allowing known applications, the firewall ensures that only legitimate and approved application traffic is permitted through the network. This approach helps maintain a secure environment by minimizing exposure to potentially harmful or unauthorized applications. It leverages the comprehensive application database maintained by Palo Alto Networks, which allows for granular control over application types and their associated risks. In this context, the security posture is strengthened since only applications that have been verified are allowed, reducing the risk of attacks that may come from unknown or untrusted sources. Thus, this setting supports both performance and security, ensuring that users can utilize necessary applications while still safeguarding the network.

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://panw-certifiednetworksecurityadministrator.examzify.com

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

SAMPLE