Palo Alto Networks (PANW) Certified Cybersecurity Entry-level Technician (PCCET) 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. 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. **Organizations are using which resource to expand their on-premises private cloud compute capacity?**

   A. Software Defined Data Centers

   B. Public Cloud

   C. Virtual Storage

   D. Virtual Networks

2. **In the context of cybersecurity, what does a vulnerability in the CVSS scoring system signify?**

   A. A weakness that can be exploited

   B. A fully secure network

   C. A type of data breach

   D. An authorized access point

3. **You downloaded a confidential file to your phone, but it's no longer there. Which MDM feature could be the reason?**

   A. Data loss prevention

   B. Malware protection

   C. Remote erase/wipe

   D. Geofencing and location services

4. **Sensors for a cultivated field must report the results once a day. These sensors are powered by batteries that need to last for years. Which form of connectivity do you use?**

   A. Bluetooth

   B. Wi-Fi

   C. LoRaWAN

   D. Satellite C-Band

5. **Which option is an example of a static routing protocol?**

   A. Open Shortest Path First (OSPF)

   B. Border Gateway Protocol (BGP)

   C. Routing Information Protocol (RIP)

   D. Split horizon

6. Which Panorama object is used to manage the security policy?

A. Template

B. Device group

C. Virtual system

D. Decryption Profile

7. Which security aspect involves the reduction of the attack surface and correlating information about discovered threats?

A. Network segmentation

B. Threat intelligence

C. Risk assessment

D. Holistic threat protection

8. Which element is a security technology that detects malicious activity by identifying anomalous behavior indicative of attacks?

A. Behavioral Analysis

B. Malware Sandboxing

C. Endpoint Security

D. Intrusion Prevention and Detection Systems

9. How many OS instances are being run when ten containers are spread between five virtual machines on two type 1 hypervisors?

A. 2

B. 5

C. 7

D. 17

10. What term refers to software versions, OS settings, and configuration file settings collectively?

A. Configuration items

B. Configurable values

C. Computer settings

D. Configuration

Answers

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

Explanations

1. Organizations are using which resource to expand their on-premises private cloud compute capacity?

A. Software Defined Data Centers

B. Public Cloud

C. Virtual Storage

D. Virtual Networks

The public cloud is a resource increasingly utilized by organizations to expand their on-premises private cloud compute capacity. It allows businesses to leverage the additional resources available in the public cloud, effectively allowing for greater flexibility and scalability. By integrating public cloud services, organizations can manage sudden spikes in demand, maintain operational efficiency, and avoid the costs associated with over-provisioning on-premises infrastructure. This hybrid approach of combining on-premises private clouds with public cloud resources facilitates a more dynamic IT environment, as organizations can quickly access and utilize vast amounts of compute storage and processing power from public cloud providers without the need for significant upfront investment in hardware. This can optimize costs and resource management, support disaster recovery strategies, and enhance overall business agility. The other options, while relevant to cloud computing, do not specifically address the method of extending private cloud capacity. Software Defined Data Centers are about the technologies that create virtualized environments, virtual storage refers to physical storage management in a more abstract way, and virtual networks pertain to networking layers rather than compute capacity directly.

2. In the context of cybersecurity, what does a vulnerability in the CVSS scoring system signify?

A. A weakness that can be exploited

B. A fully secure network

C. A type of data breach

D. An authorized access point

A vulnerability in the CVSS (Common Vulnerability Scoring System) scoring system signifies a weakness that can be exploited in a system, application, or network. CVSS is designed to provide a standardized way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. This scoring helps organizations prioritize which vulnerabilities require immediate attention based on their potential impact and exploitability. Understanding that a vulnerability indicates a weakness is crucial for cybersecurity professionals. It enables them to assess risks effectively, implement appropriate security measures, and focus on mitigating the most critical issues first. By recognizing a vulnerability as an exploitable flaw, teams can work proactively to safeguard their systems against potential attackers who may take advantage of such weaknesses.

3. You downloaded a confidential file to your phone, but it's no longer there. Which MDM feature could be the reason?

A. Data loss prevention

B. Malware protection

C. Remote erase/wipe

D. Geofencing and location services

The most appropriate answer relates to the feature of remote erase/wipe. An MDM (Mobile Device Management) system is designed to manage and secure mobile devices within an organization. One of its critical functionalities is the ability to remotely wipe or erase data from a device if it is lost, stolen, or if an employee leaves the organization, ensuring that sensitive information remains protected. In the scenario where a confidential file has disappeared from your phone, it's plausible that the MDM system has executed a remote wipe command to protect that data, which would remove all or specific files from the device to prevent unauthorized access. This function is vital for maintaining data security compliance in managed devices and is typically a proactive measure taken by IT departments to mitigate data breaches. While malware protection, data loss prevention, and geofencing/location services are all important components of MDM, they do not directly explain the absence of a file on the device in the manner that remote erase/wipe does. Malware protection focuses on detecting and preventing harmful software that could compromise data integrity. Data loss prevention targets the management of sensitive information to prevent it from leaving the organization, and geofencing/location services help monitor and manage device locations but do not necessarily remove files.

4. Sensors for a cultivated field must report the results once a day. These sensors are powered by batteries that need to last for years. Which form of connectivity do you use?

A. Bluetooth

B. Wi-Fi

C. LoRaWAN

D. Satellite C-Band

Choosing LoRaWAN as the form of connectivity for the sensors in a cultivated field is the most suitable option due to several key characteristics that align well with the requirements stated in the question. LoRaWAN (Long Range Wide Area Network) is specifically designed for low-power, long-range communication between devices. This protocol excels in scenarios where devices need to transmit small amounts of data infrequently while maintaining energy efficiency. In the case described, the sensors are only required to report results once a day, which fits well with the low data transmission needs of LoRaWAN. Furthermore, LoRaWAN is particularly advantageous for battery-operated devices. The technology allows devices to operate for several years on a single battery due to its low power consumption, which directly addresses the requirement for the sensors to last for years without needing frequent battery replacements. In contrast, other connectivity options would not fulfill the same criteria as effectively. Bluetooth typically operates over shorter distances and may require more frequent connections, which can lead to increased energy consumption. Wi-Fi offers higher data rates suitable for larger data transfers, but it consumes significantly more power than LoRaWAN, making it less desirable for battery-powered devices meant to last years. Satellite C-Band connectivity, while capable of providing extensive coverage, is also

5. Which option is an example of a static routing protocol?

A. Open Shortest Path First (OSPF)

B. Border Gateway Protocol (BGP)

C. Routing Information Protocol (RIP)

D. Split horizon

The correct answer is Border Gateway Protocol (BGP), which is indeed a routing protocol but should not be classified as static. However, understanding why the other protocols and concepts are relevant can help clarify the distinction. Static routing refers to the manually configured routes in a networking environment that do not change unless they are manually updated. BGP, on the other hand, is a dynamic routing protocol used primarily to exchange routing information across the internet and is not static in nature. Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) are also dynamic routing protocols designed to automatically update routes based on network changes. OSPF uses a link-state routing algorithm, while RIP employs a distance-vector algorithm, both of which dynamically adapt to changing network conditions. Split horizon is a routing technique used with distance-vector protocols to prevent routing loops, and it is not classified as a routing protocol itself, but rather a method for optimizing routing information. In summary, a true example of a static routing protocol would refer to methods of routing where routes are manually configured and remain constant. Neither BGP, OSPF, nor RIP fit this classification, while split horizon describes a method rather than a protocol.

6. Which Panorama object is used to manage the security policy?

A. Template

B. Device group

C. Virtual system

D. Decryption Profile

The device group is the object used to manage the security policy within Panorama. A device group allows administrators to group multiple firewalls or devices together, enabling central management of security policies and configurations across those devices. This means that policies can be defined and applied uniformly, ensuring consistent security postures across different environments. In Panorama, security policies, which include rules for allowing or blocking traffic, are assigned at the device group level. This centralizes management, simplifying the administration of security policies while allowing for flexibility in how those policies are distributed across different firewalls. Templates are used in Panorama for managing configuration settings that are applied to devices, but they do not specifically handle security policies. Virtual systems, on the other hand, refer to logical partitions within a single firewall that allow for the segmentation of environments or tenants. A decryption profile is a specific configuration for handling SSL/TLS traffic but is not related directly to the overarching management of security policy.

7. Which security aspect involves the reduction of the attack surface and correlating information about discovered threats?

A. Network segmentation

B. Threat intelligence

C. Risk assessment

D. Holistic threat protection

The correct choice focuses on the concept of holistic threat protection, which encompasses a comprehensive approach to securing an environment. Holistic threat protection involves integrating various security measures and practices to create a unified defense strategy. This approach not only aims to reduce the attack surface but also emphasizes the importance of understanding and correlating information about threats that have been identified. By reducing the attack surface, organizations are able to limit the number of potential entry points that attackers can exploit, thus making it more challenging for threats to succeed. Additionally, holistic threat protection allows organizations to gather, share, and analyze threat intelligence effectively, enabling them to adapt and respond proactively to emerging threats based on a wide range of information. The other choices, while related to aspects of cybersecurity, don't fully capture the broad integration and proactive intelligence that comes with a holistic approach. Network segmentation focuses specifically on dividing networks to limit access and control traffic, while threat intelligence is mainly about gathering and analyzing data related to threats. Risk assessment is concerned with identifying vulnerabilities and potential impacts but does not inherently include the breadth of protective measures implied in holistic threat protection.

8. Which element is a security technology that detects malicious activity by identifying anomalous behavior indicative of attacks?

A. Behavioral Analysis

B. Malware Sandboxing

C. Endpoint Security

D. Intrusion Prevention and Detection Systems

Behavioral analysis is a security technology that focuses on identifying anomalous behavior that may indicate malicious activities, such as potential attacks. By monitoring and analyzing patterns in user behavior, network traffic, and system interactions, behavioral analysis can identify deviations from the norm that could suggest a security threat. For example, if a user typically accesses certain files at specific times but suddenly attempts to access many files rapidly, that may trigger an alert. This method is particularly effective as it does not rely solely on known signatures of known threats, which means it can detect new or unknown types of attacks that may not have been previously encountered. This proactive approach helps organizations to identify potential security risks before they escalate into more serious incidents. The other options, while related to cybersecurity, serve different functions. Malware sandboxing is a technique used to analyze the behavior of malware in a controlled environment, allowing security teams to observe its actions without risk to live systems. Endpoint security encompasses a comprehensive set of measures to protect devices and endpoints but does not specifically focus on identifying anomalous behavior. Intrusion Prevention and Detection Systems (IDPS) are designed to monitor network traffic for suspicious activity and can respond to such threats; however, they primarily rely on known attack signatures or specific rule sets rather than general behavioral

9. How many OS instances are being run when ten containers are spread between five virtual machines on two type 1 hypervisors?

A. 2

B. 5

C. 7

D. 17

In this scenario, we have ten containers distributed across five virtual machines operating on two type 1 hypervisors. To understand how many operating system (OS) instances are running, it's important to recognize the relationship between containers, virtual machines, and hypervisors. Each type 1 hypervisor allows multiple virtual machines to be created, each of which typically runs its own full operating system instance. Since there are five virtual machines, assuming that each virtual machine runs a separate OS, there will be five OS instances in total. Containers, on the other hand, operate within these virtual machines and share the operating system kernel of their host. They are lightweight instances that do not run their own separate OS, which is why the number of containers does not add to the count of OS instances. Therefore, regardless of the number of containers running within those virtual machines, the total count of operating system instances remains unchanged at five. Other options suggest a different number of OS instances by either misallocating or miscalculating the relationship between containers, virtual machines, and hypervisors. However, the correct answer clearly stems from acknowledging that each of the five virtual machines represents one OS instance, resulting in a total of five OS instances running across the environment.

10. What term refers to software versions, OS settings, and configuration file settings collectively?

A. Configuration items

B. Configurable values

C. Computer settings

D. Configuration

The term that refers to software versions, operating system settings, and configuration file settings collectively is "Configuration items." This terminology is commonly used in IT and cybersecurity to describe any component that needs to be managed in order to deliver a service. Configuration items can include hardware, software, documentation, and their associated settings, which collectively ensure that the system operates correctly and consistently. Identifying and managing configuration items is essential for maintaining system integrity, performing auditing, and implementing changes effectively while minimizing the risk of disruption. This collective management helps organizations maintain international standards and compliance requirements, as well as facilitate troubleshooting and problem resolution. Other terms, while related, do not encapsulate the concept as effectively as configuration items do. For instance, "Configurable values" and "Computer settings" are more general and do not specifically capture the breadth of items managed in a configuration management context. "Configuration," on the other hand, can refer to the overall arrangement or setup but lacks the specificity of collecting various components under the term configuration items.

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-certifiedcybercecurityentryleveltechnician.examzify.com

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