# NETWORK DEFENSE ESSENTIALS (NDE) PRACTICE EXAM (SAMPLE)

## STUDY GUIDE

## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://nde.examzify.com

# 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. **In cloud computing, what is a common practice to protect Docker containers?**

   A. Running all processes as root

   B. Applying security patches regularly

   C. Limiting capabilities based on requirements

   D. Using untrusted sources for images

2. **Which IoT communication model involves the collection and analysis of data within the cloud?**

   A. Device-to-device

   B. Device-to-cloud

   C. Cloud-to-cloud

   D. Gateway-to-cloud

3. **What type of user access policy does Peter implement for employee Internet usage?**

   A. Open access policy

   B. Prudent policy

   C. Restrictive access policy

   D. Selective access policy

4. **Which feature of an IoT-enabled IT environment involves the exchange of data between IoT-enabled organizations using different communication protocols?**

   A. Data collection

   B. Data synchronization

   C. Data analytics

   D. Data governance

5. **Which of the following statements about decentralized authorization is correct?**

   A. It only allows admin users to grant access.

   B. It does not maintain separate databases for resources.

   C. Users can provide access permissions to others.

   D. It is the most secure type of authorization.

6. **Which network defense technique examines the causes for attacks using security forensics techniques and post-mortem analysis?**

A. Retrospective approach

B. Preventive approach

C. Proactive approach

D. Reactive approach

7. **Which term refers to mechanisms that restrict unauthorized access based on user identity?**

A. Firewall

B. Access Control

C. Encryption

D. Network Analysis

8. **Which technology belongs to the IEEE 802.16 family of wireless networking standards with data rates reaching up to 75 Mbps?**

A. WiMAX

B. Dipole antenna

C. WPA2 Enterprise

D. Shared key authentication

9. **Which service model is primarily targeted at providing a platform for developing, running, and managing applications?**

A. Infrastructure-as-a-Service

B. Function-as-a-Service

C. Platform-as-a-Service

D. Software-as-a-Service

10. **What type of network typically covers a wide area, encompassing nations or the globe for cellular communication?**

A. WLAN

B. WWAN

C. WPAN

D. MAN

# Answers

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

# Explanations

## 1. In cloud computing, what is a common practice to protect Docker containers?

A. Running all processes as root

B. Applying security patches regularly

C. Limiting capabilities based on requirements

D. Using untrusted sources for images

*A common practice to protect Docker containers emphasizes the principle of least privilege, where actions and permissions are limited to only those that are absolutely necessary for the function of the container. This approach helps minimize potential vulnerabilities and reduces the risk of exploitation. By limiting capabilities based on requirements, you can effectively restrict what processes within the container can do. This means that if a container is compromised, the attacker's ability to carry out harmful actions is significantly constrained. For instance, if a container does not need access to the host network or specific devices, those capabilities can be disabled. This reduces the attack surface and enhances the overall security posture of your cloud infrastructure. While applying security patches regularly is essential for maintaining secure environments, it does not inherently modify the operational capabilities of the containers in the way that limiting capabilities does. The focus here is on actively managing permissions to mitigate risks, making this practice a crucial part of securing Docker containers.*

## 2. Which IoT communication model involves the collection and analysis of data within the cloud?

A. Device-to-device

B. Device-to-cloud

C. Cloud-to-cloud

D. Gateway-to-cloud

*The IoT communication model that involves the collection and analysis of data within the cloud is known as the cloud-to-cloud model. In this context, cloud-to-cloud communication enables various cloud services and platforms to exchange data with one another, facilitating more comprehensive data analysis and processing capabilities. In the cloud-to-cloud model, devices may send data to their respective cloud infrastructures, which can then communicate with other clouds for data integration and analysis. This model optimizes data management as it centralizes resources and enables better analytics through the aggregation of data from different sources, usually hosted in various cloud environments. The other models differ in their primary interactions. Device-to-device communication focuses on the direct communication between devices, often without central cloud involvement. Device-to-cloud emphasizes the data transmission from devices to the cloud for processing, storage, or analysis, without the direct inter-cloud interaction that characterizes cloud-to-cloud. Gateway-to-cloud refers to a model where gateways collect data from multiple devices and send it to the cloud; while it still involves the cloud, the central theme is on the gateway's role in data collection rather than on analysis across cloud platforms.*

**3. What type of user access policy does Peter implement for employee Internet usage?**

A. Open access policy

B. Prudent policy

C. Restrictive access policy

D. Selective access policy

*A prudent policy for employee internet usage refers to a balanced approach that allows access to necessary resources while also considering the security and productivity implications. This type of policy typically involves guidelines that encourage employees to use the internet sensibly and responsibly, promoting an environment where access is granted to important tools and information but with an awareness of potential risks and the need for security measures. In contrast to an open access policy, which would allow unrestricted internet use, or a restrictive access policy that severely limits access to the internet, a prudent policy encourages responsible behavior while fostering efficiency. Likewise, while a selective access policy may allow some users access to specific sites or resources, the prudent policy encompasses a broader ethical and practical framework aimed at guiding overall employee behavior without imposing overly stringent restrictions. Thus, the prudent policy combines accessibility with responsibility, making it suitable for an organizational context where both internet usage and security are considered important.*

**4. Which feature of an IoT-enabled IT environment involves the exchange of data between IoT-enabled organizations using different communication protocols?**

A. Data collection

B. Data synchronization

C. Data analytics

D. Data governance

*The correct choice reflects the process in which IoT devices and systems gather and transmit data, often utilizing various communication protocols. In an IoT-enabled IT environment, data collection is crucial because it ensures that information generated by different IoT devices is gathered for further analysis and operational use. This data can originate from a myriad of devices, each potentially utilizing different standards and protocols for communication, such as MQTT, CoAP, HTTP, or others. The interoperability of these devices necessitates effective data collection methods to integrate and aggregate the data derived from these diverse sources. By focusing on data collection, organizations ensure that pertinent information is not only captured but also made available for subsequent processes, thereby facilitating the overall effectiveness of IoT systems. The ability to compile data from various protocols is paramount for the smooth functioning of an IoT ecosystem, making it a critical feature in environments that utilize a mix of IoT solutions.*

**5. Which of the following statements about decentralized authorization is correct?**

A. It only allows admin users to grant access.

B. It does not maintain separate databases for resources.

C. Users can provide access permissions to others.

D. It is the most secure type of authorization.

*Decentralized authorization allows users to manage and grant access permissions to others, which enhances flexibility and promotes peer-to-peer interactions. This approach empowers individuals within a system to control access to their resources without relying solely on a centralized authority. It is particularly beneficial in environments where collaboration is key, as it enables users to directly share access to files, tools, or services based on trust and need, rather than through a bureaucratic process managed by admin users. In contrast, centralized authorization typically restricts the ability to grant permissions to administrators only, which can slow down processes and limit flexibility. The notion that decentralized authorization does not maintain separate databases for resources is inaccurate; rather, it can involve multiple databases, often depending on the specific implementation. While decentralized systems can offer certain security advantages, stating that it is categorically the most secure type of authorization overlooks variables such as implementation quality and the specific security measures in place. Understanding these dynamics highlights why allowing users to grant access permissions to others embodies a fundamental characteristic of decentralized authorization.*

**6. Which network defense technique examines the causes for attacks using security forensics techniques and post-mortem analysis?**

A. Retrospective approach

B. Preventive approach

C. Proactive approach

D. Reactive approach

*The technique that examines the causes for attacks using security forensics techniques and post-mortem analysis is best described as a retrospective approach. This method involves analyzing past security incidents to understand how and why breaches occurred, which helps in identifying vulnerabilities and patterns that can be addressed in the future. By using security forensics, analysts can gather data from a compromised system, thoroughly investigate the incident, and learn critical lessons. This approach is particularly effective because it not only helps in refining defense measures but also contributes to the overall security strategy by leveraging historical incident data. Such insights can lead to improvements in security policies, incident response, and employee training, ultimately enhancing the organization's ability to prevent similar incidents from happening again. Other approaches, such as the preventive and proactive approaches, focus on anticipating threats and taking measures to avoid them before they can cause harm. The reactive approach, while it deals with responding to incidents after they occur, does not necessarily involve the in-depth analysis characteristic of a retrospective approach. Therefore, the retrospective method is key for understanding past events in order to bolster future defenses.*

**7. Which term refers to mechanisms that restrict unauthorized access based on user identity?**

A. Firewall

B. Access Control

C. Encryption

D. Network Analysis

*Access control refers to the mechanisms used to restrict unauthorized access to resources in a network based on user identity. This involves defining who is allowed to access certain data or systems, often through the use of user authentication methods such as passwords, biometrics, or security tokens. It is a crucial aspect of security that ensures only authorized users can access sensitive information, preventing unauthorized usage or data breaches. By implementing access control measures, organizations can enforce policies that dictate user permissions, roles, and access levels. This helps in monitoring and logging activities within the network, creating a secure environment where sensitive information is adequately protected from unauthorized access. The other options highlight different aspects of network security but do not specifically focus on user identity-based restrictions. Firewalls typically control traffic between different networks based on defined security rules, encryption secures data at rest or in transit, and network analysis involves examining data flow for security threats, but none of these focus solely on managing access based on user identity.*

**8. Which technology belongs to the IEEE 802.16 family of wireless networking standards with data rates reaching up to 75 Mbps?**

A. WiMAX

B. Dipole antenna

C. WPA2 Enterprise

D. Shared key authentication

*The technology that belongs to the IEEE 802.16 family of wireless networking standards and can achieve data rates of up to 75 Mbps is WiMAX. This standard is designed for providing wireless broadband access and is particularly well-suited for delivering high-speed internet service to large areas. WiMAX is capable of supporting a variety of applications, including mobile broadband connections and fixed wireless access, making it a significant advancement in wireless networking technologies. The other choices listed do not pertain to the IEEE 802.16 standard. A dipole antenna, for instance, is a type of radio antenna often used in various communications but does not represent a specific wireless networking standard or technology. WPA2 Enterprise and shared key authentication are security protocols and methods used for securing wireless networks rather than data transmission standards like WiMAX. These distinctions are critical in understanding the different aspects of networking technologies and their respective functions.*

## 9. Which service model is primarily targeted at providing a platform for developing, running, and managing applications?

A. Infrastructure-as-a-Service

B. Function-as-a-Service

C. Platform-as-a-Service

D. Software-as-a-Service

*The service model that is primarily targeted at providing a platform for developing, running, and managing applications is Platform-as-a-Service (PaaS). PaaS offers a complete environment for developers to build applications without worrying about the underlying infrastructure. It provides the necessary tools and services such as middleware, development frameworks, and database management systems, which streamline the application development process. With PaaS, developers can focus more on writing code and developing functionalities instead of spending time managing the servers and storage solutions. This model is designed to support the entire application lifecycle, including development, testing, deployment, and maintaining applications after they are live. The other service models serve different purposes. Infrastructure-as-a-Service (IaaS) offers virtualized computing resources over the internet, allowing users to manage servers and storage without providing a development platform. Function-as-a-Service (FaaS), often associated with serverless computing, allows the execution of individual functions without managing the infrastructure, focusing on event-driven programming. Software-as-a-Service (SaaS) delivers software applications over the internet, where users access the applications but do not engage in development or management of the underlying infrastructure. Therefore, option C is the most appropriate choice for the context of application development and management*

## 10. What type of network typically covers a wide area, encompassing nations or the globe for cellular communication?

A. WLAN

B. WWAN

C. WPAN

D. MAN

*The type of network that covers a wide area, typically encompassing nations or the globe for cellular communication, is known as a Wide Area Network (WWAN). WWANs are designed to support mobile communication over large distances, allowing devices to connect to cellular networks that can span across cities, countries, and even continents. This is particularly vital for mobile devices like smartphones, tablets, and IoT devices that require connectivity regardless of location. In contrast, other network types have more limited scopes: a Wireless Local Area Network (WLAN) typically extends to a smaller area, such as an office or home, providing local wireless connectivity. A Wireless Personal Area Network (WPAN) is even narrower, designed for short-range communication between personal devices, often within a room. Meanwhile, a Metropolitan Area Network (MAN) covers a city or a large campus, which is still smaller than the coverage provided by a WWAN. Understanding the distinctions among these network types is crucial for recognizing their applications and purposes in various communication scenarios.*

# 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://nde.examzify.com

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