

# GIAC

GDSA  
*GIAC Defensible Security Architect*

**Questions And Answers PDF Format:**

**For More Information – Visit link below:  
<https://www.certsgrade.com/>**

*Version = Product*



---

# Latest Version: 6.0

## Question: 1

How does a host-based Intrusion Detection System/Intrusion Prevention System (IDS/IPS) contribute to the security of Zero Trust Endpoints?

Response:

- A. By generating excessive logs to deter attackers
- B. By encrypting data at rest and in transit
- C. By monitoring and analyzing system activities for signs of malicious actions
- D. By serving as the primary firewall at the network perimeter

**Answer: C**

## Question: 2

Which OSI model layer is synonymous with Layer 3 defense?

Response:

- A. Managing application-specific communications over the network efficiently.
- B. Facilitating data packet routing based on logical addressing and path determination.
- C. Ensuring reliable data transfer with proper sequencing and error control mechanisms.
- D. Establishing network connections and providing error detection at the data link level.

**Answer: B**

## Question: 3

What is the primary function of a Network Intrusion Detection System (NIDS)?

Response:

- A. Preventing all malware infections
- B. Detecting potential network intrusions in real-time
- C. Encrypting network traffic
- D. Providing physical security for network devices

**Answer: B**

---

### Question: 4

Which of the following are considered best practices for secure remote access?

Response:

- A. Using outdated encryption standards
- B. Regularly updating access policies
- C. Allowing unlimited access attempts
- D. Enforcing strong authentication mechanisms

**Answer: B,D**

### Question: 5

What are the purposes of using a sandbox in network defense?

Response:

- A. Testing untrusted programs
- B. Analyzing malware behavior
- C. Storing sensitive information
- D. Enhancing user experience

**Answer: A,B**

### Question: 6

In the context of VLANs, what are the primary security concerns to address?

(Choose two)

Response:

- A. VLAN hopping
- B. Broadcast storm control
- C. DHCP starvation
- D. Quality of Service (QoS) tweaking

**Answer: A,C**

### Question: 7

What is the goal of authenticating and encrypting endpoint traffic in Zero Trust Networking?

---

Response:

- A. To prevent all network communication
- B. To allow unrestricted access to all devices
- C. To verify the identity of users and devices and protect data from interception
- D. To confuse attackers with false information

**Answer: C**

### Question: 8

Which of the following is NOT a typical feature of Data Loss Prevention (DLP) solutions?

Response:

- A. Content inspection
- B. Contextual analysis
- C. Data encryption
- D. Decreasing storage use

**Answer: D**

### Question: 9

When securing network protocols like SNMP and NTP, it is crucial to:

Response:

- A. Ensure they are unmonitored
- B. Utilize the least secure versions
- C. Configure them with public access
- D. Apply strong authentication and encryption

**Answer: D**

### Question: 10

In the context of network proxies and firewalls, what is an essential characteristic of SMTP proxies?

Response:

- A. They should enable all email attachments without scanning.
- B. They provide detailed analysis and filtering of email traffic to identify threats.
- C. They increase the speed of email delivery.
- D. They are primarily used to enhance the user interface of email applications.

---

**Answer: B**

---

For More Information – **Visit link below:**  
**<https://www.certsgrade.com/>**

## PRODUCT FEATURES

-  **100% Money Back Guarantee**
-  **90 Days Free updates**
-  **Special Discounts on Bulk Orders**
-  **Guaranteed Success**
-  **50,000 Satisfied Customers**
-  **100% Secure Shopping**
-  **Privacy Policy**
-  **Refund Policy**

**16 USD Discount Coupon Code: **NB4XKTMZ****



Visit us at <https://www.certsgrade.com/pdf/gdsa/>