Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 9:05:03 am • Time spent: 01:55

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

Which of the following tools allows the user to set security rules for an instance of an application that interacts with one organization and different security rules for an instance of the application when interacting with another organization?

- Instance awareness
- Integration
- Replication
- Encryption

EXPLANATION

Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance. This tool allows the user to set security rules for an instance of an app interacting with one organization and different security rules for an instance of the app when it interacts with another.

Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations.

Encryption is one method that a cloud provider can use to protect a customer's data.

Cloud service providers replicate data in multiple zones and within zones to provide high availability.

REFERENCES

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_awareness_secp7.question.fex

Question 2: ✔ Correct

What is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations called?

- Instance awareness
- Integration
- High availability
- Encryption

EXPLANATION

Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations.

Encryption is one method that a cloud provider can use to protect a customer's data.

Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance.

Cloud service providers replicate data in multiple zones and within zones to provide high availability.

REFERENCES

9.4.1 Cloud Services Introduction

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_integration_secp7.question.fex

Question 3: ✔ Correct

Which of the following methods can cloud providers implement to provide high availability?

- ➡ Replication
- Encryption
- Instance awareness
- Integration

EXPLANATION

Cloud service providers replicate data in multiple zones and within zones to provide high availability. Replication:

- Helps eliminate downtime (the time your data is unavailable).
- Redirects to another availability zone when a zone fails.

Cloud integration is the system that connects application repositories, systems, and IT environments in a way that allows access and exchange of data over a network by multiple devices and locations.

Encryption is one method that a cloud provider can use to protect a customer's data.

Instance awareness is the ability to apply cloud security within an application that has rules specific to an instance.

REFERENCES

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_replication_secp7.question.fex

Question 4: ✕ Incorrect

Which formula is used to determine a cloud provider's availability percentage?

- ➡ Uptime/uptime + downtime
- ~~Downtime/uptime + downtime~~
- Downtime/downtime + uptime
- Uptime/downtime + uptime

EXPLANATION

To determine the best cloud provider for your organization, compare cloud service providers' availability percentages.

- Availability percentage = uptime/uptime + downtime.
- The higher the percentage, the more resilient and reliable a provider is.

None of the other formulas are correct.

REFERENCES

9.5.3 Cloud Security Controls Facts

q_cloud_sec_ctrls_uptime_secp7.question.fex

Question 5: ✔ Correct

Which type of firewall operates at Layer 7 of the OSI model?

- Stateful
- Application layer
- Packet-filtering
- Circuit-level gateway

EXPLANATION

Application layer firewalls work on Layer 7 of the OSI model. They are considered third-generation firewalls.

Transport layer (Layer 4) firewalls are considered to be stateful firewalls. They are referred to as second-generation firewalls.

A circuit-level gateway firewall operates at the Session layer of the OSI model.

Packet-filtering firewalls work on Layer 3. They are considered first-generation firewalls.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_app_secp7.question.fex

Question 6: ✕ Incorrect

Which of the following can provide the most specific protection and monitoring capabilities?

- ~~Secure web gateway~~
- Cloud-access security broker
- Cloud native controls
- Cloud-based firewall

EXPLANATION

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider. A CASB can offer malware protection and encryption and can also give more specific protection and monitoring capabilities than secure web gateways (SWGs) and enterprise firewalls.

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

Cloud native controls refer to the security controls that are native to the cloud provider.

Secure web gateways (SWGs) detect malicious traffic and work at the Application layer in the cloud.

REFERENCES

9.4.3 Cloud Computing Security Issues

9.4.5 Cloud Storage Security Facts

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_casb_01_secp7.question.fex

Question 7: ✔ Correct

What is the on-premises, cloud-based software tool that sits between an organization and a cloud service provider called?

- ➡ Cloud-access security broker
- Secure web gateway
- Cloud native controls
- Cloud-based firewall

EXPLANATION

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider.

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

Cloud native controls refer to the security controls that are native to the cloud provider.

Secure web gateways (SWGs) detect malicious traffic and work at the Application layer in the cloud.

REFERENCES

9.4.3 Cloud Computing Security Issues

9.4.5 Cloud Storage Security Facts

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_casb_02_secp7.question.fex

Question 8: ✔ Correct

Which of the following is a network device that is deployed in the cloud to protect against unwanted access to a private network?

- Cloud-access security broker
- Virtual area network
- Cloud-based firewall
- Cloud native controls

EXPLANATION

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

Cloud native controls refer to the security controls that are native to the cloud provider.

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN. This configuration enables guest virtual machines on separate physical hosts to communicate.

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_firewall_secp7.question.fex

Question 9: ✔ Correct

Which of the following is a network security service that filters malware from user-side internet connections using different techniques?

- Cloud-access security broker
- Virtual area network
- Secure web gateway
- Cloud-based firewall

EXPLANATION

Secure web gateways (SWGs) are network security services that filter malware from user-side internet connections. SWGs use URL filtering, application control, data loss prevention, HTTPS inspections, and antivirus protection.

A cloud-based firewall is a software network device that is deployed in the cloud. It protects against unwanted access to a private network.

A cloud-access security broker (CASB) is an on-premises, cloud-based software tool or service that sits between an organization and a cloud service provider.

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN. This configuration enables guest virtual machines on separate physical hosts to communicate.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_gateway_secp7.question.fex

Question 10: ✔ Correct

Which type of firewall protects against packets coming from certain IP addresses?

- Circuit-level
- Stateful
- Packet-filtering
- Application layer

EXPLANATION

Packet-filtering firewalls work on Layer 3. They are considered to be first-generation firewalls. These firewalls check a packet's source and destination address, protocol, and destination ports. They can protect against packets coming from certain IP addresses.

Transport layer (Layer 4) firewalls are considered to be stateful firewalls. They are referred to as second-generation firewalls.

A circuit-level gateway firewall operates at the Session layer of the OSI model.

Application layer firewalls work on Layer 7 of the OSI model. They are considered third-generation firewalls.

REFERENCES

9.5.5 Cloud Security Solutions Facts

q_cloud_sec_sol_packet_secp7.question.fex