14.5 Module Quiz

Candidate: Richard Habib (richard_habib1)

Date: 12/3/2024, 10:09:01 AM • **Time Spent:** 08:15

Score: 95%

Passing Score: 80%

Question 1. ✓ Correct

What is the role of a Fibre Channel switch in a SAN?

→ ● To provide interconnections between initiators and targets

○ To assign logical unit numbers (LUNs) to storage devices

○ To encrypt data transfers between devices

○ To act as a storage device for data

Explanation

A Fibre Channel switch's primary function in a Storage Area Network (SAN) is to facilitate communication between initiators (servers) and targets (storage devices) by providing the necessary interconnections. This enables data to be transferred efficiently across the network, allowing for high-speed access to storage resources.

Acting as a storage device for data is incorrect because the Fibre Channel switch facilitates communication rather than storing data itself.

Encrypting data transfers between devices is not the primary role of a Fibre Channel switch. While security is important in SANs, encryption is typically handled by other mechanisms or devices.

Assigning logical unit numbers (LUNs) to storage devices is a function related to storage management and configuration, not the role of a Fibre Channel switch. LUNs are used to identify specific volumes or resources within a storage device for access control and management.

References

3.1.2 Modular Transceivers

14.1.4 Fibre Channel

q_san_connect_switch_role_n09.question.fex

Question 2. ✓ Correct

Your company is expanding rapidly, and the HR department is struggling to keep up with the demands of managing employee information, payroll, and benefits. The HR team is looking for a solution that is easy to implement, requires minimal IT support, and can be accessed from anywhere by the team.

Which cloud service model would BEST meet the HR department's needs?

○ IaaS

○ PaaS

→ ● SaaS

○ CDN

Explanation

Software as a Service (SaaS) is the most suitable cloud service model for the HR department's requirements. SaaS provides access to software applications over the Internet on a subscription basis. This model eliminates the need for installing, maintaining, and managing software and hardware, making it ideal for the HR team that seeks an easy-to-implement solution with minimal IT support. SaaS applications can be accessed from anywhere, providing the flexibility the HR team needs to manage employee information, payroll, and benefits efficiently as the company grows.

IaaS (Infrastructure as a Service) offers virtualized computing resources over the Internet. While it provides the infrastructure, the HR team would still need to set up, manage, and maintain any applications they use for HR tasks, which requires significant IT support and expertise.

PaaS (Platform as a Service) provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. However, it is more suited for developing custom applications rather than providing ready-to-use software solutions for HR tasks.

CDN (Content Delivery Network) is a system of distributed servers that deliver web content and other web services to users based on their geographic locations. While it improves the performance and availability of web services, it does not offer software applications for HR management and thus does not meet the HR department's needs.

References

14.2.3 Cloud Service Models

q_cloud_service_saas_scenario_n09.question.fex

Question 3. ✓ Correct

What is the purpose of a transit gateway in cloud connectivity?

- ○ To reduce the cost of cloud services
- ○ To increase the storage capacity of VPCs
- → ● To manage interconnections between VPCs and VPN gateways
- ○ To provide internet access to cloud services

Explanation

A transit gateway acts as a virtual router that simplifies the management of interconnections between VPCs and any attached VPN gateways, making it easier to handle complex network structures.

Providing internet access to cloud services is not the specific purpose of a transit gateway; it's more about managing network connections.

Increasing the storage capacity of VPCs is unrelated to the function of a transit gateway, which focuses on network routing and connectivity.

While cost efficiency can be a benefit, the primary purpose of a transit gateway is to simplify network management, not directly reduce costs.

References

14.3.4 Cloud Connectivity Options

q_cloud_option_transit_gateway_n09.question.fex

Question 4. ✓ Correct

What does an SD-WAN use to provision the fastest or most reliable transport?

→ ● Any available IP underlay network

○ Dedicated leased lines only

○ Only MPLS VPNs

○ A single broadband Internet connection

Explanation

SD-WAN's ability to leverage any available IP underlay network, such as broadband, cellular, or MPLS, ensures the best possible path for data, enhancing speed and reliability.

Only MPLS VPNs would limit the flexibility and the potential speed and reliability improvements offered by SD-WAN.

A single broadband Internet connection does not provide the redundancy or flexibility of SD-WAN.

Dedicated leased lines only would not allow SD-WAN to dynamically choose the best path for data.

References

14.4.5 Software-Defined WAN

q_sdwan_ip_underlay_network_n09.question.fex

Question 5. ✓ Correct

What is the purpose of Management and Orchestration (MANO) in NFV?

○ To provide internet services

○ To develop new virtual appliances

→ ● To position VNFs within workflows

○ To manage physical servers and hardware

Explanation

Management and Orchestration (MANO) in NFV architecture positions Virtual Network Functions (VNFs) within workflows to perform specific forwarding and filtering tasks, facilitating network function virtualization.

MANO focuses on the management and orchestration of virtual functions, not physical servers and hardware.

Providing internet services is not the specific role of MANO; it's more about managing virtual network functions.

Developing new virtual appliances is a task for vendors or developers, not the MANO component of NFV.

References

14.3.1 Cloud Instances

q_cloud_sec_mano_purpose_n09.question.fex

Question 6. ✓ Correct

An organization is facing challenges with securing access to cloud services for its remote workforce. They have noticed an increase in malware incidents and unauthorized data access attempts.

The security team is looking for a solution that can enforce strict access controls, provide single sign-on capabilities, and monitor user activities for compliance and threat detection. They are also interested in a solution that can prevent data exfiltration and scan for malware in real-time.

Which component of SASE would MOST effectively address the organization's security challenges?

○ SD-WAN

○ Zero Trust Architecture

→ ● Cloud Access Security Broker (CASB)

○ Secure Web Gateway (SWG)

Explanation

A Cloud Access Security Broker (CASB) would most effectively address the organization's security challenges by providing a set of technologies designed to mediate access to cloud services. CASBs enforce strict access controls, enable single sign-on authentication, scan for malware, monitor and audit user and resource activity, and mitigate data exfiltration, directly aligning with the organization's needs.

While Software-Defined Wide Area Network (SD-WAN) technology is a key component of SASE, it primarily focuses on optimizing network connectivity and performance, not directly addressing the specific security challenges mentioned.

Zero Trust Architecture is a principle that can be part of a SASE solution, focusing on not trusting any user or device by default. While it contributes to securing access, it does not by itself provide the comprehensive set of functionalities (like malware scanning or single sign-on) that a CASB offers.

A Secure Web Gateway (SWG) provides safe access to the Internet and cloud services by enforcing security policies and filtering unwanted software. However, it does not offer the broad range of specific functionalities (such as single sign-on or detailed user activity monitoring) that a CASB does, making CASB the more effective choice for the organization's stated needs.

References

14.4.8 Secure Access Service Edge

q_secure_edge_casb_scenario_n09.question.fex

Question 7. ✓ Correct

Which deployment model might a travel organization use to handle higher utilization forecast during certain times of the year?

○ Hosted Private

○ Private

→ ● Hybrid

○ Public

Explanation

A hybrid cloud computing solution is ideal for a travel organization that runs a sales website for most of the year using a private cloud but needs to "break out" the solution to a public cloud during times of much higher utilization. This model provides the flexibility to use both private and public clouds based on demand and requirements.

A public cloud alone might not offer the level of control and security a travel organization needs for regular operations.

A hosted private cloud might not offer the scalability needed for peak times without significant additional cost.

A private cloud might not provide the necessary scalability and cost-effectiveness for handling high utilization periods.

References

14.2.2 Cloud Deployment Models

q_cloud_deploy_hybrid_example_n09.question.fex

Question 8. ✓ Correct

What is the role of virtualized security appliances in modern data centers?

○ To store physical documents securely

○ To replace physical servers

○ To manage employee workspaces

→ ● To monitor traffic as it passes between servers

Explanation

Virtualized security appliances play a crucial role in modern data centers by monitoring traffic as it passes between servers, helping to secure east-west traffic without creating bottlenecks. They do not replace physical servers, store documents, or manage workspaces.

Virtualized security appliances are focused on security, not on replacing the core computing resources.

Virtualized security appliances are concerned with digital data security, not physical document storage.

The role of virtualized security appliances is in network security, not in workspace management.

References

14.1.1 Data Center Network Design

q_data_center_install_virtualized_appliances_n09.question.fex

Question 9. ✓ Correct

What is a Content Delivery Network (CDN)?

○ A service that provides tools for application development

○ A type of IaaS focused on providing storage solutions

→ ● A network of servers used to deliver content to users worldwide

○ A cloud service model for delivering software applications

Explanation

A Content Delivery Network (CDN) is a system of distributed servers that deliver web content and other web services to users based on their geographic locations. The goal is to provide high availability and performance by distributing the service spatially relative to end-users.

CDNs do not provide tools for application development; they are focused on content delivery.

CDNs are not a cloud service model like SaaS; they are a specific infrastructure setup for content delivery.

While CDNs involve storage, they are not a type of IaaS focused solely on providing storage solutions; their primary purpose is efficient content delivery.

References

14.2.4 Content Delivery Networks

q_cloud_service_cdn_description_n09.question.fex

Question 10. ✓ Correct

What is the purpose of threat scope reduction and least privilege access in ZTA?

○ To grant unlimited access to network resources

→ ● To limit access to resources on a need-to-know basis

○ To increase the network's attack surface

○ To simplify network management

Explanation

By granting access only as needed and limiting it to the minimum necessary resources, ZTA effectively reduces the network's attack surface and mitigates the potential impact of breaches.

Increasing the network's attack surface would be counterproductive to ZTA's security objectives.

Granting unlimited access to network resources contradicts the principle of least privilege, a cornerstone of ZTA.

Simplifying network management is not the primary goal of these ZTA concepts, which are focused on enhancing security.

References

14.4.7 Zero Trust Architecture

q_zero_trust_threat_scope_reduction_n09.question.fex

Question 11.

✓ Correct

The IT department of a large organization is considering the implementation of NVMe over Fabrics (NVMe-oF) in their Fibre Channel SAN to enhance the performance of their solid-state storage devices.

What is the primary benefit of implementing NVMe-oF in this scenario?

○ To enable wireless connectivity between servers and storage devices

→ ● To improve the performance of solid-state storage devices in the network

○ To extend the physical distance between servers and storage devices

○ To decrease the number of required storage devices

Explanation

NVMe over Fabrics (NVMe-oF) is designed to extend the NVMe protocol over a network fabric, such as Fibre Channel. This allows for the high-speed, efficient access capabilities of NVMe to be utilized across the SAN, significantly improving the performance of solid-state storage devices connected to the network. NVMe-oF is particularly beneficial for environments that require fast data access and low latency.

Extending the physical distance between servers and storage devices is not the primary benefit of NVMe-oF. While network infrastructure can impact distance, NVMe-oF focuses on performance enhancement.

Decreasing the number of required storage devices is not a direct benefit of implementing NVMe-oF. The protocol aims to improve performance, not reduce the quantity of storage hardware.

Enabling wireless connectivity is not related to NVMe-oF, which is used in wired SAN environments to improve the performance of storage access over network fabrics.

References

3.1.2 Modular Transceivers

14.1.4 Fibre Channel

q_san_connect_solid-state_storage_scenario_n09.question.fex

Question 12. ✓ Correct

Why is a SAN isolated from the main network?

- ○ To reduce the cost of data storage
- ○ To ensure it can be accessed by client PCs and laptops
- ○ To make it easier to manage and configure
- → ● To provide a fast and reliable network for storage

Explanation

A SAN is isolated from the main network to ensure that it can provide an extremely fast and reliable network dedicated solely to storage functions. This isolation helps in maintaining the performance and reliability required for accessing large amounts of shared storage.

The isolation is for performance and reliability, not cost reduction.

SANs are accessed by servers, not directly by client PCs and laptops.

The primary reason for isolation is performance and reliability, not ease of management or configuration.

References

14.1.3 Storage Area Networks

14.1.4 Fibre Channel

14.1.5 Lab: Configure an iSCSI Target

14.1.6 Lab: Configure an iSCSI Initiator

q_san_fast_network_n09.question.fex

Question 13. × Incorrect

What is an implicit trust zone in ZTA?

○ A static zone where all users are fully trusted

○ A permanent secure area within the network where all data is stored

→ ○ A dynamic, secure pathway established for a specific transaction

● ~~An area outside the network perimeter where trust is assumed~~

Explanation

The implicit trust zone is a concept in ZTA that refers to a temporary, secure communication path established for the duration of a specific transaction, emphasizing the transient and granular nature of trust.

A permanent secure area within the network for data storage misinterprets the temporary and transaction-specific nature of the implicit trust zone.

An area outside the network perimeter where trust is assumed contradicts ZTA's principle of not assuming trust based on location.

A static zone where all users are fully trusted goes against the dynamic and skeptical approach of ZTA.

References

14.4.7 Zero Trust Architecture

q_zero_trust_implicit_trust_zone_n09.question.fex

Question 14. ✓ Correct

Which of the following best describes the concept of Network Functions Virtualization (NFV)?

○ A method for increasing physical network infrastructure

○ A tool for physical network device maintenance

○ A protocol for enhancing internet speed and reliability

→ ● A strategy for virtualizing network services through software

Explanation

Network Functions Virtualization (NFV) is a strategy aimed at virtualizing network services that were traditionally carried out by hardware appliances, using software running on standard server hardware. This approach allows for more flexible, scalable, and efficient network service deployment.

NFV is about reducing reliance on physical network infrastructure, not increasing it.

NFV focuses on virtualizing network functions rather than directly enhancing internet speed and reliability.

NFV is not a tool for maintaining physical network devices; it's about moving away from physical devices towards virtualized functions.

References

14.3.1 Cloud Instances

q_cloud_sec_nfv_description_n09.question.fex

Question 15. ✓ Correct

Which of the following is a characteristic of SDN?

- ○ Increased need for manual reconfiguration
- → ● Transport agnostic
- ○ Decentralized policy management
- ○ Application unaware

Explanation

Being transport agnostic means that SDN can operate over any underlying network technology, such as Ethernet, Wi-Fi, or cellular networks. This characteristic is crucial for SDN's flexibility and adaptability, allowing it to support a wide range of networking environments and requirements.

SDN is characterized by centralized policy management, where policies are defined and managed centrally rather than distributed across individual devices.

One of the advantages of SDN is the reduction in the need for manual reconfiguration, thanks to centralized management and automation capabilities.

SDN networks are designed to be application-aware, allowing for more intelligent and efficient handling of different types of network traffic.

References

14.4.4 Software-Defined Networking

q_sd_network_sdn_characteristic_n09.question.fex

Question 16. ✓ Correct

What is the primary purpose of a data center?

○ To serve as a storage facility for physical documents

○ To function as a retail space for technology products

○ To provide a workspace for employees

→ ● To host network services and server resources

Explanation

A data center is dedicated to provisioning server resources and hosting network services such as authentication, addressing, name resolution, application servers, and storage area networks (SANs). It is not meant for employee workspaces, storing physical documents, or functioning as a retail space.

Although data centers may have staff, their main function is not to serve as a workspace but to house computing and networking equipment.

Data centers are focused on digital data storage and processing, not physical documents.

Data centers are operational facilities for IT infrastructure, not retail spaces.

References

14.1.1 Data Center Network Design

q_data_center_install_primary_purpose_n09.question.fex

Question 17. ✓ Correct

Your company is migrating its on-premises data center to a cloud environment. The migration plan includes deploying several web applications that will be accessible publicly. You are tasked with designing a security solution that protects these applications from web-based attacks while ensuring high availability and minimal latency.

Which type of firewall should you implement to secure the web applications?

→ ● Web application firewall (WAF)

○ Host-based firewall

○ Network layer firewall

○ Stateful packet filtering firewall

Explanation

The correct answer is Web application firewall (WAF). A Web Application Firewall (WAF) is specifically designed to protect web applications by monitoring and filtering HTTP/S traffic between the web application and the Internet. It is capable of identifying and blocking web-based attacks such as SQL injection, cross-site scripting (XSS), and other vulnerabilities that are common to web applications. This makes it the most suitable option for securing web applications in a cloud environment, where high availability and minimal latency are crucial.

While stateful packet filtering firewalls can track and control the state of active connections, they are not specifically designed to protect web applications from the myriad of web-based attacks.

Network layer firewalls perform basic packet filtering based on IP addresses and ports, which is not sufficient for the deep inspection required to protect web applications from sophisticated attacks.

Host-based firewalls are deployed on individual servers and can provide a layer of security, but they are not specialized in web application security like a WAF.

References

1.3.5 Transport and Application Layer and Security Functions

5.4.1 Firewall Uses and Types

5.4.2 Firewall Selection and Placement

10.5.1 Security Rules and ACL Configuration

10.5.4 Misconfigured Firewall and ACL Issues

10.5.5 Creating Firewall ACLs

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

14.3.5 Cloud Firewall Security

q_cloud_firewall_waf_scenario_n09.question.fex

Question 18. ✓ Correct

What does resource pooling mean in the context of cloud computing?

→ ● Sharing hardware resources among multiple customer accounts

○ Gathering data from various sources into a single database

○ Pooling security resources to protect against cyber threats

○ Combining physical resources to create a single, powerful server

Explanation

Resource pooling refers to the practice of using a shared set of physical resources (such as CPU, memory, and storage) to serve multiple customers. This is achieved through virtualization, allowing cloud providers to efficiently allocate resources based on demand, contributing to both scalability and elasticity.

While security is crucial in cloud computing, resource pooling specifically refers to the sharing of hardware resources, not security resources.

Combining physical resources to create a single server is more related to building high-performance computing systems, not the dynamic allocation of resources in cloud computing.

Gathering data into a single database is a data management strategy, not related to the concept of resource pooling in cloud computing.

References

14.2.1 Cloud Scalability and Elasticity

q_cloud_scale_resource_pooling_n09.question.fex

Question 19. ✓ Correct

What is the primary benefit of a highly elastic cloud system?

→ ● It can adjust resources in real-time to meet demand.

○ It ensures data is automatically backed up.

○ It can operate without internet connectivity.

○ It allows for unlimited storage capacity.

Explanation

The primary benefit of a highly elastic cloud system is its ability to automatically scale resources up or down in real-time as demand changes. This ensures that the system can handle sudden spikes in usage without performance degradation and can also reduce operational costs by deprovisioning resources when demand is low.

Internet connectivity is a requirement for accessing cloud services; elasticity does not change this.

Automatic data backup is an important feature of cloud services but is not directly related to elasticity.

While cloud systems offer scalable storage, elasticity specifically refers to the real-time adjustment of resources, not the provision of unlimited capacity.

References

14.2.1 Cloud Scalability and Elasticity

q_cloud_scale_elasticity_benefit_n09.question.fex

Question 20. ✓ Correct

Why might an organization choose a third-party firewall solution over a CSP's native firewall service?

→ ● Higher transaction costs with native services

○ No need for rule management

○ Less efficient traffic filtering

○ Lower security standards

Explanation

Organizations might opt for third-party firewall solutions due to the potentially higher transaction costs associated with cloud service provider (CSP) native firewall services, which are often based on time deployed and volume of traffic. Cost considerations can drive the choice of security solutions.

Lower security standards are not typically a reason to choose third-party solutions; security needs drive the choice.

The need for rule management exists with both CSP-native and third-party solutions.

Efficiency in traffic filtering is a requirement for all firewall solutions, not a reason to choose one over another.

References

1.3.5 Transport and Application Layer and Security Functions

5.4.1 Firewall Uses and Types

5.4.2 Firewall Selection and Placement

10.5.1 Security Rules and ACL Configuration

10.5.4 Misconfigured Firewall and ACL Issues

10.5.5 Creating Firewall ACLs

10.5.7 Lab: Configure a Security Appliance

10.5.8 Lab: Configure a Perimeter Firewall

14.3.5 Cloud Firewall Security

q_cloud_firewall_transaction_costs_n09.question.fex