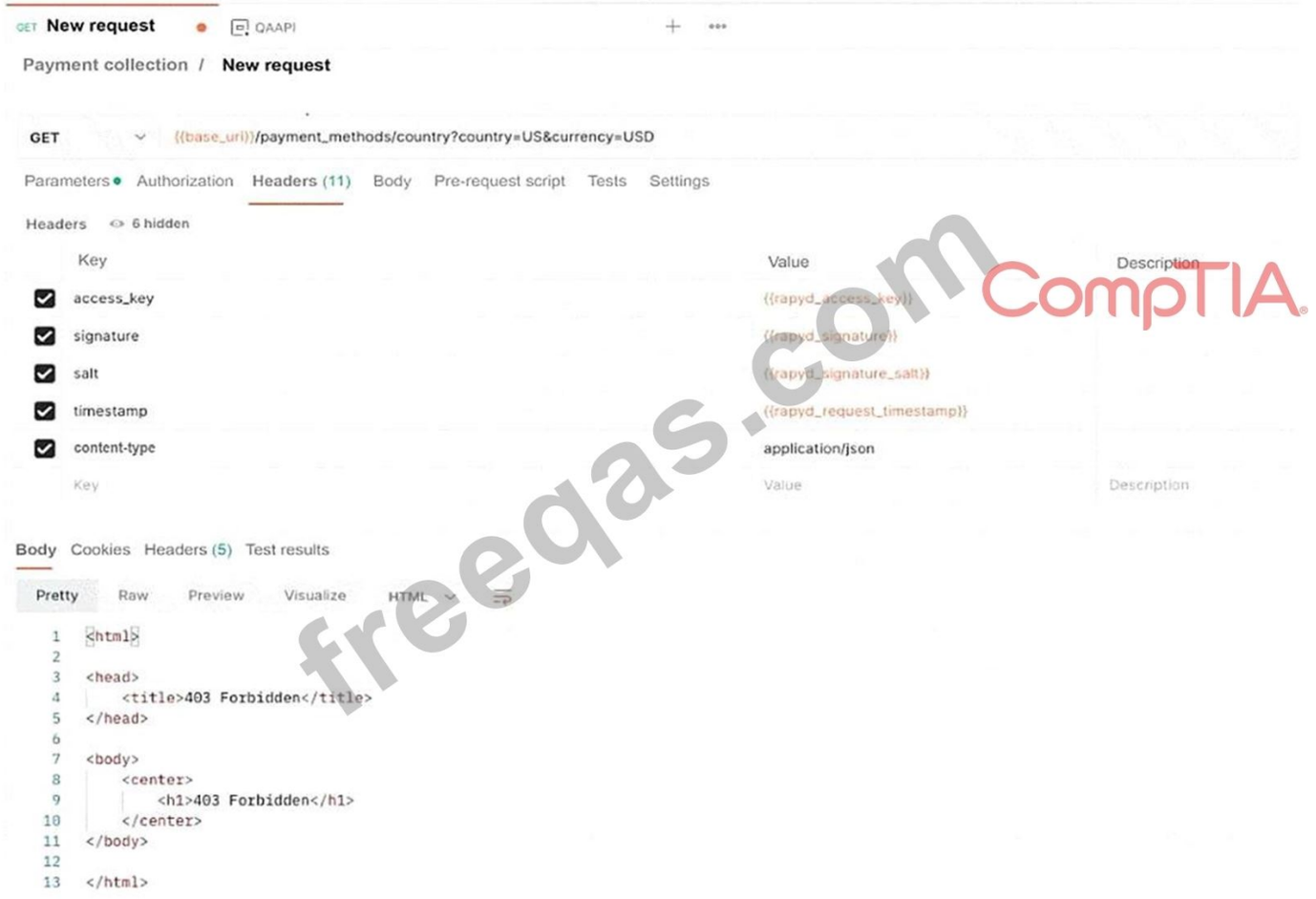
CompTIA.CNX-001.v2026-02-24.q62

Exam Code:	CNX-001
Exam Name:	CompTIA CloudNetX Certification Exam
Certification Provider:	CompTIA
Free Question Number:	62
Version:	v2026-02-24
# of views:	115
# of Questions views:	620
https://www.freeqas.com/qa/CompTIA/CNX-001/CompTIA.CNX-001.v2026-02-24.q62.html	

NEW QUESTION: 1
A network architect must ensure only certain departments can access specific resources while on premises.
Those same users cannot be allowed to access those resources once they have left campus.
Which of the following would ensure access is provided according to these requirements?
A. Enabling MFA for only those users within the departments needing access
B. Configuring geofencing with the IPs of the resources
C. Configuring UEBA to monitor all access to those resources during non-business hours
D. Implementing a PKI-based authentication system to ensure access
Answer: B (LEAVE A REPLY)
By defining an IP-based geofence around the on-premises network addresses where those resources reside, you ensure that only users connecting from inside the campus IP ranges can reach them. As soon as the same users leave that network (and thus fall outside the geofenced IP block), access is automatically denied.

NEW QUESTION: 2
Throughout the day, a sales team experiences videoconference performance issues when the accounting department runs reports. Which of the following is the best solution?
A. Running the accounting department's reports outside of business hours
B. Using a load balancer to split the video traffic evenly
C. ConfiguringQoS on the corporate network switches
D. Increasing the throughput on the network by purchasing high-end switches
Answer: C (LEAVE A REPLY)
By implementing Quality of Service rules, you can prioritize videoconference packets over the bulk data transfers generated by accounting reports, ensuring consistent call quality without disrupting either department's workflows.

NEW QUESTION: 3
A developer reports errors when trying to access a web application. The developer uses Postman to troubleshoot and receives the following error:
* HTTP Status: 403 Forbidden
* Headers include authentication-related variables such as access_key, signature, salt, and timestamp
* The request is a GET request to a payment methods API



Which of the following is the cause of the issue?
A. Requested element not found
B. Lack of user authentication
C. Too restrictive NGFW rule
D. Incorrect HTTP redirection
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A 403 Forbidden error indicates that the request was understood by the server but is refusing to fulfill it due to insufficient authorization. The developer is attempting to call a protected API that requires valid credentials such as an access key and signature (often used in HMAC-based APIs), but the values appear as Postman variables (e.g., {{rapyd_access_key}}), which suggests they were not replaced with actual credentials.

This typically means that the request lacks proper authentication or authorization headers, or the keys
/signature are incorrect or missing. The presence of access_key, signature, salt, and timestamp in the request implies the API requires authentication, but the variables were not resolved or valid.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "API Security and Authentication":
"A 403 error typically results from failed authentication or lack of proper authorization. Developers must ensure that tokens or signatures are valid, not missing, and properly injected." Other options:
* A. 404 is the code for a missing resource, not 403.
* C. A firewall rule would block the request entirely (e.g., no response or a 0 status), not result in a 403 from the server.
* D. HTTP redirection issues typically result in 3xx codes, not 403.

NEW QUESTION: 4
A partner is migrating a client from on premises to a hybrid cloud. Given the following project status information, the initial project timeline estimates need to be revised:

Phase	Initial estimate	Current status
Discovery	1 month	2 months
Design	2 weeks	1 month
Implementation	6 months	9 months
Knowledge transfer	2 months	3 months

Which of the following documents needs to be revised tobestreflect the current status of the project?
A. BIA
B. SLA
C. SOW
D. WBS
Answer: D (LEAVE A REPLY)
The Work Breakdown Structure is where each project phase and its duration are documented in detail. Since the estimated timelines for discovery, design, implementation, and knowledge transfer have all slipped, you update the WBS to reflect the new, actual phase durations.

NEW QUESTION: 5

A network engineer is setting up guest access on a Wi-Fi network. After a recent network analysis, the engineer discovered that a user could access the guest network and attack the corporate network, since the networks share the same VLAN. Which of the following should the engineer do to prevent an attack like this one from happening?

A. Configure Layer 2 client isolation for the wireless network.

B. Set up a MAC filtering rule and add the MAC addresses of all corporate devices to the allow list.

C. Set up a strong password on the guest wireless network.

D. Set up a captive portal so all guest users have to register before gaining access to the wireless network.

Answer: (SHOW ANSWER)

By enabling client isolation at Layer 2, guest clients can still reach the Internet but cannot directly communicate with any other device on that VLAN, including your corporate endpoints, stopping lateral attacks without needing MAC whitelists or overly complex captive-portal setups.

NEW QUESTION: 6

An architect needs to deploy a new payroll application on a cloud host. End users' access to the application will be based on the end users' role. In addition, the host must be deployed on the 192.168.77.32/30 subnet.

Which of the following Zero Trust elements are being implemented in this design? (Choose two.)

A. Least privilege

B. Device trust

C. Microsegmentation

D. CASB

E. WAF

F. MFA

Answer: A,C (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

A: Least privilege - This Zero Trust principle ensures users can only access the resources necessary for their job roles. Role-based access control (RBAC), as mentioned in the scenario, is a textbook implementation of least privilege.

C: Microsegmentation - Deploying the application in a small subnet (192.168.77.32/30 provides only 2 usable host IPs) limits lateral movement and isolates the host at a network level. This is a key characteristic of microsegmentation, where resources are placed in small, tightly controlled network segments.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Zero Trust Security Architecture":

"Least privilege enforces access permissions based on job responsibilities."

"Microsegmentation applies granular isolation policies between resources to reduce the attack surface and lateral movement." Other options:

* B. Device trust involves assessing device posture and compliance before granting access.

* D. CASB (Cloud Access Security Broker) governs cloud access, not access control or subnetting.
* E. WAF protects web applications but is not a Zero Trust element directly related to access control.
* F. MFA supports identity verification but is not directly evidenced in the scenario.

NEW QUESTION: 7
A network administrator recently deployed new Wi-Fi 6E access points in an office and enabled 6GHz coverage. Users report that when they are connected to the new 6GHz SSID, the performance is worse than the 5GHz SSID. The network administrator suspects that there is a source of 6GHz interference in the office.
Using the troubleshooting methodology, which of the following actions should the network administrator do next?
A. Test to see if the changes have improved network performance.
B. Use a spectrum analyzer and check the 6GHz spectrum.
C. Document the list of channels that are experiencing interference.
D. Change the channels being used bythe 6GHz radios in the APs.
Answer: B (LEAVE A REPLY)
Before making configuration changes, you should verify and pinpoint the suspected interference source by analyzing the 6 GHz band. A spectrum analyzer will reveal any non-Wi-Fi transmissions or overlapping noise that's degrading performance, allowing you to target your remediation effectively.

NEW QUESTION: 8
A company is experiencing numerous network issues and decides to expand its support team. The new junior employees will need to be onboarded in the shortest time possible and be able to troubleshoot issues with minimal assistance. Which of the following should the company create to achieve this goal?
A. Statement of work documenting what each junior employee should do when troubleshooting
B. Clearly documented runbooks for networking issues and knowledge base articles
C. Physical and logical network diagrams of the entire networking infrastructure
D. A mentor program for guiding each junior employee until they are familiar with the networking infrastructure
Answer: (SHOW ANSWER)
Runbooks provide step-by-step troubleshooting procedures, and a solid knowledge base captures known issues and resolutions. Together they let new team members ramp up quickly and resolve common network problems with minimal hand-holding.

NEW QUESTION: 9
As part of a project to modernize a sports stadium and improve the customer service experience for fans, the stadium owners want to implement a new wireless system. Currently, all tickets are

electronic and managed by the stadium mobile application. The new solution is required to allow location tracking precision within 5ft (1.5m) of fans to deliver the following services:
* Emergency/security assistance
* Mobile food order
* Event special effects
* Raffle winner location displayed on the giant stadium screen
Which of the following technologies enables location tracking?
A. SSID
B. BLE
C. NFC
D. IoT
Answer: B (LEAVE A REPLY)
BLE (Bluetooth Low Energy) is a wireless personal area network (WPAN) technology designed for applications that require lower energy consumption and reduced cost while maintaining a communication range similar to classic Bluetooth. BLE supportslocation tracking with an accuracy range typically between 1 to 2 meters (approximately 3 to 6 feet), making it ideal for applications that demandfine-grained location services, such as stadium services requiring real-time user proximity data.
According to theCompTIA CloudNetX CNX-001 Official Objectives, under theNetwork Architecture domain, specifically in the subdomain:
"Wireless Technologies: Identify capabilities of BLE, NFC, RFID, and IoT devices within a network environment,"it is outlined that:
* "BLE enables proximity-based services and real-time indoor location tracking with high accuracy when used with beacon infrastructure."
* "BLE beacons can be deployed throughout a physical space, transmitting signals received by mobile applications to determine a user's location within a few feet."
* "BLE is widely adopted for use cases including indoor navigation, asset tracking, and personalized user engagement, making it a critical technology for modern high-density venues such as stadiums." In comparison:
* SSIDmerely identifies a wireless network and has no location tracking function.
* NFCrequires close contact (under 4 cm), and is not suitable for continuous or broad-range tracking.
* IoTis an overarching category that includes connected devices and sensors; however, IoT is not a standalone location tracking technology. It may include BLE as a component, butBLE specifically provides the precise location tracking functionality.
These distinctions are explicitly addressed in theCompTIA CloudNetX CNX-001 Study Guide, under the section:
* "Emerging Network Technologies and Architectures", where BLE is described as a key enabling technology for context-aware and location-based services in enterprise and public environments.

NEW QUESTION: 10

A network architect is designing a solution to place network core equipment in a rack inside a data center.
This equipment is crucial to the enterprise and must be as secure as possible to minimize the chance that anyone could connect directly to the network core. The current security setup is:
* In a locked building that requires sign in with a guard and identification check.
* In a locked data center accessible by a proximity badge and fingerprint scanner.
* In a locked cabinet that requires the security guard to call the Chief Information Security Officer (CISO) to get permission to provide the key.
Which of the following additional measures should the architect recommend to make this equipment more secure?
A. Make all engineers with access to the data center sign a statement of work.
B. Set up a video surveillance system that has cameras focused on the cabinet.
C. Have the CISO accompany any network engineer that needs to do work in this cabinet.
D. Require anyone entering the data center for any reason to undergo a background check.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Adding video surveillance that is focused on the cabinet enhances physical security by providing monitoring, deterrence, and forensic evidence in case of unauthorized access. Video surveillance complements existing layered access controls and is a recognized best practice for protecting high-value network assets.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Physical Security Controls":
"Video surveillance provides 24/7 monitoring and records of physical access to critical infrastructure, supporting audit and incident investigation processes." Other options:
* A. A statement of work is administrative and does not enhance physical security.
* C. CISO accompaniment is impractical and not scalable.
* D. Background checks are useful but are generally a prerequisite and not a real-time security control.

NEW QUESTION: 11
A large commercial enterprise that runs a global video streaming platform recently acquired a small business that serves customers in a geographic area with limited connectivity to the global telecommunications infrastructure. The executive leadership team issued a mandate to deliver the highest possible video streaming quality to all customers around the world. Which of the following solutions should the enterprise architect suggest to meet the requirements?
A. Serve the customers in the acquired area with a highly compressed version of content.
B. Use a geographically weighted DNS solution to distribute the traffic.
C. Deploy multiple local load balancers in the newly added geographic area.
D. Utilize CDN for all customers regardless of geographic location.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:

A Content Delivery Network (CDN) distributes content across geographically distributed edge locations to provide faster access and higher quality to users, especially in areas with suboptimal connectivity to central data centers. By caching and serving content from edge servers near users, CDNs reduce latency and improve streaming performance globally.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "CDN and Cloud Edge Services":
"CDNs provide globally distributed edge nodes for content caching and delivery, ensuring low-latency, high- bandwidth access for end users regardless of their location." Other options:
* A. Reduces quality, contrary to the stated goal.
* B. DNS-based routing helps with direction but does not solve content delivery or bandwidth issues.
* C. Load balancers help distribute traffic locally, but do not provide edge caching or bandwidth optimization.

NEW QUESTION: 12
A user reports an issue connecting to a database server. The front-end application for this database is hosted on the company's web server. The network engineer has changed the network subnet that the company servers are located on along with the IP addresses of the servers. These are the new configurations:
* New subnet for the servers is 10.10.10.64/27
* Web server IP address is 10.10.10.101
* Database server IP is 10.10.10.93
Which of the following is most likely causing the user's issue?
A. The web application server is not forwarding the requests.
B. The database server firewall is blocking the port to the database.
C. The DNS server is not resolving properly.
D. The web server does not have the correct network configuration.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Since the subnet and IPs were changed recently, and users are accessing the database through a web application, the likely issue is that DNS records have not been updated to reflect the new IP addresses. If DNS is pointing to old IPs, users will fail to reach the services even if they are up and reachable on the new subnet.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "DNS and Network Configuration Troubleshooting":
"DNS misconfiguration is a common issue following IP address changes. If DNS entries are not updated accordingly, clients will attempt to reach services at outdated IPs." Other options:
* A. No indication of web server misconfiguration is provided.
* B. Firewall issues would affect all users, not just one.
* D. The web server has a valid IP in the subnet range; no misconfiguration is indicated.

NEW QUESTION: 13
An application is hosted on a three-node cluster in which each server has identical compute and network performance specifications. A fourth node is scheduled to be added to the cluster with three times the performance as any one of the preexisting nodes. The network architect wants to ensure that the new node gets the same approximate number of requests as all of the others combined. Which of the following load- balancing methodologies should the network architect recommend?
A. Round-robin
B. Load-based
C. Least connections
D. Weighted
Answer: D (LEAVE A REPLY)
Assign each of the three original nodes a weight of 1 and the new high-performance node a weight of 3. With weighted balancing, the new node will receive 3 / (1 + 1 + 1 + 3) = 50% of traffic - equal to the combined load on the other three.

NEW QUESTION: 14
A network administrator is configuring firewall rules to lock down the network from outside attacks. Which of the following should the administrator configure to create the most strict set of rules?
A. URL filtering
B. File blocking
C. Network security group
D. Allow List
Answer: D (LEAVE A REPLY)
By explicitly permitting only known, approved traffic and blocking everything else by default, an allow-list policy enforces the strictest firewall posture.

NEW QUESTION: 15
A network engineer is setting up guest access on a Wi-Fi network. After a recent network analysis, the engineer discovered that a user could access the guest network and attack the corporate network, since the networks share the same VLAN. Which of the following should the engineer do to prevent an attack like this one from happening?
A. Configure Layer 2 client isolation for the wireless network.
B. Set up a captive portal so all guest users have to register before gaining access to the wireless network.
C. Set up a MAC filtering rule and add the MAC addresses of all corporate devices to the allow list.
D. Set up a strong password on the guest wireless network.
Answer: (SHOW ANSWER)

By enabling client isolation at Layer 2, guest clients can still reach the Internet but cannot directly communicate with any other device on that VLAN, including your corporate endpoints, stopping lateral attacks without needing MAC whitelists or overly complex captive-portal setups.

NEW QUESTION: 16
A network load balancer is not correctly validating a client TLS certificate. The network architect needs to validate the certificate installed on the load balancer before progressing. Which of the following commands should the architect use to confirm whether the private key and certificate match?
A. openssl-list -noout -modulus -in cert.crt | openssl md5
openssl rsa -noout -modulus -in privkey.txt | openssl md5
B. openssl req -in certificate.csr -verify
openssl-verify -noout -modulus -in privkey.txt | openssl md5
C. openssl-rsa -noout -modulus -in cert.crt | openssl md5
openssl-verify -noout -modulus -in privkey.txt | openssl md5
D. openssl x509 -noout -modulus -in cert.crt | openssl md5
openssl rsa -noout -modulus -in privkey.txt | openssl md5
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
To verify that the certificate and the private key match, one can extract the modulus from both files and compare their hash values. The correct syntax involves using openssl x509 to extract the modulus from the certificate, and openssl rsa to extract the modulus from the private key, followed by an MD5 hash to ensure they match.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "TLS/SSL Certificate Validation and Troubleshooting":
"To verify that the private key and certificate match, compare the modulus values. A mismatch results in failed TLS handshakes." Other options:
* A & C: Incorrect syntax (openssl-list and openssl-rsa are not valid commands).
* B: The commands shown are used to verify CSRs, not matching keys.

NEW QUESTION: 17

A network administrator is troubleshooting an outage at a remote site. The administrator examines the logs and determines that one of the internet links at the site appears to be down. After the service provider confirms this information, the administrator fails over traffic to the backup link. Which of the following should the administrator do next?

A. Document the lessons learned.

B. Establish a plan of action.

C. Identify the problem.

D. Verify full system functionality.

Answer: (SHOW ANSWER)

After implementing the failover solution, you should confirm that all services and network paths are fully restored and operating correctly before closing the ticket.

NEW QUESTION: 18

A network architect is working on a physical network design template for a small education institution's satellite campus that is not yet built. The new campus location will consist of two small buildings with classrooms, one screening room with audiovisual equipment, and 200 seats for students. Which of the following enterprise network designs should the architect suggest?

A. Hybrid

B. Dual-layer

C. Three-tier

D. Collapsed core

Answer: D (LEAVE A REPLY)

In a small satellite campus with limited buildings and user density, a collapsed-core (two-tier) design combines the core and distribution layers into a single set of switches. This minimizes hardware, simplifies management, and still provides the necessary segmentation and resiliency for the classrooms, screening room, and student seating areas.

NEW QUESTION: 19

A network administrator receives a ticket from one of the company's offices about video calls that work normally for one minute and then get very choppy. The network administrator pings the video server from that site to ensure that it is reachable:

```
Ping 10.172.16.16
Pinging 10.172.16.16 with 32 bytes of data:
Reply from 10.172.16.16: bytes=32 time=40ms TTL=53
Reply from 10.172.16.16: bytes=32 time=11ms TTL=53
Reply from 10.172.16.16: bytes=32 time=672ms TTL=53
Reply from 10.172.16.16: bytes=32 time=111ms TTL=53
Reply from 10.172.16.16: bytes=32 time=117ms TTL=53
Reply from 10.172.16.16: bytes=32 time=849ms TTL=53
Reply from 10.172.16.16: bytes=32 time=34ms TTL=53
Reply from 10.172.16.16: bytes=32 time=92ms TTL=53
```

Which of the following ismostlikely the cause of the video call issue?

A. Throughput
B. Jitter
C. Latency
D. Loss
Answer: (SHOW ANSWER)
The wildly varying ping response times (from 11 ms up to 849 ms) indicate high packet-delay variation, which causes the video stream to become choppy after a short period. That fluctuation in latency is known as jitter.

NEW QUESTION: 20
Security policy states that all inbound traffic to the environment needs to be restricted, but all external outbound traffic is allowed within the hybrid cloud environment. A new application server was recently set up in the cloud. Which of the following would most likely need to be configured so that the server has the appropriate access set up? (Choose two.)
A. Application gateway
B. IPS
C. Port security
D. Firewall
E. Network security group
F. Screened subnet
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
To meet the requirement of restricting inbound traffic and allowing outbound traffic, two components are most appropriate:
D: Firewall - A firewall enforces ingress and egress traffic policies. It can be configured to deny all inbound traffic by default and allow all outbound traffic, meeting the security policy requirement.
E: Network Security Group (NSG) - In cloud environments such as Azure, NSGs serve as virtual firewalls at the subnet or interface level. NSGs allow you to define rules that block or allow inbound and outbound traffic, and they are the preferred method for enforcing network access rules for cloud resources.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Cloud Network Security Configuration":
"Network security groups and firewalls are key to enforcing inbound and outbound traffic restrictions in hybrid and public cloud environments."
"NSGs are used to define network access control policies for cloud resources at the subnet or NIC level." Other options:
* A. Application gateway controls HTTP/S traffic at Layer 7 but does not manage full access policy.
* B. IPS detects/prevents malicious behavior but is not primarily used for general traffic restriction.
* C. Port security restricts MAC addresses on switch ports, applicable in LANs, not cloud.

* F. A screened subnet (DMZ) can provide additional isolation but is not required for basic traffic control.

NEW QUESTION: 21
A company's IT department is expected to grow from 100 to 200 employees, and the sales department is expected to grow from 1,000 to a maximum of 2,000 employees. Each employee owns a single laptop with a single IP allocated. The network architect wants to deploy network segmentation using the IP range 10.0.0.0
/8. Which of the following is the best solution?
A. Allocate 10.1.0.0/30 to the IT department. Allocate 10.2.0.0/16 to the sales department.
B. Allocate 10.1.0.0/16 to the IT department. Allocate 10.2.1.0/24 to the sales department.
C. Allocate 10.1.0.0/22 to the IT department. Allocate 10.2.0.0/15 to the sales department.
D. Allocate 10.1.0.0/16 to the IT department. Allocate 10.2.1.0/25 to the sales department.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
To accommodate 200 devices in IT and 2,000 devices in Sales, subnetting must allow for appropriate address allocation:
* /22 provides 1,024 addresses # sufficient for IT (200 users)
* /15 provides 65,536 addresses # more than sufficient for Sales (2,000 users) Option C ensures both departments are placed in separate, appropriately sized segments within the private 10.0.0.0/8 range.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "IP Addressing and Subnetting":
"Proper subnetting ensures sufficient host addresses and supports future growth. Network segmentation improves manageability and security." Other options:
* A. /30 provides only 2 usable IPs - insufficient for IT.
* B & D: /24 and /25 do not support 2,000 users in Sales.
* B & D also misallocate resources inefficiently.

NEW QUESTION: 22
A partner is migrating a client from on-premises to a hybrid cloud. Given the following project status information, the initial project timeline estimates need to be revised:

Phase	Initial estimate	Current status
Discovery	1 month	2 months
Design	2 weeks	1 month
Implementation	6 months	9 months
Knowledge transfer	2 months	3 months

(Refer to image: Phases like Discovery, Design, Implementation, and Knowledge Transfer have all exceeded their initial estimated timelines.) Which of the following documents needs to be revised to best reflect the current status of the project?

A. BIA

B. SLA

C. SOW

D. WBS

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

The WBS (Work Breakdown Structure) is the document that outlines all project tasks, associated timelines, and deliverables. Since the project timeline has significantly deviated from its original estimates, updating the WBS will allow for accurate tracking, reallocation of resources, and setting new expectations. It directly reflects the phase durations and current project status.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Project and Lifecycle Documentation":

"A Work Breakdown Structure provides a detailed timeline and scope of project tasks. Revisions to WBS are essential when milestones or phase durations change significantly." Other options:

* A. BIA (Business Impact Analysis) deals with criticality, not project scheduling.
* B. SLA (Service Level Agreement) defines performance guarantees, not project phases.
* C. SOW (Statement of Work) outlines scope and deliverables but doesn't track current status or time spent.

NEW QUESTION: 23

A company deployed new applications in the cloud and configured a site-to-site VPN to connect the internal data center with the cloud. The IT team wants the internal servers to connect to those applications without using public IP addresses. Which of the following is thebestsolution?

A. Create a DNS server in the cloud. Configure the DNS server in the customer data center to forward DNS requests for cloud resources to the cloud DNS server.

B. Configure a NAT server on the cloud to allow internal servers to connect to the applications through the NAT server.

C. Register applications on the cloud with a public DNS sever and configure internal servers to connect to them using their public DNS names.

D. Configure proxy service in the site-to-site VPN to allow internal servers to access applications through the proxy.

Answer: A (LEAVE A REPLY)

By forwarding only the cloud application DNS queries to a cloud-hosted DNS zone that returns private IP addresses, your internal servers will resolve and connect over the site-to-site VPN without ever touching public IPs.

NEW QUESTION: 24

A network engineer is setting up guest access on a Wi-Fi network. After a recent network analysis, the engineer discovered that a user could access the guest network and attack the corporate network, since the networks share the same VLAN. Which of the following should the engineer do to prevent an attack like this one from happening?

A. Configure Layer 2 client isolation for the wireless network.

B. Set up a MAC filtering rule and add the MAC addresses of all corporate devices to the allow list.

C. Set up a strong password on the guest wireless network.

D. Set up a captive portal so all guest users have to register before gaining access to the wireless network.

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

Layer 2 client isolation ensures that devices connected to the same wireless network (such as a guest SSID) cannot communicate with each other or other VLANs. This prevents guest users from scanning or attacking internal devices. It's a fundamental security control for guest Wi-Fi access.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Wireless Network Segmentation and Security":

"Client isolation prevents peer-to-peer attacks over Wi-Fi by ensuring wireless clients cannot communicate with one another, a necessary control on shared guest networks." Other options:

* B. MAC filtering is easy to spoof and hard to manage at scale.
* C. Strong passwords improve access control but don't isolate guest traffic.
* D. Captive portals add a registration layer but don't address VLAN or broadcast isolation.

NEW QUESTION: 25

After a company migrated all services to the cloud, the security auditor discovers many users have administrator roles on different services. The company needs a solution that:

Protects the services on the cloud.

Limits access to administrative roles.

Creates a policy to approve requests for administrative roles on critical services within a limited time.

Forces password rotation for administrative roles.

Audits usage of administrative roles.

Which of the following is the best way to meet the company's requirements?

A. Privileged access management

B. Session-based token

C. Conditional access

D. Access control list

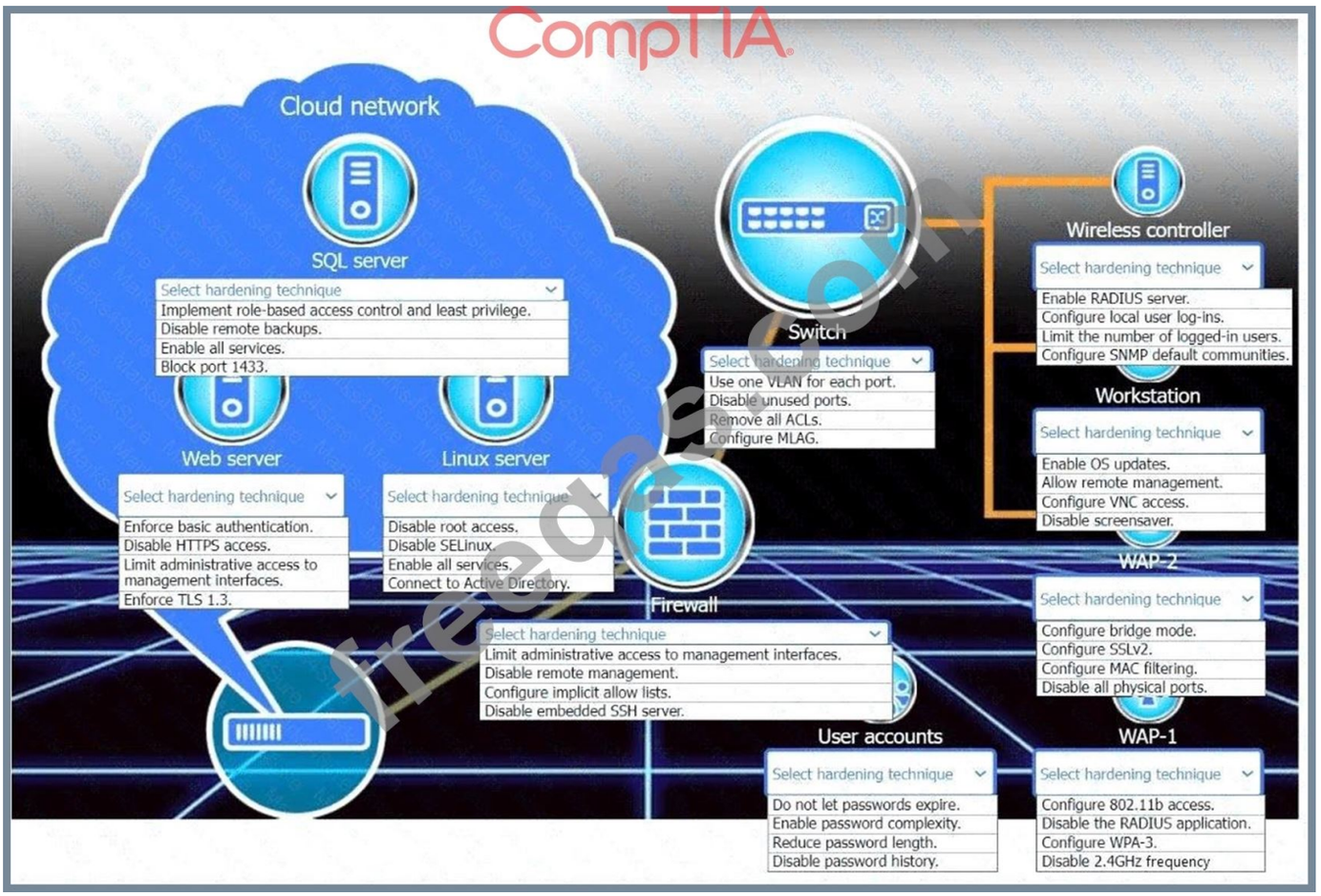
Answer: A (LEAVE A REPLY)

A Privileged Access Management (PAM) solution provides just-in-time elevation to administrative roles, enforces approval workflows with time-bound access, requires credential rotation, and

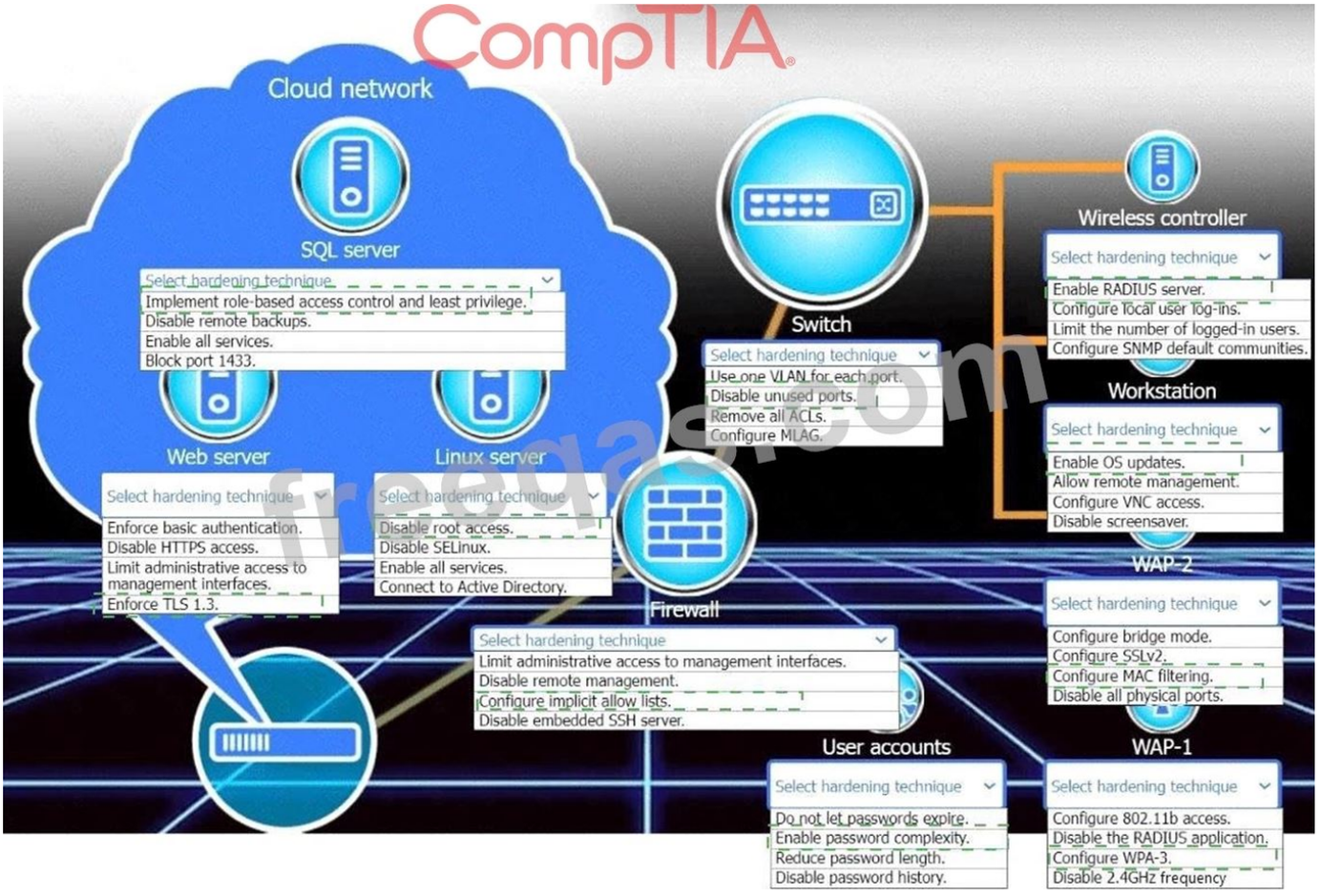
offers comprehensive auditing of all privileged sessions, fully meeting the company's requirements.

NEW QUESTION: 26
A network engineer is establishing a wireless network for handheld inventory scanners in a manufacturing company's warehouse. The engineer needs an authentication mechanism for these scanners that uses the Wi-Fi network and works with the company's Active Directory. The business requires that the solution authenticate the users and authorize the scanners. Which of the following provides the best solution for authentication and authorization?
A. TACACS+
B. RADIUS
C. LDAP
D. PKI
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
RADIUS (Remote Authentication Dial-In User Service) is the best-fit protocol for this requirement. It supports both authentication and authorization and is widely used in Wi-Fi network environments for client device authentication using credentials stored in centralized directories such as Active Directory.
RADIUS integrates seamlessly with enterprise authentication sources and supports EAP (Extensible Authentication Protocol), making it compatible with Wi-Fi-based client devices. It also allows for role-based access control, enabling policy enforcement specific to device types (e.g., inventory scanners).
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - "Authentication and Authorization Technologies":
"RADIUS provides centralized authentication, authorization, and accounting (AAA) services and is commonly used for securing wireless access in conjunction with Active Directory."
"Organizations use RADIUS to manage Wi-Fi authentication for user devices and enforce security policies during access attempts." Using a RADIUS server with 802.1X on the Wi-Fi infrastructure allows the scanners (and their users) to be authenticated against Active Directory and mapped to the correct authorization policies. TACACS+ is geared toward device management, LDAP alone doesn't handle the Wi-Fi 802.1X handshake, and PKI by itself wouldn't provide the user-to-device authorization flow needed. RADIUS gives you both authentication and authorization tied into AD.

NEW QUESTION: 27
New devices were deployed on a network and need to be hardened.
INSTRUCTIONS
Use the drop-down menus to define the appliance-hardening techniques that provide themostsecure solution.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

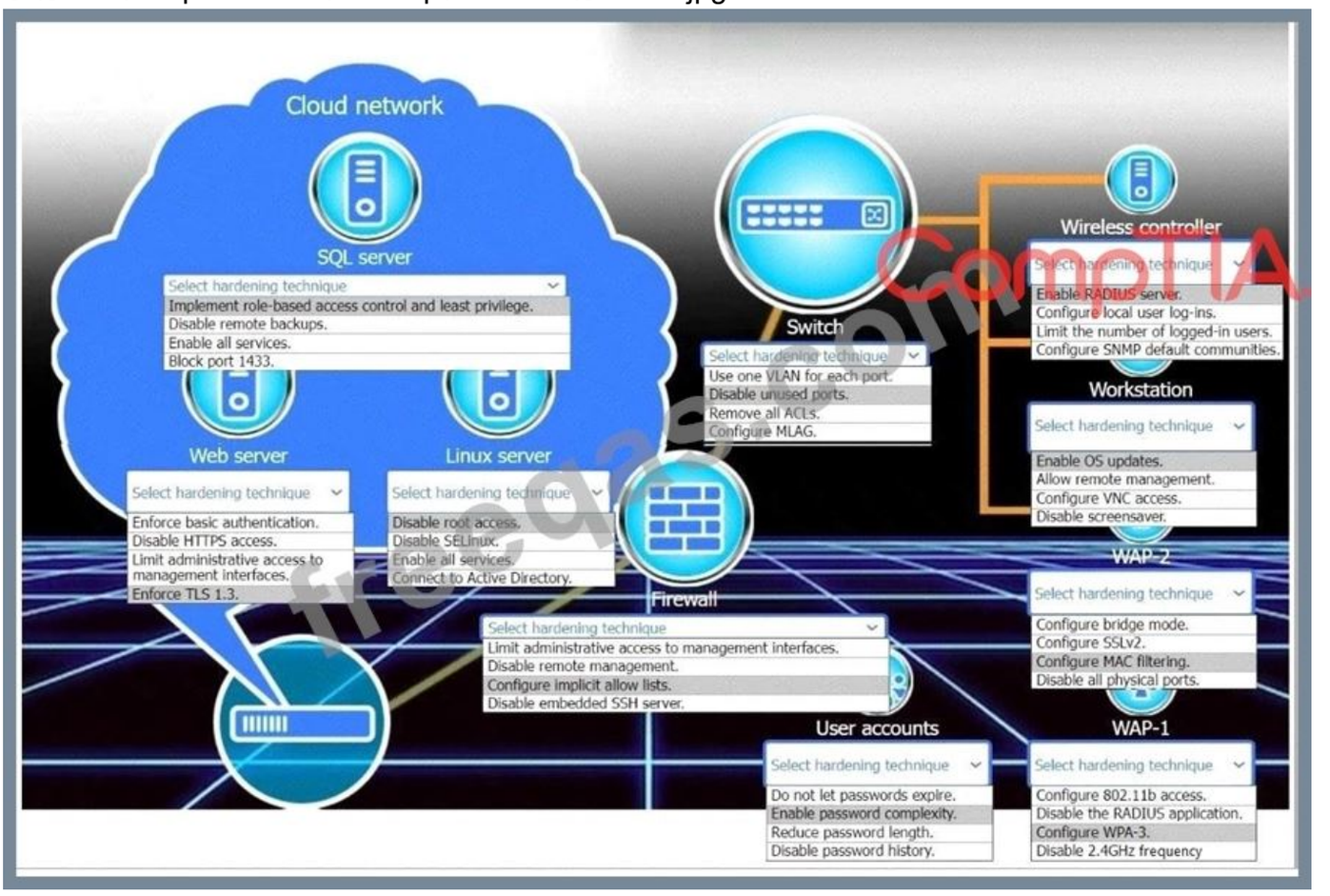

CompTIA
Cloud network
SQL server
Select hardening technique
Implement role-based access control and least privilege.
Disable remote backups.
Enable all services.
Block port 1433.
Web server
Select hardening technique
Enforce basic authentication.
Disable HTTPS access.
Limit administrative access to management interfaces.
Enforce TLS 1.3.
Linux server
Select hardening technique
Disable root access.
Disable SELinux.
Enable all services.
Connect to Active Directory.
Switch
Select hardening technique
Use one VLAN for each port.
Disable unused ports.
Remove all ACLs.
Configure MLAG.
Wireless controller
Select hardening technique
Enable RADIUS server.
Configure local user log-ins.
Limit the number of logged-in users.
Configure SNMP default communities.
Workstation
Select hardening technique
Enable OS updates.
Allow remote management.
Configure VNC access.
Disable screensaver.
WAP-2
Select hardening technique
Configure bridge mode.
Configure SSLv2.
Configure MAC filtering.
Disable all physical ports.
WAP-1
Select hardening technique
Configure 802.11b access.
Disable the RADIUS application.
Configure WPA-3.
Disable 2.4GHz frequency
Firewall
Select hardening technique
Limit administrative access to management interfaces.
Disable remote management.
Configure implicit allow lists.
Disable embedded SSH server.
User accounts
Select hardening technique
Do not let passwords expire.
Enable password complexity.
Reduce password length.
Disable password history.

Answer:


CompTIA
Cloud network
SQL server
Select hardening technique
Implement role-based access control and least privilege.
Disable remote backups.
Enable all services.
Block port 1433.
Web server
Select hardening technique
Enforce basic authentication.
Disable HTTPS access.
Limit administrative access to management interfaces.
Enforce TLS 1.3.
Linux server
Select hardening technique
Disable root access.
Disable SELinux.
Enable all services.
Connect to Active Directory.
Switch
Select hardening technique
Use one VLAN for each port.
Disable unused ports.
Remove all ACLs.
Configure MLAG.
Wireless controller
Select hardening technique
Enable RADIUS server.
Configure local user log-ins.
Limit the number of logged-in users.
Configure SNMP default communities.
Workstation
Select hardening technique
Enable OS updates.
Allow remote management.
Configure VNC access.
Disable screensaver.
WAP-2
Select hardening technique
Configure bridge mode.
Configure SSLv2.
Configure MAC filtering.
Disable all physical ports.
WAP-1
Select hardening technique
Configure 802.11b access.
Disable the RADIUS application.
Configure WPA-3.
Disable 2.4GHz frequency
Firewall
Select hardening technique
Limit administrative access to management interfaces.
Disable remote management.
Configure implicit allow lists.
Disable embedded SSH server.
User accounts
Select hardening technique
Do not let passwords expire.
Enable password complexity.
Reduce password length.
Disable password history.

Explanation:

C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg



NEW QUESTION: 28

A network architect is choosing design options for a new SD-WAN installation that has the following requirements:

All network traffic from the cloud must pass through inspection devices in a dedicated data center.

Ensure redundancy.

Centralize egress traffic.

Which of the following network topologies best meets these requirements?

A. Point-to-point

B. Hub-and-spoke

C. Partial mesh

D. Star

Answer: B (LEAVE A REPLY)

A hub-and-spoke design sends all branch and cloud traffic into the central hub (your data center) for inspection, then back out, meeting the requirement for centralized egress and security inspection. By deploying multiple hub nodes and using dynamic path selection, you also achieve redundancy without losing the centralized control plane.

NEW QUESTION: 29

A network administrator recently deployed new Wi-Fi 6E access points in an office and enabled 6GHz coverage. Users report that when they are connected to the new 6GHz SSID, the performance is worse than the 5GHz SSID. The network administrator suspects that there is a source of 6GHz interference in the office.
Using the troubleshooting methodology, which of the following actions should the network administrator do next?
A. Test to see if the changes have improved network performance.
B. Use a spectrum analyzer and check the 6GHz spectrum.
C. Document the list of channels that are experiencing interference.
D. Change the channels being used by the 6GHz radios in the APs.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Using a spectrum analyzer to inspect the 6GHz frequency range allows the administrator to confirm the presence and source of interference. This step aligns with the "identify the problem" phase of the CompTIA troubleshooting methodology. Before making changes or documenting channels, the administrator must validate whether interference exists and collect diagnostic data.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Troubleshooting Methodology and Wireless Interference":
"Spectrum analyzers provide a visual representation of frequency usage and interference in wireless bands, allowing administrators to isolate the root cause of degraded performance before implementing corrective actions." Other options:
* A. Testing performance (Step 5 in the methodology) comes after identifying and resolving the issue.
* C. Documentation is performed during the final step of troubleshooting.
* D. Changing channels without evidence may worsen interference if the problem is not confirmed.

NEW QUESTION: 30
A cafe uses a tablet-based point-of-sale system. Customers are complaining that their food is taking too long to arrive. During an investigation, the following is noticed:
Every kitchen printer did not print the orders.
Payments are processing correctly.
The cloud-based system has record of the orders.
This issue occurred when the cafe was busy.
Which of the following is the best way to mitigate this issue?
A. Updating the application
B. Adding an access point exclusively for the kitchen
C. Upgrading the kitchen printers' wireless dongles
D. Assigning the kitchen printers static IP addresses
Answer: (SHOW ANSWER)

By dedicating a separate Wi-Fi access point to the printers, you isolate their traffic from the customer-facing tablets. This prevents congestion during busy periods, ensuring orders reliably print even when the main network is under heavy load.

NEW QUESTION: 31
A company is replacing reserved public IP addresses with dynamic IP addresses. The network architect creates a list of assets with some dependencies to these reserved IPs:

IP	Used by
IP_US_Reserved_A	Allow rule on NSG_1
IP_CA_Reserved_B	Allow rule on NSG_2
IP_BR_Reserved_C	VM A - Network Interface 1
IP_BR_Reserved_D	Network Load Balancer IP 1
IP_GB_Reserved_E	Not allocated

Which of the following issues may begin to affect cloud assets after the replacement is made?
A. IP asymmetric routing
B. IP spoofing
C. IP exhaustion
D. IP reuse
Answer: D (LEAVE A REPLY)
Once you switch those public IPs from reserved (static) to dynamic, the cloud provider can reassign them to other tenants as soon as you deallocate. That "reuse" can lead to unexpected conflicts and broken security rules (for example your NSG allow lists still pointing to the old IPs might suddenly open traffic to an unrelated resource).

NEW QUESTION: 32
Security policy states that all inbound traffic to the environment needs to be restricted, but all external outbound traffic is allowed within the hybrid cloud environment. A new application server was recently set up in the cloud. Which of the following would most likely need to be configured so that the server has the appropriate access set up? (Choose two.)

A. Application gateway
B. IPS
C. Port security
D. Firewall
E. Network security group
F. Screened subnet
Answer: D,E (LEAVE A REPLY)
A perimeter firewall enforces the organization's "deny inbound by default, allow all outbound" policy at the edge of the cloud environment, while an Azure-style NSG applies the same rule set at the VM/subnet level.
Together they ensure no inbound connections slip through and that outbound traffic remains unrestricted.

NEW QUESTION: 33
Server A (10.2.3.9) needs to access Server B (10.2.2.7) within the cloud environment since they are segmented into different network sections. All external inbound traffic must be blocked to those servers.
Which of the following need to be configured to appropriately secure the cloud network? (Choose two.)
A. Network security group rule:
allow 10.2.3.9 to 10.2.2.7
B. Network security group rule:
allow 10.2.0.0/16 to 0.0.0.0/0
C. Network security group rule:
deny 0.0.0.0/0 to 10.2.0.0/16
D. Firewall rule:
deny 10.2.0.0/16 to 0.0.0.0/0
E. Firewall rule:
allow 10.2.0.0/16 to 0.0.0.0/0
F. Network security group rule:
deny 10.2.0.0/16 to 0.0.0.0/0
Answer: A,C (LEAVE A REPLY)
Network security group rule: allow 10.2.3.9 to 10.2.2.7
Explicitly permits Server A's IP to reach Server B.
Network security group rule: deny 0.0.0.0/0 to 10.2.0.0/16
Blocks all inbound traffic from any external source into the 10.2.0.0/16 address space, ensuring no external access.

NEW QUESTION: 34
A network architect must design a new branch network that meets the following requirements:
* No single point of failure

* Clients cannot be impacted by changes to the underlying medium
* Clients must be able to communicate directly to preserve bandwidth
Which of the following network topologies should the architect use?
A. Hub-and-spoke
B. Mesh
C. Spine-and-leaf
D. Star
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A Mesh topology provides multiple redundant paths between all nodes, ensuring there is no single point of failure. Clients can communicate directly with each other without passing through a central hub, reducing bottlenecks and preserving bandwidth. Mesh networks are fault tolerant and resilient to changes in the underlying medium, making them ideal for distributed environments requiring high availability.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "WAN and LAN Topologies":
"In a mesh topology, every device is connected to every other device. This design offers fault tolerance and allows for direct communication paths between endpoints, maximizing bandwidth efficiency and eliminating single points of failure." Other options:
* A. Hub-and-spoke introduces a central point of failure and may limit bandwidth.
* C. Spine-and-leaf is ideal for data centers but not typically used for branch office designs.
* D. Star topology relies on a central switch and has a single point of failure.

NEW QUESTION: 35
A network architect needs to build a new data center for a large company that has business units that process retail financial transactions. Which of the following information should the architect request from the company?
A. Regulatory requirements
B. Statement of work
C. Business case study
D. Internal reference architecture
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
When building infrastructure for business units that process financial transactions (such as in the retail or banking sector), the architect must first understand all relevant compliance and regulatory requirements.
These may include PCI DSS, SOX, or GDPR, depending on the nature of the data and jurisdiction. These regulations influence design decisions regarding encryption, segmentation, data retention, and logging.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Compliance and Regulatory Considerations":

"Regulatory requirements such as PCI DSS, HIPAA, and others dictate the security controls, logging, data protection, and architectural design of infrastructure handling sensitive or financial data." Other options:
* B. Statement of Work defines project scope, but doesn't include legal/compliance mandates.
* C. Business case studies illustrate value or ROI, not security or compliance needs.
* D. Internal reference architectures may help with standards but are based on already defined requirements.

NEW QUESTION: 36
A cafe uses a tablet-based point-of-sale system. Customers are complaining that their food is taking too long to arrive. During an investigation, the following is noticed:
* Every kitchen printer did not print the orders
* Payments are processing correctly
* The cloud-based system has record of the orders
* This issue occurred when the cafe was busy
Which of the following is the best way to mitigate this issue?
A. Updating the application
B. Adding an access point exclusively for the kitchen
C. Upgrading the kitchen printers' wireless dongles
D. Assigning the kitchen printers static IP addresses
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Since payments are working and orders are being recorded in the cloud, the issue likely lies in the local wireless network between the tablets and the kitchen printers. If the issue only occurs during high usage periods, it's likely a congestion or signal quality issue. Adding a dedicated access point for the kitchen can isolate printer traffic and improve reliability.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Wireless Performance and Interference Management":
"Segmenting traffic or deploying dedicated APs for mission-critical devices can reduce contention and ensure reliability in congested wireless environments." Other options:
* A. App updates won't fix wireless interference.
* C. Dongle upgrades may help but don't isolate the traffic.
* D. Static IPs help with addressing, not with wireless reliability.

NEW QUESTION: 37
A network architect is choosing design options for a new SD-WAN installation that has the following requirements:
* All network traffic from the cloud must pass through inspection devices in a dedicated data center.
* Ensure redundancy.
* Centralize egress traffic.

Which of the following network topologies best meets these requirements?

A. Point-to-point

B. Hub-and-spoke

C. Star

D. Partial mesh

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

The Hub-and-Spoke topology is ideal for SD-WAN environments where traffic from branch offices or cloud workloads must route through a central location (the hub) for inspection, monitoring, or security enforcement.

This structure centralizes egress and allows for redundant spoke paths via the hub. It also simplifies control and enforces compliance policies.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "SD-WAN Topologies and Cloud Egress Strategies":

"In a hub-and-spoke topology, spokes (remote offices or cloud nodes) connect through a central hub, allowing for centralized egress, traffic inspection, and simplified routing." Other options:

* A. Point-to-point doesn't scale and lacks centralized control.
* C. Star topology is similar to hub-and-spoke but is more rigid and less suited for SD-WAN scalability.
* D. Partial mesh allows direct spoke-to-spoke communication, bypassing centralized inspection.

NEW QUESTION: 38

A company has a 40Gbps network that uses a network tap to inspect the traffic using an IDS. The IDS usually performs normally except when the servers are downloading patches from their local update repository

10.10.10.139 using HTTPS. During the patch windows, the IDS cannot handle the extra load and drops a significant number of packets. Which of the following would allow a network engineer to prevent this issue without compromising the network visibility?

A. Configuring the IDS to ignore traffic from 10.10.10.139

B. Using PF_RING offload to filter out "host 10.10.10.139 and port 443"

C. Adding a "dst host 10.10.10.139" BPF on the tap

D. Scheduling a cron job to stop the IDS service during the patch window

Answer: C (LEAVE A REPLY)

By applying a Berkeley Packet Filter to drop only the HTTPS patch#repo traffic before it reaches the IDS, you relieve the processing burden during patch windows while preserving full visibility for all other flows.

This avoids reconfiguring the IDS itself or losing visibility across the rest of the network.

NEW QUESTION: 39

A network administrator is configuring firewall rules to lock down the network from outside attacks. Which of the following should the administrator configure to create the most strict set of rules?

A. URL filtering

B. File blocking

C. Network security group

D. Allow List

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From Exact Extract:

An Allow List (also known as Whitelisting) is the most restrictive firewall rule approach. It blocks all traffic by default and only permits explicitly defined trusted IPs, URLs, or applications. This minimizes the attack surface and ensures that only known, safe traffic is allowed into the network.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Firewall and Security Rule Configuration":

"Whitelisting or Allow Listing enforces a default-deny security posture by permitting only specified trusted sources. This approach offers the highest level of control and reduces exposure to unknown threats." Other options:

* A. URL filtering restricts content access but is not as strict as allow lists.
* B. File blocking targets malicious payloads but doesn't limit traffic sources.
* C. Network Security Groups (NSGs) are effective but broader in scope; they use allow/deny rules but may not be as tightly controlled as explicit allow lists.

NEW QUESTION: 40

A network engineer is working on securing the environment in the screened subnet. Before penetration testing, the engineer would like to run a scan on the servers to identify the OS, application versions, and open ports. Which of the following commands should the engineer use to obtain the information?

A. tcpdump -ni eth0 src net 10.10.10.0/28

B. nmap -A 10.10.10.0/28

C. nc -v -n 10.10.10.x 1-1000

D. hping3 -1 10.10.10.x -rand-dest -I eth0

Answer: (SHOW ANSWER)

The -A flag enables aggressive scanning, which combines OS detection, version detection, script scanning, and traceroute to give you detailed information on hosts in the 10.10.10.0/28 range.

NEW QUESTION: 41

A network architect needs to design a solution to ensure every cloud environment network is built to the same baseline. The solution must meet the following requirements:

* Use automated deployment.
* Easily update multiple environments.
* Share code with a community of practice.

Which of the following are the best solutions? (Choose two.)
A. CI/CD pipelines
B. Public code repository
C. Deployment runbooks
D. Private code repository
E. Automated image deployment
F. Deployment guides
Answer: A,B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A: CI/CD pipelines - Continuous Integration and Continuous Deployment (CI/CD) pipelines allow automated and repeatable deployments of infrastructure and application code. This ensures consistency across environments and supports rapid, reliable updates to multiple environments simultaneously.
B: Public code repository - A public repository (e.g., GitHub, GitLab public projects) allows sharing code with the broader community of practice, enabling collaboration, peer review, and reuse. It supports version control and standardized deployment scripts (e.g., Terraform, Ansible).
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Infrastructure as Code and Automation Pipelines":
"CI/CD pipelines enable automated, consistent deployments across environments, reducing manual configuration errors."
"Public repositories facilitate code sharing and collaboration, supporting standardized infrastructure templates." Other options:
* C. Deployment runbooks are static and not inherently automated.
* D. Private repositories restrict sharing, conflicting with the requirement to share code.
* E. Image deployment refers to server builds, not full network configuration.
* F. Deployment guides are manual documents, not automation tools.

NEW QUESTION: 42
A company is expanding operations and opening a new facility. The executive leadership team decides to purchase an insurance policy that will cover the cost of rebuilding the facility in case of a natural disaster.
Which of the following describes the team's decision?
A. Business continuity
B. Disaster recovery
C. Risk transference
D. Memorandum of understanding
Answer: C (LEAVE A REPLY)
By purchasing an insurance policy, the company shifts the financial burden of rebuilding after a natural disaster to the insurer, which is the essence of risk transference.

NEW QUESTION: 43

A cloud architect needs to change the network configuration at a company that uses GitOps to document and implement network changes. The Git repository uses main as the default branch, and the main branch is protected. Which of the following should the architect do after cloning the repository?

A. Use the main branch to make and commit the changes back to the remote repository.

B. Create a new branch for the change, then create a pull request including the changes.

C. Check out the development branch, then perform and commit the changes back to the remote repository.

D. Rebase the remote main branch after making the changes to implement.

Answer: B (LEAVE A REPLY)

Because main is protected, you must make your network-configuration edits on a separate feature branch and submit them via a pull request. This preserves the integrity of the protected branch and aligns with GitOps best practices for change review and automated deployment.

NEW QUESTION: 44

A company is experiencing multiple switch failures. The network analyst discovers the following:

Network recovery time is unacceptable and occurs after the shutdown of some switches.

Some loops were detected in the network.

No broadcast storm was detected.

Which of the following is the most cost-effective solution?

A. Add a new Layer 3 switch.

B. Add multiple VLANs.

C. Implement STP.

D. Implement tagging.

Answer: C (LEAVE A REPLY)

Spanning Tree Protocol prevents and automatically resolves layer-2 loops without requiring new hardware. It also improves convergence times after a link or switch failure, meeting the recovery and loop-avoidance requirements most cost-effectively.

NEW QUESTION: 45

A network administrator must connect a remote building at a manufacturing plant to the main building via a wireless connection. Which of the following should the administrator choose to get thegreatestpossible range from the wireless connection? (Choose two.)

A. 2.4GHz

B. 5GHz

C. 6GHz

D. Omnidirectional antenna

E. Patch antenna

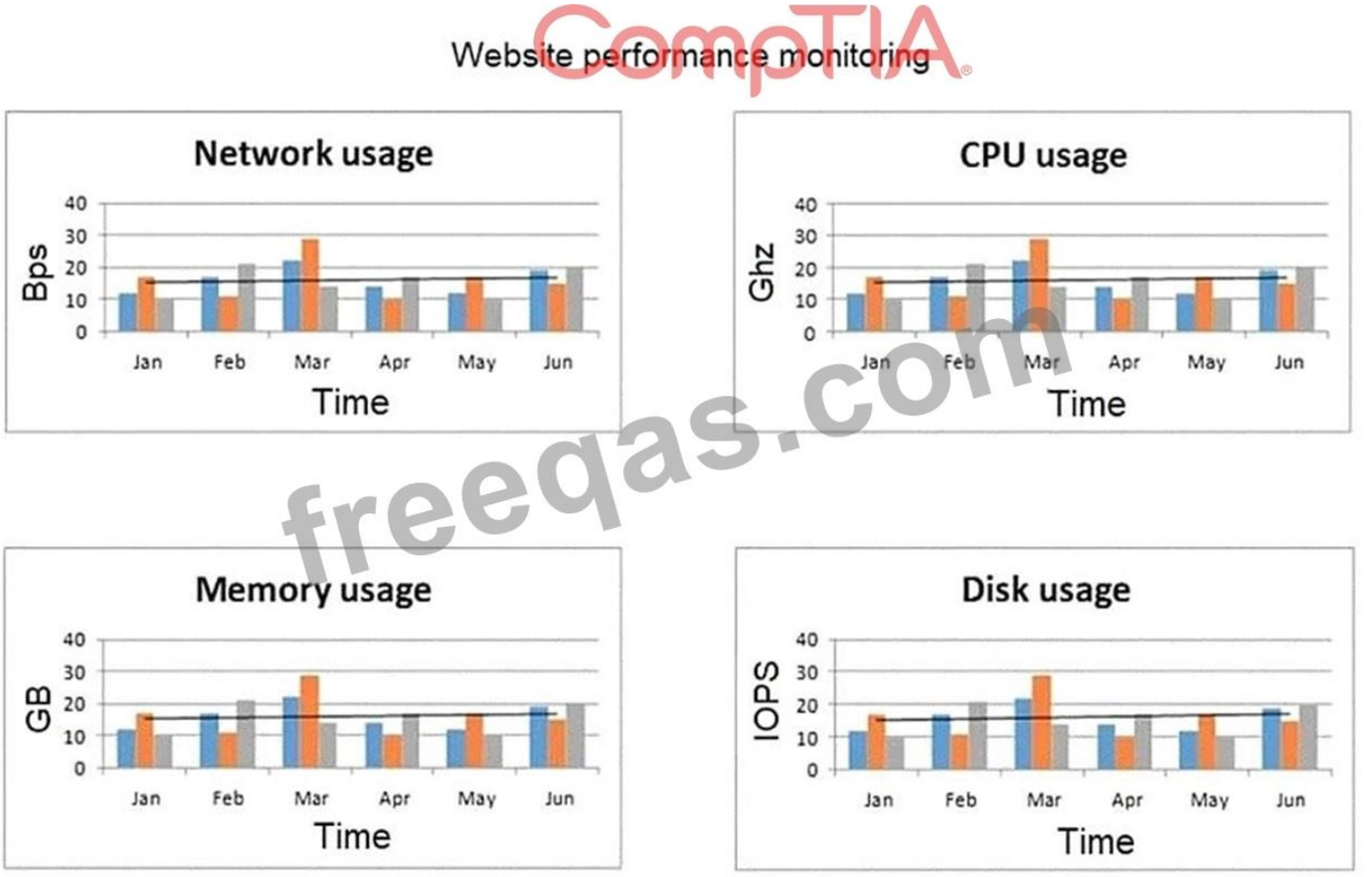
F. Built-in antenna

Answer: A,E (LEAVE A REPLY)

2.4 GHz: The lower-frequency 2.4 GHz band propagates farther and better penetrates obstacles than 5 GHz or
6 GHz, giving you greater link distance.
Patch antenna: A directional (patch) antenna focuses RF energy into a narrow beam, maximizing gain and range between two fixed points - the best for a long-haul wireless link.

NEW QUESTION: 46
A network architect needs to build a new data center for a large company that has business units that process retail financial transactions. Which of the following information should the architect request from the company?
A. Regulatory requirements
B. Statement of work
C. Business case study
D. Internal reference architecture
Answer: A (LEAVE A REPLY)
Before designing a facility that will handle retail financial transactions, you need to understand all applicable compliance and security mandates (e.g. PCI DSS, SOX, GDPR). Those regulatory requirements will drive your choices around physical security, network segmentation, encryption, logging, redundancy, and operational controls, ensuring the data center meets its legal and industry-specific obligations.

NEW QUESTION: 47
A network engineer at an e-commerce organization must improve the following dashboard due to a performance issue on the website:
(Refer to the image: Website performance monitoring dashboard showing metrics like network usage, CPU usage, memory usage, and disk usage over time.)



Which of the following is the most useful information to add to the dashboard for the operations team?

A. 404 errors

B. Concurrent users

C. Number of orders

D. Number of active incidents

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation From Exact Extract:

While resource usage metrics (CPU, memory, disk, network) are important, the missing context here is user demand. Adding "Concurrent users" helps correlate resource utilization spikes with actual user load. For performance monitoring in web applications, concurrent sessions provide crucial insight into whether performance issues are demand-related.

Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Performance Monitoring and User Metrics":

"Monitoring user load metrics such as concurrent users provides insight into performance degradation and capacity planning. These are critical for identifying thresholds and auto-scaling requirements." Other options:

* A. 404 errors indicate broken links but don't explain performance issues.
* C. Number of orders tracks business activity, not system strain.
* D. Active incidents belong in an ITSM system, not real-time performance monitoring.

NEW QUESTION: 48

A network architect is designing an expansion solution for the branch office network and requires the following business outcomes:
* Maximize cost savings with reduced administration overhead
* Easily expand connectivity to the cloud
* Use cloud-based services to the branch offices
Which of the following should the architect do to best meet the requirements?
A. Design a SD-WAN solution to integrate with the cloud provider; use SD-WAN to connect branch offices to the cloud provider.
B. Design point-to-site branch connectivity for offices to headquarters; deploy ExpressRoute and/or DirectConnect between headquarters and the cloud; use headquarters connectivity to connect to the cloud provider.
C. Design an MPLS architecture for the branch offices and site-to-site VPN between headquarters and branch offices; use site-to-site connectivity to the cloud provider.
D. Design a dark fiber solution for headquarters and branch offices' connectivity; deploy point-to-site VPN between headquarters and the cloud provider; use the headquarters connectivity to the cloud provider.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
SD-WAN (Software-Defined Wide Area Networking) is ideal for enterprises that want to simplify WAN management, reduce operational overhead, and optimize connectivity to cloudservices. SD-WAN provides intelligent traffic routing, dynamic path selection, and direct-to-cloud access without backhauling traffic through a central data center.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "SD-WAN and Cloud Connectivity":
"SD-WAN enables efficient cloud access from branch offices and simplifies management through centralized policy control. It is cost-effective and reduces the need for complex hardware configurations and manual routing." Other options:
* B. Adds latency and overhead by backhauling through headquarters.
* C. MPLS is expensive and less flexible than SD-WAN.
* D. Dark fiber is high-cost and not scalable for cloud-first architectures.

NEW QUESTION: 49
A company hosts a cloud-based e-commerce application and only wants the application accessed from certain locations. The network team configures a cloud firewall with WAF enabled, but users can access the application globally. Which of the following should the network team do?
A. Reconfigure WAF rules.
B. Configure a NAT gateway.
C. Implement a CDN.
D. Configure geo-restriction.
Answer: D (LEAVE A REPLY)

Geo-restriction lets you block or allow traffic based on the requester's geographic region, preventing access from locations you haven't authorized.

NEW QUESTION: 50
An organization with an on-premises data center is adopting additional cloud-based solutions. The organization wants to keep communication secure between remote employees' devices and workloads. Which of the following ZTA featuresbestachieves this goal?
A. Secure service edge
B. Cloud access security broker
C. Principle of least privilege
D. Identity as the perimeter
Answer: (SHOW ANSWER)
Shifting to "identity as the perimeter" means that each remote user and device's identity (and context) becomes the basis for granting secure, encrypted access directly to workloads, regardless of the underlying network, ensuring communications are authenticated and authorized per-session.

NEW QUESTION: 51
A company is expanding operations and opening a new facility. The executive leadership team decides to purchase an insurance policy that will cover the cost of rebuilding the facility in case of a natural disaster.
Which of the following describes the team's decision?
A. Business continuity
B. Disaster recovery
C. Risk transference
D. Memorandum of understanding
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
Risk transference is a risk management strategy in which the financial impact of a risk is shifted to a third party, such as an insurance company. In this scenario, the purchase of an insurance policy to cover potential damage or loss from a natural disaster is an example of transferring risk, not avoiding, mitigating, or accepting it.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide under "Risk Management Concepts":
"Risk transference involves moving the responsibility or financial burden of a risk to a third party, often through the purchase of insurance or third-party service agreements." This approach is contrasted with mitigation (reducing risk), acceptance (living with the risk), or avoidance (eliminating the risk).

NEW QUESTION: 52

A company is replacing reserved public IP addresses with dynamic IP addresses. The network architect creates a list of assets with some dependencies to these reserved IPs:

IP	Used by
IP_US_Reserved_A	Allow rule on NSG_1
IP_CA_Reserved_B	Allow rule on NSG_2
IP_BR_Reserved_C	VM A - Network Interface 1
IP_BR_Reserved_D	Network Load Balancer IP 1
IP_GB_Reserved_E	Not allocated

(Refer to image: Reserved IPs are in use by NSGs, VMs, load balancers, and one is unallocated.)
Which of the following issues may begin to affect cloud assets after the replacement is made?

A. IP asymmetric routing

B. IP spoofing

C. IP exhaustion

D. IP reuse

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From Exact Extract:
Replacing reserved IPs with dynamic ones can lead to IP reuse issues. Dynamic public IPs can be reallocated to other customers once released. If DNS entries or firewall rules still refer to the original IP, this can lead to data leakage or incorrect routing. Also, some services (e.g., NSGs, load balancers) may require persistent IPs.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Public IP Management in Cloud Environments":
"Dynamic public IPs are subject to reuse after release. Services that rely on IP persistence, such as security groups or load balancers, may encounter unexpected behavior or security risks if replaced with dynamically assigned IPs." Other options:
* A. Asymmetric routing involves traffic leaving and returning via different paths.
* B. IP spoofing is a malicious attack, not related to address reassignment.
* C. IP exhaustion relates to resource limits, not dynamic reuse.

NEW QUESTION: 53

A global company has depots in various locations. A proprietary application was deployed locally at each of the depots, but issues with getting the consolidated data instantly occurred. The Chief Information Officer decided to centralize the application and deploy it in the cloud. After the cloud deployment, users report the application is slow. Which of the following is most likely the issue?

A. Throttling

B. Overutilization

C. Packet loss

D. Latency

Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
When an application is moved from local deployment to a centralized cloud deployment, remote users must connect over the WAN. If the application is sensitive to delays, latency becomes a significant issue, especially across geographically distributed regions. This is a common performance concern for centralized applications serving remote offices.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Cloud Performance and WAN Connectivity":
"Cloud-hosted applications accessed by remote users may suffer from latency-related performance issues.
Optimization strategies may include CDN, caching, or edge deployment."
Other options:
* A. Throttling usually refers to bandwidth or rate-limiting, not general slowness.
* B. Overutilization is possible, but infrastructure was said to be centralized and new.
* C. Packet loss would likely cause disconnects or failures, not just slowness.

NEW QUESTION: 54
A company is migrating an application to the cloud for modernization. The engineer needs to provide dependencies between application and database tiers in the environment. Which of the following should the engineer reference in order to best meet this requirement?
A. Internal knowledge base article
B. CMDB
C. WBS
D. Diagram of physical server locations
E. SOW
Answer: B (LEAVE A REPLY)
A Configuration Management Database (CMDB) explicitly maps and documents the relationships and dependencies among configuration items, such as your application and database tiers, making it the ideal reference when migrating to the cloud.

NEW QUESTION: 55
A network architect is working on a new network design to better support remote and on-campus workers.
Traffic needs to be decrypted for inspection in the cloud but is not required to go through the company's data center. Which of the following technologies best meets these requirements?
A. Secure web gateway
B. Transit gateway
C. Virtual private network
D. Intrusion prevention system
E. Network access control system
Answer: A (LEAVE A REPLY)

A cloud-delivered Secure Web Gateway can terminate and decrypt user HTTPS sessions directly in the cloud for policy enforcement and inspection without hair-pinning traffic back through the data center.

NEW QUESTION: 56
A network engineer adds a large group of servers to a screened subnet and configures them to use IPv6 only.
The servers need to seamlessly communicate with IPv4 serverson the internal networks. Which of the following actions is the best way to achieve this goal?
A. Add IPv6 to the network cards on the internal servers so they can communicate with the screened subnet.
B. Set up a bridge between the screened subnet and internal networks to handle the conversion.
C. Change the servers in the screened subnet from IPv6 addresses to IPv4 addresses.
D. Implement NAT64 on the router between the screened subnet and the internal network.
Answer: D (LEAVE A REPLY)
NAT64 provides automatic protocol translation between IPv6-only clients and IPv4-only servers at the router, letting your new IPv6-only servers communicate seamlessly with existing IPv4 resources without changing their addresses.

NEW QUESTION: 57
A company is migrating an application to the cloud for modernization. The engineer needs to provide dependencies between application and database tiers in the environment. Which of the following should the engineer reference in order to best meet this requirement?
A. Internal knowledge base article
B. CMDB
C. WBS
D. Diagram of physical server locations
E. SOW
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation From Exact Extract:
A CMDB (Configuration Management Database) is a centralized repository used to store information about IT assets and their relationships, including configuration items such as servers, applications, and databases. It provides visibility into dependencies between infrastructure components, including application and database tiers. This is essential for cloud migration and modernization projects where understanding interdependencies ensures accurate planning and reduces risks.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under the "Infrastructure Documentation and Planning" domain:
"CMDBs are used to track asset relationships, allowing network and systems engineers to visualize and manage dependencies between services, applications, and infrastructure components critical for change management and cloud migration." Other options:

* A. Internal knowledge base articles may offer general guidance but not structured dependency mapping.
* C. WBS (Work Breakdown Structure) outlines tasks and deliverables, not technical dependencies.
* D. Physical server diagrams are not relevant in virtualized/cloud environments.
* E. SOW (Statement of Work) defines project scope but lacks infrastructure-level detail.

NEW QUESTION: 58
A network administrator is troubleshooting an outage at a remote site. The administrator examines the logs and determines that one of the internet links at the site appears to be down. After the service provider confirms this information, the administrator fails over traffic to the backup link. Which of the following should the administrator do next?
A. Document the lessons learned.
B. Establish a plan of action.
C. Identify the problem.
D. Verify full system functionality.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation From Exact Extract:
According to the standard CompTIA troubleshooting methodology, once the issue has been identified and a solution has been implemented (e.g., failing over traffic to the backup link), the next logical step is to verify full system functionality. This ensures that the backup path is working as intended and that services have resumed properly for the users.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "Troubleshooting Process":
"After implementing the solution, it is critical to verify full system functionality to ensure the resolution has addressed the problem without causing unintended consequences." Other options:
* A. Documenting lessons learned is the final step.
* B. The plan of action should have been created before the failover.
* C. Identifying the problem already occurred earlier in the scenario.

NEW QUESTION: 59
A network architect is creating a network topology for a global SD-WAN deployment. The business has offices in Asia, Europe, and the United States and makes use of data centers in theUnited States and Europe.
Most traffic between sites must have the lowest latency possible. Which of the following topologies best meets this requirement?
A. Star
B. Spine-and-leaf
C. Mesh
D. Hub-and-spoke
Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation From Exact Extract:
A mesh topology allows every site to connect directly to every other site, enabling the shortest and lowest- latency path between locations. This is ideal for SD-WAN deployments that must minimize latency for inter- site communication globally. In contrast, hub-and-spoke models force all traffic through a central hub, increasing latency.
Relevant Extract from CompTIA CloudNetX CNX-001 Study Guide - under "WAN Technologies and Topologies":
"Mesh topologies offer direct connectivity between all participating sites, reducing latency and avoiding single points of failure. They are optimal for SD-WAN deployments requiring performance and resilience." Other options:
* A. Star topology routes all traffic through a central node, introducing latency.
* B. Spine-and-leaf is used in data center architectures, not global WANs.
* D. Hub-and-spoke centralizes routing and increases latency between remote sites.
A full-mesh SD-WAN topology allows each site to establish direct overlays with every other site, minimizing the number of hops and avoiding backhauling through a central hub, thereby delivering the lowest latency paths between Asia, Europe, and the US.

NEW QUESTION: 60
A network architect must design a new branch network that meets the following requirements:
*No single point of failure
*Clients cannot be impacted by changes to the underlying medium
*Clients must be able to communicate directly to preserve bandwidth
Which of the following network topologies should the architect use?
A. Hub-and-spoke
B. Mesh
C. Spine-and-leaf
D. Star
Answer: (SHOW ANSWER)
A full-mesh topology gives every node redundant paths to every other node, eliminating any single point of failure, and lets clients communicate directly over the optimal link without depending on an intermediate hub or core.

NEW QUESTION: 61
A network architect is designing a solution to secure the organization's applications based on the security policy. The requirements are:
Users must authenticate using one set of credentials.
External users must be located in authorized sites.
Session timeouts must be enforced.
Network access requirements should be changed as needed.
Which of the following best meet these requirements? (Choose two.)
A. Role-based access

B. Single sign-on
C. Static IP allocation
D. Multifactor authentication
E. Conditional access policy
F. Risk-based authentication
Answer: (SHOW ANSWER)
Single sign-on: Provides users with one set of credentials for authentication across all applications, simplifying access and reducing password fatigue.
Conditional access policy: Enforces location-based restrictions for external users, configurable session timeouts, and dynamic network access controls that can be updated as requirements evolve.

NEW QUESTION: 62
A network engineer is designing a Layer 2 deployment for a company that occupies several floors in an office building. The engineer decides to make each floor its own VLAN but still allow for communication between all user VLANs. The engineer also wants to reduce the time necessary for STP convergence to occur when new switches come online. Which of the following should the engineer enable to accomplish this goal?
A. BPDU Guard
B. Priority
C. Tagging
D. Portfast
Answer: (SHOW ANSWER)
Enabling PortFast on access ports lets them immediately enter the forwarding state, skipping the STP listening
/learning timers, and dramatically speeds up convergence when switches or end-stations come online.