ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

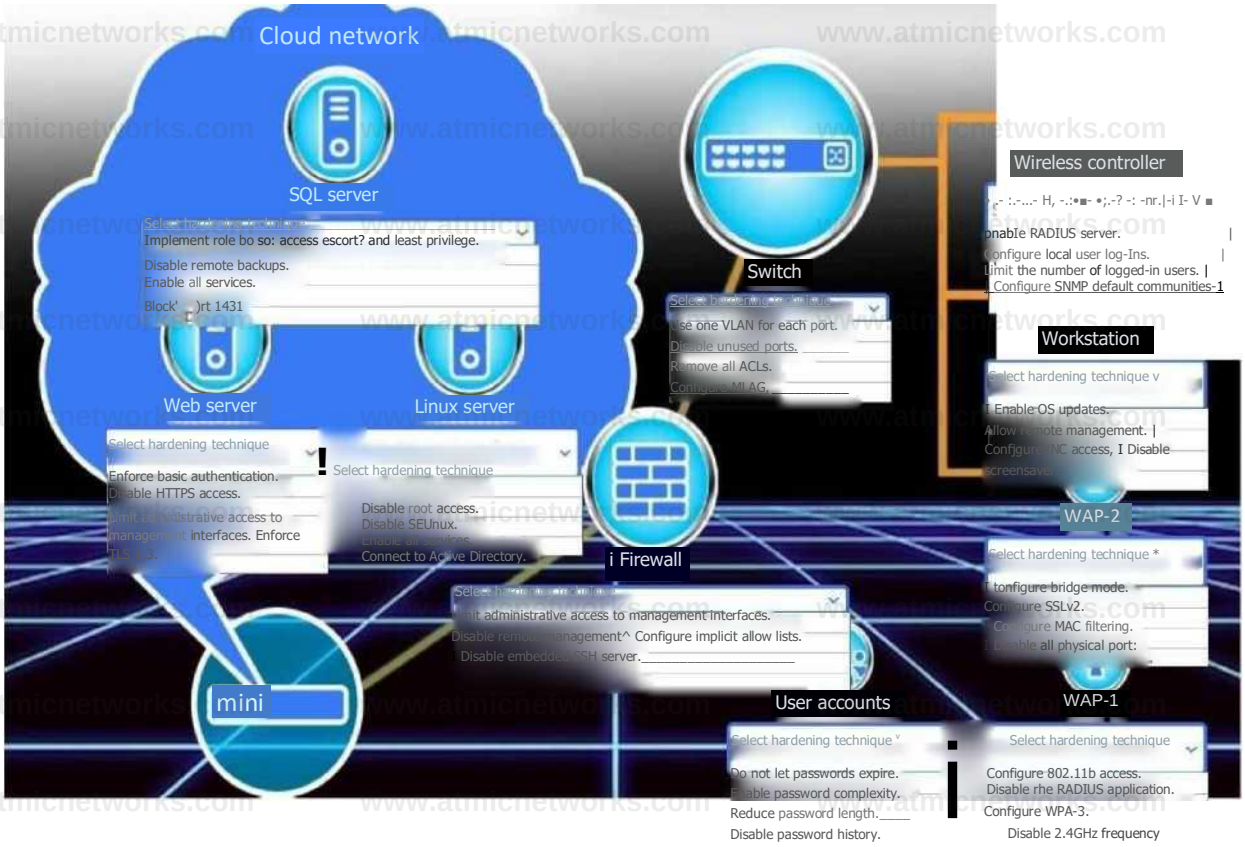
HOTSPOT

New devices were deployed on a network and need to be hardened.

INSTRUCTIONS

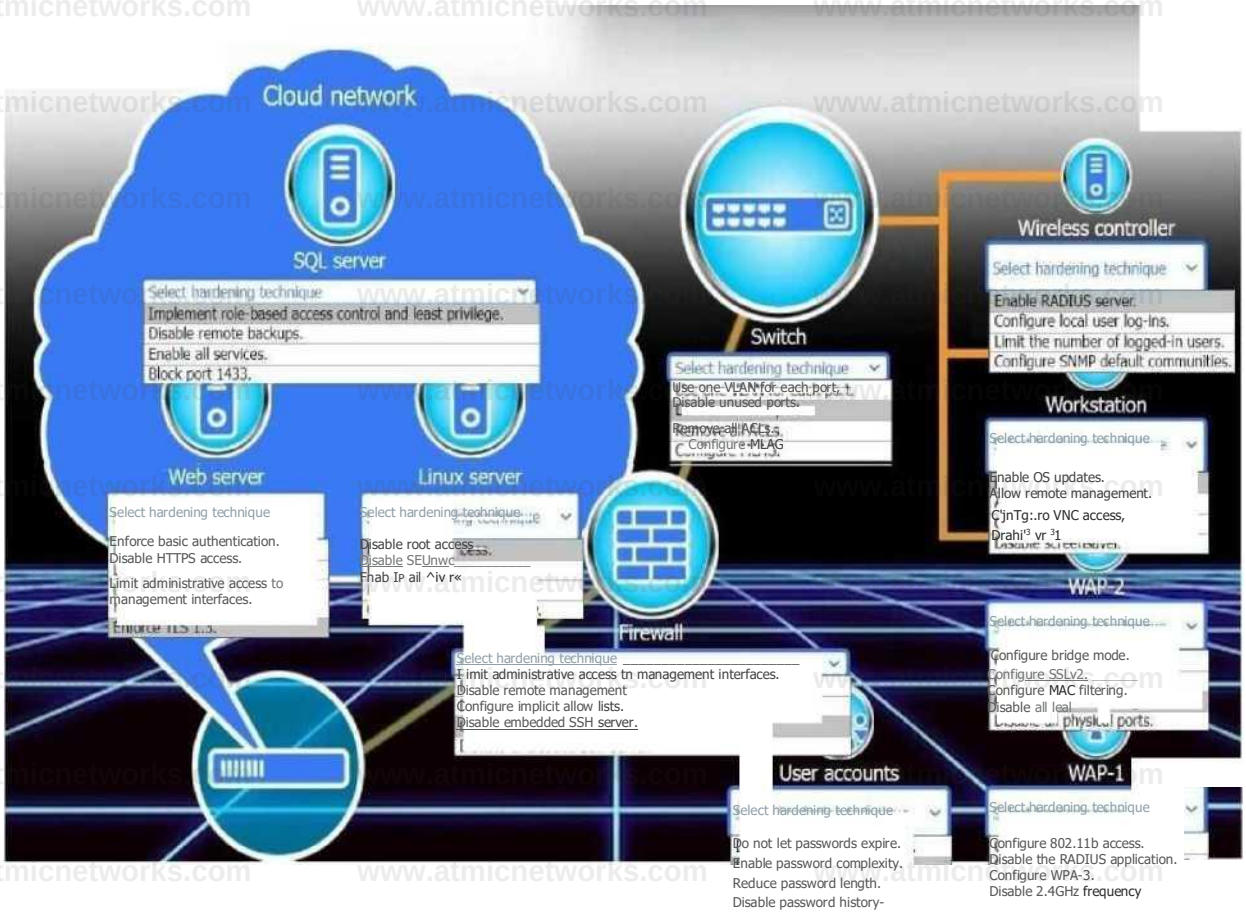
Use the drop-down menus to define the appliance-hardening techniques that provide the most secure solution.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

Explanation:


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.
Linux server
Select hardening technique
Disable root access.
Switch
Select hardening technique
Use one VLAN for each port.
Disable unused ports.
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.
WAP-2
Select hardening technique
Configure bridge mode.
Configure SSLv2.
Configure MAC filtering.
Disable all leal
physical ports.
Firewall
Select hardening technique
Limit administrative access tn 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-
WAP-1
Select hardening technique
Configure 802.11b access.
Disable the RADIUS application.
Configure WPA-3.
Disable 2.4GHz frequency

Question: 3

HOTSPOT

You are designing a campus network with a three-tier hierarchy and need to ensure secure connectivity between locations and traveling employees.

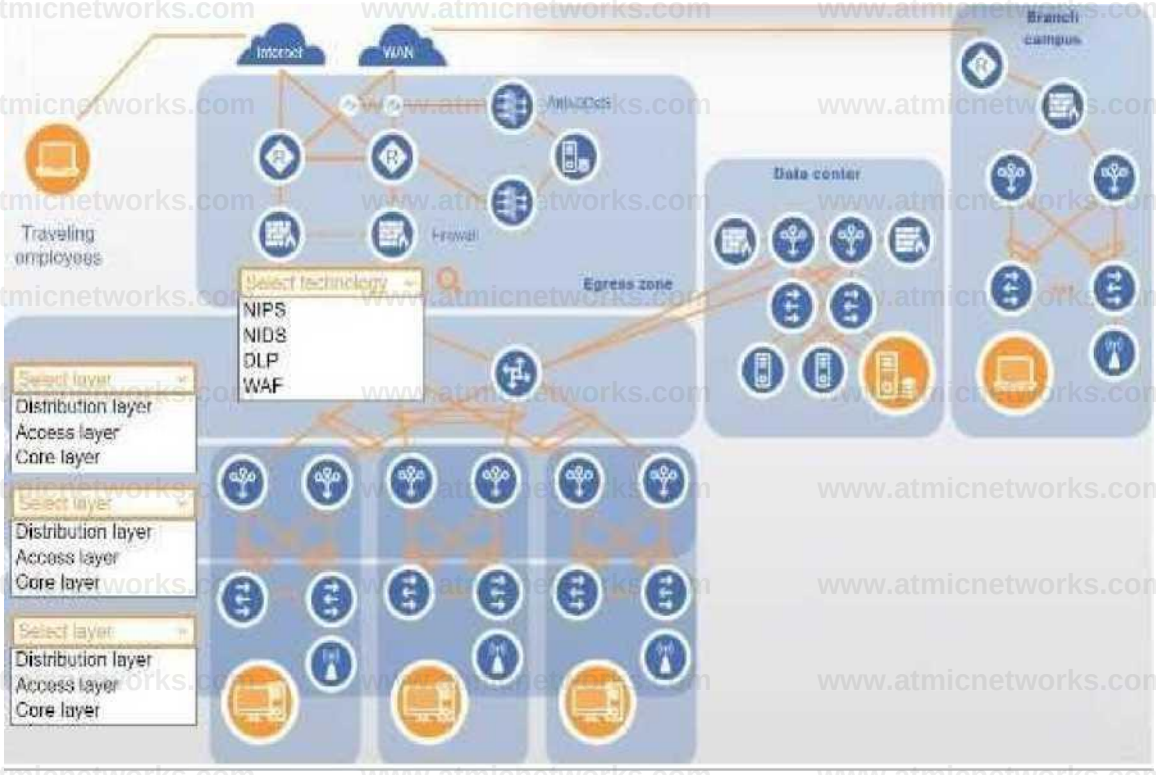
INSTRUCTIONS

Review the command output by clicking on the server, laptops, and workstations on the network.

Use the drop-down menus to determine the appropriate technology and label for each layer on the diagram. Options may only be used once.

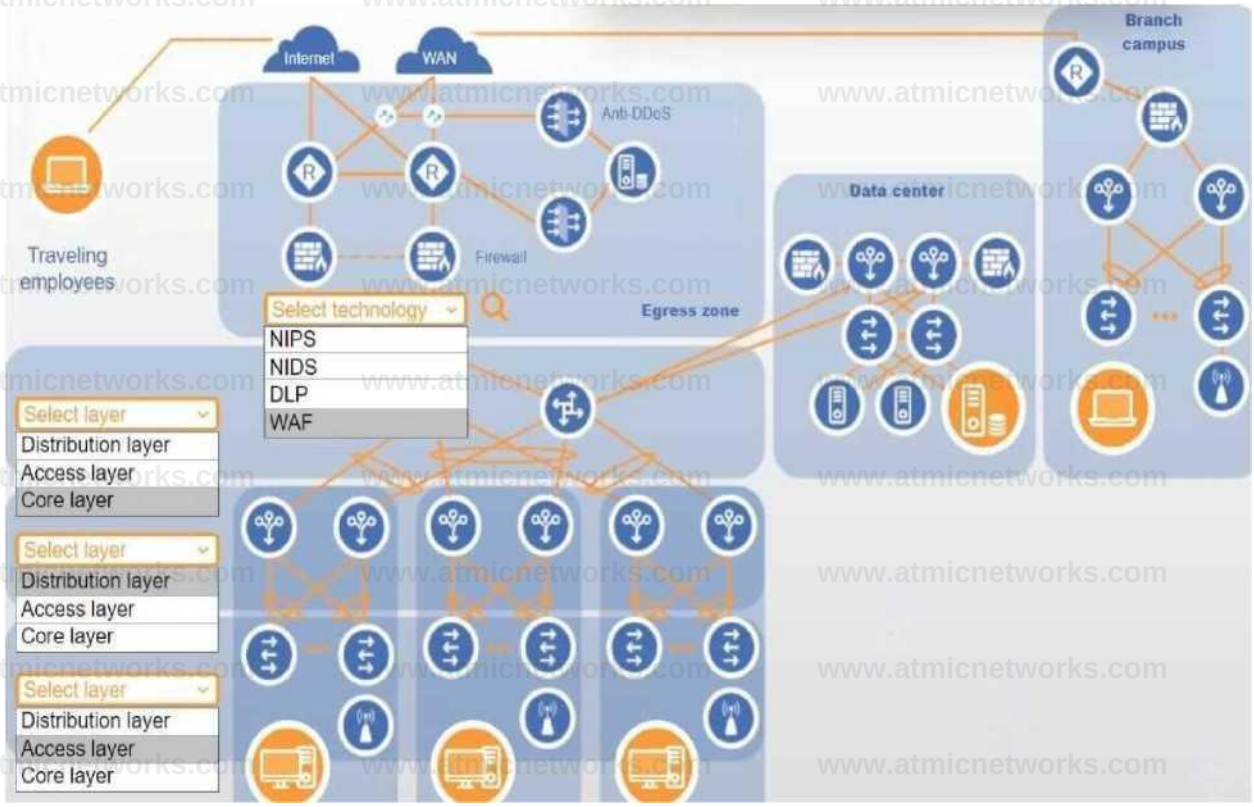
Click on the magnifying glass to make additional configuration changes.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

Explanation:



Question: 4

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

Rafle winner location displayed on the giant stadium screen

Which of the following technologies enables location tracking?

A. SSID
A. BLE
C. NFC
D. IoT

Answer: B

Explanation:

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 supports location tracking with an accuracy range typically between 1 to 2 meters (approximately 3 to 6 feet), making it ideal for applications that demand fine-grained location services, such as stadium services requiring real-time user proximity data.

According to the CompTIA CloudNetX CNX-001 Official Objectives, under the Network 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:

SSID merely identifies a wireless network and has no location tracking function.

NFC requires close contact (under 4 cm), and is not suitable for continuous or broad-range tracking.

IoT is 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, but BLE specifically provides the precise location tracking functionality.

These distinctions are explicitly addressed in the CompTIA 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.

Question: 5

A company is experiencing Wi-Fi performance issues. Three Wi-Fi networks are available, each running on the 2.4 GHz band and on the same channel. Connecting to each Wi-Fi network yields slow performance. Which of the following channels should the networks be configured to?

A. Channel 1, Channel 2. and Channel 3

B. Channel 2. Channel 4, and Channel 9

C. Channel 1, Channel 6, and Channel 11

D. Channel 3, Channel 5, and Channel 10

Answer: C

Explanation:

These are the three non-overlapping channels in the 2.4 GHz band, eliminating co-channel and adjacent-channel interference for optimal Wi-Fi performance.

Question: 6

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

Explanation:

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

Question: 7

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

Explanation:

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.

Question: 8

A security architect needs to increase the security controls around computer hardware installations.

The requirements are:

Auditable access logs to computer rooms

Alerts for unauthorized access attempts

Remote visibility to the inside of computer rooms

Which of the following controls best meet these requirements? (Choose two.)

A. Video surveillance

B. NFC access cards

C. Motion sensors

D. Locks and keys

E. Security patrols

F. Automated lighting

Answer: A, B

Explanation:

Video surveillance provides continuous, remote visibility into computer rooms and can be integrated with analytics to generate alerts on unauthorized presence.

NFC access cards enforce controlled entry with a system that logs every card swipe and issues alerts on failed or out-of-hours attempts, giving you auditable access records and immediate notifications of any suspicious activity.

Question: 9

A network security engineer must secure a web application running on virtual machines in a public cloud. The virtual machines are behind an application load balancer. Which of the following technologies should the engineer use to secure the virtual machines? (Choose two.)

A. CDN

B. DLP

C. IDS

D. WAF

E. SIEM

F. NSG

Answer: D, F

Explanation:

WAF: Protects the web application by inspecting incoming HTTP/HTTPS requests at the load balancer, blocking SQL injection, XSS, and other common web attacks.

NSG: Enforces network-layer controls on the VMs' subnets or interfaces, allowing only approved ports and IP ranges to reach the application servers.

Question: 10

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

Explanation:

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.

Question: 11

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

Explanation:

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.

Question: 12

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

Explanation:

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.

Question: 13

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

Explanation:

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.

Question: 14

A SaaS company is launching a new product based in a cloud environment. The new product will be provided as an API and should not be exposed to the internet. Which of the following should the company create to best meet this requirement?

A. A transit gateway that connects the API to the customer's VPC

B. Firewall rules allowing access to the API endpoint from the customer's VPC

C. A VPC peering connection from the API VPC to the customer's VPC

D. A private service endpoint exposing the API endpoint to the customer's VPC

Answer: D

Explanation:

AWS PrivateLink (a private service endpoint) lets you expose your API over an interface endpoint directly into each customer's VPC without ever traversing the public internet, ensuring the service remains fully private.

Question: 15

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

Explanation:

By explicitly permitting only known, approved traffic and blocking everything else by default, an allow-list policy enforces the strictest firewall posture.

Question: 16

A network engineer is installing new switches in the data center to replace existing infrastructure. The previous network hardware had administrative interfaces that were plugged into the existing network along with all other server hardware on the same subnet. Which of the following should the engineer do to better secure these administrative interfaces?

A. Connect the switch management ports to a separate physical network.

B. Disable unused physical ports on the switches to keep unauthorized users out.

C. Set the administrative interfaces and the network switch ports on the same VLAN.

D. Upgrade all of the switch firmware to the latest hardware levels.

Answer: A

Explanation:

Segregating management interfaces onto their own dedicated network ensures that administrative access is isolated from general user and server traffic, greatly reducing the attack surface and preventing lateral movement if the production network is compromised.

Question: 17

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=llms TTL=53
 Reply from 10.172.16.16: bytes=32 time=672ms TTL=53 Reply from
10.172.16.16: bytes=32 time=lllms 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 is most likely the cause of the video call issue?

A. Throughput

B. Jitter

C. Latency

D. Loss

Answer: B

Explanation:

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.

Question: 18

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

Explanation:

Recording and monitoring all activity at the cabinet greatly strengthens security by providing a realtime deterrent, an audit trail of who accessed it and when, and forensic evidence if an incident ever occurs.

Question: 19

An organization has centralized logging capability at the on-premises data center and wants a solution that can consolidate logging from deployed cloud workloads. The organization would like to automate the detection and alerting mechanism. Which of the following best meets the requirements?

A. IDS/IPS

B. SIEM

C. Data lake

D. Syslog

Answer: B

Explanation:

A Security Information and Event Management system ingests and normalizes logs from on-premises and cloud sources, applies automated correlation rules for detection, and issues alerts, exactly matching the need for centralized logging, analysis, and automated notification.

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: D, E

Explanation:

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.

Question: 21

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

Explanation:

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.

Question: 22

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

Explanation:

Least privilege: Granting users access to the payroll app strictly according to their roles enforces the principle of least privilege.

Microsegmentation: Placing the host in its own 192.168.77.32/30 subnet isolates it from other

workloads, achieving microsegmentation.

Question: 23

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 the United 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: C

Explanation:

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.

Question: 24

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: D

Explanation:

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

Question: 25

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

Explanation:

By deploying SD-WAN you centrally manage and orchestrate all branch connections, minimizing administration overhead, while establishing direct, optimized tunnels into the cloud provider for low- latency, scalable access to cloud services.

Question: 26

End users are getting certificate errors and are unable to connect to an application deployed in a cloud. The application requires HTTPS connection. A network solution architect finds that a firewall is deployed between end users and the application in the cloud. Which of the following is the root cause of the issue?

A. The firewall on the application server has port 443 blocked.

B. The firewall has port 443 blocked while SSL/HTTPS inspection is enabled.

C. The end users do not have certificates on their laptops.

D. The firewall has an expired certificate while SSL/HTTPS inspection is enabled.

Answer: D

Explanation:

When SSL inspection is turned on, the firewall intercepts and re-signs HTTPS traffic with its own certificate. If that certificate has expired, end users will see certificate errors even though port 443 is open and the backend application's certificate is valid.

Question: 27

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

Explanation:

A global Content Delivery Network caches and serves video streams from edge nodes close to end users, minimizing latency and packet loss over limited backhaul links and ensuring the highest possible quality everywhere. By ofloading traffic to a CDN, even customers in regions with constrained connectivity will receive optimized streams from the nearest POP rather than traversing the congested core network.

Question: 28

A company is transitioning from on premises to a hybrid environment. Due to regulatory standards, the company needs to achieve a high level of reliability and high availability for the connection between its data center and the cloud provider. Which of the following solutions best meets the requirements?

A. Establish a Direct Connect with the cloud provider and peer to two different VPCs in the cloud network.

B. Establish a Direct Connect with the cloud provider and a redundant connection with a VPN over the internet.

C. Establish two Direct Connect connections to the cloud provider using two different suppliers.

D. Establish a VPN with two tunnels to a transit gateway at the cloud provider.

Answer: C

Explanation:

By provisioning two dedicated Direct Connect circuits from separate carriers (diverse physical paths and providers), you achieve a true highly available, fault-tolerant link that meets stringent reliability and regulatory requirements without relying on the public internet.

Question: 29

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: B, E

Explanation:

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.

Question: 30

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

Explanation:

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.

Question: 31

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

Explanation:

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.

Question: 32

An administrator logged in to a cloud account on a shared machine but forgot to log out after the session ended. Which of the following types of security threats does this action pose?

A. IP spoofing

B. Zero-day

C. On-path attack

D. Privilege escalation

Answer: C

Explanation:

By leaving an active session open on a shared machine, an attacker with access to that machine can intercept or hijack the administrator's session tokens or credentials - classic on-path behavior - allowing them to impersonate the admin without needing elevated exploits.

Question: 33

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: D

Explanation:

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.

Question: 34

After a malicious actor used an open port in a company's lobby, a network architect needs to enhance network security. The solution must enable:

Security posture check

Auto remediation capabilities

Network isolation

Device and user authentication

Which of the following technologies best meets these requirements?

A. IPS

B. Microsegmentation

C. 802.1X

D. NAC

Answer: D

Explanation:

NAC solutions perform health-and-posture assessments before granting network access, authenticate both devices and users, automatically quarantine or remediate noncompliant machines, and enforce dynamic isolation policies, fully

satisfying all four requirements.

Question: 35

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 the best solution?

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

Explanation:

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.

Question: 36

An outage occurred after a software upgrade on core switching. A network administrator thinks that the firmware

installed had a bug. Which of the following should the network administrator do next?

A. Establish a plan of action to resolve the issue.

B. Test the theory to determine cause.

Document lessons learned.

D. Implement the solution.

Answer: B

Explanation:

Before taking corrective action, you need to verify that the new firmware is indeed the root cause, such as by rolling back to the previous version in a controlled test or reproducing the failure in a lab, so you're sure your fix addresses the actual problem.

Question: 37

A network engineer identified several failed log-in attempts to the VPN from a user's account. When the engineer inquired, the user mentioned the IT help desk called and asked them to change their password. Which of the following types of attacks occurred?

A. Initialization vector

B. On-path

C. Evil twin

D. Social engineering

Answer: D

Explanation:

The attacker tricked the user into revealing credentials by impersonating the help desk over the phone—an archetypal social engineering tactic.

Question: 38

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 NSG1
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
IPGBReservedE	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

Explanation:

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).

Question: 39

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

Explanation:

CI/CD pipelines: Automate the provisioning and configuration of network baselines across all environments, and make it easy to roll out updates consistently.

Public code repository: Enables your community of practice to collaborate, review, and contribute to shared IaC modules and templates, while making updates discoverable and reusable.

Question: 40

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 servers on 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

Explanation:

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.

Question: 41

A customer asks a MSP to propose a ZTA design for its globally distributed remote workforce. Given the following requirements:

Authentication should be provided through the customer's SAML identity provider.

Access should not be allowed from countries where the business does not operate.

Secondary authentication should be added to the workflow to allow for passkeys.

Changes to the user's device posture and hygiene should require reauthentication into the network.

Access to the network should only be allowed to originate from corporate-owned devices.

Which of the following solutions should the MSP recommend to meet the requirements?

A. Enforce certificate-based authentication.

Permit unauthenticated remote connectivity only from corporate IP addresses.

Enable geofencing.

Use cookie-based session tokens that do not expire for remembering user log-ins.

Increase RADIUS server timeouts.

B. Enforce posture assessment only during the initial network log-on.

Implement RADIUS for SSO.

Restrict access from all non-U.S. IP addresses.

Configure a BYOD access policy.

Disable auditing for remote access.

C. Chain the existing identity provider to a new SAML.

Require the use of time-based one-time passcode hardware tokens.

Enable debug logging on the VPN clients by default.

Disconnect users from the network only if their IP address changes.

D. Configure geolocation settings to block certain IP addresses.

Enforce MFA.

Federate the solution via SSO.

Enable continuous access policies on the WireGuard tunnel.

Create a trusted endpoints policy.

Answer: D

Explanation:

Federate the solution via SSO ensures authentication is handled by the customer's SAML identity provider.

Enforce MFA supports secondary authentication with passkeys.

Configure geolocation settings to block certain IP addresses prevents access from unauthorized countries.

Enable continuous access policies on the WireGuard tunnel forces re-authentication whenever device posture or hygiene changes.

Create a trusted endpoints policy restricts access to corporate-owned devices only.

Question: 42

Application development team users are having issues accessing the database server within the cloud environment. All other users are able to use SSH to access this server without issues. The network architect reviews the following information to troubleshoot the issue:

IPAM information:

```
Application development gateway: 192.168.2.1/24
Application development firewall: 192.168.3.1
Server segment gateway: 192.168.1.1/24
Server segment firewall: 192.168.4.1
Database server: 192.168.1.9
Core firewall: 192.168.10.1
```

Traceroute output from an application developer's machine with the assigned IP 192.168.2.7:

```
Tracing route to 192.168.1.9 over a max of 30 hops
1. <lms<lms<lmsl92.168.2.1
2. <lms<lms<lmsl92.168.2.2
3.  3ms 2ms 3msl92.168.1.1
4.  3ms 2ms 3msl92.168.4.1
5.            *Request Time out
6.  *    *Request Time out
7.   *  * *Request Time out
```

Which of the following is the most likely cause of the issue?

A. The core firewall is blocking the traffic.

B. Network security groups do not have the correct outbound rule configured.

C. The server segment firewall is dropping the traffic.

D. The server segment gateway is having bandwidth issues.

Answer: C

Explanation:

The traceroute from 192.168.2.7 reaches the server-segment gateway (192.168.1.1) and then the server-segment firewall (192.168.4.1), but never progresses to the database's subnet. That indicates the firewall at 192.168.4.1 is blocking or not forwarding packets to 192.168.1.9.

Question: 43

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
i Implementation	6 months	9 months
Knowledge transfer	2 months	3 months

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

Explanation:

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.

Question: 44

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: C

Explanation:

A /22 gives you 1,022 usable addresses, ample headroom for 200 IT laptops, while a /15 yields 32,766 addresses, covering up to 2,000 sales laptops with room to grow, all within the 10.0.0.0/8 space.

Question: 45

A network security administrator needs to set up a solution to:

Gather all data from log files in a single location.

Correlate the data to generate alerts.

Which of the following should the administrator implement?

A. Syslog
B. Event log monitoring
C. Log management
D. SIEM

Answer: D

Explanation:

A Security Information and Event Management system centralizes log collection from disparate sources and applies correlation rules to generate actionable alerts.

Question: 46

A cloud network engineer needs to enable network flow analysis in the VPC so headers and payload of captured data can be inspected. Which of the following should the engineer use for this task?

A. Application monitoring

B. Syslog service

C. Traffic mirroring

D. Network flows

Answer: C

Explanation:

VPC Traffic Mirroring lets you capture copies of inbound and outbound network traffic, full packet headers and payload, and send them to appliances or analysis tools for deep inspection, which goes beyond the metadata provided by standard flow logs.

Question: 47

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: B

Explanation:

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.

Question: 48

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

Explanation:

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.

Question: 49

An architecture team needs to unify all logging and performance monitoring used by global applications across the enterprise to perform decision-making analytics. Which of the following technologies is the best way to fulfill this purpose?

A. Relational database

B. Content delivery network

C. CIEM

D. Data lake

Answer: D

Explanation:

A data lake provides a scalable, centralized repository that can ingest and store massive volumes of structured and unstructured data, including logs and performance metrics, from across your global applications. By keeping raw data in its native format, you can run batch and real-time analytics, machine learning, and business-intelligence workloads on one unified platform, making it ideal for enterprise-wide decision-making.

Question: 50

A company is expanding its network and needs to ensure improved stability and reliability. The proposed solution must fulfill the following requirements:

Detection and prevention of network loops

Automatic configuration of ports

Standard protocol (not proprietary)

Which of the following protocols is the most appropriate?

A. STP

B. SIP

C. RTSP

D. BGP

Answer: A

Explanation:

The Spanning Tree Protocol (IEEE 802.1D) is a non-proprietary standard that automatically detects Layer 2 loops and dynamically places redundant switch ports into a blocking or forwarding state, ensuring loop prevention and automatic port configuration.

Question: 51

A network engineer needs to implement a cloud native solution. The solution must allow the recording of network conversation metadata of the host and appliances attached to a VPC. Which of the following will accomplish these goals with the least effort?

A. Enabling network flow

B. Configuring SNMP traps

C. Implementing QoS network tagging

D. Installing a cloud monitoring agent

Answer: A

Explanation:

Enabling VPC (or equivalent) flow logs is the native, zero-agent way to capture metadata about every network conversation, source/destination IPs, ports, protocols, bytes transferred, across both hosts and managed appliances in your virtual network. It requires minimal setup (just a checkbox or API call) and scales automatically with your VPC.

Question: 52

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. Configuring QoS on the corporate network switches

D. Increasing the throughput on the network by purchasing high-end switches

Answer: C

Explanation:

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.

Question: 53

A network architect needs to design a new network to connect multiple private data centers. The network must:
Provide privacy for all traffic between locations.

Use preexisting internet connections.
Use intelligent steering of application traffic over the best path.

Which of the following best meets these requirements?

A. MPLS connections
B. SD-WAN
C. Site-to-site VPN
D. ExpressRoute

Answer: B

Explanation:

By running encrypted tunnels over your existing Internet links and dynamically steering traffic across the optimal path, an SD-WAN solution delivers privacy and performance intelligence without requiring new private circuits.

Question: 54

A network administrator is troubleshooting a user's workstation that is unable to connect to the company network. The results of commands the administrator runs on the workstation are shown below:

```
c:\>ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet 1:
   Physical Address.    . . :  1A-21-11-33-44-5A
   DHCP Enabled..... :    Yes
   IPv4 Address..... :    10.21.12.8
   Subnet Mask ..... :    255.255.255.0
   Default Gateway  . . . :  10.21.12.254
```

A router on the same network shows the following output:

```
#arp -a                          10.21.12.10
Internet Address                 Physical    Address
  10.21.12.254                   12-34-56-78-9a-bc
  10.21.12.255                   ff-ff-ff-ff-ff-ff
  10.21.12.2                     1A-21-11-2E-1E-11
  10.21.12.3                     1A-21-11-1B-2C-44
  10.21.12.8                     1A-21-11-31-74-4C
                                 1A-21-11-43-10-BB
```

Which of the following is the most likely cause of the issues?

A. Asynchronous routing

B. IP address conflict

C. DHCP server down

D. Broadcast storm

Answer: B

Explanation:

Question: 55

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: D

Explanation:

With a /27 mask on 10.10.10.64/27, valid host addresses run from 10.10.10.65 through 10.10.10.94. The database server's IP (10.10.10.93) is in that range, but the web server's IP (10.10.10.101) falls outside it—so it's mis-configured and cannot reach the database.

Question: 56

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: B

Explanation:

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.

Question: 57

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 ofload 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

Explanation:

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.

Question: 58

A cloud engineer is planning to build VMs in a public cloud environment for a cloud migration. A cloud security policy restricts access to the console for new VM builds. The engineer wants to replicate the settings for each of the VMs to ensure the network settings are preconfigured. Which of the following is the best deployment method?

A. IaC template
B. Custom SDK
C. API script
D. CLI command

Answer: A

Explanation:
Using an Infrastructure-as-Code template lets you define and version all VM configurations, including network settings, in code that's automatically applied during deployment, eliminating the need for console changes and ensuring consistency across each build.

Question: 59

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

Explanation:

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.

Question: 60

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

Explanation:

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 industryspecific obligations.

Question: 61

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

Explanation:

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.

Question: 62

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

Explanation:

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.

Question: 63

A developer reports errors when trying to access a web application. The developer uses Postman to troubleshoot and receives the following error:

New request • goAAPi

Payment collection / New request

GET ^ < /paymenLmeihods/country?country»US&currency«USD

Parameters* Authorization Headers (11) Body Pre-request script Tests Settings

Headers < > 6 hidden

Key	Value
Q accessjcey	({rapyd.
Q signature	((rapyd.
Q salt	({opvd.
Q timestamp	({rap yd.
Q content-type	appllcat

Body Cookies Headers (5) Test results

Pretty Raw Preview Visualise HTML

```
1   <htnl>
3   <head>
4   <title>403 Forbidden</title*
5   </head>
6
7   <body>
8       <center>
9           <hl>403 Forbidden</hl>
10      </center*
11  </body>
12
13 </html>
```

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

Explanation:

The 403 Forbidden HTML response indicates the API is rejecting the call due to missing or invalid credentials (no valid access key/signature), not because of a missing resource (404), a network-level block (you'd see a timeout or TCP reject), or an HTTP redirect. Proper authentication headers with a valid signature are required to avoid the 403 error.

Question: 64

Which of the following helps the security of the network design to align with industry best practices?

A. Reference architectures

B. Licensing agreement

C. Service-level agreement

D. Memorandum of understanding

Answer: A

Explanation:

Reference architectures provide standardized, vendor-agnostic blueprints that incorporate industry best practices for security, ensuring your network design aligns with proven frameworks.

Question: 65

An organization's Chief Technical Officer is concerned that changes to the network using IaC are causing unscheduled outages. Which of the following best mitigates this risk?

A. Making code changes to the master branch

B. Enforcing code review of the change by the author

C. Forking the code repository before making changes

D. Adding review/approval steps to the CI/CD pipelines

Answer: D

Explanation:

Introducing mandatory review and approval gates in your deployment pipelines ensures that every Infrastructure-as-Code change is peer-reviewed, tested, and explicitly signed off before going live, reducing the chance of unvetted code causing unexpected outages.

Question: 66

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

Explanation:

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.

Question: 67

A cloud architect must recommend an architecture approach for a new medical application that requires the lowest downtime possible. Which of the following is the best application deployment strategy given the high-availability requirement?

A. Two different availability zones (per region) using an active-active topology in two different regions
B. Four different availability zones using an active-passive topology in a single region
C. Four different availability zones using an active-active topology in a single region
D. Two different availability zones (per region) using an active-passive topology in two different regions

Answer: A

Explanation:

Deploying active-active clusters across two AZs in each of two regions ensures the application can survive both AZ- and entire-region failures, delivering the highest possible uptime.

Question: 68

A company just launched a cloud-based application. Some users are reporting the application will not load. A cloud engineer investigates the issues and reports the following:

* Not all users are experiencing the issue.

* The application infrastructure is optimal.

* Users experiencing the issue belong to the company's remote sales team.

Which of the following is most likely misconfigured?

A. Application load balancers

B. Ports and protocols

C. IP addressing

D. Geolocation rules

Answer: D

Explanation:

Since only the remote sales team is affected and the infrastructure and network settings are correct, it's most likely that your geolocation or geo-restriction policies are blocking traffic from the regions where those users are located. Correcting those rules to allow their locations should restore access without impacting other users.

Question: 69

An organization wants to evaluate network behavior with a network monitoring tool that is not inline. The organization will use the logs for further correlation and analysis of potential threats. Which of the following is the best solution?

A. Syslog to a common dashboard used in the NOC

B. SNMP trap with log analytics

C. SSL decryption of network packets with preconfigured alerts

D. NetFlow to feed into the SIEM

Answer: D

Explanation:

NetFlow provides detailed, flow-level metadata (source/destination IPs, ports, protocols, byte counts, timestamps) without sitting inline. By exporting these records into your SIEM, you gain centralized logging and can correlate network behaviors with other security events for threat detection and analysis.

Question: 70

A company hosts its application s on the cloud and is expanding its business to Europe. The company must comply with General Data Protection Regulation to limit European customers' access to dat

a. The network team configures the firewall rules but finds that some customers in the United States can access data hosted in Europe. Which of the following is the best option for the network team to configure?

A. SASE

B. Network security groups

C. CDN

D. Geofencing rule

Answer: D

Explanation:

Using a geofencing (geo-restriction) policy lets you block or allow traffic based on the client’s geographic location. This ensures that only users in approved regions (e.g., the United States) can reach the European-hosted data, effectively preventing unintended European customer access without complex IP ACLs.

Question: 71

An administrator needs to add a device to the allow list in order to bypass user authentication of an AAA system. The administrator uses MAC filtering and needs to discover the device's MAC address to accomplish this task. The device receives an IP address from DHCP, but the IP address changes daily.

Which of the following commands should the administrator run on the device to locate its MAC address?

A. ipconfig /all

B. netstat -an

C. arp -a

D. nslookup

Answer: A

Explanation:

Running ipconfig /all on the device will display the physical (MAC) address of each network adapter, allowing you to copy the correct MAC for your allow-list entry.

Question: 72

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

Explanation:

If the MD5 hashes match, the certificate and private key correspond correctly.

Question: 73

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: D

Explanation:

Centralizing the application in the cloud introduces longer round-trip times for geographically dispersed users. The increased propagation delay ("latency") is the most likely cause of the perceived slowness.

Question: 74

A network architect is designing a new network for a rural hospital system. Given the following requirements:

* Highly available
* Consistent data transmission
* Resilient to simultaneous failures

Which of the following topologies should the architect use?

A. Collapsed core
B. Hub-and-spoke
C. Mesh
D. Star

Answer: D

Explanation:

A full-mesh topology provides multiple redundant, direct paths between every site, eliminating

single points of failure, ensuring consistent transmission even if one or more links fail, and maximizing overall availability.

Question: 75

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

Explanation:

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.

Question: 76

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 features best achieves this goal?

A. Secure service edge

B. Cloud access security broker

C. Principle of least privilege

D. Identity as the perimeter

Answer: D

Explanation:

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.

Question: 77

A company provides an API that runs on the public cloud for its customers. A fixed number of VMs host the APIs. During peak hours, the company notices a spike in usage that results in network communication speeds slowing down for all customers. The management team has decided that access for all customers should be fair and accessible at all times. Which of the following is the most
cost-effective way to address this issue?

A. Use an allow list for customers using APIs.

B. Increase the number of VMs running APIs.

C. Enable throttling on APIs.

D. Increase the MTU on the VMs.

Answer: C

Explanation:

Implementing request throttling (rate limiting) lets you cap how many requests each customer can make per time unit. This ensures no single user can saturate the API servers, providing fair access across all customers without the recurring costs of adding more VMs.

Question: 78

An administrator must ensure that credit card numbers are not contained in any outside messaging or file transfers from the organization. Which of the following controls meets this requirement?

A. Intrusion detection system

B. Egress filtering

C. Data loss prevention

D. Encryption in transit

Answer: C

Explanation:

Data Loss Prevention solutions inspect outbound communications and file transfers for sensitive data patterns, such as credit

card numbers, and block or quarantine any messages that contain them, ensuring that no payment card details leave the organization.

Question: 79

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 the greatest possible 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

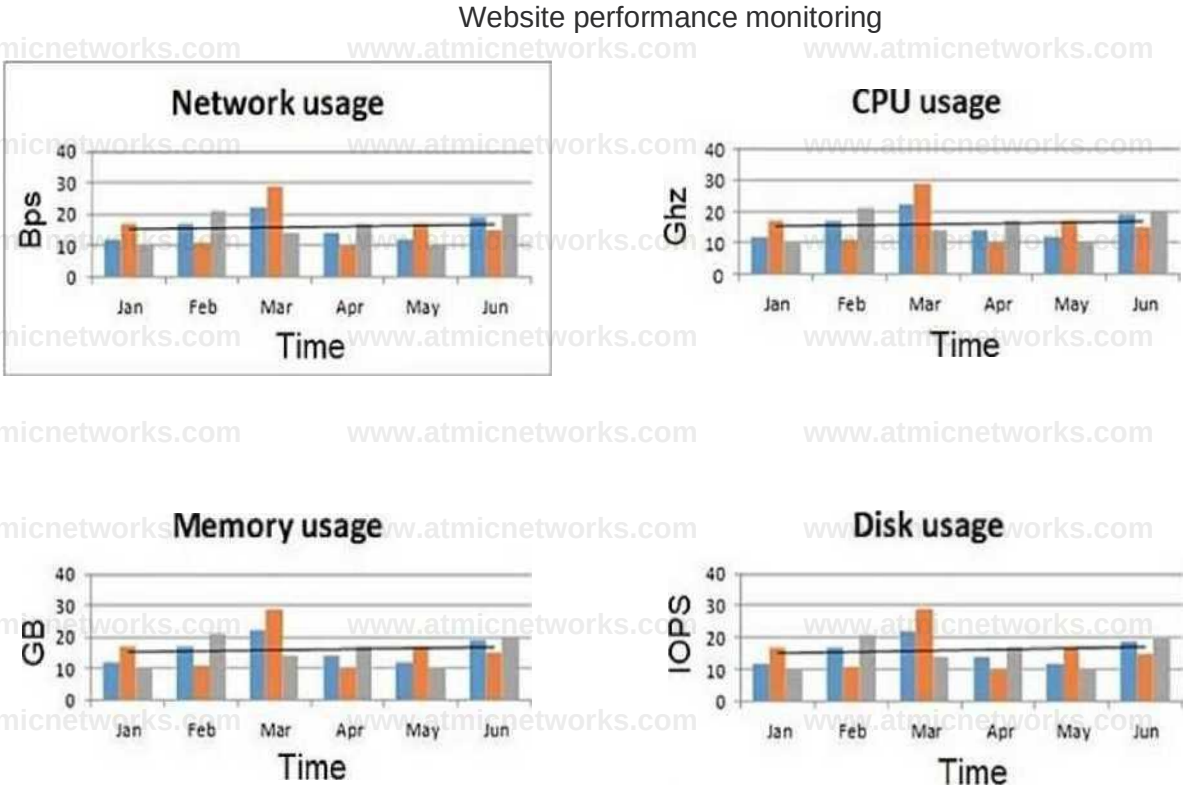
Explanation:

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.

Question: 80

A network engineer at an e-commerce organization must improve the following dashboard due to a performance issue on the website:



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

A. 404 errors

B. Concurrent users

C. Number of orders

D. Number of active incidents

Answer: B

Explanation:

Adding a concurrent-user count gives you the key context you're missing: it ties spikes in CPU, memory, disk I/O, and network traffic directly to how many people are actively hitting the site. You can then see whether performance issues align with increases in user load, enabling more targeted capacity planning and troubleshooting.

Question: 81

A SaaS company's new service currently is being provided through four servers. The company's end users are having connection issues, which is affecting about 25% of the connections. Which of the following is most likely the root cause of this issue?

A. The service is using round-robin load balancing through a DNS server with one server down.

B. The service is using weighted load balancing with 40% of the traffic on server A, 20% on server B, 20% on server C, and server D is down.

C. The service is using a least-connection load-balancing method with one server down.

D. Load balancing is configured with a health check in front of these servers, and one of these servers is unavailable.

Answer: A

Explanation:

With simple round-robin DNS distributing 25% of requests to each of four servers, a single server outage directly causes exactly 25% of connections to fail, matching the reported impact.

Question: 82

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

Explanation:

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.

Question: 83

A call center company provides its services through a VoIP infrastructure. Recently, the call center set up an application to manage its documents on a cloud application. The application is causing recurring audio losses for VoIP callers. The network administrator needs to fix the issue with the least expensive solution. Which of the following is the best approach?

A. Adding a second internet link and physically splitting voice and data networks into different routes

B. Configuring QoS rules at the internet router to prioritize the VoIP calls

C. Creating two VLANs, one for voice and the other for data

D. Setting up VoIP devices to use a voice codec with a higher compression rate

Answer: B

Explanation:

Prioritizing VoIP packets over the document-management traffic ensures that voice gets the necessary bandwidth and low latency even when the network is congested - all without the cost of new links or hardware.

Question: 84

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

Explanation:

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.