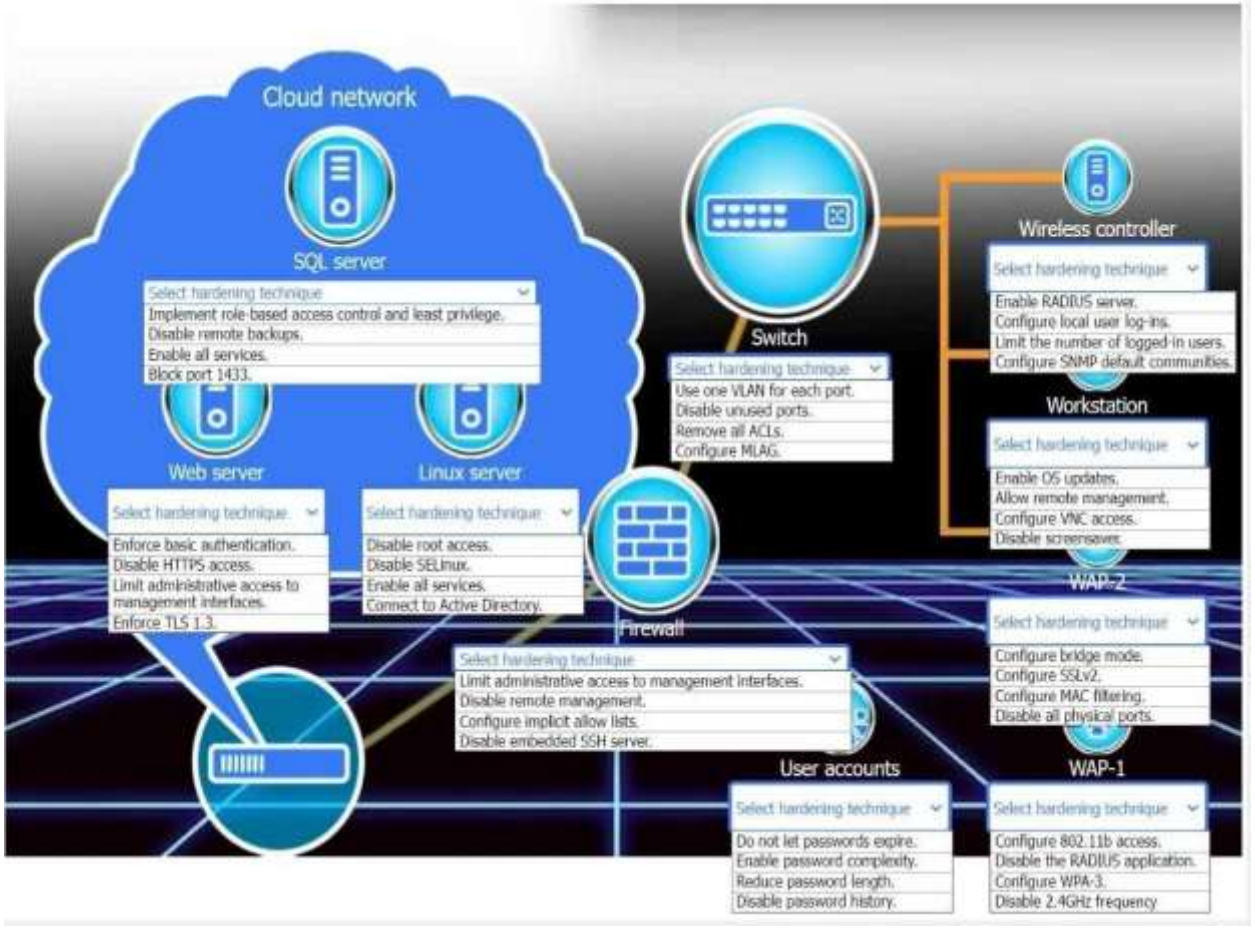
- **Vendor: CompTIA**
- **Exam Code: CNX-001**
- **Exam Name: CompTIA CloudNetX Certification Exam**
- **New Updated Questions from Braindump2go (Updated in May/2025)**

Question:1

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

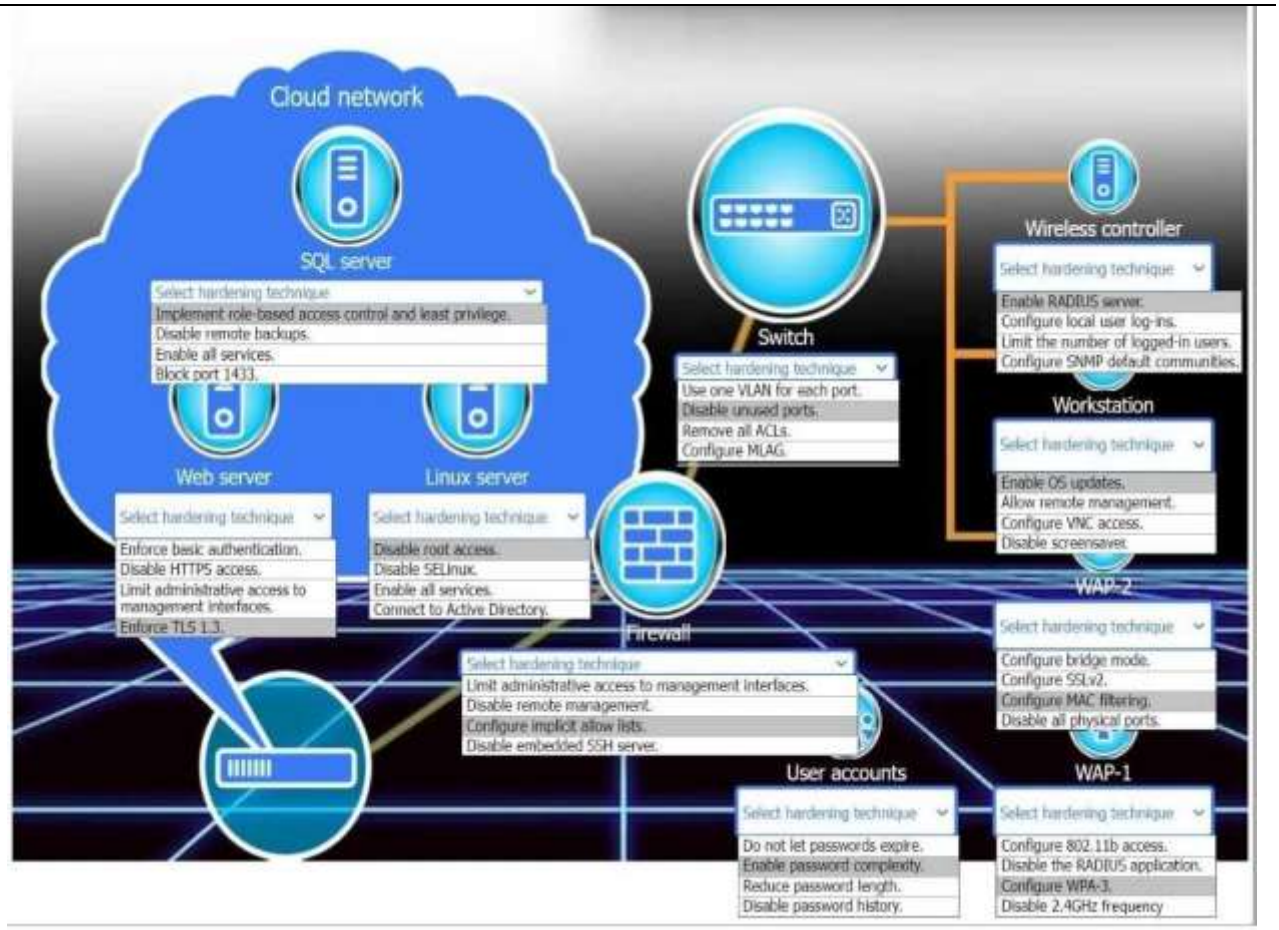
INSTRUCTIONS

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:



Question:2

SIMULATION

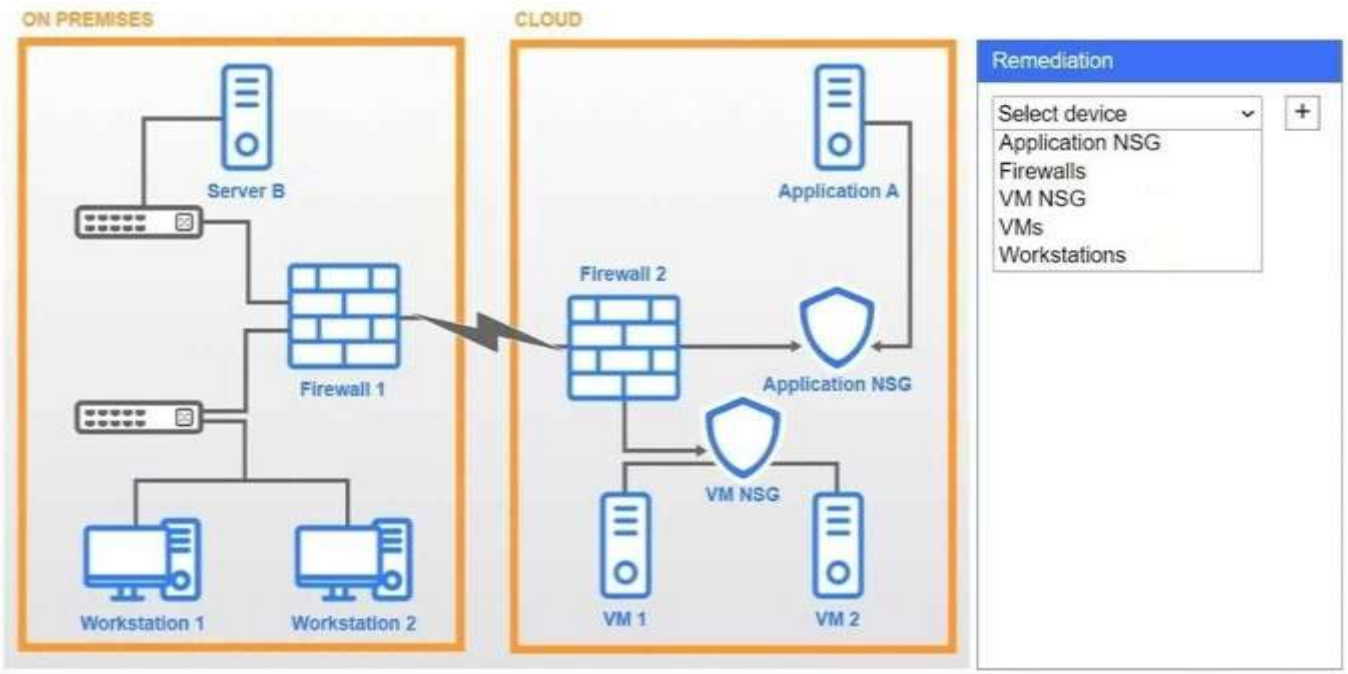
A network administrator needs to resolve connectivity issues in a hybrid cloud setup. Workstations and VMs are not able to access Application
A. Workstations are able to access Server B.

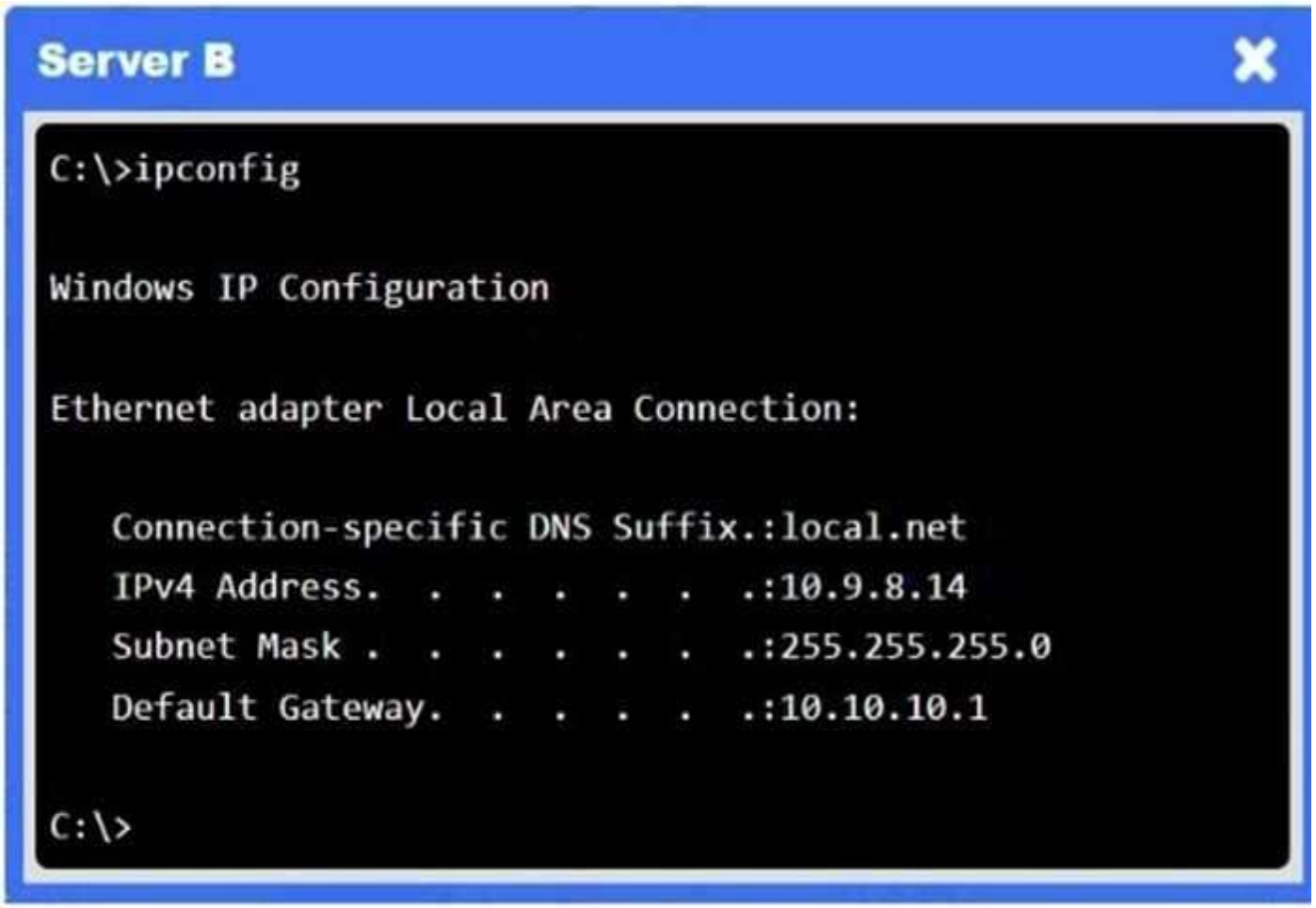
INSTRUCTIONS

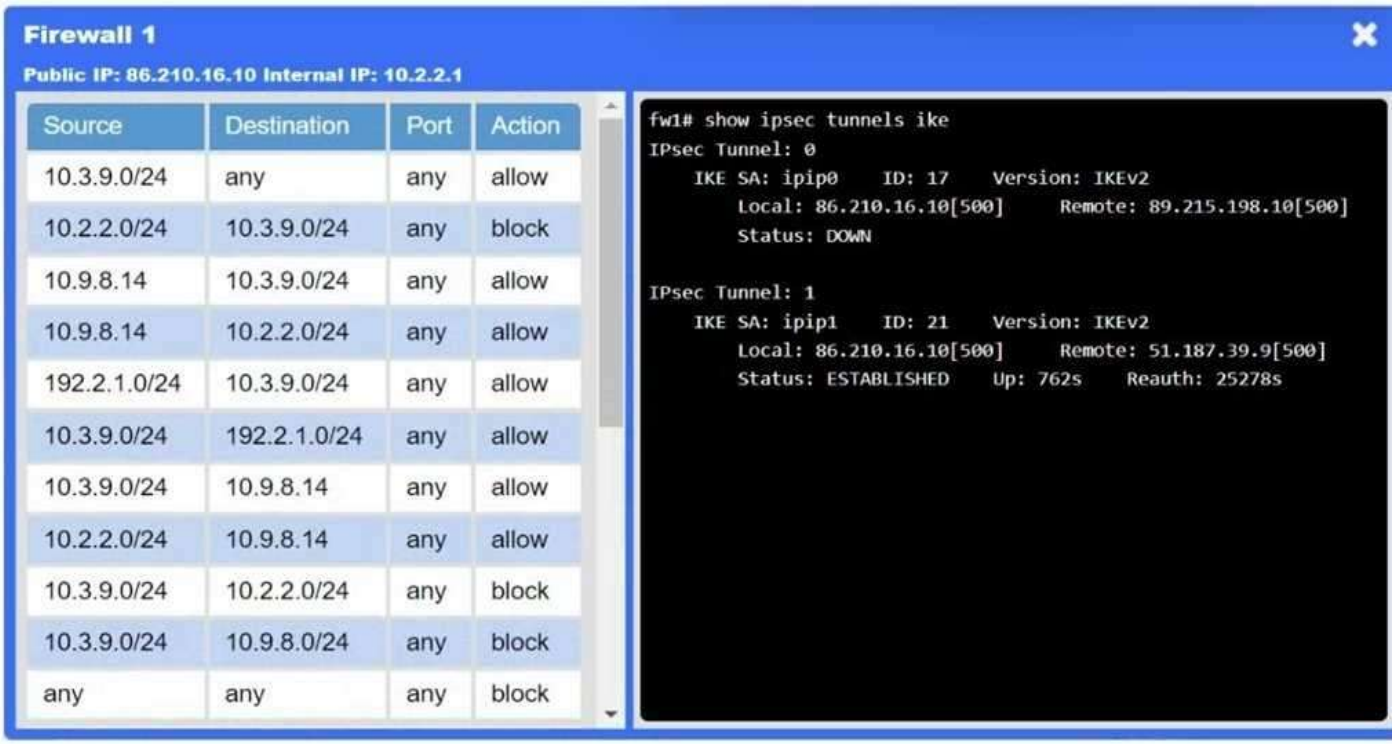
Click on workstations, VMs, firewalls, and NSGs to troubleshoot and gather information. Type help in the terminal to view a list of available commands.

Select the appropriate device(s) requiring remediation and identify the associated issue(s).

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

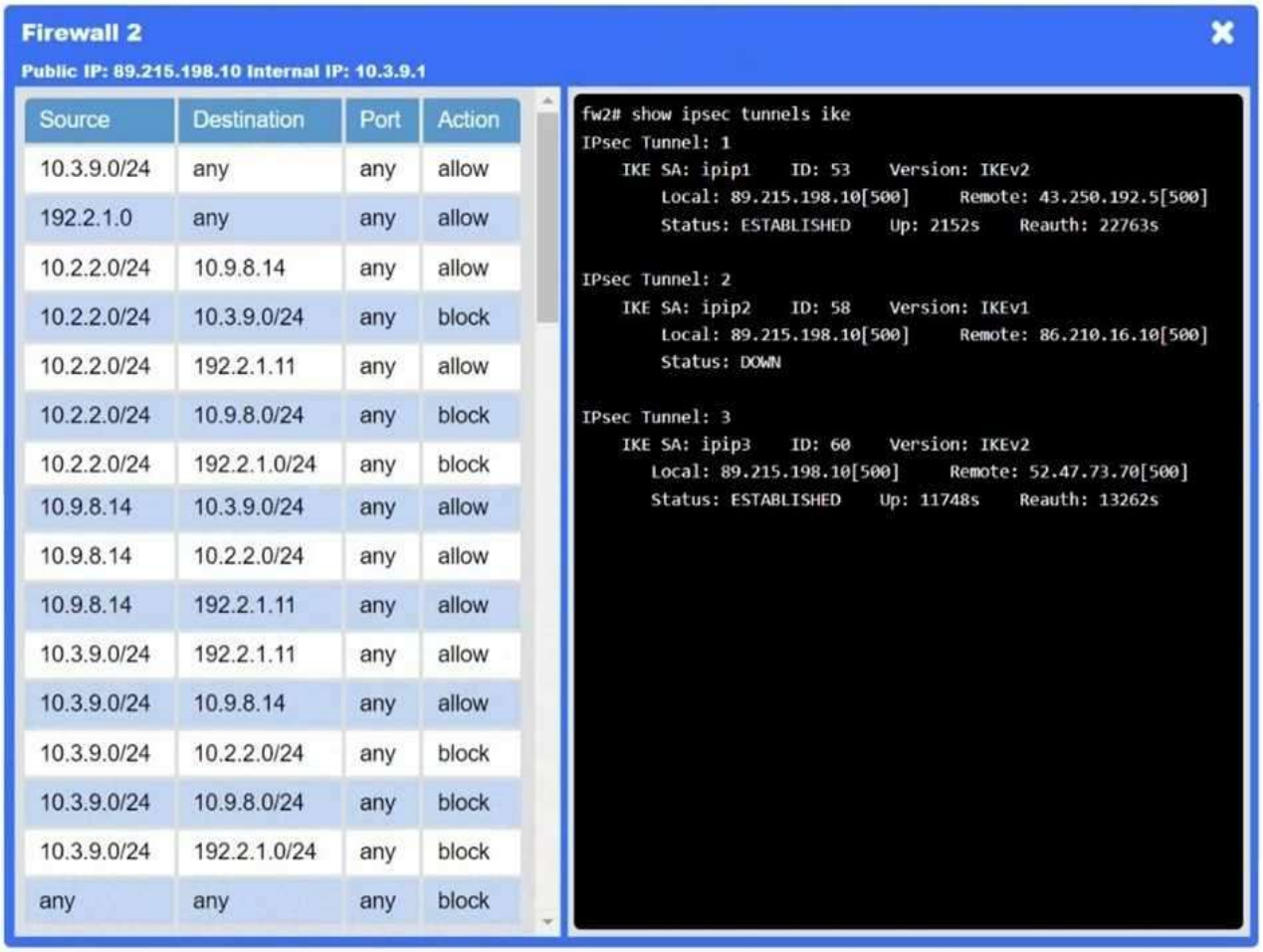



Server B
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix.:local.net
IPv4 Address. . . . . .:10.9.8.14
Subnet Mask . . . . . .:255.255.255.0
Default Gateway. . . . . .:10.10.10.1
C:\>


Firewall 1
Public IP: 86.210.16.10 Internal IP: 10.2.2.1
Source Destination Port Action
10.3.9.0/24 any any allow
10.2.2.0/24 10.3.9.0/24 any block
10.9.8.14 10.3.9.0/24 any allow
10.9.8.14 10.2.2.0/24 any allow
192.2.1.0/24 10.3.9.0/24 any allow
10.3.9.0/24 192.2.1.0/24 any allow
10.3.9.0/24 10.9.8.14 any allow
10.2.2.0/24 10.9.8.14 any allow
10.3.9.0/24 10.2.2.0/24 any block
10.3.9.0/24 10.9.8.0/24 any block
any any any block
fw1# show ipsec tunnels ike
IPsec Tunnel: 0
IKE SA: ipip0 ID: 17 Version: IKEv2
Local: 86.210.16.10[500] Remote: 89.215.198.10[500]
Status: DOWN
IPsec Tunnel: 1
IKE SA: ipip1 ID: 21 Version: IKEv2
Local: 86.210.16.10[500] Remote: 51.187.39.9[500]
Status: ESTABLISHED Up: 762s Reauth: 25278s


Workstation 1
C:\>


Workstation 2
C:\>


Firewall 2
Public IP: 89.215.198.10 Internal IP: 10.3.9.1
Source Destination Port Action
10.3.9.0/24 any any allow
192.2.1.0 any any allow
10.2.2.0/24 10.9.8.14 any allow
10.2.2.0/24 10.3.9.0/24 any block
10.2.2.0/24 192.2.1.11 any allow
10.2.2.0/24 10.9.8.0/24 any block
10.2.2.0/24 192.2.1.0/24 any block
10.9.8.14 10.3.9.0/24 any allow
10.9.8.14 10.2.2.0/24 any allow
10.9.8.14 192.2.1.11 any allow
10.3.9.0/24 192.2.1.11 any allow
10.3.9.0/24 10.9.8.14 any allow
10.3.9.0/24 10.2.2.0/24 any block
10.3.9.0/24 10.9.8.0/24 any block
10.3.9.0/24 192.2.1.0/24 any block
any any any block
fw2# show ipsec tunnels ike
IPsec Tunnel: 1
IKE SA: ipip1 ID: 53 Version: IKEv2
Local: 89.215.198.10[500] Remote: 43.250.192.5[500]
Status: ESTABLISHED Up: 2152s Reauth: 22763s
IPsec Tunnel: 2
IKE SA: ipip2 ID: 58 Version: IKEv1
Local: 89.215.198.10[500] Remote: 86.210.16.10[500]
Status: DOWN
IPsec Tunnel: 3
IKE SA: ipip3 ID: 60 Version: IKEv2
Local: 89.215.198.10[500] Remote: 52.47.73.70[500]
Status: ESTABLISHED Up: 11748s Reauth: 13262s

Application NSG

Source	Destination	Port	Action
192.2.1.0/24	any	any	allow
10.2.2.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	block
10.9.8.14	192.2.1.0/24	any	allow
192.2.1.0/24	10.9.8.14	any	allow
192.2.1.0/24	10.2.2.0/24	any	block
192.2.1.0/24	10.3.9.0/24	any	allow
192.2.1.0/24	10.9.8.0/24	any	block
any	192.2.1.0/24	any	block

Application A

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix.:local.net
   IPv4 Address. . . . . .:192.2.1.11
   Subnet Mask . . . . . .:255.255.255.0
   Default Gateway. . . . . .:192.2.1.1

C:\>
```

VM NSG

Source	Destination	Port	Action
10.3.9.0/24	any	any	allow
10.2.2.0/24	10.3.9.0/24	any	block
10.9.8.14	10.3.9.0/24	any	allow
192.2.1.0/24	10.3.9.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	10.9.8.14	any	allow
10.3.9.0/24	10.2.2.0/24	any	block
10.3.9.0/24	10.9.8.0/24	any	block
any	10.3.9.0/24	any	block

Answer: See explanation below.

Explanation:

Firewalls → VPN tunnel down
The IPsec tunnel between on-prem Firewall 1 and cloud Firewall 2 (ipip0/ipip2) is down, so no traffic can traverse to the cloud.

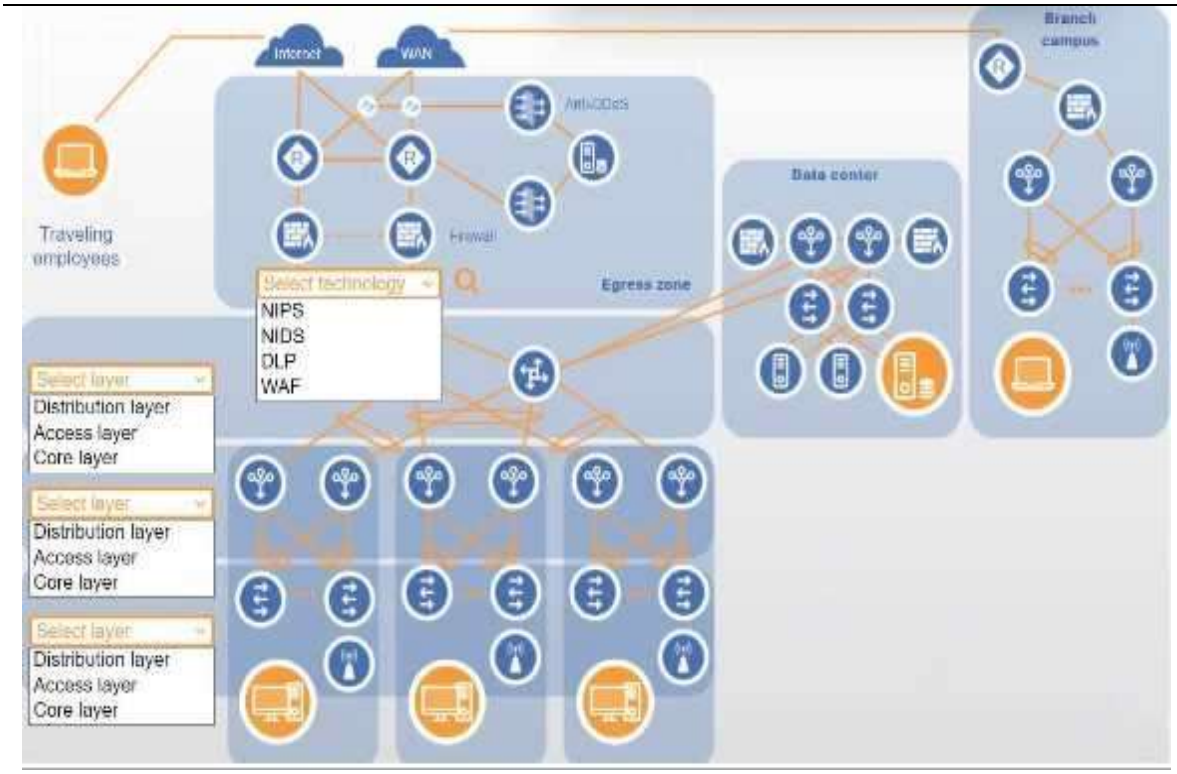
Application NSG → Misconfigured rule
There's a "block" rule for 10.3.9.0/24 → 192.2.1.0/24, preventing legitimate on-prem clients from reaching Application A.

Question:3

HOTSPOT

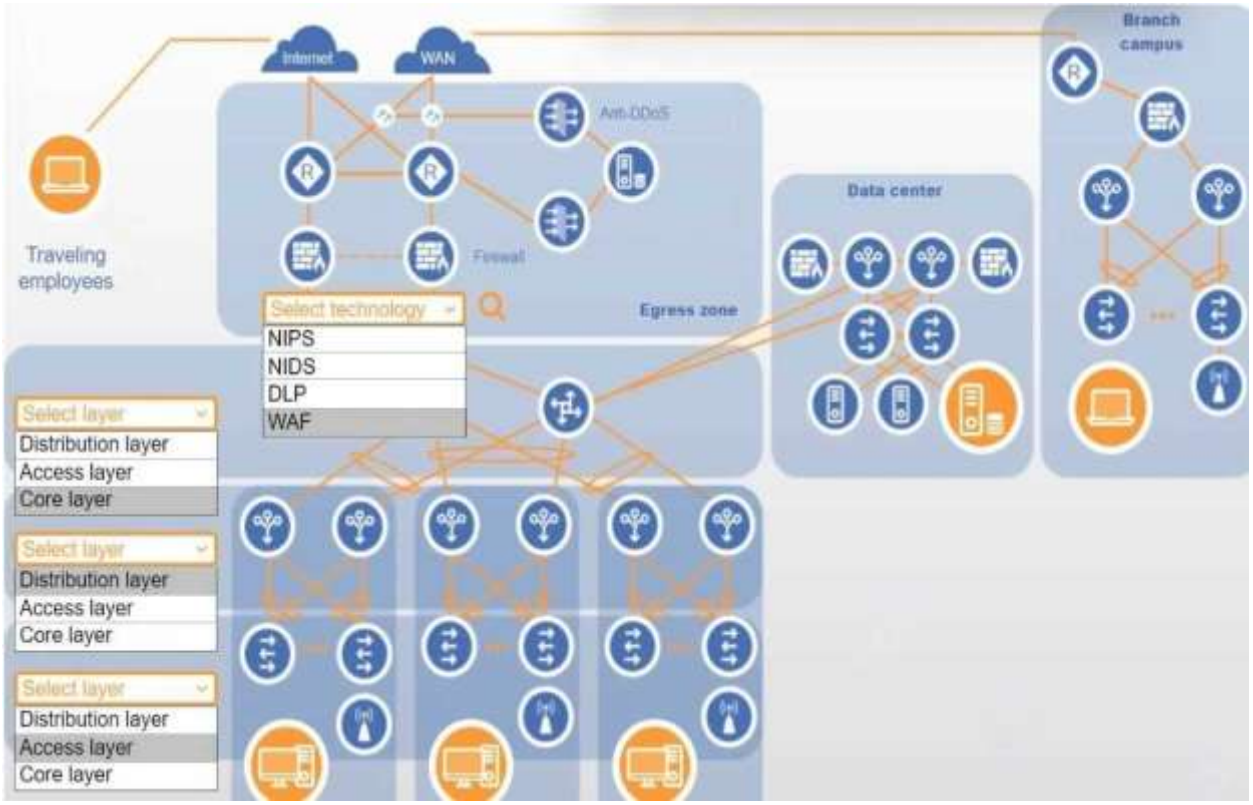
You are designing a campus network with a three-tier hierarchy and need to ensure secure connectivity between locations and traveling employees.

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
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

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
E. 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=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 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 real-time 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 offloading 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.