CompTIA CloudNetX CNX-001 Practice Questions

Shared by Guerra on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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 2

Question Type: MultipleChoice

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?

Options:

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 3

Question Type: MultipleChoice

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 option best best meets these requirements?

Options:

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 4

Question Type: MultipleChoice

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 option best should the company create to best meet this requirement?

Options:

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 5

Question Type: MultipleChoice

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 option best is the root cause of the issue?

Options:

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 6

Question Type: MultipleChoice

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 option best would ensure access is provided according to these requirements?

Options:

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 7

Question Type: MultipleChoice

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 Select to get the greatest possible range from the wireless connection? (Select two.)

Options:

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 8

Question Type: MultipleChoice

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?

Options:

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 9

Question Type: MultipleChoice

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 option best controls best meet these requirements? (Choose two.)

Options:

A- Video surveillance
B- NFC access cards
C- Motion sensors
D- Locks and keys
E- Automated lighting
E- Security patrols

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 10

Question Type: MultipleChoice

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?

Options:

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 11

Question Type: MultipleChoice

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 option best is most likely the root cause of this issue?

Options:

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 12

Question Type: MultipleChoice

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?

Options:

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.