



CompTIA

Exam Questions CNX-001

CompTIA CloudNetX Exam

NEW QUESTION 1

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 industry-specific obligations.

NEW QUESTION 2

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.

NEW QUESTION 3

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: DE

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.

NEW QUESTION 4

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.

NEW QUESTION 5

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
- C. 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.

NEW QUESTION 6

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.

NEW QUESTION 7

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

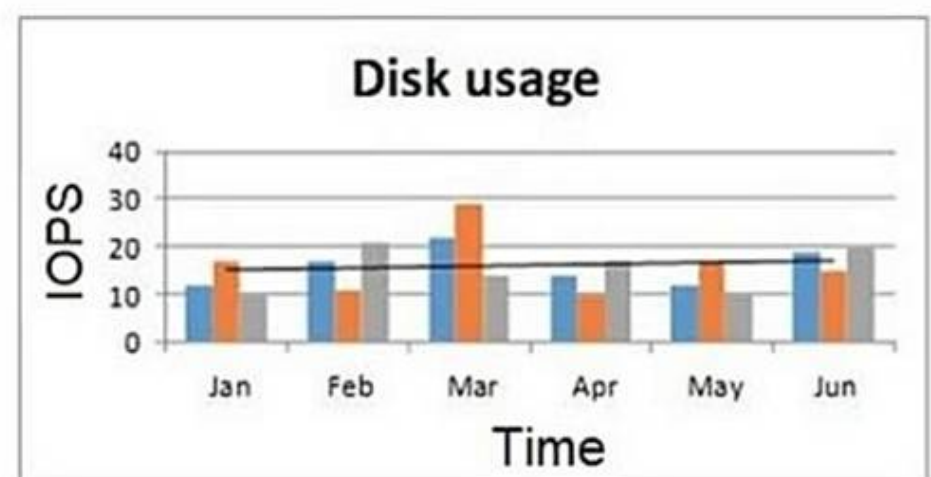
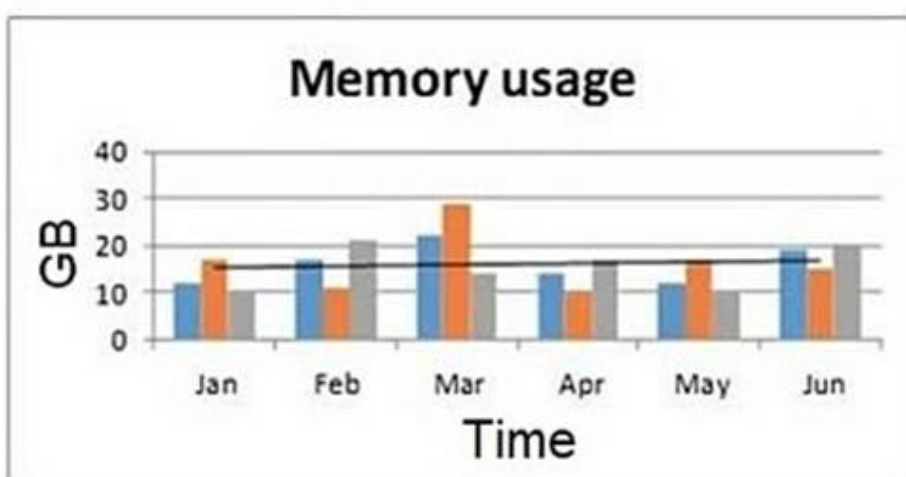
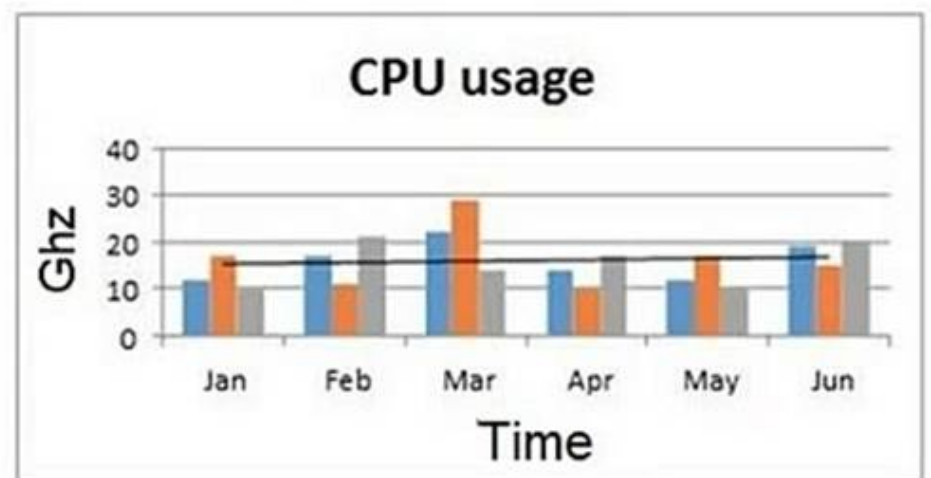
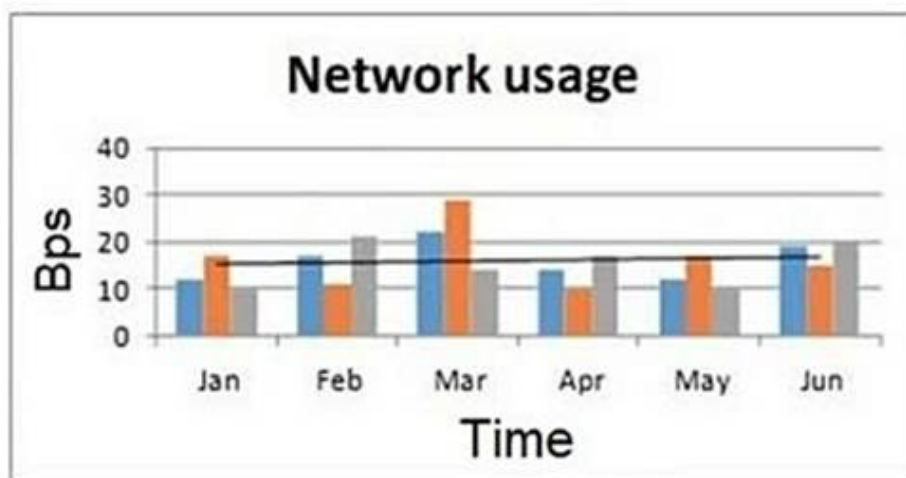
Explanation:

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

NEW QUESTION 8

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

Website performance monitoring



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.

NEW QUESTION 9

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.

NEW QUESTION 10

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.

NEW QUESTION 10

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

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

Which of the following issues may begin to affect cloud assets after the replacement is made?

- A. IP asymmetric routing
- B. IP spoofing
- C. IP exhaustion
- D. IP reuse

Answer: D

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).

NEW QUESTION 12

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 departmen
- B. Allocate 10.2.0.0/16 to the sales department.
- C. Allocate 10.1.0.0/16 to the IT departmen
- D. Allocate 10.2.1.0/24 to the sales department.
- E. Allocate 10.1.0.0/22 to the IT departmen
- F. Allocate 10.2.0.0/15 to the sales department.
- G. Allocate 10.1.0.0/16 to the IT departmen
- H. 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.

NEW QUESTION 13

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 data. 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 (georestriction) 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.

NEW QUESTION 16

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: DF

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.

NEW QUESTION 17

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.

NEW QUESTION 20

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.

NEW QUESTION 25

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.

NEW QUESTION 26

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.

NEW QUESTION 30

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.

NEW QUESTION 31

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.

NEW QUESTION 36

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: AE

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.

NEW QUESTION 40

A company has a 40Gbps network that uses a network tap to inspect the traffic using an IDS. The IDS usually performs normally except when the servers are downloading patches from their local update repository 10.10.10.139 using HTTPS. During the patch windows, the IDS cannot handle the extra load and drops a significant number of packets. Which of the following would allow a network engineer to prevent this issue without compromising the network visibility?

- A. Configuring the IDS to ignore traffic from 10.10.10.139
- B. Using PF_RING offload to filter out "host 10.10.10.139 and port 443"
- C. Adding a "dst host 10.10.10.139" BPF on the tap
- D. Scheduling a cron job to stop the IDS service during the patch window

Answer: C

Explanation:

By applying a Berkeley Packet Filter to drop only the HTTPS patchrepo traffic before it reaches the IDS, you relieve the processing burden during patch windows while preserving full visibility for all other flows. This avoids reconfiguring the IDS itself or losing visibility across the rest of the network.

NEW QUESTION 43

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.

NEW QUESTION 48

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.

NEW QUESTION 51

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.

NEW QUESTION 55

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.

NEW QUESTION 60

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.

NEW QUESTION 61

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.

NEW QUESTION 66

SIMULATION

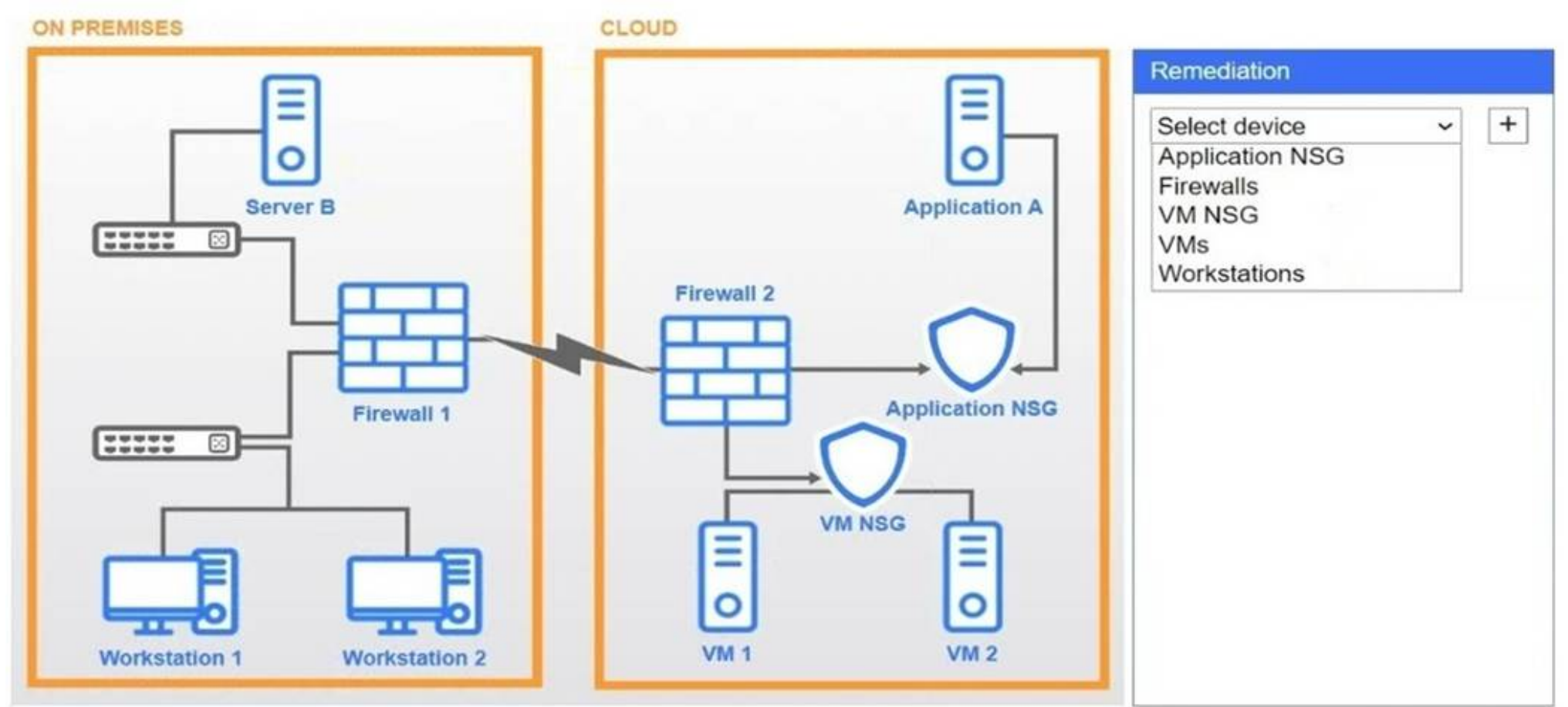
A network administrator needs to resolve connectivity issues in a hybrid cloud setup. Workstations and VMs are not able to access Application A. Workstations are able to

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.



Remediation

Select device

Application NSG
Firewalls
VM NSG
VMs
Workstations

+

Application NSG
X

Issue:

Incorrect routing table
Misconfigured rule
Packet loss
Blocked outbound traffic
VPN tunnel down
Duplicated IP addresses
Misconfigured subnet mask
Overly permissive configuration

Firewalls
X

Issue:

Incorrect routing table
Misconfigured rule
Packet loss
Blocked outbound traffic
VPN tunnel down
Duplicated IP addresses
Misconfigured subnet mask
Overly permissive configuration

VM NSG
X

Issue:

Incorrect routing table
Misconfigured rule
Packet loss
Blocked outbound traffic
VPN tunnel down
Duplicated IP addresses
Misconfigured subnet mask
Overly permissive configuration

VMs
X

Issue:

Incorrect routing table
Misconfigured rule
Packet loss
Blocked outbound traffic
VPN tunnel down
Duplicated IP addresses
Misconfigured subnet mask
Overly permissive configuration

Workstations
X

Issue:

Incorrect routing table
Misconfigured rule
Packet loss
Blocked outbound traffic
VPN tunnel down
Duplicated IP addresses
Misconfigured subnet mask
Overly permissive configuration

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

X

C:\>

Workstation 2

X

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Remediation

Select device

Application NSG

Firewalls

VM NSG

VMs

Workstations

+

Application NSG

Issue:

Incorrect routing table

Misconfigured rule

Packet loss

Blocked outbound traffic

VPN tunnel down

Duplicated IP addresses

Misconfigured subnet mask

Overly permissive configuration

Firewalls

Issue:

Incorrect routing table

Misconfigured rule

Packet loss

Blocked outbound traffic

VPN tunnel down

Duplicated IP addresses

Misconfigured subnet mask

Overly permissive configuration

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.

NEW QUESTION 69

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.

NEW QUESTION 71

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.

NEW QUESTION 73

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.

NEW QUESTION 78

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.

NEW QUESTION 83

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
- B. Configure the DNS server in the customer data center to forward DNS requests for cloud resources to the cloud DNS server.
- C. Configure a NAT server on the cloud to allow internal servers to connect to the applications through the NAT server.
- D. Register applications on the cloud with a public DNS server and configure internal servers to connect to them using their public DNS names.
- E. 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.

NEW QUESTION 87

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: AC

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.

NEW QUESTION 89

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.

NEW QUESTION 92

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CNX-001 Practice Exam Features:

- * CNX-001 Questions and Answers Updated Frequently
- * CNX-001 Practice Questions Verified by Expert Senior Certified Staff
- * CNX-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CNX-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CNX-001 Practice Test Here](#)