



IT認證考試題庫 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CNX-001**

Title : **CompTIA CloudNetX Exam**

Version : **DEMO**

1.HOTSPOT

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

INSTRUCTIONS

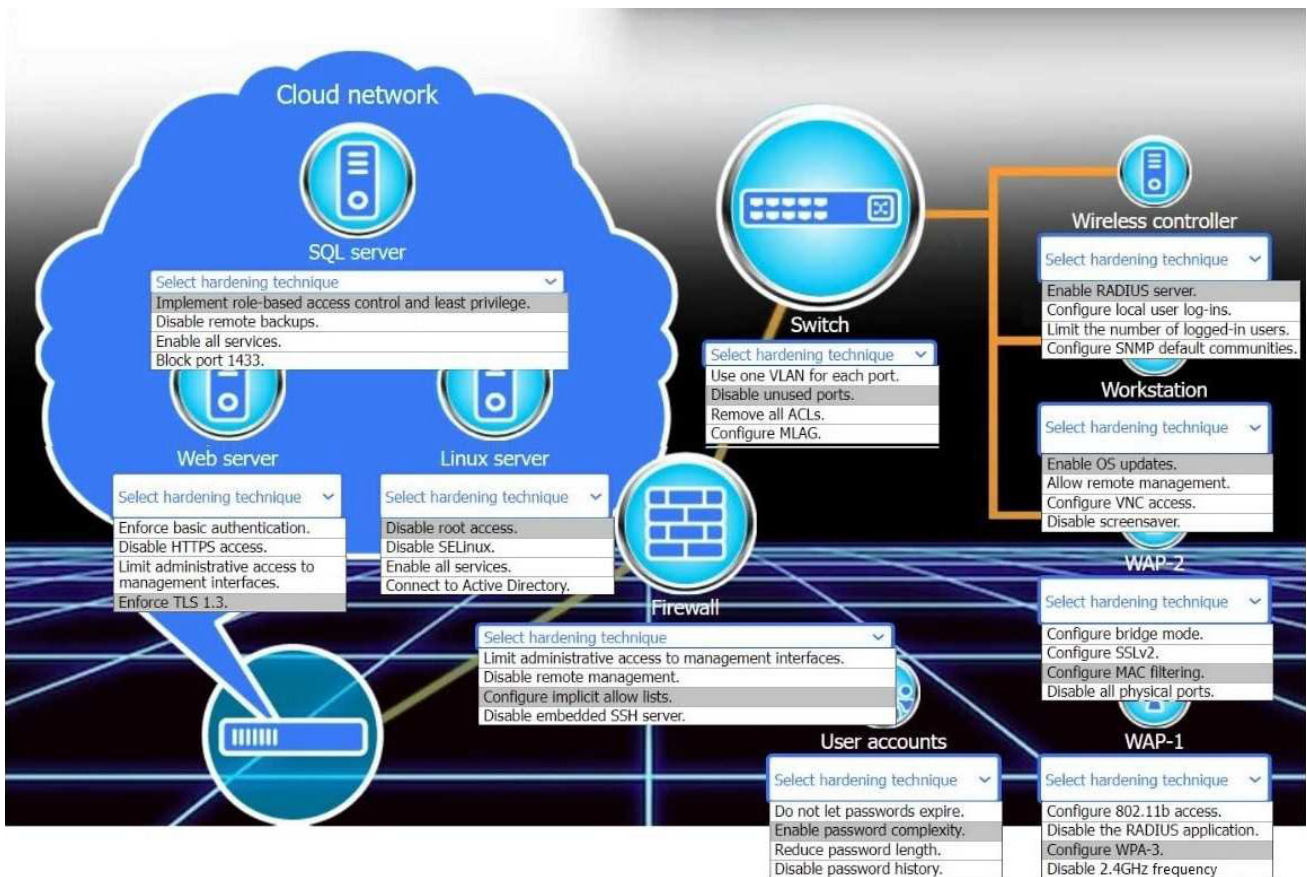
Use the drop-down menus to define the appliance-hardening techniques that provide the most secure solution.

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

The diagram shows a network topology with the following components and their associated hardening options:

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

Answer:



2.SIMULATION

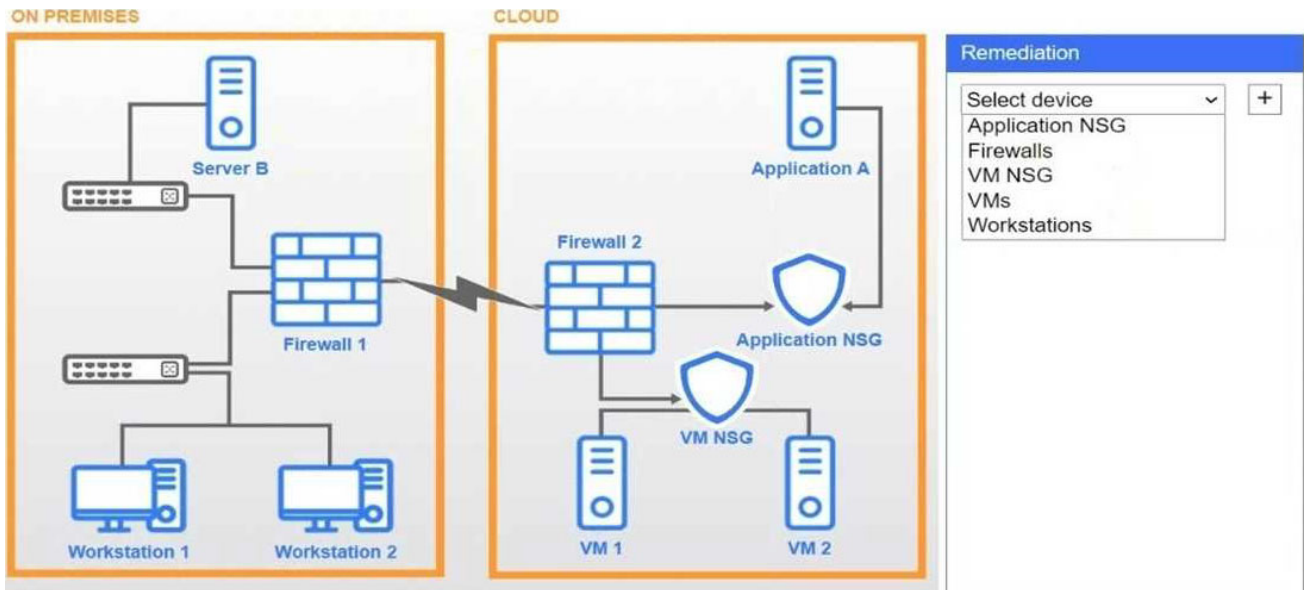
A network administrator needs to resolve connectivity issues in a hybrid cloud setup. Workstations and VMs are not able to access Application A. Workstations are able to access Server B.

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.



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

VM NSG

Issue:

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

VMs

Issue:

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

Workstations

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:\>
```

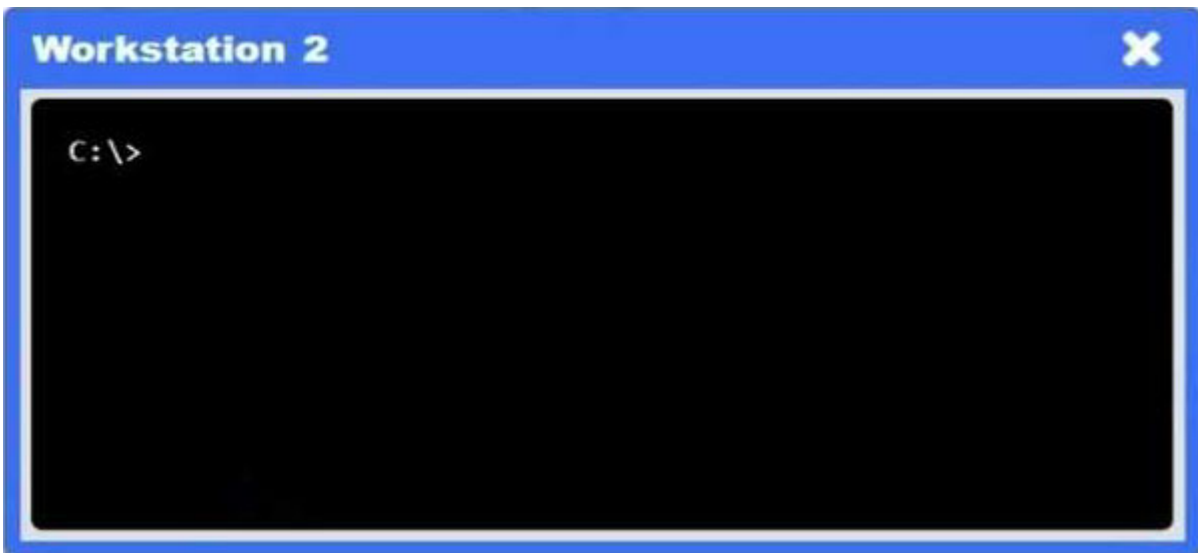
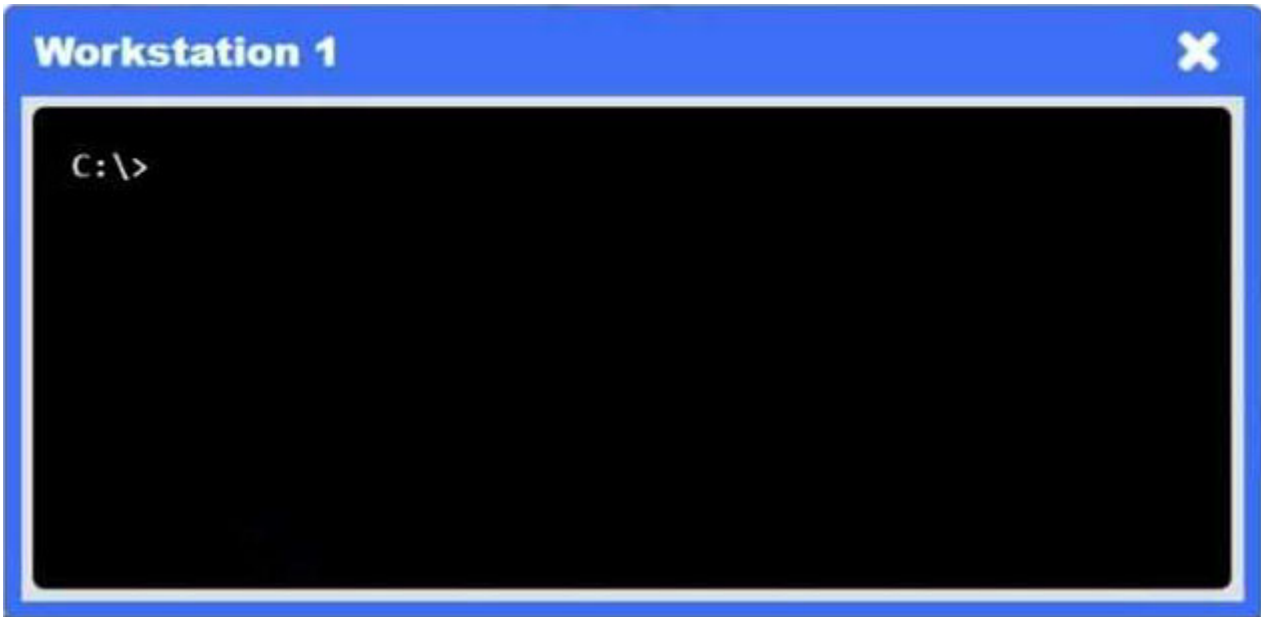
Firewall 1

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
```



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
```

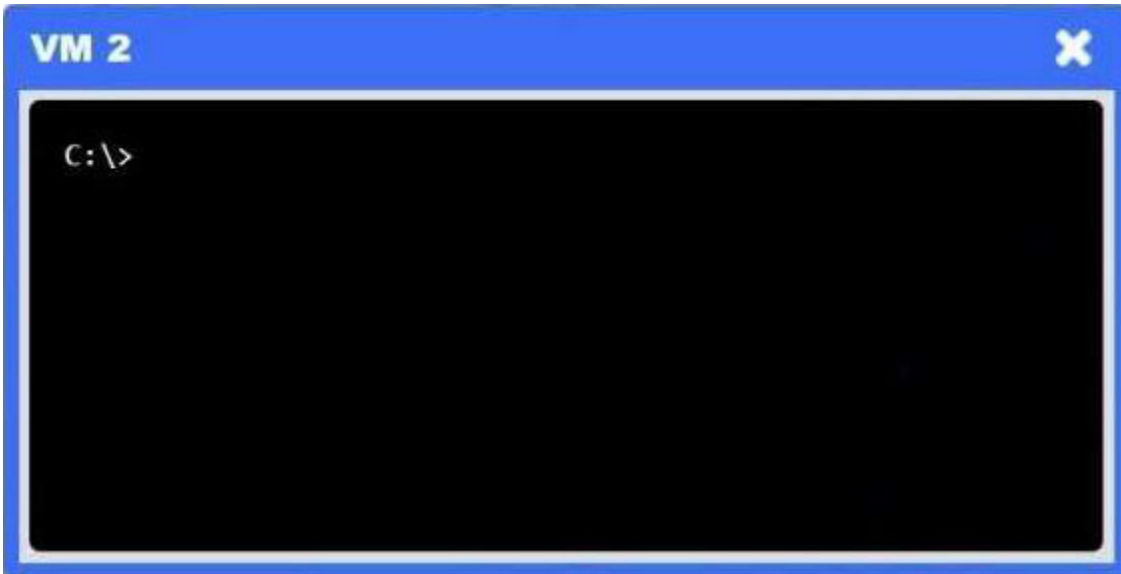
```
C:\>
```

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

VM 1 ✕

```
C:\>
```



Answer:

A screenshot of the "Remediation" pane in the Azure Portal. The pane has a blue header with the word "Remediation". Below the header is a "Select device" dropdown menu with a plus sign button to its right. The dropdown menu is open, showing a list of devices: "Application NSG", "Firewalls", "VM NSG", "VMs", and "Workstations". Below this are two sections, each with a title and a close button (X). The first section is titled "Application NSG" and has an "Issue:" dropdown menu open, showing a list of issues: "Incorrect routing table", "Misconfigured rule", "Packet loss", "Blocked outbound traffic", "VPN tunnel down", "Duplicated IP addresses", "Misconfigured subnet mask", and "Overly permissive configuration". The second section is titled "Firewalls" and has an "Issue:" dropdown menu open, showing a list of issues: "Incorrect routing table", "Misconfigured rule", "Packet loss", "Blocked outbound traffic", "VPN tunnel down", "Duplicated IP addresses", "Misconfigured subnet mask", and "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.

3.HOTSPOT

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

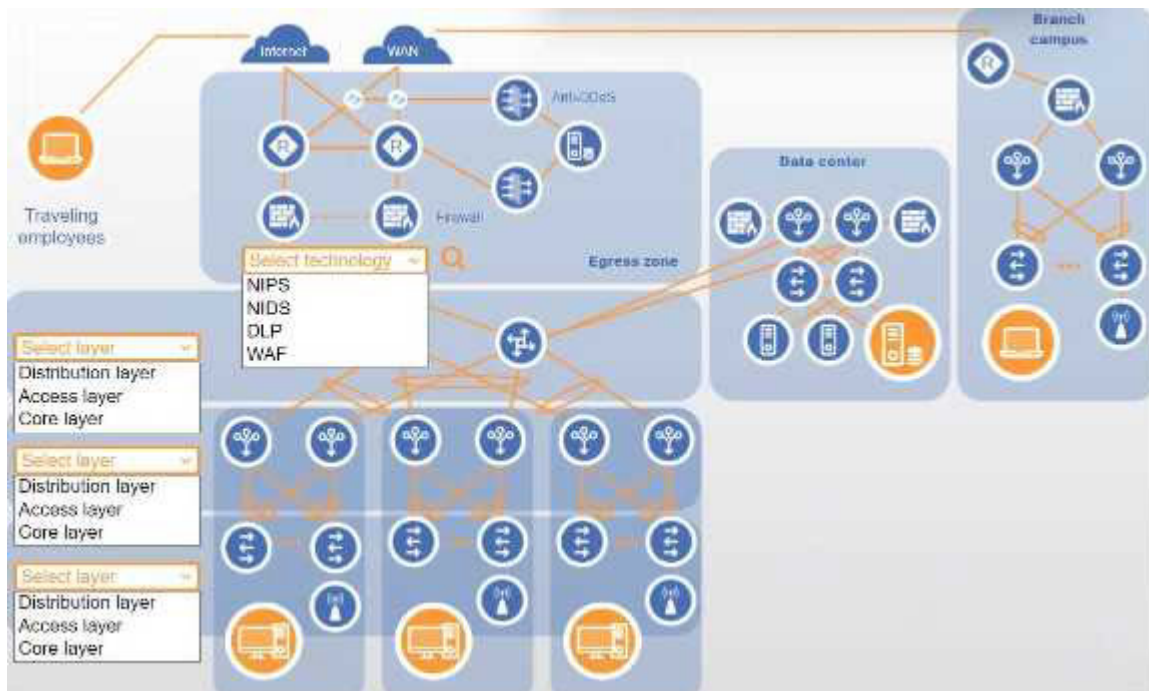
INSTRUCTIONS

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

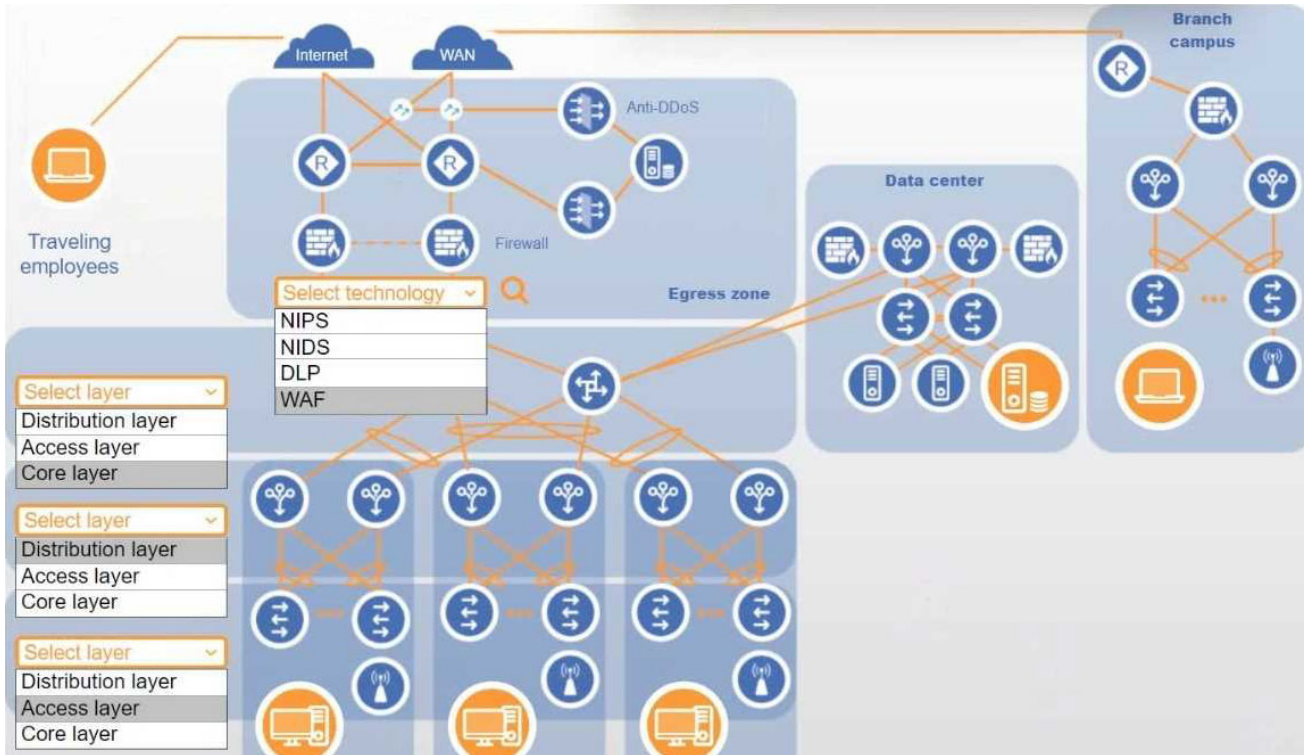
Use the drop-down menus to determine the appropriate technology and label for each layer on the diagram. Options may only be used once.

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:



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.

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.