Product Questions: 84

Question: 1

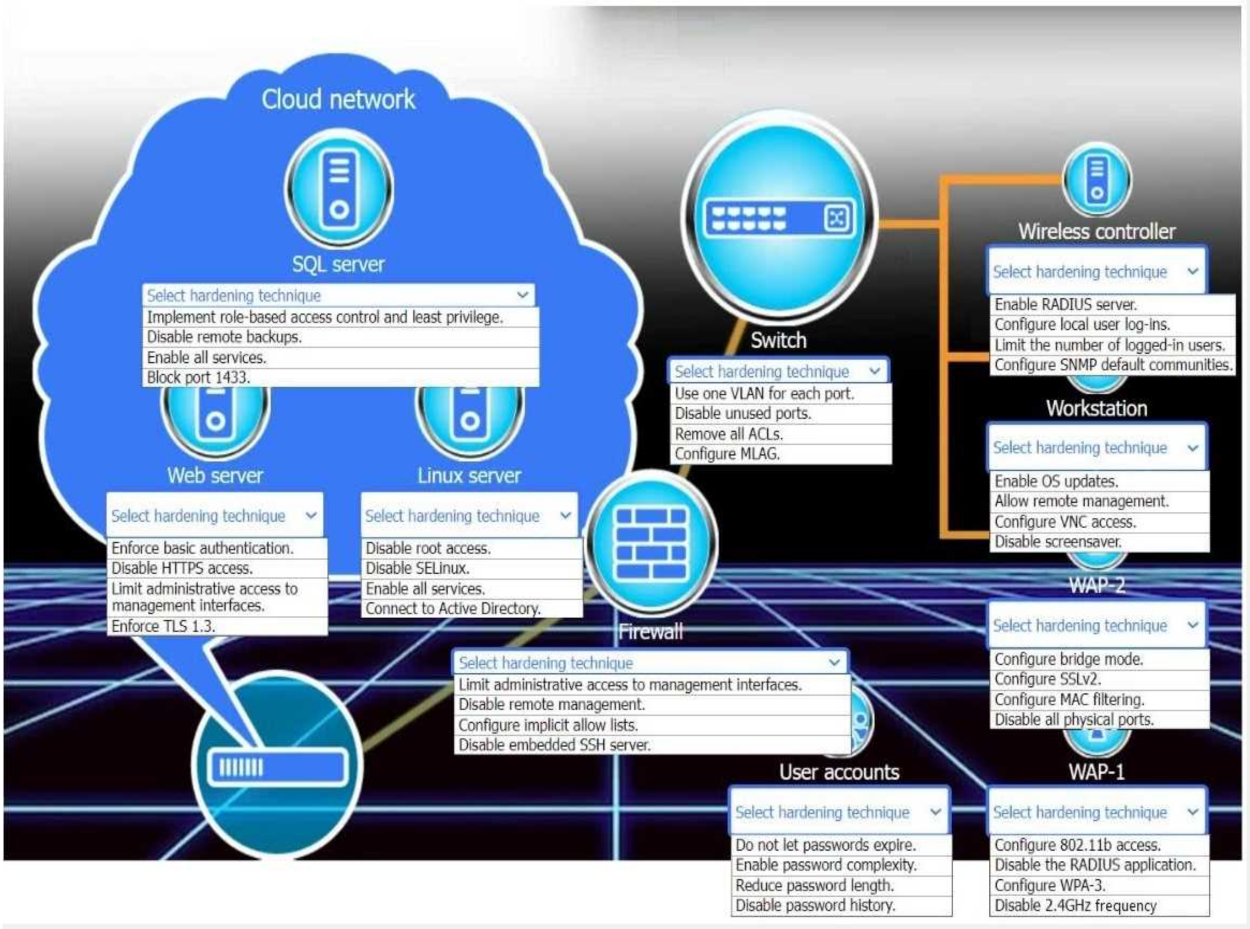
HOTSPOT

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

INSTRUCTIONS

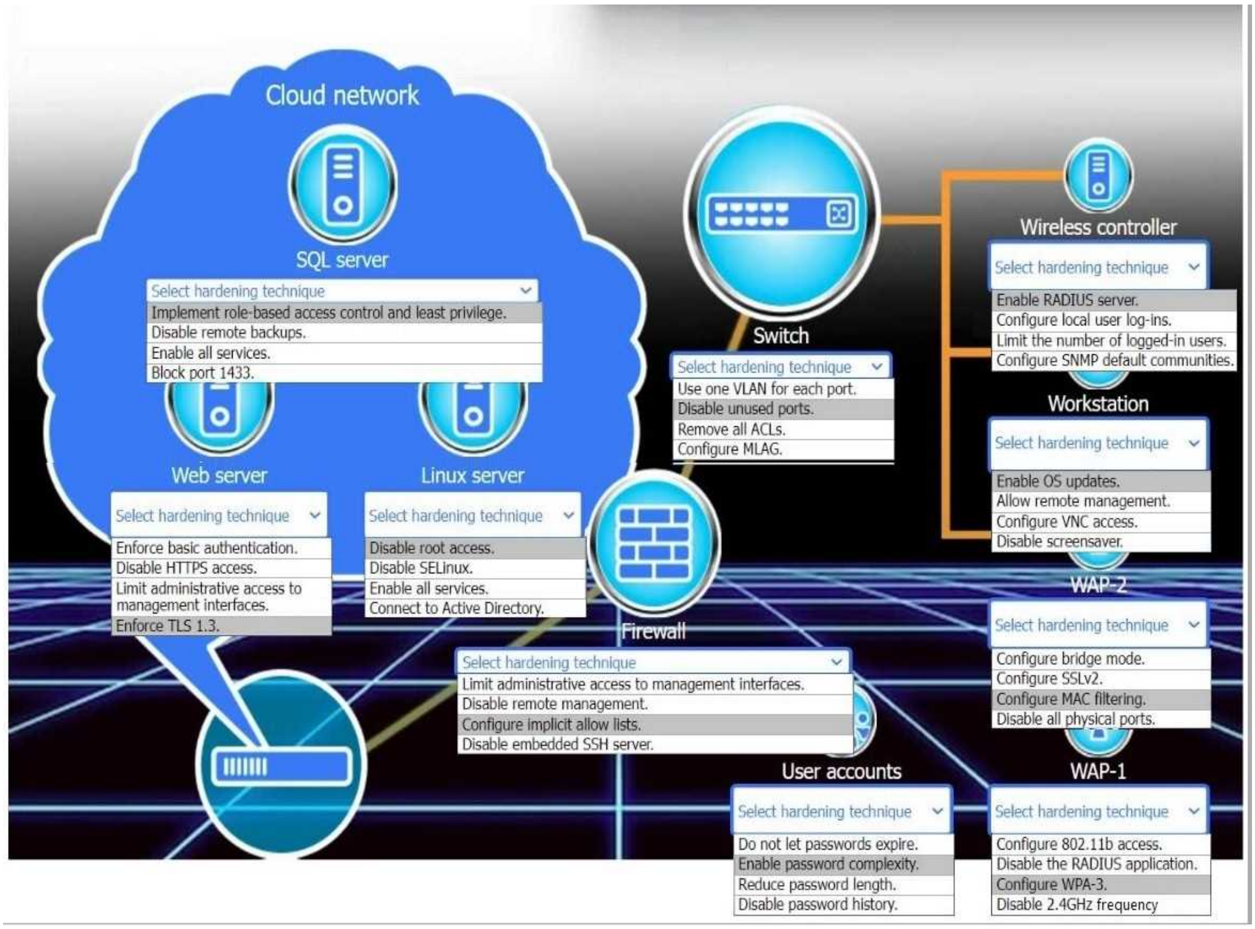
Use the drop-down menus to define the appliance-hardening techniques that provide the most secure solution.

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


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.
Firewall
Select hardening technique
Limit administrative access to management interfaces.
Disable remote management.
Configure implicit allow lists.
Disable embedded SSH server.
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.
WAP-2
Select hardening technique
Configure bridge mode.
Configure SSLv2.
Configure MAC filtering.
Disable all physical ports.
User accounts
Select hardening technique
Do not let passwords expire.
Enable password complexity.
Reduce password length.
Disable password history.
WAP-1
Select hardening technique
Configure 802.11b access.
Disable the RADIUS application.
Configure WPA-3.
Disable 2.4GHz frequency

Answer:

Explanation:


Cloud network
SQL server
Select hardening technique
Implement role-based access control and least privilege.
Disable remote backups.
Enable all services.
Block port 1433.
Web server
Select hardening technique
Enforce basic authentication.
Disable HTTPS access.
Limit administrative access to management interfaces.
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.
WAP-2
Select hardening technique
Configure bridge mode.
Configure SSLv2.
Configure MAC filtering.
Disable all physical ports.
User accounts
Select hardening technique
Do not let passwords expire.
Enable password complexity.
Reduce password length.
Disable password history.
WAP-1
Select hardening technique
Configure 802.11b access.
Disable the RADIUS application.
Configure WPA-3.
Disable 2.4GHz frequency

Question: 2

SIMULATION

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

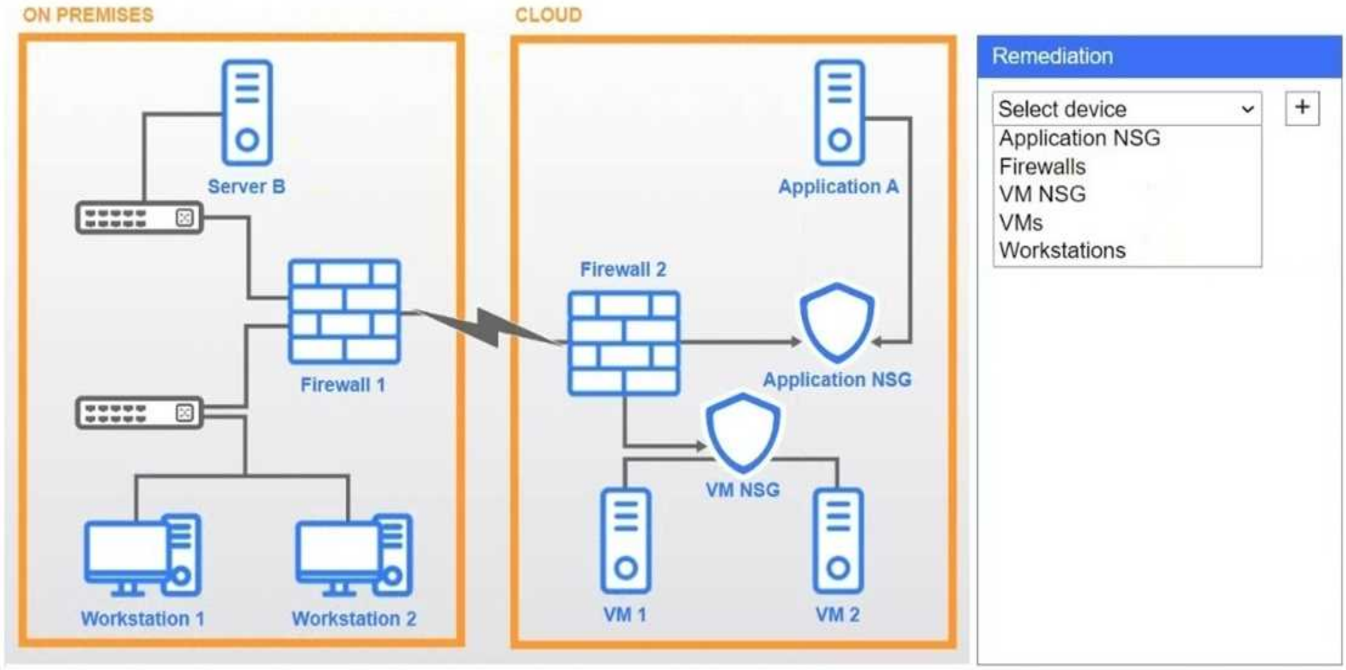
A. Workstations are able to access Server B.

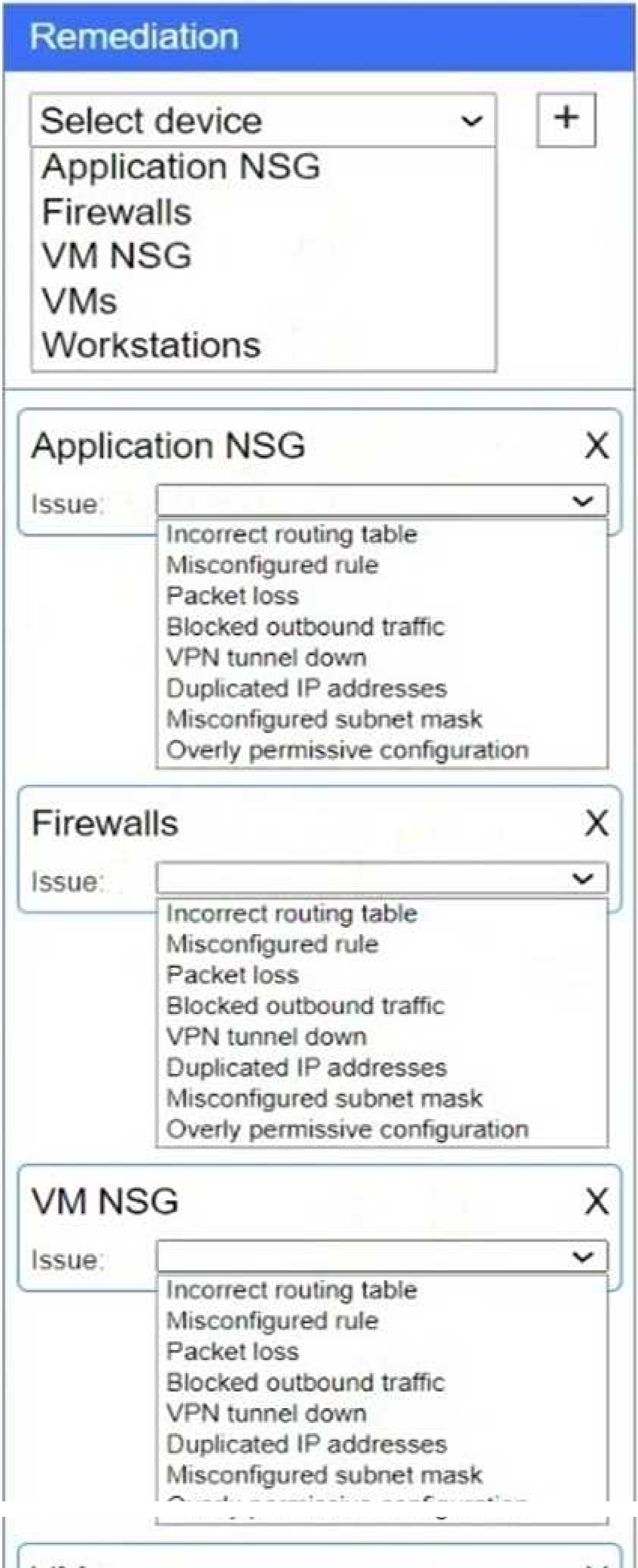
INSTRUCTIONS

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 X

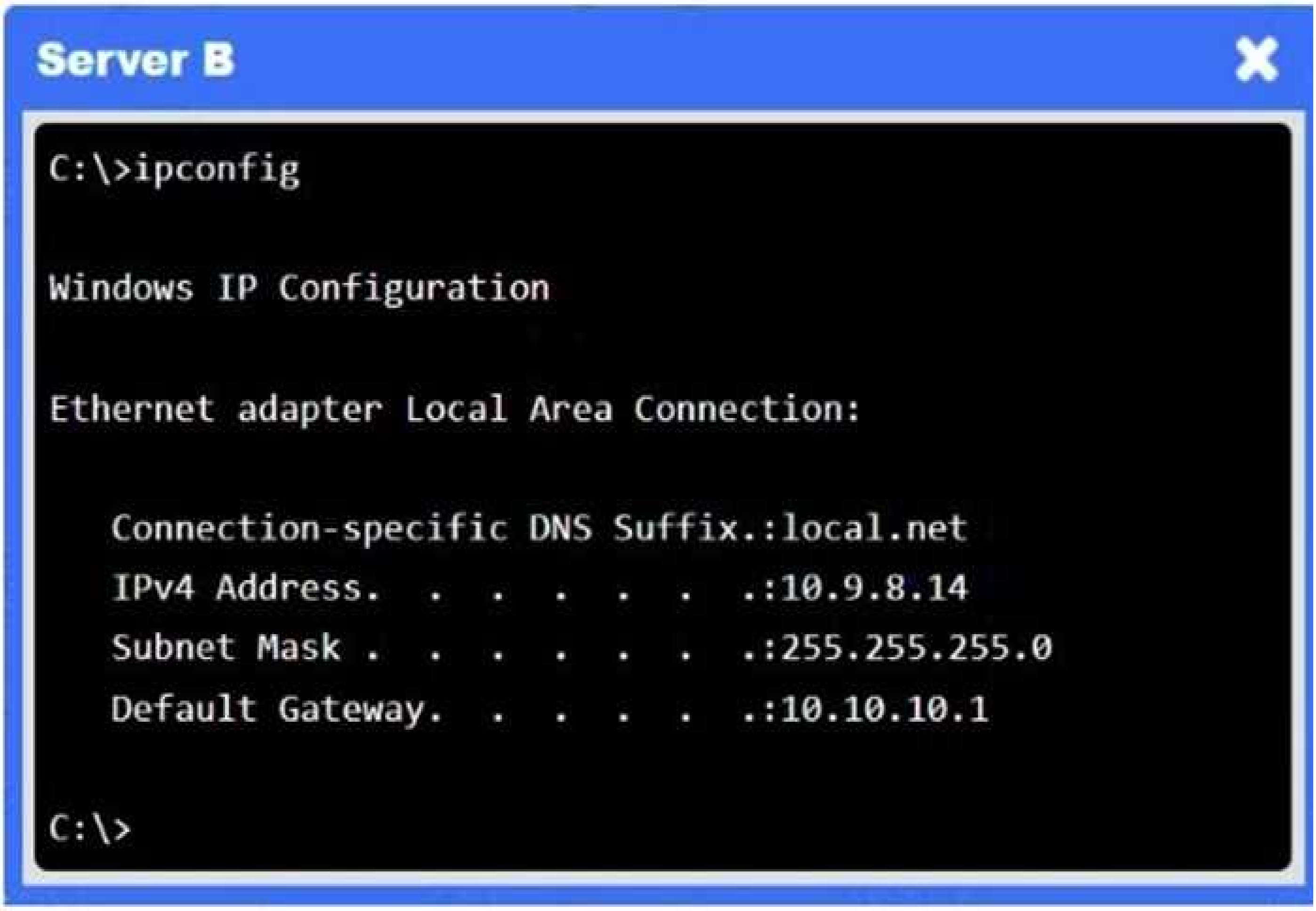
Issue:
- Incorrect routing table
- Misconfigured rule
- Packet loss
- Blocked outbound traffic
- VPN tunnel down
- Duplicated IP addresses
- Misconfigured subnet mask
- Overly permissive configuration

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

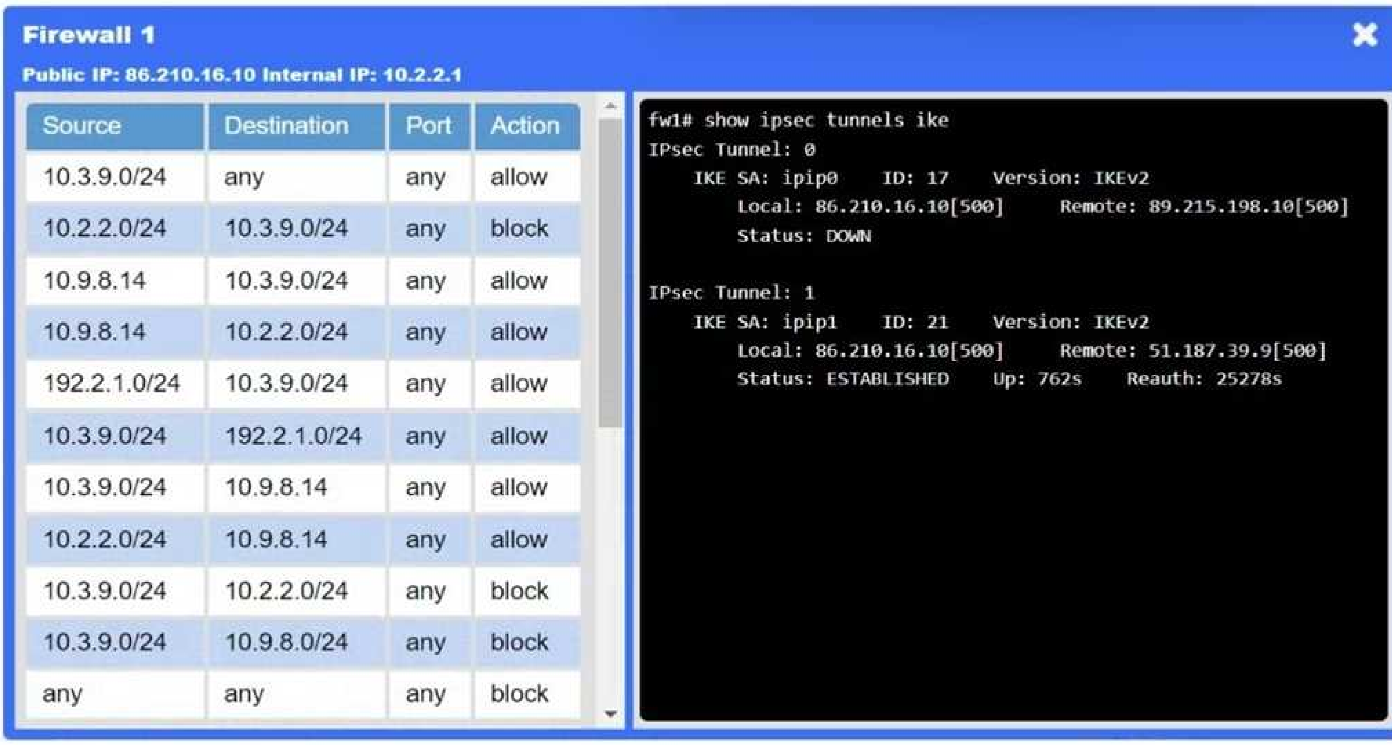
VM NSG X

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



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:\>
```

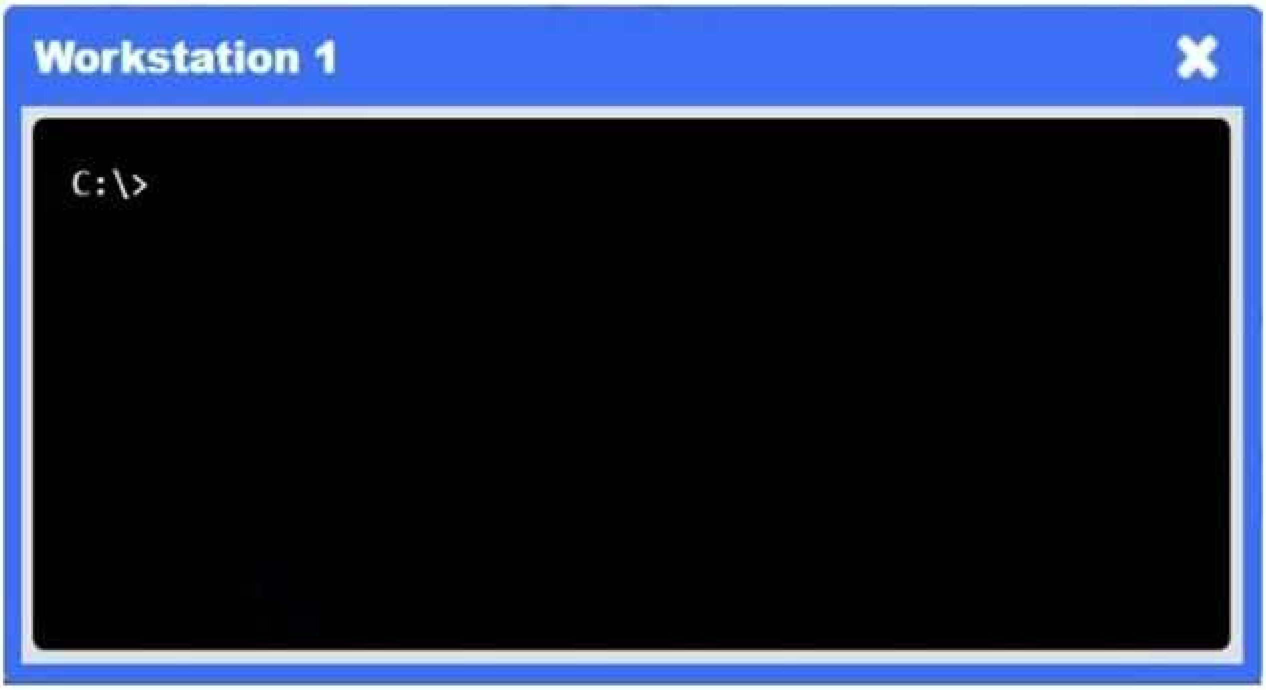


Firewall 1

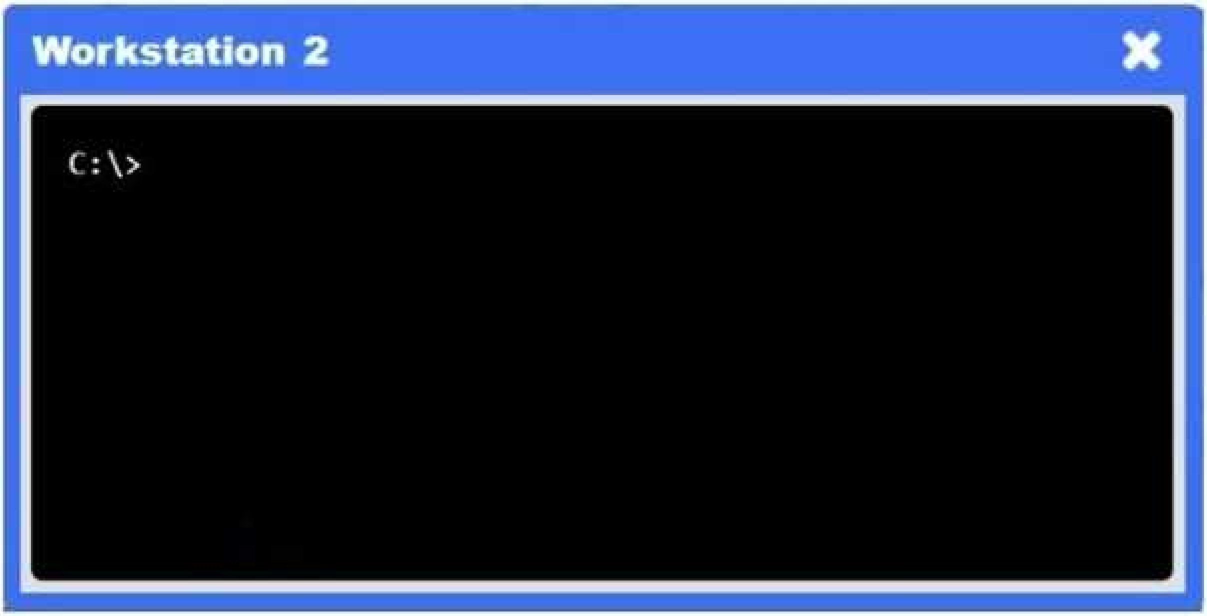
Public IP: 86.210.16.10 Internal IP: 10.2.2.1

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

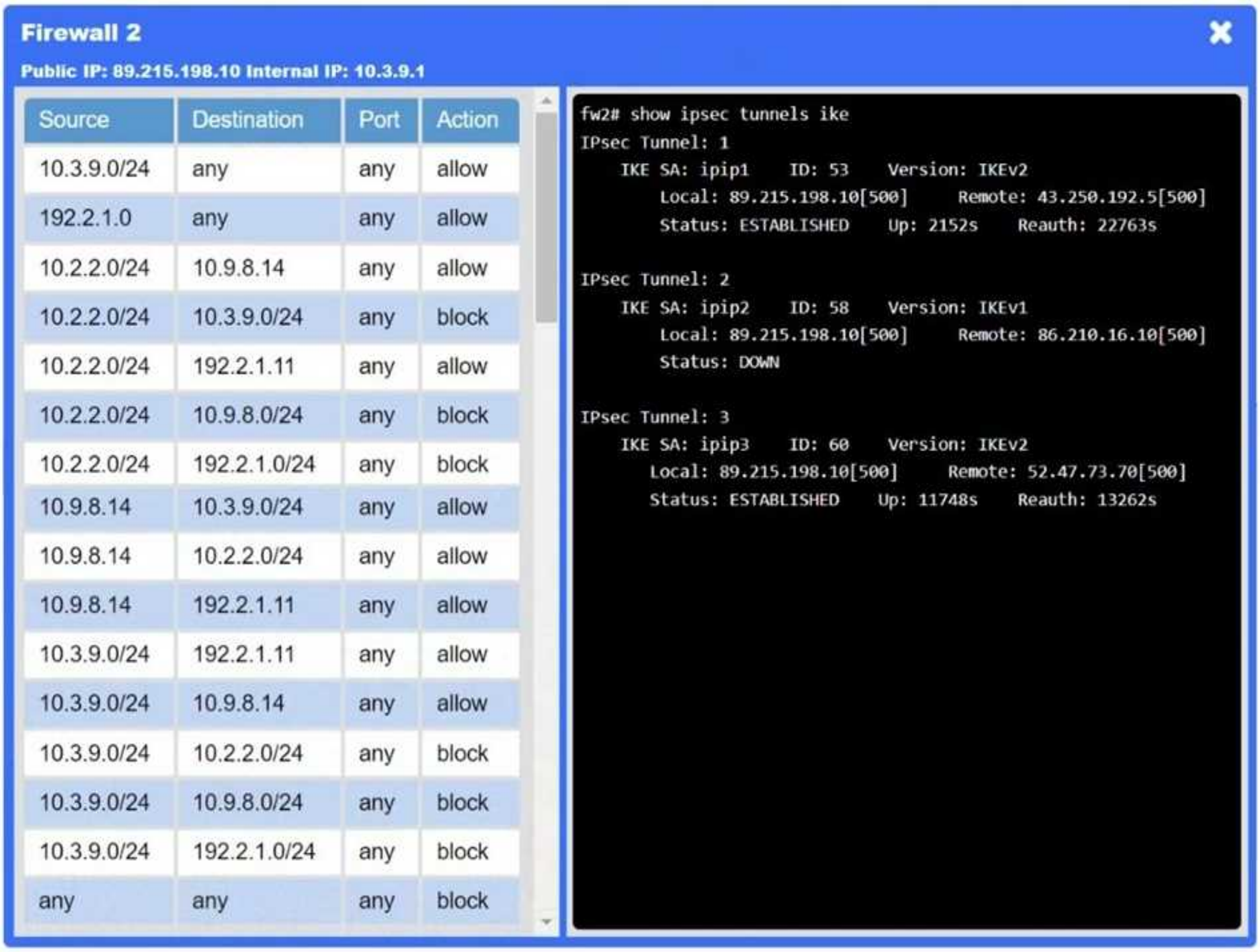
```
fw1# show ipsec tunnels ike
IPsec Tunnel: 0
    IKE SA: ipip0     ID: 17     Version: IKEv2
        Local: 86.210.16.10[500]     Remote: 89.215.198.10[500]
        Status: DOWN

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
```



```
C:\>
```



```
C:\>
```

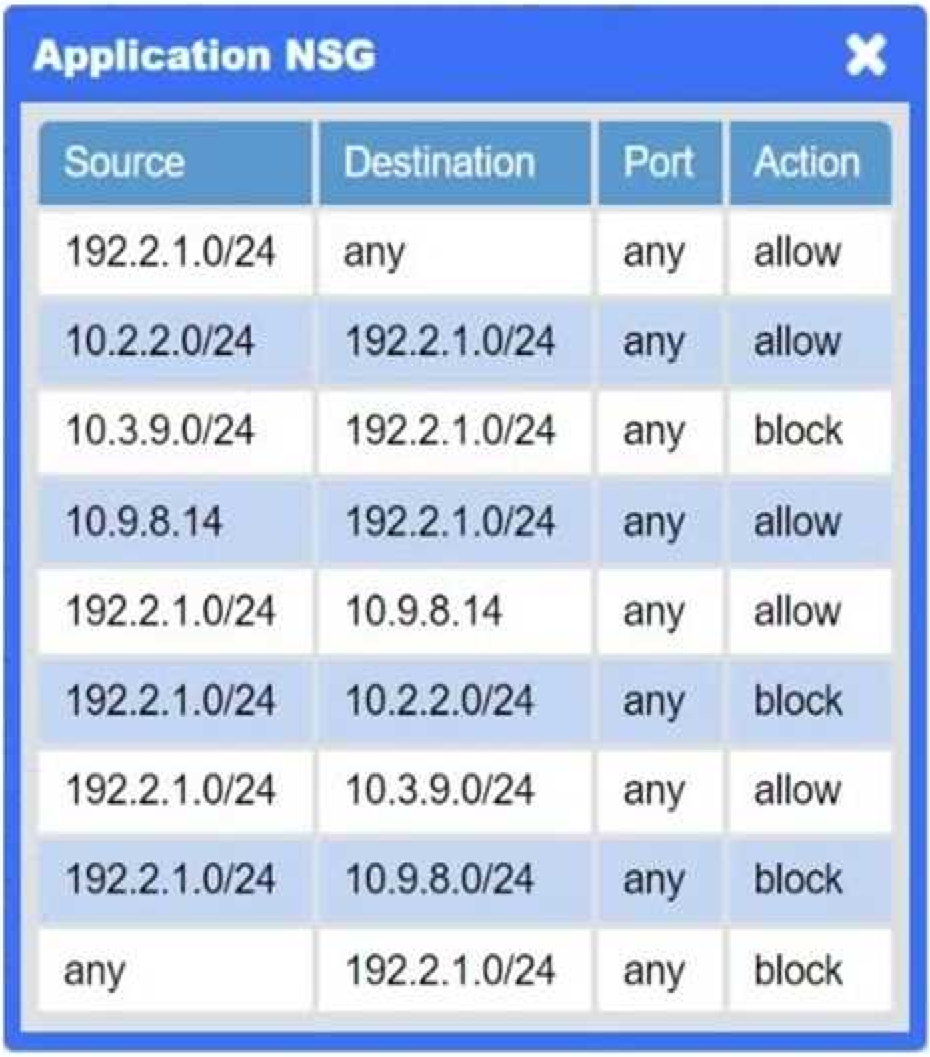


Firewall 2

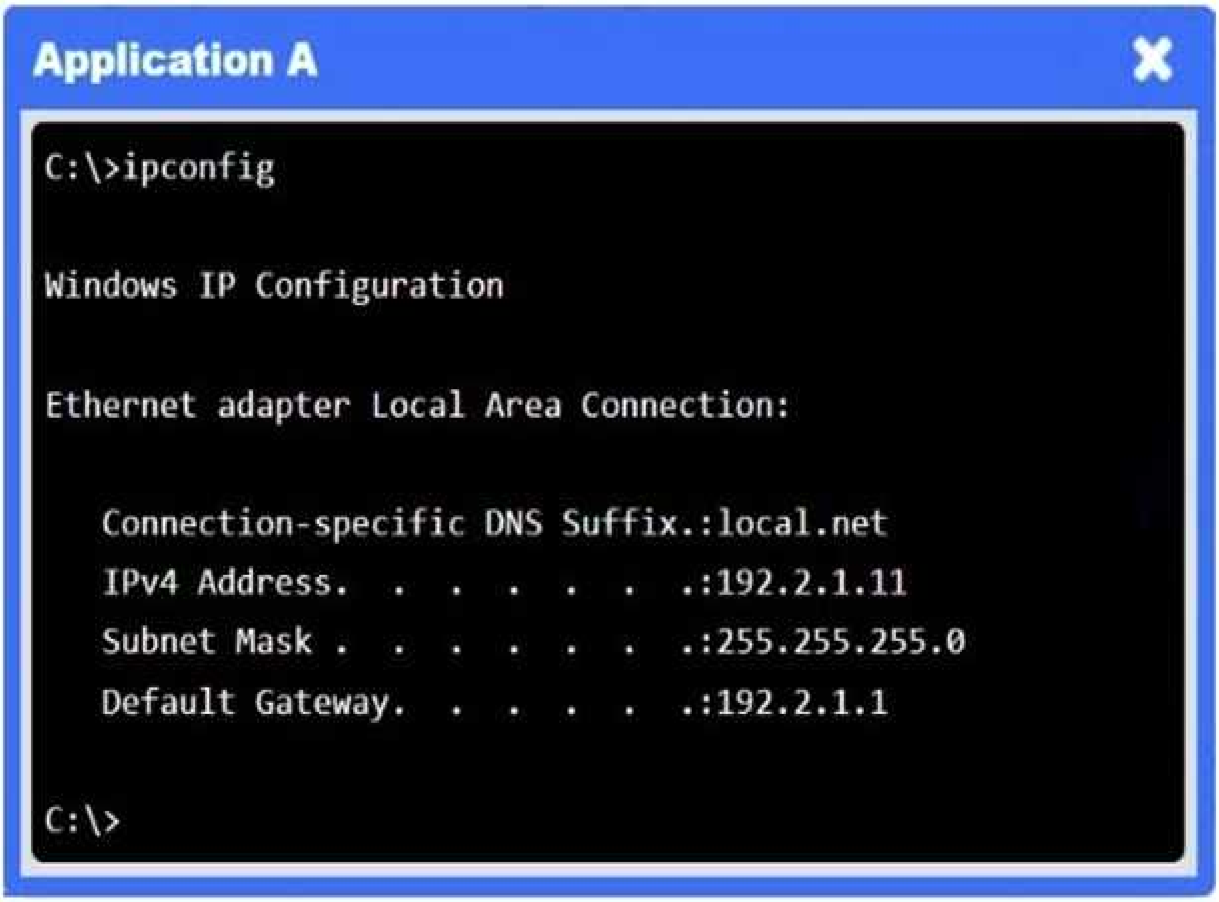
Public IP: 89.215.198.10 Internal IP: 10.3.9.1

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
```

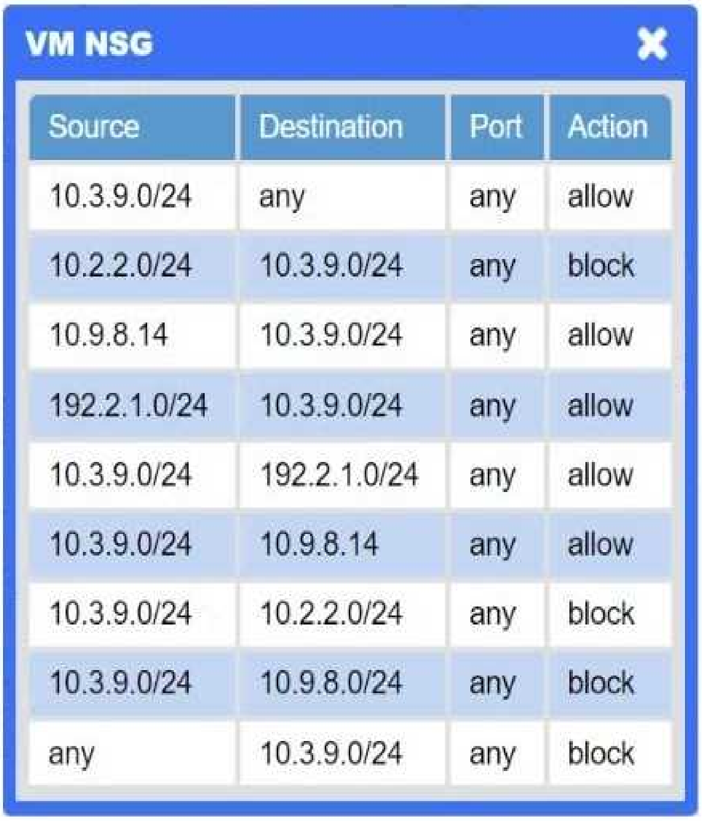


Source	Destination	Port	Action
192.2.1.0/24	any	any	allow
10.2.2.0/24	192.2.1.0/24	any	allow
10.3.9.0/24	192.2.1.0/24	any	block
10.9.8.14	192.2.1.0/24	any	allow
192.2.1.0/24	10.9.8.14	any	allow
192.2.1.0/24	10.2.2.0/24	any	block
192.2.1.0/24	10.3.9.0/24	any	allow
192.2.1.0/24	10.9.8.0/24	any	block
any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



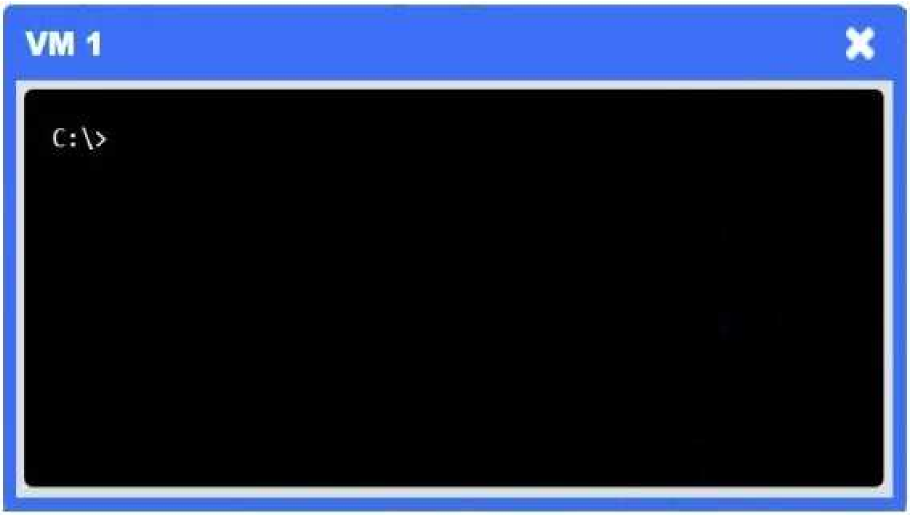
Application A

```
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:\>
```

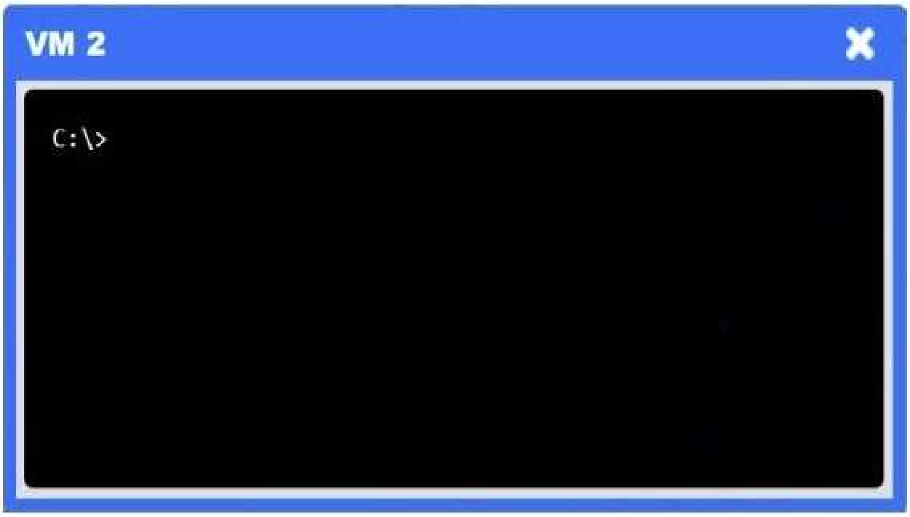


VM NSG

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



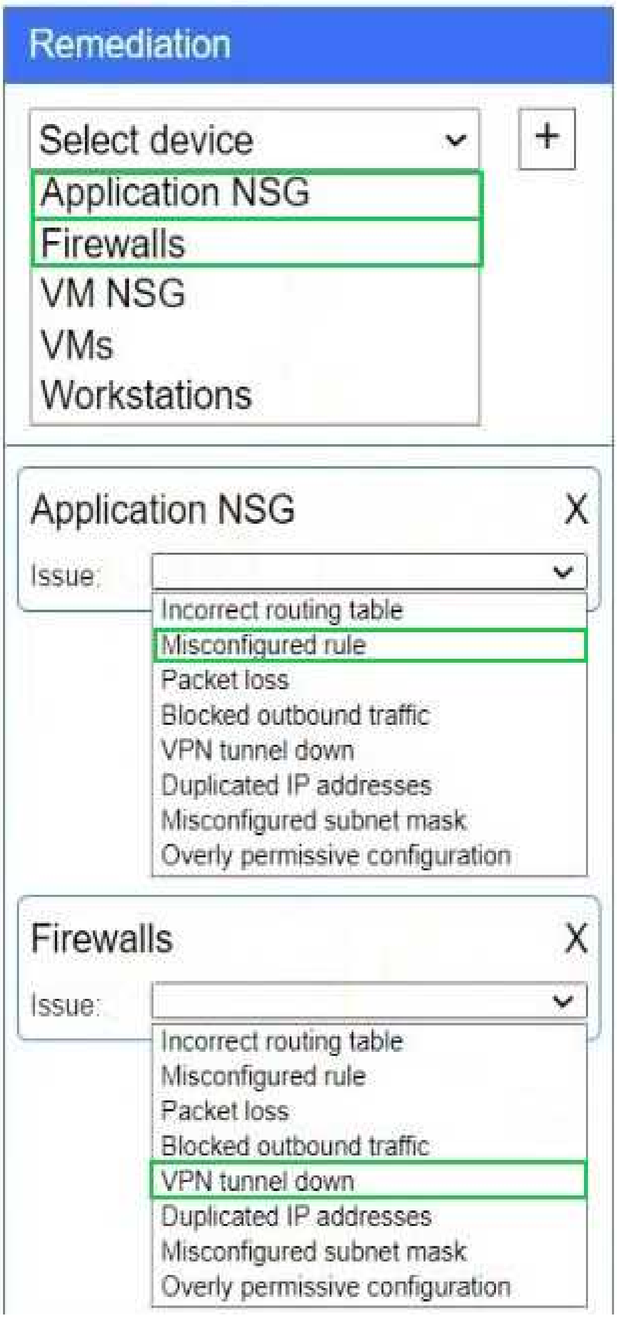
```
C:\>
```



```
C:\>
```

Answer: See explanation below.

Explanation:



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

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.

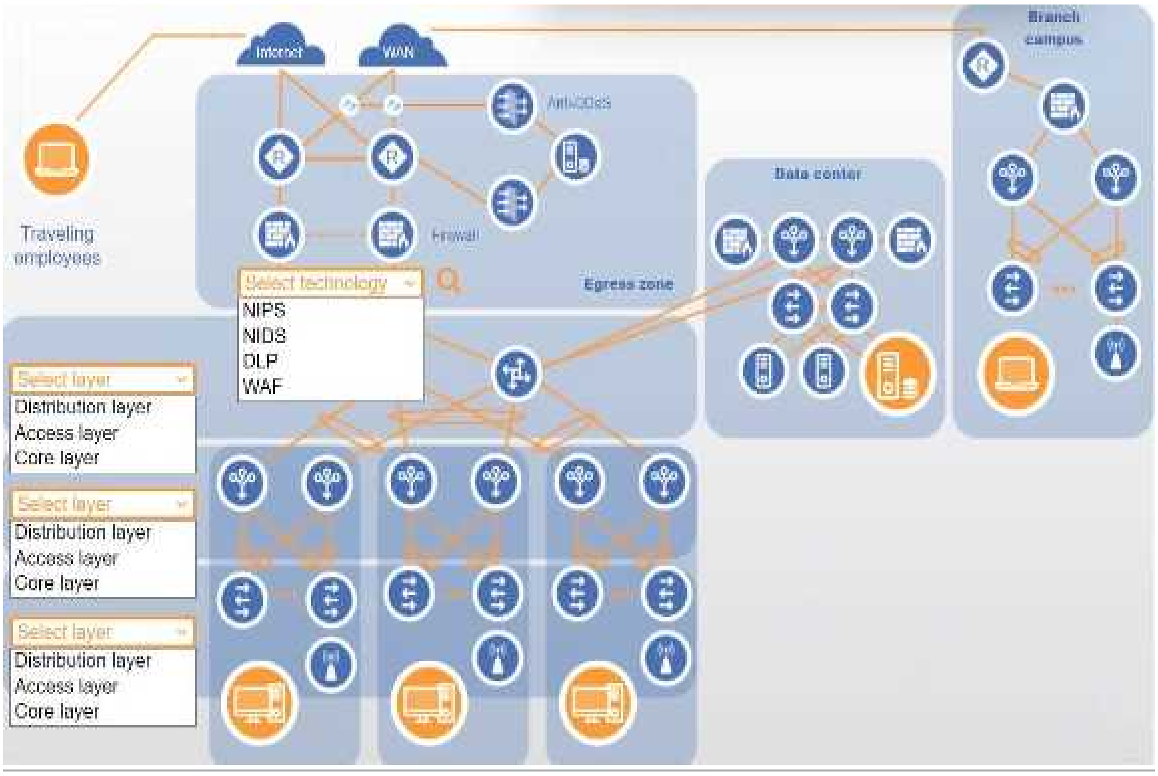
INSTRUCTIONS

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.

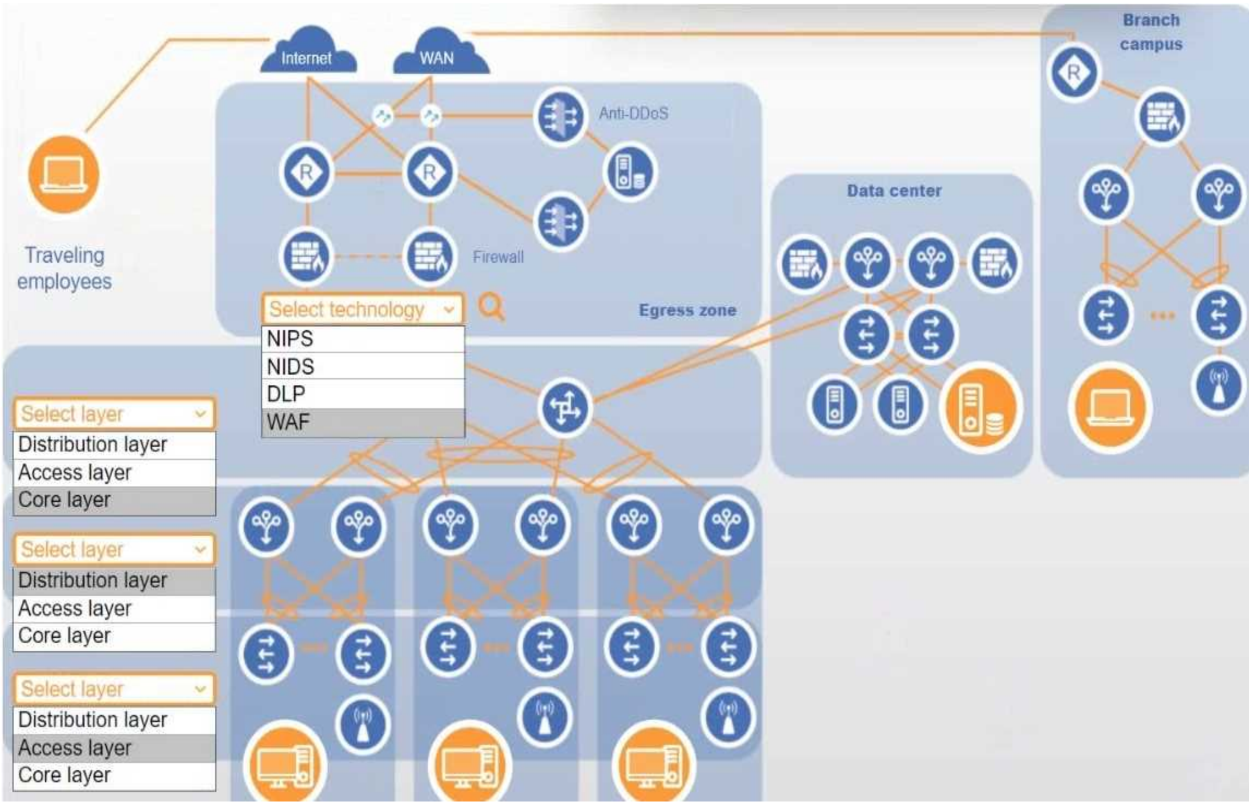
Click on the magnifying glass to make additional configuration changes.

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.)