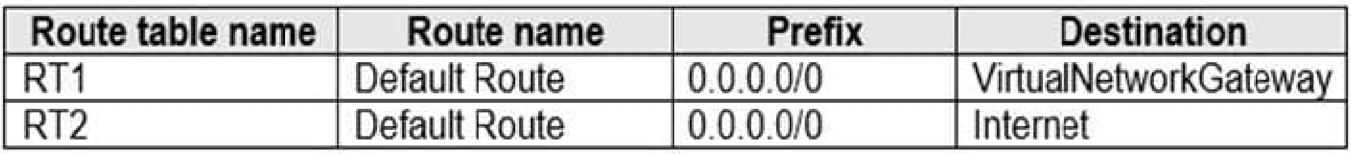
AZ-700$^{Q\&As}$

Designing and Implementing Microsoft Azure Networking Solutions

QUESTION 1

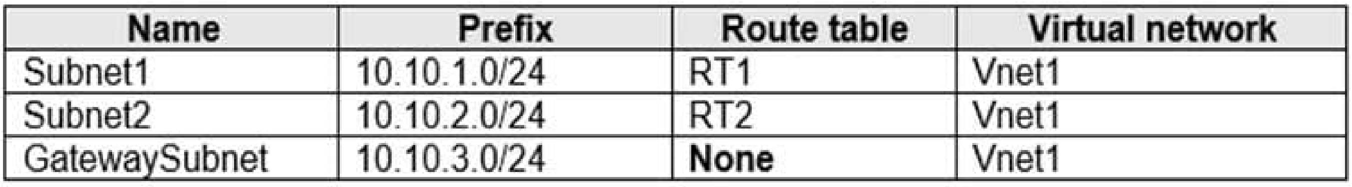
HOTSPOT

You have an Azure subscription that contains the route tables and routes shown in the following table.



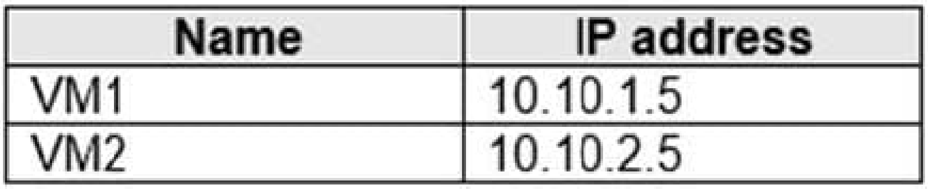
Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

The subscription contains the subnets shown in the following table.



Name	Prefix	Route table	Virtual network
Subnet1	10.10.1.0/24	RT1	Vnet1
Subnet2	10.10.2.0/24	RT2	Vnet1
GatewaySubnet	10.10.3.0/24	**None**	Vnet1

The subscription contains the virtual machines shown in the following table.



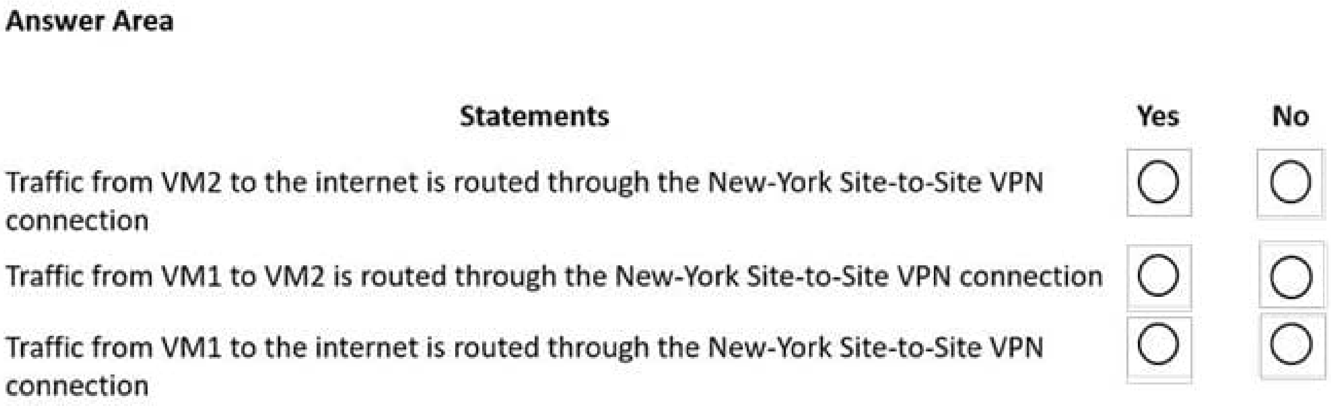
Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

There is a Site-to-Site VPN connection to each local network gateway.

For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

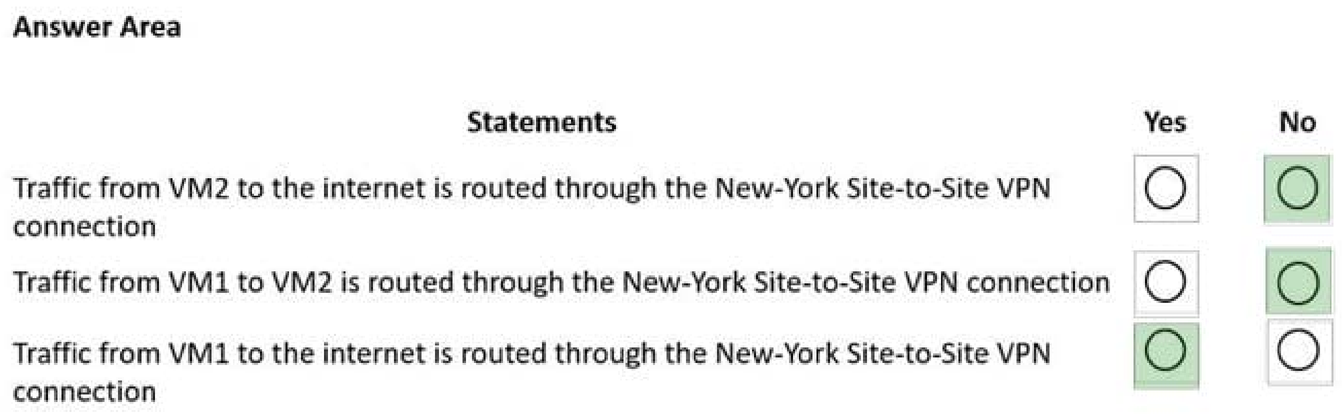
Hot Area:



Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	●
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	●
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	●	○

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

QUESTION 2

You are preparing to connect your on-premises network to VNET4 by using a Site-to-Site VPN. The on-premises endpoint of the VPN will be created on a firewall named Firewall1. The on-premises network has the following configuration:

1.

internal address range: 10.10.0.0/16

2.

Firewall1 internal IP address: 10.10.1.1

3.

Firewall public IP address: 131.107.50.60

BGP is NOT used.

You need to create the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN. You do NOT need to create a virtual network gateway to complete this task.

To complete this task, sign in to the Azure portal.

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

Create a site-to-site VPN connection in the Azure portal We only create a local network gateway

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you\\'ll create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Step 1: From the Azure portal, in Search resources, services, and docs (G+/) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

Step 2: On the Create local network gateway page, on the Basics tab, specifiy the values for your local network gateway.

*

Select Endpoint type: IP address

*

Endpoint: Enter 131.107.50.60 (The Firewall public IP address)

(IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN

device that you want Azure VPN gateway to connect to. If you don\\'t have the IP address right now, you can use the values shown in the example, but you\\'ll need to go back and replace your placeholder IP address with the public IP address

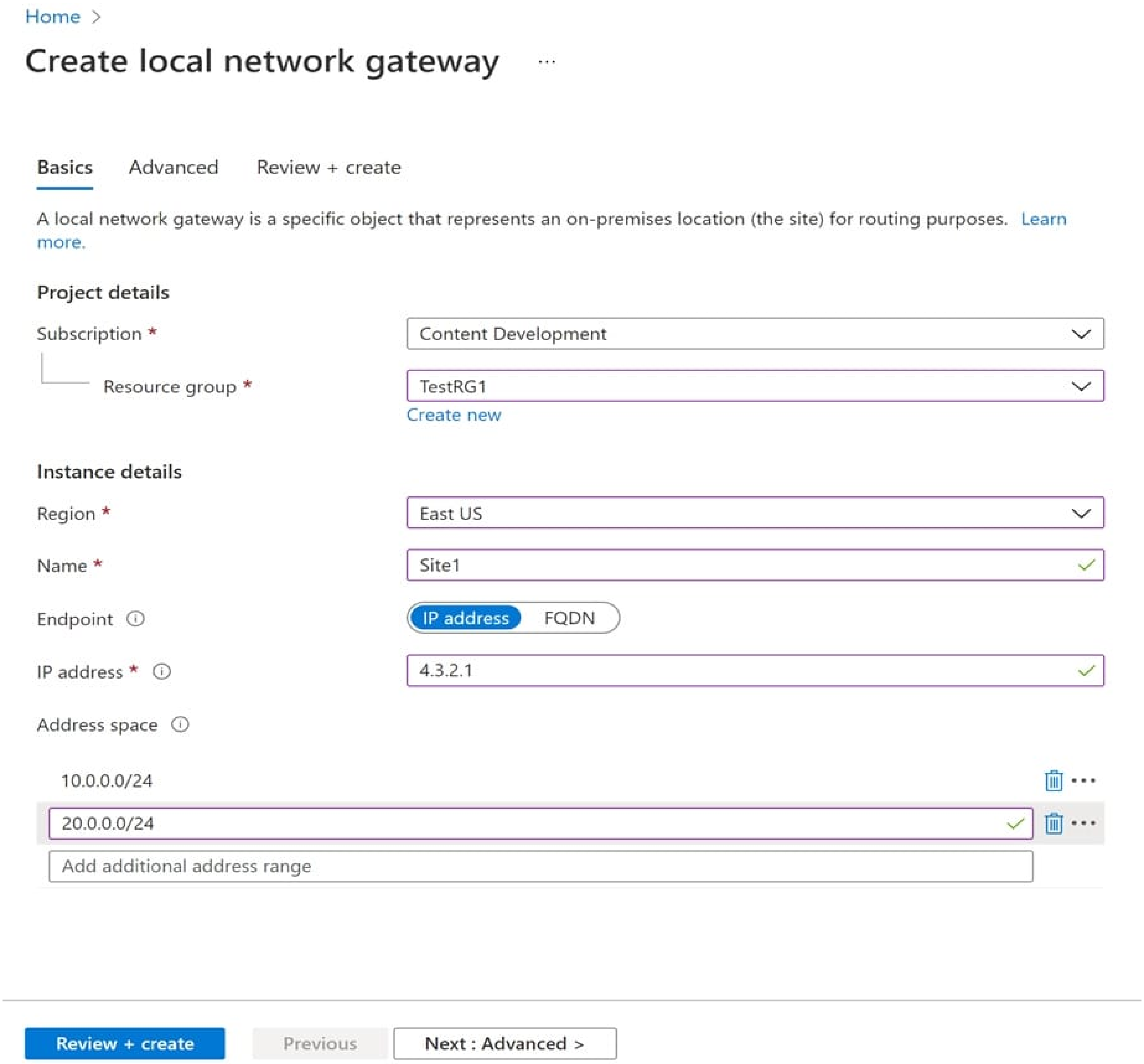
of your VPN device. Otherwise, Azure won\\'t be able to connect.)

*

Address Space: Enter 10.10.0.0/16 (The internal address range)

Select the endpoint type for the on-premises VPN device - IP address or FQDN (Fully Qualified Domain Name).

IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device.



Home >

Create local network gateway ...

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. Learn more.

Project details

Subscription * Content Development

Resource group * TestRG1

Create new

Instance details

Region * East US

Name * Site1

Endpoint: IP address (selected) FQDN

IP address * 4.3.2.1

Address space

10.0.0.0/24

20.0.0.0/24

Add additional address range

Step 3: On the Advanced tab, you can configure BGP settings if needed. Skip this.

Step 4: When you have finished specifying the values, select Review + create at the bottom of the page to validate the page.

Step 5: Select Create to create the local network gateway object.

Reference:

https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

QUESTION 3

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

A. User Access Administrator

B. Network Contributor

C. Resource Policy Contributor

D. Monitoring Contributor

Correct Answer: A

As an administrator, you can lock an Azure subscription, resource group, or resource to protect them from accidental user deletions and modifications. The lock overrides any user permissions.

Unlike role-based access control (RBAC), you use management locks to apply a restriction across all users and roles.

Who can create or delete locks

To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You

can create a custom role with the required permissions.

Note: Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS

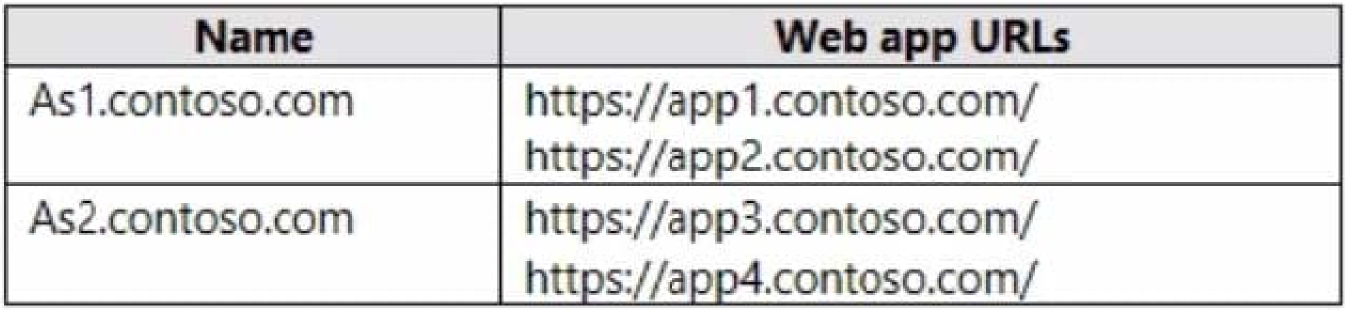
(Infrastructure-as-a-Service) products including Virtual Machines (VM), Virtual Networks, Application Gateways, Load balancers, etc.

Reference: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

QUESTION 4

HOTSPOT

You have two Azure App Service instances that host the web apps shown the following table.



Name	Web app URLs
As1.contoso.com	https://app1.contoso.com/ https://app2.contoso.com/
As2.contoso.com	https://app3.contoso.com/ https://app4.contoso.com/

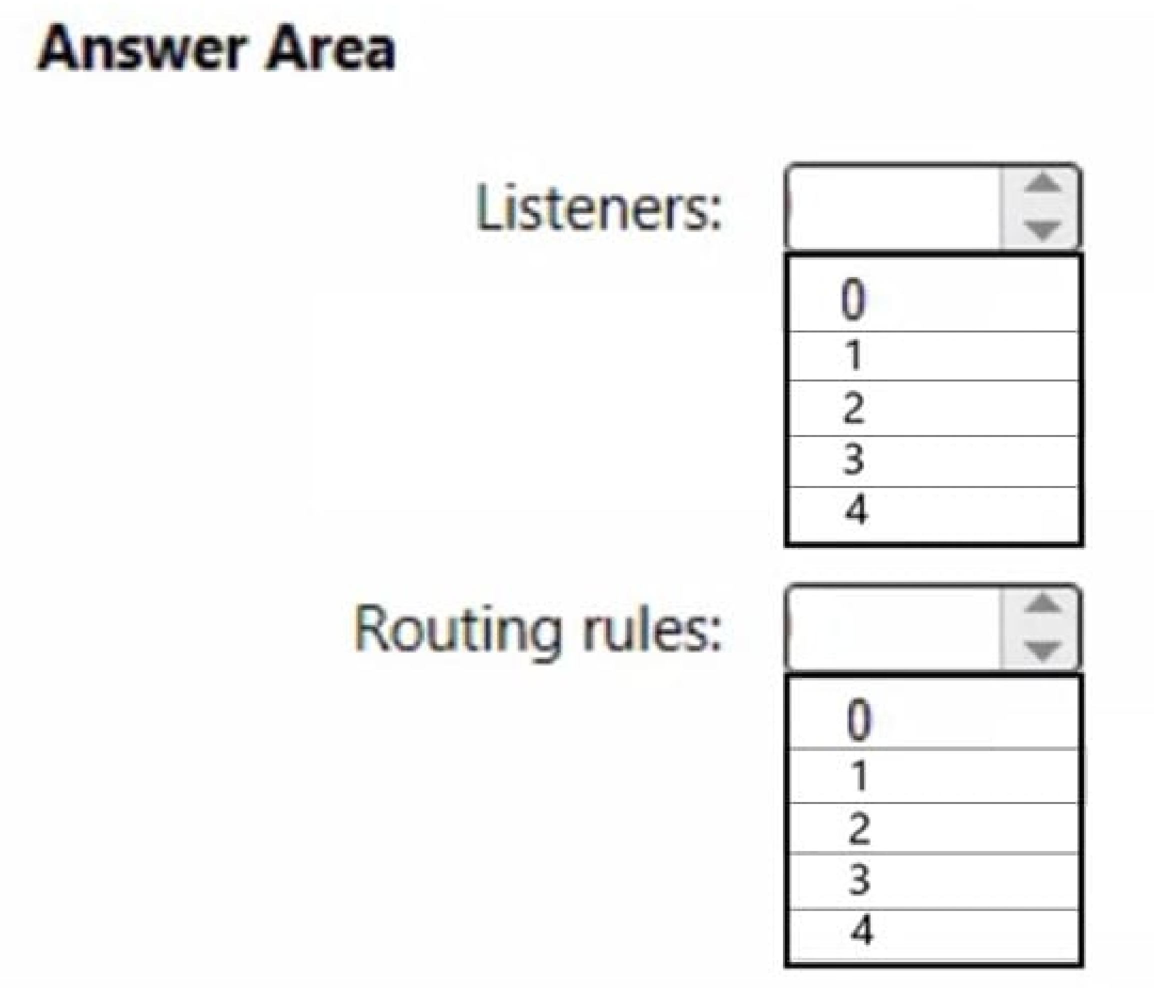
You deploy an Azure 2 that has one public frontend IP address and two backend pools.

You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.

What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

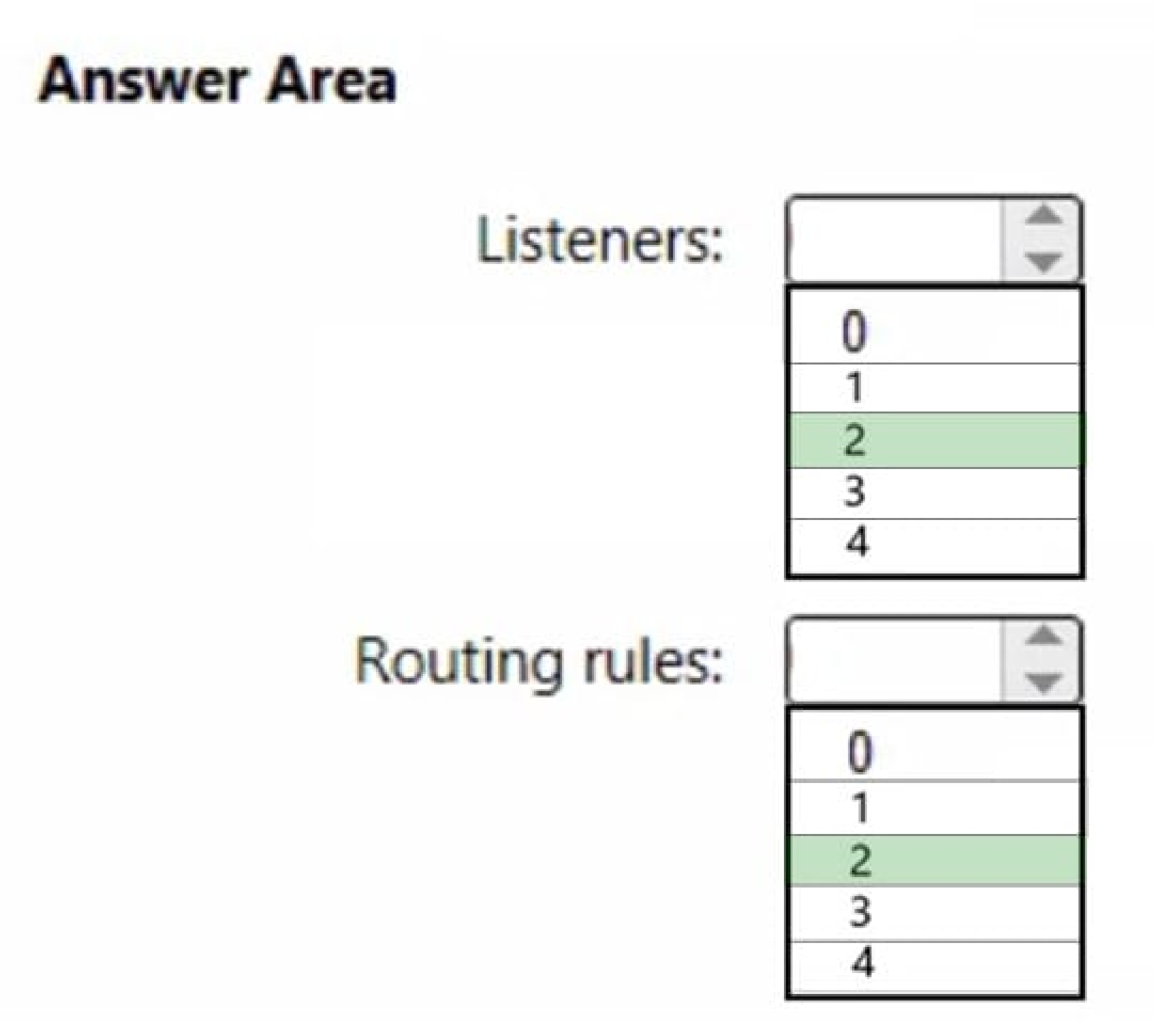


Answer Area

Listeners:
- 0
- 1
- 2
- 3
- 4

Routing rules:
- 0
- 1
- 2
- 3
- 4

Correct Answer:



Answer Area

Listeners:

- 0
- 1
- 2
- 3
- 4

Routing rules:

- 0
- 1
- 2
- 3
- 4

Box 1: 2 Listeners

One listener for As1.contoso.com, and one listener for As2.contoso.com.

Note: Multiple site hosting enables you to configure more than one web application on the same port of application gateways using public-facing listeners. It allows you to configure a more efficient topology for your deployments by adding up to 100+ websites to one application gateway. Each website can be directed to its own backend pool. For example, three domains, contoso.com, fabrikam.com, and adatum.com, point to the IP address of the application gateway. You\\'d create three multi-site listeners and configure each listener for the respective port and protocol setting.

You can also define wildcard host names in a multi-site listener and up to 5 host names per listener.

Box 2: 2 Routing rules

Application Gateway request routing rules Rule type When you create a rule, you choose between basic and path-based.

*

Choose basic if you want to forward all requests on the associated listener (for example, blog.contoso.com/*) to a single backend pool.

*

Choose path-based if you want to route requests from specific URL paths to specific backend pools. The path pattern is applied only to the path of the URL, not to its query parameters.

Associated backend pool

Associate to the rule the backend pool that contains the backend targets that serve requests that the listener receives.

*

For a basic rule, only one backend pool is allowed. All requests on the associated listener are forwarded to that backend pool.

*

For a path-based rule, add multiple backend pools that correspond to each URL path. The requests that match the URL path that\\'s entered are forwarded to the corresponding backend pool. Also, add a default backend pool. Requests that

don\\'t match any URL path in the rule are forwarded to that pool.

Reference: https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview

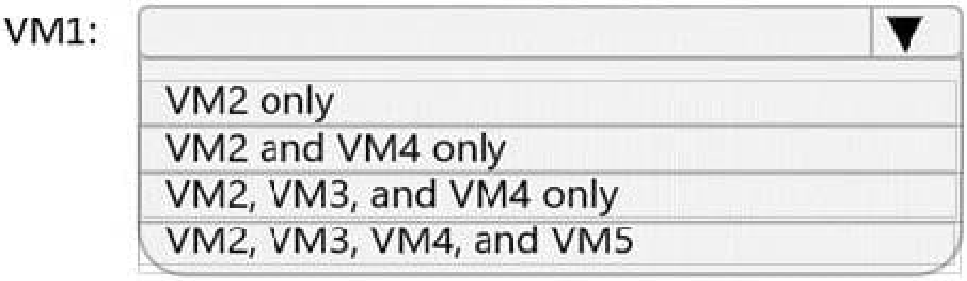
QUESTION 5

HOTSPOT

Which virtual machines can VM1 and VM4 ping successfully? To answer, select the appropriate options in the answer area.

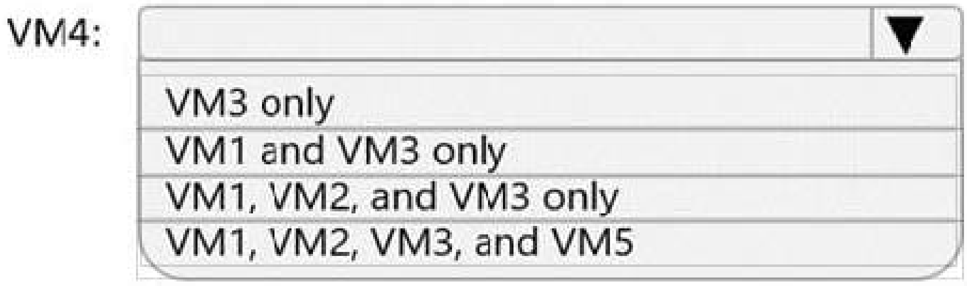
NOTE: Each correct selection is worth one point.

Hot Area:



VM1: ▼

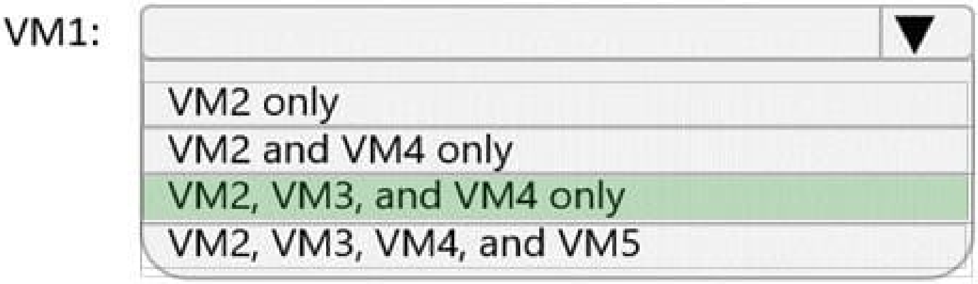
- VM2 only
- VM2 and VM4 only
- VM2, VM3, and VM4 only
- VM2, VM3, VM4, and VM5



VM4: ▼

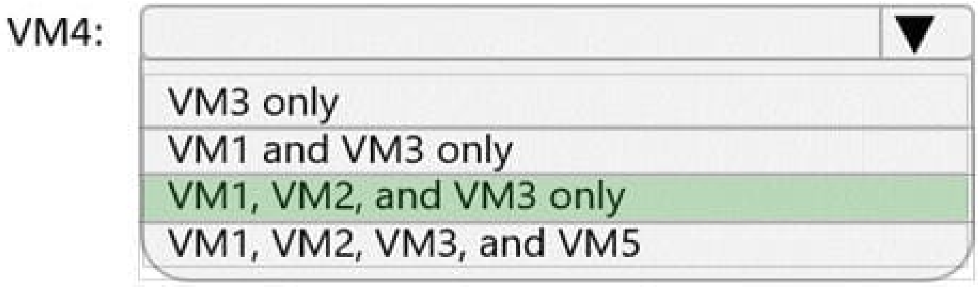
- VM3 only
- VM1 and VM3 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM5

Correct Answer:



VM1: ▼

- VM2 only
- VM2 and VM4 only
- [✓ VM2, VM3, and VM4 only]
- VM2, VM3, VM4, and VM5



VM4: ▼

- VM3 only
- VM1 and VM3 only
- [✓ VM1, VM2, and VM3 only]
- VM1, VM2, VM3, and VM5

Box 1: VM2, VM3 and VM4.

VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3.

There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3. Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.

Box 2:

VM4 is in VNet3. VNet3 is peered with VNet1 and VNet2. There are no NSGs blocking outbound ICMP from VNet3. There are no NSGs blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3 (NSG10 blocks

inbound ICMP from VNet4 but not from VNet3). Therefore, VM4 can ping VM1 in VNet1/Subnet1, VM2 in VNet1/Subnet2 and VM3 in VNet2.

Latest AZ-700 Dumps AZ-700 VCE Dumps AZ-700 Study Guide