AZ-700 Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your company has an office in New York.

The company has an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
Vnet1	East US
Vnet2	North Europe
Vnet3	West US
Vnet4	West Europe

You need to connect the virtual networks to the office by using ExpressRoute. The solution must meet the following requirements:

1.

The connection must have up to 1 Gbps of bandwidth.

2.

The office must have access to all the virtual networks.

3.

Costs must be minimized.

How many ExpressRoute circuits should be provisioned, and which ExpressRoute SKU should you enable?

A. one ExpressRoute Premium circuit

B. two ExpressRoute Premium circuits

C. four ExpressRoute Standard circuits

D. one ExpressRoute Standard circuit

Correct Answer: A

One SKU Premium required.

Azure ExpressRoute offers three different circuit SKUs, known as Local, Standard, and Premium, which provide varying degrees of connectivity scope.

Standard: a Standard SKU ExpressRoute circuit provides connectivity to resources in all Azure regions in a geopolitical area. Under this scenario, the on-premises network in London can connect to resources and access Azure\\'s cloud

services hosted in regions such as West Europe (Amsterdam, Netherlands) and France Central (Paris, France) through ExpressRoute

Premium: a Premium SKU ExpressRoute circuit facilitates connectivity to resources and cloud services globally across

all Azure regions. Specifically, this global connectivity is delivered over the Microsoft core network. In this case, the on-

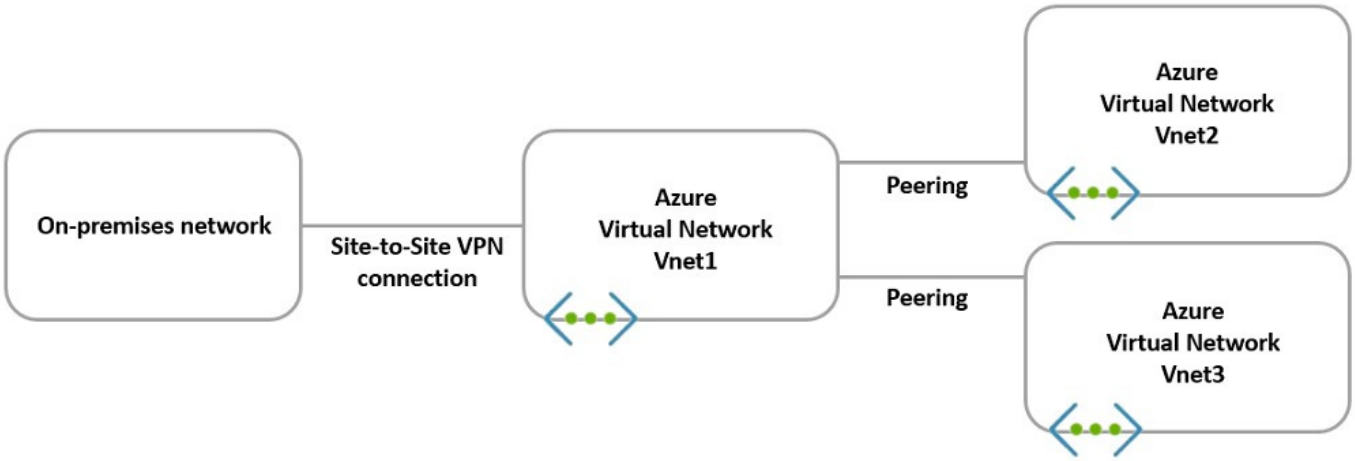
premises network in London can link a virtual network created in West Europe (Amsterdam, Netherlands) to an Azure ExpressRoute circuit created in Japan East (Tokyo, Japan)

Reference: https://dgtlinfra.com/azure-expressroute-benefits-pricing-providers-locations/

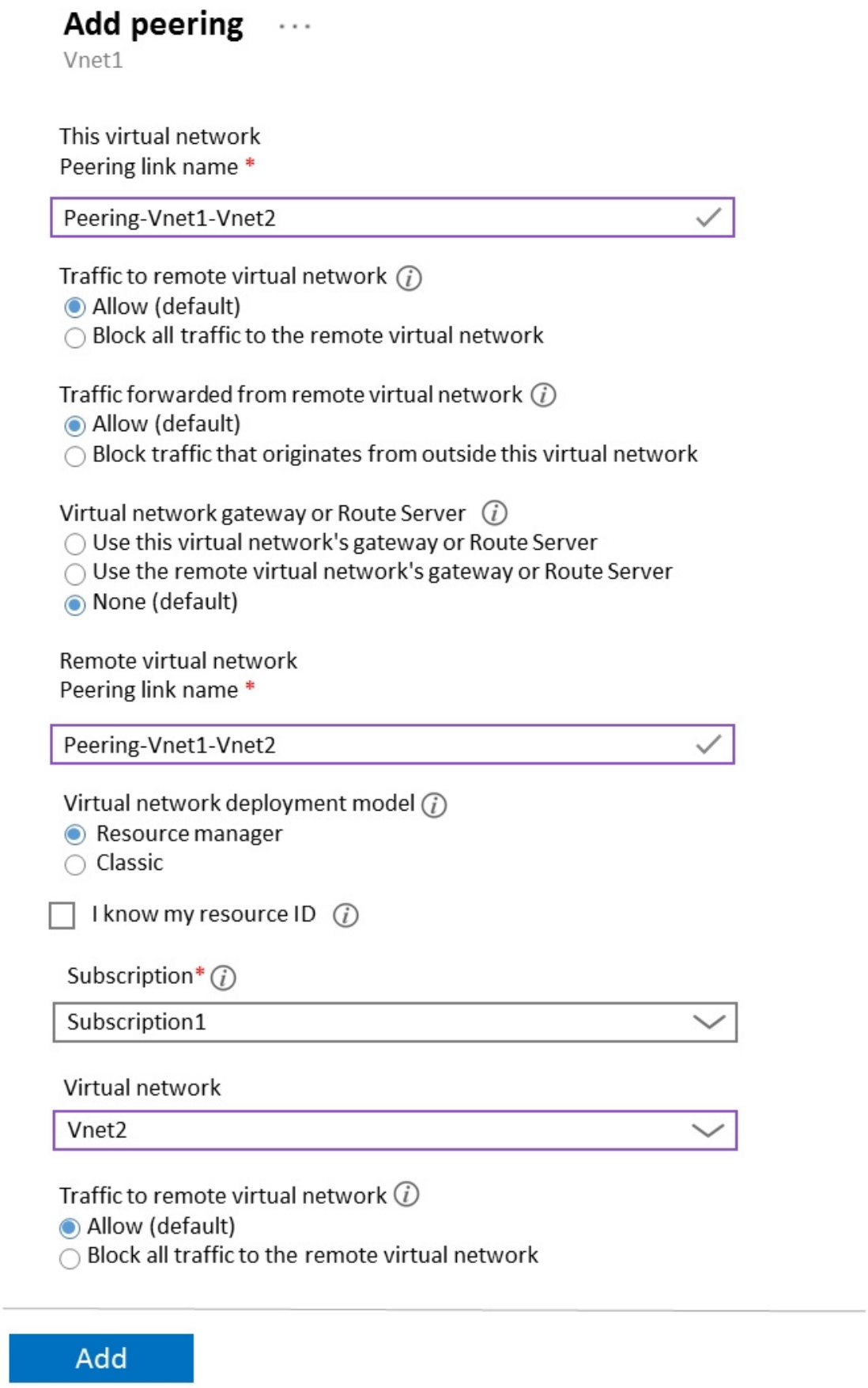
QUESTION 2

HOTSPOT

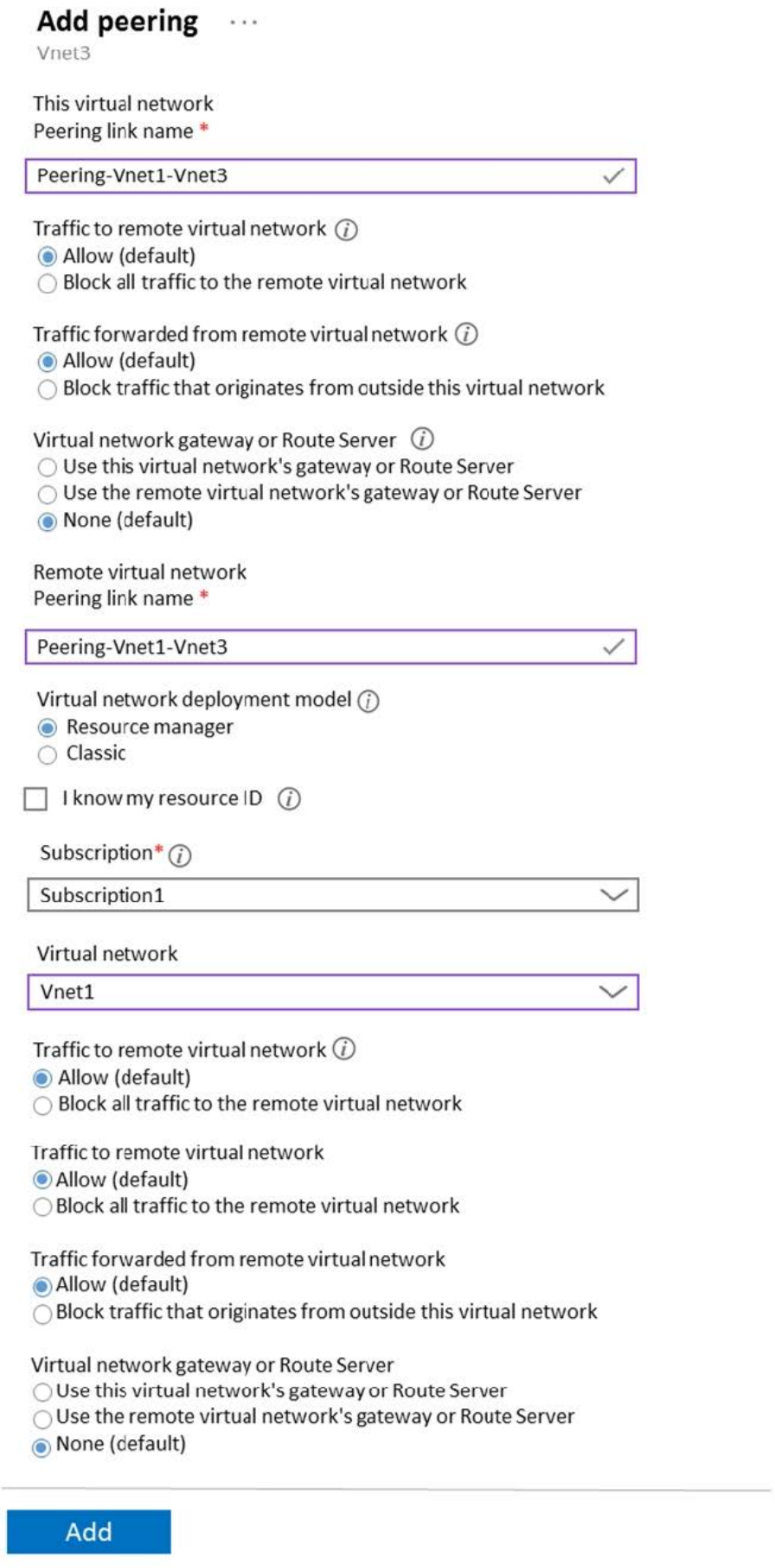
You have the hybrid network shown in the Network Diagram exhibit.



You have a peering connection between Vnet1 and Vnet2 as shown in the Peering-Vnet1-Vnet2 exhibit.


Add peering
Vnet1
This virtual network
Peering link name *
Peering-Vnet1-Vnet2
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network
Allow (default)
Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server
Use this virtual network's gateway or Route Server
Use the remote virtual network's gateway or Route Server
None (default)
Remote virtual network
Peering link name *
Peering-Vnet1-Vnet2
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription*
Subscription1
Virtual network
Vnet2
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Add

You have a peering connection between Vnet1 and Vnet3 as shown in the Peering-Vnet1-Vnet3 exhibit.


Add peering
Vnet3
This virtual network
Peering link name *
Peering-Vnet1-Vnet3
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network
Allow (default)
Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server
Use this virtual network's gateway or Route Server
Use the remote virtual network's gateway or Route Server
None (default)
Remote virtual network
Peering link name *
Peering-Vnet1-Vnet3
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription*
Subscription1
Virtual network
Vnet1
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network
Allow (default)
Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server
Use this virtual network's gateway or Route Server
Use the remote virtual network's gateway or Route Server
None (default)
Add

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	○	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	○
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	○

Correct Answer:

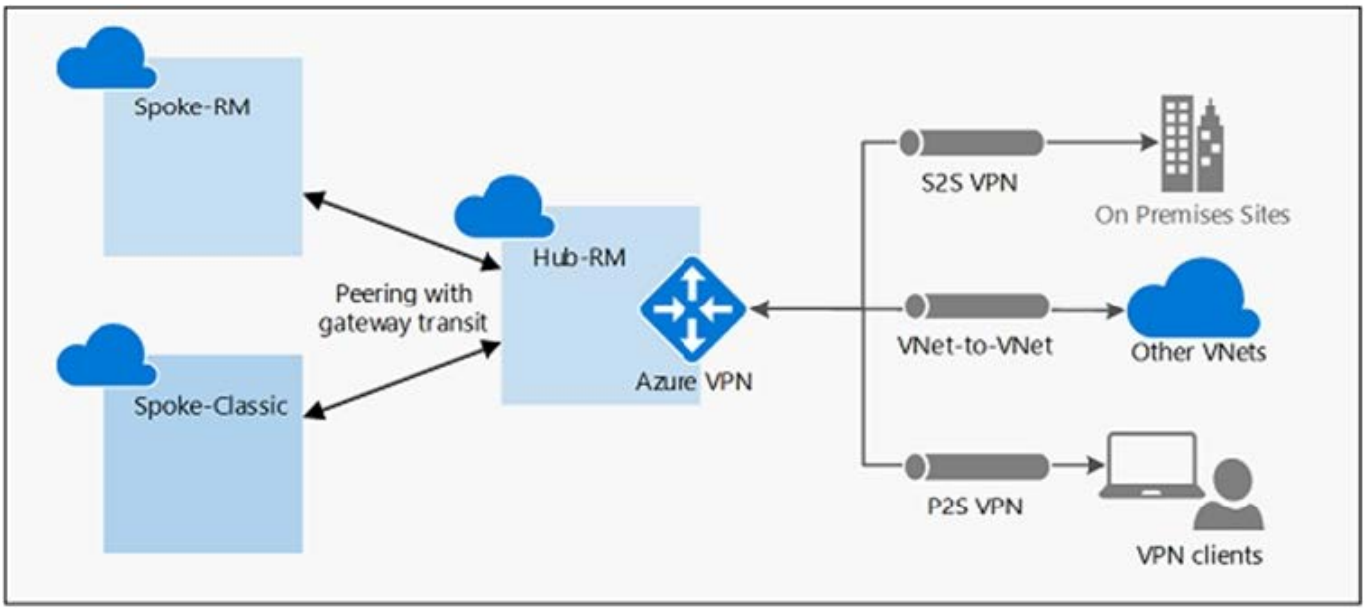
Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	●	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	●
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	●

Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.

Box 2: No No Virtual Gateway is used. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual

networks.

Box 3: No

No Virtual Gateway is used.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

QUESTION 4

You have an Azure subscription and an on-premises environment that is connected via ExpressRoute circuit.

You have two additional branch offices that you need to connect to the network.

Several employees work remotely.

Employees change locations frequently but still need access to Azure resources.

You need to deploy a solution at the earliest. The costs must be minimal.

What should you deploy?

A. Point-to-Site VPN

B. Site-to-Site VPN

C. Virtual WAN

D. Hub-and-Spoke Network Topology

Correct Answer: C

Correct Answer(s):

The Virtual WAN architecture is a hub and spoke architecture for branches and users. It enables global transit network architecture, where the cloud-hosted network \\'hub\\' enables transitive connectivity between endpoints that may be

distributed across different types of \\'spokes\\'. All hubs are connected in full mesh in a Standard Virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity. This satisfies the requirement to

provide the quickest set up at the lowest cost.

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Wrong Answers:

Point-to-Site VPN - A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.

Site-to-Site VPN Site-to-Site VPN gateways provide cross-premises connectivity between customer premises and Azure.

Hub-and-Spoke Network Topology This is one of the architecture model used to deploy Azure environment.

QUESTION 5

HOTSPOT

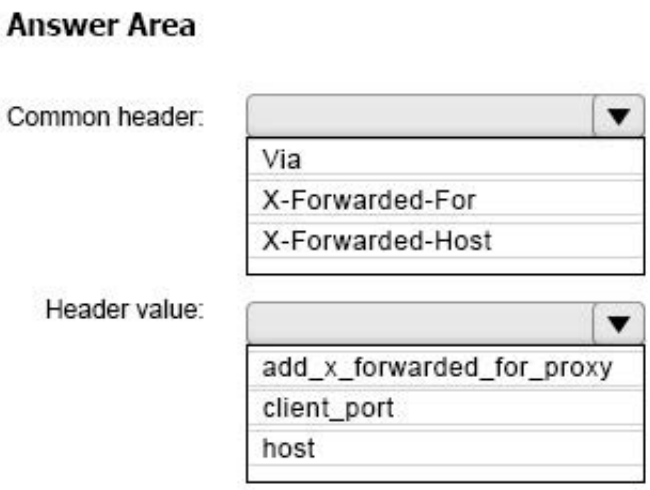
You have an Azure application gateway.

You need to create a rewrite rule that will remove the origin port from the HTTP header of incoming requests that are being forwarded to the backend pool.

How should you configure each setting? To answer, select the appropriate options in the answer area.

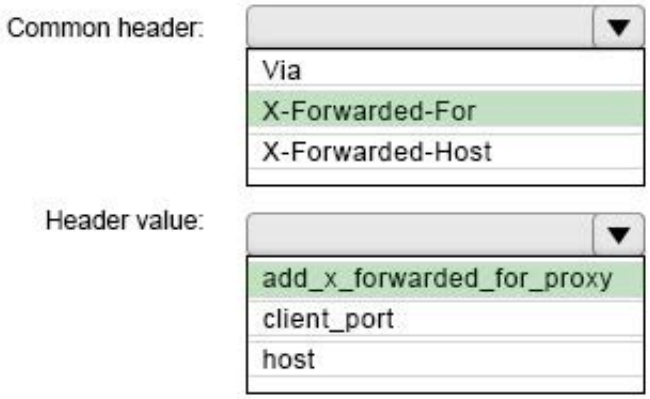
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



The X-Forwarded-For client request header field with the client_ip variable (see explanation later in this table) appended to it in the format IP1, IP2, IP3, and so on. If the X-Forwarded-For field isn\\'t in the client request header, the add_x_forwarded_for_proxy variable is equal to the $client_ip variable. This variable is particularly useful when you want to rewrite the X-Forwarded-For header set by Application Gateway so that the header contains only the IP address without the port information.

https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url

QUESTION 6

DRAG DROP

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure App Service app	Accessed by using a URL of https://app1.contoso.com/
FD1	Azure Front Door Premium profile	Configured as an endpoint for App1
contoso.com	Azure DNS zone	Contains a DNS CNAME record for App1 that resolves to an FQDN of app1.azurewebsites.net

You discover that users connect directly to App1. You need to meet the following requirements:

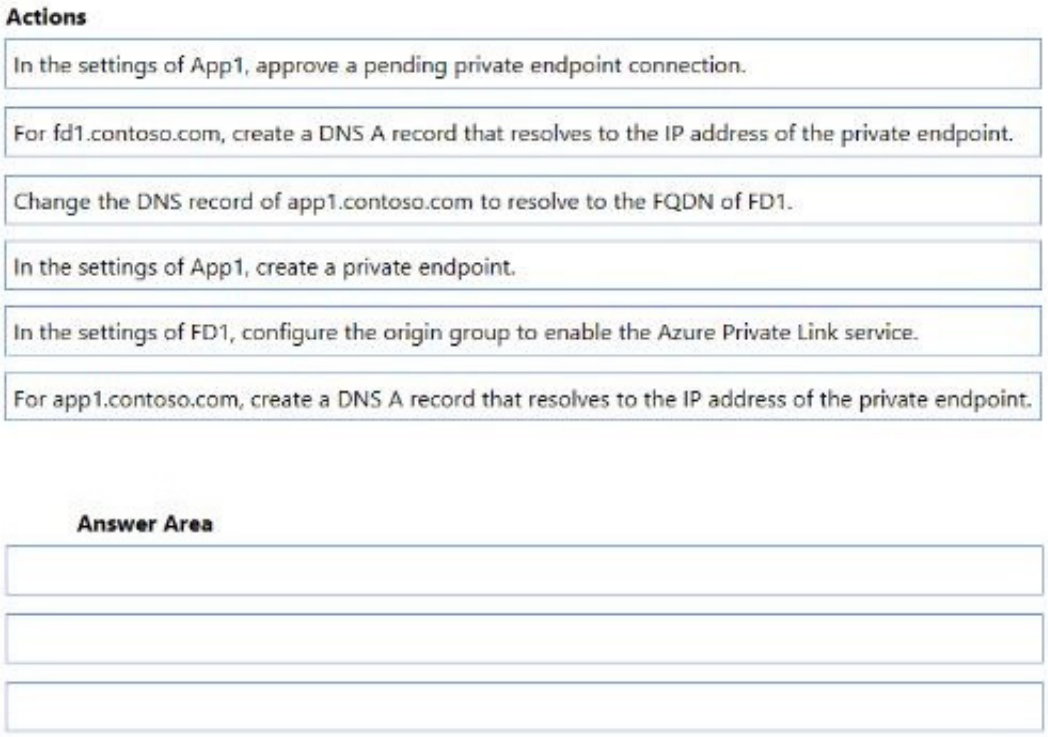
Administrators must only access App1 by using a private endpoint.

All user connections to App1 must be routed through FD1.

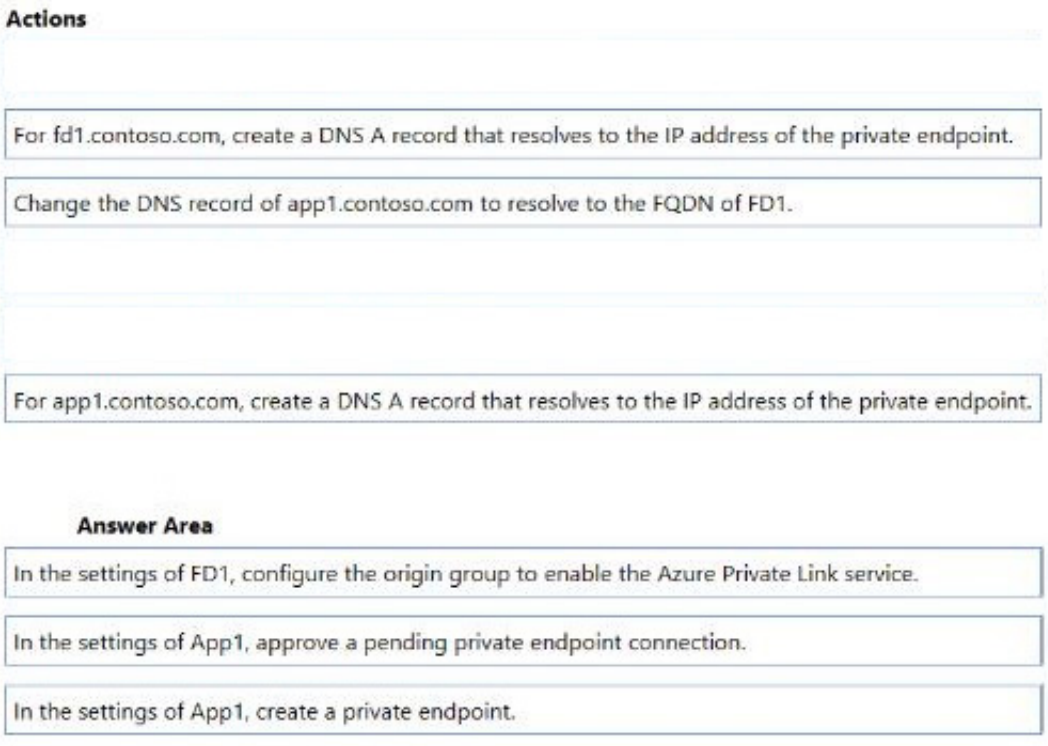
The downtime of connections to App1 must be minimized.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



QUESTION 7

You have an Azure virtual network that contains two subnets named Subnet1 and Subnet2. Subnet1 contains a virtual machine named VM1. Subnet2 contains a virtual machine named VM2.

You have two network security groups (NSGs) named NSG1 and NSG2. NSG1 has 100 inbound security rules and is associated to VM1. NSG2 has 200 inbound security rules and is associated to Subnet1.

VM2 cannot connect to VM1.

You suspect that an NSG rule blocks connectivity.

You need to identify which rule blocks the connection. The issue must be resolved as quickly as possible.

Which Azure Network Watcher feature should you use?

A. Effective security rules

B. Connection troubleshoot

C. NSG diagnostic

D. NSG flow logs

Correct Answer: C

QUESTION 8

DRAG DROP

Your company, named Contoso, Ltd., has an Azure subscription that contains the resources shown in the following table.

Name	Type	Location	Description
App1us	Azure App Service	East US	A website for the United States office of Contoso
App1uk	Azure App Service	UK West	A website for the United Kingdom office of Contoso
St1us	Storage account	East US	Contains images for the United States website
St1uk	Storage account	UK West	Contains images for the United Kingdom website

You plan to deploy Azure Front Door. The solution must meet the following requirements:

1.

Requests to a URL of https://contoso.azurefd.net/uk must be routed to App1uk.

2.

Requests to a URL of https://contoso.azurefd.net/us must be routed to App1us.

3.

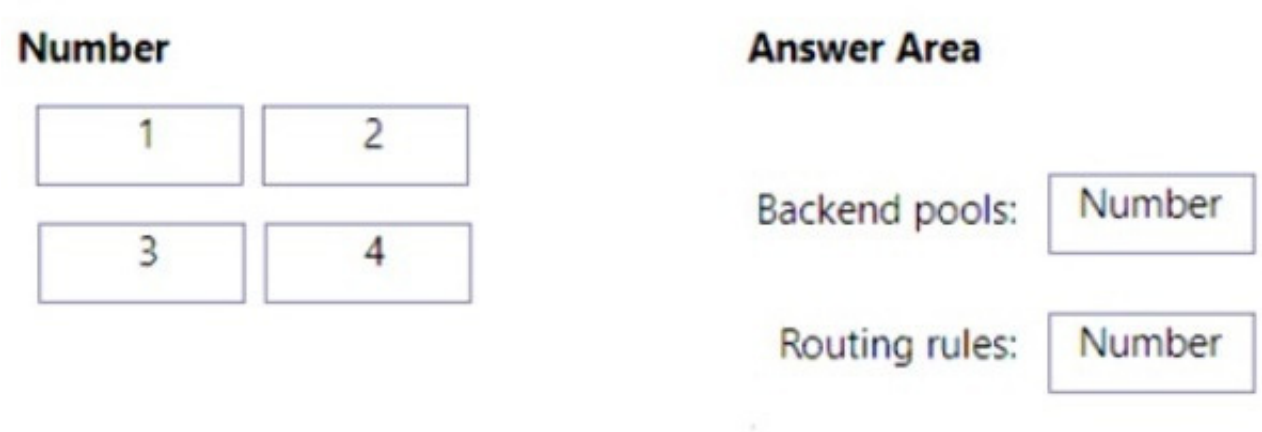
Requests to a URL of https://contoso.azurefd.net/images must be routed to the storage account closest to the user.

What is the minimum number of backend pools and routing rules you should create? To answer, drag the appropriate number to the correct components. Each number may be used once, more than once, or not at all. You may need to drag

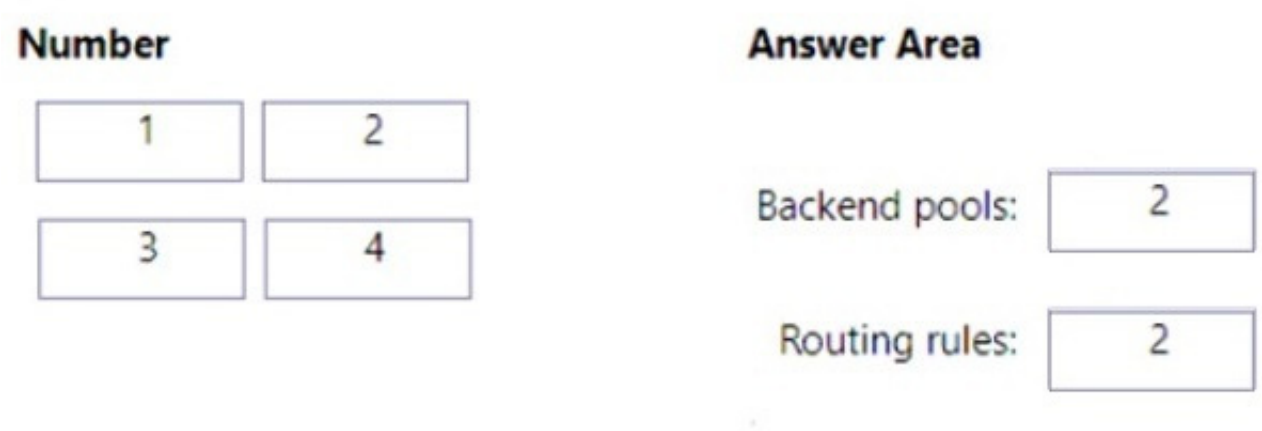
the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: 2

One backend pool in East US, and One backend pool in UK West.

Note: The backend pool is a critical component of the load balancer. The backend pool defines the group of resources that will serve traffic for a given load-balancing rule.

Box 2: 2

One rule to handle: Requests to a URL of https://contoso.azurefd.net/uk must be routed to App1uk.

One rule to handle: Requests to a URL of https://contoso.azurefd.net/us must be routed to App1us.

The third requirement (Requests to a URL of https://contoso.azurefd.net/images must be routed to the storage account closest to the user) does not need any rule. Just need to set up latency routing. Note:

Azure Front Door supports four different traffic routing methods to determine how your HTTP/HTTPS traffic is distributed between different origins. When user requests reach the Front Door edge locations, the configured routing method gets applied to ensure requests are forwarded to the best backend resource. The four traffic routing methods are: Latency: The latency-based routing ensures that requests are sent to the lowest latency origins acceptable within a sensitivity range. In other words, requests get sent to the nearest set of origins in respect to network latency. Priority Weighted Session Affinity Reference: https://learn.microsoft.com/en-us/azure/frontdoor/routing-methods

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management

---

QUESTION 9

HOTSPOT

You have an on-premises datacenter.

You have an Azure subscription that contains 10 virtual machines and a virtual network named VNet1 in the East US Azure region. The virtual machines are connected to VNet1 and replicate across three availability zones.

You need to connect the datacenter to VNet1 by using ExpressRoute. The solution must meet the following requirements:

1.

Maintain connectivity to the virtual machines if two availability zones fail.

2.

Support 1000-Mbps connections.

3.

Minimize costs.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of ExpressRoute circuits:

One ExpressRoute Standard circuit
One ExpressRoute Premium circuit
Two ExpressRoute Standard circuits
Two ExpressRoute Premium circuits
Three ExpressRoute Standard circuits
Three ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways:

One ExpressRoute gateway of the ErGw1AZ SKU
One ExpressRoute gateway of the High performance SKU
Two ExpressRoute gateway of the ErGw1AZ SKU
Two ExpressRoute gateway of the High performance SKU
Three ExpressRoute gateway of the ErGw1AZ SKU
Three ExpressRoute gateway of the High performance SKU

Correct Answer:

Answer Area

Minimum number of ExpressRoute circuits:

One ExpressRoute Standard circuit
One ExpressRoute Premium circuit
Two ExpressRoute Standard circuits
Two ExpressRoute Premium circuits
Three ExpressRoute Standard circuits
Three ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways:

One ExpressRoute gateway of the ErGw1AZ SKU
One ExpressRoute gateway of the High performance SKU
Two ExpressRoute gateway of the ErGw1AZ SKU
Two ExpressRoute gateway of the High performance SKU
Three ExpressRoute gateway of the ErGw1AZ SKU
Three ExpressRoute gateway of the High performance SKU

1.

https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview;

2.

https://learn.microsoft.com/en-us/azure/vpn-gateway/create-zone-redundant-vnet-gateway

3.

https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#gwsku

When deploying an ErGw1AZ, it is possible to define its zone availability as "Zone-Redundant", in addition it is also essential that the ip used by the ER Gateway be "Standard", because at the time of provisioning this ip will become

redundant between the availability zones . Regarding the ER Circuit, it can be "Local", but in this scenario it would be unlimited and more expensive than the "Standard" Limited in 1Gbps. In my opinion the best answer would be:

1.

One ExpressRoute Standard circuit

2.

One ExpressRoute gateway of the ErGw1AZ SKU

QUESTION 10

Azure virtual networks in the East US Azure region as shown in the following table.

Name	IP address space
Vnet1	192.168.0.0/20
Vnet2	10.0.0.0/20

The virtual networks are peered to one another. Each virtual network contains four subnets.

You plan to deploy a virtual machine named VM1 that will inspect and route traffic between all the subnets on both the virtual networks.

What is the minimum number of IP addresses that you must assign to VM1?

A. 1

B. 2

C. 4

D. 8

Correct Answer: A

https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#can-azure-firewall-forward-and-filter-network-traffic-between-subnets-in-the-same-virtual-network-or-peered-virtual-networks

Can Azure Firewall forward and filter network traffic between subnets in the same virtual network or peered virtual networks?

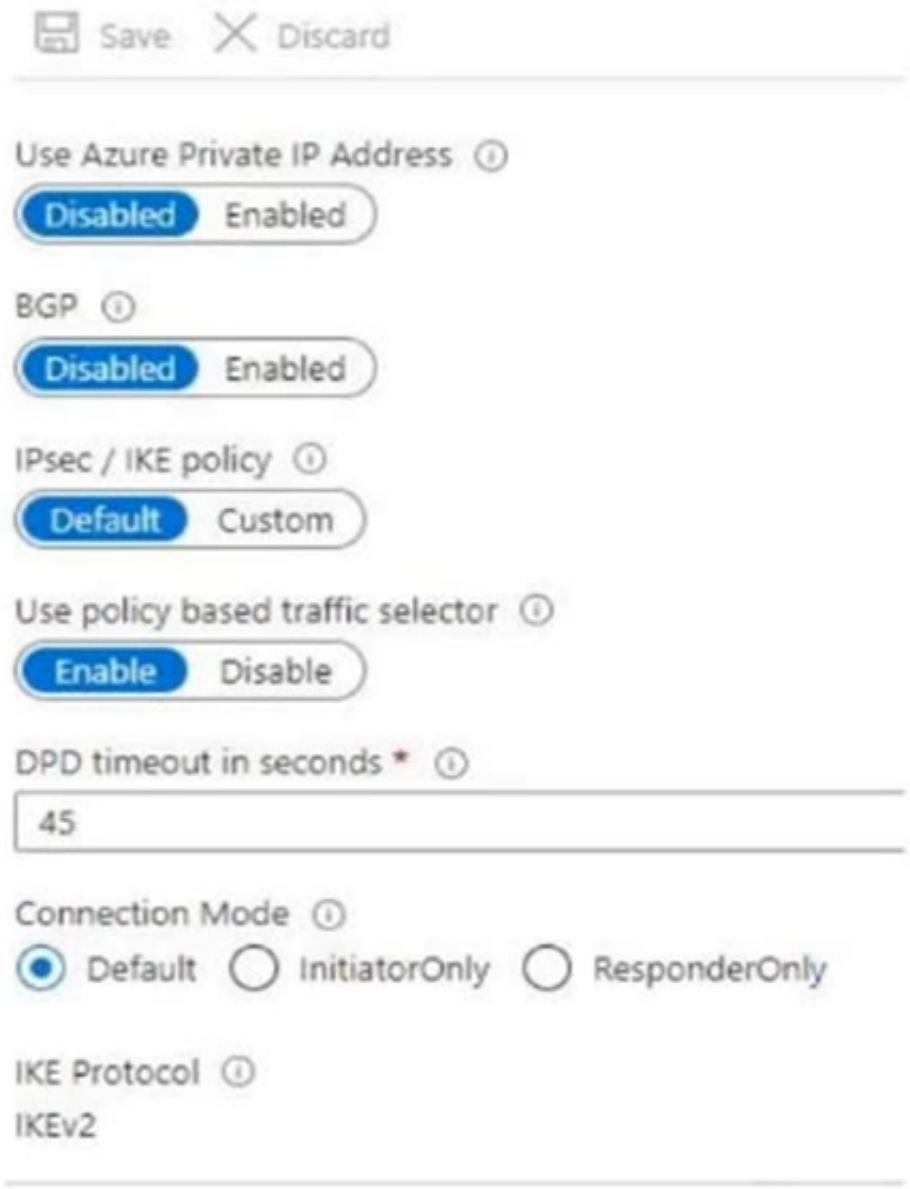
Yes. However, configuring the UDRs to redirect traffic between subnets in the same VNET requires additional attention. While using the VNET address range as a target prefix for the UDR is sufficient, this also routes all traffic from one machine to another machine in the same subnet through the Azure Firewall instance. To avoid this, include a route for the subnet in the UDR with a next hop type of VNET. Managing these routes might be cumbersome and prone to error. The recommended method for internal network segmentation is to use Network Security Groups, which don\\'t require UDRs.

QUESTION 11

You have an Azure virtual network named Vnet1 and an on-premises network.

The on-premises network has policy-based VPN devices. In Vnet1, you deploy a virtual network gateway named GW1 that uses a SKU of VpnGw1 and is route-based.

You have a Site-to-Site VPN connection for GW1 as shown in the following exhibit.



You need to ensure that the on-premises network can connect to the route-based GW1. What should you do before you create the connection?

A. Set Connection Mode to ResponderOnly.

B. Set BGP to Enabled.

C. Set Use Azure Private IP Address to Enabled.

D. Set IPsec / IKE policy to Custom.

Correct Answer: D

BGP is the standard routing protocol commonly used in the Internet to exchange routing and reachability information between two or more networks. BGP enables the Azure VPN Gateways and your on-premises VPN devices, called BGP

peers or neighbors, to exchange "routes" that will inform both gateways on the availability and reachability for those prefixes to go through the gateways or routers involved. BGP can also enable transit routing among multiple networks by

propagating routes a BGP gateway learns from one BGP peer to all other BGP peers.

Incorrect:

Not C: A VPN gateway must have a Public IP address. Verify that you have an externally facing public IPv4 address for your VPN device.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-cli

QUESTION 12

You have an Azure Front Door instance that has a single frontend named Frontend1 and an Azure Web Application Firewall (WAF) policy named Policy1. Policy1 redirects requests that have a header containing "string1" to https://

www.contoso.com/redirect1. Policy1 is associated to Frontend1.

You need to configure additional redirection settings. Requests to Frontend1 that have a header containing "string2" must be redirected to https://www.contoso.com/redirect2.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a custom rule.

B. Create a policy.

C. Create a frontend host.

D. Create a frontend host.

E. Add a custom rule to Policy1.

F. Create an association.

Correct Answer: ABF

the question itself makes no sense as already have the policy1 created hence the available options tends you to do the all process again.

B. Create a policy.

A. Create a custom rule.

F. Create an association.

QUESTION 13

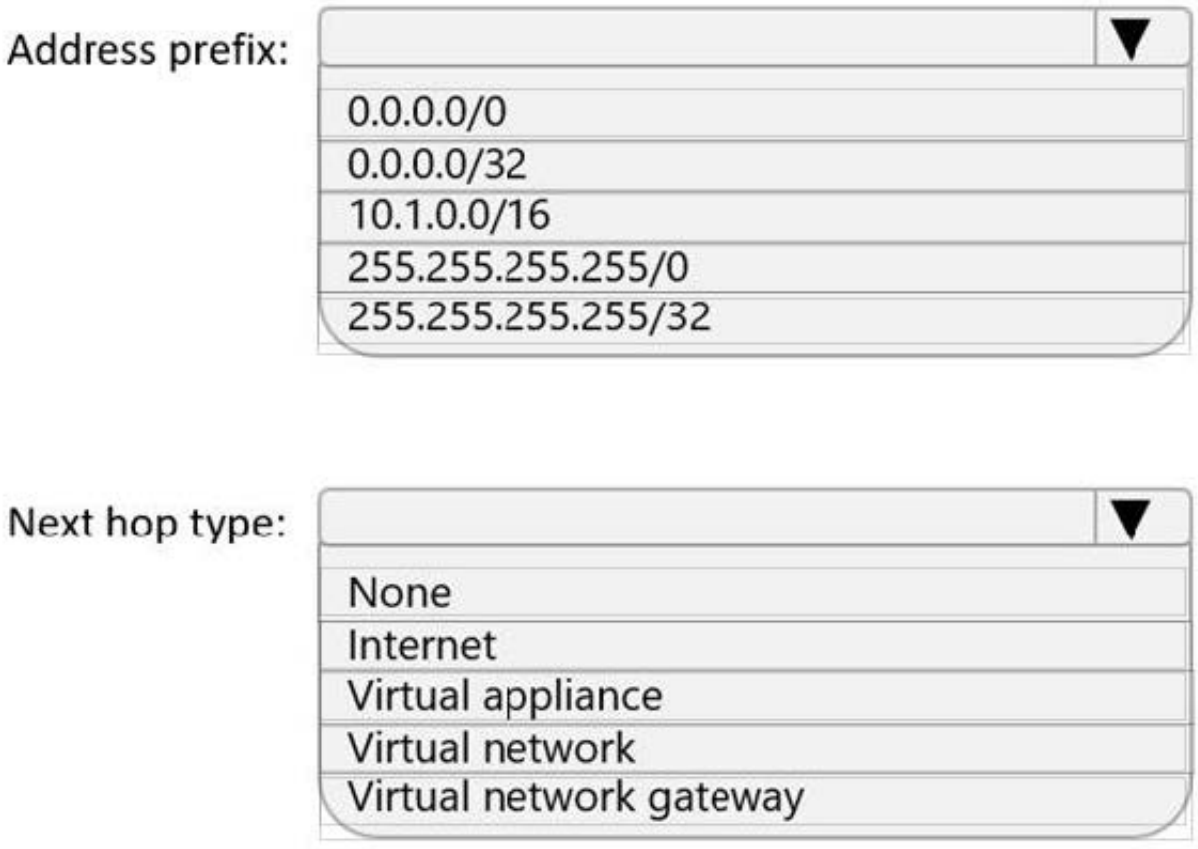
HOTSPOT

You are implementing the virtual network requirements for VM-Analyze.

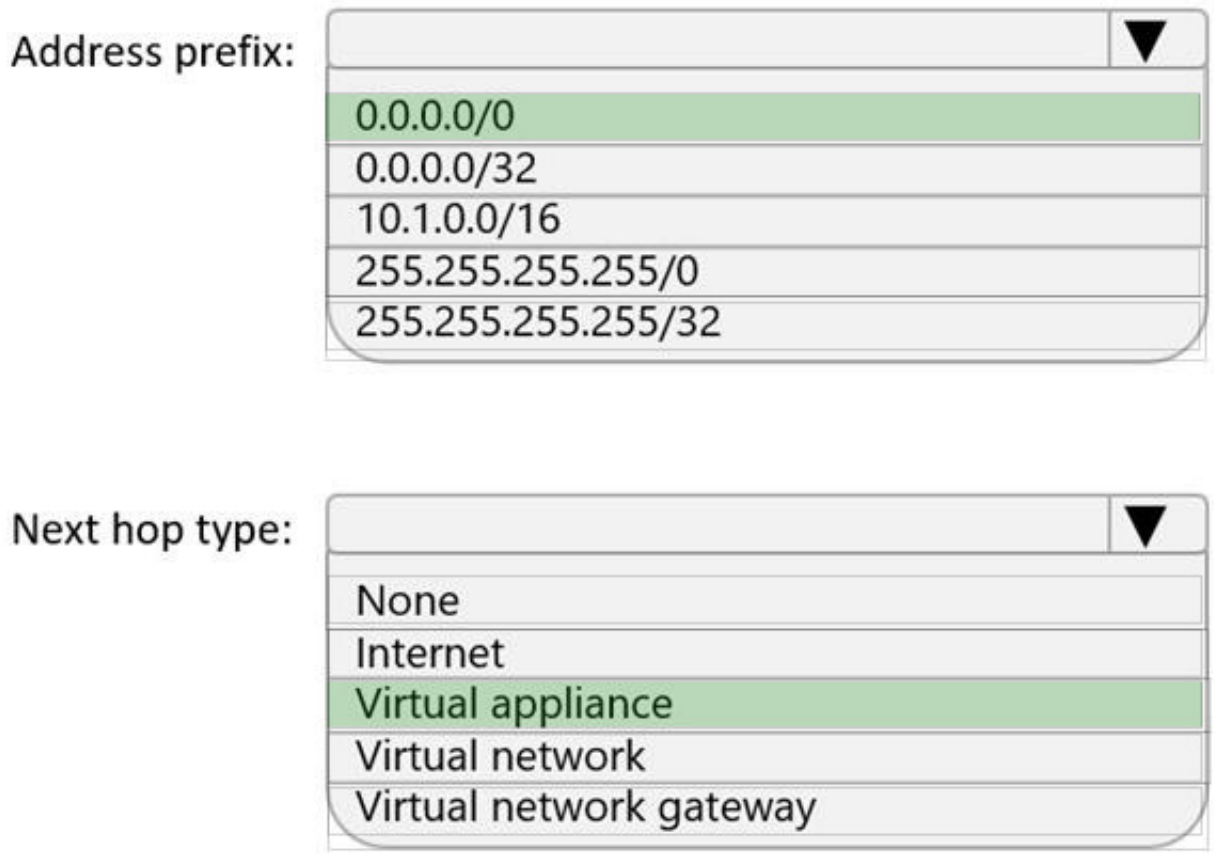
What should you include in a custom route that is linked to Subnet2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

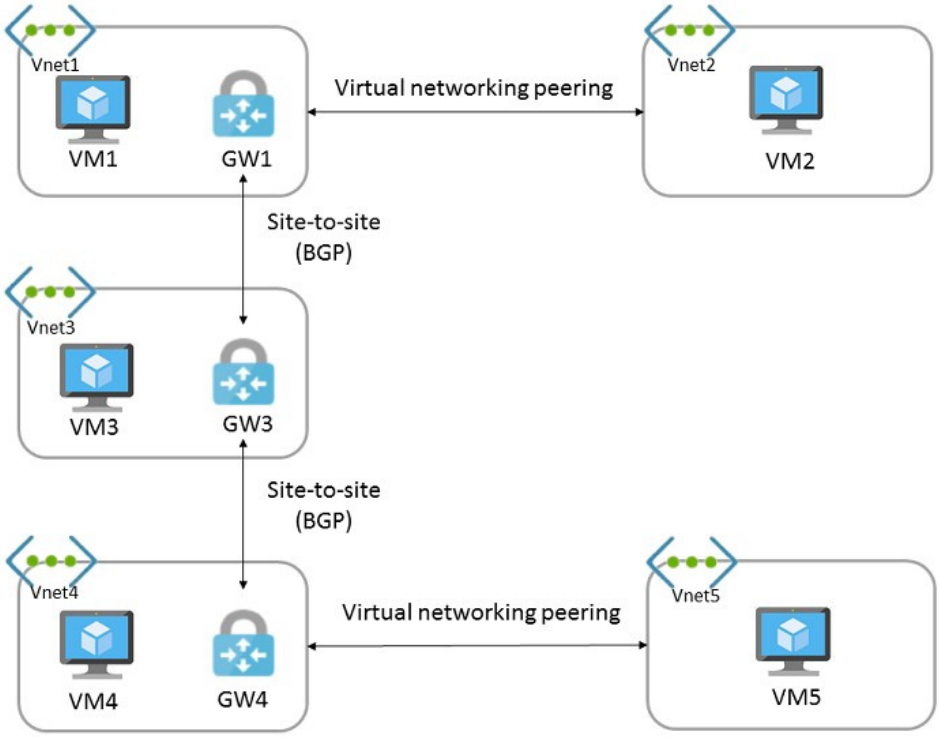


Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

QUESTION 14

HOTSPOT

You have the Azure environment shown in the exhibit.



You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.

Virtual network	Traffic to remote virtual network	Use remote gateway	Allow gateway transit
Vnet1	Allow	**None**	Enabled
Vnet2	Allow	Enabled	**None**
Vnet4	Allow	**None**	Enabled
Vnet5	Block	Enabled	**None**

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

Hot Area:

Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	○	○
VM2 and VM4 can communicate.	○	○
VM1 and VM5 can communicate.	○	○

Correct Answer:

Answer Area:

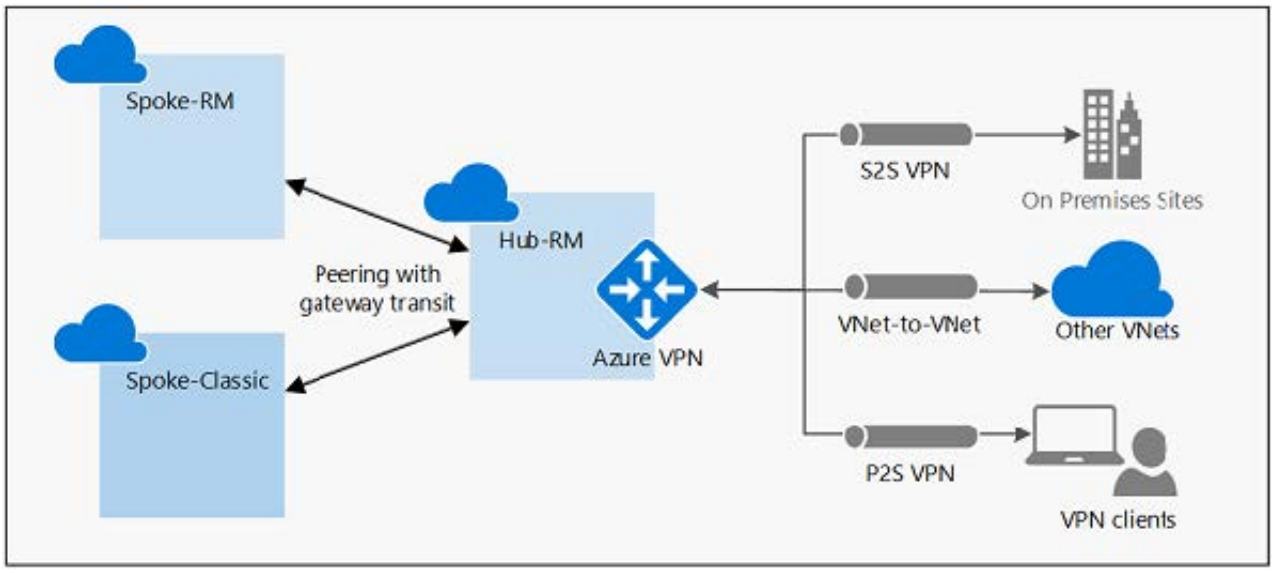
Statements	Yes	No
VM1 and VM4 can communicate.	○	○
VM2 and VM4 can communicate.	○	○
VM1 and VM5 can communicate.	○	○

Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the

peered virtual network for cross-premises or VNet-to-VNet connectivity.

The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual

networks.

In hub-and-spoke network architecture, gateway transit allows spoke virtual networks to share the VPN gateway in the hub, instead of deploying VPN gateways in every spoke virtual network.

Box 2: Yes

VM2 uses the remote gateway GW1 to reach VM4.

Box 3: Yes

Select Block all traffic to the remote virtual network if you don\\'t want traffic to flow to the peered virtual network by default. You can select this setting if you have peering between two virtual networks but occasionally want to disable default

traffic flow between the two. You may find enabling/disabling is more convenient than deleting and re-creating peerings. When this setting is selected, traffic doesn\\'t flow between the peered virtual networks by default; however, traffic may still

flow if explicitly allowed through a network security group rule that includes the appropriate IP addresses or application security groups.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues

QUESTION 15

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

A. storage account

B. internal load balancers

C. service endpoints

D. virtual network peering

Correct Answer: B

During the creation of the load balancer, you\\'ll configure:

1.

Frontend IP address

2.

Backend pool

3.

Inbound load-balancing rules

When you create an internal load balancer, a virtual network is configured as the network for the load balancer.

A private IP address in the virtual network is configured as the frontend for the load balancer. The frontend IP address can be Static or Dynamic.

Reference:

https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-internal-portal