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.leads4pass.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

You have an Azure virtual network named Vnet1.

You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources.

Which two outbound network security group (NSG) rules should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a deny rule that has a source of VirtualNetwork and a destination of Sql

B. an allow rule that has the IP address range of Vnet1 as the source and destination of Sql.EastUS

C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24

D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage

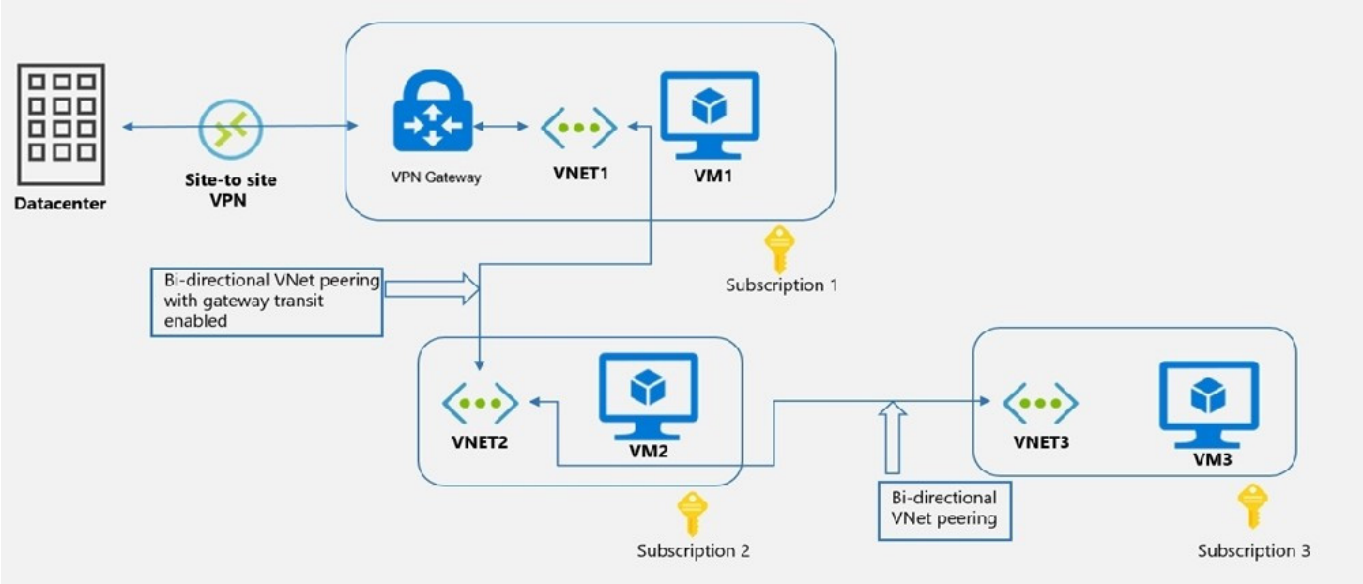
Correct Answer: BD

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

QUESTION 2

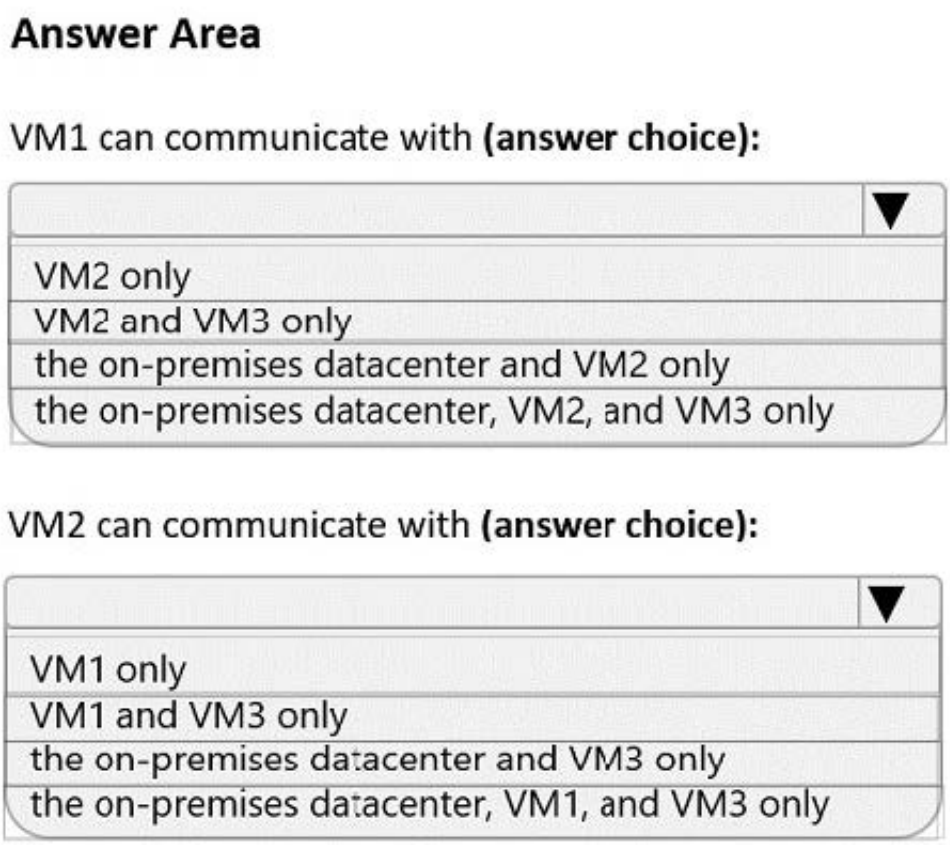
HOTSPOT

You have an Azure environment shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

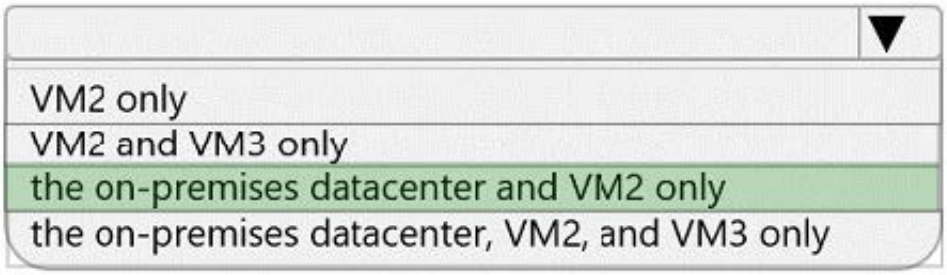
Hot Area:



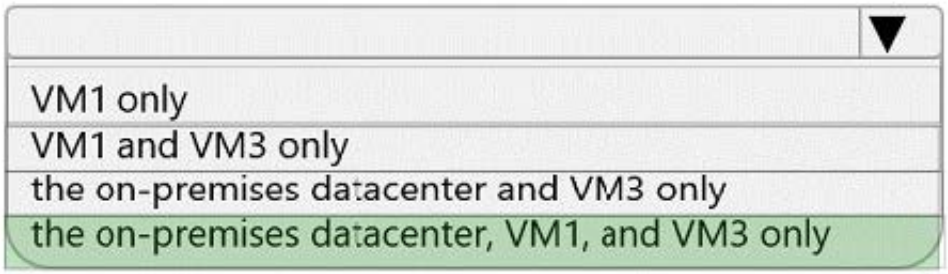
Correct Answer:

Answer Area

VM1 can communicate with **(answer choice):**



VM2 can communicate with **(answer choice):**



1.

VM1 Can Communicate with On-Premise datacenter due to S2S VPN and VM2 due to Bi-Directional VNet Peering

2.

VM2 an Communicate with On-Premise datacenter, VM1 due Gateway transit(VNET1-VNET2) and S2S VPN (VNET1-Datacenter), and VM3 (VNET2-VNET3 VNet Peering)

Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit?toc=/azure/virtual-network/toc.json

QUESTION 3

You have an Azure subscription that contains a virtual network named VNet1.

You deploy several web apps and configure the apps to use private endpoints on VNet1.

You need to identify which DNS records the web apps registered automatically.

Where will the records be created?

A. an Azure DNS zone named privatelink.azurewebsites.net

B. an Azure Private DNS zone named azurewebsites.net

C. an Azure Private DNS zone named privatelink.azurewebsites.net

D. an Azure DNS zone named azurewebsites.net

Correct Answer: C

On creating a private endpoint in portal:

Your private endpoint will be integrated with the private DNS zone \\'privatelink.azurewebsites.net\\' in the resource group of the selected subnet. If the private DNS zone does not exist, it will be created automatically.

C. an Azure Private DNS zone named privatelink.azurewebsites.net

QUESTION 4

You have an internal Basic Azure Load Balancer named LB1 that has two frontend IP addresses. The backend pool of LB1 contains two Azure virtual machines named VM1 and VM2. You need to configure the rules on LB1 as shown in the following table.

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.0.2	TCP	80	IP address of the NIC of VM1 and VM2	80

What should you do for each rule?

A. Enable Floating IP.

B. Disable Floating IP.

C. Set Session persistence to Enabled.

D. Set Session persistence to Disabled.

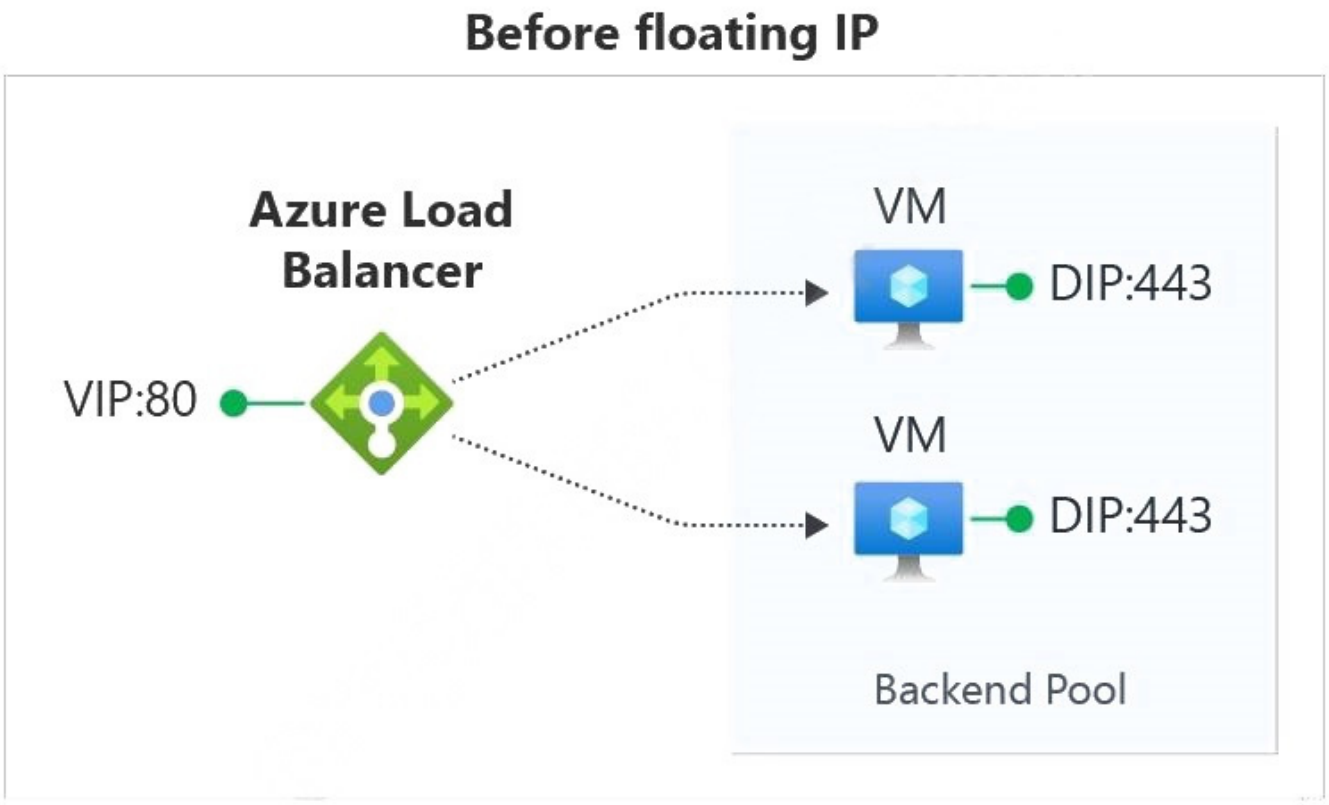
Correct Answer: A

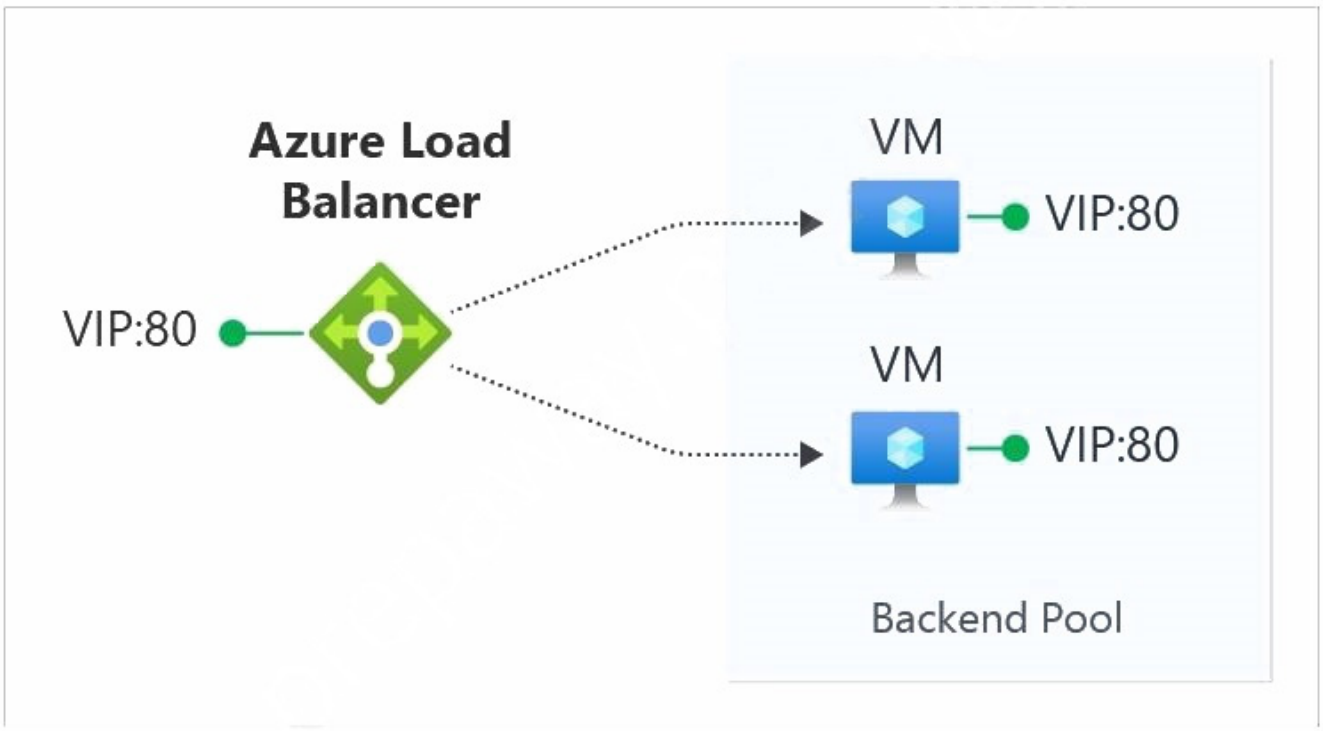
Azure Load Balancer Floating IP configuration Floating IP Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include:

clustering for high availability network virtual appliances exposing multiple TLS endpoints without re-encryption.

If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

In the diagrams below, you see how IP address mapping works before and after enabling Floating IP: Note: Azure Load Balancer supports rules to configure traffic to the backend pool. There are four types of rules:


Before floating IP
Azure Load Balancer
VIP:80
VM
DIP:443
VM
DIP:443
Backend Pool


After floating IP
Azure Load Balancer
VIP:80
VM
VIP:80
VM
VIP:80
Backend Pool

*

Load-balancing rules - A load balancer rule is used to define how incoming traffic is distributed to the all the instances within the backend pool. A load-balancing rule maps a given frontend IP configuration and port to multiple backend IP addresses and ports.

*

High availability ports

*

Inbound NAT rule

*

Outbound NAT rule Reference:

https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip https://learn.microsoft.com/en-us/azure/load-balancer/manage-rules-how-to

---

QUESTION 5

You have an Azure subscription that contains an ExpressRoute Standard gateway named GW1.

You need to upgrade GW1 to support ExpressRoute FastPath. The solution must minimize downtime.

Which SKU should you use?

A. Ultra performance

B. ErGw3AZ

C. ErGw2AZ

D. High performance

Correct Answer: B

Explanation:

To configure FastPath, the virtual network gateway must be either:

Ultra Performance

ErGw3AZ

The difference is that ErGw3AZ is zone redundant whereas Ultraperformance is not.

Reference:

https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath

https://learn.microsoft.com/en-us/answers/questions/885158/whats-the-difference-between-ergw3az-vs-ultraperfo

---

QUESTION 6

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure NAT Gateway.

Does this meet the requirement?

A. Yes

B. No

Correct Answer: B

Explanation:

Correct Solution: You implement Azure Firewall.

What is a secured virtual hub?

A virtual hub is a Microsoft-managed virtual network that enables connectivity from other resources. When a virtual hub is created from a Virtual WAN in the Azure portal, a virtual hub VNet and gateways (optional) are created as its

components.

A secured virtual hub is an Azure Virtual WAN Hub with associated security and routing policies configured by Azure Firewall Manager.

Create a secured virtual hub

Using Firewall Manager in the Azure portal, you can either create a new secured virtual hub, or convert an existing virtual hub that you previously created using Azure Virtual WAN.

Reference:

https://learn.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub

QUESTION 7

HOTSPOT

You have an Azure subscription.

You plan to use Azure Virtual WAN.

You need to deploy a virtual WAN hub that meets the following requirements:

1.

Supports 4 Gbps of Site-to-Site (S2S) VPN traffic

2.

Supports 8 Gbps of ExpressRoute traffic

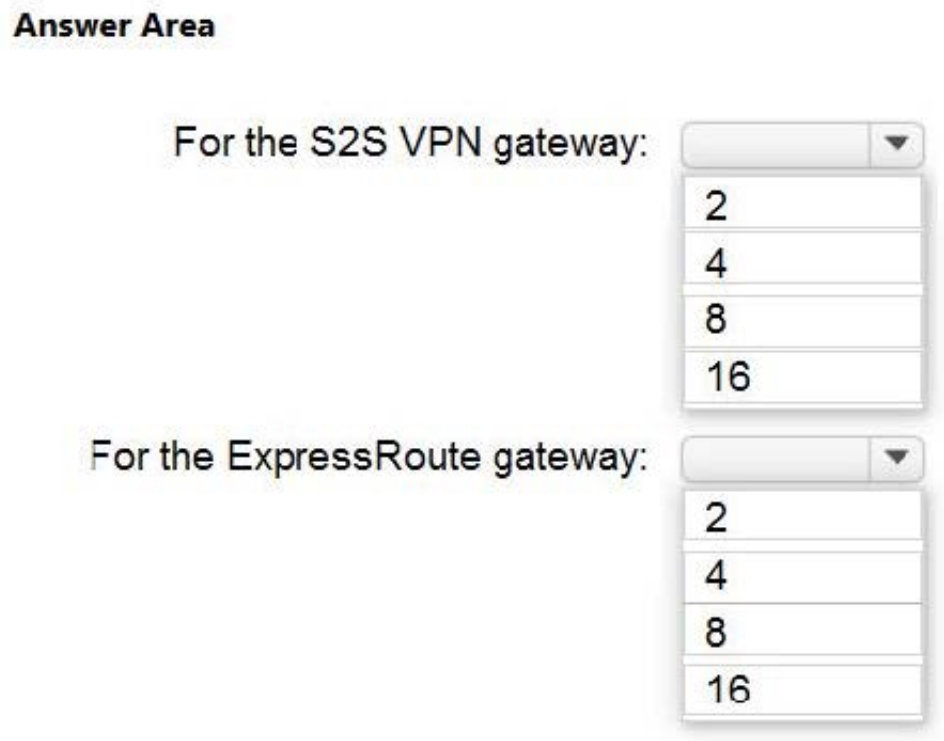
3.

Minimizes costs

How many scale units should you configure? To answer, select the appropriate options in the answer area.

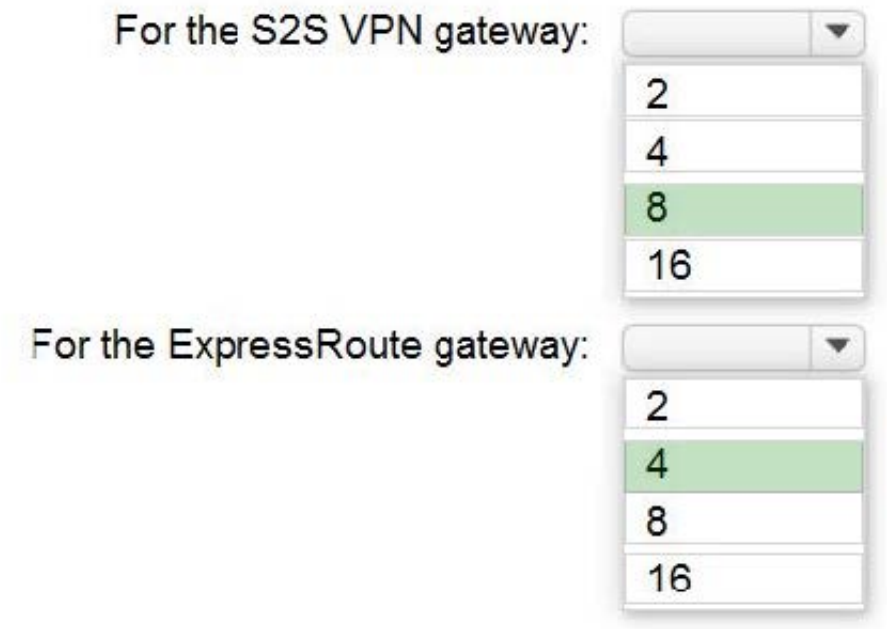
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



For S2S 1 scale unit = 500 Mbps 4000/500 = 8 scale units https://learn.microsoft.com/en-us/azure/virtual-wan/gateway-settings#s2s

For ExpressRoute 1 scale unit = 2Gbps 8/2 = 4 https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-about#expressroute-performance

QUESTION 8

You plan to publish a website that will use an FQDN of www.contoso.com. The website will be hosted by using the Azure App Service apps shown in the following table.

Name	FQDN	Location	Public IP address
AS1	As1.contoso.com	East US	131.107.100.1
AS2	As2.contoso.com	West US	131.107.200.1

You plan to use Azure Traffic Manager to manage the routing of traffic for www.contoso.com between AS1 and AS2.

You need to ensure that Traffic Manager routes traffic for www.contoso.com.

Which DNS record should you create?

A. two A records that map www.contoso.com to 131.107.100.1 and 131.107.200.1

B. a CNAME record that maps www.contoso.com to TMprofile1.azurefd.net

C. a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net

D. a TXT record that contains a string of as1.contoso.com and as2.contoso.com in the details

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile
https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager

QUESTION 9

HOTSPOT

Your on-premises network contains the subnets shown in the following table.

Name	IPv4 network address
Subnet1	192.168.10.0/24
Subnet2	192.168.20.0/24

The network contains a firewall named FW1 that uses a public IP address of 131.107.100.200. You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNet1	Virtual network	Uses an address space of 10.1.0.0/16
GW1	Virtual network gateway	• Uses a public IP address of 20.231.231.174 • Uses a private IP address of 10.1.255.10
GatewaySubnet	Subnet	Uses an address space of 10.1.255.0/27
LNG1	Local network gateway	*None*

You plan to configure a Site-to-Site (S2S) VPN named VPN1 that will connect GW1 to FW1.

You need to configure LNG1 to support VPN1. The solution must meet the following requirements:

Ensure that the resources on Subnet1 and Subnet2 can communicate with the resources on VNet1.

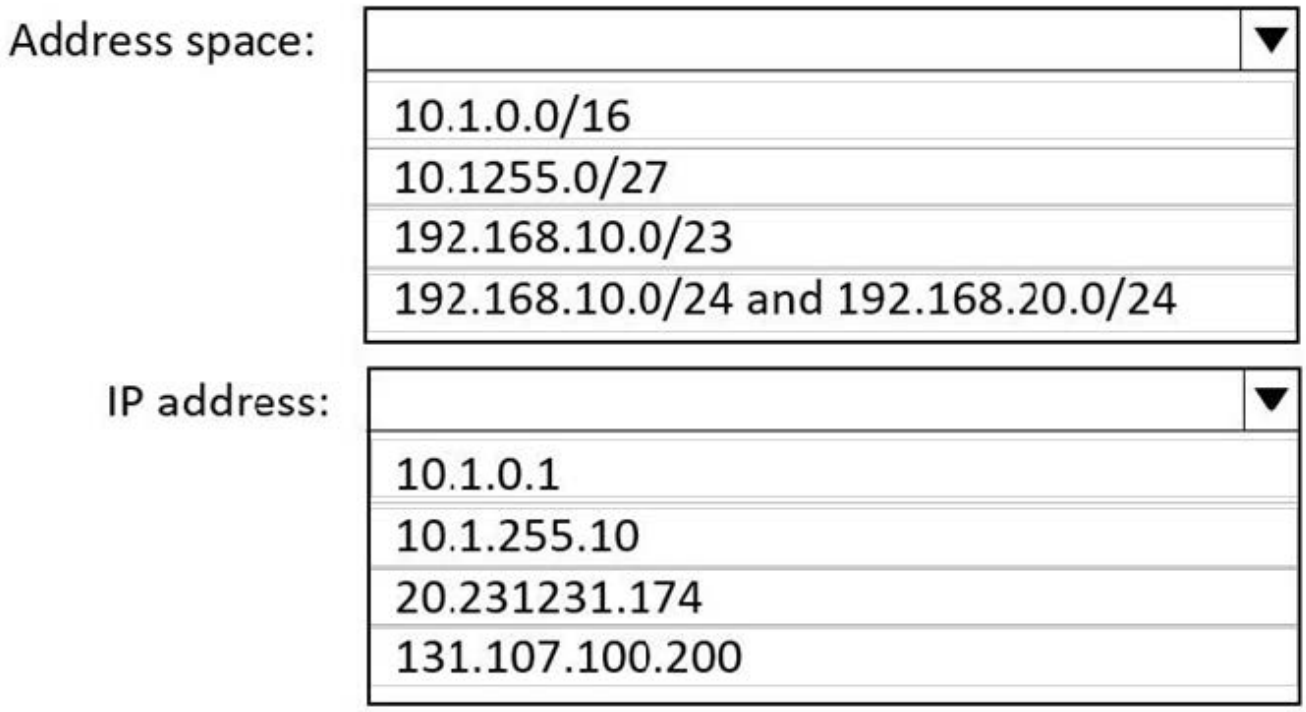
Minimize administrative effort.

How should you configure LNG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

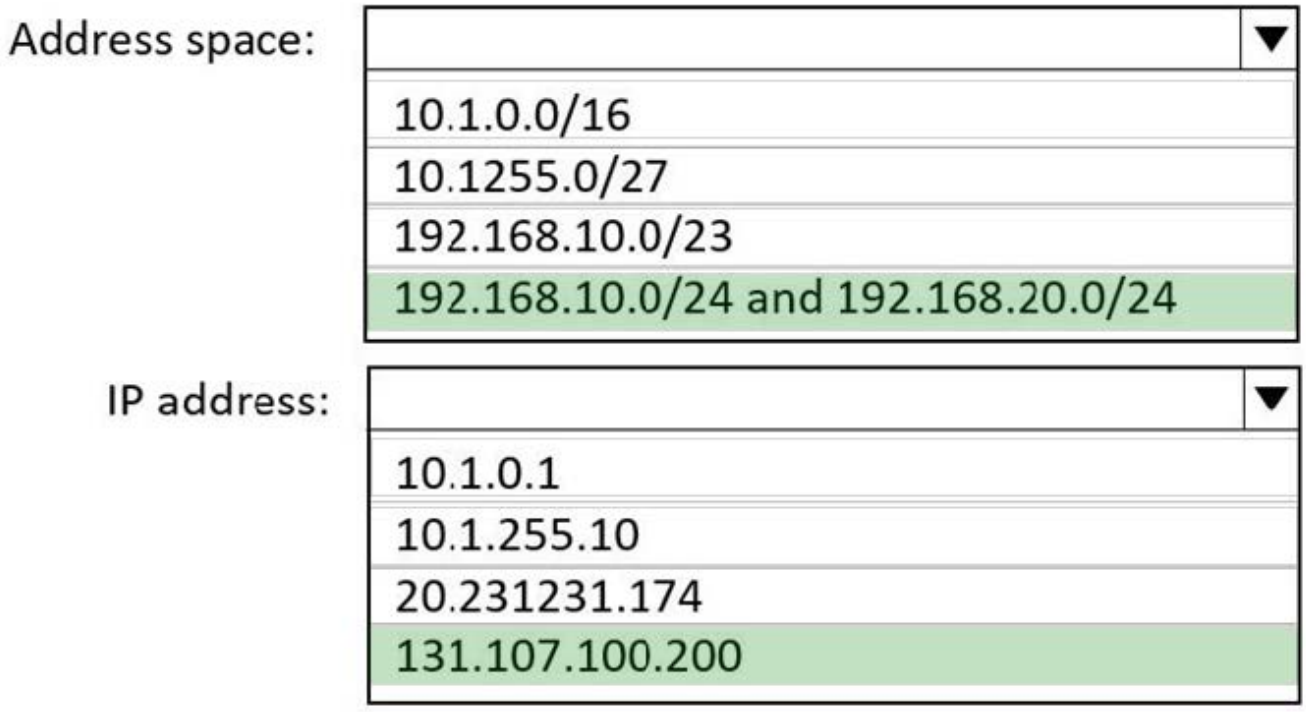
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 10

You have an Azure environment that contains a virtual network named VNet1 with IP address space of 10.2.0.0/16.

No devices are connected to VNet1.

You plan to peer VNet1 with another virtual network named VNet2.

VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

A. Configure a service endpoint on VNet2.

B. Add a gateway subnet to VNet1.

C. Create a subnet on VNEt1 and VNet2.

D. Modify the address space of VNet1.

Correct Answer: D

Correct Answer(s):

Modify the address space of VNet1 - Address spaces of virtual networks (VNet) must not overlap to enable VNet Peering. The IP address range for VNet1 and VNet2 are overlapping. Therefore, the first step is to modify the IP address range for VNet1. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq#vnet-peering

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and- constraints

Wrong Answers:

Configure a service endpoint on VNet2 - Service endpoints provide secure and direct connectivity to Azure services over Azure backbone network.

Add a gateway subnet to VNet1 - You need to create a gateway subnet for your VNet to configure a virtual network gateway. It is not required for Vnet peering.

Create a subnet on VNEt1 and VNet2 - Subnets are not mandatory for VNet peering.

QUESTION 11

You have an Azure Private Link service named PL1 that uses an Azure load balancer named LB1.

You need to ensure that PL1 can support a higher volume of outbound traffic.

What should you do?

A. Increase the number of frontend IP configurations for LB1.

B. Increase the number of NAT IP addresses assigned to PL1.

C. Deploy an Azure Application Gateway v2 instance to the source NAT subnet.

D. Redeploy LB1 with a different SKU.

Correct Answer: B

Since the question ask for outbound traffic:

Each NAT IP provides 64k TCP connections (64k ports) per VM behind the Standard Load Balancer. In order to scale and add more connections, you can either add new NAT IPs or add more VMs behind the Standard Load Balancer. Doing

so will scale the port availability and allow for more connections. Connections will be distributed across NAT IPs and VMs behind the Standard Load Balancer.

https://learn.microsoft.com/en-us/azure/private-link/private-link-faq#what-is-the-nat--network-address-translation--ip-configuration-used-in-private-link-service--how-can-i-scale-in-terms-of-available-ports-and-connections-

QUESTION 12

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 13

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 an Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1
                              /PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against
                          \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "appl.contoso.com",
   "transactionId": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You disable the WAF rule that has a ruleld of 920300.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 14

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

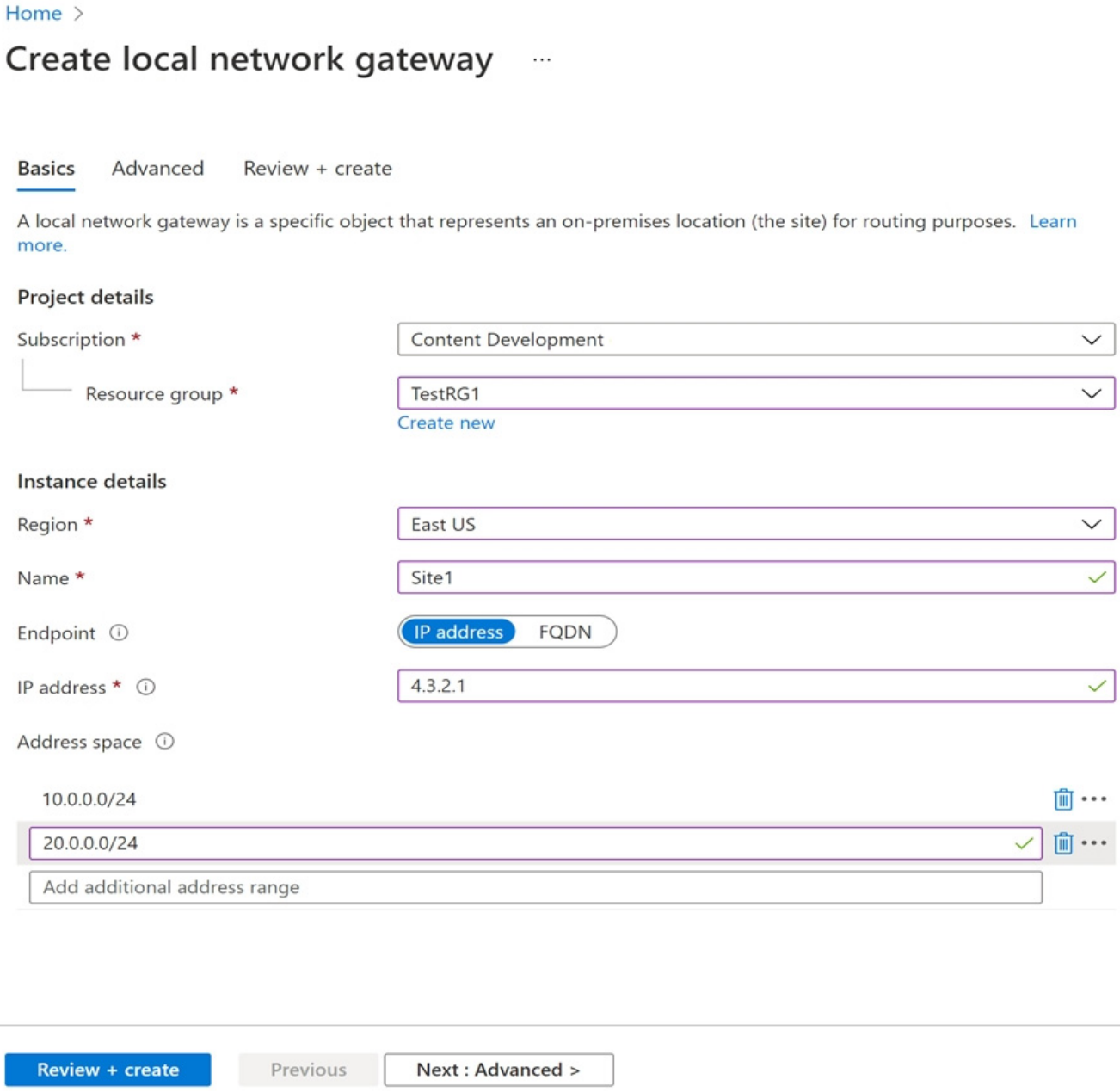
of your VPN device. Otherwise, Azure won\\'t be able to connect.)

*

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.



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 15

You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the

contoso.com zone.

Vnet1 connects to an on-premises datacenter by using ExpressRoute.

You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone.

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

NOTE: Each correct selection is worth one point.

A. Modify the DNS server settings of Vnet1.

B. For FW1, configure custom DNS server.

C. For FW1, enable DNS proxy.

D. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.

E. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.

Correct Answer: CD

Reference: https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/