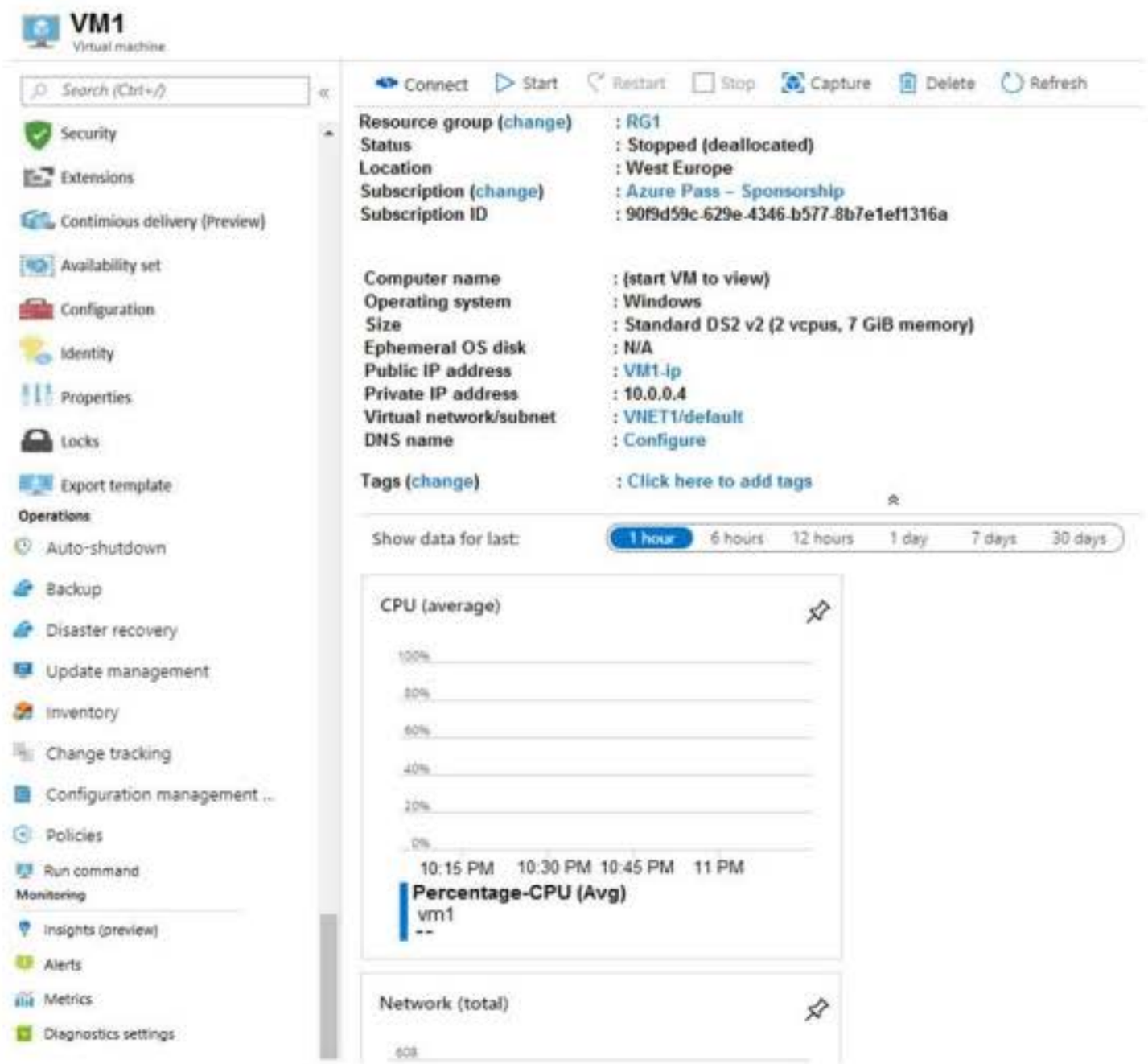
Question : 1 ✓ Total: 50

You create an Azure VM named VM1 that runs Windows Server 2019.

VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)



You need to enable Desired State Configuration for VM1.

What should you do first?

- ○ Connect to VM1.
- ◉ Start VM1.
- ○ Capture a snapshot of VM1.
- ○ Configure a DNS name for VM1.

Validate ✓

Solution:

Explanation:

Status is Stopped (Deallocated).

The DSC extension for Windows requires that the target virtual machine is able to communicate with Azure.

The VM needs to be started.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-windows

Question : 2 ✓ Total: 50

You have five Azure virtual machines that run Windows Server 2016. The virtual machines are configured as web servers.

You have an Azure load balancer named LB1 that provides load balancing services for the virtual machines.

You need to ensure that visitors are serviced by the same web server for each request.

What should you configure?

- ○ Floating IP (direct server return) to Disabled
- ○ Session persistence to None
- ○ Floating IP (direct server return) to Enabled
- ◉ Session persistence to Client IP

Validate ✓

Solution:

Explanation:

With Sticky Sessions when a client starts a session on one of your web servers, session stays on that specific server. To configure An Azure Load-Balancer For Sticky Sessions set Session persistence to Client IP or to Client IP and

protocol.

On the following image you can see sticky session configuration:

Note:

✶ Client IP and protocol specifies that successive requests from the same client IP address and protocol combination will be handled by the same virtual machine.

✶ Client IP specifies that successive requests from the same client IP address will be handled by the same virtual machine.

Reference:

https://cloudopszone.com/configure-azure-load-balancer-for-sticky-sessions/

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 subscription that contains the following resources:

✣ A virtual network that has a subnet named Subnet1

✣ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

✣ A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

✣ Priority: 100

✣ Source: Any

✣ Source port range: *

✣ Destination: *

✣ Destination port range: 3389

✣ Protocol: UDP

✣ Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Question : 3 ✓ Total: 50

Refer from above paragraph Q.No : 3

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the Any source to the *destination for port range 3389 and uses the TCP protocol. You remove NSG-VM1 from the network interface of VM1.

Does this meet the goal?

◉ Yes

○ No

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 subscription that contains the following resources:

✣ A virtual network that has a subnet named Subnet1

✣ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1

✣ A virtual machine named VM1 that has the required Windows Server configurations to allow Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

✣ Priority: 100

✣ Source: Any

✣ Source port range: *

✣ Destination: *

✣ Destination port range: 3389

✣ Protocol: UDP

✣ Action: Allow

VM1 has a public IP address and is connected to Subnet1. NSG-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Question : 4 ✓ Total: 50

Refer from above paragraph Q.No : 3

Solution: You add an inbound security rule to NSG-Subnet1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the UDP protocol.

Does this meet the goal?

○ Yes

◉ No

Validate ✓

Solution:

Explanation:

The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

Question : 5 ✓ Total: 50

Refer from above paragraph Q.No : 3

Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

- (●) Yes
- ( ) No

Question : 6 ✓ Total: 50

HOTSPOT

You have a virtual network named VNet1 that has the configuration shown in the following exhibit.

```
Name                 : VNet1
ResourceGroupName    : Production
Location             : westus
Id                   : /subscriptions/14d26092-8e42-4ea7-b770-
9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/virtualNetworks/VNet1
Etag                 : W/"76f7edd6-d022-455b-aeae-376059318e5d"
ResourceGuid         : 562696cc-b2ba-4cc5-9619-0a735d6c34c7
ProvisioningState    : Succeeded
Tags                 :
AddressSpace         : {
                       "AddressPrefixes": [
                          "10.2.0.0/16"
                       ]
                     }
DhcpOptions          : {}
Subnets              : [
                       {
                         "Name": "default",
                         "Etag": "W/\ "76f7edd6-d022-455b-aeae-376059318e5d\"",
                          "Id": "/subscriptions/14d26092-8e42-4ea7-b770-
                          9dcef70fb1ea/resourceGroups/Production/providers/Microsoft.Network/
                          virtualNetworks/VNet1/subnets/default",
                          "AddressPrefix": "10.2.0.0/24",
                          "IpConfigurations": [],
                          "ResourceNavigationLinks": [],
                          "ServiceEndpoints": [],
                          "ProvisioningState": "Succeeded"
                          }
                       ]
VirtualNetworkPeerings   : []
EnableDDoSProtection     : false
EnableVmProtection       : false
```

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:

Before a virtual machine on VNet1 can receive an IP address from 192.168.1.0/24, you must first _____

- ○ add a network interface
- ○ add a subnet
- ◉ add an address space
- ○ delete a subnet
- ○ delete an address space

Before a virtual machine on VNet1 can receive an IP address from 10.2.1.0/24, you must first _____

- ○ add a network interface
- ◉ add a subnet
- ○ add an address space
- ○ delete a subnet
- ○ delete an address space

Validate ✓

Solution:

Explanation:

Box 1: add an address space

Your IaaS virtual machines (VMs) and PaaS role instances in a virtual network automatically receive a private IP address from a range that you specify, based on the address space of the subnet they are connected to. We need to add the

192.168.1.0/24 address space.

Box 2: add a subnet

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/designing-networking-for-microsoft-azure-iaas

Question : 7 ✓ Total: 50

You have an Azure subscription that contains a virtual network named VNET1. VNET1 contains the subnets shown in the following table.

Name	Connected virtual machines
Subnet1	VM1, VM2
Subnet2	VM3, VM4
Subnet3	VM5, VM6

Each virtual machine uses a static IP address.

You need to create network security groups (NSGs) to meet following requirements:

✣ Allow web requests from the internet to VM3, VM4, VM5, and VM6.

✣ Allow all connections between VM1 and VM2.

✣ Allow Remote Desktop connections to VM1.

✣ Prevent all other network traffic to VNET1.

What is the minimum number of NSGs you should create?

- (●) 1
- ( ) 3
- ( ) 4
- ( ) 12

Question : 8 ✓ Total: 50

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

Name	Type	Resource group
VNET1	Virtual network	RG1
VM1	Virtual machine	RG1

The Not allowed resource types Azure policy is assigned to RG1 and uses the following parameters:

Microsoft.Network/virtualNetworks

Microsoft.Compute/virtualMachines

In RG1, you need to create a new virtual machine named VM2, and then connect VM2 to VNET1.

What should you do first

- (●) Remove Microsoft.Compute/virtualMachines from the policy.
- ( ) Create an Azure Resource Manager template
- ( ) Add a subnet to VNET1.
- ( ) Remove Microsoft.Network/virtualNetworks from the policy.

Validate ✓

Solution:

Explanation:

The Not allowed resource types Azure policy prohibits the deployment of specified resource types. You specify an array of the resource types to block.

Virtual Networks and Virtual Machines are prohibited.

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/samples/not-allowed-resource-types

Question : 9 ✓ Total: 50

Your company has an Azure subscription named Subscription1.

The company also has two on-premises servers named Server1 and Server2 that run Windows Server 2016. Server1 is configured as a DNS server that has a primary DNS zone named adatum.com. Adatum.com contains 1,000 DNS

records.

You manage Server1 and Subscription1 from Server2. Server2 has the following tools installed:

➟ The DNS Manager console

➟ Azure PowerShell

➟ Azure CLI 2.0

You need to move the adatum.com zone to an Azure DNS zone in Subscription1. The solution must minimize administrative effort.

What should you use?

- (●) Azure CLI
- ( ) Azure PowerShell
- ( ) the Azure portal
- ( ) the DNS Manager console

Question : 10 ✓ Total: 50

You have a public load balancer that balances ports 80 and 443 across three virtual machines.

You need to direct all the Remote Desktop Protocol (RDP) connections to VM3 only.

What should you configure?

- (●) an inbound NAT rule
- ( ) a new public load balancer for VM3
- ( ) a frontend IP configuration
- ( ) a load balancing rule

Question : 11 ✓ Total: 50

HOTSPOT

You have an Azure subscription named Subscription1 that contains the virtual networks in the following table.

Name	Subnets
VNet1	Subnet11, Subnet12
VNet2	Subnet13

Subscription1 contains the virtual machines in the following table

Name	Subnet	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet11	Not applicable
VM4	Subnet11	Not applicable
VM5	Subnet12	Not applicable
VM6	Subnet12	Not applicable

In Subscription1, you create a load balancer that has the following configuration

- Name: LB1
- SKU: Basic
- Type: Internal
- Subnet: Subnet12
- Virtual network: VNET1

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:

LB1 can balance the traffic between VM1 and VM2. _____

- (●) Yes
- ( ) No

LB1 can balance the traffic between VM3 and VM4. _____

- ( ) Yes
- (●) No

LB1 can balance the traffic between VM5 and VM6 _____

- ( ) Yes
- (●) No

Question : 12 ✓ Total: 50

QUESTION 48

HOTSPOT

You have an Azure virtual machine that runs Windows Server 2019 and has the following configurations:

+ Name: VM1
+ Location: West US
+ Connected to: VNET1
+ Private IP address: 10.1.0.4
+ Public IP addresses: 52.186.85.63
+ DNS suffix in Windows Server: Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Location
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

Which zones should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

DNS zones that you can link to VNET1: _____

- ○ Adatum.com only
- ○ Adatum.pri and adatum.com only
- ◉ The private zones only
- ○ The public zones only

DNS zones to which VM1 can automatically register: _____

- ○ Adatum.com only
- ○ Adatum.pri and adatum.com only
- ◉ The private zones only
- ○ The public zones only

Question : 13 ✓ Total: 50

DRAG DROP

You have an on-premises network that you plan to connect to Azure by using a site-so-site VPN.

In Azure, you have an Azure virtual network named VNet1 that uses an address space of 10.0.0.0/16 VNet1 contains a subnet named Subnet1 that uses an address space of 10.0.0.0/24.

You need to create a site-to-site VPN to Azure.

Which four 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.

NOTE: More than one order of answer choice is correct. You will receive credit for any of the correct orders you select.

Select and Place:

1. Create a local gateway.
2. Create a VPN gateway.
3. Create a gateway subnet.
4. Create a custom DNS server.
5. Create a VPN connection.
6. Create an Azure Content Delivery Network (CDN) profile.

- (●) 3,2,1,5
- ( ) 6,4,3,5
- ( ) 2,5,1,3
- ( ) 4,3,2,5

Question : 14 ✓ Total: 50

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

Name	Type	Details
VNet1	Virtual network	Not applicable
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1

VM1 and VM2 are deployed from the same template and host line-of-business applications.

You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit tab.)

Inbound security rules

PRORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	A
100	Port_80	80	TCP	Internet	Any	
65000	AllowVnetinBound	Any	Any	VirtualNetwork	VirtualNetwork	
65001	Allow AzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	
65500	DenyAllInBound	Any	Any	Any	Any	

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	A DenyWebSites	80	TCP	Any	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

You need to prevent users of VM1 and VM2 from accessing websites on the Internet over TCP port 80.

What should you do?

- ○ Disassociate the NSG from a network interface
- ○ Change the Port_80 inbound security rule.
- ◉ Associate the NSG to Subnet1.
- ○ Change the DenyWebSites outbound security rule.

Question : 15 ✓ Total: 50

You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.

Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.

Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.

You need to connect VNet1 to VNet2.

What should you do first?

- ○ Move VM1 to Subscription2.
- ○ Move VNet1 to Subscription2.
- ○ Modify the IP address space of VNet2.
- ◉ Provision virtual network gateways.

Validate ✓

Solution:

Explanation:

The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory

tenant.

Configuring a VNet-to-VNet connection is a good way to easily connect VNets. Connecting a virtual network to another virtual network using the VNet-to-VNet connection type (VNet2VNet) is similar to creating a Site-to-Site IPsec

connection to an on-premises location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE, and both function the same way when communicating.

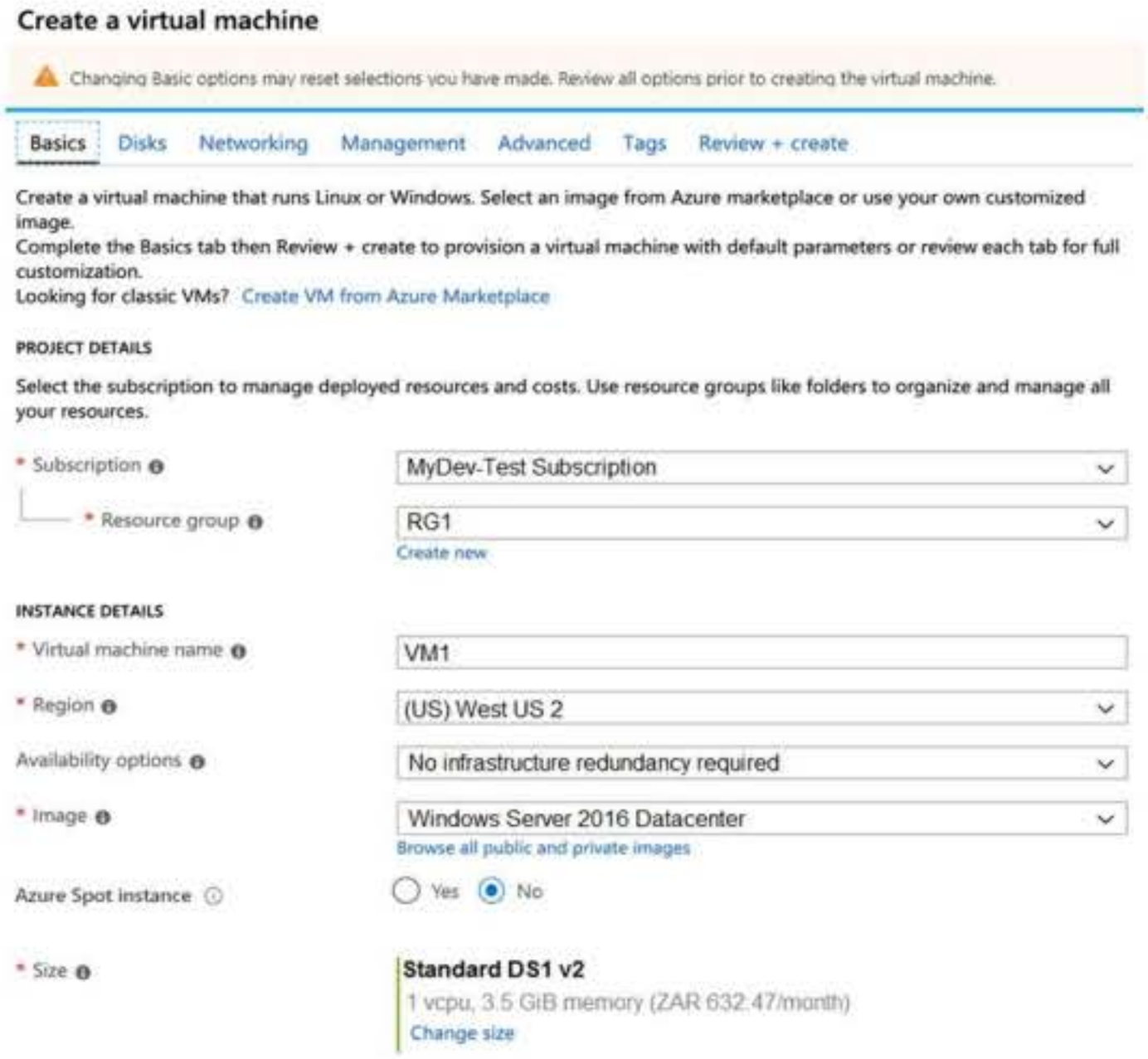
The local network gateway for each VNet treats the other VNet as a local site. This lets you specify additional address space for the local network gateway in order to route traffic.

Reference:

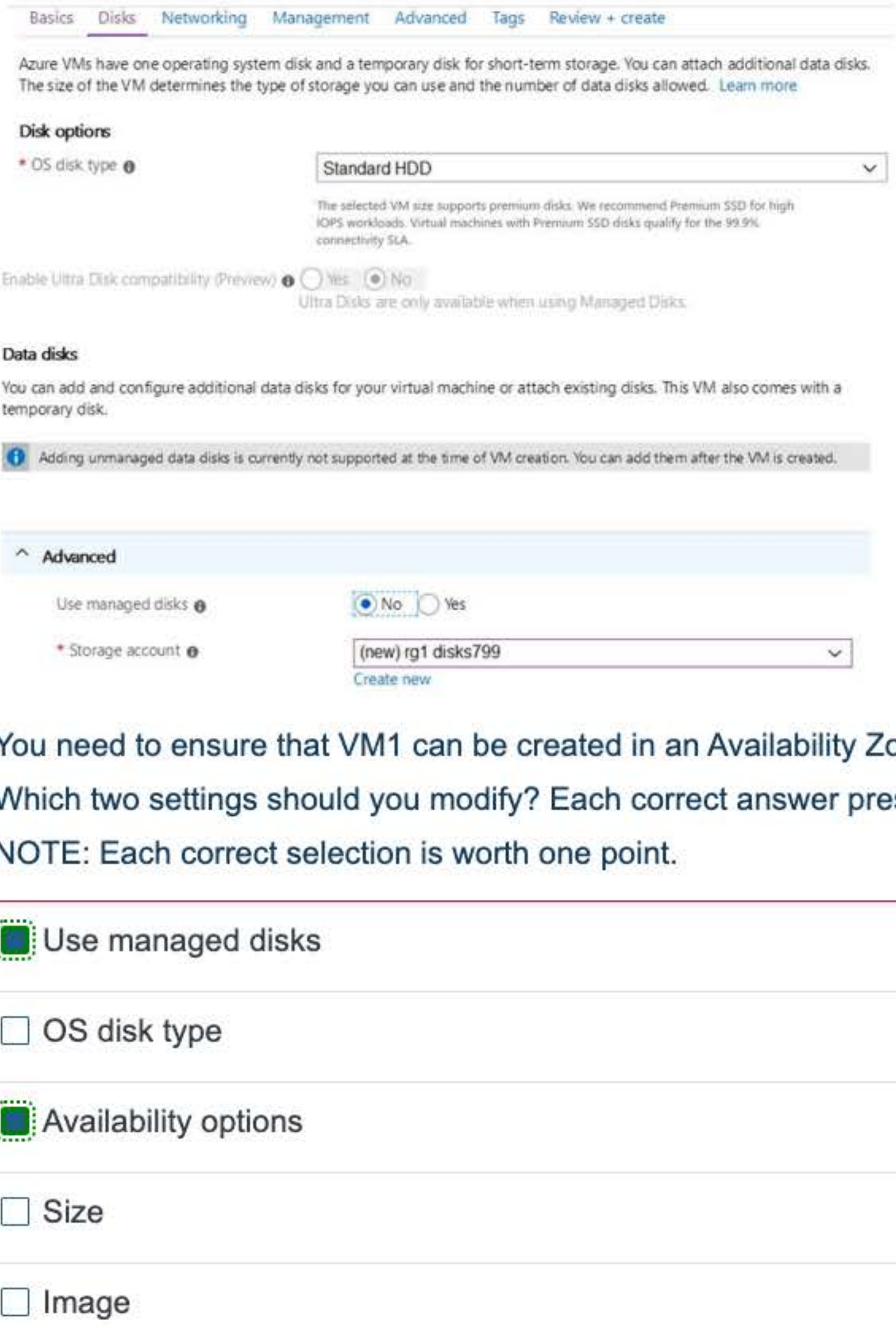
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal

Question : 16 ✓ Total: 50

You plan to create an Azure virtual machine named VM1 that will be configured as shown in the following exhibit



The planned disk configurations for VM1 are shown in the following exhibit



You need to ensure that VM1 can be created in an Availability Zone.

Which two settings should you modify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- [x] Use managed disks
- [ ] OS disk type
- [x] Availability options
- [ ] Size
- [ ] Image

Question : 17 ✓ Total: 50

HOTSPOT

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

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	Central US
RG2	Resource group	Not applicable	West US
RG3	Resource group	Not applicable	East Us
VMSS1	Virtual machine scale set	RG1	West US

VMSS1 is set to VM (virtual machines) orchestration mode.

You need to deploy a new Azure virtual machine named VM1, and then add VM1 to VMSS1.

Which resource group and location should you use to deploy VM1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Resource group _____

- ○ RG1 only
- ○ RG2 only
- ○ RG1 or RG2 only
- ◉ RG1, RG2, or RG3

Location: _____

- ◉ West US only
- ○ Central US only
- ○ Central US or West US only
- ○ East US, Central US, or West US

Validate ✓

Solution:

Explanation:

Box 1: RG1, RG2, or RG3

The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored.

Box 2: West US only

Note: Virtual machine scale sets will support 2 distinct orchestration modes:

ScaleSetVM – Virtual machine instances added to the scale set are based on the scale set configuration model. The virtual machine instance lifecycle - creation, update, deletion - is managed by the scale set.

VM (virtual machines) – Virtual machines created outside of the scale set can be explicitly added to the scaleset.

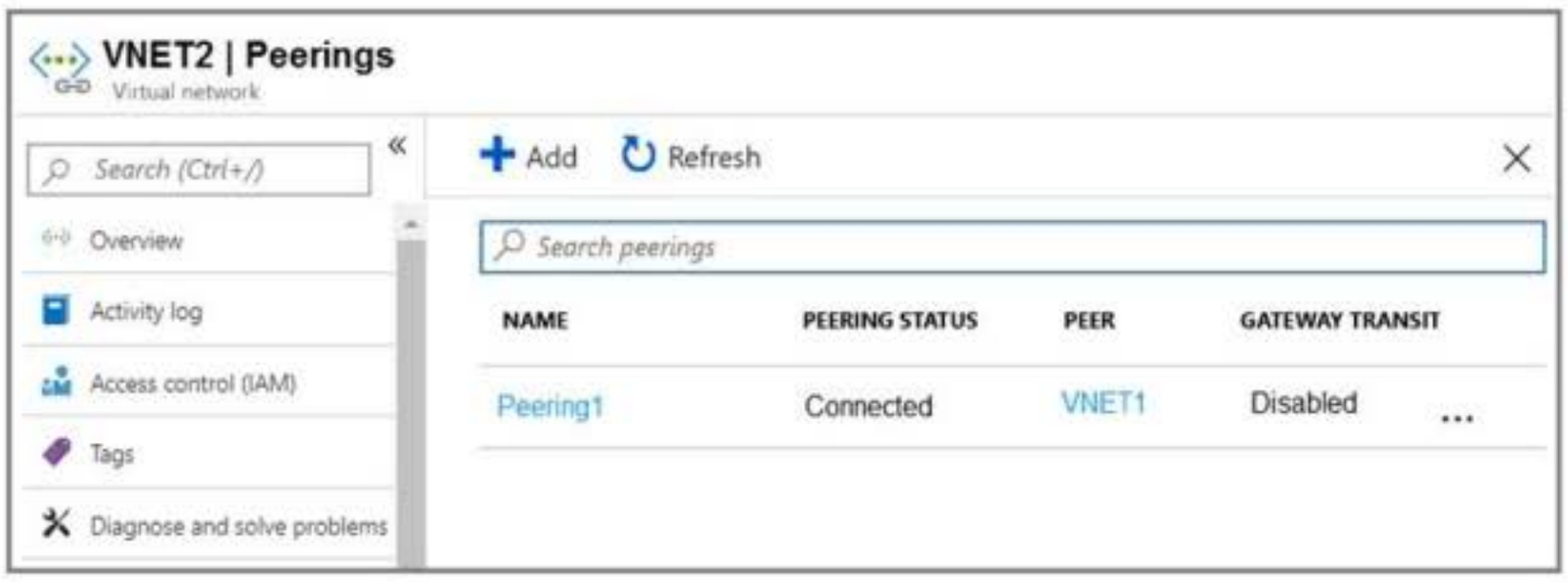
Reference:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview

Question : 18 ✓ Total: 50

HOTSPOT

Peering for VNET2 is configured as shown in the following exhibit.



Peering for VNET3 is configured as shown in the following exhibit.

How can packets be routed between the virtual networks? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Packets from VNET1 can be routed to: _____

- ○ VNET2 only
- ○ VNET3 only
- ◉ VNET2 and VNET3

Packets from VNET2 can be routed to: _____

- ◉ VNET1 only
- ○ VNET3 only
- ○ VNET1 and VNET3

Validate ✓

Solution:

Explanation:

Box 1. VNET2 and VNET3

Box 2: VNET1

Gateway transit is disabled.

Reference:

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

Question : 19 ✓ Total: 50

HOTSPOT

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

Name	Type
VM1	Virtual machine
VM2	Virtual machine
LB1	Load balancer (Basic SKU)

You install the Web Server server role (IIS) on VM1 and VM2, and then add VM1 and VM2 to LB1.

LB1 is configured as shown in the LB1 exhibit. (Click the LB1 tab.)

Rule1 is configured as shown in the Rule1 exhibit. (Click the Rule1 tab.)

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:

VM1 is in the same availability set as VM2. _____

- (●) Yes
- ( ) No

If Probe1.htm is present on VM1 and VM2, LB1 will balance TCP port 80 between VM1 and VM2. _____

- (●) Yes
- ( ) No

If you delete Rule1, LB1 will balance all the requests between VM1 and VM2 for all the ports. _____

- ( ) Yes
- (●) No

Validate ✓

Solution:

Explanation/Reference:

Explanation:

Box 1: Yes

A Basic Load Balancer supports virtual machines in a single availability set or virtual machine scale set.

Box 2: Yes

When using load-balancing rules with Azure Load Balancer, you need to specify health probes to allow Load Balancer to detect the backend endpoint status. The configuration of the health probe and probe responses determine which

backend pool instances will receive new flows. You can use health probes to detect the failure of an application on a backend endpoint. You can also generate a custom response to a health probe and use the health probe for flow control to

manage load or planned downtime. When a health probe fails, Load Balancer will stop sending new flows to the respective unhealthy instance. Outbound connectivity is not impacted, only inbound connectivity is impacted.

Box 3: No

Reference:

https://docs.microsoft.com/en-us/azure/load-balancer/skus

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

Question : 20 ✓ Total: 50

HOTSPOT

You have an Azure virtual machine named VM1 that connects to a virtual network named VNet1. VM1 has the following configurations:

* Subnet: 10.0.0.0/24
* Availability set: AVSet
* Network security group (NSG): None
* Private IP address: 10.0.0.4 (dynamic)
* Public IP address: 40.90.219.6 (dynamic)

You deploy a standard, Internet-facing load balancer named slb1.

You need to configure slb1 to allow connectivity to VM1.

Which changes should you apply to VM1 as you configure slb1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Before you create a backend pool on slb1, you must: _____

- ○ Create and assign an NSG to VM1
- ◉ Remove the public IP address from VM1
- ○ Change the private IP address of VM1 to static

Before you can connect to VM1 from slb1, you must: _____

- ◉ Create and configure an NSG
- ○ Remove the public IP address from VM1

Validate ✓

Solution:

Explanation:

Change the private IP address of VM1 to static

Box 1: Remove the public IP address from VM1

Note: A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load

Balancers are used to load balance internet traffic to your VMs.

Box 2: Create and configure an NSG

NSGs are used to explicitly permit allowed traffic. If you do not have an NSG on a subnet or NIC of your virtual machine resource, traffic is not allowed to reach this resource.

Reference:

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Question : 21 ✓ Total: 50

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

Name	Type	Location
VNET1	Virtual network	East US
IP1	Public IP address	West Europe
RT1	Route table	North Europe

You need to create a network interface named NIC1.

In which location can you create NIC1?

- ○ East US and North Europe only
- ◉ East US only
- ○ East US, West Europe, and North Europe
- ○ East US and West Europe only

Validate ✓

Solution:

Explanation:

Before creating a network interface, you must have an existing virtual network in the same location and subscription you create a network interface in.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

Question : 22 ✓ Total: 50

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Virtual network name	DNS suffix configured in Windows Server
VM1	VNET1	Contoso.com
VM2	VNET2	Contoso.com

You create a public Azure DNS zone named adatum.com and a private Azure DNS zone named contoso.com.

For controso.com, you create a virtual network link named link1 as shown in the exhibit. (Click the Exhibit tab.)
You discover that VM1 can resolve names in contoso.com but cannot resolve names in adatum.com. VM1 can resolve other hosts on the Internet.

You need to ensure that VM1 can resolve host names in adatum.com.

What should you do

- ○ Update the DNS suffix on VM1 to be adatum.com
- ◉ Configure the name servers for adatum.com at the domain registrar
- ○ Create an SRV record in the contoso.com zone
- ○ Modify the Access control (IAM) settings for link1

Question : 23 ✓ Total: 50

HOTSPOT

You plan to use Azure Network Watcher to perform the following tasks:

✣ Task1: Identify a security rule that prevents a network packet from reaching an Azure virtual machine.

✣ Task2: Validate outbound connectivity from an Azure virtual machine to an external host.

Which feature should you use for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Task1: _____

- (●) IP flow verify
- ( ) Next hop
- ( ) Packet capture
- ( ) Security group view
- ( ) Traffic Analytics

Task2: _____

- (●) Connection troubleshoot
- ( ) IP flow verify
- ( ) Next hop
- ( ) NSG flow logs
- ( ) Traffic Analytics

Validate ✓

Solution:

Explanation:

Box 1: IP flow verify

At some point, a VM may become unable to communicate with other resources, because of a security rule. The IP flow verify capability enables you to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic

direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails. If the connection fails, IP flow verify tells you which.

Box 2: Connection troubleshoot

Diagnose outbound connections from a VM: The connection troubleshoot capability enables you to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when

using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does. Learn more about how to troubleshoot connections using connection-troubleshoot.

Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

Question : 24 ✓ Total: 50

HOTSPOT

You have an Azure subscription that contains the Azure virtual machines shown in the following table

Name	Operating system	Subnet	Virtual network
VM1	Windows Server 2019	Subnet1	VNET1
VM2	Windows Server 2019	Subnet2	VNET1
VM3	Red Hat Enterprise Linux 7.7	Subnet3	VNET1

You configure the network interfaces of the virtual machines to use the settings shown in the following table.

Name	DNS server
VM1	None
VM2	192.168 .10 .15
VM3	102168.1015

From the settings of VNET1 you configure the DNS servers shown in the following exhibit

The virtual machines can successfully connect to the DNS server that has an IP address of 192.168.10.15 and the DNS server that has an IP address of 193.77.134.10.

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:

VM1 connects to 193.77 .134 .10 for DNS queries. _____

- ◉ Yes
- ○ No

VM2 connects to 193.77 .134 .10 for DNS queries. _____

- ○ Yes
- ◉ No

VM3 connects to 192.168 .10 .15 for DNS queries. _____

- ◉ Yes
- ○ No

Question : 25 ✓ Total: 50

HOTSPOT

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

Name	Lock name	Lock type
RG1	None	None
RG2	Lock	Delete

RG1 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage1	Storage account	Lock1	Delete
VNET1	Virtual network	Lock2	Read-only
IP1	Public IP address	None	None

RG2 contains the resources shown in the following table.

Name	Type	Lock name	Lock type
storage2	Storage account	Lock1	Delete
VNET2	Virtual network	Lock2	Read-only
IP2	Public IP address	None	None

You need to identify which resources you can move from RG1 to RG2, and which resources you can move from RG2 to RG1.

Which resources should you identify? To answer, select the appropriate options in the answer area.

Hot Area:

Resources that you can move from RG1 to RG2: _____

- ○ None
- ○ IP1 only
- ○ IP1 and storage1 only
- ○ IP1 and VNET1 only
- ◉ IP1, VNET2, and storage1

Resources that you can move from RG2 to RG1: _____

- ○ None
- ○ IP2 only
- ○ IP2 and storage 2 only
- ○ IP2 and VNET2 only
- ◉ IP2, VNET2, and storage2

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

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

✣ Name: LB1

✣ Type: Internal

✣ SKU: Standard

✣ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Question : 26 ✓ Total: 50

Refer paragraph From Q.No : 26

Refer Solution: You create a Basic SKU public IP address, associate the address to the network interface of VM1, and then start VM1.

Does this meet the goal?

○ Yes

◉ No

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

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

✣ Name: LB1

✣ Type: Internal

✣ SKU: Standard

✣ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Question : 27 ✕ Total: 50

Refer paragraph From Q.No : 26

Solution: You create a Standard SKU public IP address, associate the address to the network interface of VM1, and then stop VM2.

Does this meet the goal?

○ Yes

◉ No

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

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

✣ Name: LB1

✣ Type: Internal

✣ SKU: Standard

✣ Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Question : 28 ✓ Total: 50

Refer paragraph From Q.No : 26

Solution: You create two Standard public IP addresses and associate a Standard SKU public IP address to the network interface of each virtual machine.

Does this meet the goal?

- (●) Yes
- ( ) No

Question : 29 ✓ Total: 50

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 a computer named Computer1 that has a point-to-site VPN connection to an Azure virtual network named VNet1. The point-to-site connection uses a self-signed certificate.

From Azure, you download and install the VPN client configuration package on a computer named Computer2.

You need to ensure that you can establish a point-to-site VPN connection to VNet1 from Computer2.

Solution: You export the client certificate from Computer1 and install the certificate on Computer2.

Does this meet the goal

- (●) Yes
- ( ) No

Validate ✓

Solution:

Explanation:

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client

certificate is not installed, authentication fails.

Reference:

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

Question : 30 ✓ Total: 50

You have an Azure virtual machine named VM1.

The network interface for VM1 is configured as shown in the exhibit. (Click the Exhibit tab.)

INBOUND PORT RULES

Network security group VM1-nsg (attached to network interface: vm1175)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	3389	TCP	Any	Any	Allow
400	Rule1	80	TCP	Any	Any	Deny
500	Rule2	80,443	TCP	Any	Any	Deny
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny
3000	Rule6	150-300	Any	Any	Any	Allow
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You deploy a web server on VM1, and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the Internet.

What should you do?

- ○ Modify the protocol of Rule4
- ○ Delete Rule1
- ◉ For Rule5, change the Action to Allow and change the priority to 401
- ○ Create a new inbound rule that allows TCP protocol 443 and configure the rule to have a priority of 501.

Validate ✓

Solution:

Explanation:

HTTPS uses port 443.

Rule2, with priority 500, denies HTTPS traffic.

Rule5, with priority changed from 2000 to 401, would allow HTTPS traffic.

Note: Priority is a number between 100 and 4096. Rules are processed in priority order,with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a

result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. Change the priority of Rule3 to 450.

2. For Rule5, change the Action to Allow and change the priority to 401.

Other incorrect answer options you may see on the exam include the following:

■ Modify the action of Rule1.

■ Change the priority of Rule6 to 100.

■ For Rule4, change the protocol from UDP to Any.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Question : 31 ✓ Total: 50

HOTSPOT

You manage two Azure subscriptions named Subscription1 and Subscription2.

Subscription1 has following virtual networks

Name	Address space	Location
VNET1	10.10 .10 .0 / 24	West Europe
VNET2	172.16 .0 .0 / 16	West US

The virtual networks contain the following subnets:

Name	Address space	In virtual network
Subnet11	10 · 10 · 10.0/24	VNET1
Subnet21	172 · 16.0 .0/18	VNET2
Subnet22	172 · 16.128 .0/ 18	VNET2

Subscription 2 contains the following virtual network:

- Name: VNETA
- Address space: 10.10.128.0/17
- Location: Canada Central

VNETA contains the following subnets:

Name	Address space
SubnetA1	10.10 .130 .0 / 24
SubnetA2	10.10 .131 .0 / 24

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:

A Site-to-Site connection can be established between VNET1 and VNET2. _____

○ Yes

● No

VNET1 and VNET2 can be peered. _____

● Yes

○ No

VNET1 and VNETA can be peered. _____

● Yes

○ No

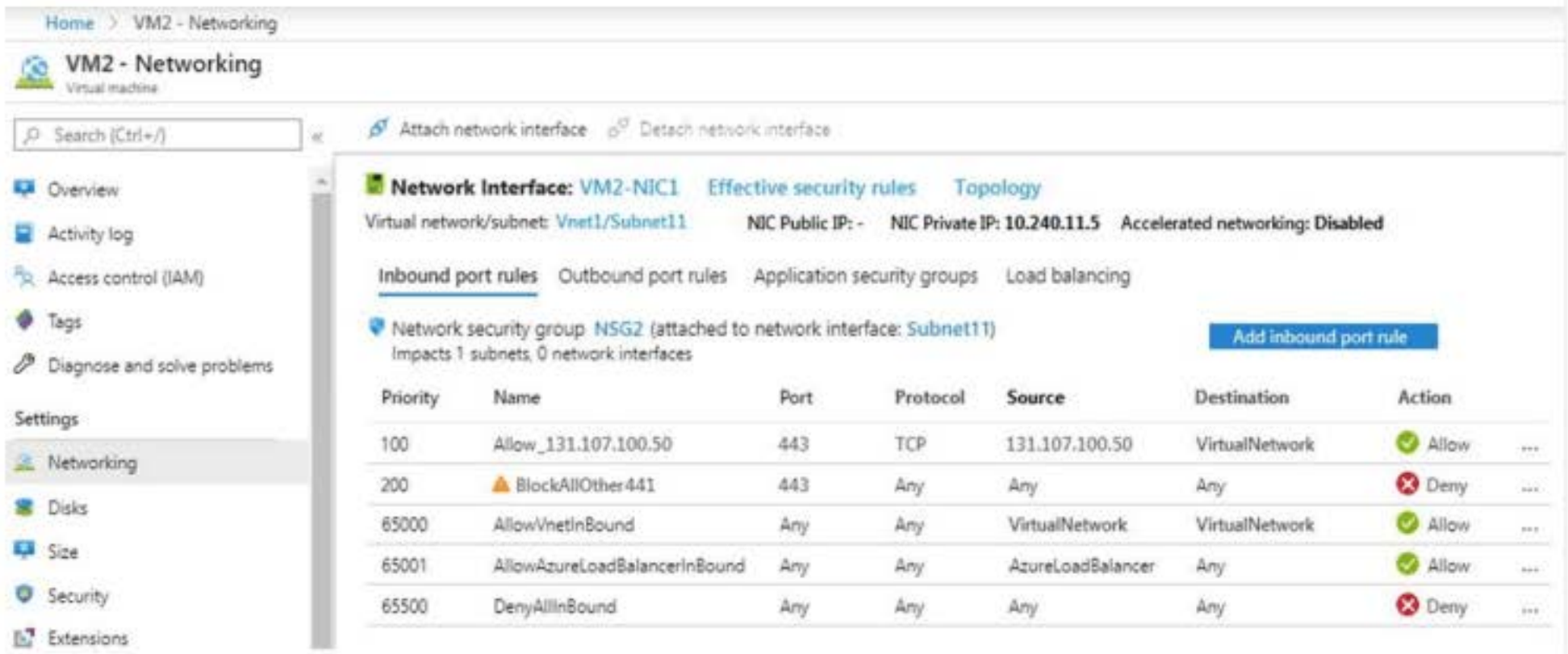
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Question : 32 ✓ Total: 50

Refer paragraph From Q.No : 32

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a cost of 64999.

Does this meet the goal

- ○ Yes
- ◉ No

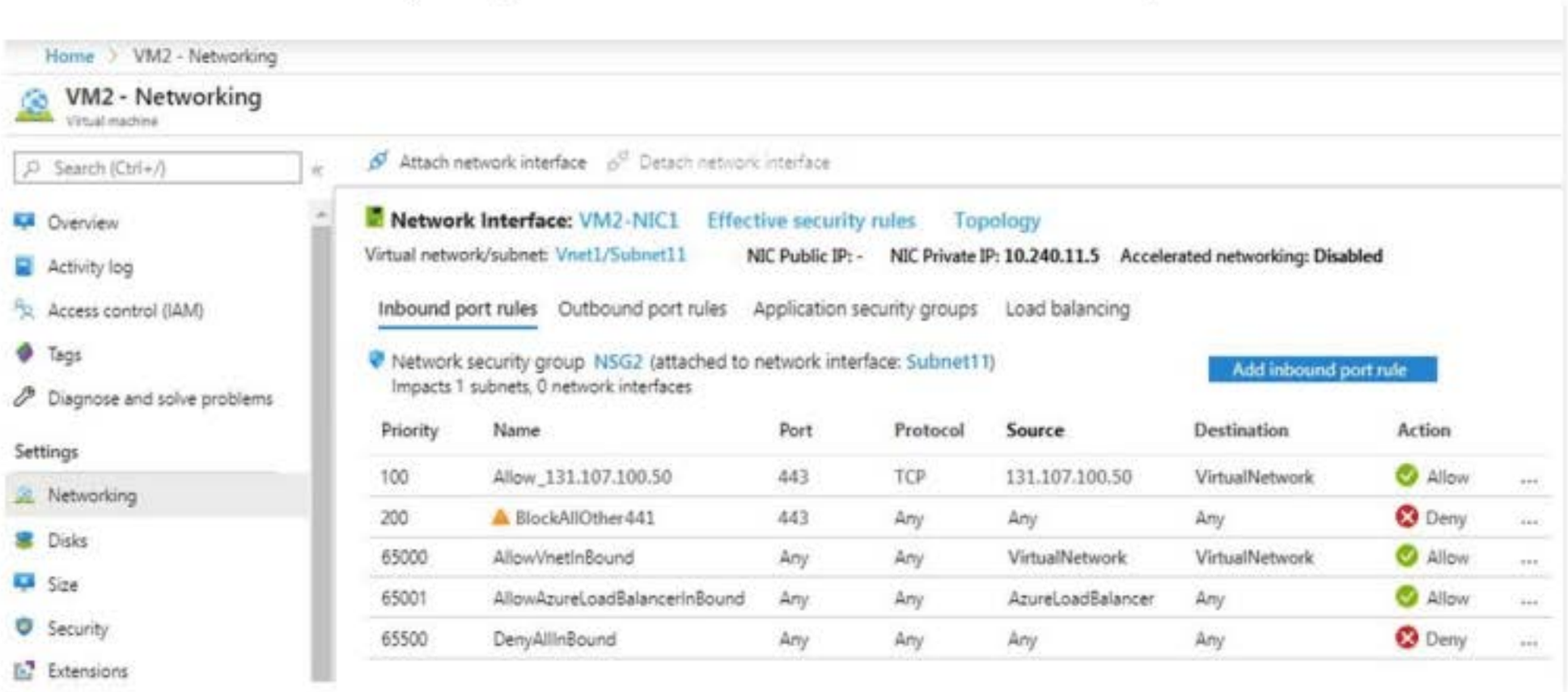
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Question : 33 ✓ Total: 50

Refer paragraph From Q.No : 32

Solution: You delete the BlockAllOther443 inbound security rule.

Does this meet the goal?

- ○ Yes
- ◉ No

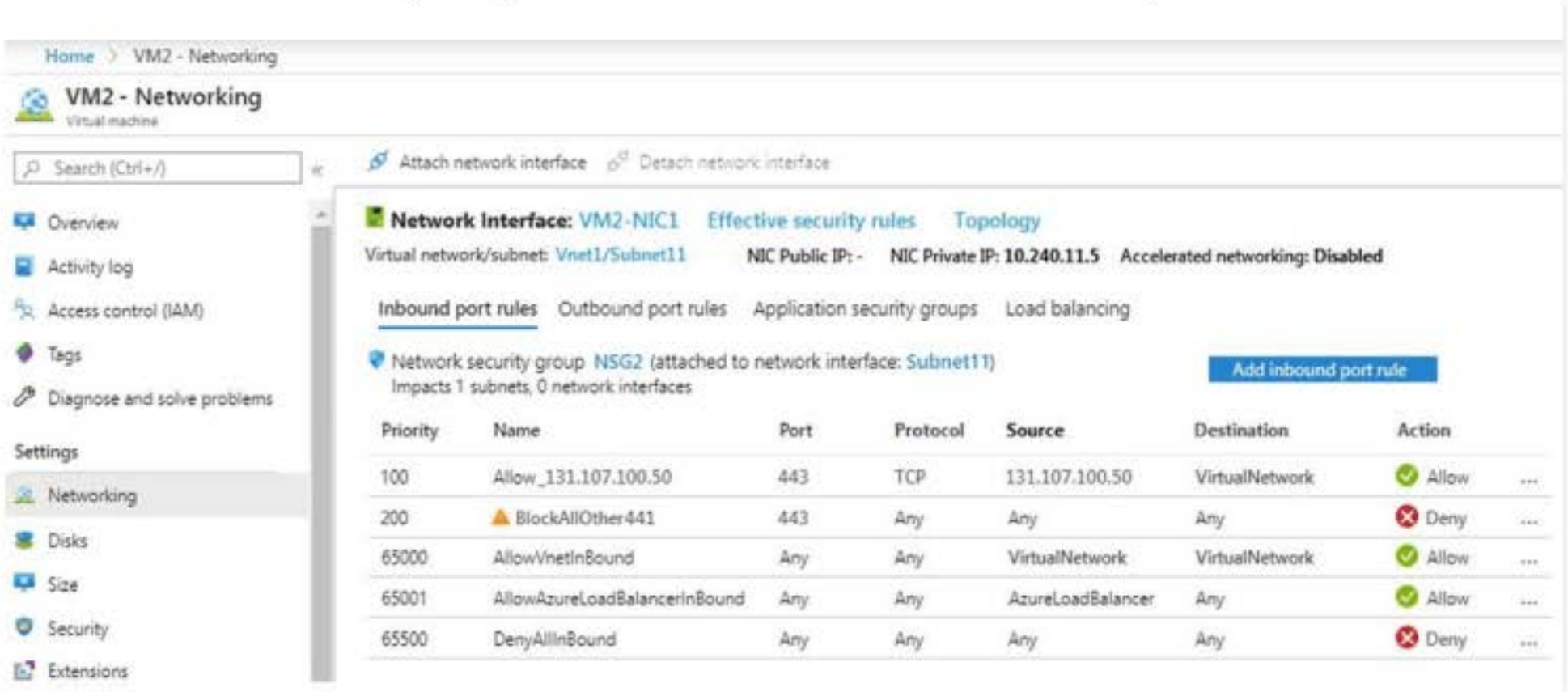
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Question : 34 ✓ Total: 50

Refer paragraph From Q.No : 32

Solution: You modify the priority of the Allow_131.107.100.50 inbound security rule.

Does this meet the goal?

- (●) Yes
- ( ) No

Question : 35 ✓ Total: 50

You have an Azure subscription.

You plan to deploy an Azure Kubernetes Service (AKS) cluster to support an app named App1. On-premises clients connect to App1 by using the IP address of the pod.

For the AKS cluster, you need to choose a network type that will support App1.

What should you choose?

- ○ kubenet
- ◉ Azure Container Networking Interface (CNI)
- ○ Hybrid Connection endpoints
- ○ Azure Private Link

Question : 36 ✓ Total: 50

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

Name	Public IP SKU	Connected to	Status
VM1	None	VNET1/Subnet1	Stopped (deallocated)
VM2	Basic	VNET1/Subnet2	Running

You deploy a load balancer that has the following configurations:

- Name: LB1
- Type: Internal
- SKU: Standard
- Virtual network: VNET1

You need to ensure that you can add VM1 and VM2 to the backend pool of LB1.

Solution: You disassociate the public IP address from the network interface of VM2.

Does this meet the goal?

- ○ Yes
- ◉ No

Question : 37 ✓ Total: 50

HOTSPOT

You have an Azure subscription that contains the public load balancers shown in the following table

Name	SKU
LB1	Basic
LB2	Standard

You plan to create six virtual machines and to load balance requests to the virtual machines. Each load balancer will load balance three virtual machines.

You need to create the virtual machines for the planned solution.

Hot Area:

The virtual machines that will be load balanced by using LB1 must: _____

- ○ be connected to the same virtual network
- ○ be created in the same resource group
- ● be created in the same availability set or virtual machine scale set
- ○ run the same operating system

The virtual machines that will be load balance by using LB2 must: _____

- ● be connected to the same virtual network
- ○ be created in the same resource group
- ○ be created in the same availability set or virtual machine scale set
- ○ run the same operating system

Question : 38 ✓ Total: 50

HOTSPOT

You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network named VNet1. VNet1 contains a gateway subnet.

You need to create a site-to-site VPN. The solution must ensure that if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.

What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Public IP addresses: _____

- ○ 1
- ○ 2
- ○ 3
- ◉ 4

Virtual network gateways: _____

- ○ 1
- ◉ 2
- ○ 3
- ○ 4

Local network gateways: _____

- ○ 1
- ◉ 2
- ○ 3
- ○ 4

Validate ✓

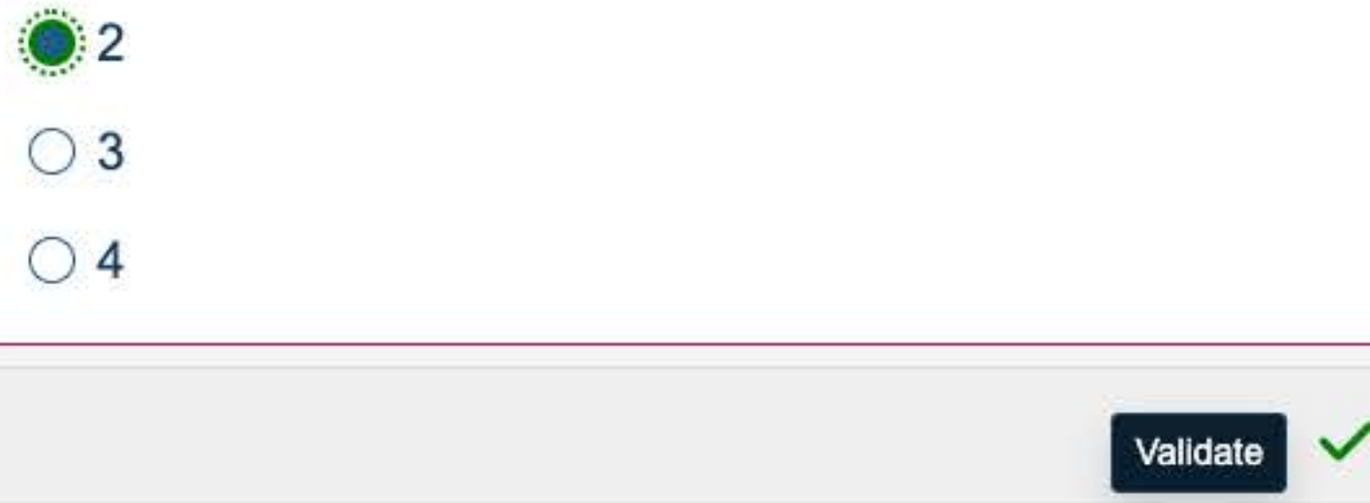
Solution:

Explanation:

Box 1: 4

Two public IP addresses in the on-premises data center, and two public IP addresses in the VNET.

The most reliable option is to combine the active-active gateways on both your network and Azure, as shown in the diagram below.



Box 2: 2

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover)

automatically, and resume the S2S VPN or VNet-to-VNet connections.

Box 3: 2

Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks

Reference:

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

Question : 39 ✓ Total: 50

You have an Azure subscription that contains two virtual machines as shown in the following table

Name	Operating system	Location	IP address	DNS server
VM1	Windows Server 2019	West Europe	10.0 .0 .4	Default (Azure-provided)
VM2	Windows Server 2019	West Europe	10.0 .0 .5	Default (Azure-provided)

You perform a reverse DNS lookup for 10.0.0.4 from VM2.

Which FQDN will be returned?

- ○ vm1.core.windows.net
- ○ vm1.azure.com
- ○ vm1.westeurope.cloudapp.azure.com
- ◉ vm1.internal.cloudapp.net

Question : 40 ✓ Total: 50

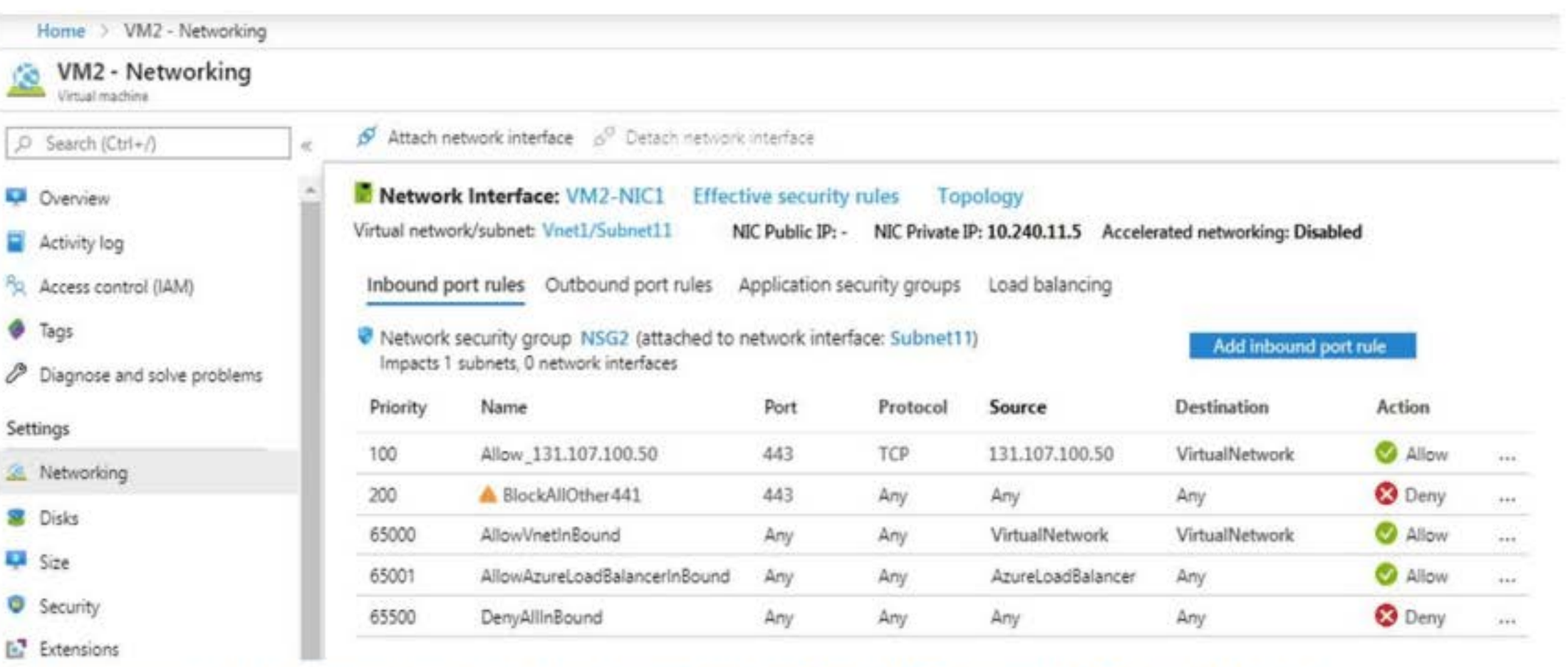
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that allows any traffic from the AzureLoadBalancer source and has a cost of 150.

Does this meet the goal?

- (●) Yes
- ( ) No

Question : 41 ✓ Total: 50

HOTSPOT

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

Name	Location
VNET1	West US
VNET2	West US
VNET3	East US

The subscription contains the private DNS zones shown in the following table

Name	Location
Zone1.com	West US
Zone2.com	West US
Zone3.com	East US

You add virtual network links to the private DNS zones as shown in the following table.

Name	Private DNS zone	Virtual network	Enable auto registration
Link1	Zone1.com	VNET1	Yes
Link2	Zone2.com	VNET2	No
Link3	Zone3.com	VNET3	No

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:

You can enable auto registration for Link2. _____

- ○ Yes
- ◉ No

You can add a virtual network link for VNET1 1 to Zone3.com. _____

- ○ Yes
- ◉ No

You can add a virtual network link for VNET2 to Zone1.com and enable auto registration. _____

- ○ Yes
- ◉ No

Question : 42 ✓ Total: 50

HOTSPOT

You have an Azure subscription.

You plan to use an Azure Resource Manager template to deploy a virtual network named VNET1 that will use Azure Bastion.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

_____

- (●) AzureBastionSubnet
- ( ) AzureFirewallsubnet
- ( ) LAN01
- ( ) RemoteAccessSubnet

Blank(i) _____

- (●) 10.10 .10 .0 / 27
- ( ) 10.10 .10 .0 / 29
- ( ) 10.10 .10 .0 / 30

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Question : 43 ✓ Total: 50

Refer paragraph From Q.No : 43

Solution: From Azure Network Watcher, you create a packet capture.

Does this meet the goal?

- (●) Yes
- ( ) No

Validate ✓

Solution:

Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactively. Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communications and much more.

Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-overview

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Question : 44 ✓ Total: 50

Refer paragraph From Q.No : 43

Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

- ○ Yes
- ◉ No

Question : 45 ✓ Total: 50

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Network Watcher, you create a connection monitor.

Does this meet the goal?

- ○ Yes
- ◉ No

Question : 46 ✓ Total: 50

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Performance Monitor, you create a Data Collector Set (DCS).

Does this meet the goal?

- ○ Yes
- ◉ No

Question : 47 ✓ Total: 50

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

Name	Type
LB1	Load balancer
VM1	Virtual machine
VM2	Virtual machine

LB1 is configured as shown in the following table.

Name	Type	Value
bepool1	Backend pool	VM1, VM2
LoadBalancerFrontEnd	Frontend IP configuration	Public IP address
hprobe1	Health probe	Protocol: TCP Port: 80 Interval:5 seconds Unhealthy threshold:2
rule1	Load balancing rule	IP version: IPv4 Frontend IP address: LoadBalancerFrontEnd Port: 80 Backend Port: 80 Backend pool: bepool1 Health probe: hprobe1

You plan to create new inbound NAT rules that meet the following requirements:

- Provide Remote Desktop access to VM1 from the internet by using port 3389.
- Provide Remote Desktop access to VM2 from the internet by using port 3389.

What should you create on LB1 before you can create the new inbound NAT rules?

- (●) a frontend IP address
- ( ) a load balancing rule
- ( ) a health probe
- ( ) a backend pool

DRAG DROP

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

Name	Type	Description
vm1	Virtual machine	Uses a basic public IP address
vm2	Virtual machine	Uses a basic public IP address
nsg1	Network security group (NSG)	Allows incoming traffic from port 443
lb1	Azure Standard Load Balancer	Not applicable

You need to load balance HTTPS connections to vm1 and vm2 by using lb1.

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:

1. Remove nsg1.
2. Remove the public IP addresses from vm1 and vm2.
3. Create a health probe and backend pool on lb1.
4. Create an availability set.
5. Create a load balancing rule on lb1.

- (●) 2,3,5
- ( ) 1,4,3
- ( ) 2,4,3
- ( ) 4,5,1

Question : 49 ✓ Total: 50

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 manage a virtual network named VNet1 that is hosted in the West US Azure region.

VNet1 hosts two virtual machines named VM1 and VM2 that run Windows Server.

You need to inspect all the network traffic from VM1 to VM2 for a period of three hours.

Solution: From Azure Monitor, you create a metric on Network In and Network Out.

Does this meet the goal?

- ○ Yes
- ◉ No

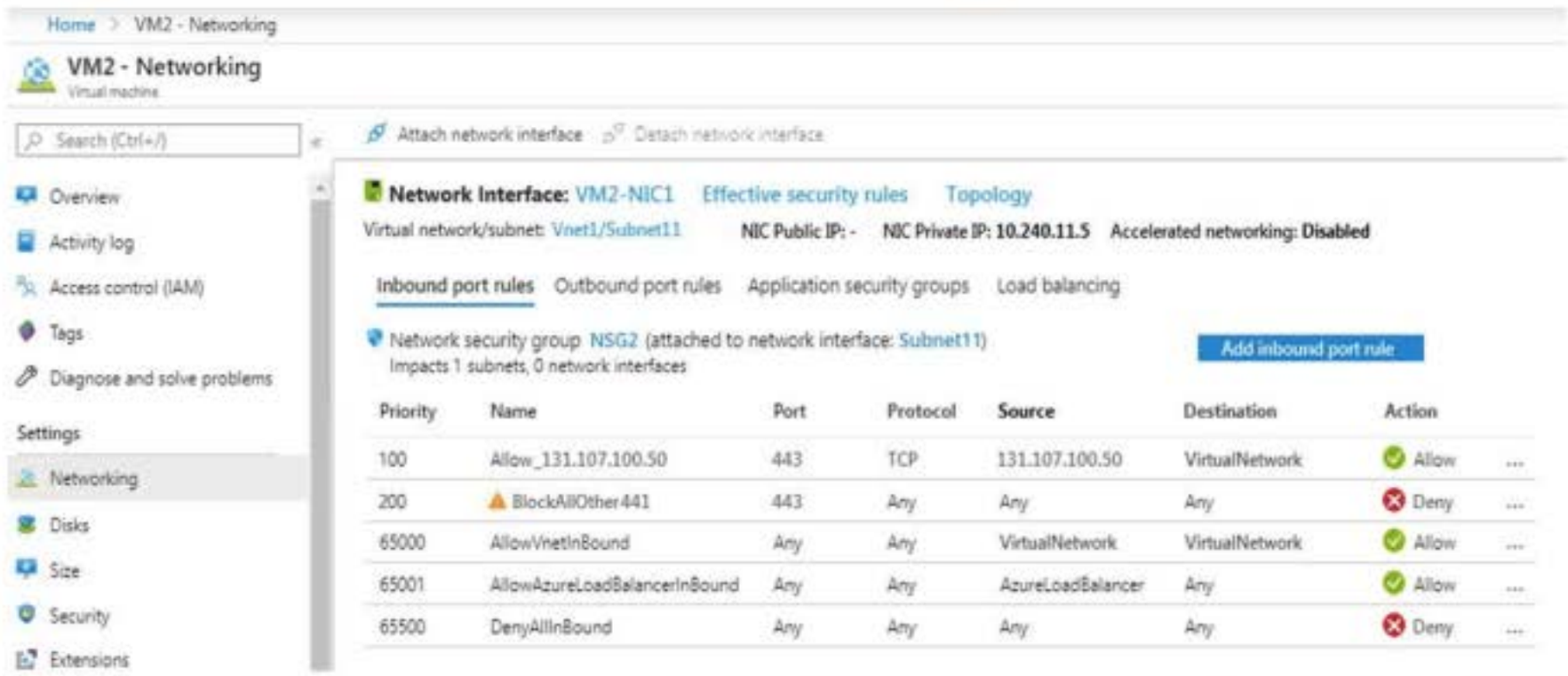
Question : 50 ✓ Total: 50

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 app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer. The effective network security configurations for VM2 are shown in the following exhibit.



You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You create an inbound security rule that denies all traffic from the 131.107.100.50 source and has a priority of 64999.

Does this meet the goal?

- ○ Yes
- ◉ No