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.geekcert.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You plan to deploy 100 virtual machines to subnet-1. The virtual machines will NOT be assigned a public IP address. The virtual machines will call the same API which is hosted by a third party. The virtual machines will make more than 10,000 calls per minute to the API.

You need to minimize the risk of SNAT port exhaustion. The solution must minimize administrative effort.

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

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

SNAT exhaustion occurs when a backend instance runs out of given SNAT Ports. A load balancer can still have unused SNAT ports. If a backend instance\\'s used SNAT ports exceed its given SNAT ports, it will be unable to establish new

outbound connections.

Use a NAT gateway for outbound connectivity to the Internet

Virtual network NAT gateway is a highly resilient and scalable Azure service that provides outbound connectivity to the internet from your virtual network. A NAT gateway\\'s unique method of consuming SNAT ports helps resolve common

SNAT exhaustion and connection issues.

(Basic load balancers and basic public IP addresses aren\\'t compatible with NAT.)

Create a NAT gateway

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab.

* Details omitted *

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

* Public IP addresses

Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Reference: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections
https://learn.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection

QUESTION 2

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a subnet named Subnet1.

You deploy an instance of Azure Application Gateway v2 named AppGw1 to Subnet1. You create a network security group (NSG) named NSG1 and link NSG1 to Subnet1.

You need to ensure that AppGw1 will only load balance traffic that originates from VNet1. The solution must minimize the impact on the functionality of AppGw1.

What should you add to NSG1?

A. an outbound rule that has a priority of 4096 and blocks all internet traffic

B. an inbound rule that has a priority of 4096 and blocks all internet traffic

C. an inbound rule that has a priority of 100 and blocks all internet traffic

D. an outbound rule that has a priority 100 and blocks all internet traffic

Correct Answer: B

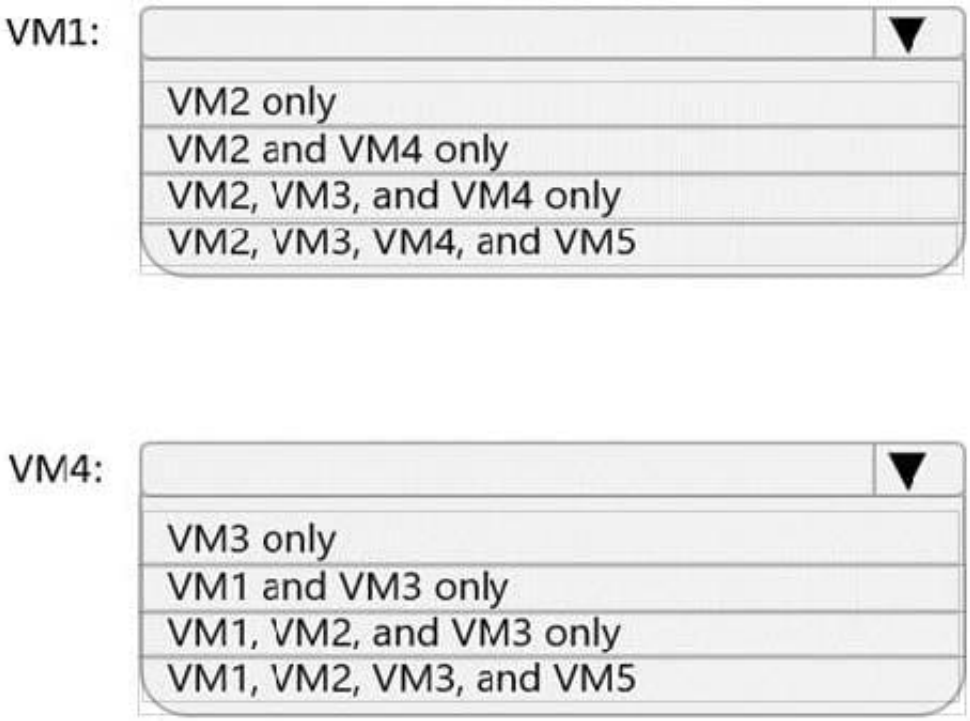
QUESTION 3

HOTSPOT

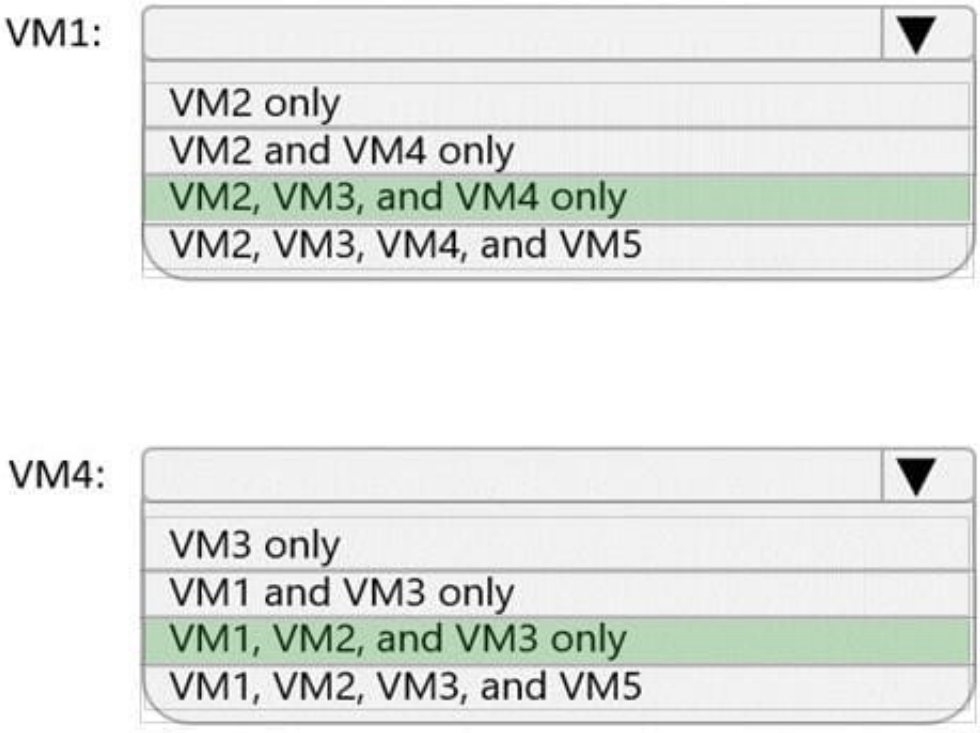
Which virtual machines can VM1 and VM4 ping successfully? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: VM2, VM3 and VM4.

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

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

Box 2:

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

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

QUESTION 4

You have an Azure subscription that contains a virtual network.

You plan to deploy an Azure VPN gateway and 90 Site-to-Site VPN connections. The solution must meet the following requirements:

1.

Ensure that the Site-to-Site VPN connections remain available if an Azure datacenter fails.

2.

Minimize costs.

Which gateway SKU should you specify?

A. VpnGw1AZ

B. VpnGw2AZ

C. VpnGw4AZ

D. VpnGw5AZ

Correct Answer: C

VpnGw4AZ supports 90 Site-to-Site VPN connections at a lower cost than VpnGw5AZ. VpnGw1AZ, VpnGw2AZ, and VpnGw4AZ supports max 30.

Gateway SKUs by tunnel, connection, and throughput

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redund
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	No
Generation2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	No
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	No
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	No

Reference: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

QUESTION 5

You need to validate outbound connectivity from an Azure virtual machine to an external host. What should you use?

A. Connection Troubleshoot

B. Next hop

C. NSG flow logs

D. Traffic Analytics

Correct Answer: A

Correct Answer(s):

Connection Troubleshoot - 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

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

Wrong Answers:

Next hop -- Next hop helps you determine if traffic is being directed to the intended destination, or whether the traffic is being sent nowhere.

NSG flow logs -- NSG flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG.

Traffic Analytics It provides visibility into user and application activity in cloud networks.