



# AZ-700<sup>Q&As</sup>

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.passapply.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****HOTSPOT**

You have two Azure virtual networks named Vnet1 and Vnet2 in an Azure region that has three availability zones.

You deploy 12 virtual machines to each virtual network, deploying four virtual machines per zone. The virtual machines in Vnet1 host an app named App1. The virtual machines in Vnet2 host an app named App2.

You plan to use Azure Virtual Network NAT to implement outbound connectivity for App1 and App2.

You need to identify the minimum number of subnets and Virtual Network NAT instances required to meet the following requirements:

1.

A failure of two zones must NOT affect the availability of either App1 or App2.

2.

A failure of two zones must NOT affect the outbound connectivity of either App1 or App2.

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

NOTE: Each correct selection is worth one point.

Hot Area:



### Permissions requested

### Accept for your organization

**Azure VPN**  
[App info](#)

This app would like to:

- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

CancelAccept

7. Under your Azure AD, in Enterprise applications, you see Azure VPN listed.

Home > Contoso Corp > Enterprise applications > All applications

Enterprise applications - All applications

Contoso Corp - Azure Active Directory

Overview

Overview

Diagnose and solve problems

Manage

All applications

Application proxy

User settings

Security

Conditional Access

Activity

Sign-ins

Usage & insights (Preview)

Audit logs

Provisioning logs (Preview)

Access reviews

Troubleshooting & Support

Virtual assistant (Preview)

New support request

+ New application

Columns

Application Type

Enterprise Applications

Applications status

Any

Application visibility

Any

Apply

Reset

First 50 shown. To search all of your applications, enter a display name or the application ID.

NAME	Homepage URL	OBJECT ID	APPLICATION ID
Azure VPN	<a href="https://www.microsoft.com">https://www.microsoft.com</a>		

Correct Answer:

Name	Address space	Associated network security group (NSG)
Subnet1	10.10.0.0/24	NSG1
Subnet2	10.10.1.0/24	NSG2

6 Subnets and 6 GW

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal-nat-gateway-resource-for-each-zone-in-a-region-to-create-zone-resiliency>

"The pattern you want to use for zone isolation is creating a "zonal stack" per availability zone. This "zonal stack" consists of virtual machine instances, a NAT gateway resource with public IP addresses or prefix on a subnet all in the

AZ-700 Study Guide | AZ-700 Exam Questions | AZ-700 Braindumps

3 / 8



same

zone.

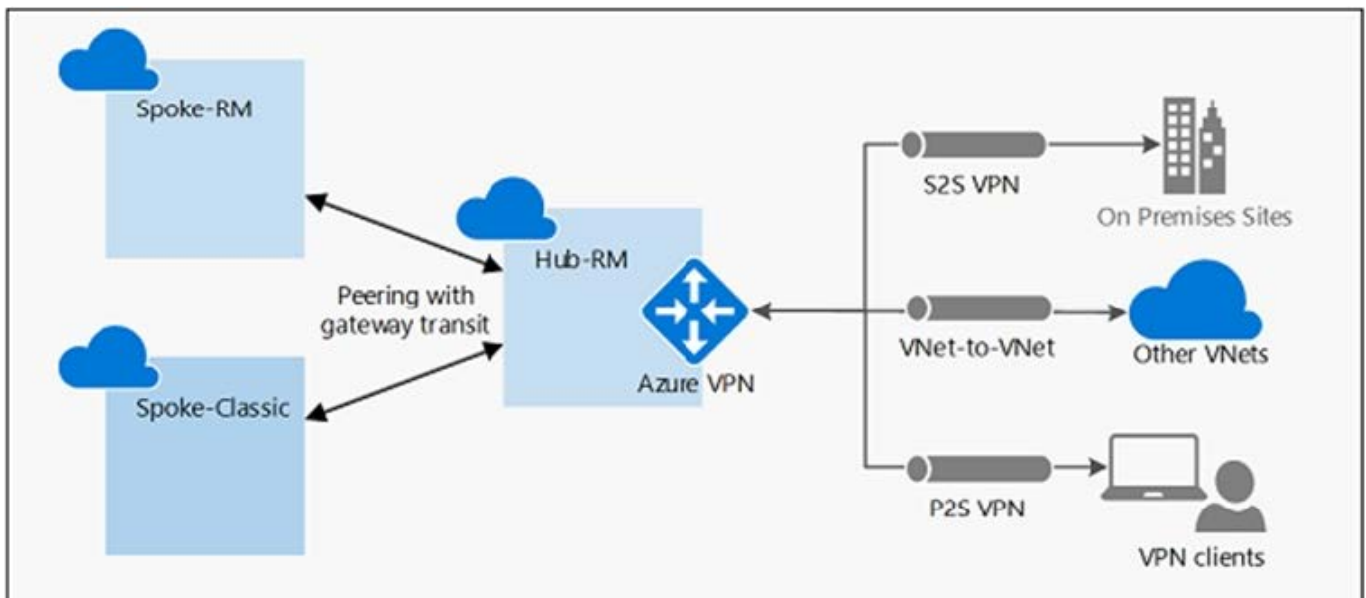
Failure of outbound connectivity due to a zone outage is isolated to the specific zone affected. The outage won't affect the other zonal stacks where other NAT gateways are deployed with their own subnets and zonal public IPs."

## QUESTION 2

### HOTSPOT

You have an Azure subscription.

You have the on-premises sites shown the following table.



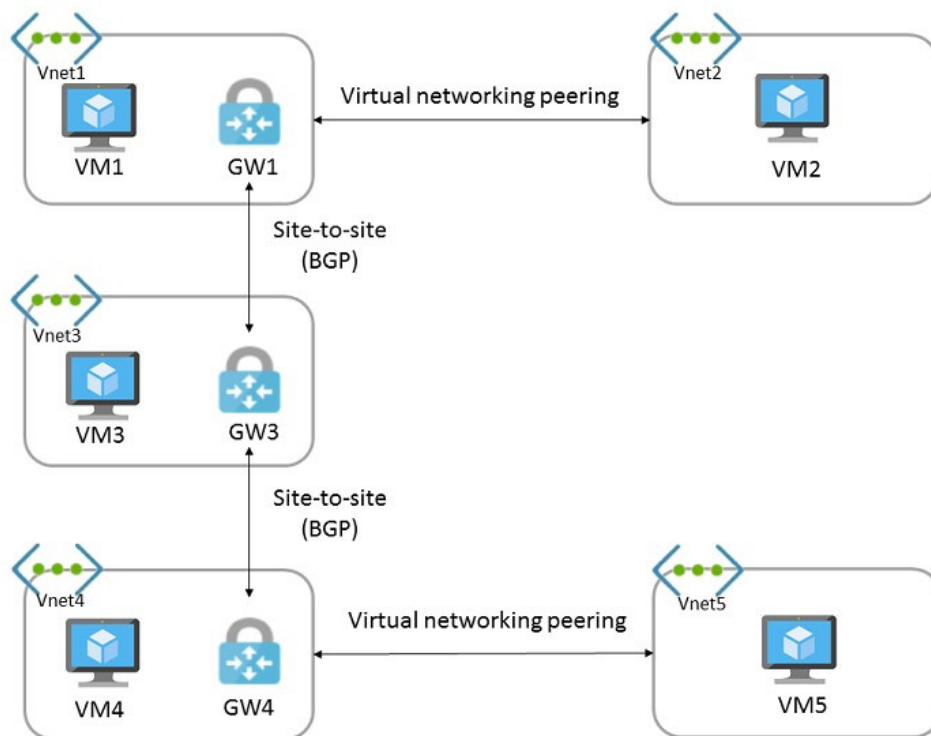
You plan to deploy Azure Virtual WAN.

You are evaluating Virtual WAN Basic and Virtual WAN Standard.

Which type of Virtual WAN can you use for each site? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

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

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

### QUESTION 3

#### HOTSPOT

You have an Azure Traffic Manager parent profile named TM1. TM1 has two child profiles named TM2 and TM3.

TM1 uses the performance traffic-routing method and has the endpoints shown in the following table.



## Private Endpoint connections

+ Add Refresh | ✓ Approve ✗ Reject 🗑 Remove



### Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network [Learn more](#)

Filter by name or description

All connection states

Connection name ↑↓ Connection state ↑↓ Private endpoint ↑↓ Description

No results.

TM2 uses the weighted traffic-routing method with MinChildEndpoint = 2 and has the endpoints shown in the following table.

#### Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input type="radio"/>

TM3 uses priority traffic-routing method and has the endpoints shown in the following table.

#### Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input checked="" type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input checked="" type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input checked="" type="radio"/>

The App2, App4, and App6 endpoints have a degraded monitoring status.

To which endpoint is traffic directed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:



### Answer Area

Routing type:

	▼
Policy-based	
Route-based	
Static routing	

Number of virtual network gateways:

	▼
1	
2	
3	

Correct Answer:

### Answer Area

Routing type:

	▼
Policy-based	
Route-based	
Static routing	

Number of virtual network gateways:

	▼
1	
2	
3	

Reference: <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles>

### QUESTION 4

You have an Azure subscription that contains the following resources:

A virtual network named Vnet1

A subnet named Subnet1 in Vnet1





A virtual machine named VM1 that connects to Subnet1

Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

To achieve the requirement, you create a network security group (NSG). You configure a service tag for Microsoft Storage and link the tag to Subnet1.

Did you achieve the requirement?

A. Yes

B. No

Correct Answer: B

This will either allow or deny traffic to all storage accounts from all virtual machines in Subnet1.

---

#### QUESTION 5

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines. Which Azure Network Watcher feature should you implement first?

A. Connection monitor

B. Packet capture

C. NSG flow logs

D. IP flow verify

Correct Answer: C

Network Watcher: A regional service that enables you to monitor and diagnose conditions at a network scenario level in Azure. You can turn NSG flow logs on and off with Network Watcher.

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

Why use NSG Flow Logs?

It is vital to monitor, manage, and know your own network for uncompromised security, compliance, and performance.

Common use cases include Network Monitoring: Identify unknown or undesired traffic. Monitor traffic levels and bandwidth consumption. Filter flow logs by IP and port to understand application behavior.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>