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.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 an Azure application gateway named AppGW1 that provides access to the following hosts: www.adatum.com

www.contoso.com www.fabrikam.com AppGW1 has the listeners shown in the following table.

Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

You create Azure Web Application Firewall (WAF) policies for AppGW1 as shown in the following table.

Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

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
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Correct Answer:

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Reference: https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/per-site-policies

QUESTION 2

Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address.

You create an Azure Front Door instance named FD1 that has Azure Web Application Firewall (WAF) enabled. You configure a WAF policy named Policy1 that has a rule named Rule1. Rule1 applies a rate limit of 100 requests for traffic that

originates from the office in Montreal.

You need to apply a rate limit of 100 requests for traffic that originates from each office.

What should you do?

A. Modify the rate limit threshold of Rule1.

B. Create two additional associations.

C. Modify the conditions of Rule1.

D. Modify the rule type of Rule1.

Correct Answer: C

QUESTION 3

Which virtual machines can VM4 ping successfully?

A. VM3 only

B. VM1 and VM3 only

C. VM1, VM2 and VM3 only

D. VM1, VM2, VM3 and VM5

Correct Answer: C

VM4 is in VNet3.

VNet3 is peered with VNet1 and VNet2.

There is no NSG rule blocking outbound ICMP from VNet3.

There are no NSG rule blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3.

NSG10 blocks inbound ICMP from VNet4 (Source IP address is 10.10.0.0/16).

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 the resources is shown in the following table.

Name	Type	Description
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
VM1	Virtual machine	Connected to Subnet1
azsql1	Azure SQL Database logical server	Has a private endpoint on Subnet2

You need to ensure that the apps hosted on VM1 can resolve the IP address of the What should you create first?

A. a public DNS zone named database.windows.net

B. a private DNS zone named database.windows.net

C. a public DNS zone named private link.database.windows.net

D. a private DNS zone named private link.database.windows.net

Correct Answer: D

Azure Private Endpoint DNS configuration

You can use the following options to configure your DNS settings for private endpoints:

*

Use the host file (only recommended for testing). You can use the host file on a virtual machine to override the DNS.

*

Use a private DNS zone. You can use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone can be linked to your virtual network to resolve specific domains.

*

Use your DNS forwarder (optional).

For Azure services, use the recommended zone names as described in the following table:

*

Azure SQL Database (Microsoft.Sql/servers) / sqlServer Private DNS zone name: privatelink.database.windows.net

*

Etc.

Reference: https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns

QUESTION 5

You are planning an Azure deployment that will contain three virtual networks in the East US Azure region as shown in the following table.

Name	Description
Vnet1	Hub virtual network for shared services
Vnet2	Virtual machines for the IT department
Vnet3	Virtual machines for the research department

A Site-to-Site VPN will connect Vnet1 to your company\\'s on-premises network.

You need to recommend a solution that ensures that the virtual machines on all the virtual networks can communicate with the on-premises network. The solution must minimize costs.

What should you recommend for Vnet2 and Vnet3?

A. VNet-to-VNet VPN connections

B. peering

C. service endpoints

D. route tables

Correct Answer: B

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft\\'s private network only.

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