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

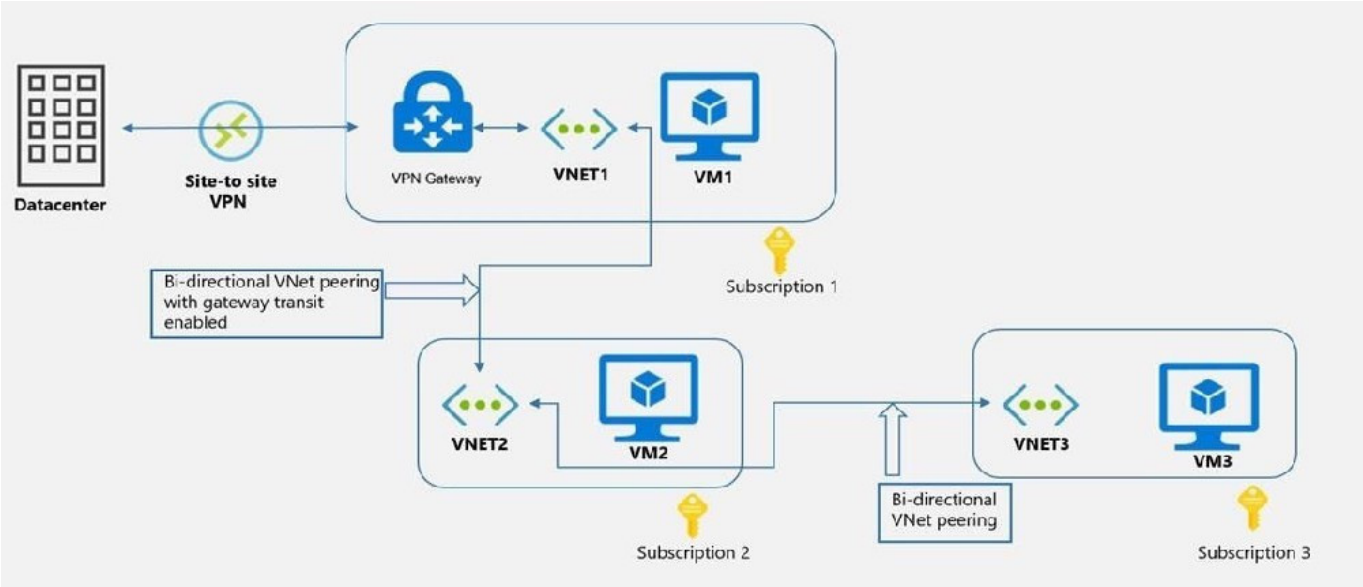
100% Passing Guarantee
100% Money Back Assurance

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

You have an Azure environment as shown below.



You need to find to which environments/virtual machines that VM2 can communicate?

A. VM1 Only

B. VM1 and VM3 Only

C. The on-premise datacenter and VM1 only

D. The on-premise datacenter, VM1 and VM3 only

Correct Answer: D

VM2 is in VNET2. VNET2 is peered with VNET1. So, VM2 can connect to VM1.

VM2 is in VNET2. VNET2 is peered with VNET1 with gateway transit enabled. So, VM2 can connect to on-premises datacenter.

VM2 is in VNET2. VNET2 is peered with VNET3. So, VM2 can connect to VM3.

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

QUESTION 2

You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN. Users will authenticate by using an on-premises Active Directory domain. Which additional service should you deploy to support the VPN authentication?

A. an Azure key vault

B. a RADIUS server

C. a certification authority

D. Azure Active Directory (Azure AD) Application Proxy

Correct Answer: B

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

QUESTION 3

HOTSPOT

Your company has an Azure virtual network named Vnet1 that uses an IP address space of 192.168.0.0/20. Vnet1 contains a subnet named Subnet1 that uses an IP address space of 192.168.0.0/24.

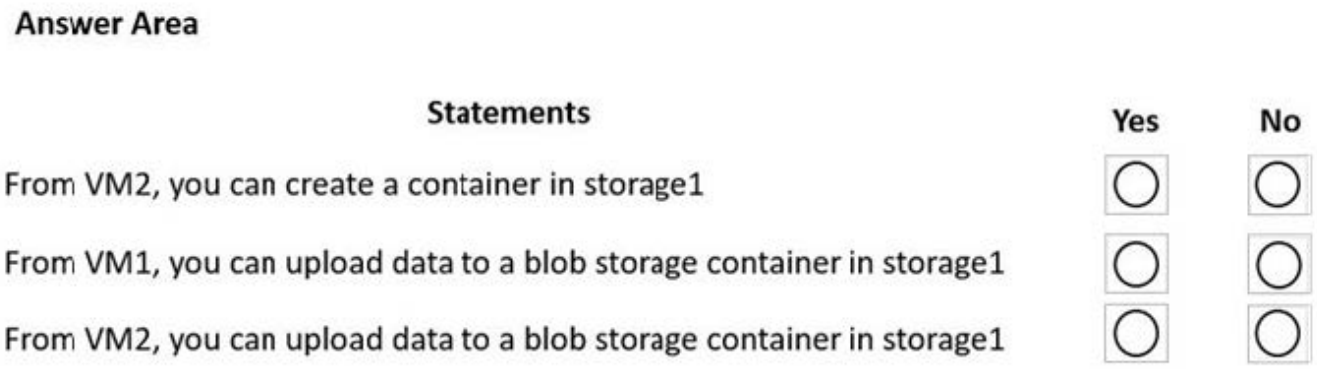
You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48.

You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company. The solution must minimize the number of additional IPv4 addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1	○	◉
From VM1, you can upload data to a blob storage container in storage1	◉	○
From VM2, you can upload data to a blob storage container in storage1	○	◉

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview

https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-add-to-existing-vnet-powershell

QUESTION 4

You plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.

You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application 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

Web Application Firewall Policies contain all the WAF settings and configurations. This includes exclusions, custom rules, managed rules, and so on. These policies are then associated to an application gateway (global), a listener (per-site),

or a path-based rule (per-URI) for them to take effect.

Part 1: Create a WAF policy

Create a basic WAF policy with a managed Default Rule Set (DRS) using the Azure portal.

Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

Step 2: On Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:

Policy for - Regional WAF (Application Gateway)

Subscription - Select your subscription name

Resource group - Select your resource group

Policy name - Type a unique name for your WAF policy.

Location: East US

Step 3: On the Association tab, select Add association, then select one of the following settings:

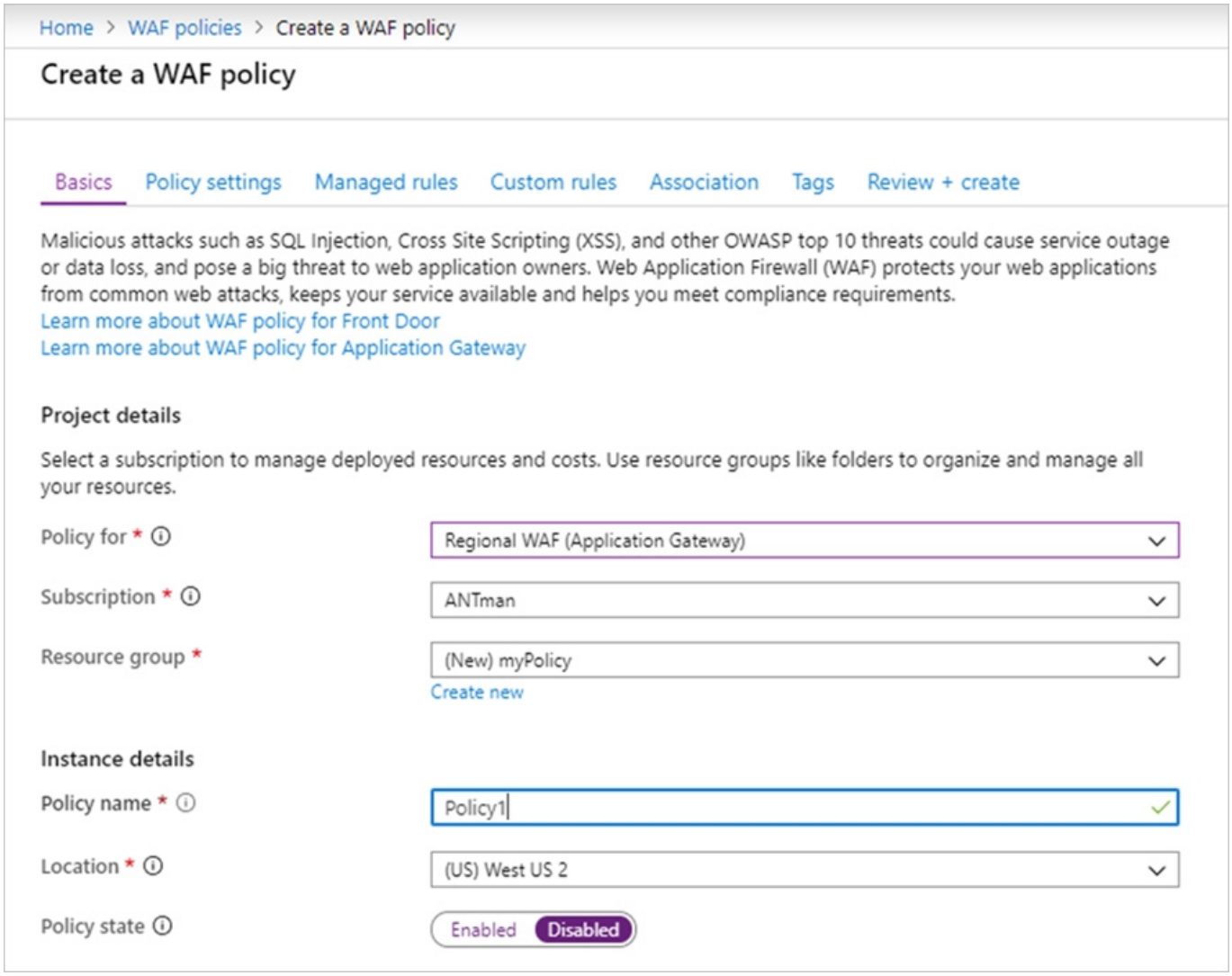
Setting - Value

Application Gateway- Select the application gateway, and then select Add.

HTTP Listener - Select the application gateway, select the listeners, then select Add.

Route Path - Select the application gateway, select the listener, select the routing rule, and then select Add.

Step 4: Select Review + create, then select Create.



Part 2: Configure WAF rule

When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn\\'t block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, you can change the mode settings to

Prevention. In Prevention mode, matching rules defined in the CRS Ruleset you selected are blocked and/or logged in the WAF logs.

Custom rules

Step 5: To create a custom rule, select Add custom rule under the Custom rules tab.

This opens the custom rule configuration page.

Step 6: On the Add custom rule page, use the following test values to create a custom rule:

Setting - Value

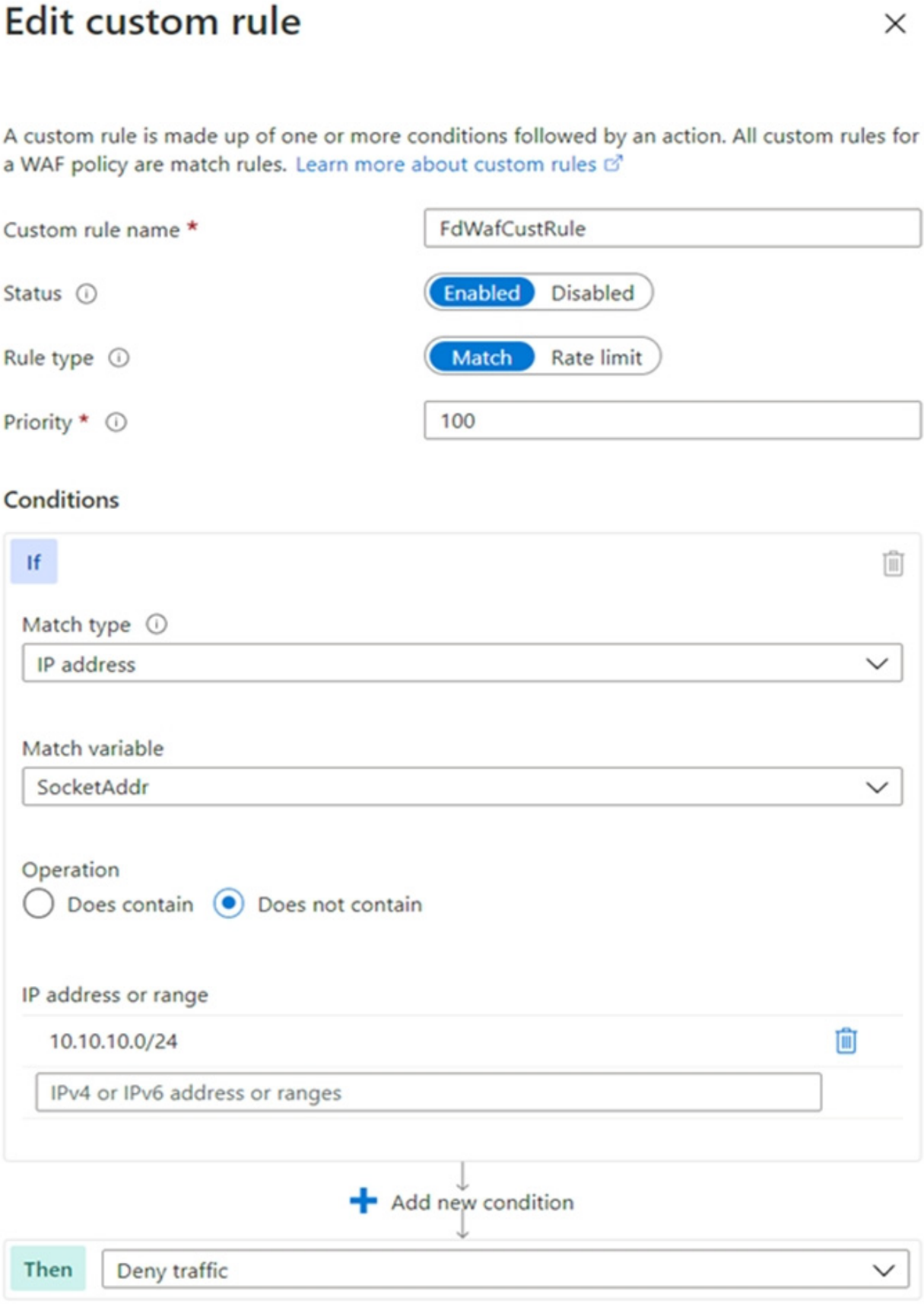
Custom rule name - AnyName

Status - Enabled

Rule type- Match

Priority - 100

Match type- IP address Match variable - SocketAddr (for example) Operation - Does contain IP address or range - 131.107.150.0/24 Then Deny traffic


Edit custom rule
A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules
Custom rule name *
FdWafCustRule
Status
Enabled
Disabled
Rule type
Match
Rate limit
Priority *
100
Conditions
If
Match type
IP address
Match variable
SocketAddr
Operation
Does contain
Does not contain
IP address or range
10.10.10.0/24
IPv4 or IPv6 address or ranges
Add new condition
Then
Deny traffic

Step 7: Select Add.

Step 8: Select Next: Association.

Step 9: Select Associate a WAF policy.

Step 10: For WAF policy, select your WAF policy.

Step 11: For Domain, select the domain.

Step 12. Select Add.

Step 13: Select Review + create.

Step 14: After your policy validation passes, select Create.

Reference:

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag

https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-configure-ip-restriction#configure-a-waf-policy-with-the-azure-portal

QUESTION 5

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.

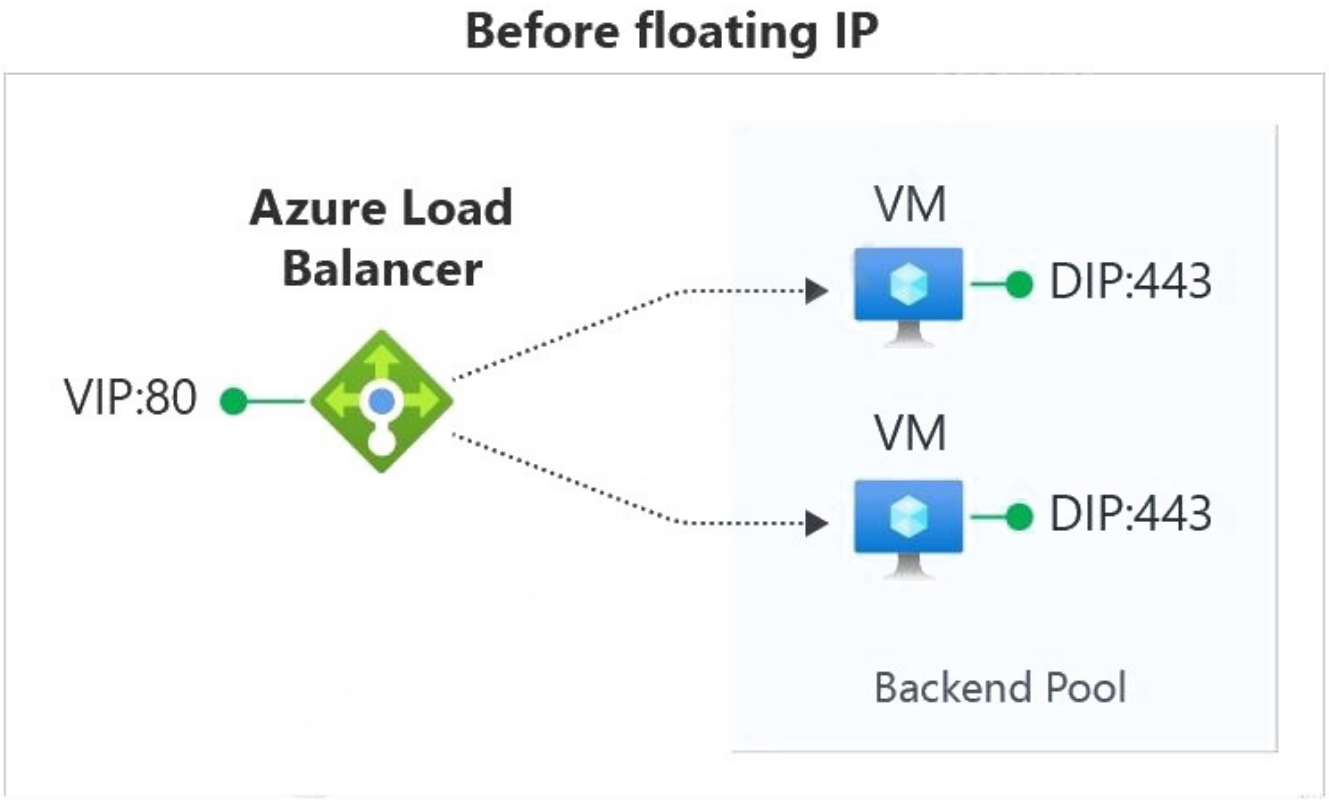
Correct Answer: A

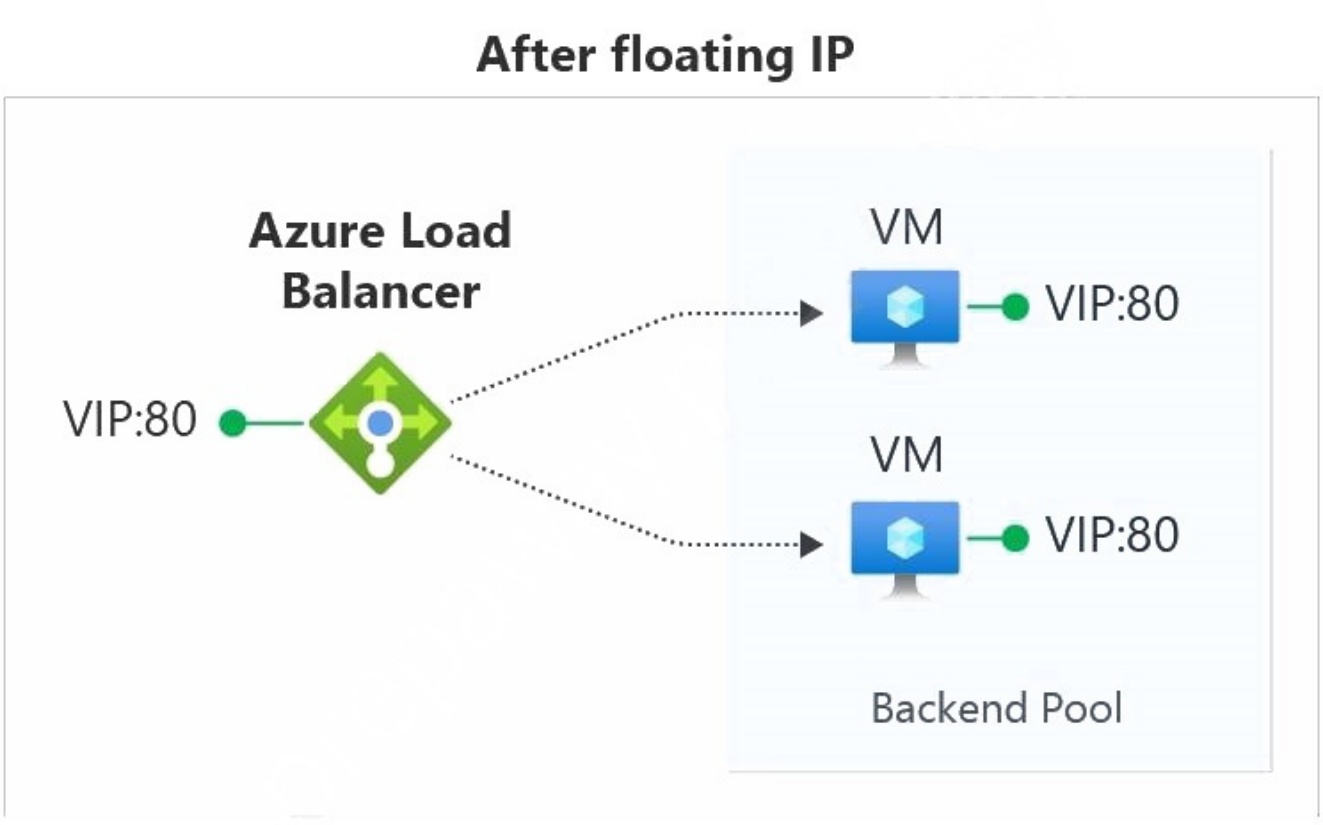
Azure Load Balancer Floating IP configuration Floating IP Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include:

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:





*

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