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 are planning the IP addressing for the subnets in Azure virtual networks. Which type of resource requires IP addresses in the subnets?

A. internal load balancers

B. storage account

C. service endpoints

D. service endpoint policies

Correct Answer: A

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

QUESTION 2

You need to ensure that hosts on VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

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

A. See explanation below.

B. Placeholder

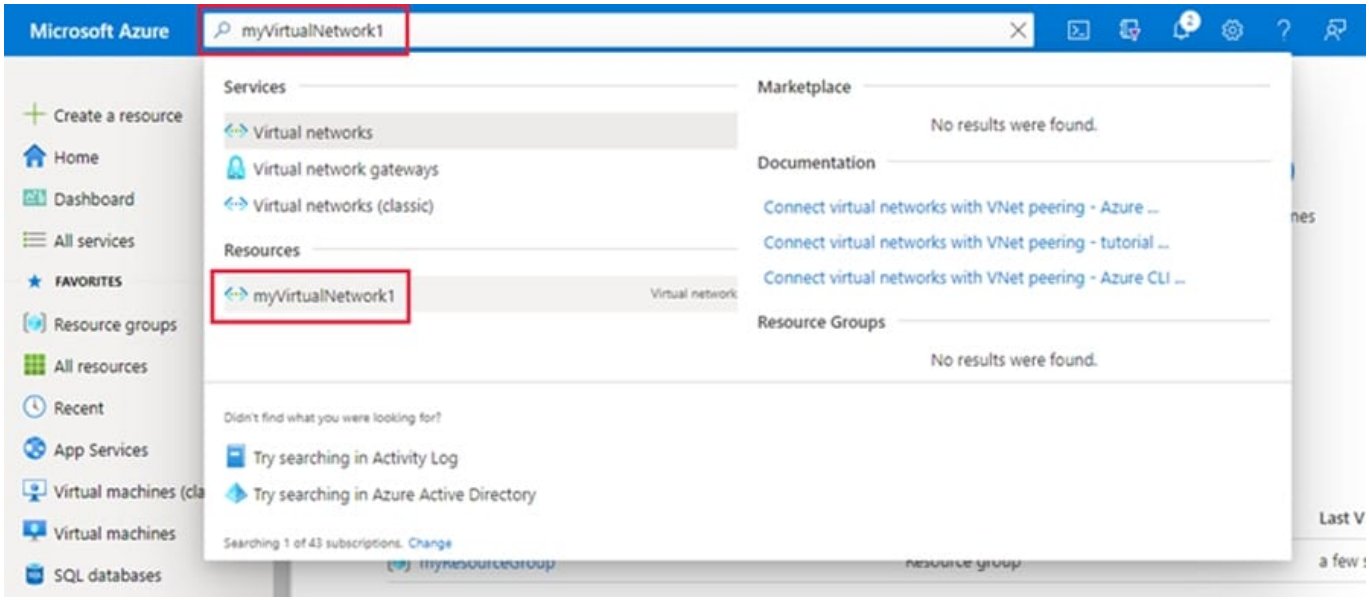
C. Placeholder

D. Placeholder

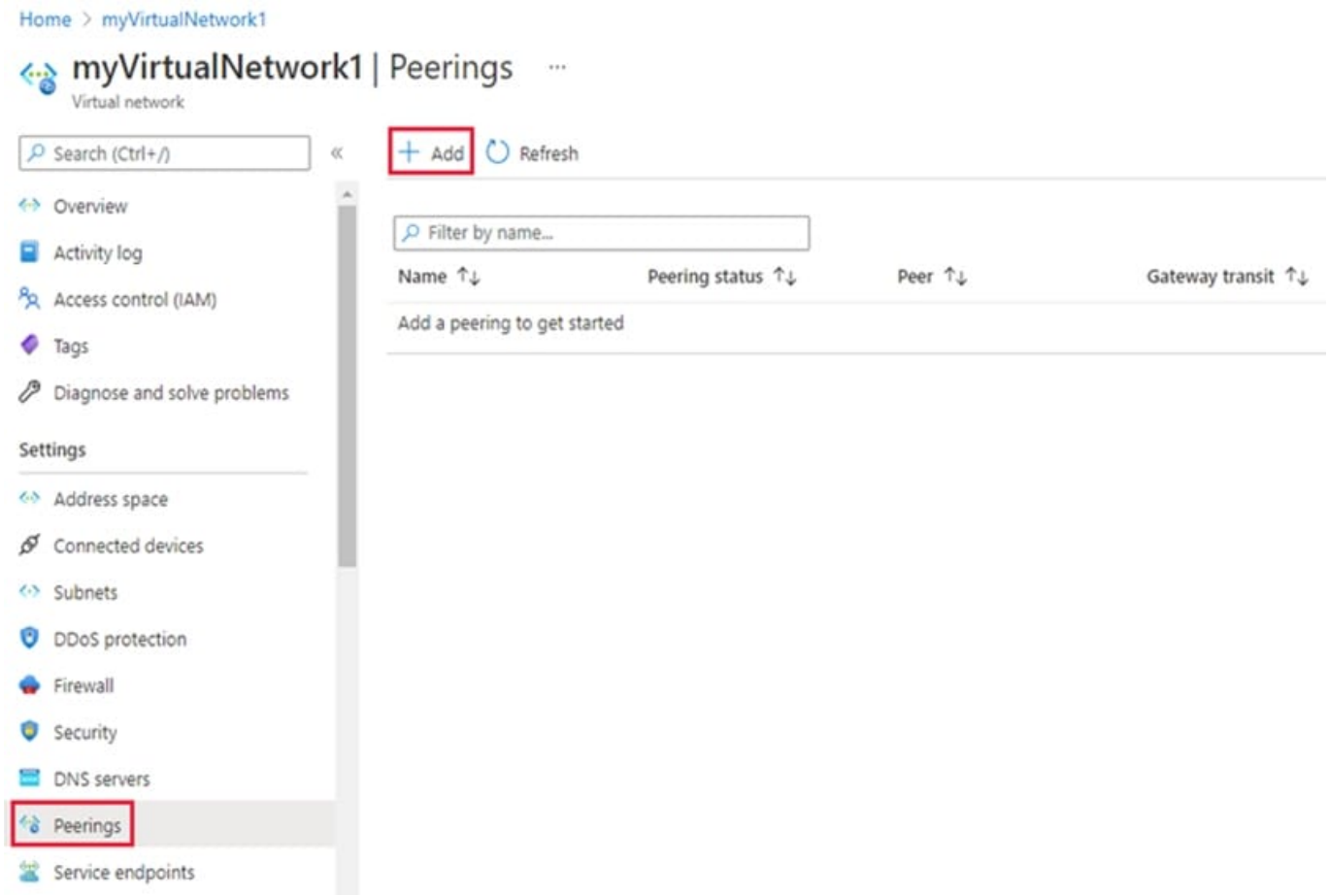
Correct Answer: A

Peer virtual networks

Step 1: In the search box at the top of the Azure portal, look for VNet1. When VNET1 appears in the search results, select it.



Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:



Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.

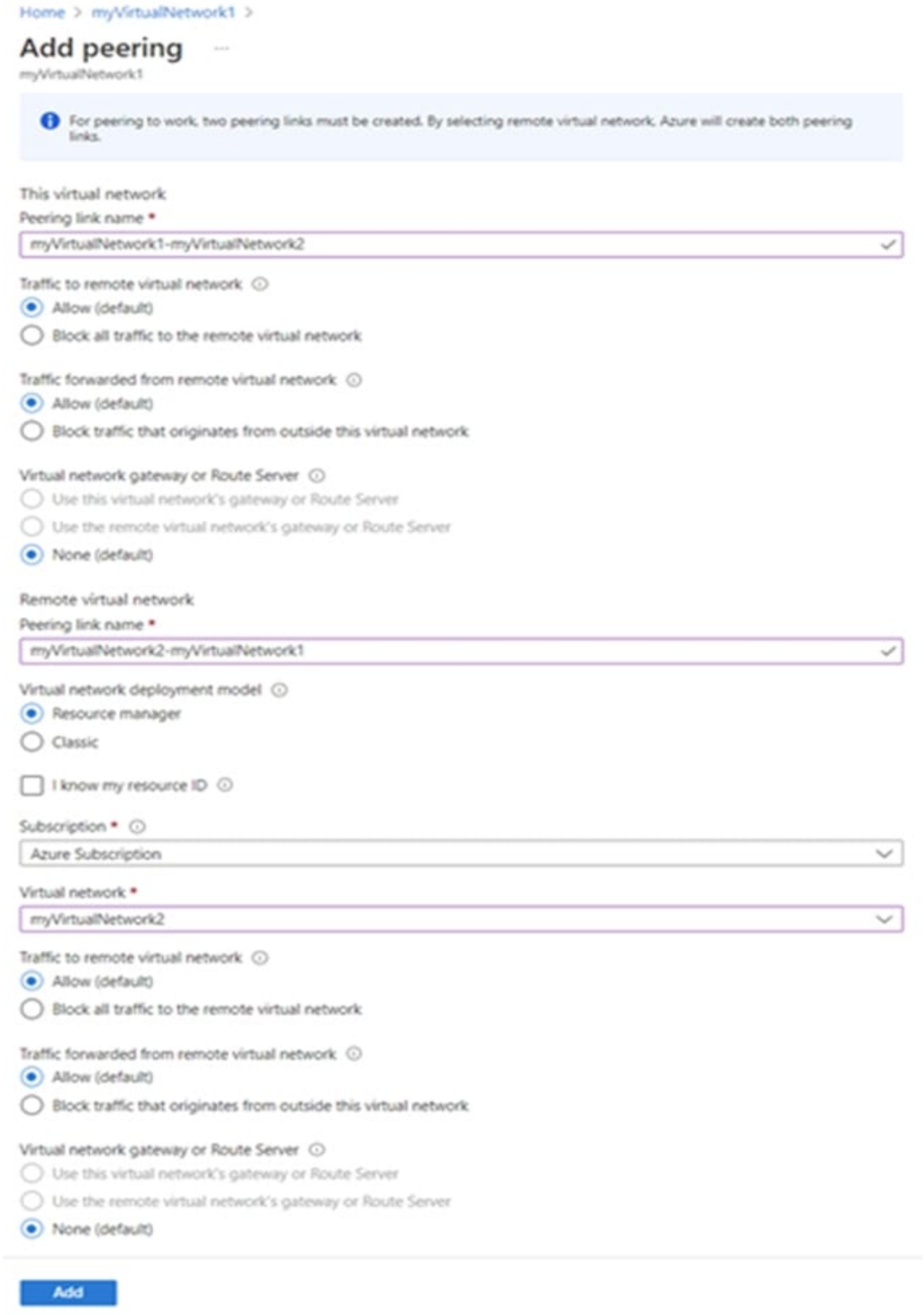
*

..

*

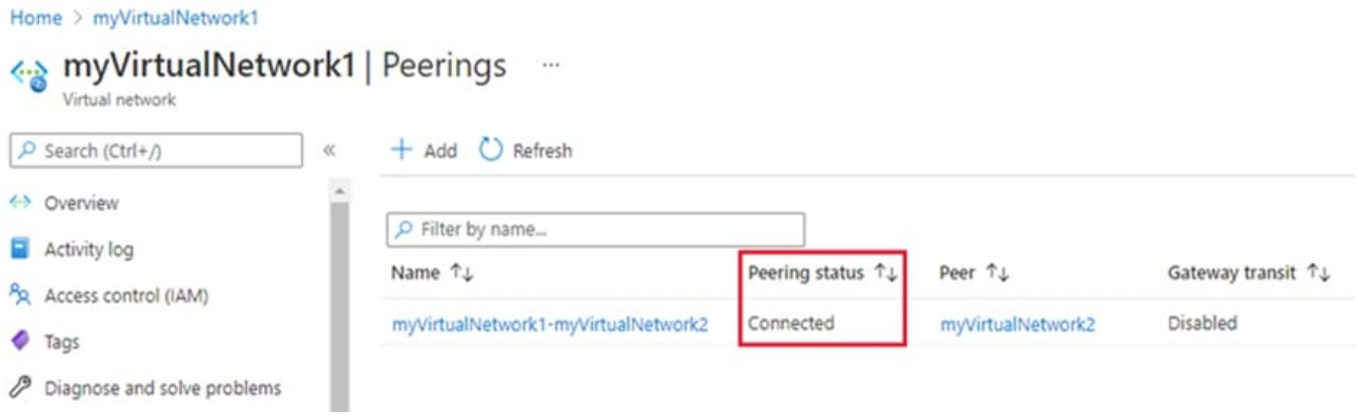
Virtual network

Select VNET2 for the name of the remote virtual network. The remote virtual network can be in the same region of VNET1 or in a different region.


Home > myVirtualNetwork1 >
Add peering
myVirtualNetwork1
For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.
This virtual network
Peering link name *
myVirtualNetwork1-myVirtualNetwork2
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network
Allow (default)
Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server
Use this virtual network's gateway or Route Server
Use the remote virtual network's gateway or Route Server
None (default)
Remote virtual network
Peering link name *
myVirtualNetwork2-myVirtualNetwork1
Virtual network deployment model
Resource manager
Classic
I know my resource ID
Subscription *
Azure Subscription
Virtual network *
myVirtualNetwork2
Traffic to remote virtual network
Allow (default)
Block all traffic to the remote virtual network
Traffic forwarded from remote virtual network
Allow (default)
Block traffic that originates from outside this virtual network
Virtual network gateway or Route Server
Use this virtual network's gateway or Route Server
Use the remote virtual network's gateway or Route Server
None (default)
Add

Step 4: Click Add

In the Peerings page, the Peering status is Connected, as shown in the following picture:



Reference: https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal

QUESTION 3

HOTSPOT

You have two Azure App Service instances that host the web apps shown the following table.

Name	Web app URLs
As1.contoso.com	https://app1.contoso.com/ https://app2.contoso.com/
As2.contoso.com	https://app3.contoso.com/ https://app4.contoso.com/

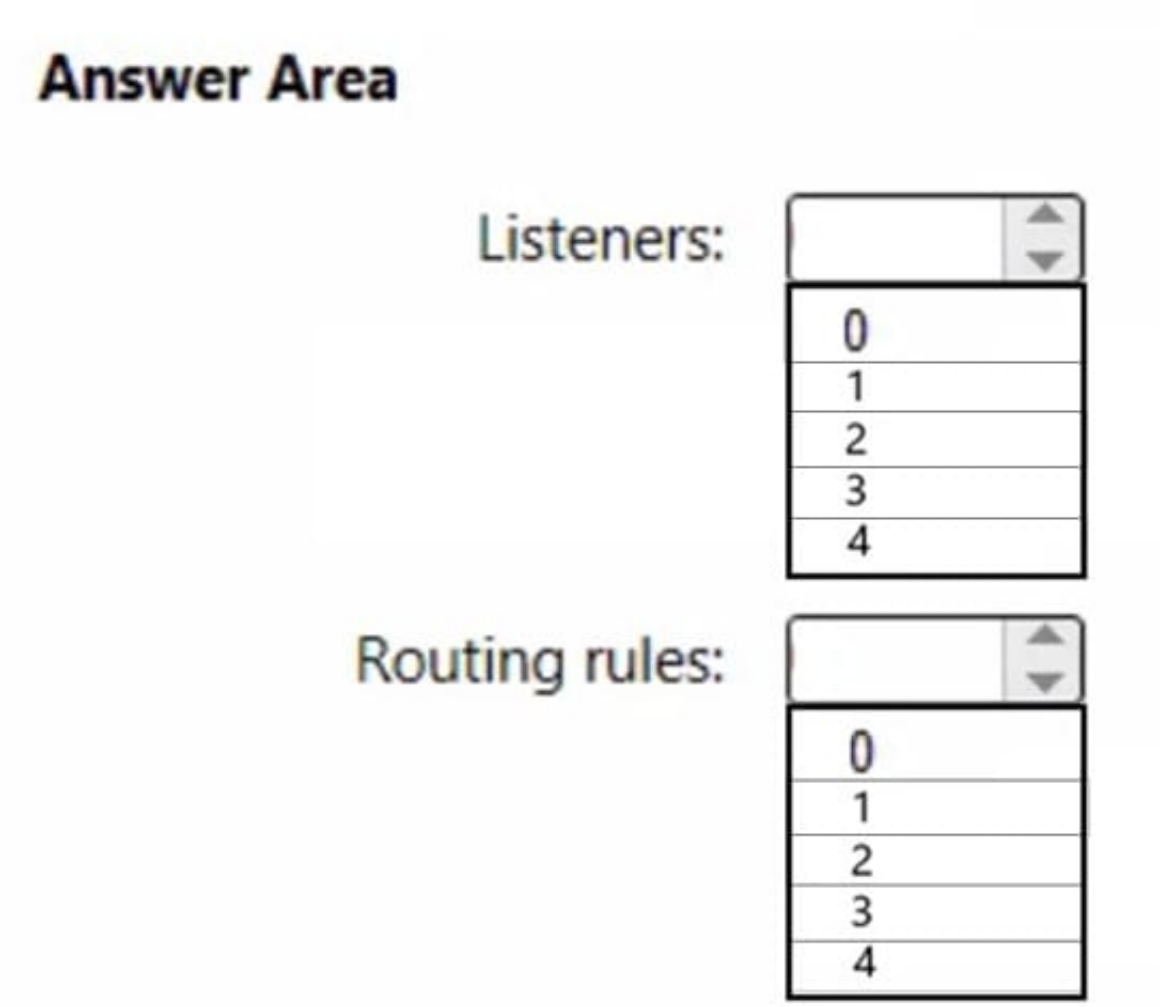
You deploy an Azure 2 that has one public frontend IP address and two backend pools.

You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.

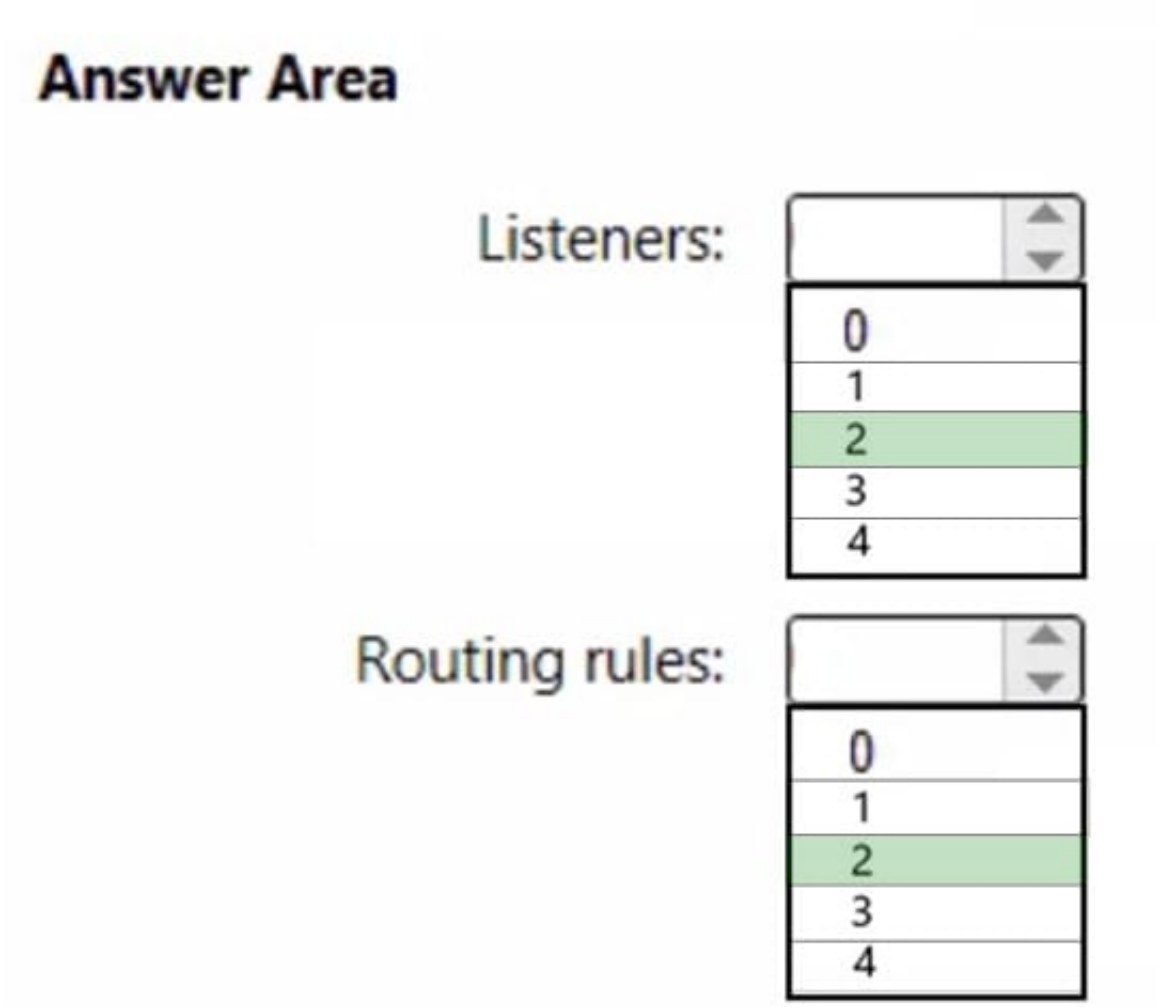
What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: 2 Listeners

One listener for As1.contoso.com, and one listener for As2.contoso.com.

Note: Multiple site hosting enables you to configure more than one web application on the same port of application gateways using public-facing listeners. It allows you to configure a more efficient topology for your deployments by adding up to 100+ websites to one application gateway. Each website can be directed to its own backend pool. For example, three domains, contoso.com, fabrikam.com, and adatum.com, point to the IP address of the application gateway. You\\'d create three multi-site listeners and configure each listener for the respective port and protocol setting.

You can also define wildcard host names in a multi-site listener and up to 5 host names per listener.

Box 2: 2 Routing rules

Application Gateway request routing rules Rule type When you create a rule, you choose between basic and path-based.

*

Choose basic if you want to forward all requests on the associated listener (for example, blog.contoso.com/*) to a single backend pool.

*

Choose path-based if you want to route requests from specific URL paths to specific backend pools. The path pattern is applied only to the path of the URL, not to its query parameters.

Associated backend pool

Associate to the rule the backend pool that contains the backend targets that serve requests that the listener receives.

*

For a basic rule, only one backend pool is allowed. All requests on the associated listener are forwarded to that backend pool.

*

For a path-based rule, add multiple backend pools that correspond to each URL path. The requests that match the URL path that\\'s entered are forwarded to the corresponding backend pool. Also, add a default backend pool. Requests that

don\\'t match any URL path in the rule are forwarded to that pool.

Reference: https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview

QUESTION 4

You have the Azure resources shown in the following table.

Name	Type	Location	Description
storage1	Storage account	East US	Read-access geo-redundant storage (RA-GRS)
Vnet1	Virtual network	East US	Contains one subnet

You configure storage1 to provide access to the subnet in Vnet1 by using a service endpoint.

You need to ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region.

What should you do first?

A. Configure the firewall settings for storage1.

B. Fail over storage1 to the paired Azure region.

C. Create a virtual network in the paired Azure region.

D. Create another service endpoint.

Correct Answer: C

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts. https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

QUESTION 5

You need to ensure that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

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

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway

specifies which static IP addresses virtual machines use when creating outbound flows.

Plan:

Stage 1: Create a NAT gateway

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Stage 1: 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:

* NAT gateway name: Enter myNATgateway

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.

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. Here choose subnet3-2 connect.

Step 5: In the subnet page, change the NAT Gateway to myNATgateway (the one we created in Stage 1).

Step 6: Select Save.

Reference:

https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/quickstart-create-nat-gateway-portal

QUESTION 6

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

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region. To which virtual networks can you deploy AF1?

A. Vnet1 and Vnet4 only

B. Vnet1, Vnet2, Vnet3, and Vnet4

C. Vnet1 only

D. Vnet1 and Vnet2 only

E. Vnet1, Vnet2, and Vnet4 only

Correct Answer: C

Azure Firewall operates in a single VNET.

Azure Firewall is a regional service.

Yes. Vnet1: Same VNET and same region.

No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.

No. Vnet3: Different VNET, different region. Must be in the same region.

No. Vnet4: Different VNET, same region.

Reference:

https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall

QUESTION 7

Your on-premises network contains an SMB share named Share1. You have an Azure subscription that contains the following resources:

A web app named webapp1

A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1.

What should you deploy?

A. an Azure Application Gateway

B. an Azure Active Directory (Azure AD) Application Proxy

C. an Azure Virtual Network Gateway

Correct Answer: C

Correct Answer(s):

an Azure Virtual Network Gateway - A Site-to-Site VPN gateway connection can be used to connect your on- premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a

VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

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

Wrong Answers:

an Azure Application Gateway -- Azure Application Gateway is a web traffic load balancer. It does not provide connectivity to on-premises resources.

an Azure Active Directory (Azure AD) Application Proxy -- Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications. It does not provide connectivity to on-premises file shares.

QUESTION 8

You have the on-premises networks shown in the following table.

Name	ASN	IP address space	Connection type	Description
Branch1	64551	10.50.0.0/24,10.61.0.0/16	VPN	Is an on-premises datacenter
Branch2	64551	10.50.0.0/16,10.61.0.0/16	VPN and ExpressRoute	AS Path has a prefix of 64551,64551,64551
Branch3	64551	10.50.2.0/24,10.61.0.0/16	ExpressRoute	*None*

You have an Azure subscription that contains an Azure virtual WAN named VWAN1 and a virtual network named VNet1. VWAN is connected to the on-premises networks and VNet1 in a full mesh topology. The virtual hub routing preference

for VWAN1 is AS Path.

You need to route traffic from VNet1 to 10.61.1.5.

Which path will be used?

A. the VPN connection to Branch1

B. the VPN connection to Branch2

C. the ExpressRoute connection to Branch2

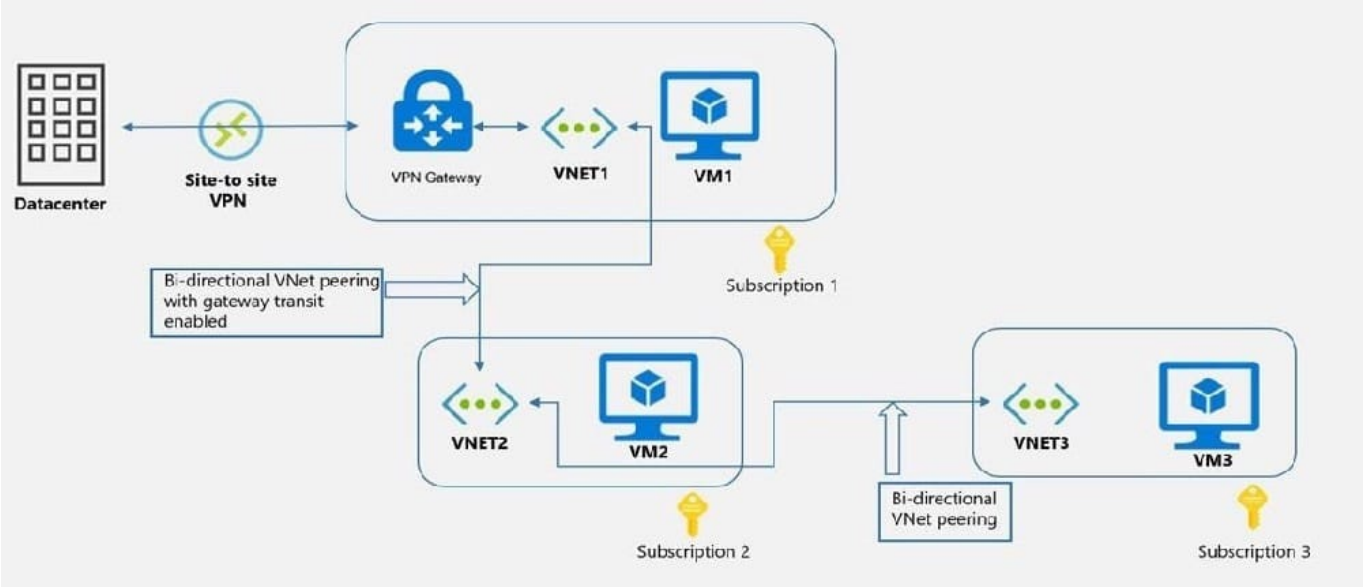
D. the ExpressRoute connection to Branch3

Correct Answer: D

1- VWAN prefers ER over VPN2- it doesn\\'t have BGP prepend .. Branch 2 has three AS hops so it is less preferred

QUESTION 9

You have an Azure environment as shown below.



You need to find to which environments/virtual machines that VM1 can communicate?

A. VM2 Only

B. VM2 and VM3 Only

C. The on-premise datacenter and VM2 only

D. The on-premise datacenter, VM2 and VM3 only

Correct Answer: C

VM1 is in VNET1. VNET1 has a Site-to-Site VPN connection with on-premise data center. So, VM1 can communicate with on-premise datacenter.

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

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

---

QUESTION 10

You need to ensure that the storage12345678 storage account will only accept connections from the hosts on VNET1.

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

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

Azure storage account accepts connections from Virtual network. Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet. Link the private endpoint to the existing storage account

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Select or Searchandfind storage account storage12345678

Step 3: Select the Networking tab or select Next: Advanced then Next: Networking.

Step 4: In the Networking tab, under Network connectivity select Disable public access and use private access.

Step 5: In Private endpoint, select + Add private endpoint.

Step 6: In the Basics tab of Create a private endpoint, enter or select basic information for the endpoint.

Step 7: Select Next: Resource.

Step 8: In the Resource pane, enter or select basic information for the resource.

Step 9: Select Next: Virtual Network.

Step 10: In Virtual Network, enter or select:

* Virtual network: VNET1.

Step 11: Select Next: DNS.

Step 12: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

Step 13: Select Create.

Back in the setting of settings of the Storage Account.

Step 14: Save.

Reference: https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal
https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal

---

QUESTION 11

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:

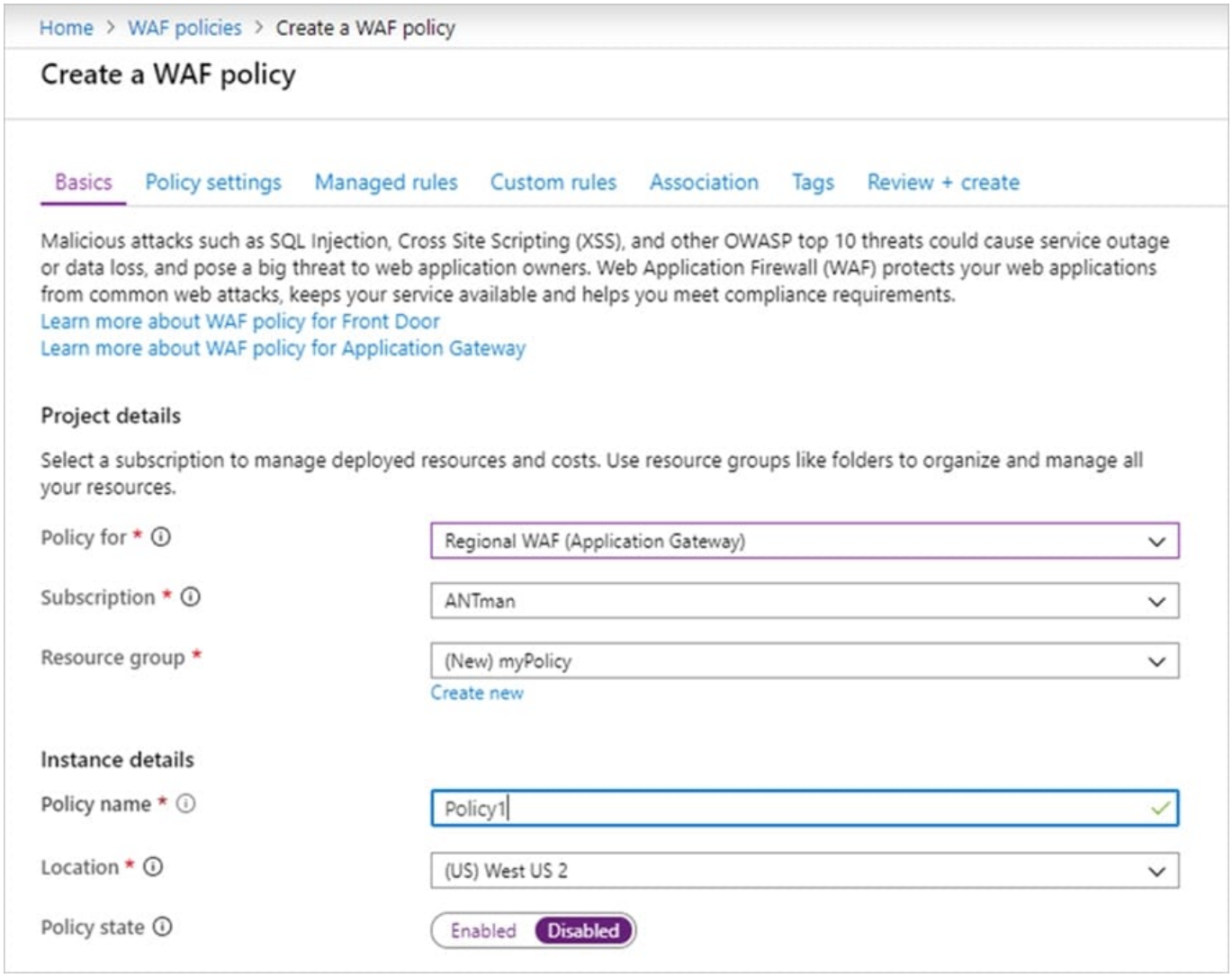
Setting - Value

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

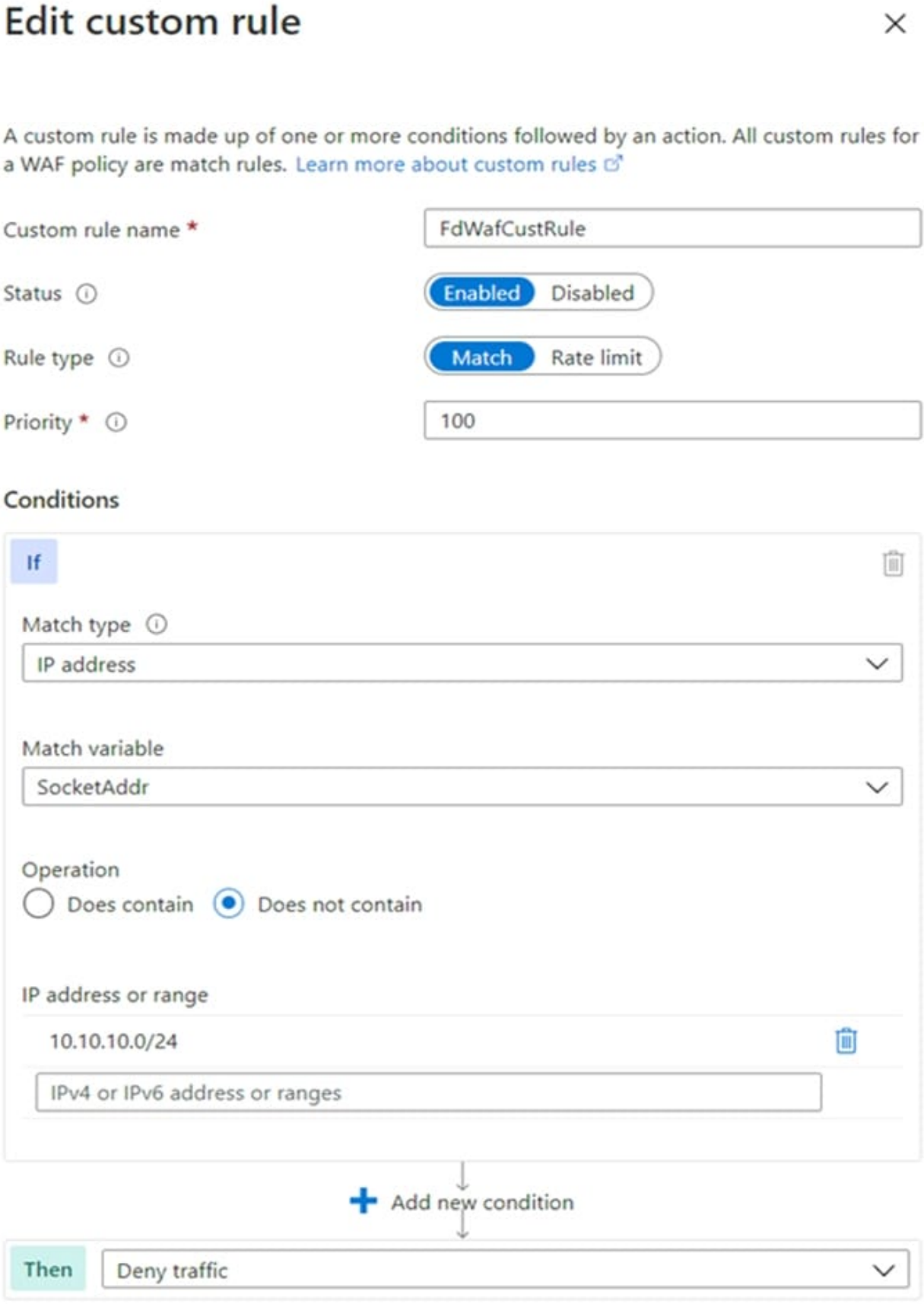
Match type- IP address

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:

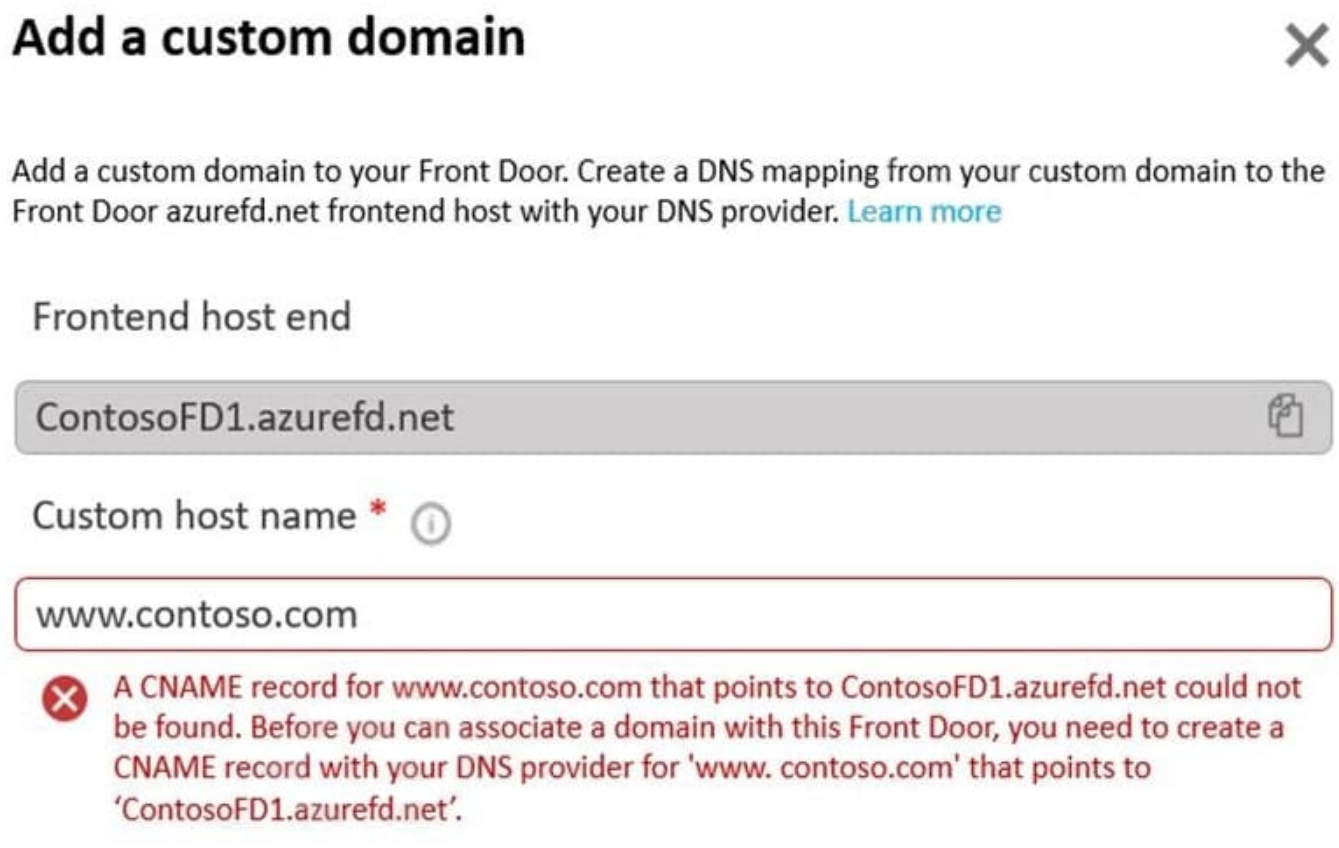
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag

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 12

You have a website that uses an FQDN of www.contoso.com. The DNS record for www. contoso.com resolves to an on-premises web server.



You plan to migrate the website to an Azure web app named Web1. The website on Web1 will be published by using an Azure Front Door instance named ContosoFD1.

You build the website on Web1.

You plan to configure ContosoFD1 to publish the website for testing.

When you attempt to configure a custom domain for www.contoso.com on ContosoFD1, you receive the error message shown in the exhibit. (Click the Exhibit tab.)

You need to test the website and ContosoFD1 without affecting user access to the on-premises web server.

Which record should you create in the contoso.com DNS domain?

You have a website that uses an FQDN of www.

A. a CNAME record that maps afdverify.www.contoso.com to ContosoFD1.azurefd.net

B. a CNAME record that maps www.contoso.com to ContosoFD1.azurefd.net

C. a CNAME record that maps afdverify.www.contoso.com to afdverify.ContosoFD1.azurefd.net

D. a CNAME record that maps www.contoso.com to Web1.contoso.com

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary-afdverify-subdomain

QUESTION 13

You have an application named App1 that listens for incoming requests on a preconfigured group of 50 TCP ports and UDP ports.

You install App1 on 10 Azure virtual machines.

You need to implement load balancing for App1 across all the virtual machines. The solution must minimize the number of load balancing rules.

What should you include in the solution?

A. Azure Application Gateway V2 that has multiple listeners

B. Azure Standard Load Balancer that has Floating IP enabled

C. Azure Standard Load Balancer that has high availability (HA) ports enabled

D. Azure Application Gateway v2 that has multiple site hosting enabled

Correct Answer: C

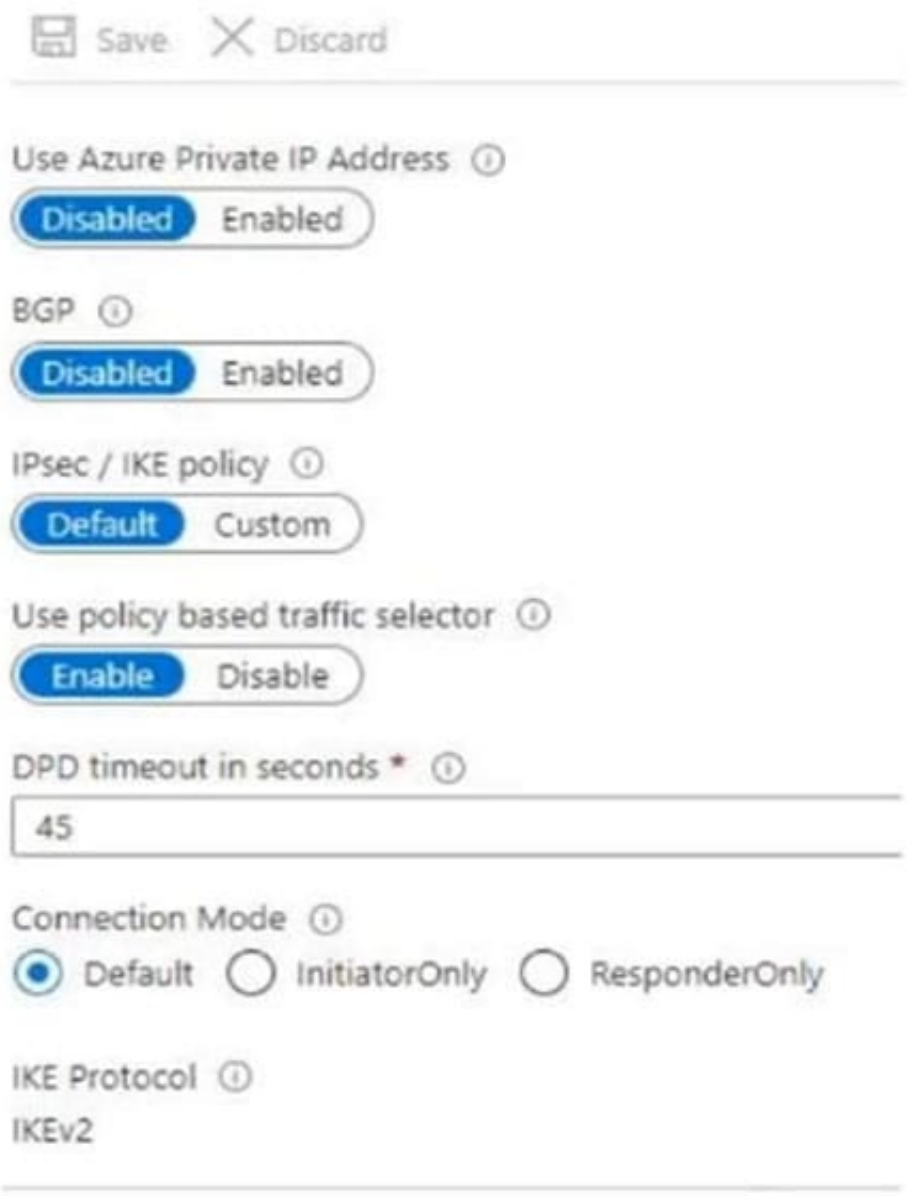
C. Azure Standard Load Balancer that has high availability (HA) ports enabled App1 is installed on 10 VMs which can be put in a Backend pool. The req is to minimize the number of load balancing rules. If you select HA it will allow you to have 1 rule for TCP and UDP ports, if you don\\'t select HA you will need to have a minimum of 2 rules for TCP and UDP with a * range.

QUESTION 14

You have an Azure virtual network named Vnet1 and an on-premises network.

The on-premises network has policy-based VPN devices. In Vnet1, you deploy a virtual network gateway named GW1 that uses a SKU of VpnGw1 and is route-based.

You have a Site-to-Site VPN connection for GW1 as shown in the following exhibit.



You need to ensure that the on-premises network can connect to the route-based GW1. What should you do before you create the connection?

A. Set Connection Mode to ResponderOnly.

B. Set BGP to Enabled.

C. Set Use Azure Private IP Address to Enabled.

D. Set IPsec / IKE policy to Custom.

Correct Answer: D

BGP is the standard routing protocol commonly used in the Internet to exchange routing and reachability information between two or more networks. BGP enables the Azure VPN Gateways and your on-premises VPN devices, called BGP

peers or neighbors, to exchange "routes" that will inform both gateways on the availability and reachability for those

prefixes to go through the gateways or routers involved. BGP can also enable transit routing among multiple networks by

propagating routes a BGP gateway learns from one BGP peer to all other BGP peers.

Incorrect:

Not C: A VPN gateway must have a Public IP address. Verify that you have an externally facing public IPv4 address for your VPN device.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-cli

QUESTION 15

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:

1.

A virtual network named Vnet1

2.

A subnet named Subnet1 in Vnet1

3.

A virtual machine named VM1 that connects to Subnet1

4.

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.

Solution: You create a network security group (NSG). You configure a service tag for Microsoft.Storage and link the tag to Subnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

AZ-700 PDF Dumps AZ-700 Practice Test AZ-700 Braindumps