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.pass4itsure.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 need to ensure that you can deploy Azure virtual machines to the France Central Azure region. The solution must ensure that virtual machines in the France Centralregion are in a network segment that has an IP address range of 10.5.1.0/24.

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

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

You can create a virtual network before you create a virtual machine or you can create the virtual network as you create a virtual machine.

You create these resources to support communication with a virtual machine:

Network interfaces

IP addresses

Virtual network and subnets

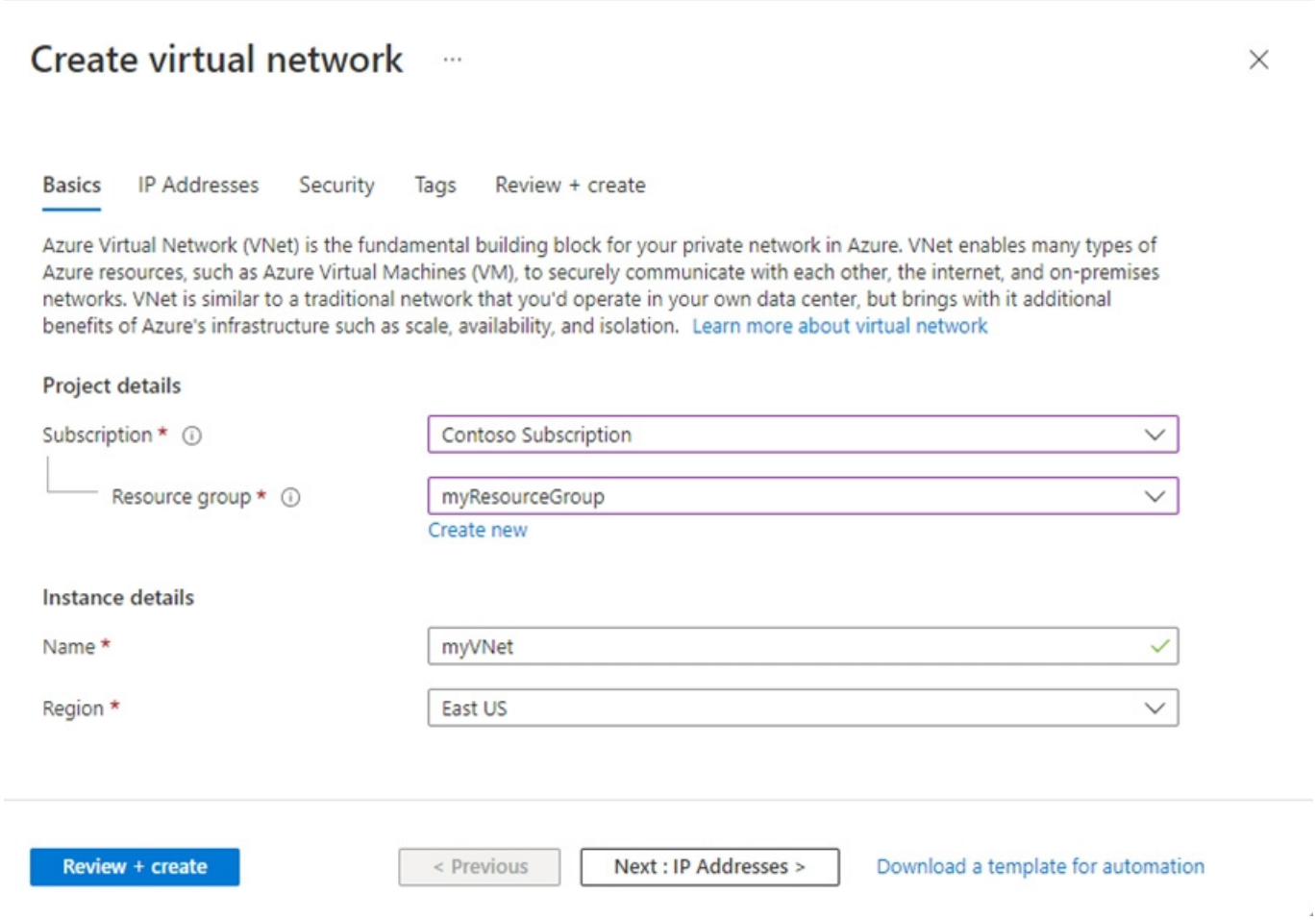
Create a virtual network

Step 1: Select Create a resource in the upper left-hand corner of the portal.

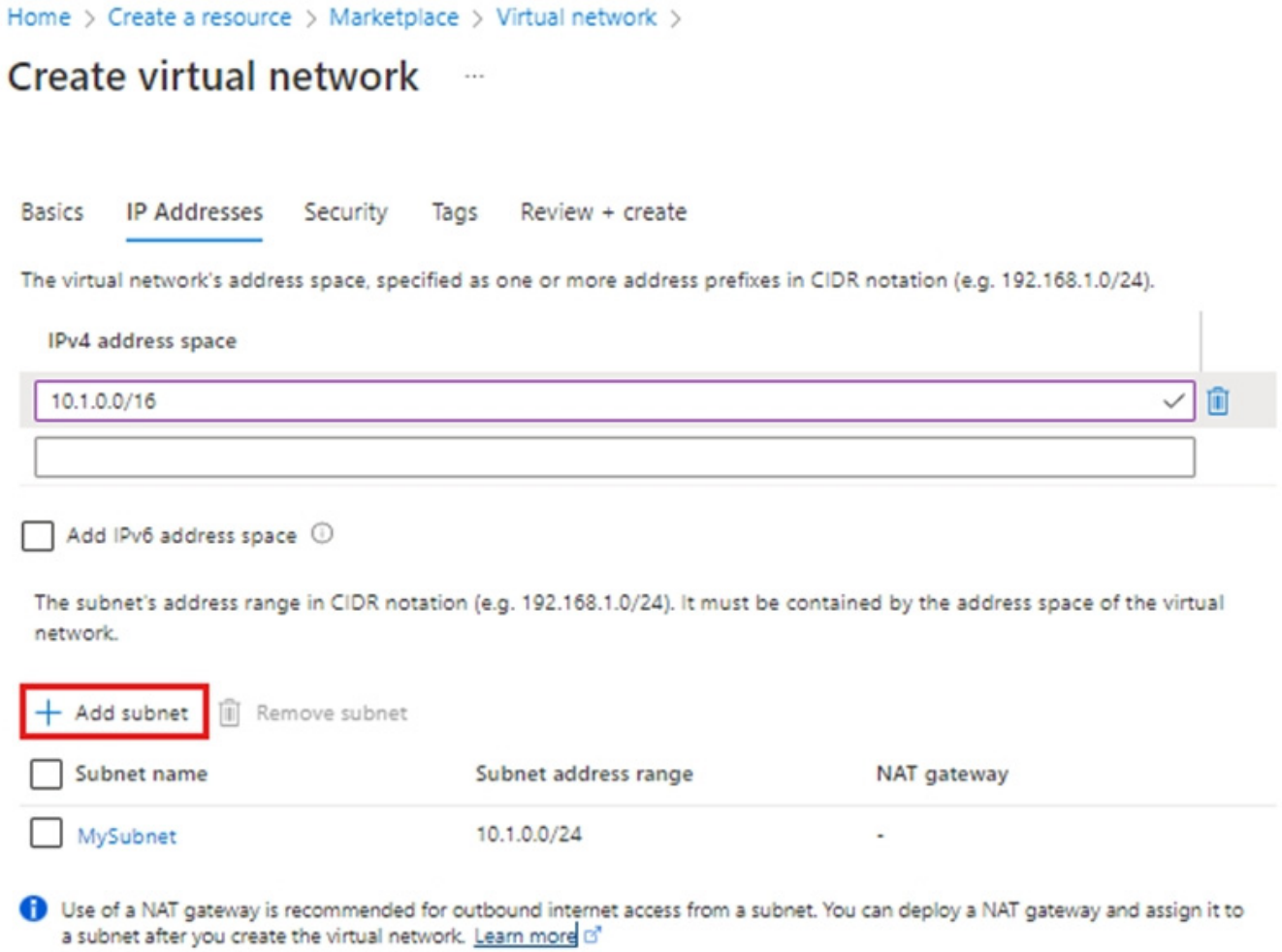
Step 2: In the search box, enter Virtual Network. Select Virtual Network in the search results.

Step 3: In the Virtual Network page, select Create.

Step 4: In Create virtual network, enter or select this information in the Basics tab:



Step 5: Enter Region: France Central



Step 6: Select the IP Addresses tab, or select the Next: IP Addresses button at the bottom of the page and enter in the following information then select Add:

Step 7: For IPv4 address space enter: 10.5.1.0/16

Step 8: Click Add subnet

Step 9: For Subnet address range Enter 10.5.1.0/24.

Step 10: Finish the wizard.

Reference: https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal

QUESTION 2

HOTSPOT

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	East US
RG2	UK West

You have the virtual networks shown in the following table.

Name	Location	Subnet	Resource group
Vnet1	East US	Sb1	RG1
Vnet1	East US	Sb2	RG1
Vnet2	West US	Sb3	RG2
Vnet2	West US	Sb4	RG2

Vnet1 contains two virtual machines named VM1 and VM2. Vnet2 contains two virtual machines named VM3 and VM4.
You have the network security groups (NSGs) shown in the following table that include only default rules.

Name	Associated to
Nsg1	Sb1
Nsg2	Network interface of VM2
Nsg3	Network interface of VM3
Nsg4	Sb4

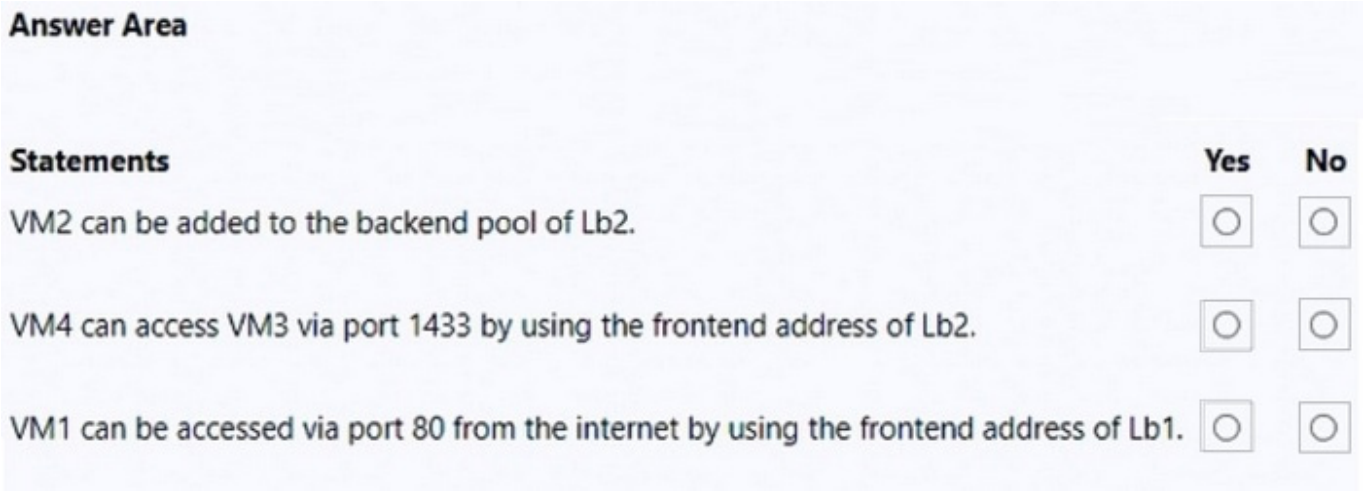
You have the Azure load balancers shown in the following table.

Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnet1	VM1	Protocol: TCP Port: 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port: 1433 Backend port: 1433

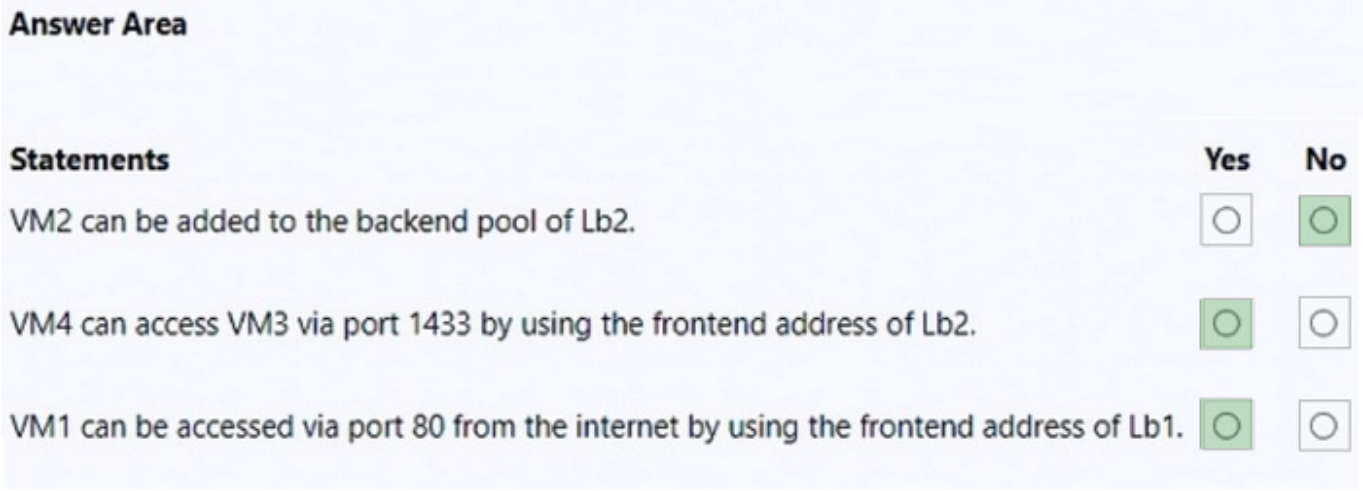
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: No

VM2 is in Vnet1.

Vnet1 is located in East US.

Vnet1 has the two subnets Sb1 and Sb2, both in RG1.

Lb2 is in West US and has the Backend pool in Vnet2.

Note: The backend resources must be in the same virtual network as the load balancer for IP based LBs

Box 2: Yes

VM4 and VM3 are both in Vnet2.

Lb2 is also in Vnet2. Lb2 is an internal load balancer. VM3 is in the backend pool of Lb2. Rule is TCP port 1433, backend port 1433.

Note: Public Load Balancers are used to load balance internet traffic to your VMs. An internal (or private) load balancer is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a

virtual network.

Box 3: Yes

VM1 is in the backend pool of Lb1. Lb1 is a public load balancer.

Rule is TCP port 80, backend port 80.

Note: A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load

Balancers are used to load balance internet traffic to your VMs.

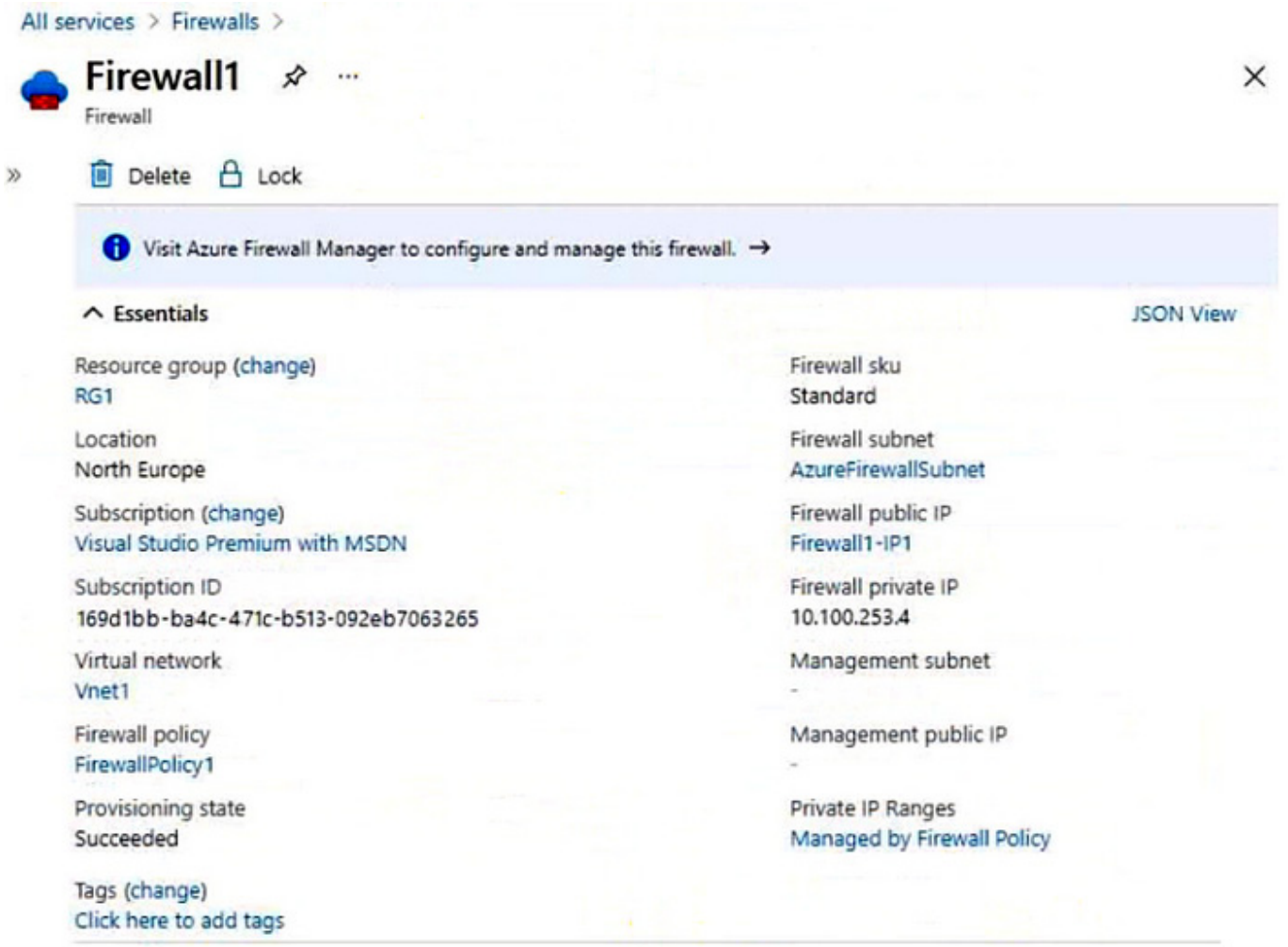
Reference: https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management

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

QUESTION 3

HOTSPOT

You have the Azure firewall shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On Firewall1, forced tunneling **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

On Firewall1, management by Azure Firewall Management **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

Correct Answer:

Answer Area

On Firewall1, forced tunneling **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

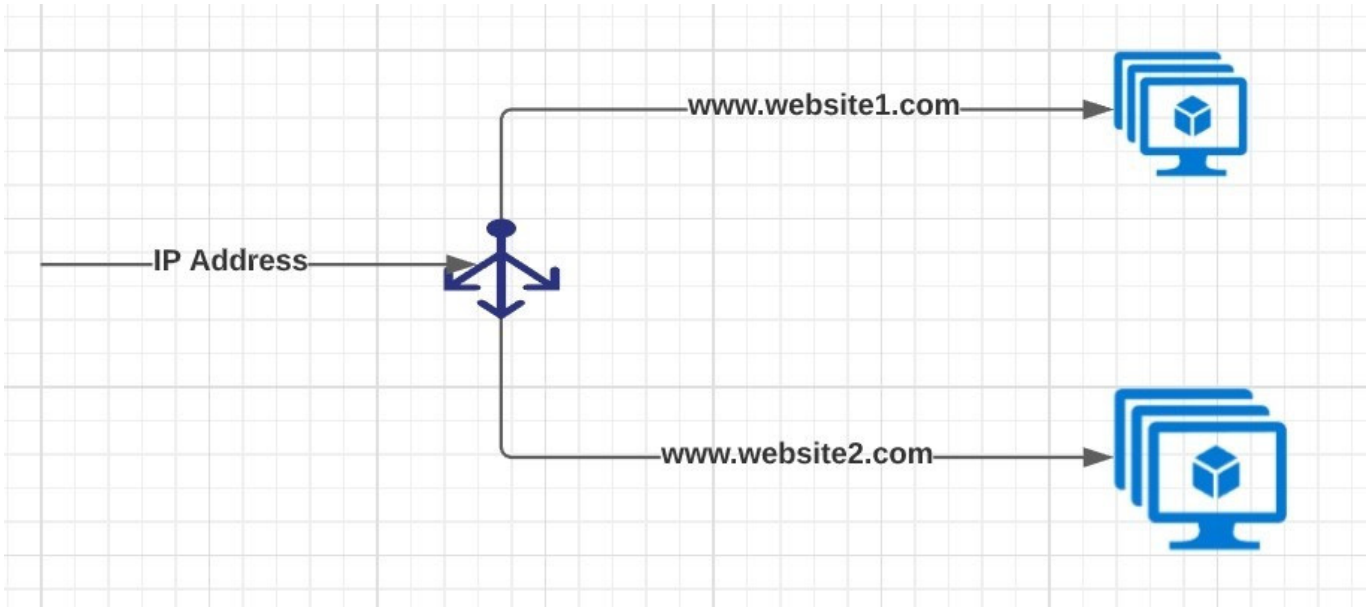
On Firewall1, management by Azure Firewall Management **[answer choice]**.

- is enabled already
- cannot be enabled
- is disabled but can be enabled

QUESTION 4

You have deployed multiple websites in Internet Information Server (IIS) by using Azure virtual machine scale sets (VMSS).

User sessions must be routed to the same server by using cookie-based session affinity. The below image depicts the network traffic flow for the websites to the VMSS.



What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

A. Routing rules and backend listeners

B. CNAME and A records

C. Routing method and DNS time to live (TTL)

D. Path-based redirection and websockets

Correct Answer: A

Correct Answer(s):

Routing rules and backend listeners - You can configure the hosting of multiple web sites when you create an application gateway. You need to define backend address pools using virtual machines. You then configure listeners and rules

based on domains that you own to make sure web traffic arrives at the appropriate servers in

the pools.

https://docs.microsoft.com/bs-latn-ba/azure//application-gateway/create-multiple-sites-portal

Wrong Answers:

CNAME and A records - These are used for domain registrations.

Routing method and DNS time to live (TTL) - DNS TTL (time to live) is a setting that tells the DNS resolver how long to cache a query before requesting a new one. This is nothing to do with routing.

Path-based redirection and websockets - Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request.

QUESTION 5

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to create a new Azure subscription and deploy 25 virtual machines.

The requirements are as follows:

All Azure virtual machines must be placed on the same subnet named Subnet1.

All the Azure virtual machines must be able to communicate with all on-premises servers.

The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

What should you include in the recommendation for Subnet1 and Gateway subnet IP address space?

A. 172.16.0.0/16 and 172.16.1.0/28

B. 172.16.0.0/16 and 192.168.0.0/24

C. 172.16.1.0/28 and 192.168.0.0/24

D. 192.168.0.0/24 and 172.16.1.0/28

E. 192.168.0.0/24 and 192.168.1.0/28

Correct Answer: E

We cannot use these IP address spaces - 172.16.0.0/16 and 172.16.1.0/28 in Azure as these overlap with on- premises IP address space. The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part

of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require

more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

So, the subnet1 IP address space must be 192.168.0.0/24 and Gateway subnet IP address space must be 192.168.1.0/28

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

Wrong Answers:

172.16.0.0/16 and 172.16.1.0/28 - Overlaps with on-premises IP address space.

172.16.0.0/16 and 192.168.0.0/24 - Overlaps with on-premises IP address space.

172.16.1.0/28 and 192.168.0.0/24 - Overlaps with on-premises IP address space.

192.168.0.0/24 and 172.16.1.0/28 - Overlaps with on-premises IP address space.

QUESTION 6

You have an Azure subscription that contains an Azure Front Door named FD1.

You plan to deploy an app named App1 by using Azure App Service. Users will access App1 by using FD1.

You need to provide FD1 with access to App1. The solution must meet the following requirements:

1.

Ensure that users can only access App1 by using FD1.

2.

Ensure that users cannot access App1 directly from the internet. What should you create for App1?

A. an access restriction

B. a private endpoint

C. a subnet delegation

D. a service endpoint

Correct Answer: A

Create a Rule pointing to Azure Front Door https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/ba-p/2000173

QUESTION 7

You plan to use VNET4 for an Azure API Management implementation.

You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canada. You do NOT need to create 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

Azure Front Door web application firewall (WAF) protects web applications from common vulnerabilities and exploits. Azure-managed rule sets provide an easy way to deploy protection against a common set of security threats.

You can restrict access to your web applications by country/region.

Plan:

Stage 1: Create a WAF policy Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

First, 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:

* details omitted *

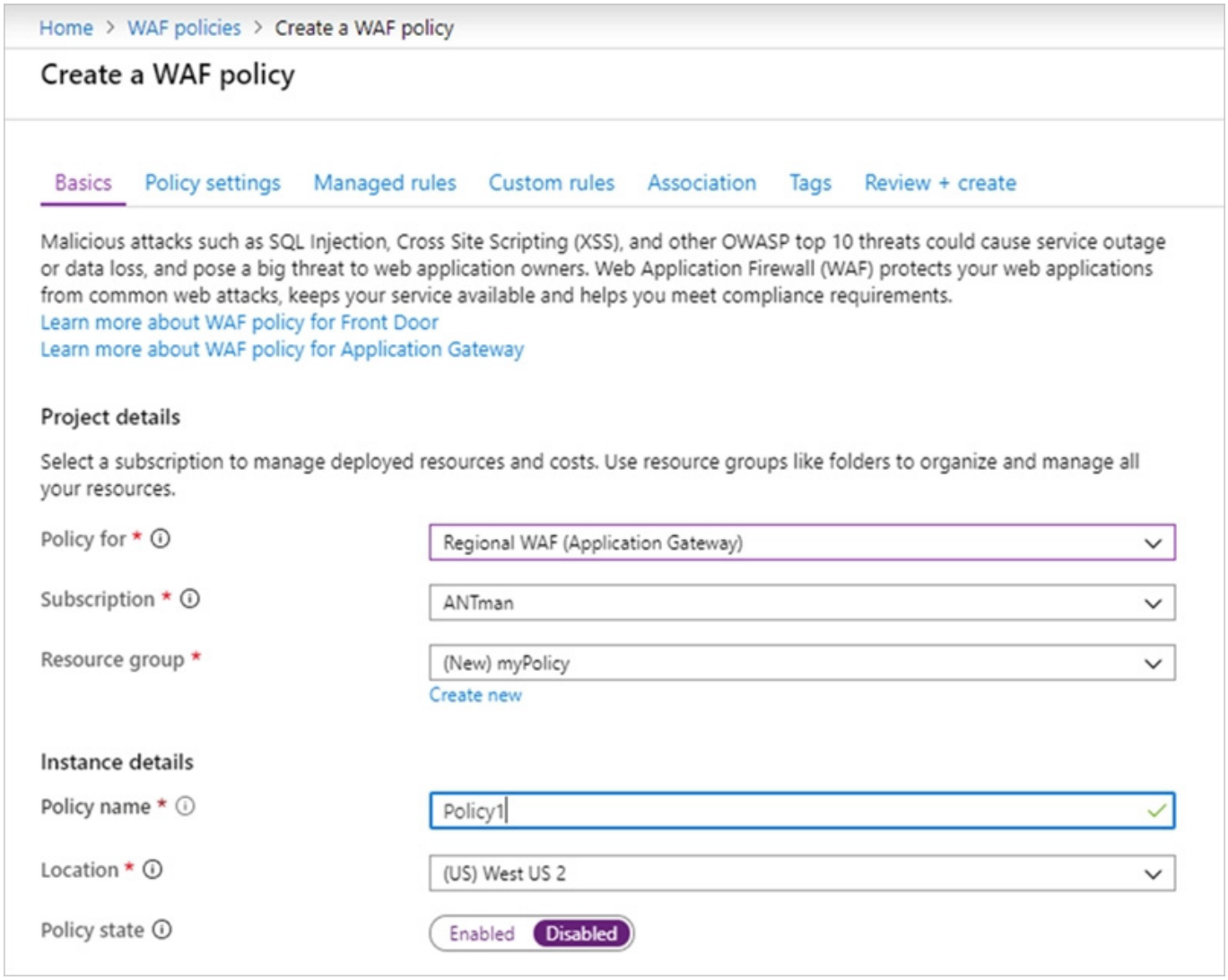
Step 3: On the Association tab, select Add association, then select one of the following settings:

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.

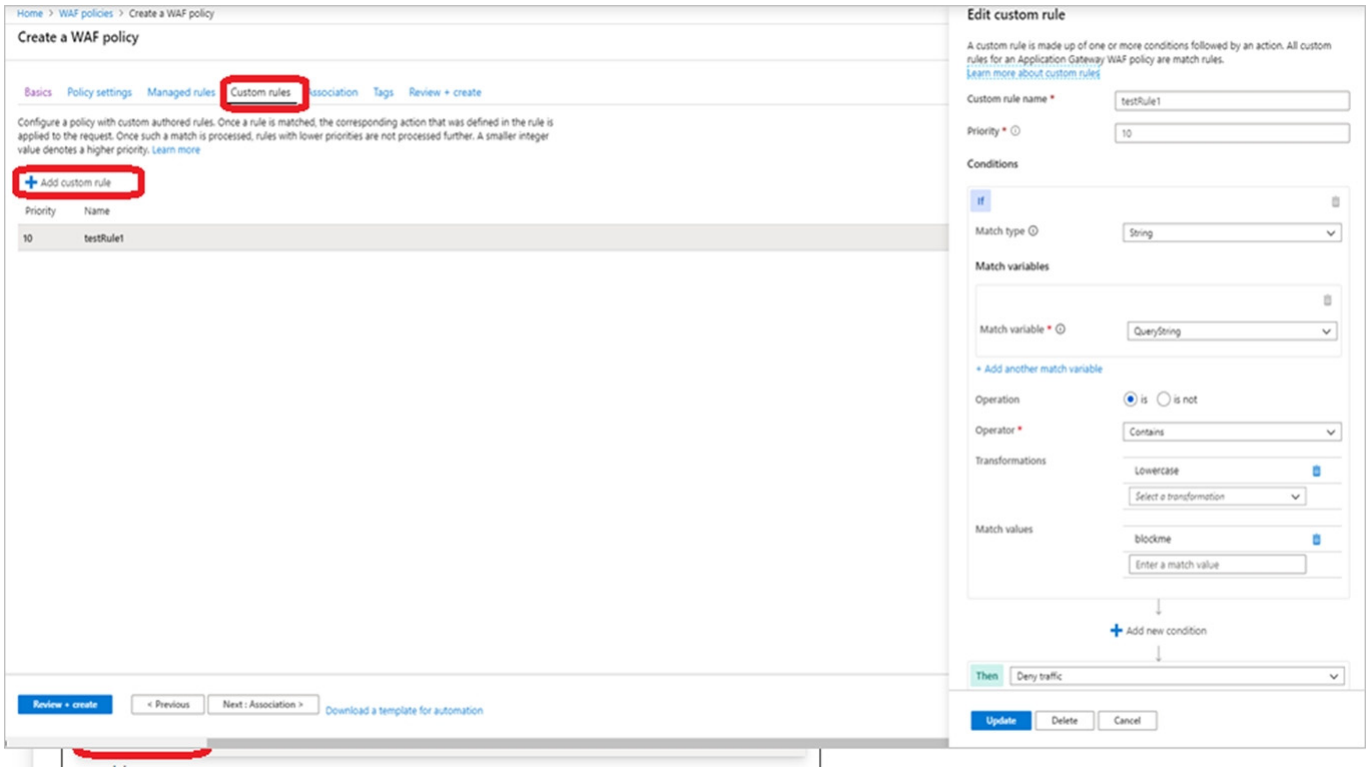
Step 4: Select Review + create, then select Create.



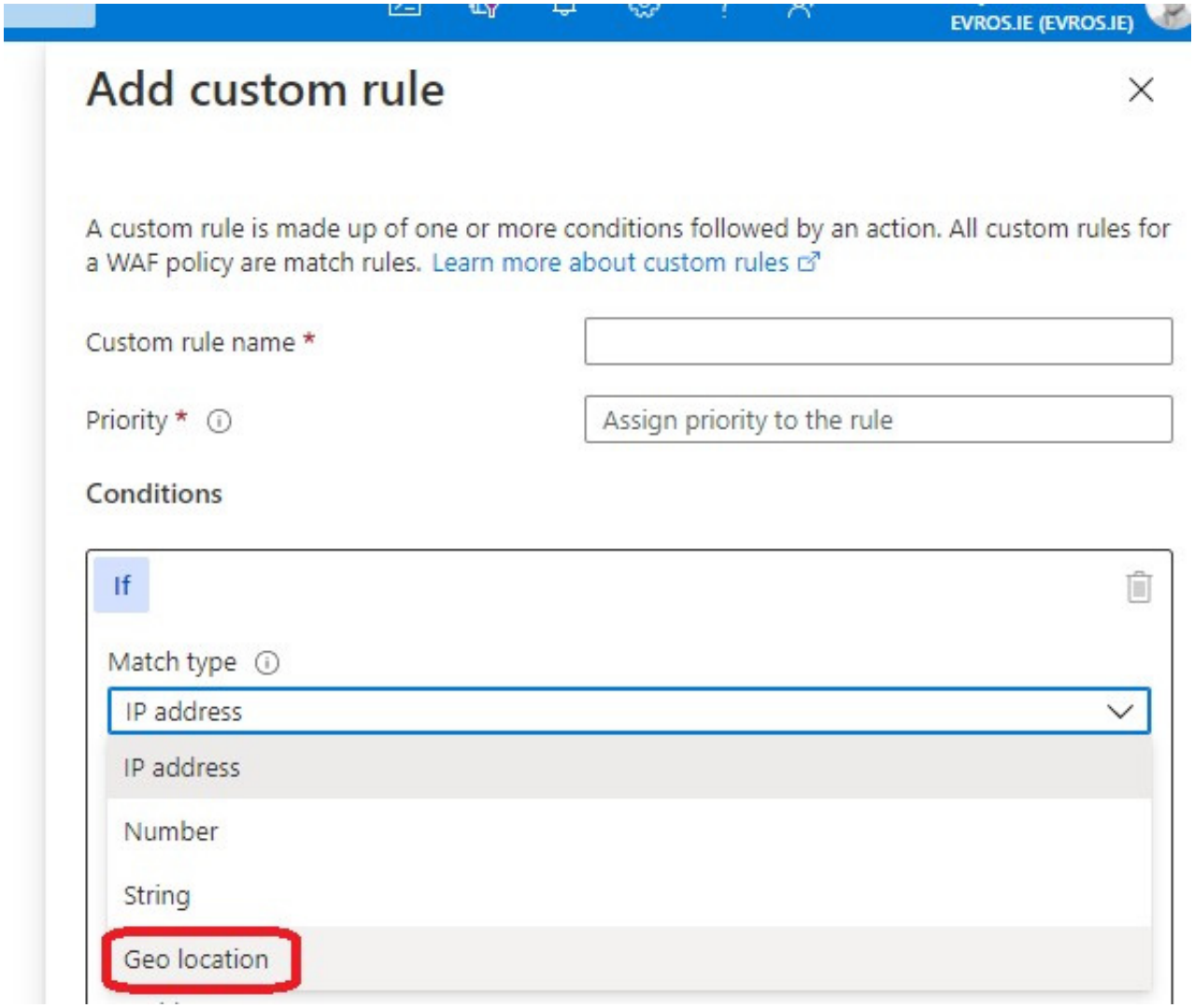
Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada Configure WAF rules When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn\\'t block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, 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.



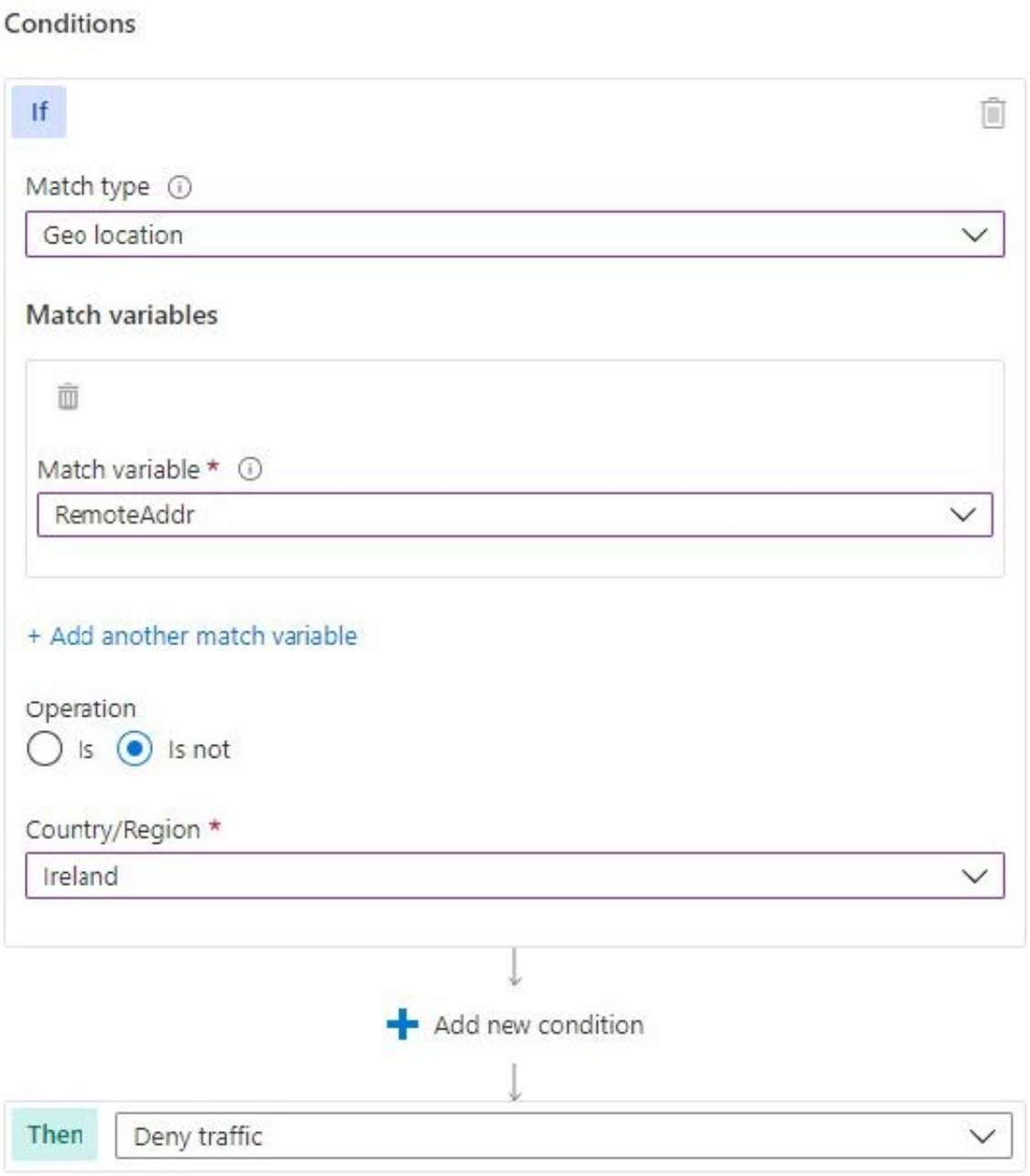
Step 6: To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application. Step 7: Select Add Custom rule



Step 8: Select Geo location

Create your Custom Rule with an appropriate name and priority, then choose 'Geo location' from the Match type drop down as above. Next, you'll want to ensure you choose RemoteAddr as the match variable, and decide what logic you want to apply. By logic I mean the pattern that will fire the rule. In this example, I want all traffic except Ireland blocked. So I will choose the Operation 'Is not', then location Ireland, then Deny. If I wanted all traffic allowed and Ireland blocked, I would simply choose the Operation 'Is'. I recommend figuring out your pattern then working your way through the final section of the CR.

Step 9: Set Match variable to Canada, choose IS NOT, Choose country Canada, and finally Then: Deny traffic.



Step 10: Repeat steps 5 to 9 but instead use: Operation: IS Country/Region: Canada Then: Allow traffic

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

Step 11: Finish the creation of the policy. Click Review+Create

Reference: https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-drs
https://wedoazure.ie/2021/08/09/how-to-enable-web-application-firewall-geomatch-custom-rules/
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag

QUESTION 8

HOTSPOT

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

Name	Type	Description
appservice1	Azure App Service	Hosts an app named App1
contoso.com	Azure DNS zone	Resolves name requests from the internet
FD1	Azure Front Door	Standard profile with App1 configured as the origin
KeyVault1	Azure Key Vault	Key vault with Permission model set to **Vault access policy**
KeyVault2	Azure Key Vault	Key vault with Permission model set to **Azure role-based access control**

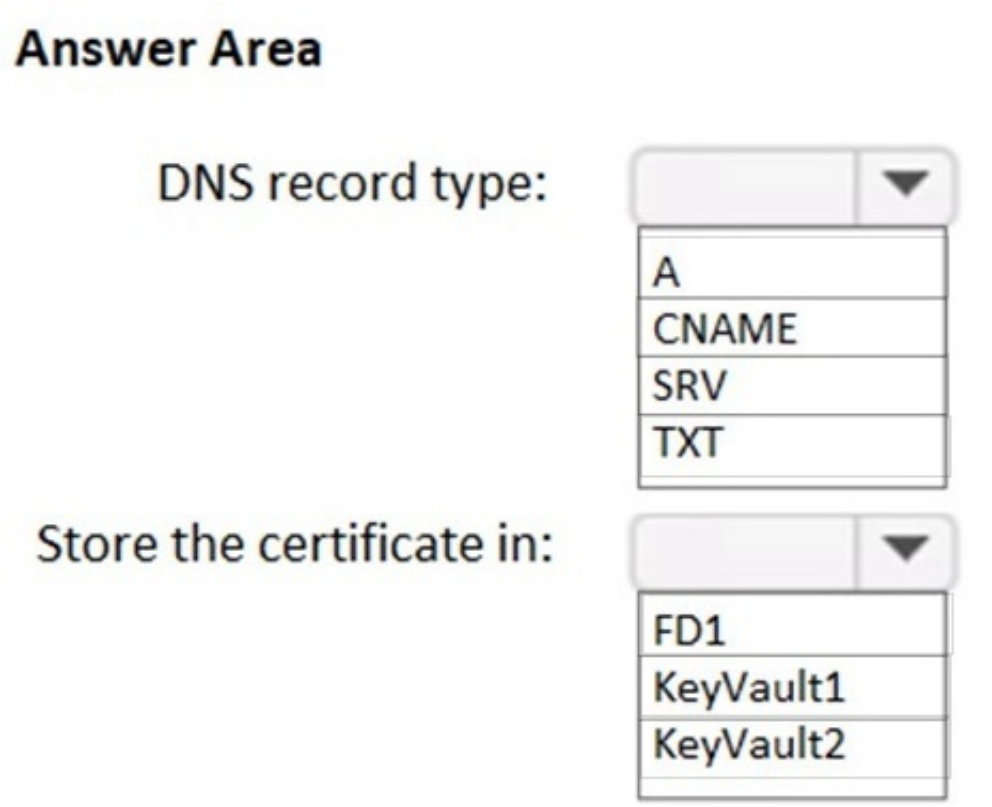
You purchase a certificate for app1.contoso.com from a public certification authority (CA) and install the certificate on appservice1.

You need to ensure that App1 can be accessed by using a URL of https://app1.contoso.com. The solution must ensure that all the traffic for App1 is routed via FD1.

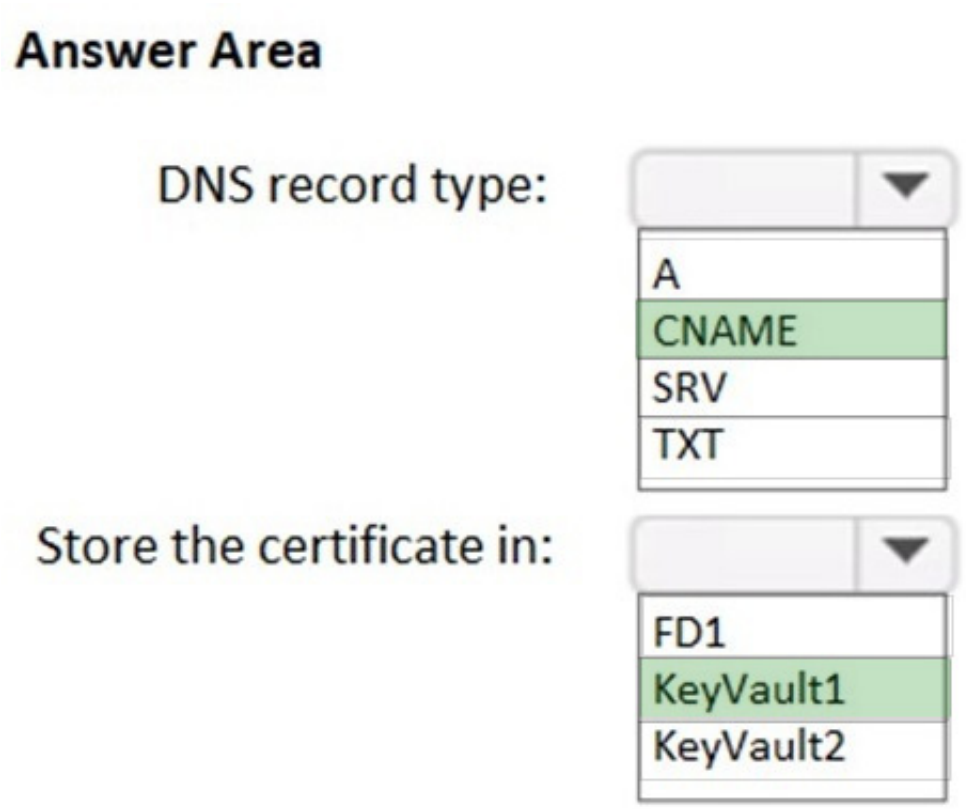
Which type of DNS record should you create, and where should you store the certificate? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



DNS: CNAME (When you added a custom domain to your Front Door\\'s frontend hosts, you created a CNAME record in the DNS table of your domain registrar to map it to your Front Door\\'s default .azurefd.net hostname)

Store certificate in: KeyVault1 (Your key vault must be configured to use the Key Vault access policy permission model.)

There you have a link with all explained https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https.

QUESTION 9

You have a web application that uses a hostname of www.healthengine.com

You have an Azure Front Door instance that provides access to the web application.

You have the routing rules shown in the following table.

Name	Path
RuleA	/abc/def
RuleB	/ab
RuleC	/*
RuleD	/abc/*

Which rule will apply to www.healthengine.com/abc/def incoming request?

A. RuleA

B. RuleB

C. RuleC

D. RuleD

Correct Answer: A

Correct Answer(s):

RuleA - When a request lands on a Front Door environment one of the first things that Front Door does is determine which particular routing rule to match the request to and then take the defined action in the configuration. It uses the below

logic.

Look for any routing rule with an exact match on the Path.

If no exact match Paths, look for routing rules with a wildcard Path that matches.

If no routing rules are found with a matching Path, then reject the request and return a 400: Bad Request error HTTP response.

The path defined in RuleA is an exact match.

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-route-matching

Wrong Answers:

RuleB The path defined in the RuleB is not a match with incoming request.

RuleC There is an exact match with RuleA. The path defined in the RuleB is not an exact match with incoming request.

RuleD There is an exact match with RuleA. The path defined in the RuleB is not an exact match with incoming request.

QUESTION 10

Which three actions should you perform in sequence from the below list of actions?

1.

Create a health probe

2.

Create a public load balancer in the Standard SKU

3.

Create a public load balancer in the Basic SKU

4.

Create a backend pool that contains VMScaleSet1

5.

Create a NAT rule

6.

Create an outbound rule

A. 1,4,6

B. 3,4,5

C. 3,4,6

D. 2,4,6

E. 2,4,5

Correct Answer: D

Only standard SKU load balancer supports outbound connections.

The backend pool must be VMScaleSet1 since the requirement is to implement outbound connectivity for VMScaleSet1.

Outbound rules allow you to explicitly define SNAT(source network address translation) for a public standard load balancer.

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

https://docs.microsoft.com/en-us/azure/load-balancer/outbound-rules

QUESTION 11

You have an Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You disable the WAF rule that has a ruleId 920300.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 12

You have an Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

You configure the application gateway to direct traffic to the URL of the application gateway.

You attempt to access the URL and receive an HTTP 403 error. You view the diagnostics log and discover the following error.

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You create a WAF policy exclusion request headers that contain 137.135.10.24.

Does this meet the goat?

A. Yes

B. No

Correct Answer: B

QUESTION 13

You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure NAT Gateway.

Does this meet the requirement?

A. Yes

B. No

Correct Answer: B

Explanation:

Correct Solution: You implement Azure Firewall.

What is a secured virtual hub?

A virtual hub is a Microsoft-managed virtual network that enables connectivity from other resources. When a virtual hub is created from a Virtual WAN in the Azure portal, a virtual hub VNet and gateways (optional) are created as its

components.

A secured virtual hub is an Azure Virtual WAN Hub with associated security and routing policies configured by Azure Firewall Manager.

Create a secured virtual hub

Using Firewall Manager in the Azure portal, you can either create a new secured virtual hub, or convert an existing virtual hub that you previously created using Azure Virtual WAN.

Reference:

https://learn.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub

QUESTION 14

HOTSPOT

You have an Azure subscription that contains an Azure Firewall policy named FWPolicy1.

You need to configure FWPolicy1 to meet the following requirements:

Allow traffic based on the FQDN of the destination.

Allow TCP traffic based on the source.

Which types of rules should you use for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Allow traffic based on the FQDN of the destination:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic based on the source:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Correct Answer:

Answer Area

Allow traffic based on the FQDN of the destination:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic based on the source:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Explanation:

Box 1: Application only

Allow traffic based on the FQDN of the destination.

You can use an FQDN tag in application rules to allow the required outbound network traffic through your firewall. For example, to manually allow Windows Update network traffic through your firewall, you need to create multiple application

rules per the Microsoft documentation. Using FQDN tags, you can create an application rule, include the Windows Updates tag, and now network traffic to Microsoft Windows Update endpoints can flow through your firewall.

Box 2: Network or DNAT only

Allow TCP traffic based on the source.

There are three types of rule collections:

Application rules: Configure fully qualified domain names (FQDNs) that can be accessed from a Virtual Network.

Network rules: Configure rules that contain source addresses, protocols, destination ports, and destination addresses.

NAT rules: Configure DNAT rules to allow incoming Internet connections.

Note NAT:

Microsoft refers to the form of NAT as being Destination Network Address Translation (DNAT). The rules work with the following parameters:

Name: A label for the rule.

*-> Protocol: TCP or UDP.

Source Address: * (Internet), a specific Internet address, or a CIDR block.

Destination Address: Expect this to be renamed – this refers to the external address of the firewall that the rule will inspect.

Destination Ports: The TCP or UDP ports that the rule will listen to on the external IP address of the firewall.

Translated Address: The IP address of the service (virtual machine, internal load balancer, and so on) that privately hosts or presents the service.

Translated Port: The port that the inbound traffic will be routed to by the Azure Firewall.

Reference:

https://learn.microsoft.com/en-us/azure/firewall/fqdn-tags

https://learn.microsoft.com/en-us/azure/firewall/firewall-faq

https://petri.com/the-three-different-types-of-rules-that-are-in-the-azure-firewall/

QUESTION 15

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